

DeepSec CfP Submissions

René Pfeiffer

deepsec@deepsec.net

+43.676.5626390, +43.720.349387, +43.1.5036081

deepsec.net

July 16, 2009

DEEPSEC

This is an automatically generated document from the Call for Papers database. Please mind the date stamp on the cover page and check for updates.

Contents

1	Presentations and Talks	10
1.1	Leveraging Python to Attack Anything (Presentation)	10
1.1.1	Sample	10
1.1.2	Synopsis	10
1.1.3	Biography	10
1.1.4	Innovation	10
1.2	Tactical Exposure : Web Malware Ontology (Presentation)	11
1.2.1	Sample	11
1.2.2	Synopsis	11
1.2.3	Biography	12
1.2.4	Innovation	12
1.3	Untamed XSS Wars - Filters vs Payloads (Presentation)	13
1.3.1	Sample	13
1.3.2	Synopsis	13
1.3.3	Biography	15
1.3.4	Innovation	15
1.4	What if? Simulation of a large-scale network under attack (Presentation)	15
1.4.1	Sample	15
1.4.2	Synopsis	15
1.4.3	Biography	15
1.4.4	Innovation	16
1.5	Anti-malware protection bypassing techniques (Presentation)	16
1.5.1	Sample	16
1.5.2	Synopsis	16
1.5.3	Biography	16
1.5.4	Innovation	16
1.6	Security 2.0 - a different approach to security (Presentation)	16
1.6.1	Sample	17
1.6.2	Synopsis	17
1.6.3	Biography	17
1.6.4	Innovation	17
1.7	#TwitterRisks: Bot C&C, Data Loss, Intel Collection & More (Presentation)	17
1.7.1	Sample	17
1.7.2	Synopsis	17
1.7.3	Biography	18
1.7.4	Innovation	18
1.8	45' - 60' (Presentation)	18
1.8.1	Sample	18
1.8.2	Synopsis	19
1.8.3	Biography	19
1.8.4	Innovation	19
1.9	Breaking software protections - The hacker techniques (Presentation)	19

1.9.1	Sample	19
1.9.2	Synopsis	19
1.9.3	Biography	19
1.9.4	Innovation	20
1.10	NOSSL - Killing the Man in the Middle (Presentation)	20
1.10.1	Sample	20
1.10.2	Synopsis	20
1.10.3	Biography	20
1.10.4	Innovation	21
1.11	Unicode Transformations: Finding Elusive Vulnerabilities in Software (Presentation)	21
1.11.1	Sample	21
1.11.2	Synopsis	21
1.11.3	Biography	22
1.11.4	Innovation	22
1.12	Flawed shutdown policies and implication to security (Presentation)	22
1.12.1	Sample	22
1.12.2	Synopsis	22
1.12.3	Biography	22
1.12.4	Innovation	23
1.13	Dynamic Binary Instrumentation for Deobfuscation and Unpacking (Presentation)	23
1.13.1	Sample	23
1.13.2	Synopsis	23
1.13.3	Biography	23
1.13.4	Innovation	23
1.14	Mobile phone forensic (Presentation)	23
1.14.1	Sample	24
1.14.2	Synopsis	24
1.14.3	Biography	24
1.14.4	Innovation	24
1.15	Security on the GSM Air Interface (Training)	24
1.15.1	Sample	24
1.15.2	Synopsis	25
1.15.3	Biography	25
1.15.4	Innovation	25
1.16	"Hackerspaces: Friend or Foe, the new thrill in private and public research" (Presentation)	25
1.16.1	Sample	25
1.16.2	Synopsis	25
1.16.3	Biography	26
1.16.4	Innovation	26
1.17	A Proof-of-Concept Attack on SmartCard-secured Online-Banking (Presentation)	26
1.17.1	Sample	26

1.17.2	Synopsis	26
1.17.3	Biography	27
1.17.4	Innovation	27
1.18	Windows Secure Kernel Development (Presentation)	27
1.18.1	Sample	27
1.18.2	Synopsis	27
1.18.3	Biography	27
1.18.4	Innovation	28
1.19	Results of a security assessment of the TCP and IP protocols and common implementation strategies (Presentation)	28
1.19.1	Sample	28
1.19.2	Synopsis	28
1.19.3	Biography	28
1.19.4	Innovation	29
1.20	Security Talk From The World's No. 1 Hacker! (Presentation)	30
1.20.1	Sample	30
1.20.2	Synopsis	30
1.20.3	Biography	30
1.20.4	Innovation	31
1.21	Ksplice: Patch without disruption (Presentation)	32
1.21.1	Sample	32
1.21.2	Synopsis	32
1.21.3	Biography	32
1.21.4	Innovation	32
1.22	Get your head out of the clouds: Security in Software-plus-Services (Presentation)	32
1.22.1	Sample	33
1.22.2	Synopsis	33
1.22.3	Biography	33
1.22.4	Innovation	33
1.23	Reversing and Exploiting an Apple Firmware Update (Presentation)	34
1.23.1	Sample	34
1.23.2	Synopsis	34
1.23.3	Biography	34
1.23.4	Innovation	34
1.24	Lust 2.0 – Desire for free WiFi and the threat of the Imposter (Presentation)	34
1.24.1	Sample	34
1.24.2	Synopsis	34
1.24.3	Biography	35
1.24.4	Innovation	35
1.25	Playing in a Satellite environment 1.2 (Presentation)	35
1.25.1	Sample	35
1.25.2	Synopsis	35
1.25.3	Biography	35

1.25.4	Innovation	36
1.26	Internet election for the German Bundestag (Presentation)	36
1.26.1	Sample	36
1.26.2	Synopsis	36
1.26.3	Biography	36
1.26.4	Innovation	36
1.27	Key Management Death Match? Competing KM Standards Technical Deep Dive (Presentation)	36
1.27.1	Sample	36
1.27.2	Synopsis	37
1.27.3	Biography	37
1.27.4	Innovation	37
1.28	Breaking Tor sessions with HTML5 (Presentation)	38
1.28.1	Sample	38
1.28.2	Synopsis	38
1.28.3	Biography	38
1.28.4	Innovation	38
1.29	BSD Rootkit Programming (Training)	38
1.29.1	Sample	39
1.29.2	Synopsis	39
1.29.3	Biography	39
1.29.4	Innovation	39
1.30	User input piercing for Cross Site Scripting (Presentation)	39
1.30.1	Sample	39
1.30.2	Synopsis	39
1.30.3	Biography	40
1.30.4	Innovation	40
1.31	Rootkits are awesome: Insider Threat for Fun and Profit (Presentation)	40
1.31.1	Sample	40
1.31.2	Synopsis	40
1.31.3	Biography	40
1.31.4	Innovation	41
1.32	Unicode Shellcode 2.0: New methods, algorithms and tool (Presentation)	41
1.32.1	Sample	41
1.32.2	Synopsis	41
1.32.3	Biography	41
1.32.4	Innovation	41
1.33	USB Device Drivers: A Stepping Stone into your Kernel (Presentation)	42
1.33.1	Sample	42
1.33.2	Synopsis	42
1.33.3	Biography	42
1.33.4	Innovation	43
1.34	Evaluating Secure Protocols and Intercepting Secure Communication (Training)	43
1.34.1	Sample	43

1.34.2	Synopsis	43
1.34.3	Biography	43
1.34.4	Innovation	44
1.35	Advance MySQL Exploitation (Presentation)	44
1.35.1	Sample	44
1.35.2	Synopsis	44
1.35.3	Biography	44
1.35.4	Innovation	44
1.36	VOIP, Operating System Security,WLAN/WiFi, GPRS, IPv6 and 3G Security,Security Management (Training)	45
1.36.1	Sample	45
1.36.2	Synopsis	45
1.36.3	Biography	45
1.36.4	Innovation	45
1.37	Tuning of ACO Algorithms for optimization solution Using TSP (Presentation)	45
1.37.1	Sample	45
1.37.2	Synopsis	45
1.37.3	Biography	45
1.37.4	Innovation	46
1.38	Top 10 Security Issues Developers Don't Know About (Presentation)	46
1.38.1	Sample	46
1.38.2	Synopsis	46
1.38.3	Biography	46
1.38.4	Innovation	47
1.39	Thick Client Application (In)Security (Presentation)	47
1.39.1	Sample	47
1.39.2	Synopsis	47
1.39.3	Biography	48
1.39.4	Innovation	48
1.40	Outspect: live memory forensic for Virtual machine (Presentation)	49
1.40.1	Sample	49
1.40.2	Synopsis	49
1.40.3	Biography	49
1.40.4	Innovation	49
1.41	eKimono: detecting rootkits inside Virtual Machine (Presentation)	50
1.41.1	Sample	50
1.41.2	Synopsis	50
1.41.3	Biography	50
1.41.4	Innovation	50
1.42	The Dark Side of the Fox: Abusing Firefox Extensions (Presentation)	51
1.42.1	Sample	51
1.42.2	Synopsis	51
1.42.3	Biography	51
1.42.4	Innovation	51

1.43	Stoned Bootkit: Your PC is now Stoned! ..again (Presentation)	52
1.43.1	Sample	52
1.43.2	Synopsis	52
1.43.3	Biography	52
1.43.4	Innovation	52
1.44	HostileWRT: Turn Your Friendly Wireless Access Point into an Autonomous, Curious, Standalone, ... (Presentation)	52
1.44.1	Sample	53
1.44.2	Synopsis	53
1.44.3	Biography	53
1.44.4	Innovation	53
1.45	The Worries of Today (Presentation)	54
1.45.1	Sample	54
1.45.2	Synopsis	54
1.45.3	Biography	54
1.45.4	Innovation	54
1.46	Living on the Edge: The Sources of Creativity (Presentation)	54
1.46.1	Sample	54
1.46.2	Synopsis	54
1.46.3	Biography	55
1.46.4	Innovation	55
1.47	Hacking, Biohacking, and the Future of Humanity (Presentation)	55
1.47.1	Sample	55
1.47.2	Synopsis	55
1.47.3	Biography	56
1.47.4	Innovation	56
1.48	WebAppSec.php: Developing Secure Web Applications (Training)	57
1.48.1	Sample	57
1.48.2	Synopsis	57
1.48.3	Biography	57
1.48.4	Innovation	57
1.49	Hijacking Mobile Data Connections 2.0: Automated and Improved (Presentation)	58
1.49.1	Sample	58
1.49.2	Synopsis	58
1.49.3	Biography	58
1.49.4	Innovation	59
1.50	Web Application Vulnerabilities and Countermeasures (Training)	59
1.50.1	Sample	59
1.50.2	Synopsis	59
1.50.3	Biography	60
1.50.4	Innovation	61
1.51	Essential Computer Forensic with FOSS Tools (Training)	61
1.51.1	Sample	61
1.51.2	Synopsis	61

1.51.3	Biography	62
1.51.4	Innovation	63
1.52	Ownage 2.0 (Presentation)	63
1.52.1	Sample	64
1.52.2	Synopsis	64
1.52.3	Biography	64
1.52.4	Innovation	64
1.53	Sticking it to the Airlines (Hacker Lounge)	65
1.53.1	Sample	65
1.53.2	Synopsis	65
1.53.3	Biography	65
1.53.4	Innovation	65
1.54	Social Engineering Training for IT Security Professionals (Training)	65
1.54.1	Sample	65
1.54.2	Synopsis	66
1.54.3	Biography	66
1.54.4	Innovation	67
1.55	Web 2.0 Security – Advanced Attacks and Defense (Training)	67
1.55.1	Sample	67
1.55.2	Synopsis	67
1.55.3	Biography	68
1.55.4	Innovation	68
1.56	Security Awareness Campaigns (Training)	68
1.56.1	Sample	69
1.56.2	Synopsis	69
1.56.3	Biography	69
1.56.4	Innovation	69
1.57	The Developmental Psychology of Intrusion Detection Systems (Pre- sentation)	69
1.57.1	Sample	69
1.57.2	Synopsis	69
1.57.3	Biography	70
1.57.4	Innovation	70
1.58	Recent trends in VoIP security and its countermeasures (Presentation)	70
1.58.1	Sample	70
1.58.2	Synopsis	70
1.58.3	Biography	71
1.58.4	Innovation	71
1.59	Open source for securing data with advanced Crypto-Steganography technology (Presentation)	71
1.59.1	Sample	71
1.59.2	Synopsis	71
1.59.3	Biography	72
1.59.4	Innovation	72

1.60	Keykeriki - Universal Wireless Keyboard Sniffing For The Masses (Presentation)	72
1.60.1	Sample	72
1.60.2	Synopsis	72
1.60.3	Biography	73
1.60.4	Innovation	73
1.61	Exploit Analysis and Malware Reverse Engineering (Training)	73
1.61.1	Sample	73
1.61.2	Synopsis	73
1.61.3	Biography	73
1.61.4	Innovation	73
1.62	Enterprise Web Application Security - Attacks & Defense (Training)	74
1.62.1	Sample	74
1.62.2	Synopsis	74
1.62.3	Biography	75
1.62.4	Innovation	75
1.63	Malware for SoHo Routers - The war has begun (Presentation)	76
1.63.1	Sample	76
1.63.2	Synopsis	76
1.63.3	Biography	76
1.63.4	Innovation	76
1.64	Malware case study: The Zeus evolution (Presentation)	76
1.64.1	Sample	77
1.64.2	Synopsis	77
1.64.3	Biography	77
1.64.4	Innovation	77

1 Presentations and Talks

1.1 Leveraging Python to Attack Anything (Presentation)

Adam Pridgen	adam.pridgen@thecoverofnight.com
The Cover of Night	
1.512.809.7615	US

1.1.1 Sample

thecoverofnight.com

1.1.2 Synopsis

Python is the language of choice for --over-the-hill-hackers-- and this presentation will show why. In this presentation, we will outline how to research various issues, analyze data, and build your own attack tools and scripts on the fly. As part of the project, I will discuss a process for rapid research and development for attack tools that I use regularly. The talk will make use of what I learned and where I failed, and how I used that to succeed. The talk will highlight some success stories, but it will also show some shortcomings in the process. Some of my success stories include a rapid host resolution script that can resolve about 1000 IPs/minute over Tor. Another tool development process I will discuss is my Python .Net ViewState 2.0 decoder. From my grab bag, I also have failures such as my failed pyElf project or my failed project to turn Sulley into a Web App fuzzer.

1.1.3 Biography

Adam Pridgen is a hacker that likes to hang back and let his mind race. He develops and prototypes Python tools and scripts daily. He has done some work with reverse engineering the .Net LoS Format, developed scripts to help analyze vulnerability assessments, and developing one-off scripts to make life a little easier. He has also developed several academic research projects combining digital forensics and text mining and trusted computing and mobile agents. Aside from be an underdosed caffiene dependent, Adam has held a variety of positions in IT and security domain and is currently a freelance security consultant.

1.1.4 Innovation

it draws on my experience as a pen-tester, researcher, and a programmer. I actively treat pen-testing as a programming challenge, and I develop tools and scripts to help me automate, verify, and even mine systems for information. I have done things such as developing a basic Mobile Agent Platform on Python and developed code and tools based around common security frameworks, and I have experience with combining frameworks, such as Scapy and Sulley, to help leverage their strengths. Another thing that this presentation draws on are my failures. While I have not completed or released many of my tools, my presentation also draws how or why I was unable to complete some tools or projects.

1.2 Tactical Exposure : Web Malware Ontology (Presentation)

Aditya K Sood adi.zerok@gmail.com Founder SecNiche Security / Independent Security Re- searcher / Security Advisor KPMG 91-98738-90299 India Asia Pacific
--

1.2.1 Sample

No it is structured specifically.

1.2.2 Synopsis

Note: The talk sheds light on the new trends of web based malware. Technology and Insecurity goes hand in hand. With the advent of new attacks and techniques the distribution of malware through web has been increased tremendously. Browser based exploits mainly Internet Explorer have given a birth to new world of malware infection. The attackers spread malware elegantly by exploiting the vulnerabilities and drive by downloads. The infection strategies opted by attackers like malware distribution through IFRAME injections and Search Engine Optimization. In order to understand the intrinsic behavior of these web based malware a typical analysis is required to understand the logic concept working behind these web based malwares. It is necessary to dissect these malwares from bottom to top in order to control the devastating behavior. The talk will cover structured methodologies and demonstrate the static, dynamic and behavioral analysis of web malware including PCAP analytics. Demonstrations will prove the fact and necessity of web malware analysis. The under stated part will discuss about in brief regarding the Web Malware Methodology.

=====
Analysis Methodology ===== Brief Overview of - Web Malware
methodology covers the generic steps that are required to be followed while analyzing PCAP's for the exploits and malwares. To perform an analysis of capture packets below mentioned steps should be followed. 1. End Point Communication: ===== The very basic step in analyzing a PCAP is to understand the end to end point communication. Based on client server architecture, an analyst has to determine the machines that are communicating and the port numbers in use. The protocols used for communication and their dependency behavior should be checked. Once the generic information is collected below mentioned issues should be taken care of: 1.1 Premature Truncation of Connection. 1.2 Server Identity checks through communication medium. 1.3 Error Generation like Checksum Integrity. 1.4 Encrypted Data in packets. 1.5 Protocol Switching. This presents us with the communication flow. 2. Session Stream Analysis { Deep Inspection
===== The second step to be followed is analysis of the session in progress when PCAP is generated from egress/ingress filtering. The analyst tries to understand the request response mechanism used between client and server. During the stream analysis, it is necessary to check the responses when a particular request is sent to the server. The packet frequency determines the strength of connection with the server from client side. Deep inspection of HTTP parameters and the data present in it explains the nature of the running stream. For Example check the number of bytes transferred in one session. Analyze the secure tunnels used for traffic encryption. It is necessary to scrutinize the file downloading procedure if it is happening through captured packets. 3. Behavioral Analysis

===== This is a major step which explains the behavior of captured packets in detail. After performing above mentioned steps the packets behavior should be explained. In this step, we not only decide the impact on the system but also check for the third part binaries requested by the client, mainly malwares. For Example: If a client is requesting a binary or PE (Portable Executable) and the PCAP has required set of data (mainly present in hexadecimal), it should be extracted accurately out of the raw data with the help of Hex Editor. The analyst should search for two byte header MZ (\$4D5A in hex) which begins at a certain offset to trace the starting point of PE. The analyst has to delete all the other raw data from top to bottom except the executable file. As a result of it, PE file is ready for analysis. Try to execute that file in a virtual machine to analyze the impact on the base operating system to determine the ingrained behavior. 4. Statistical Analysis ===== If the file is executable, one has to perform statistical analysis through disassembler to understand the functioning of the downloaded file. Always use Dump bin to locate the sections and other binary related information. There is stringency if data is present in Unicode, most of the tools do not support this encoding. The object entry point is required for analysis which can be extracted as: 1. IDA Pro SDK ships with EPF i.e. Entry Point Finder 2. Use Dump Segment Plug-in to dump all the segments. The detection of entry point is critical in malware analysis. Follow the approach of standard binary analysis with in core Debugging. If the JavaScript is detected for any rogue functioning by malwares, trace the source through raw data and download it for analysis. Always check for obfuscated code in it. The above presented layout is the brief outline of the web malware analysis methodology. We will also talk about browser based vulnerabilities that diversifies the attack pattern thereby increasing the malware infection on internet. 5. Packer Analysis ===== Analyzing the Packers used to pack the malware and other hindrances in analyzing the malware. The audience will learn the new aspects of web malware analysis and nurture the concepts by the demonstration given. This is the brief overview of methodology to give a flavor of this talk.

1.2.3 Biography

Aditya K Sood is the founder of SecNiche Security. He is an independent security researcher having an experience of more than 6 years. He holds BE and MS in Cyber Law and Information Security. He is an active speaker at conferences like EuSecwest, XCON, XKungfoo, OWASP, Clubhack, Troopers ,CERT-IN etc. He has written journals for Hakin9, BCS, Usenix and Elsevier. His work has been quoted at eWeek, SCMagazine, ZDNet, internet news etc. He has given number of advisories to fore front companies. On professional front he works for KPMG as a penetration tester. Website: <http://www.secniche.org> Blog: <http://zeroknock.blogspot.com> <http://www.secniche.com>

1.2.4 Innovation

Demonstration Driven. Based on methodology and discuss new trends of malware infection on web.

1.3 Untamed XSS Wars - Filters vs Payloads (Presentation)

Aditya K Sood adi.zerok@gmail.com Security Researcher , Vulnerability Research Labs CO- SEINC 0-98738-90299 INDIA,SINGAPORE
--

1.3.1 Sample

Not Yet

1.3.2 Synopsis

Talk Details: The web is an ever changing arena. The most versatile attack pattern is Cross Site Scripting. Lot of advancements has been taken place in recent times to prevent these attacks. Strategic filters have been designed. The XSS vector is considered to be a randomized vector and is not easy to prevent these attacks. Attackers use definitive payloads to trigger advanced level attacks to bypass filters. The payloads cannot be trusted which is a part of ingrained input into applications. Are the filters smart enough to trace the variants of XSS and preventing the further diversified attacks? The web 2.0 is facing untamed war in relation to XSS. This war is prevailing between the designed filters and attacker driven payloads. This talk will dissect different articulated payloads and design level deficiencies in filters that impact the application flow and robustness. It also sheds deep knowledge about black box reversing of XSS Filters too by following techniques such as Metacharacter Fuzzing etc. Our thinking approach and research is based on below mentioned statements.

[P1] XSS Vector is always randomized. It's very hard to defend it from all perspectives. [P2] No design is perfect. There are certain exceptions where the design fails or allow well definitive attacks. Based on the above stated principles we conduct our research and scrutinize the XSS Filter behavior.

[1] Generic and Articulated Payloads: We will talk in detail about the generic and well crafted payloads that are used to trigger XSS. The payloads are not restricted to single entity but depend on the browser capability too. The payloads are based on the DOM and other HTML specifications. The attacker crafts a payload based on the application design and scrutinizing the responses returned by the web server. We will discuss about the structuring of payloads and which payloads are used effectively to bypass filters.

[2] Real Time and After Fact Correlation XSS Analysis We will discuss in detail about the correlation analysis of the responses sent by web server when a payload is injected into an application. The correlation is based on two specific set of methods which proves beneficial in analyzing the XSS filters. Analyzing reflective XSS responses with the injected payload is a good mechanism of correlation in understanding the flow of application and the way XSS filter works. We have noticed there are certain cases where --Real Time-- analysis proves beneficial. But the --Time Delay-- factor plays a crucial role in scrutinizing the --False Positive-- that comes out of the --heuristic/neuter-- component of XSS Filter. We have tested number of real time websites against reflective XSS which results in ingress testing of XSS Filter.

[3] Design Validation of XSS Filters: Scrutinizing Request/Response The design should be validated in relation to request/response mechanism. Most of the filters design is based on validating the data passed through POST request and the way it is replayed back. It means the heuristics are defined on request/response mechanism. The XSS Filter checks the response sent back by

the server to scan the presence of XSS payload which is reflected back in the browser in the context of domain. Looking at this factor we will determine and analyze the possible way to bypass filters and other design level inaccuracies that impact the behavior of XSS filters with different payloads. If we stick to the [P1] stated above then randomization can lead to bypass this vector too. No doubt generic injections can be neutralized by the filter. [4] Black Box Reversing of XSS Filters: We will talk in detail about the black box reversing of XSS filters through Metacharacter Fuzzing to scrutinize the impact on application flow and resultant analysis on the behavior of filters applied. The use of Meta characters in an appropriate way can thwart the filter functioning to a great extent. We will discuss about the variation of XSS filters with direct linking having a injected payload with meta characters. The insertion of NULL character completely dismantles number of XSS filters by truncating the injected payload. We will discuss the facts and certain issues in relation to black box analysis of XSS filters. [5] The XSS War { Payload or Filters In this part we will demonstrate the different high level attacks that persist in web 2.0 encompassing the different XSS payloads that can thwart the filters too. Being a randomized vector it is not easy to control it fully. Our approach here is to present the way attackers used advanced attack to completely bypass the implement filters and successfully incorporating the payload into the applications and getting a required response. For Example: - We will talk about below mentioned new attack vectors Bypassing XSS Filters with MS Office. We will talk about the evasion of web XSS filters. We will cover the latest approach of pwning web applications through MSWord documents (A new attack vector that has been structured recently. A whitepaper has been released already). This attack is not restricted to only word documents but also covers other Office components too. The web XSS filters present in the enterprise web application are not designed appropriately to trace the injection parameters. Numbers of vendors have been intimated against this XSS vector. This can also be used to launch other variants of XSS including Cross Site Request forging and Remote File Inclusion attacks. It works efficiently in most number of cases. The risk factor and feasibility depends on the ease of victim interacting with the enterprise web application. The attack vector works efficiently with Microsoft word and Open Office. Note: This attack vector is used to detect vulnerabilities in the Oracle E-Business Suite. The vulnerabilities have been reported to Oracle. The vendor is working to fix these vulnerabilities based on the attack vector discussed above. We will demonstrate different attack vectors such as IFRAME injections, CSRF, Malware infection etc through this attack vector. PDF Silent HTTP Form Repurposing Attacks We will talk about another attack vector of pen testing web applications by using PDF documents in uploading functionality in web applications. We will exploit the same domain functions to test the web application security. This attack is termed as PDF Silent HTTP Form Repurposing Attacks. It is based on the execution of inline JavaScript code on the same domain. This attacks work fine on all browsers and all versions of PDF. It uses the inherent functionality of PDF document itself. Due to ingrained security mechanism in PDF Reader, it is hard to launch certain attacks. But with this technique an attacker can steal generic information from website by executing the code directly in the context of the domain where it is uploaded. The attack surface can be diversified by randomizing the attack vector. On further analysis it has been observed that it is possible to trigger phishing attacks too. The detailed paper has already released. Please find it at links structured below: [1]
<http://www.securiteam.com/securityreviews/5MP0D00R5G.html> [2]
http://www.secniche.org/papers/SNS_09_01_Evad_Xss_Filter_Msword.pdf Note: We will completely dissect the Internet Explorer 8 XSS filter and will present our

findings by demonstrating the incapability, false positives on real time websites.

1.3.3 Biography

Aditya K Sood is a Security Researcher at Vulnerability Research Labs (VRL), COSEINC He has been working in the security field for past 7 years. He has written number of whitepapers for Hakin9, Usenix, Elsevier and BCS. He has already spoken number of security conferences including EuSecWest , Xcon ,Xkungfoo, Troopers , Owasp , CERT-In etc. He has released number of advisories to forefront companies. During free time he loves to do lot of web based research and designing cutting edge attack vectors.

1.3.4 Innovation

The research will completely provide a new Trifecta of XSS Filters, Payloads and Advanced attacks.

1.4 What if? Simulation of a large-scale network under attack (Presentation)

Alexei Kachalin a.kachalin@gmail.com
Calc.Math and Cybernetics department of Moscow State
University
+7 (916) 8040895 Russia

1.4.1 Sample

http://lvk.cs.msu.su/~sadman/papers/2009_Confidence_GloNeHyS.pdf

1.4.2 Synopsis

Information Security systems affect network traffic generated both by malware and legitimate software. Virus outbreaks may overload security services as well as network infrastructure. To analyze efficiency of IS systems in global networks simulation is often used, but straight-forward approach (packet-level simulation), while being precise, does not fit for global networks due to high memory demands and computational complexity. To reduce computational complexity hybrid simulation approach could be used. Describing global network and traffic flows on different level of abstraction we could analyze impact of malware activity and attack consequences on network performance. On top of it information security systems could be brought in the model to counter malware.

1.4.3 Biography

Graduated from Moscow State University in 2004, M.Sc in Computer Science and Calculation Math, Ph.D-in-waiting. Areas of expertise: • Network and malware outbreaks simulation • Simulation and modeling for security systems design and performance analysis • Data mining algorithms in attack and virus detection Presently employed at Computer Systems Laboratory

at CMC faculty of Moscow State University as research and development projects manager. Co-leading Network Security seminar for CMC students, provides advisory and critics for security-related research efforts.

1.4.4 Innovation

Interesting problem (malware dynamics in global networks). Original solution of complexity and simulation feasibility.

1.5 Anti-malware protection bypassing techniques (Presentation)

Alisa Shevchenko	alisa@esagelab.com
none / business owner	
+7 (903) 163-35-18	Russia

1.5.1 Sample

The presentation is not ready yet. This is a continued research. You can find earlier outline of the same research in the InSecure Mag \#17:
<http://www.net-security.org/dl/insecure/INSECURE-Mag-17.pdf>

1.5.2 Synopsis

The talk will be focusing on programming techniques embedded in advanced malware and allowing anti-malware protection bypassing. The talk will include:
* a retrospective review of such techniques found in real malware; * a review of the most modern techniques, those causing headaches to antivirus vendors; * a generalization of approaches used by malware developers aiming to attain timely protection bypassing.

1.5.3 Biography

Into security since 15 years old. Kaspersky Lab virus analyst / security researcher for 4 years, until 2008. Currently running my own IT security consulting firm named eSage Lab. Specialities: advanced malware, protection bypassing, rootkits.

1.5.4 Innovation

because it aims at revealing the very nature of protection bypassing, which is an timeless quest :)

1.6 Security 2.0 - a different approach to security (Presentation)

Arshad Noor	arshad.noor@strongauth.com
StrongAuth, Inc.	
+11 (408) 331-2001	USA

1.6.1 Sample

This is a new talk, so the material for this talk is not available on the internet yet.

1.6.2 Synopsis

After 20 years of securing the network and hosts, we have failed abysmally. While we have the appropriate defense mechanisms/technologies available to solve the problem, we lack the vision and road-map to securing our data. This presentation shows what the important components of Security 2.0 are, and how to implement the solution.

1.6.3 Biography

Arshad Noor is the CTO of StrongAuth, Inc., a Cupertino, CA-based company that specializes in enterprise key-management. he is the architect and lead-developer of StrongKey, the industry's first open-source Symmetric Key Management System (SKMS) for managing encryption keys across the enterprise.

1.6.4 Innovation

I am neither a computer scientist nor a security expert. I am a self-taught computer hobbyist and have a different way of looking at problems towards solving them.

1.7 #TwitterRisks: Bot C&C, Data Loss, Intel Collection & More (Presentation)

Ben Feinstein	bfeinstein@secureworks.com
SecureWorks	
+1 678-772-4126	USA

1.7.1 Sample

N/A

1.7.2 Synopsis

Twitter is an immensely popular web service for social networking and interaction. In 140 characters or less, millions of users are routinely sharing the intimate details of their daily lives. The popularity of this service has created new opportunities for mischief. Twitter's set of well-defined APIs makes it relatively straight forward for one to programatically automate all sorts of interactions with the service, including malicious ones. This talk will explore the risks that Twitter represents both to the individual user, as well as to an Organization. For an individual, their Twitter timeline can reveal a wealth of sensitive information. For example, the profile of many Twitter users publicly discloses their current physical location down to 10^{-6} of a degree of longitude and latitude. An individual's Twitter network can be used to map their personal and professional

interrelationships. Sensitive information regarding an individual can be reliably deduced through inference, such as their employer, job responsibilities, and the projects they work on. Such information falls under the purview of open source intelligence gathering, a process now routine for both pen-testers and true adversaries. Twitter has proven useful for political dissidents to covertly coordinate their activities and reliably disseminate information. The same properties that make Twitter attractive to political dissidents also make it well suited for use as a distributed, resilient, stealthy and scalable botnet command and control mechanism. A hierarchy of Twitter --followers-- can be used to provide for resiliency in the face of takedowns, and to effectively partition a botnet. Twitter updates (tweets) can be used to send commands to an entire whole botnet or to just an individual bot. Tweets can also be used by individual bots to communicate the result of a command back to the botnet master, and to exfiltrate data from the compromised host in 140 character chunks. The talk will include demonstrations of these concepts. Proof-of-concept code will be made available under the GPL.

1.7.3 Biography

Ben Feinstein is a Director with the SecureWorks Counter Threat Unit (SM). He first became involved in information security in 2000, working on a DARPA / US Air Force contract when he should have been spending more time in lecture. Ben is the author of RFC 4765 and RFC 4767. He has nearly a decade of experience designing and implementing security-related information systems. Ben's major areas of expertise include IDS/IPS, digital forensics and incident response, secure messaging, and small caliber arms. In the past, he has presented at Black Hat USA, DEFCON, ToorCon, ACSAC, IT Security World, as well as at several IETF meetings. Ben graduated with a B.Sc. in Computer Science from Harvey Mudd College in Claremont, California USA. He earned a CISSP certification in 2005 and a GCFA certification in 2007.

1.7.4 Innovation

I am unaware of any similar research on risks presented by use of the Twitter service. Open source intelligence gathering has gained popularity for use in targeted attacks from both pen testers and real, malicious individuals/organizations. Using Twitter for botnet C&C and data exfiltration is new and innovative.

1.8 45' - 60' (Presentation)

Chema Alonso	chema@informatica64.com
Informática64	
+34 696 45 74 79	Spain

1.8.1 Sample

About this topic I have only published info in spanish.
<http://elladodelmal.blogspot.com/2009/06/correo-falseados-en-yahoocom-gmailcom.html> <http://elladodelmal.blogspot.com/2009/06/enviar-un-amigo-i-de-iii.html>

1.8.2 Synopsis

This talk is about spoofed email address. How big companies dela with them? Are Gmail.com, Yahoo.com and Microsoft hotmail giving good resources to recognice them? Is possible to discover them easily? This talk shows how Gmail, Yahoo! and Hotmail fail with this old topic even with SPF and DKIM solutions.

1.8.3 Biography

Chema Alonso is a Computer Engineer by the Rey Juan Carlos University and System Engineer by the Politecnica University of Madrid. He has been working as security consultant last seven years and had been awarded as Microsoft Most Valuable Professional since 2005 to present time. He is a Microsoft frequent speaker in Security Conferences. He writes monthly in several Spanish Technical Magazines. He is currently working on his PhD thesis about Blind Techniques.

1.8.4 Innovation

We are going to deliver a tool to recognize easily spoofed emails in Gmail which performs an extra-analysis on SPF and MX DNS-records and with an extra check in DKIM sings.

1.9 Breaking software protections - The hacker techniques (Presentation)

Chintan Shah shahchintanh@gmail.com Nevis Labs , Nevis Networks India Pvt Ltd 919975356768 India
--

1.9.1 Sample

Material yet to be prepared

1.9.2 Synopsis

This paper will cover some of the reverse engineering and Binary Analysis techniques with debuggers and disassemblers, which the hacker uses to break the software protections and bypass the registration schemes . I would plan to cover the follwing topics in this talk :

- 1) Software Reverse Engineering - An introduction
- 2) Binary Analysis / identification and Analysis of interesting code segments in the target software
- 3) Software protection mechanisms
- 4) Bypassing software protections
 - a) Bypassing software usage limitations
 - b) Hacking software registration schemes
 - c) Serial-Key fishing
- 5) Hacking softwares using resources

1.9.3 Biography

I work as a Security Research Engineer at Nevis Labs which is an independent security research division of Nevis Networks India Pvt Ltd . specializing in security solutions . I have attended Anti Virus Asia Research 2008 (AVAR 2008

) , and I would be interested in presenting a paper at this conference for the first time .. My areas of interest and research includes IPS development / Signature development / Vulnerability Research / Malware Analysis / Reverse Engineering and Binary Analysis / Exploit coding / Software Reverse Engineering and protection mechanisms.

1.9.4 Innovation

I would give the demo of how the hackers use the binary analysis and software reversing techniques to reverse engineer the softwares for breaking the protections and bypassing the registration schemes

1.10 NOSSL - Killing the Man in the Middle (Presentation)

Chris Potter chris@sdnaconsulting.com Secure DNA Consulting 808-388-8883 USA
--

1.10.1 Sample

None.

1.10.2 Synopsis

People rely on SSL Certificates to secure all of their web traffic. These certificates are issued by corporations that are supposed to be trusted. SSL as it is used currently has been proven to be flawed. The technology behind it is still good but, as with all things in the security field, the way it is handled and delivered is poor. This talk to discuss the technical aspects of how SSL is currently used and basic overviews of current attacks against SSL. The basis of this talk will demonstrate how SSL can be implemented using a combination of AJAX (transportation) and SMS (cert. verification) to completely encrypt all web traffic across the wire. This method of protection is far more secure than the current method because it completely removes the possibility of Man In the Middle attacks as well as verifies the authenticating user via a physical device outside of the web-space. This talk can also be tailored to suit the target audience from a high level executive perspective (boring) or a highly technical discussion (not boring =P).

1.10.3 Biography

Chris is a Security Consultant with Secure DNA Consulting. He has four years experience working within the Information Technology (IT) and Information Security (INFOSEC) industry. He has participated in numerous research projects with leading INFOSEC and IT experts from around the world. He has performed security audits for companies in the United States including leading industry fortune 500 firms. He is proficient in numerous programming languages and application development strategies. His core research and expertise lies in web application auditing and network engineering.

1.10.4 Innovation

This talk shows an interesting way of using current technologies to better the advancement of web based security. Also there are only a few methods that propose to use AJAX as an SSL implementation, none of which address the issue of Man in the Middle Attacks. This talk greatly expands on that earlier research to produce a fully secure non-exploitable SSL implementation within the web application and browser.

1.11 Unicode Transformations: Finding Elusive Vulnerabilities in Software (Presentation)

Chris Weber	chrisweber@live.com
Casaba Security	
1-949-637-4155	USA

1.11.1 Sample

<http://www.lookout.net/2009/03/26/exploiting-unicode-enabled-software-slides-from-cansecwest-and-source-boston/>

1.11.2 Synopsis

(Please do not release this in full, this is only for reviewers) The complex landscape of Unicode provides many angles for exploiting software and end users. We've known about some of these for years, we've seen buffer overflows exploited because of faulty Unicode handling, and we've seen homograph attacks in URL's. However, the real mysteries remain latent, unapparent to most software developers and even to the security testing community. I'm going to raise awareness around interesting attack vectors and new areas of research into Unicode, as well as open people's eyes to the modern Visual Spoofing attacks of today. This talk will include demonstrations of several uncommon vulnerabilities/attack vectors, and will also include a tool release to assist in finding these issues. A separate Spoof-detection component will also be released to demonstrate how we can defend users against Visual Spoofing attacks. We'll take a close look at many of the issues in Unicode software which are not commonly known:

- How Unicode characters can be mishandled to take on powerful formatting properties such as white space.
- When unexpected UTF-8 sequences can lead to over-consumption and character deletion which enable attacks such as cross-site scripting and file system manipulation.
- What happened to non-shortest form UTF-8 and UTF-7?
- Why best-fit mappings lurking in common frameworks and API's will enable drastic misbehavior and attacks within your applications, allowing for control over file systems and interpreters/parsers such as HTML.
- When casing operations enable a special character to be converted into something useful for cross-site scripting and other attacks.
- Why normalization operations can enable a Latin Modifier character to be converted into an exploitable HTML greater than sign.
- How normalization and casing operations can expand a single character by up to 18x leading to buffer overflows.
- Why the BOM and Mongolian Vowel Separator are great inputs to use in test cases.
- How Internationalized Domain Names work and why they're still vulnerable to Visual Spoofing attacks today.

This presentation's intention is to educate the audience on categorized security issues around Unicode and Internationalized software in a clear and structured

way, while giving real-world test cases, inputs, and practices for finding and avoiding vulnerabilities. I'll also cover the visual security issues relating to script spoofing and the 'confusables'. Internationalized Domain Names have been with us since 2003 yet are less understood in the security community. Internationalized top-level-domains are coming up, as are email addresses. I'll be demonstrating how I can fool end users with lookalikes and homograph attacks in modern browsers with common .COM and .ORG domains.

1.11.3 Biography

Chris Weber is co-founder at Casaba Security where he's leading product development for new tools to assist in the field of Unicode and Web-application security. He has spent years focusing on software security testing for some of the world's leading software development companies and online properties. He's authored several security books, articles and presentations, and regularly speaks at industry conferences. He's worked as a security researcher and consultant for over a decade identifying hundreds of security vulnerabilities in many widely used products including Web browsers and Web-applications.

1.11.4 Innovation

The subject matter of Unicode, character sets and encodings has confused people for many years. When you learn enough to go under the covers, you'll realize there's tons of potential for widespread vulnerability. In time for this conference I'll also have a Unicode Security Handbook completed. I'll also be releasing a tool to assist in testing and finding vulnerabilities related to Unicode string transformations in Web-applications. This will be the first of its kind.

1.12 Flawed shutdown policies and implication to security (Presentation)

Constantinos Patsakis	kpatsak@gmail.com
Department of Informatics, University of Piraeus	
+302104142267	Greece

1.12.1 Sample

1.12.2 Synopsis

The talk aims to show how flawed shutdown policies in OSs can lead to major security vulnerabilities, using as case study Windows XP.

1.12.3 Biography

2002 University of Athens, Department of Mathematics Ba 2003 MSc Information Security, Royal Holloway, University of London 2008 PhD, --Cryptanalysis and malicious cryptography--, Department of Informatics, University of Piraeus 2002-today Programmer in several projects, main area .Net development

1.12.4 Innovation

Windows XP have been by far the most widely used OS and will remain for while. Their core is been used be its successors, yet some of the policies that are being used are flawed.

1.13 Dynamic Binary Instrumentation for Deobfuscation and Unpacking (Presentation)

Daniel Reynaud and Jean-Yves Marion	reynaud.daniel@gmail.com
Nancy University - Loria	
+33.6.62.41.29.55	France

1.13.1 Sample

-

1.13.2 Synopsis

We propose to extend the toolbox of reverse engineers beyond disassemblers, debuggers and emulators. Using dynamic binary instrumentation, it is very simple to write advanced tools such as automatic unpackers, system call tracers and deobfuscators. We conducted a large-scale experiment on a corpus of 60.000 malicious binaries to confirm that DBI is suitable for malware analysis. In this presentation, we will present a simple and accurate automatic unpacker integrated with IDA Pro and a Javascript deobfuscator, all written using DBI techniques.

1.13.3 Biography

After a 4-years military training in Signals and Electronic Warfare, Daniel Reynaud is now a PhD student in Nancy (France), focusing on the analysis of malware and deobfuscation techniques. He has a background in reverse engineering and finding vulnerabilities in unconventional platforms, such as Java, mobile phones and Firefox extensions. Always looking for new challenges, he is now training to become a cage fighter.

1.13.4 Innovation

dynamic binary instrumentation is not yet a common tool for reverse engineers. We would like to demonstrate that it is actually a simple and powerful platform to write advanced malware analysis tools.

1.14 Mobile phone forensic (Presentation)

David Batanero	dabi@greencom.net
Independent researcher	
34605501025	Spain

1.14.1 Sample

1.14.2 Synopsis

I will speak about forensic in gsm phones, symbian, iphone and android platform. Also I will show how to recover call logs, phonebook, calendar, text, audio, video, messages, internet cache and settings, etc... How to get and read flash memory and how to use it, identify the model, because some time you get a destroy phone with no brand outside, one you have the flash, you could find the unlock code. Also I will show how to read the sim card and cloning it. To understand better what we have to find and recovering, I will show a software that show in real time what happened \inside" the phone, how begin the encryption inside the phone with the network, of for example what happened when a phone send/receive a sms, because is possible some mobile phones had been modify, so we see in real time, what information is been exchanging with the network or with another phone. Among other uses, we can investigate if the phone has been altered. Also I will show how begin the communication with our mobile phone, because some time we cant download the flash, due the encryption of the phone, this is usual in new mobile phones.

1.14.3 Biography

I'm playing and doing research with telecommunications since I was a child. Nowadays, I was the coordinator of the telecommunications line at Imaginarium, which is the most specialized toy retail chain in the world, with 340 shops in 28 countries. You can find more information at www.imaginarium.info. Besides, I was the coordinator for two models of mobile phones for children Mol <http://gizmodo.com/gadgets/cellphones/imaginarium-mol-mobile-phone-for-kids-206928.php> and Cam1 <http://www.electronista.com/articles/07/02/06/imaginarium.caml>. Also I have been working at www.indra.es in the past

1.14.4 Innovation

The use of mobile phones has grown in recent year, we have a lot of private information inside. Is normal people lose their phone, but really are we aware of all the information we have?

1.15 Security on the GSM Air Interface (Training)

David Burgess dburgess@kestrelsp.com Kestrel Signal Processing, Inc. 707 208 2622 USA

1.15.1 Sample

A court injunction prevents me from posting most technical material on publicly accessible web sites at this time. See <http://openbts.sourceforge.net> for details. However, here is the proposed outline for the workshop: Legal disclaimers and warnings DO NOT TRY THIS AT HOME Intellectual property

history Legitimate government concerns Why GSM still matters Normal security procedures Best practices Common variations Security flaws Design shortcomings Intentional weaknesses Common bugs Attacks Passive collection False basestation Rogue mobile station GSM as a UMTS security hole Defenses Subscriber defenses Network defenses Open topics for exploration I do keep a blog at <http://openbts.blogspot.com> that touches on some of these topics.

1.15.2 Synopsis

I will describe the basic security flaws of the GSM air interface, specific attacks that exploit these flaws and steps that can be taken to defend against them. We will consider attacks from both the network and subscriber sides of the interface.

1.15.3 Biography

Currently working on open source GSM networks. For ten years prior to that, provided software radio and protocol processing components for a range of law enforcement and intelligence applications.

1.15.4 Innovation

Many of these attacks are already known in theory but several will be demonstrated in practical examples. Some presented attacks may be novel.

1.16 "Hackerspaces: Friend or Foe, the new thrill in private and public research" (Presentation)

Eric Michaud eric@hackerspaces.org Argonne National Laboratory, HacDC, hackerspaces.org , Pumping Station: One NFP, TOOOL.US +0012017577702 USA
--

1.16.1 Sample

I am currently creating a new slide deck for this series. Originally for my previous sessions I was working with Deviant and Babek on the physical security talks so the relevant previous material would be here.
http://deviating.net/lockpicking/slides/2007-09-05-hitb_malaysia.rar and
<http://conference.hitb.org/hitbsecconf2007k1/materials/DIT1%20-%20TOOOL%20USA%20-%20Security%20-%20Past%20Present%20and%20Future.zip>
http://deviating.net/lockpicking/media/electronic_safe_spiking.avi
http://www.thelasthope.org/media/audio/64kbps/Building_Hacker_Spaces_Everywhere_Your_Excuses_are_Invalid.mp3

1.16.2 Synopsis

From my current developments and collaboration with the hackerspace community worldwide I've put together a macro vision of developments in exploitation and vulnerability research in the near future. I'll be covering attack time lines

based on collaboration remotely and locally, and where security is going with these new centers of collaborative education. Security systems originally relegated to either physical or cyber now converged into a blend with examples including the RFID, Medeco NexGen, SCADA, medical devices, among others. The available resources that hackerspace NGO's are creating will pose a dilemma for how quickly integration can be achieved across existing organizations and the uptake of this potential threat or benefit model. As an addendum this is a developing talk. It might also include new developments up till the date of the talk.

1.16.3 Biography

Eric Michaud a professional autodidact by trade. A founding member of TOOOL-US, Co-Founder of HacDC, Founder and President of Pumping Station: One. Eric has participated in lockpicking and cyber and physical security demonstrations and now at ToorCon, DefCon, HOPE conferences, ShmooCon, What The Hack, Hack In The Box, and the Chaos Communication Congress. Now is collaborating world wide in connecting hackerspaces together and spreading the good word.

1.16.4 Innovation

The recent explosion of organized hackers working in public physical locations has made it a very interesting arena in the last year and a half. People are finally realizing that they don't have to hide behind a terminal as much, or any more to do research on their particular passion. Plus the pooling of limited resources and the economic realization of --Super Abundance-- lends to people acquiring the tools that originally universities, corporations, and government had, that now allow them to also exploit systems recently inaccessible including electro mechanical systems. I'll also be presenting how the --closed source-- mindset of those systems is really false especially in embedded systems. As an aside Fin aka Markus says I'll be doing disservice by not submitting.

1.17 A Proof-of-Concept Attack on SmartCard-secured Online-Banking (Presentation)

Felix Groebert felix@groebert.org Jörg Schwenk, Christoph Wegener, Chair for Network and Data Security, Ruhr-University Bochum +49 176 2409 5390 Germany

1.17.1 Sample

1.17.2 Synopsis

The talk demonstrates, along a real-world PoC example, that it is possible to write Malware, which intercepts and manipulates online-banking transactions before they are signed with a class-1 SmartCard reader. Therefore techniques like API-Hooking and Javascript-Injection are employed and explained in the

talk. We underline the importance of using trusted in- and outputs for SmartCard-driven banking applications.

1.17.3 Biography

Felix Gröbert studies IT security (Dipl Ing) at the Ruhr-University Bochum. Besides articles on the topics web-security, phishing and malware, he has organized a hacking practical course at the Chair for Network and Data Security. When he is not doing freelance work in the field of IT, he is participating in Linux capture-the-flag contests or windsurfing in the netherlands.

1.17.4 Innovation

it demonstrates the weakness of a security concept by attacking a real-world implementation of the concept.

1.18 Windows Secure Kernel Development (Presentation)

Fermin J. Serna fermin.serna@microsoft.com Microsoft +34 654589469 Spain
--

1.18.1 Sample

Got slides already done. Please ask for them if interested.

1.18.2 Synopsis

The talk will cover several kernel mode topics on win32. The main target are kernel developers and testers so they will learn what to do, what to look for in the testing stage and how to make their lives easier with automated tools. It is divided in four sections: 1) Basic concepts on kernel space, entry points and how to validate and capture data locally. 2) Common mistakes and how to avoid them. 3) MSRC kernel cases samples and how we fixed them. 4) What developers can do to catch these common mistakes: static analysis, WDK fuzzers, dynamic analysis, etc...

1.18.3 Biography

Fermin J. Serna is a Security Software Engineer in the MSRC Engineering team. Prior to joining Microsoft, he spent 7 years in Spain working as a Penetration tester and lately running his own company in the security field. He has collaborated with US-CERT in the responsible disclosure of several vulnerabilities, such as CA-2002-12 for ISC-DHCP, and published documents on exploitation techniques on rare architectures such as SPARC and PA-RISC (at phrack). He loves security, coding, challenges, and chess.

1.18.4 Innovation

Will show common mistakes on kernel development and some MSRC real cases as examples. Will also show how we take advantage of automated tools to help us find variants of reported vulnerabilities.

1.19 Results of a security assessment of the TCP and IP protocols and common implementation strategies (Presentation)

Fernando Gont fernando@gont.com.ar
UK CPNI (Centre for the Protection Of National Infrastructure)
+54 9 11 6536 4380 Argentina

1.19.1 Sample

<http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf>
<http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>

1.19.2 Synopsis

Fernando Gont will present the results of a security assessment of the TCP and IP protocols carried out on behalf of the UK CPNI (United Kingdom's Centre for the Protection of National Infrastructure). He will explain the security implications arising from the protocol specifications themselves, and from a number of implementation strategies followed by most of the popular TCP/IP stacks, and will also discuss the new insights that were gained as a result of this project that can help to mitigate the aforementioned issues. Finally, Fernando will provide an overview of the ongoing efforts at the IETF community to incorporate these insights into the corresponding protocol specifications and the efforts in the vendor community to incorporate these recommendations into popular implementations of the protocols.

1.19.3 Biography

Fernando Gont specializes in the field of communications protocols security, working for private and gubernamental organizations both in Argentina and overseas. Gont has worked on a number of projects for the UK National Infrastructure Security Co-ordination Centre (NISCC) and the UK Centre for the Protection of National Infrastructure (CPNI) in the field of communications protocols security. As part of his work for these organizations, he has written a series of documents with recommendations for network engineers and implementers of the TCP/IP protocol suite. Gont is working on security assessments of communications protocols on behalf of the United Kingdom's Centre for the Protection of National Infrastructure. Additionally, he is a member of the Centro de Estudios de Informatica (CEDI) at Universidad Tecnológica Nacional/Facultad Regional Haedo (UTN/FRH) of Argentina, where he works in the field of Internet engineering. As part of his work, he is active in several working groups of the Internet Engineering Task Force (IETF). He has published a number of IETF RFCs, and has also authored a number of IETF Internet-Drafts, most of which have already been adopted by the IETF for their

future publication as RFCs. Gont has been a speaker at a number of conferences and technical meetings about information security, operating systems, and Internet engineering, including: CanSecWest 2005, BSDCan 2005, Midnight Sun Vulnerability and Security Workshop/Retreat 2005, FIRST Technical Colloquium 2005, IETF 64, IETF 67, IETF 73, LACNIC X, LACNIC XI, and JCC 2007.

1.19.4 Innovation

The TCP/IP protocols were conceived during a time that was quite different from the hostile environment that they operate in now. Yet a direct result of their effectiveness and widespread early adoption is that much of today's global economy remains dependent upon them. While many textbooks and articles have created the myth that the Internet Protocols were designed for warfare environments, the top level goal for the DARPA Internet Program was the sharing of large service machines on the ARPANET. As a result, many protocol specifications focus only on the operational aspects of the protocols they specify and overlook their security implications. Though Internet technology has evolved, the building blocks are basically the same core protocols adopted by the ARPANET more than two decades ago. During the last twenty years many vulnerabilities have been identified in the TCP/IP stacks of a number of systems. Some were flaws in protocol implementations which affect only a reduced number of systems. Others were flaws in the protocols themselves affecting virtually every existing implementation. Even during the last few years researchers have still been working on security problems in the core protocols. The discovery of these vulnerabilities led in most cases to reports being published by a number of CSIRTs and vendors, which helped to raise awareness about the threats and the best possible mitigations known at the time the reports were published. However, for some reason much of the effort of the security community on the Internet protocols did not result in official documents (RFCs) being issued by the organization in charge of the standardization of the communication protocols in use by the Internet: the Internet Engineering Task Force (IETF). This basically led to a situation in which "known" security problems have not always been addressed by all vendors. In addition, in many cases vendors have implemented quick "fixes" to the identified vulnerabilities without a careful analysis of their effectiveness and their impact on interoperability. During 2006, the United Kingdom's Centre for the Protection of National Infrastructure embarked itself in an ambitious and arduous project: performing a security assessment of the IETF specifications of the TCP and IP protocols. The project did not limit itself to an analysis of the relevant IETF specifications, but also included an analysis of common implementation strategies found in the most popular TCP and IP implementations. Additionally, it included a security assessment of new features, such as TCP window auto-tuning, that have been recently incorporated in operating systems such as Windows Vista and FreeBSD, but whose security implications have never been thoroughly evaluated. As strange as it may sound, this is the first thorough security assessment of the TCP and IP protocols and their common implementation strategies, the first security assessment of newly-incorporated mechanisms (such as TCP window auto-tuning), and the first attempt to take much of the work and wisdom of the security community to the IETF (Internet Engineering Task Force) and the vendor community.

1.20 Security Talk From The World's No. 1 Hacker! (Presentation)

Gregory D. Evans pr@ligatt.com LIGATT Security International 678-528-4525 USA

1.20.1 Sample

1.20.2 Synopsis

What happens if your computer is stolen? Laptops are listed as one of the most stolen items in the world today according to Safeware: The Insurance Agency. Do you travel with your laptop? Do you leave your laptop in the car? Do you carry it into heavily populated or busy places? According to the FBI, in year 2000 there were 418,000 laptops and PCs lost or stolen in the USA. Insurance statistics shows that if you own a laptop you have a 1 in 14 chance it will be stolen. This works out to about one computer theft every 53 seconds. Gregory Evans was the founder of a publicly traded computer security company called, The Cyber Group Network Corporation, which specialized in stolen computer recovery. While at the helm of The Cyber Group Network, Evans was the first African American to write a computer encryption program called, Password Protection Information Retrieval Technology (PPIRT). This program was sold in all major computer retail stores such as Fry's, Radio Shack, and CompUSA. PPIRT is the first security software of its kind, which includes a 2,048-bit encryption program, and computer recovery technology. PPIRT has the ability to track stolen computers over the Internet and across landline telephones. Evans has also invented the 1st wireless tracking device for computers, called eSnitch (Electronic Snitching Device), which enables a person to track a stolen computer from anywhere in the world. Every computer thief leaves tracks; you just need to know how to find them. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases, so does computer-related criminal activity and the need to anticipate and safeguard against it. Evans's expertise is frequently featured in a variety of media outlets including, The History Channel's "Modern Marvels". On the program, he demonstrated the capabilities of computer surveillance and the destruction of cyber terrorism, as well as discussed how spyware works and taught viewers how to protect their wireless networks. Evans has also been consulted on the highly rated, NBC's Dateline "To Catch a Predator". He has been featured in numerous newspapers and magazines including the Sun Newspaper, LA Times, USA Today, Black Enterprise, Wells Fargo Business Journal, and JET magazine, to name a few. Computer and digital forensics are a continually changing focus. Evans specializes in retrieving lost or deleted digital pictures and sound files from digital cameras and mp3 players, rescuing lost emails even if you have emptied the trash, creating emergency disk images and using a disk image as the ultimate backup tool, creating clones of hard disks and securely and permanently deleting sensitive or private data.

1.20.3 Biography

Providing a helpful service to the public has always been at the forefront of Mr. Evans's mind. It was this passion that led him to create LIGATT Security (www.LIGATTSECURITY.com) 6 years ago. LIGATT Security employs over 65 computer

security experts, and has conducted more security penetration tests than any other company in the nation. The company's client list includes the FBI and other government agencies, banks, and even entertainers such as Jim Carey and Chris \Ludacris" Bridges. Before embarking and starting LIGATT Security, Mr. Evans was the founder of a publicly traded computer security company called, The Cyber Group Network Corporation, which specialized in stolen computer recovery. While at the helm of The Cyber Group Network, Mr. Evans was the first African American to write a computer encryption program called, Password Protection Information Retrieval Technology (PPIRT). This program was sold in all major computer retail stores such as Fry's, Radio Shack, and CompUSA. PPIRT is the first security software of its kind, which includes a 2,048-bit encryption program, and computer recovery technology. PPIRT has the ability to track stolen computers over the Internet and across landline telephones. Along with being a successful business owner, Gregory Evans is a notable business educator. He has taught hi-tech crime continuing education courses and has spoken at a plethora of community colleges, universities and city government facilities. Such courses range from Computer Crime Investigation and Identity Theft, to Password Cracking and Recovery. As an author Mr. Evans has written 8 books. The first book was dedicated to laptop security entitled Laptop Security Short & Simple. Mr. Evans also wrote the first book ever dedicated to Spyware called, Spyware Reference & Study Guide. His other book titles include Memoirs of a Hi-Tech Hustler, Hi-Tech Hustler Scrap Book, Hi-Tech Identity Theft Short and Simple, 125 Ways to Protect Your Computer Short and Simple, Laptop Security Short and Simple, Fighting Hi-Tech Crime, and How to Become the World's No. 1 Hacker Short and Simple. In addition, Evans has written articles for both Upscale and Essence magazine.

1.20.4 Innovation

Every 6 seconds an individual's computer is being hacked into and 90% of Fortune 500 networks have been hacked. Every 79 seconds identity theft occurs through a thief stealing someone's identity, opening accounts in the victim's name and going on buying sprees. In one notorious case of identity theft, the US Department of Justice reported that the criminal incurred over \$100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and hand guns in the victim's name all the while calling his victim to taunt him. An ex-computer hacker turned Certified Ethical Hacker (CHE), Evans has been deemed the world's most advanced hacking expert as he successfully hacked into ATT, MCI and Sprint's computer systems which allowed him to revenue \$1,000,000 a week in the late 90's. After entering a guilty plea, Evans was sentenced to 24 months in federal prison and ordered to pay back \$9.8 million in fines and restitution. Evans' leadership in high-tech security has even extended to his presence in the media. He has recently been featured on several programs such as CNN, BET, CBS News and Atlanta's famous V103 with Frank and Wanda in the Morning. In May, Evans was also named one of Black Enterprise magazine's Top 20 \Masters of Innovation," and has been featured in numerous newspapers and magazines, including the LA Times, USA Today, Wells Fargo Business Journal, Essence and JET magazine. On The History Channel's series, \Modern Marvels," he demonstrated the often-startling capabilities of computer surveillance and the potential for destruction at the hands of cyber-terrorists, showed how spyware works, and taught viewers how to protect their wireless networks. In addition, he served as a consultant on NBC's highly rated Dateline series, \To Catch a Predator."

1.21 Ksplice: Patch without disruption (Presentation)

Jeff Arnold	jbarnold@ksplice.com
Ksplice, Inc.	
1-703-772-6460	USA

1.21.1 Sample

<http://www.ksplice.com/paper> contains the research paper.
<http://www.ksplice.com/software> contains the software.

1.21.2 Synopsis

The most important step for keeping systems secure is applying security updates in a timely manner. Since updating the core of the operating system, the kernel, always requires a reboot, people are forced into the uncomfortable dilemma of choosing between security and convenience. New technology out of MIT, called Ksplice, solves this problem by making it possible to apply all security updates without the disruption of rebooting. The Ksplice utilities are now available for the Linux kernel; they make it possible to construct rebootless updates from traditional source code patches. This year, this technology is being deployed on top of mainstream Linux distributions to eliminate the troublesome need to reboot for security updates. This talk will describe how this new rebootless update technology works and how it can be used by system administrators to improve the security of their systems.

1.21.3 Biography

Jeff Arnold started development on the Ksplice software in early 2007 as a research project at MIT. In 2008, Jeff and three other MIT alumni started Ksplice, Inc. in order to further develop and deploy the Ksplice technology. Jeff currently works in Cambridge, Massachusetts.

1.21.4 Innovation

1. Ksplice (the subject of the presentation) is the first system to make it possible to take traditional security patches (in the form of source code patches) and apply them to a running operating system without requiring a reboot. The work has been awarded MIT's computer science thesis prize and other awards. 2. The presentation addresses an important problem--patching is critical to security, yet system administrators and end-users commonly delay patching, leaving their systems vulnerable, because of the downtime and disruption of rebooting the OS or restarting applications. 3. The software demonstrated in this presentation is open source and currently available for use by system administrators and hackers.

1.22 Get your head out of the clouds: Security in Software-plus-Services (Presentation)

John Walton	jowalt@microsoft.com
Microsoft	
425-421-8738	USA

1.22.1 Sample

http://cid-669824398e613c5c.skydrive.live.com/self.aspx/.Documents/deepsec%7C_outline.docx

1.22.2 Synopsis

Software-plus-Services (S+S) is a rapidly growing industry approach for the next generation of computing. It is a convergence of multiple industry phenomena including SaaS, SOA, and Web 2.0. Software-plus-Services combines these approaches to bring together the best of cloud-based services and the software that resides on a world of devices. The power of local client and/or on-premises software combined with the reach and always up-to-date nature of services in the cloud offers greater flexibility than software- or service-only offerings. This presentation will examine both the challenges and advantages of engineering and operating trustworthy S+S. Additionally, it will compare and contrast security within traditional and agile development practices. Businesses and consumers considering this new computing model will benefit from the foundation this talk lays out for assessing risks and expectations of security in S+S.

1.22.3 Biography

John Walton is a Principal Security Lead with Microsoft, where he spends his time managing the engineering security team responsible for enabling and driving the secure development of Trustworthy Microsoft Online Services and evangelizing security best practices across the broader Online Services community at Microsoft. His team's responsibilities include security research, threat modeling, code auditing, tool development and penetration testing of software-plus-services Microsoft develops and hosts for businesses. Prior to joining Microsoft, John started a security consulting company, Penetration Technologies, specializing in application and infrastructure security and worked as Lead Security Engineer at Avaya. While at Avaya John built the Avaya Product Security Support Team, hacked every piece of Voice over IP (VoIP) equipment imaginable and helped develop VoIP encryption and security technology. Admittedly John is a self proclaimed computer security nut who rarely ponders anything else. He holds a Bachelors degree in Computer Science and is a Certified Information Systems Security Professional. While not working on security at Microsoft John spends his time security consulting for major financial and government institutions and occasionally finds time to sleep.

1.22.4 Innovation

Recent studies of market opportunities show that security is the number one barrier for adoption of Software-plus-Services (S+S). The processes and best practices surrounding software security continue to mature across the industry; however, S+S bring both new security challenges and advantages that conference attendees need to evaluate when considering the development, operation, and/or consumption of S+S.

1.23 Reversing and Exploiting an Apple Firmware Update (Presentation)

K. Chen	kchen.deepsec@gmail.com
Georgia Tech	
+1 404 290 0225	USA

1.23.1 Sample

Whitepaper will be sent via e-mail to cfp@deepsec.net.

1.23.2 Synopsis

I describe how an attacker can install malicious code into the firmware of an Apple aluminum keyboard.

1.23.3 Biography

Student at Georgia Tech, USA.

1.23.4 Innovation

this attack is stealthy and many people are ignorant of the dangers of malicious firmware.

1.24 Lust 2.0 – Desire for free WiFi and the threat of the Imposter (Presentation)

Lavakumar Kuppan	lavakumar.in@gmail.com
Independent Researcher	
+919833320286	India

1.24.1 Sample

1.24.2 Synopsis

This presentation will discuss how some design assumptions in Flash Browser Plug-in in Internet Explorer and Google Gears can be abused when users connect to unsecured Wi-Fi and attempt to browse. The three main attacks discussed are:

- 1) Stealing of files from the user's local hard drive using Flash
- 2) Stealing the entire Google gears data store of the victim which can contain information like the entire Gmail inbox or Google docs store
- 3) Placing permanent backdoors in sites using Google gears, either Gears Database(if implementation is flawed) or the Local Server (always, design weakness of Gears)

A tool named Imposter is also going to be released which would automate the attacks described during the talk and would also support well-know attacks against Web Clients like stealing cookies, LSOs, Saved form field values etc.

1.24.3 Biography

I am currently a member of the Global Information Security Assessment Team of Royal Bank of Scotland. I have been working in the areas of Penetration Testing, Application Security and Network Security for 3.5 years and have helped clients from across the globe and industry verticals. I have also trained more than 200 IT professionals across the country on Ethical hacking. I am a self-taught programmer with a special liking for Perl and c\# and find great creative satisfaction in writing code. I enjoy writing tools and giving presentations and have spoken at multiple OWASP chapter meets.

1.24.4 Innovation

The areas and technologies chosen are completely new and unexplored but still the impacts of these attacks are critical. The attacks would be demonstrated on some of the most popular sites like gmail.com, docs.google.com, myspace.com etc who are all vulnerable. There is a critical bug in myspace.com's Google Gears implementation which allows setting of permanent backdoors and am currently in the process of disclosing this to them, being an undiscussed attack this could possible affect far more websites. Since the target is design weakness there is no need for any 0-day or Social Engineering to carry out these attacks.

1.25 Playing in a Satellite environment 1.2 (Presentation)

Leonardo Nve	Inve@s21sec.com
S21Sec	
+34626955953	Spain

1.25.1 Sample

1.25.2 Synopsis

This presentation is a warning call to those responsible for the companies that use or provide data connection (especially the Internet) via satellite, proving some of the attacks that are possible in this environment. The presentation outline is: - Insecurity in Satellite communications. - Malicious Active Attacks - Getting an anonymous connection - Conclusions The attendees will learn how insecure satellite connections are and why they need a more secure platform for this environment or how we must use secured protocols if we have this technology hired. Also, they will learn how these attacks can be made, including how to get an anonymous satellite connection.

1.25.3 Biography

Senior security auditor and trainer interested in computer security since 1996, working as consultant and auditor from 2000, 2002. I managed several research on various security technologies such as DOCSIS and Wireless, with various papers published in various Spanish specialized publications.

1.25.4 Innovation

Previously satellite presentations exists, but these are focused only in feeds capturing and a bit in sniffing data, treating this as a passive vulnerability.

I focused my presentation in the active attacks someone can make to the clients and ISP. This presentation is focused for a high technical attendees.

1.26 Internet election for the German Bundestag (Presentation)

Lutz Donnerhacke	lutz@iks-jena.de
IKS GmbH, Fitug e.V., Thüringen Netz, Euralo/ICANN	
+49-3641-460861	Germany

1.26.1 Sample

The netzwahltag web page is currently offline.

1.26.2 Synopsis

To demonstrate a secure, secret, and provable election over the Internet, the Fitug e.V. organized a real world election in parallel in the Internet. For the upcoming election this year a similar action is planned (will be done at the time of the conference). In this talk the technical background is presented as well as the lessons learned from 2005 and 2009 election.

1.26.3 Biography

Lutz Donnerhacke (38) studied physics and mathematics. Main interests are Internet deployment (Thüringen Netz e.V., Individual Network e.V.), privacy and free speech (Fitug e.V., Religio), cryptography (i.e. OpenPGP), network security, software safety, and esoteric programming languages. As one of the founders of IKS GmbH he is working for this company since 1996.

1.26.4 Innovation

There no cryptographic breakthrough, no special technical innovation and of course nothing real innovative. It's just classical work brought to a larger audience. It addresses the problems with voting machines and solves several of the issues, the BVerfG (Federal Constitutional Court's) complained about.

1.27 Key Management Death Match? Competing KM Standards Technical Deep Dive (Presentation)

Marc Massar	marc@techandbull.com
Semtek	
805-407-1891	USA

1.27.1 Sample

Technical specs are available from the various standards bodies' web sites.

1.27.2 Synopsis

In the enterprise cryptography space the hottest topic these days is key management. And it's no surprise right? After several years now of increasing pressure to encrypt sensitive data, enterprise practitioners are feeling the pain of managing encryption systems using diverse tools, methods, and processes. Key Management is the core of this problem. In the last few years a growing clamor for a standards-based approach to key management has arisen. And the answer has been somewhat confusing. Today there are a number of key management standards that are in development. With the recent founding of yet another standard (the OASIS Key Management Interoperability Protocol { KMIP}) many in the market are left wondering why so many? This presentation will be an in depth comparison of the relative strengths and weaknesses of 4 of these standards (IETF Keyprov, IEEE 1619.3, OASIS EKMI, and OASIS KMIP). In addition this presentation will identify the in scope and out of scope areas for each and map these standards in an understandable and complete manner. Each standard or protocol will be explained in basic terms as well as very technical terms in order to demonstrate the gaps and overlapping areas. In addition to a technical review and comparison, this presentation will show enterprise security professionals how these standards will impact the design, deployment, and support of cryptographic systems in the future. Because many of the players in the standards community are vendors, this will significantly drive product offerings in the near future and security professionals need to be armed with this information in order to make informed decisions about encryption technologies.

1.27.3 Biography

As a leader in technology, security and encryption management, Marc Massar has been sought after and consulted by both Government and Industry for assistance with political policy, strategic roadmaps and product development. Currently as an independent consultant, and recently as a Principal Solutions Architect for Venafi, Marc assists global organizations in the deployment of enterprise IT and security solutions. Previously at First Data Corporation (the world's largest processor of electronic payment transactions), Marc's insight into encryption management was instrumental as he developed and deployed the global encryption strategy, encompassing all aspects of data protection with encryption, while serving as the lead architect for the Global Encryption Program. Marc is a member of the OASIS EKMI (Enterprise Key Management Infrastructure) Technical Committee and KMIP (Key Management Interoperability Protocol) TC, has been a vocal advocate for application integration to encryption services. Marc holds a degree from Occidental College, is a Certified Information Systems Security Professional, and is also Infosec Assessment Methodology certified by the National Security Agency.

1.27.4 Innovation

The confusion over competing key management standards is starting to cause disruption in enterprise practitioner's decisions to implement crypto products. There is even disagreement among the various standards bodies over who's standard is --the one-- that covers all of the needs of a key management system. This presentation will compare these standards and show where they do and do not overlap and where the gaps are on the path the the --mother of all key management systems.--

1.28 Breaking Tor sessions with HTML5 (Presentation)

Marco Bonetti	mbonetti@cutaway.it
CutAway Srl	
+393490985572	Italy

1.28.1 Sample

<http://html5.doesntexist.com/> and <http://sid77.slackware.it/>

1.28.2 Synopsis

Tor is a software project that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Unfortunately, with the new features of HTML5 and browser built-in geolocation being pushed into the Web2.0 world, it's becoming harder and harder to keep the users' privacy safe. This presentation will describe the problems which are arising around the use of these new technologies and how they can be (ab)used to attack Tor users, even without the need of Javascript support.

1.28.3 Biography

Marco Bonetti is a Computer Science engineer with a lot of passion for free and open source operating systems. As he didn't find any suitable distribution for his PowerBook, he created Slackintosh: the unofficial PowerPC port of the famous Slackware Linux distribution. Interested in privacy and security themes, he's following the emerging platforms for the protection of privacy in hostile environments. He's currently working as a security consultant for CutAway.

1.28.4 Innovation

...Tor is a nice piece of software which have to be used with much attention. I traveled around Italy talking about how it works and how to use it safely and yet, after almost three years, there're still people which don't use Firefox and TorButton for daily Tor usage. Also, html5 will spread out quickly: all of the major browser (except IE so far (if we acknowledge it the status of --browser--)) are supporting some of the new tags and functionalities, with them is going to be even easier to disrupt users' privacy and with no need of Javascript support at all!

1.29 BSD Rootkit Programming (Training)

Marco Lux	marco.lux@nruns.com
N.RUNS AG	
+4915155002776	Deutschland

1.29.1 Sample

1.29.2 Synopsis

This training involves strategies to create your own BSD Rootkit through the runtime Kernel Patching and loadable Module support. The attendee will be given the practical knowledge to write his own software to defend or subvert his system. The targeted operating systems will be FreeBSD 7.x and NetBSD 3.0. The students will be delivered with the attack types and methodologies how to defend against those attacks and how to implement them by themselves.

Description of the Course ----- 1. Introduction of my person 2. Brief History of rootkits 3. Brief History of different techniques of rootkits 4. What is /dev/(k)mem 5. Writing the code (examples for FreeBSD and NetBSD) - syscall hijacking - memory patching - hiding processes - hiding network connections - hiding files 6. Defences against such kinds of rootkits 7. Programming a defence module The course is highly hands-on. This means, no long talk and deep technical.

1.29.3 Biography

- Working with computers over 18 years - over 8 years in the industry

1.29.4 Innovation

A lot of information and papers were published about Linux Rootkits. But very few information is available for the BSD Land. There is no practical training in how to write and defend against kernel land BSD rootkits. Also no current work/information is published about those 2 targeted operating systems.

1.30 User input piercing for Cross Site Scripting (Presentation)

Matias Xavier Blanco	matiasblanco18@gmail.com
Core Security Technologies	
(5411) 5556-2673 (int 2434)	Argentina

1.30.1 Sample

Will upload the paper in this link shortly:
<http://corelabs.coresecurity.com/index.php?module=FrontEndMod&action=list&type=publication>

1.30.2 Synopsis

The increasing amount of vulnerable sites with Cross Site Scripting was the starting point for this research. This paper presents the algorithms and techniques to perform user input piercing on a web application. We introduce an heuristic to determine if a given Cross Site Scripting attack will effectively execute scripting code on the compromised browser, minimizing the false-positives and giving reliable results. To perform this task, we have

implemented a Dynamic Encoding Detection Algorithm and a Validation Heuristic.

1.30.3 Biography

Matias works at Core Security Technologies as WebApps Exploit Writer. He is also a Ms. Student in Computer Science at Buenos Aires University. He enjoys to learn everything about WebApps Security, Interpreted Languages, Graph Theory and Language Theory.

1.30.4 Innovation

We improve on previous fuzzers, which have only focused in black-box analysis with a static set of vectors and encodings, by providing a black-box heuristic method that will construct a XSS attack from a vulnerability. The methodology allows as to solve the problems around Injection points, Encoding Detection, Injection Validation, Egg Injection and devising the XSS vectors. The approach is automated, has a very low rate of false positives and does not rely on updating a static set of XSS vectors.

1.31 Rootkits are awesome: Insider Threat for Fun and Profit (Presentation)

Michael Kemp	clappymonkey@gmail.com
XRL	
+44(0)7748305690	United Kingdom

1.31.1 Sample

www.clappymonkey.com

1.31.2 Synopsis

Addressing the insider threat is now rightly recognised as playing a crucial element in improving the security posture of organisations and preventing all kinds of embarrassment. Recent years have seen a growth in all manner of vendors promising panaceas to address ordinary user activities, but what exactly are the solutions offered? In a lot of instances, legitimate rootkits. This talk examines the current state of the insider threat marketplace, the technical solutions to the issues presented, and an actual analysis of user activities in RL and how they may well negate the the promises of vendors and the expectations of security minded organisations.

1.31.3 Biography

Michael is an experienced UK based security consultant, with a specialization in the penetration testing of web applications and the testing of compiled code bases and DB environments to destruction. As well as the day job, Michael has been published in a range of journals and magazines, including heise, Network Security, Inform IT and Security Focus. To date, Michael has worked for NGS Software, CSC (Computer Sciences Corporation), and a host of freelance clients throughout the globe. Presently, Mike is currently planning on touting his

shoddy wares via a new start up, which keeps not starting up thanks to life getting in the way. When not breaking things, Michael enjoys loud music, bad movies, weird books and writing about himself in the third person. Mike has previously presented at security conferences in Jakarta, Hawaii, New York, Munich, Warsaw, Prague, Zagreb and London, and is always keen to embarrass himself in new and exotic locales.

1.31.4 Innovation

I'll be demo-ing a new DLP detection tool. In addition, it is my contention that legitimate applications can be used for illegitimate purposes, and those technologies used to prevent threat actually introduce it...

1.32 Unicode Shellcode 2.0 : New methods, algorithms and tool (Presentation)

Minh Bui Quang minhbq@bkav.com.vn Network Security Researcher +84 169 7371 622 Vietnam
--

1.32.1 Sample

1.32.2 Synopsis

Buffer overflow bugs are amongst the most prevalent and the most critical bugs today. On exploiting these bugs, we often encounter the problem of Unicode format which prevents our shellcodes from executing properly. This is caused by the fact that many software use functions like MultiByteToWideChar() to convert character (ANSI) strings into their wide character (Unicode) equivalents. As we were looking through these materials to perform some Unicode Buffer Overflow exploitation, we saw that there is still room for improvement in Unicode Shellcode. This documentation will propose new methods, algorithms and our tool that we have applied for Unicode Shellcode.

1.32.3 Biography

Mr. Bui Quang Minh is senior researcher of Bkav. He has 5 experience years in software and network security research. He is now the leader of Security Vulnerability Research Team of Bkav. His team has discovered and announced many famous vulnerabilities, such as: Google Chrome, Windows Media Encoder, Hosting Controller, ... Recently, the research in face recognition vulnerability of Asus, Lenovo and Toshiba laptops, co-discovered by him, was presented at Black Hat DC 2009 Conference.

1.32.4 Innovation

My research is serious and improvements are very useful.

1.33 USB Device Drivers: A Stepping Stone into your Kernel (Presentation)

Moritz Jodeit, Martin Johns	moritz@jodeit.org
Moritz Jodeit: n.runs AG, Martin Johns: University of Pas-sau, faculty of informatics	
Moritz Jodeit: +49 170 2884291, Martin Johns: +49 40 42883 2654	Germany

1.33.1 Sample

Slides and paper referenced at --Synopsis of Talk-- above: [1]
http://www.jodeit.org/files/zUv9E3mz6Xkq2j3/slides_09-01-13-OS-Jodeit-Evaluating_Security_Aspects_of_USB.pdf [2]
<http://www.jodeit.org/files/zUv9E3mz6Xkq2j3/usboot09.pdf>

1.33.2 Synopsis

Talk outline: - Description of attack scenarios - Presentation of our fuzzing environments. We will discuss both the hardware-aided approach (see slides at [1]) as well as the software-based man-in-the-middle fuzzer (see paper at [2]). - Short demo using the emulation environment (we are also thinking about preparing a demo for a application level attack, e.g., malicious HID device which uses keystrokes to install a backdoor) - Summary of results

Abstract: The widely-used Universal Serial Bus exposes a physical attack vector which has received comparatively little attention in the past. While most research on device driver vulnerabilities concentrated on wireless protocols, we show that USB device drivers provide the same potential for vulnerabilities but offer a larger attack surface resulting from the universal nature of the USB protocol. To demonstrate the effectiveness of fuzzing USB device drivers, we present our prototypical implementation of a mutation-based, man-in-the-middle USB fuzzing framework based on an emulated environment. We practically applied our framework to fuzz the communication between an Apple iPod device and a Windows XP system. This way, we found several potential vulnerabilities. This supports our claim that the USB architecture exposes real attack vectors and should be considered when assessing the physical security of computer systems in the future.

1.33.3 Biography

Moritz Jodeit: Studied Computer Science at the university of Hamburg with a focus on information security where he received his diploma in 2008. Since the beginning of 2009 he's working as a penetration tester at n.runs AG in Germany. In 2005 he joined the OpenBSD project as an official OpenBSD developer. The rest of his free he spends doing private security research and bug hunting which resulted in several disclosed vulnerabilities in software such as OpenSSL, Sendmail, ClamAV, MacOSX or Quicktime. Martin Johns: Studied Mathematics and Computer Science at the Universities of Göttingen (Germany), Santa Cruz (CA) and Hamburg (Germany) where he received his diploma in 2003. During the 1990ties and the early years of the new millennium he earned his living as a software engineer in German companies (including Infoseek Germany, TC Trustcenter and SAP). 2005 he joined the --security in distributed systems-- group at the University of Hamburg to work on the project --Secologic--, which

was investigating the state of the art in software security. In 2008 he followed his PhD advisor to the University of Passau where he recently submitted his PhD thesis (which deals with web application security). Currently he is a security researcher and PhD candidat at the University of Passau, Germany with a focus on software- and webapp-security.

1.33.4 Innovation

USB is everywhere. A well placed USB stick in front of a office building is a almost fool-proof way to get physical access to a kernel driver within a targeted company. As USB can access kernel components, such as file system implementations, which are usually regarded to be out of reach of external attackers and, therefore, are not as thoroughly audited as public interfaces.

Our man-in-the-middle approach enables very convenient and fast detection of existing faults in the respective device drivers, applications, etc.

1.34 Evaluating Secure Protocols and Intercepting Secure Communication (Training)

Moxie Marlinspike	moxie@thoughtcrime.org
Institute For Disruptive Studies	
011-415-267-1806	USA

1.34.1 Sample

<http://www.thoughtcrime.org>

1.34.2 Synopsis

This class will start with a thorough examination of how secure protocols are built. Most everyone is familiar with the building blocks of secure protocols -- block ciphers, hash functions, asymmetric encryption. But what are these things, really? How do we model them and how do we put them together in order to build protocols that are provably secure? Participants will emerge from this training as cryptographers who are capable of understanding and composing most cryptographic proofs (with very little math required). Armed with this knowledge of how secure protocols are built, this training will continue by examining the protocols that we depend on today to see how they stack up. Suddenly we can look at things like SSH, SSL, and Tor with new eyes. Finally, this training will cover tricks that overcome it all. Even with provably secure protocols, there are always implementation problems and holes in the glue between different layers. Participants will be given training with the most recent copies of `sslstrip` and `sslsniff`, and will have opportunities to practice using them in different settings.

1.34.3 Biography

Moxie Marlinspike is a fellow at the Institute For Disruptive Studies with over thirteen years of experience in attacking networks. He is the author of `sslsniff` and `sslstrip`, the former of which was used by the MD5 Hash Collision team to deploy their rogue CA cert and the latter of which continues to implement Moxie's deadly `--stripping--` technique for rendering communication

insecure. His tools have been featured in many publications including Hacking Exposed, Forbes Magazine, The Wall Street Journal, the New York Times, and Security Focus as well as on international TV.

1.34.4 Innovation

This training is innovative because it teaches cryptography from a real-world perspective and does not ignore implementation problems. It also gives people time to experiment with tools like sslstrip and sslsniff, which have proven deadly for intercepting secure communication.

1.35 Advance MySQL Exploitation (Presentation)

Muhaimin Dzulfakar	muhaimin.dzulfakar@security-assessment.com
Security-Assessment.com	
+6421776410	New Zealand

1.35.1 Sample

1.35.2 Synopsis

This talk focuses on how MySQL SQL injection vulnerabilities can be used to gain remote code execution on the LAMP and WAMP environments. Due to the limitation of the features on MySQL, for example unsupported multiple statements in one query-make MySQL an unpopular platform for an attacker to execute remote code execution, compared to MSSQL platform. This talk will prove that the same result can be achieved on the MySQL platform. In this presentation, the author will present a new tool title MySQLoject. This tool is able to upload and execute metasploit shellcode through SQL Injection vulnerability onto the MySQL platform.

1.35.3 Biography

Muhaimin Dzulfakar is a Security Consultant for Security-Assessment.com, located in Wellington, New Zealand. His primary duties include network and application penetration testing. Muhaimin Dzulfakar has a bachelor degree in Software Engineering from Multimedia University, Kuala Lumpur where he developed his own Intrusion Detection System. His research interests include exploit development and post exploitation process.

1.35.4 Innovation

It's interesting and original. Audience would be impressed in you can show how you can pop a shell in front of them and my talk will do!

1.36 VOIP, Operating System Security,WLAN/WiFi, GPRS, IPv6 and 3G Security,Security Management (Training)

Muhammad Zubair Rafiq	zubair@elpk.com
ELINKS	
07553244144	Pakistan

1.36.1 Sample

yes

1.36.2 Synopsis

VOIP, Operating System Security,WLAN/WiFi, GPRS, IPv6 and 3G Security,Security Management,Security Management

1.36.3 Biography

Expert in Computrization, CCTV, Learnig VOIP, Software Developments, Networking

1.36.4 Innovation

i m selfmade

1.37 Tuning of ACO Algorithms for optimization solution Using TSP (Presentation)

NATARAJ H	nataraj.cse@gmail.com
MSRIT	
919964624994	INDIA

1.37.1 Sample

1.37.2 Synopsis

This paper proposes a novel ant colony optimization Named ACO algorithms for solving the traveling salesman problem more effectively in the congested transportation systems. Global heuristic/local heuristic information related to time-distance is put into the probabilistic selection rule of the ant tour construction. The parameters of the algorithm are analyzed by experiments. Numerical results also shown for the different ACO algorithms and the effective ACO algorithm is suggested using TSP environment

1.37.3 Biography

POST GRADUATE STUDENT

1.37.4 Innovation

Aim is to demonstrate and conclude the performance of different ACO algorithm, which yields to produce optimal solution for a given set of parameter values. It is our hope that following these routes, ultimately the performance and applicability of ACO algorithms can be further improved.

1.38 Top 10 Security Issues Developers Don't Know About (Presentation)

Neelay S Shah neelay.shah@foundstone.com Foundstone Inc., A Division of McAfee +1-225-937-8693 USA
--

1.38.1 Sample

I don't have an outline of the presentation accessible over the Internet. I will be happy to provide the detailed outline if needed,

1.38.2 Synopsis

Applications are getting more and more complex every day, and it is not uncommon to find an application which relies on multiple technologies to achieve the desired goal. As a result developers are now, more than ever, exposed and expected to be proficient in multiple technologies. With this increased exposure come increased security issues, especially at the development level. And often developers are not even aware of these security issues. During this talk we'll cover the top 10 security issues I have run into time and again while performing security code reviews and which developers are least educated about. Attendees will learn the security Do's and Don'ts with setting up inter-process communication, using cryptography, launching new processes, developing and deploying ActiveX controls, integrating and leveraging third-party components and more. We'll also link the issues we cover to the common application features such as "Auto-update" or "Scheduled Tasks" where they are most likely to be present. This talk will NOT cover security issues such as Buffer Overflows, SQL Injection, and Cross Site Scripting, which developers are reasonably likely to know.

1.38.3 Biography

Neelay is a Senior Software Security Consultant and a lead instructor at Foundstone, where he specializes in performing threat modeling and security code reviews for a variety of enterprise products ranging from user mode applications to complex hardware virtualization software, file system device drivers and custom kernels. Neelay developed the Writing Secure Code { C++ class and is responsible for delivering the class as well as maintaining current content for it. Neelay has a strong background and a rich experience in developing C++ based applications. Prior to joining Foundstone, Neelay worked as a software development engineer at BindView Inc. More recently, Neelay worked as a software engineer with Citrix Systems Inc. on the Citrix Metaframe presentation server, the industry-standard for application virtualization using a centralized, secure architecture. Neelay has been

honored with the Microsoft Most Valuable Professional (MVP) - Developer Security Award in recognition of his thought leadership and contributions to the application security and developer communities. Neelay has presented at various software security and IT security conferences such as Dr. Dobbs Architecture and Design World, SD West, Open Web Application Security Project (OWASP), ISACA, Information Systems Security Association (ISSA) and InfoSec Canada. Neelay is the author of the Foundstone CredDigger penetration testing tool and the HacmeTravel training tool. Neelay has been a regular contributor to the Spot the Bug column on the Microsoft Security Developer Center website, which educates developers on secure coding practices using real-world coding examples. Neelay also presented the "Identifying, Exploiting and Remediating Vulnerabilities in C++ Based Applications" webinar at the Foundstone webinar series

1.38.4 Innovation

As part of the various manual security code reviews that I have been doing over the past four years I have seen the developer community becoming slowly but surely increasingly more educated about security issues such as Buffer Overflows, SQL Injection, and Cross Site Scripting. However, there are quite a few other equally impacting security issues that I have seen time and again during code reviews that when I discuss with the concerned development team, the typical development team response is "Wow! We did not even know about this till now. Most probably our other applications/products also afflicted with these security issues". My goal is to educate and increase the awareness amongst the developer community about these issues and as such I will cover these security issues in my presentation

1.39 Thick Client Application (In)Security (Presentation)

Neelay S Shah neelay.shah@foundstone.com Foundstone Inc., A Division of McAfee +1-225-937-8693 USA
--

1.39.1 Sample

I don't have an outline of the presentation accessible over the Internet. I will be happy to provide the detailed outline if needed,

1.39.2 Synopsis

Applications are becoming richer in terms of their user interface, attempting to leave a lasting impression on the users and wanting them to come back for more. Applications these days expose various ways for the user to interact with the application to create a "rich" application experience for the user. Thick client applications are the preferred choice to guarantee the above principles since they can leverage existing robust frameworks such as JAVA and .NET to create a rich user interface and are not limited by the browsers' (in)ability to render the user interface elements. However with the increased sophistication, comes increased complexity and hence it is not uncommon to find client applications that are not only serving as the "presentation" tier but also potentially comprise of business logic to a varied extent. Security testing for thick client applications is a fairly involved and specialized task

as compared to security testing web applications since each thick client is custom designed and developed for the application at hand. As such security testing each thick client application potentially involves dealing with different technologies and communication protocols and hence necessitates the use of different approaches. Attendees will learn the different strategies and methods that can be used for successfully testing thick client applications. We will discuss at length the different techniques to be able to bypass client side checks including methods for successfully understanding and intercepting client { server network communication. We will also evaluate the above mentioned techniques at depth in terms of their advantages, disadvantage and when to use the particular technique. This talk is intended for application testers, developers, project managers and application security professionals.

1.39.3 Biography

Neelay is a Senior Software Security Consultant and a lead instructor at Foundstone, where he specializes in performing threat modeling and security code reviews for a variety of enterprise products ranging from user mode applications to complex hardware virtualization software, file system device drivers and custom kernels. Neelay developed the Writing Secure Code { C++ class and is responsible for delivering the class as well as maintaining current content for it. Neelay has a strong background and a rich experience in developing C++ based applications. Prior to joining Foundstone, Neelay worked as a software development engineer at BindView Inc. More recently, Neelay worked as a software engineer with Citrix Systems Inc. on the Citrix Metaframe presentation server, the industry-standard for application virtualization using a centralized, secure architecture. Neelay has been honored with the Microsoft Most Valuable Professional (MVP) - Developer Security Award in recognition of his thought leadership and contributions to the application security and developer communities. Neelay has presented at various software security and IT security conferences such as Dr. Dobbs Architecture and Design World, SD West, Open Web Application Security Project (OWASP), ISACA, Information Systems Security Association (ISSA) and InfoSec Canada. Neelay is the author of the Foundstone CredDigger penetration testing tool and the HacmeTravel training tool. Neelay has been a regular contributor to the Spot the Bug column on the Microsoft Security Developer Center website, which educates developers on secure coding practices using real-world coding examples. Neelay also presented the "Identifying, Exploiting and Remediating Vulnerabilities in C++ Based Applications" webinar at the Foundstone webinar series

1.39.4 Innovation

As part of the various thick client application security testing that I have been performing over the past 4 years, one common trend / issue seems to be present: There is an inherent tendency for the server to implicitly trust the thick client. This tendency encourages vital security checks viz. authorization and data validation checks to be performed at the client side. This essentially means that once the malicious user / attacker is successful in bypassing the client side security checks then he / she is going to be able to --call the shots-- and compromise the security of the application / system at will. My goal is to educate the testers/security auditors/developers about the various strategies/techniques that can be successfully used for testing the security of thick client applications

1.40 Outspect: live memory forensic for Virtual machine (Presentation)

Nguyen Anh Quynh	aquynh@gmail.com
AIST	
818050845258	Vietnam

1.40.1 Sample

<http://www.xchg.info/ARTeam/Syscan09/Outspect%20-%20Live%20Memory%20Forensic%20&%20Incident%20Response%20for%20Virtual%20Machine%20by%20Nguyen%20Anh%20Quynh.pdf>

1.40.2 Synopsis

Recently, memory analyzing has become a popular mechanism to perform incident response and forensic. However, traditional approach of memory forensic has some major drawbacks that cannot be solved in current systems. The first shortcoming is the inconsistency memory problem: memory cannot be consistently acquired because system is still functioning in the process. Another issue is that existent rootkits can easily tamper with the acquired and analyzed steps. Last but not least, loading forensic tools into the memory will inevitably erase evidences in the memory. This research presents --Outspect--, a new tool set to perform memory forensic and incident response for live virtual machine (VM). By running Outspect outside of the inspected VM, we can solve the above-mentioned problems of traditional memory forensic. While Outspect and its architecture is designed to support all kind of guest Oses and hypervisors, in this presentation we focus on Windows guests running on Xen hypervisor. The talk dedicates some time to discuss the advantages and challenges of our approach. The mechanism to inspect and extract important system objects from raw memory will also be examined. We will go into detail on our architecture, and prove that it is useful for many things other than just live memory forensic. The presentation includes some live demos to demonstrate the effectiveness of Outspect. We will use Outspect to inspect and detect some popular kernel rootkits and userspace malware on Windows VM. The demo will also show that it is trivial to detect exploitation using sophisticated attack technique like Metasploit with Meterpreter payload (which cannot be detected by any anti-virus at the moment).

1.40.3 Biography

Nguyen Anh Quynh is a researcher at The National Institute of Advanced Industrial Science and Technology (AIST), Japan. He interests include computer security, networking, operating system, virtualization, digital forensic, intrusion detection. He published a lot of academic papers in those fields, and frequently gets around the world to present his research results in various hacking conferences. Quynh obtained his PhD degree in Computer Science from Keio university, Japan. He is also a member of Vnsecurity, a pioneer security research group in Vietnam.

1.40.4 Innovation

The first ever live memory forensic tool for Virtual machine

1.41 eKimono: detecting rootkits inside Virtual Machine (Presentation)

Nguyen Anh Quynh	aquynh@gmail.com
AIST	
818050845258	Vietnam (Residence: Japan)

1.41.1 Sample

1.41.2 Synopsis

Recently, virtual machine (VM) has become widely-used, but still we do not have adequate protection for them. This talk discusses the advantages that virtual machine can bring to security from malware detection point-of-view, and presents a new rootkit detector named eKimono. While the whole architecture has been designed to be independent of hypervisor and guest OS, we focus on protecting Windows VM running on Xen in this talk. To spot rootkits inside a guest Windows, we run eKimono in Xen's Dom0 and let it scan the memory of the guest VM for suspicious things. To find the most advanced rootkits, we employ various tactics to detect rootkit's behaviours, so it is highly possible that a rootkit can be detected by at least one of our methods. As a result, eKimono can detect a range of rootkits, from userland to kernel-based types. Technically, eKimono is only the top component of a multiple framework architecture. The talk details all the layers, explains how we solve challenges in designing and implementing eKimono. The extended application of the below layers is also examined to prove that our design is not just useful for detecting rootkits, but also can be the base to create many new tools such as live forensic and VM administration for VM. The presentation dedicates a part to discuss different types of rootkits, and how eKimono can detect them. We also have some live demos to show how effectively eKimono is against some popular kernel-based and userland rootkits. Finally, we discuss the possibility of recovering the infected systems, and how that can be done with eKimono.

1.41.3 Biography

Nguyen Anh Quynh is a researcher at The National Institute of Advanced Industrial Science and Technology (AIST), Japan. His interests include computer security, networking, operating system, virtualization, digital forensic, intrusion detection. He published a lot of academic papers in those fields, and frequently gets around the world to present his research results in various hacking conferences. Quynh obtained his PhD degree in Computer Science from Keio university, Japan. He is also a member of Vnsecurity, a pioneer security research group in Vietnam.

1.41.4 Innovation

The first ever talk about detecting malware in virtual machine by analyzing its raw memory

1.42 The Dark Side of the Fox: Abusing Firefox Extensions (Presentation)

Nick Freeman, Roberto Suggi Liverani	nick.freeman@security-assessment.com
Security-Assessment.com	
+6421424777	New Zealand

1.42.1 Sample

<http://atta.cked.me/tmp/deepsec/outline.txt>

1.42.2 Synopsis

Hundreds of Firefox addons are created every week. Millions of users download them. Some addons are even recommended by the Mozilla community, and users implicitly trust them. We don't trust a single one, and we will show you why. This talk details how we have abused some of the most popular and recommended Firefox addons, with previously unreleased vulnerabilities. From the Mozilla download statistics, over 30 million users are potentially affected. Demos will cover remote code execution, local file disclosure and other tailored Firefox Addon exploits. Don't panic - the Addons manager can be found under the 'Tools' tab in your Firefox menu. We expect to see a lot of people clicking the --Uninstall-- button after this presentation.

1.42.3 Biography

Roberto Suggi Liverani is a senior security consultant for Security-Assessment.com. He is the founder and leader of the OWASP (Open Web Application Security Project) Chapter in New Zealand. Roberto has worked with companies such as Google, Oracle and Opera by reporting and helping to fix security vulnerabilities in their products. Roberto is a co-author of the most recent OWASP Testing Guide and has spoken at various security conferences around the globe. Nick Freeman is a security consultant at Security-Assessment.com based in Auckland, New Zealand. After a couple of years of building systems for companies he has turned to breaking them instead, and spends his spare time searching for shells and the ultimate combination of whisky and bacon.

1.42.4 Innovation

It's a large, under-researched attack surface with many avenues of exploitation. If you think NoScript will save you, you're wrong. This talk details how Firefox extensions are built and why they are vulnerable. Our methodology will be incorporated into the next OWASP Testing Guide. From theory to the practice: the talk includes live demonstrations previously undisclosed vulnerabilities in some of the most recommended and used Firefox extensions.

1.43 Stoned Bootkit: Your PC is now Stoned! ..again (Presentation)

Peter Kleissner	Peter@Kleissner.at
I am independent ppl :)	
+43 676 6612209	Austria

1.43.1 Sample

Paper (version 1 of Stoned Bootkit):
<http://www.stoned-vienna.com/downloads/upload3/Paper.pdf> But it's going to change within the next months, I will implement much more features.

1.43.2 Synopsis

Stoned Bootkit is a brand new Windows bootkit. It is loaded before Windows starts and is memory resident up to the Windows Kernel. Thus Stoned is executed beside the Windows Kernel and has full access to the entire system. It is able to handle all modern Windows OSes, including XP, Vista and for the future 7. It has exciting features like integrated file system drivers, automatic Windows pwning, plugins and boot applications, and much much more. Inside itx a small operating system! It goes back to the roots - so 2010 your screen will show --Your PC is now Stoned! ..again--

1.43.3 Biography

Since 2005 I am developing operating system software. I like open source, reverse engineering and Windows internals! I rock at assembly language and am an OS development enthusiast. Today I am working together with researchers all over the world on reverse engineering malware in the wild. I have done some quite big projects, including my own operating system totally written in assembly language and now since a year a Windows Simulator developed with an AV company.

1.43.4 Innovation

..my bootkit is just sexy! It is going to be mostly open source, covers multiple operating systems (all modern Windows versions) and for the future also Linux planned. Heh it is bypassing full volume encryption, right now its bypassing TrueCrypt! Not to forget that I will give a live demonstration, infecting my own full volume encrypted top-secure Dell Studio XPS 16. No one's secure!

1.44 HostileWRT: Turn Your Friendly Wireless Access Point into an Autonomous, Curious, Standalone, ... (Presentation)

Philippe Langlois	philippe.langlois@gmail.com
P1 Security, /tmp/lab, Telecom Security Task Force	
+33 6 11 52 16 71	FRANCE

1.44.1 Sample

not online, can send by email.

1.44.2 Synopsis

HostileWRT: Turn Your Friendly Wireless Access Point into an Autonomous, Curious, Standalone, Malicious & Really Annoying Device. Have you ever imagined what a recalcitrant access point would look like? Well... neither do we. So we're going to show you what REAL love is all about. HostileWRT tends to make love to your antennas thanks to the 802.11 protocol suite. Then, sharing the love is more than natural. No wonder then that HostileWRT, despite its very blackhat touch, is the most desirable item in one's sado-(techno)-masochist outfit. Computer and network security professionals are confronted on a daily basis with the issues of testing the reality of perceived problems and suggesting fixes with high applicability potential. Such issues are particularly difficult in wireless environments since the measures are not of binary nature but depend on the capacity to detect effectively WiFi networks, access points and other radio equipments. There is always the chance of missing a radio equipment or not having good and accurate measurements. We propose in this paper to automate several critical parts of the wireless network security audit using pervasive and inexpensive platforms and thus to free more time to focus on the applicability of the fix, and even the verification of the application of the fix. HostileWRT aims at automating scanning and cracking in wireless environment and improving results using different behaviours depending on the goal of the auditor. By using an hostile approach, we want to prove that it's not possible to fully audit a wireless environment without taking in account the several different kinds of vulnerabilities that affect both the infrastructure and the end-users.

1.44.3 Biography

Founder of P1 Security and Senior Security Consultant for Telecom Security Task Force. Philippe Langlois has proven expertise in network security. He founded and led technical teams in several security companies (Qualys, WaveSecurity, INTRINsec) as well as security research teams (Solsoft, TSTF). He founded Qualys and led the world-leading vulnerability assessment service. He founded a pioneering network security company Intrinsec in 1995 in France, as well as Worldnet, France's first public Internet service provider, in 1993. Philippe was also lead designer for Payline, one of the first e-commerce payment gateways. He has written and translated security books, including some of the earliest references in the field of computer security, and has been giving speeches on network security since 1995 (RSA, COMDEX, Interop, HITB Dubai, Hack.lu).

1.44.4 Innovation

This talk will have an Onsite embedded demo with active exploitation and tool release. HostileWRT represent a different (active & hostile) approach to wireless network security audits and differs in the goal (behaviours) and usage (audit, flash setup, mesh) of the result of the audit.

1.45 The Worries of Today (Presentation)

Rene pfeiffer	pfeiffer@luchs.at
DeepSec GmbH	
+43.676.5626390	Austria

1.45.1 Sample

<http://www.google.com/>

1.45.2 Synopsis

You'll see.

1.45.3 Biography

Yes.

1.45.4 Innovation

I am an evil genius and spiek wiz a Tscherman akzent.

1.46 Living on the Edge: The Sources of Creativity (Presentation)

Richard Thieme	rthieme@thiemeworks.com
ThiemeWorks (self employed)	
414 351 2321	USA

1.46.1 Sample

www.thiemeworks.com or google Richard Thieme or go through Black Hat or Def Con sites

1.46.2 Synopsis

The edges of our thinking, the edges of consensus reality, the edges of organizational structures - that's where new ideas first show up. Those we call --geniuses-- see them first and give them names. Using the insights and wisdom of the best and the brightest of the infosec and hacking worlds as well as the practice of the craft of intelligence, this presentation demonstrates how creativity infuses the best practices of security and intelligence, how to tend it and make it more likely to happen, and how to capture it on the fly. The questions for information security practitioners include: How do you generate your creative best in a world driven by cyber attacks and down-sizing? How does creativity fit into the big picture we all know is true in the Dilbert-world of the real work place? This keynote responds to those questions with deep and real insights, grounded in the nitty-gritty of life in the trenches. Thieme argues persuasively that you must tap into your creative potential to succeed as a person-of-interest /and/ a security professional. This talk helps professionals recontextualize how they think about challenges in security by seeing the deeper context of their work.

1.46.3 Biography

--And those who were seen dancing were thought to be insane by those who could not hear the music.-- - Frederick Nietzsche Richard Thieme has been hearing the music for a long time. His track record includes hundreds of published articles, dozens of published short stories, one published book with more coming, several thousand speeches, and { in a former incarnation - hundreds of sermons, all original, all unique. In the nineteen eighties, Thieme began writing about the impact of new technologies on societal systems, spirituality and identity. Mostly he delivers keynotes and closing speeches that unite the diverse themes of a conference. He has spoken in Sydney and Brisbane, Wellington and Auckland, Dublin and Berlin, Amsterdam and The Hague, Eilat (Israel), and all around the States, including many hacker, security and intelligence cons. Clients include: GE Medical Systems; Medtronic; Microsoft; Johnson Controls; the Pentagon; the FBI; the US Secret Service; Los Alamos National Laboratory; US Department of the Treasury; OmniTech; Neohapsis; Network Flight Recorder; System Planning Corporation (SPC); UOP; Psynapse/Center for the Advancement of Intelligent Systems; Allstate Insurance; Governor's Conference on Economic Development; Purdue University (CERIAS); and the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas.

1.46.4 Innovation

nobody else in infosec makes people think as deeply or move outside their comfort zones to look in from the outer edges and see the context of their work in new ways. The introducer at IT Defense said, I could have listened to you for another hour ... others say, --you made me think-- or --it was thrilling to see a thousand geeks mesmerized by a speech without any audio visuals ...--

1.47 Hacking, Biohacking, and the Future of Humanity (Presentation)

Richard Thieme rthieme@thiemeworks.com ThiemeWorks (self employed) 414 351 2321 USA

1.47.1 Sample

www.thiemeworks.com or google Richard Thieme or go through Black Hat or Def Con sites

1.47.2 Synopsis

The skills we have come to associate with hacking { seeing things cleanly and for the first time every time we look, innovative and creative thinking, cross-disciplinary knowledge, and a heart laced with a love of larceny and a refusal to accept the consensus reality of society, insisting on making things new, enabling life to do things that were unanticipated ... and cool ... these skills apply to biohacking as well as hacking information and communications systems. Biohacking is hacking the genome, the organism, the species, to create new possibilities. Beyond enhancements of humanity-of-the-moment, it

aims to generate new qualities and capabilities. Biohacking takes the work of corporate and government labs and puts it back in the garage where it belongs. Biohacking aims to create new organisms, DNA that enables living creatures to do new things. Biohacking is the new frontier of hacking. I was asked in 2006 at AusCert in Australia, my second of three years of keynoting, where did I see hacking headed in the future? I described biohacking and noted that genetic engineering, neuroscience (both black and white R&D) and the availability of everything one needs for a few thousand bucks to hack the genome in a garage, all made hacking human attributes and identity the next level of the transformation of human possibility. This talk illuminates how current and future developments in information systems, robotics, biotechnology, nanotechnology, and the colonization of the solar system through telerobotic and human exploration, all suggest ways human identity will be hacked and enhanced. The evolution of post-human identity is in our hands. This talk sounds like science fiction but isn't. It delivers profound insights into the next chapter of human civilization.

1.47.3 Biography

--And those who were seen dancing were thought to be insane by those who could not hear the music.-- - Frederick Nietzsche Richard Thieme has been hearing the music for a long time. His track record includes hundreds of published articles, dozens of published short stories, one published book with more coming, several thousand speeches, and { in a former incarnation - hundreds of sermons, all original, all unique. In the nineteen eighties, Thieme began writing about the impact of new technologies on societal systems, spirituality and identity. Mostly he delivers keynotes and closing speeches that unite the diverse themes of a conference. He has spoken in Sydney and Brisbane, Wellington and Auckland, Dublin and Berlin, Amsterdam and The Hague, Eilat (Israel), and all around the States, including many hacker, security and intelligence cons. Clients include: GE Medical Systems; Medtronic; Microsoft; Johnson Controls; the Pentagon; the FBI; the US Secret Service; Los Alamos National Laboratory; US Department of the Treasury; OmniTech; Neohapsis; Network Flight Recorder; System Planning Corporation (SPC); UOP; Psynapse/Center for the Advancement of Intelligent Systems; Allstate Insurance; Governor's Conference on Economic Development; Purdue University (CERIAS); and the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas.

1.47.4 Innovation

nobody else in infosec makes people think as deeply or move outside their comfort zones to look in from the outer edges and see the context of their work in new ways. This one is a jolt to even the most creative innovative people. It discloses new possibilities for hacking in a dynamic exciting way. The introducer at IT Defense said, I could have listened to you for another hour ... others say, --you made me think-- or --it was thrilling to see a thousand geeks mesmerized by a speech without any audio visuals ...--

1.49 Hijacking Mobile Data Connections 2.0: Automated and Improved (Presentation)

Roberto Piccirillo	r.piccirillo@mseclab.com
Mobile Security Lab	
+39 340 5847738	Rome (Italy)

1.49.1 Sample

<http://poc.mseclab.com/research/BlackHat-Europe-2009-Mune-Gassira-Piccirillo-Hijacking-Mobile-Data-Connections-slides.pdf>

1.49.2 Synopsis

The talk will go further into the topic of hijacking mobile data connections via remote handset reconfiguration, as presented at Black Hat Europe 2009. New enhancements and vectors will be introduced and analyzed in order to automate the attack and improve its effectiveness while reducing chances for it to be spotted. The first part will explain how to create a working provisioning message, employing a network pin security mechanism for message integrity and authentication. An interesting feature of this type of provisioning message, as opposed to a user pin, is that no user input is required; a confirmation is sufficient in order to install the carried configuration as the default one. This mechanism requires the knowledge of International Mobile Subscriber Identity (IMSI), supposedly known by the mobile operator network and the user's SIM card. The talk will show how to programmatically retrieve IMSI using one of the several on-line sites providing IMSI lookup service, and how to extract from it other information that could be used in order to build a completely automated massive attack tool. Then, a live session will demonstrate the forging of a malicious provisioning message by putting together all techniques just described; by means of source spoofing, the received configuration message from user's perspective will be virtually indistinguishable from a legitimate one. In the second part of the talk, new enhancements related to web traffic hijacking will be covered in details. We will explain the advantages of injecting an HTTP proxy configuration, as opposed to subverting DNS queries, which we have previously shown. This will provide a better handling of HTTPS connections, and will enable us to use readily available and more advanced tools. Most mobile sites use HTTP protocol to exchange data and switch on HTTPS only for logging in; sidejacking and forced sidejacking can be applied in these cases. By integrating Moxie Marlinspike SSLStrip tool, it's now possible to perform HTTPS stripping attack and to eavesdrop on the data usually sent in an encrypted session. Even with sites on which the tool is ineffective, HTTPS connections are transparently proxied so the user won't notice he's been hijacked. The mix of these enhancements, apart from extending the reach of the attack to a larger number of mobile platforms, makes the hijacking very effective and hard to detect. A live step-by-step attack demo will conclude the talk.

1.49.3 Biography

I'm currently working as a Security Researcher for Mobile Security Lab. I graduated in Computer Science with the thesis --Graphical Representation and Animation for Cryptography Education--. I mainly deal with Mobile Applications

and Protocol Security but I'm also interested in binaries reverse engineering.

1.49.4 Innovation

The talk is about putting together, for the first time, a number of different techniques in order to build a fully automated and highly effective attack to hijack mobile data connections, starting from just a single spoofed SMS message. Armed with that, a skilled attacker can compromise the security of mobile originated data connections for a large number of users, with a minimal chance of being detected. Publicly available mobile services are leveraged and concur in making the attack more effective, suggesting that Mobile Security should be dealt with an holistic approach to the overall system.

1.50 Web Application Vulnerabilities and Countermeasures (Training)

Sandro Melo / Nelson Uto	sandro@ginux.ufla.br
Locaweb / CPqD	
55 11 94202941	Brasil

1.50.1 Sample

http://altabooks.tempsite.ws/index.php?manufacturers_id=105&osCsid=k7v9o3857052uiqarlin22ukc1
http://altabooks.tempsite.ws/index.php?manufacturers_id=62&osCsid=k7v9o3857052u1qarlin22ukc1
http://altabooks.tempsite.ws/index.php?manufacturers_id=37&osCsid=k7v9o3857052u1qarlin22ukc1

1.50.2 Synopsis

In the present days, web application vulnerabilities have been largely exploited by attackers for stealing confidential data and accessing corporate networks. However, it is not an easy task to build secure software, considering its complexity nowadays. Quite often a system is composed of thousands of lines of code, which invariably contain some bugs. Part of them have impact on system security and can lead, for instance, to unavailability and complete control of the machine by an attacker. The number of vulnerabilities reported by the Common Vulnerabilities and Exposures has been increasing year after year. Buffer overflow was for a long time the most common security problem found in software, but it lost that position for vulnerabilities like cross site scripting and SQL injection. These types of weaknesses basically affect web applications and indicate: - The popularization of that type of software, be it for electronic commerce, internet banking, or for configuring a network element, such as an access point; - The security issues related to this domain have not been properly addressed during software development, which is aggravated by security unconscious developers and tight development schedules. The purpose of this tutorial is to discuss the present most common web application vulnerabilities, according to OWASP, to show possible attack scenarios, how to test, and countermeasures that can be used to avoid those weaknesses. Topic: - Introduction and motivation about web application (in)security and

the need for considering security in the whole software development lifecycle.

- Review of fundamental concepts from cryptography (ciphers, hash functions, digital signatures, digital certificates, and SSL) and HTTP (request methods, error codes, session management, and authentication).
- Presentation of a secure software development lifecycle.
- Overview of OWASP and the main projects they support.
- Presentation of the main tools employed in web application pentesting.
- Cross site scripting is nowadays the most common vulnerability and allows powerful attacks such as session hijacking, clipboard stealing, and network scanning.
- Injection flaws occur when an application does not validate user input and may lead to unauthorized information access and broken authentication.
- Malicious file execution may lead to complete server compromise.
- Insecure direct object reference in URLs may be modified to allow unauthorized information access.
- Cross site request forgery takes advantage of an authenticated session to submit valid but illegitimate requests to the application.
- Information leakage and improper error handling may provide valuable information to a malicious user.
- Broken authentication and session management can be the result of low-entropy session ids and inadequate protection of credentials.
- Insecure cryptographic storage often results from improper key management.
- Misconfigured servers may lead to insecure communications
- Failure to restrict URL access can result in unauthorized information access.
- Final remarks about web application (in)security.

1.50.3 Biography

Sandro Melo has been working with Information Technology for 16 years, specially, as a network and security analyst. He worked for large companies such as EDS and currently he is employed by Locaweb, the largest hosting company in Latin America, where he is responsible for security incident response, computer forensics, and Linux administration and deployment. He holds a bachelor's degree in Data Processing from Mackenzie University and a master's degree in Network Engineering from IPT/USP. He also attended graduate programs in System Analysis and Computer Networks from Mackenzie University and UFPA, respectively. During his M.Sc., worked under supervision of Dr. Antonio Rigo, wrote several technical reports and reviewed scientific papers for conferences. Sandro holds the following professional certifications: SCSA, Novell CLE, Novell CLP, Novell CIA, RHCT, LPIC 3, LPIC 2, and LPIC 1. Besides articles in newspapers and specialized magazines, Sandro has published the following books by Alta Books: - Security with Free Software, ISBN: 8576080265; - BS7799 { From Tactics to Practice in Linux Servers, ISBN: 8576081261; - Exploiting Vulnerabilities in TCP/IP Networks, ISBN: 8576081342; - Computer Forensics with Free Software, ISBN: 9788576082880. The most important professional achievements worth mentioning are: - Invitation from Brazilian Presidential Committee on Information Security to give a Linux security course to high ranking army officers; - Invitation from LPI Canada to prepare questions for the certification exam; Invitation from Italian consulate to work for the Kantea Project. Nelson Uto holds a bachelor's and a master's degrees in Computer Science from State University of Campinas { Unicamp. During his M.Sc., worked, under the supervision of Dr. Ricardo Dahab, on a mobile agent systems security project, specially developing new security mechanisms for the Aglets system. Also reviewed scientific papers for conferences (SSI 2001, WSeg 2003, and CTIC 2003) and for the Journal of Universal Computer Science and published himself several academic papers in national and international security conferences. Nelson has been an Information Technology professional for 13 years and an Information Security specialist for the last 7 years. He currently works at CPqD Telecom & IT

Solutions as a Security Consultant and Researcher, in the areas of Cryptography and Application Security, and also as a PCI QSA and a PCI PA-QSA: he worked on cryptographic key management, evaluated free libraries supporting elliptic curve cryptography for the XScale and x86 platforms, performed pentests on several web applications as part of a risk analysis project, prepared hardening guidelines for Oracle and Unix systems, researched the application of K-Means clustering algorithm for semiautomatic generation of security event correlation rules, specified a security event management system, and elaborated security policies. He also worked as a C/C++/Assembly x86/Java programmer and as an Oracle DBA. The most interesting projects he got involved include an ODBC-JDBC driver and a 4GL to Java translator, which automatically generated semantically-equivalent Java code from 4GL programs. Finally, he coordinates a graduate program on information security and is a professor at graduate and undergraduate levels. He taught the following courses so far: \Information Security", \Introduction to Cryptography", \Operating Systems", \Data structures", \Object-oriented programming", \Introduction to Information Technology", and \Programming techniques".

1.50.4 Innovation

Because this is training very important for experts in Security of Internet and also is hand on.

1.51 Essential Computer Forensic with FOSS Tools (Training)

Sandro Melo / Nelson Uto	sandro@ginux.ufla.br
Locaweb / CPqD	
55 11 94202941	Brasil

1.51.1 Sample

http://altabooks.tempsite.ws/index.php?manufacturers_id=105&osCsId=k7v9o3857052ulqarlin22ukc1
http://altabooks.tempsite.ws/index.php?manufacturers_id=62&osCsId=k7v9o3857052ulqarlin22ukc1
http://altabooks.tempsite.ws/index.php?manufacturers_id=37&osCsId=k7v9o3857052ulqarlin22ukc1

1.51.2 Synopsis

In past, one server was configured, their risks but these risks were physically dimensioned, corresponding to the limits of the LAN of the corporation or institution. The Internet has radically changed this scenario. It is more secure than a system with Firewall or other security devices, there will always be the possibility of human error or hitherto unknown failure in the operating system or applications, whether proprietary or FOSS system. Given this degree of risk, at first intangible, the threat of an invasion is something that we can't overlook. In this context, the forensic techniques are essential during the response to an incident, to identify where the computer has violated its security, which was changed, the identity of the attacker and preparing the environment for expertise of Forensic Computer. Bearing in mind the care of an expert as a Computer Forensic invasion is electronic Incident. A digital evidence must be preserved so that it can have value. About Tutorial .

1a part (1 session) - Main Title: Concepts of Live Forensic Subtitle: Concepts and Response to Incidents using Live Forensic methodology Synopsis: This Tutorial focuses on the Forensic Expertise in Linux servers and the main topics will be: - World Scenario Operating System - State of the Art of Computer Forensic - Data expert - Devices for storage of CPU - Memory Peripherals - Main Memory System - Traffic Network - State of Operating System - Modules Kernel System - Secondary storage devices - File System - Analysis of malicious programs - Standardization in the Acquisition of Evidence - RFC's importants - Forensic Expertise Applied to Networking - Expertise for Forensic Collection of Evidence - Invasion and identify attacker - Performing a Computer Forensic Expertise

2a part (1 session) - Título Principal: Netorkw FOSS Subtítulo: Evidence collection and analysis of network assets with FOSS Tools Synopsis: In some contexts of security incidents it is possible to collect evidence from the network, not only from the computer under investigation but from other network assets having data as well. It is a fact that when the network is well designed with security attributes of the that can be identify information inherent a computer victimized in a security incident may be of extreme value in Forensic Computer Expertise. It is a fact that when the network is well designed with security attributes the information, inherent to a victimized computer, can be identified in a security incident. This may be of extreme value in Computer Forensic Expertise. Main topics will be Concepts about process in a Forensic Network; - Pcap format; - Tools for data capture; - Using tcpdump; - Using Ngrep; - Using Wireshark; - Analysis of Connections; - Static analysis of evidence; - Using Chaosreader; - UsingTCPstrings; - Identification and Recovery of Artifacts in TCP; - Using TCPxtract; - Dynamic Analysis of Evidence; - Using TCPreplay; - Limits of Forensic Network; - Designing networks Ideal for retention of best evidence.

3a part (2 sessions) - Título Principal: Post Mortem Forense Subtítulo:Bits brushing, Scanning Data, Identifying and analyzing evidence. Synopsis: The task of analysis of media such as HD, Pendrive and other devices like digital cameras is very important for a Computer Forensic Expertise, where besides the possibility of identification of important information also necessary to cross-information raised during the Live and Forensic Network Forense. This Tutorial aims to give overview point of the whole process of a Post Mortem Analysis tools using FOSS (Free and Open Source Software). Main topics will be: - Concepts about process in a Post Mortem Forensic; - - Conceituando the analysis in five layers; - Copy Bit by Bit; - Mounting images for analysis; - Search and / or retrieval of information from Partitioning; - Search and / or retrieval of information in metadata; - Search and / or retrieval of information from data; - Search and / or retrieval of information in Slackspace; - Building a Timeline; - Identification of Artifacts; - Dynamic Analysis of Artifacts; - Static Analysis of Artifacts; - Expertise of Expert versus Anti-forensic techniques; - Preparation of a Technical Report;

1.51.3 Biography

Sandro Melo has been working with Information Technology for 16 years, specially, as a network and security analyst. He worked for large companies such as EDS and currently he is employed by Locaweb, the largest hosting company in Latin America, where he is responsible for security incident response, computer forensics, and Linux administration and deployment. He holds a bachelor's degree in Data Processing from Mackenzie University and a master's degree in Network Engineering from IPT/USP. He also attended graduate programs in System Analysis and Computer Networks from Mackenzie University and

UFLA, respectively. During his M.Sc., worked under supervision of Dr. Antonio Rigo, wrote several technical reports and reviewed scientific papers for conferences. Sandro holds the following professional certifications: SCSA, Novell CLE, Novell CLP, Novell CLA, RHCT, LPIC 3, LPIC 2, and LPIC 1. Besides articles in newspapers and specialized magazines, Sandro has published the following books by Alta Books: - Security with Free Software, ISBN: 8576080265; - BS7799 { From Tactics to Practice in Linux Servers, ISBN: 8576081261; - Exploiting Vulnerabilities in TCP/IP Networks, ISBN: 8576081342; - Computer Forensics with Free Software, ISBN: 9788576082880. The most important professional achievements worth mentioning are: - Invitation from Brazilian Presidential Committee on Information Security to give a Linux security course to high ranking army officers; - Invitation from LPI Canada to prepare questions for the certification exam; Invitation from Italian consulate to work for the Kantea Project. Nelson Uto holds a bachelor's and a master's degrees in Computer Science from State University of Campinas { Unicamp. During his M.Sc., worked, under the supervision of Dr. Ricardo Dahab, on a mobile agent systems security project, specially developing new security mechanisms for the Aglets system. Also reviewed scientific papers for conferences (SSI 2001, WSeg 2003, and CTIC 2003) and for the Journal of Universal Computer Science and published himself several academic papers in national and international security conferences. Nelson has been an Information Technology professional for 13 years and an Information Security specialist for the last 7 years. He currently works at CPqD Telecom & IT Solutions as a Security Consultant and Researcher, in the areas of Cryptography and Application Security, and also as a PCI QSA and a PCI PA-QSA: he worked on cryptographic key management, evaluated free libraries supporting elliptic curve cryptography for the XScale and x86 platforms, performed pentests on several web applications as part of a risk analysis project, prepared hardening guidelines for Oracle and Unix systems, researched the application of K-Means clustering algorithm for semiautomatic generation of security event correlation rules, specified a security event management system, and elaborated security policies. He also worked as a C/C++/Assembly x86/Java programmer and as an Oracle DBA. The most interesting projects he got involved include an ODBC-JDBC driver and a 4GL to Java translator, which automatically generated semantically-equivalent Java code from 4GL programs. Finally, he coordinates a graduate program on information security and is a professor at graduate and undergraduate levels. He taught the following courses so far: \Information Security", \Introduction to Cryptography", \Operating Systems", \Data structures", \Object-oriented programming", \Introduction to Information Technology", and \Programming techniques".

1.51.4 Innovation

Because this is training very important for experts in Security of Internet and also is hand on.

1.52 Ownage 2.0 (Presentation)

Saamil Udayan Shah	saamil@net-square.com
Net-Square	
+91 98254 31192	India

1.52.1 Sample

Not online yet

1.52.2 Synopsis

It is 2009 and the underground cyber economy is flourishing. Spam has become a lucrative business, writing exploits fetches real money, financial fraud is on the rise and the worms are loose. Although this is nothing compared to the financial blunders that led to the current recession, it is interesting to know how all the pieces fit together. We've known about classic web hacking, exploiting binaries, shellcode, abusing protocols and tricking users. This talk explores how each vulnerability plays a key part in making the larger system come together - attack patterns of tomorrow, the objectives, motives and where all the pieces of the puzzle fit together. How do individual SQL Injection, Browser exploits, PDF bugs, XSS, etc fit together? What have we learned from the past, and what are the core design issues in HTTP, HTML, Browsers and application programming that make for mass ownership opportunities? In our quest for mashups and Web 2.0, have we compromised on fundamental security principles? Last year, I had been talking about some of the core problems that plagued browsers. This year, my work goes beyond just browsers and looks at examples of mass ownage, new infection vectors, advanced client-side exploitation, malicious payloads, browser infection with toolbars and more. Everything is assembled before your very eyes! And as a bonus, I will demonstrate some of my own attempts at defeating Web Application Firewalls and Browser Firewalls (yes there is such a creature called a Browser Firewall)

1.52.3 Biography

Saumil continues to lead the efforts in security research at Net-Square. Saumil has had more than ten years experience with system administration, network architecture, integrating heterogenous platforms, and information security and has performed numerous ethical hacking exercises for many significant companies in the IT area. Saumil has been a regular speaker and trainer at conferences such as Blackhat, RSA, Hack-in-the-Box, IT Underground, CanSecWest, EUsecWest, Hack.LU, etc. Previously, Saumil held the position of Director of Indian operations at Foundstone Inc. and a senior consultant with Ernst & Young. Saumil has also worked at the Indian Institute of Management, Ahmedabad, as a research assistant. Saumil graduated from Purdue University with a master's degree in computer science and a strong research background in operating systems, networking, information security, and cryptography. He got his undergraduate degree in computer engineering from Gujarat University, India. Saumil is a co-author of --Web Hacking: Attacks and Defense-- (Addison Wesley, 2002) and is the author of --The Anti-Virus Book-- (Tata McGraw-Hill, 1996)

1.52.4 Innovation

a) I thought that web hacking was dead, but SQL injection and XSS are still wide open avenues of attack. These have now turned into excellent avenues for automated mass attacks. b) Browser vulnerabilities and file format vulnerabilities continue to increase. This talk carries off from where my previous talk left off at, with a fresh look into why browsers will never be fixed the way they are. Browser exploits are one thing, and delivering them to a mass audience is another. This talk connects all the dots together. c)

Blow weak attempts at protection (read WAFs and Browser Firewalls) out of the water. I'm going to show my own real-life attacks to prove my point.

1.53 Sticking it to the Airlines (Hacker Lounge)

Saumil Udayan Shah	saumil@net-square.com
Net-Square	
+91 98254 31192	India

1.53.1 Sample

There won't be any online material for this talk. It's best left to be discussed only at the conference :)

1.53.2 Synopsis

An off-the-record presentation of my attempts (and successes) at messing around with online reservation systems, e-check in, airport security and more.

1.53.3 Biography

Saumil continues to lead the efforts in security research at Net-Square. Saumil has had more than ten years experience with system administration, network architecture, integrating heterogenous platforms, and information security and has performed numerous ethical hacking exercises for many significant companies in the IT area. Saumil has been a regular speaker and trainer at conferences such as Blackhat, RSA, Hack-in-the-Box, IT Underground, CanSecWest, EUSecWest, Hack.LU, etc.

1.53.4 Innovation

... well, hacking airlines is fun.

1.54 Social Engineering Training for IT Security Professionals (Training)

Sharon Conheady & Martin Law	sconheady@gmail.com
First Defence Information Security	
+44 (0)7824 383940	UK

1.54.1 Sample

1.54.2 Synopsis

Social engineering is the use of deception or impersonation to gain unauthorised access to sensitive information or facilities. Because computer security is becoming more sophisticated, hackers are combining their technical expertise with social engineering to gain access to sensitive information or valuable resources in your organisation. Social engineering attacks can have disastrous consequences, both financially and reputationally. You can have the best technical security controls in the world, from the most expensive firewall to the most sophisticated biometrics, but they will not protect you from a social engineering attack. In any security programme people are the weakest link. Social engineering tests can be used to evaluate and strengthen this link. Like any penetration test, social engineering tests can help to identify security weaknesses that could allow your IT systems to be compromised. Such tests can:

- Give a good indication of and even improve your staff's level of security awareness
- Teach your staff how to identify and deal with social engineering situations
- Provide valuable recommendations on both security awareness and physical security

However, it can be difficult to know how to conduct a social engineering test. This training course will teach participants how to conduct an ethical social engineering test as well as giving recommendations on how to defend against social engineers. The two-day training course is split into four parts and will include practical exercises:

Part 1: Social engineering theory - What is social engineering? The evolution of social engineering - Why social engineering works? The principles on which social engineering is based - Who are the social engineers? - The legal and ethical aspects of social engineering tests

Part 2: Practical social engineering - Common social engineering techniques (eg, mumble attack, road apples, 10 attack, phishing) - Analysis of social engineering attacks: o personal experience o media case studies - How to practice social engineering techniques

Part 3: The social engineering test - The 'get out of jail free' card - How to conduct a social engineering test: o Target identification o Reconnaissance (passive information gathering and physical reconnaissance) o Pretexting/scenario creation o Attack execution - Evidence collection - How to create a social engineering report - Specific scenarios: o Offices o Data centres o Call centres

Part 4: Defending against social engineering - Logical security controls - Physical security - Security policies - Education and awareness

1.54.3 Biography

Sharon: Sharon Conheady is a social engineer/penetration tester at First Defence Information Security in the UK. She has social engineered her way into dozens of organisations across the UK and abroad, including company offices, sports stadiums, government facilities and more. She has presented on social engineering at security conferences including Deepsec, Recon, CONFidence, ISSE, ISF, SANS Secure Europe and more. After inventing the Internet alongside Al Gore, Sharon moved on to the development of security protocols that were used to crack 128 bit encryption. She holds a degree in Computer Science from Trinity College Dublin and a MSc in Information Security from Westminster University. Three times winner of the Nobel Prize, Sharon enjoys belly dancing and space travel. If you see Sharon around your office, she kindly requests that you open the door to let her in.

Martin: Martin has over 18 years security expertise and has been performing social engineering tests since 1994. He specialises in accessing data centres by using social engineering techniques and bypassing physical security like a geeky James Bond. Martin also undertakes investigations into actual or suspected security breaches, and

specialises in the area of Information Warfare. He attempts to breach not only the logical security of systems and networks, but also the physical security of the infrastructure and buildings, including the use of social engineering when engaged in an "All-Out-Attack" against an enterprise. Having a considerable depth of technical experience in open and distributed systems, as well as networking, in multi-vendor environments, Martin has spent nearly 22 years in the UNIX and TCP/IP arena, having started his career as a developer of UNIX systems.

1.54.4 Innovation

Social engineering is a growing problem in the world of IT security. Because of this, many organisations have started to request social engineering tests as part of their security programmes. It can be difficult to know how to execute an ethical social engineering test. This course will help participants

1.55 Web 2.0 Security – Advanced Attacks and Defense (Training)

Shreeraj Shah shreeraj@blueinfy.com Blueinfy Solutions Pvt. Ltd. +919879027018 India
--

1.55.1 Sample

1.55.2 Synopsis

Description: Introduction and adaptation of new technologies like Ajax, Rich Internet Applications and Web Services has changed the dimension of Application Hacking. We are witnessing new ways of hacking web based applications and it needs better understanding of technologies to secure applications. The only constant in this space is change. In this dynamically changing scenario in the era of Web 2.0 it is important to understand new threats that emerge in order to build constructive strategies to protect corporate application assets. Application layers are evolving and lot of client side attack vectors are on the rise like Ajax based XSS, CSRF, Widget injections, RSS exploits, Mashup manipulations and client side logic exploitations. At the same time various new attack vectors are evolving around SOA by attacking SOAP, XML-RPC and REST. It is time to understand these advanced attack vectors and defense strategies. The course is designed by the author of "Web Hacking: Attacks and Defense", "Hacking Web Services" and "Web 2.0 Security { Defending Ajax, RIA and SOA" bringing his experience in application security and research as part of curriculum to address new challenges. Application Hacking 2.0 is hands-on class. The class features real life cases, hands on exercises, new scanning tools and defense mechanisms. Participants would be methodically exposed to various different attack vectors and exploits. In the class instructor will explain new tools like wsScanner, scanweb2.0, AppMap, AppCodeScan etc. for better pen-testing and application audits. Target audience: Security Consultants, Administrators, Developers, QA team, Code reviewers Course outline: We are going to address following topics in detail: .
Application security fundamentals: Application evolution, Web 2.0 framework, Layered threats, Threat models, Attack vectors and Hacker's perspective. .

Application infrastructure overview: Protocols (HTTP/SSL), SOAP, XML-RPC, REST, Tools for analysis, Server layers and Browsers with plugins. • Application Architecture: Overview to .NET and J2EE application frameworks, Web 2.0 application architecture, Widgets framework, Application layers and components, Resources and interactions, other languages. • Advanced Web Technologies: Ajax, Rich Internet Applications (RIA) and Web Services. • Application attack vectors and detail understanding: SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Path traversal, Session hijacking, LDAP/XPATH/Command injection, Buffer overflow, Input validation bypassing, Database hacks and Blind SQL injections. • Advanced Attacks: Ajax based XSS, CSRF with Web Services, Decompiling Flash and RIA apps, WSDL scanning, XML poisoning, SQL injections through XML, External Entity attacks, Widget exploitation, RSS injections, Cross Domain bypass, and many more. • Application methodologies: Blackbox /Whitebox approaches, tools, techniques and little tricks • Advanced application footprinting and discovery: Leveraging search engines, Cross domain mashup discovery and Web 2.0 application domain enumeration. • Fingerprinting: Web and Application server, Ajax framework, Flash based application and technology fingerprinting. • Advanced browser based attacks: XSS proxy and browser hijacking, Intranet scanning, JavaScript manipulation and DOM injections. • Web Fuzzing: Fuzzing XML, JSON, RPCs etc. for vulnerability detection. • Scanning Web Services: Footprinting, discovery, scanning and attacking XML-RPC, SOAP and REST based applications. • Scanning for vulnerabilities through Source: Function and Method signature mapping, entry point identification, data access layer calls, tracing variables and functions. • Applying validations: Input validations, Output validations, Data access filtering, and Authentication validates. • Web Application Firewall: Advanced content filtering by tools and techniques.

1.55.3 Biography

Shreeraj Shah, B.E., MSCS, MBA, is the founder of Blueinfy, a company that provides application security services. Prior to founding Blueinfy, he was founder and board member at Net Square. He also worked with Foundstone (McAfee), Chase Manhattan Bank and IBM in security space. He is also the author of popular books like Hacking Web Services (Thomson 06) and Web Hacking: Attacks and Defense (Addison-Wesley 03). In addition, he has published several advisories, tools, and whitepapers, and has presented at numerous conferences including RSA, AusCERT, InfosecWorld (Misti), HackInTheBox, Blackhat, OSCON, Bellua, Syscan, ISACA etc. His articles are regularly published on Securityfocus, InformIT, DevX, O'reilly, HNS. His work has been quoted on BBC, Dark Reading, Bank Technology as an expert.

1.55.4 Innovation

Web 2.0 hacking and analysis is new topic and should have lot of interest as well.

1.56 Security Awareness Campaigns (Training)

Stefan Schumacher	stefan.schumacher@kaishakunin.com
Kaishakunin.com	
+49 178 7045957	DE

1.56.1 Sample

<http://kaishakunin.com> (but mostly in German, however I can send you my slides from DeepSec 2008)

1.56.2 Synopsis

The Training aims at system administrators and Tech personal that is responsible for security in an organization. The training will teach the social point of view on security including the psychological fundamentals of social engineering, motivational psychology, learning theories and roles and responsibilities within an organisation.

1.56.3 Biography

Stefan Schumacher is a freelance security consultant with focus on Social-Engineering, Security-Awareness and Counter-Intelligence. He has been active in Open Source and Hacker scene for about 15 yrs. He is a NetBSD developer and is interested in operating systems, cryptography and backup technology. He also writes technical articles and documentation. Since 2007 he is studying Educational Science and Psychology at Otto-von-Guericke-University Magdeburg/Germany and does research in the security field from a social science point of view.

1.56.4 Innovation

it focuses on people, not on technology and is held by an Psychologist ;-)

1.57 The Developmental Psychology of Intrusion Detection Systems (Presentation)

Stefan Schumacher	stefan.schumacher@kaishakunin.com
Kaishakunin.com	
+49 178 7045957	DE

1.57.1 Sample

<http://kaishakunin.com> (but mostly in German, however I can send you my slides from DeepSec 2008)

1.57.2 Synopsis

Intrusion Detection Systems are considered to be an important part of each security strategy. However, there is no IDS available that is able to analyze the social level of an organization. There is also no IDS that is able to adapt to new events and situations and can therefore be considered to be intelligent.

This talk will show how Jean Piaget's Model of Genetic Epistemology can be used to describe how humans acquire knowledge and how it can be used to describe knowledge about security. It will also include a part about theory of knowledge, because this is important if one (eg an IDS) wants to measure security. Concluding, I will give some hints about experiences from the

psychological research of --intelligence--, as there are some parallels regarding --security--.

1.57.3 Biography

Stefan Schumacher is a freelance security consultant with focus on Social-Engineering, Security-Awareness and Counter-Intelligence. He has been active in Open Source and Hacker scene for about 15 yrs. He is a NetBSD developer and is interested in operating systems, cryptography and backup technology. He also writes technical articles and documentation. Since 2007 he is studying Educational Science and Psychology at Otto-von-Guericke-University Magdeburg/Germany and does research in the security field from a social science point of view.

1.57.4 Innovation

it describes security from a complete different point of view. It will include psychology and philosophy and raise fundamental questions about security. Therefore it might help to identify structural problems of a technology orientated security research.

1.58 Recent trends in VoIP security and its countermeasures (Presentation)

Suhas Desai	suhasde@techmahindra.com
Tech Mahindra	
91-9850711221	INDIA

1.58.1 Sample

1.58.2 Synopsis

The purpose of this session is to focus on recent trends in VoIP Security and Open source countermeasures for it. VoIP is being rapidly embraced across most markets as an alternative to the traditional PSTN. The cost savings of VoIP compared to that of circuit switched networks is encouraging companies to move to VoIP. Applications on VoIP technology are getting wide acceptance and securing these applications and its protocols has become essentials for vendors and practitioners. VoIP deployment has brought with it many security concerns like Non-Repudiation, Authentication, Call Quality and Integrity and Privacy; motivating the need for security solutions to deal with the many issues. VoIP security is complicated by the requirement of multiple components which are deployed on the current data network. VoIP is getting wide acceptance and growing rapidly and it leads towards VoIP threats from hacker community. Some common VoIP attacks are Phreaking, eavesdropping, Vishing, viruses and worms, DoS (Denial of Service) and SPIT (Spamming over Internet Telephony), call tampering and man-in-the middle attacks. This session will be more beneficial to security professionals to learn about VoIP Security framework, threats and its countermeasures with available powerful Open source tools and methodology.

1.58.3 Biography

Suhas Desai is a distinguished Security engineer working with Tech Mahindra Ltd in India. He has contributed definitive work in Biometrics security. Suhas is a contributing writer for "Linux Journal", "Linux for You", "Linux+ DVD". He is a feature writer for www.linuxsecurity.com. His articles are translated in world's all major languages. He is a frequent speaker at prominent industry and customer forums, conferences which are important to IT executives and academics. He has been on technical advisory committee for national and International conferences on Security, RFID and Image Processing. He has conducted over 150 workshops on Linux related technology at various reputed universities, institutes and colleges across the world. He has delivered noted sessions at Universiti Sains Malaysia, Penang, Malaysia under "Professor of a day" programme and also at OSSPAC'09 (Open source Singapore Pacific Asia Conference), Singapore at breakout sessions in Feb 2009. Suhas is computer engineering graduate. He has conducted over 150 workshops on Linux and security across the globe. Suhas is a 'Certified Ethical Hacker'. He can be reached at desai.suhas@gmail.com.

1.58.4 Innovation

1. This presentation aims for exploring open source opportunities for securing VoIP network which is a very demanding field nowadays. 2. Security Framework for VoIP Network has been explained in detailed manner. 3. Real attack taxonomy and security testing for VoIP stacks and protocols are explained with case studies and examples. 4. Latest VoIP threats and countermeasure are explained in this presentation. 5. VoIP Security testing methodology is not yet standardized; this presentation will focus on to standardize it.

1.59 Open source for securing data with advanced Crypto-Steganography technology (Presentation)

Suhas Desai	suhasde@techmahindra.com
Tech Mahindra	
919850711221	INDIA

1.59.1 Sample

1.59.2 Synopsis

The purpose of this session is to focus on recent trends in data security. Data security is being rapidly embraced across most markets as threats to the sensitive information are highly increased in recent years. Due to these threats, companies are encouraged to use advanced Cryptography, Steganography techniques to secure their sensitive data. Wide acceptance to the open source technology is also encouraging community to use open solutions for Crypto-Steganography technology with open source tools like Stepic and EzPyCrypto. EzPyCrypto encrypts and decrypts arbitrary-sized pieces of data. It is mainly used for adding digital signatures. Stepic is new Python module which can be used to hide arbitrary data within images. In older

Steganography techniques, hiding plain data in images was main objective. However with usage of open source tools with advanced Crypto-Steganography techniques we can easily encrypt data with some key and hide it inside image then that is more secure. This session will be more beneficial to security professionals to learn about data Security framework, threats and its countermeasures by applying advanced Crypto-Steganography technology with available powerful Open source tools like Stepic and EzPyCrypto.

1.59.3 Biography

Suhas Desai is a distinguished Security analyst working with Tech Mahindra Ltd in India. In TechM, he is developing capabilities in VoIP security services. He has undertaken vulnerability assessments for leading Telco's in Europe and USA.

Suhas is a contributing writer for "Linux Journal", "Linux for You", "Linux+ DVD" magazines. He is Feature writer for www.linuxsecurity.com. His articles are translated in world's all major languages. His research papers on RFID are published in various reputed proceedings and journals like - ISA EXPO 2004, TX, USA.; "InTech" Journal, Global Automation Magazine, TX, USA ; WIA'05, 11th IEEE real time & Embedded Systems Symposium, CA, USA.; E-SMART 2005, France. Suhas is an IPv6 certified Network engineer. He has delivered sessions on "Linux Programming and security" at Universiti Sains Malaysia, Penang, Malaysia. He will be speaking at OSSPAC'09 (Open source Singapore Pacific Asia Conference), Singapore at breakout sessions in Feb 2009 on --Open Source considerations for VoIP Security--. He is a frequent speaker at prominent industry and customer forums, conferences which are important to IT executives and academics. He has been on technical advisory committee for national and International conferences on Security, RFID and Image Processing.

Suhas is a computer engineering graduate.

1.59.4 Innovation

*Recent trends in cryptography and steganography has been covered. *More focused on data security with combination of cryptography and steganography with open source tools like Stepic and EzPyCrypto.

1.60 Keykeriki - Universal Wireless Keyboard Sniffing For The Masses (Presentation)

Thorsten Schroeder	ths@remote-exploit.org
Remote-Exploit.org	
+49-171-3872835	Germany

1.60.1 Sample

<http://www.remote-exploit.org/Keykeriki.html>

1.60.2 Synopsis

1.5 years after releasing our whitepaper --27Mhz Wireless Keyboard Analysis Report-- about wireless keyboard insecurities, we are proud to present the universal wireless keyboard sniffer: Keykeriki. This device enables everybody to analyse wireless keyboard signals of different vendors. A proof-of-concept

device was released in the end of May 2009 and we are still extending the techniques, hardware and software. For example: 2.4GHz, sending keystrokes using big antennas after crypto is cracked etc.

1.60.3 Biography

TÜV Rheinland Secure iT (technical leader) -> Reurity Labs (sr security consultant) -> Dreamlab Technologies (sr security consultant)

1.60.4 Innovation

It's a neat device which is small and can be used as standalone application with a mass storage (SDCard) attached and a connector for external antennas. It decrypts and cracks crypto keys on-the-fly using a very simple but efficient statistic analysis approach and is maybe able to send keystrokes to a remote computer in the future ;)

1.61 Exploit Analysis and Malware Reverse Engineering (Training)

Tillmann Werner werner@cs.uni-bonn.de University of Bonn +49 228 73 4587 Germany
--

1.61.1 Sample

1.61.2 Synopsis

The training gives an introduction into deep analysis of common system compromises from an incident handler's perspective. This includes the analysis of attack traces that contain buffer overflow exploits both with static methods and in a debugger at the assembly level. The second half of the training provides an introduction to malware reverse engineering. Attendees will work on real attack traces and malware samples caught in the wild. Each person will receive a USB drive with a pre-installed virtual analysis lab environment.

1.61.3 Biography

Tillmann Werner used to work as an incident handler at the German national CERT and is currently employed as a computer scientist at the University of Bonn. He is a member of the Honeynet Project and has been doing research in the area of network-based attacks for more than 6 years.

1.61.4 Innovation

... people can start using what they learn right away.

1.62 Enterprise Web Application Security - Attacks & Defense (Training)

Vimal Patel	vimal@blueinfy.com
Blueinfy Solutions Pvt. Ltd.	
+919909985867	India

1.62.1 Sample

1.62.2 Synopsis

Overview: Enterprise application source code, independent of languages and platforms, is a major source of vulnerabilities. The class is designed and developed to focus on enterprise architecture and application analytics to discover vulnerabilities. One of the CSI surveys on vulnerability distribution suggests that in 64% of cases, a vulnerability crops up due to programming errors and in 36% of cases, due to configuration issues. We will be covering analysis techniques, with tools, for assessment and review of enterprise application source code. Enterprise 2.0 and mashups, along with other different Web 2.0 concepts, reinforced by hands-on experience, will help in understanding next generation application requirements. It is imperative to know source code review methodologies and strategies for analysis. The emphasis of the class would be to develop a complete understanding of source code analysis, audit methodologies, techniques and tools. Knowledge gained would help in analyzing and securing enterprise applications at all different stages - architecture, design and/or development. The course is designed by the author of --Web Hacking: Attacks and Defenses--, "Hacking Web Services" and "Web 2.0 Security { Defending Ajax, RIA and SOA", bringing his experience in application security and research to the curriculum. Special focus is given to compliance and Top-25 errors for enterprise applications. This class is hands-on and needs laptops to implement its numerous exercises designed to run hand-in-hand with their concepts. The class features real life cases, hands-on exercises, code scanning tools and defense plans. Participants would be methodically taken down to the source code level and exposed to the possible flaws in architecture, design and coding practices. The class would then focus on the proper ways of writing secure code and analyzing the code base.

Course pre-requisite

- Basic knowledge on Enterprise Application Architecture and Design.
- Understanding of one of the languages from Java, C# (.NET) or PHP.
- Familiarity with application scanning tools and approaches would be handy.
- Script writing ability using perl, ruby or python would help in coding quick tools (Not a must)
- It is also recommended for someone who is new to the application security space and is looking for quick lessons in source code audit and testing.

Who Should Attend the Class

- Source code analyzers, auditors (PCI-DSS), consultants, pen-testers and security professionals who are looking to upgrade their skill-set on enterprise application security and source code analysis.
- QA and Developers who are looking for new tools and methodologies.
- Program managers and team leaders, responsible for securing SDLC in their enterprise environment.

Learning Objectives:

- Application Source Code Assessment and Audit Methodologies
- Detecting OWASP Top 10 and CWE Top 25 Errors and vulnerabilities?
- Enhancing your ability to understand Enterprise Application Framework and Structures
- Dealing with different protocols and structures in enterprise environment for vulnerability

assessment. • Enterprise Architecture overview, .NET and J2EE application frameworks and security, Application layers and components, Resources and interactions, Enterprise RPC and API calls. • Detecting the state of source code for attack vectors like SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Path traversal, Session hijacking, LDAP/XPATH/Command injection, Buffer overflow, Input validation bypassing, Database hacks, Ajax exploits, Web Services attack vectors etc. • Using tools and writing scripts for source code analysis and vulnerability mapping • Code review methodologies by Spidering the code, enumerating blocks and identifying modules. • Scanning for vulnerabilities and analysis by Function and Method signature mapping, entry point identification, data access layer calls, tracing variables and functions. • Source Code Auditing in an enterprise environment for compliance and standards like PCI-DSS. • Applying validations across an enterprise application by Input validations, Output encoding/validations, Data access layer filtering, Authentication validations etc. • Decomposing assemblies to discover other security vulnerabilities and structured analysis. • Key security aspects and Domains for enterprise security like Authentication, Authorization, Session management, Crypto usage and Error handling. • Defense plans and strategies, Secure objects, functions and wrappers • Detecting vulnerabilities in advanced technologies like Ajax, Rich Internet Applications (RIA) and SOA • XML and Web Services security for SOAP, XML-RPC and REST base attacks and secure coding. • Client side coding and security for Ajax and JavaScript analysis, Flash based application reviews and Browser security. • Understanding of various tools and frameworks with hands-on experience. What to bring To participate in hands-on exercises you will need to come with a windows-based laptop. • OS : XP, Vista or Server family • Please install .NET framework • 1 GB RAM • All other tools will be provided • Laptop should be wi-fi enabled Hands-on: All concepts taught in this class are punctuated with hands-on exercises based on situations observed in real life. The class ends with a challenge exercise. Working within a limited time period, participants are expected to analyze the code, identify loopholes, exploit vulnerabilities present in the applications and suggest appropriate defense strategies.

1.62.3 Biography

Vimal Patel (Founder and Director) Vimal Patel is founder of Blueinfy, a company that provides products and services for application security. Vimal leads research and product development efforts at Blueinfy. Prior to founding Blueinfy, he held position of Vice President at Citigroup where he led architecture, design and development of various financial applications. Vimal holds Masters in Computer Science. Vimal has over a decade of experience and expertise in many technologies. His experience ranges from design of complex digital circuits and microcontroller based products to enterprise applications.

1.62.4 Innovation

It is great training for security analyst and developers.

1.63 Malware for SoHo Routers - The war has begun (Presentation)

naxxatoe	naxx@nicenamecrew.com
NNC Security Research, Myself ;)	
+436645211403	.at

1.63.1 Sample

1.63.2 Synopsis

Malware for soho routers has been a hot topic thru-out the last year and to this day the trend continues. With new super worms like psyb0t and other yet unnamed fears on the rise, we will take a close look at the current situation and discuss the things to come. So called Soho (Small home and office) routers have become extremely popular in the last few years. While the good guys where busy trying to prevent malware from infiltrating their desktop systems, the bad guys had gone one step ahead of the game and started to experiment with these devices. With new possible cyber threads emerging from the web every day, this is your chance to gain the necessary knowledge to protect yourself and your business. Participants will learn the fundamental basics how routers can be taken over. After a few practical examples we will then move into the field of malware. You will not only gain the basic knowlege of router hacking and a bit of knowledge about malware here. This is the real stuff, detailed analysis of current threads, counter measures and a lot of cool shit.

1.63.3 Biography

naxxatoe (Sebastian Maier) is a security researcher based in Vienna, Austria. His bleeding edge research and extensive knowledge led him to travel the world and be a speaker on a lot of security conferences thru-out 2008. Current topics of his research include malware analysis, all different types of fraud that are committed over the internet. Not to mention he was the first one to bring up router security issues and router malware research at all.

1.63.4 Innovation

Should be accepted because of entertainment purposes, 0sec it security threats, live demo's, bleeding edge security research,...

1.64 Malware case study: The Zeus evolution (Presentation)

vicente diaz	vdiaz@s21sec.com
s21sec	
34625570927	spain

1.64.1 Sample

1.64.2 Synopsis

Zeus is a banking trojan active since years who has evolved over time making it increasingly more difficult for researchers and security experts to analyse it. This is done by using different types of encryption, hiding techniques, new features (screenshots, execution of binaries...), changes in the C&C, etc. This presentation aims to give technical information about this evolution, including, as innovation, the process of extracting the encryption key for the configuration files, which will be useful in combating this type of malware. This talk is intended to give an idea of the state of the art of malware today - major players, behaviour, institutions involved - focusing on one of the main malware families we face today: Zeus / Zbot / Wsnpoem.

1.64.3 Biography

ecrime manager at s2lsec computer sciences engineering degree PhD in Artificial Intelligence (in progress)

1.64.4 Innovation

Provides a global overview of the latests trends in malware and dark market, explaining the main reasons for a banking trojan to succeed and overpass existing countermeasures.