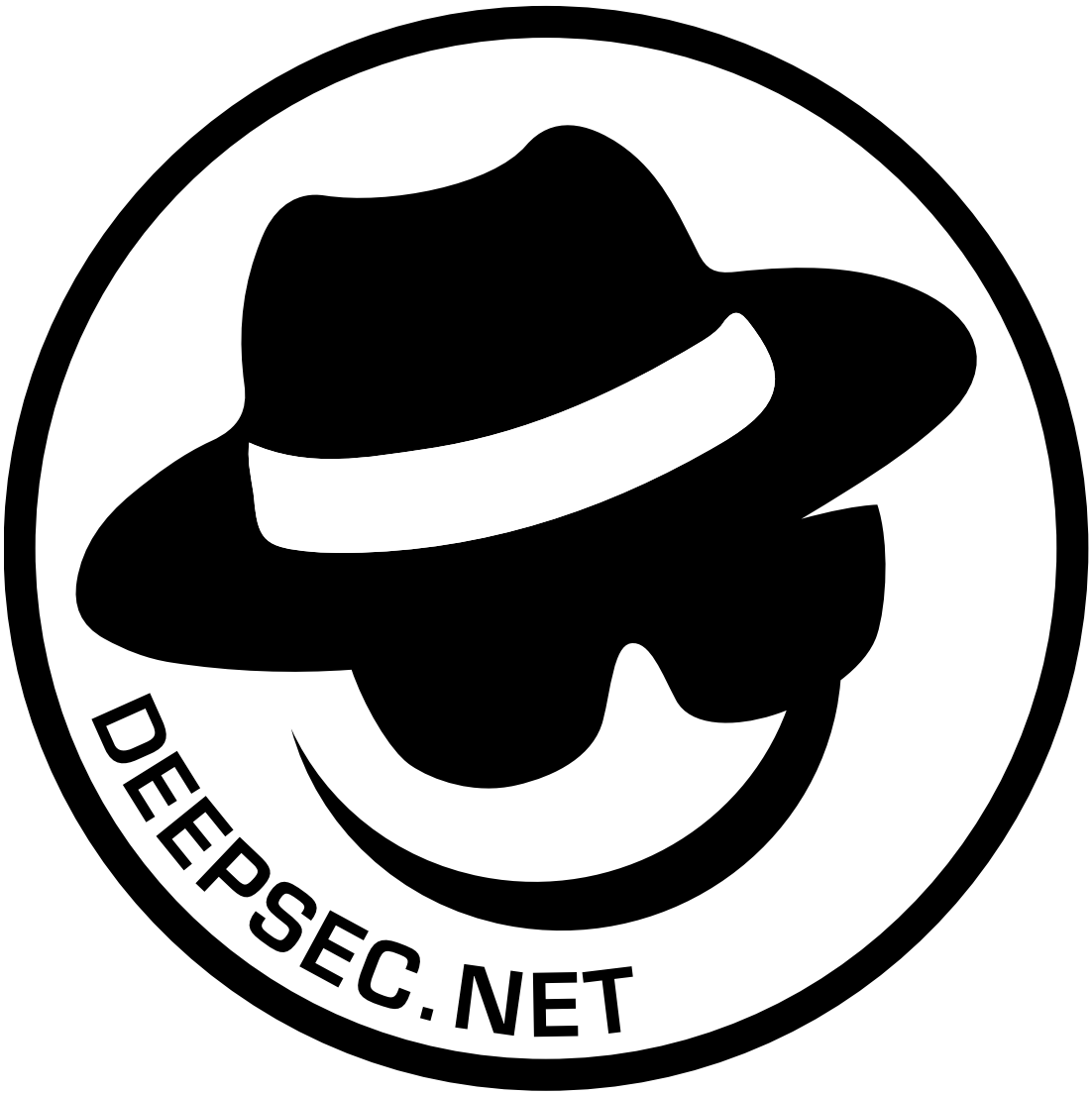


press review 2014

media coverage

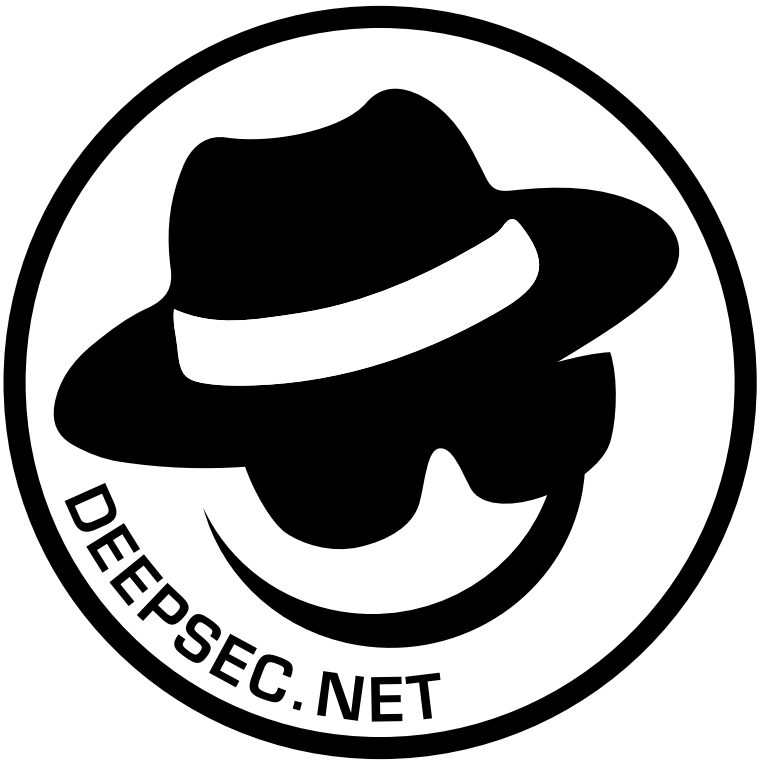
2014

contents

press releases

2014

media coverage 2014



http://www.golem.de/news/aslr-speicherrandomisierung-unter-linux-mangelhaft-1412-111010.html

ASLR

Speicher-Randomisierung unter Linux mangelhaft

Datum: 8.12.2014

Autor: Hanno Böck

Die Randomisierung des Speicherlayouts (ASLR) gilt als wichtige Maßnahme, um die Ausnutzung von Sicherheitslücken zu erschweren. Unter Linux hat das Konzept Mängel, aber viel gravierender ist, dass vielfach ASLR überhaupt nicht eingesetzt wird.Zu den häufigsten Sicherheitslücken gehören Fehler in der Speicherverwaltung von C-Programmen, beispielsweise klassische Buffer Overflows. Moderne Betriebssysteme haben inzwischen eine Reihe von Schutzmaßnahmen implementiert, um die Ausnutzung von solchen Fehlern zu erschweren. Eine Möglichkeit ist die sogenannte Address Space Layout Randomisation (ASLR).

Eine Strategie zur Ausnutzung von Sicherheitslücken ist es häufig, das System des Opfers dazu zu bringen, an eine bestimmte Stelle im Speicher zu springen und dort Code auszuführen. Damit derartige Angriffe jedoch funktionieren, muss der Angreifer wissen, an welchen Speicheradressen sich was befindet. Hier setzt ASLR an: Durch die zufällige Verteilung von Code, Heap und Stack im Speicher werden solche Angriffe enorm erschwert. ASLR ist nicht perfekt. Durch die Nutzung von weiteren Lücken kann ein Angreifer Speicheradressen erfahren, das sogenannte Heap Spraying setzt darauf, bösartigen Code möglichst oft im Speicher zu wiederholen, so dass bei einem zufälligen Sprung die Chance besteht, den entsprechenden Code zu erreichen. Doch auch wenn ASLR nicht alle Angriffe verhindert, gilt es als wichtiger Baustein moderner Sicherheitskonzepte.

Linux war Pionier in Sachen ASLR

Linux war eigentlich einst Pionier in Sachen Speicherrandomisierung. Das PaX-Projekt hatte bereits 2002 mittels eines Kernel-Patches die Möglichkeit von ASLR eingeführt. Ein Jahr später führte OpenBSD als erstes Betriebssystem ASLR als Standardfunktion ein. PaX existiert noch heute und ist Teil des Grsecurity-Projekts, das einen Kernel-Patch mit zahlreichen zusätzlichen Sicherheitsfunktionen für den Linux-Kernel bereitstellt. Doch PaX wurde nie Teil des offiziellen Linux-Kernels. Mit der Version 2.6.12 führte Linux eine eigene Implementierung von ASLR ein. Doch das Problem dabei: In vielen Fällen greift diese überhaupt nicht. Während unter Windows, Mac OS X, Android und iOS ASLR inzwischen Standard ist, wird es unter Linux nach wie vor nur mangelhaft genutzt.

Der Hintergrund ist, dass nicht jedes Programm automatisch an beliebige Speicherbereiche geladen werden kann. Klassischerweise können Sprungbefehle in Software auf feste Adressen verweisen. Damit der Code an beliebige

Speicherbereiche geladen werden kann, muss dies bereits bei der Kompilierung berücksichtigt werden. Der gcc-Compiler bietet hierfür die Option -fpic (pic steht für "Position Independent Code"), für den Linker muss die Option -pie (für "Position Independent Executable") angegeben werden. Und genau hier hapert es: Alle großen Distributionen nutzen standardmäßig noch Programme, die nicht mit den entsprechenden Optionen für positionsunabhängigen Code kompiliert wurden.

Geringe Auswirkungen auf die Leistungen

Die Nutzung von positionsunabhängigem Code hat Auswirkungen auf die Performance. Insbesondere auf alten PC-Systemen mit 32 Bit ist das ein Problem, denn hier ist die Zahl der Prozessorregister knapp und für den positionsunabhängigen Code wird ein zusätzliches Register benötigt. Auf 64-Bit-Systemen sind die Performanceeinbußen hingegen sehr gering. Bei einem Test von uns mit der Codierung eines Videos mit dem Programm ffmpeg betrug der Unterschied etwa 1,5 Prozent. Es gibt Patches für den gcc-Compiler und Binutils, welche die Leistungseinbußen noch weiter reduzieren und die in den kommenden Versionen der entsprechenden Tools enthalten sein werden. Auch ohne positionsunabhängigen Code ist die Adressrandomisierung nicht völlig nutzlos. Der Stack- und der Heap-Speicher landen trotzdem an zufälligen Adressen und Bibliotheken werden generell mit positionsunabhängigem Code kompiliert. Aber für einen wirklichen Schutz reicht das nicht. Insbesondere um vor sogenannten Return-Oriented-Programming-Angriffen zu schützen, ist eine Randomisierung des eigentlichen Programmcodes wichtig.

Firefox hat ASLR nach Problemen wieder deaktiviert

Mozilla hatte vor kurzem versucht, Firefox für Linux mit den entsprechenden Optionen zu kompilieren. Dabei trat ein unerwartetes Problem auf: Der GNOME-Dateimanager Nautilus erkannte die entsprechend kompilierten ausführbaren Dateien nicht als solche und Firefox ließ sich über den Dateimanager nicht starten. Firefox schaltete daraufhin die entsprechende Funktion wieder ab.

Der Grund für die Nautilus-Probleme, die bei einem Test von Golem.de unter dem KDE-Dateimanager Dolphin in genau derselben Form auftraten: Der Dateimanager greift zur Erkennung von ausführbaren Dateien auf die Bibliothek libmagic zurück, die Teil des Tools file ist. Die libmagic-Bilbiothek wiederum kann positionsunabhängige Linux-Binaries nicht von Bibliotheken unterscheiden und liefert den MIME-Type für Bibliotheken zurück. Sowohl Binaries als auch Bibliotheken verwenden unter Linux das Elf-Dateiformat.

Chrome wird standardmäßig mit Adressrandomisierung ausgeliefert, ebenso der auf Firefox basierende Tor-Browser. Anders als Mozilla liefern diese beiden Browser ein Shellskript zum Starten mit, sie sind somit von dem Problem in den Dateimanagern nicht betroffen.

In Linux-Distributionen kein Standard

Bei den Linux-Distributionen ist die Situation in Sachen ASLR sehr gemischt. Fedora und Debian aktivieren das Feature nur für einzelne Tools, die als besonders sicherheitskritisch gelten. Gleiches gilt auch für andere auf Debian basierende Distributionen wie Ubuntu. Selbst Tails, ein auf Datenschutzeinstellungen und Sicherheit getrimmtes Linux-System, nutzt ASLR nicht standardmäßig. Es gibt auch immer wieder generelle Probleme mit der ASLR-Implementierung von Linux. Mitglieder von Google's Projekt Zero entdeckten beim Versuch, eine Glibc-Sicherheitslücke auszunutzen, dass man zumindest unter 32-Bit-Systemen die Speicherrandomisierung von Suid-Binaries mit Hilfe des Befehls ulimit weitgehend deaktivieren kann.

offset2lib-Schwäche entdeckt

Zuletzt hatten die Sicherheitsforscher Hector Marco-Gisbert und Ismael Ripoll auf der Deepsec-Konferenz in Wien eine ausführliche Analyse des ASLR-Konzepts von Linux vorgestellt und ein weiteres Problem entdeckt, das sie offset2lib getauft haben: Linux legt zwar den Programmcode an einer zufälligen Stelle im Speicher ab, aber der Hauptprogrammcode und der Code von nachgeladenen Bibliotheken wird immer im selben Abstand abgelegt. Das bedeutet, dass ein Angreifer, der im Hauptprogramm aufgrund eines Fehlers möglicherweise Kenntnis von einer Speicheradresse erlangt, damit eine Sicherheitslücke in einer Bibliothek ausnutzen kann.

Android ist von der offset2lib-Schwäche ebenfalls betroffen. Anders als unter gängigen Linux-Distributionen kommt unter Android in aller Regel auch Adressrandomisierung zum Einsatz. Nicht betroffen sind Linux-Systeme, die Pax benutzen. Die Forscher haben einen Patch vorgelegt, der zur Zeit auf der Kernel-Mailingliste diskutiert wird.
Solange die meisten Linux-Distributionen aber keine Dateien mit positionsunabhängigem Code ausliefern, hilft das alles nicht viel. Die Distributionen sollten hier dringend handeln und die Speicherrandomisierung mittels ASLR auch unter Linux zum Standard machen.

ASLR

Speicher-Randomisierung unter Linux mangelhaft

Die Randomisierung des Speicherlayouts (ASLR) gilt als wichtige Maßnahme, um die Ausnutzung von Sicherheitslücken zu erschweren. Unter Linux hat das Konzept Mängel, aber viel gravierender ist, dass vielfach ASLR überhaupt nicht eingesetzt wird.

Zu den häufigsten Sicherheitslücken gehören Fehler in der Speicherverwaltung von C-Programmen, beispielsweise klassische Buffer Overflows. Moderne Betriebssysteme haben inzwischen eine Reihe von Schutzmaßnahmen implementiert, um die Ausnutzung von solchen Fehlern zu erschweren. Eine Möglichkeit ist die sogenannte Address Space Layout Randomisation (ASLR).

Eine Strategie zur Ausnutzung von Sicherheitslücken ist es häufig, das System des Opfers dazu zu bringen, an eine bestimmte Stelle im Speicher zu springen und dort Code auszuführen. Damit derartige Angriffe jedoch funktionieren, muss der Angreifer wissen, an welchen Speicheradressen sich was befindet. Hier setzt ASLR an: Durch die zufällige Verteilung von Code, Heap und Stack im Speicher werden solche Angriffe enorm erschwert. ASLR ist nicht perfekt. Durch die Nutzung von weiteren Lücken kann ein Angreifer Speicheradressen erfahren, das sogenannte Heap Spraying setzt darauf, bösartigen Code möglichst oft im Speicher zu wiederholen, so dass bei einem zufälligen Sprung die Chance besteht, den entsprechenden Code zu erreichen. Doch auch wenn ASLR nicht alle Angriffe verhindert, gilt es als wichtiger Baustein moderner Sicherheitskonzepte.

Linux war Pionier in Sachen ASLR

Linux war eigentlich einst Pionier in Sachen Speicherrandomisierung. Das PaX-Projekt hatte bereits 2002 mittels eines Kernel-Patches die Möglichkeit von ASLR eingeführt. Ein Jahr später führte OpenBSD als erstes Betriebssystem ASLR als Standardfunktion ein. PaX existiert noch heute und ist Teil des Grsecurity-Projekts, das einen Kernel-Patch mit zahlreichen zusätzlichen Sicherheitsfunktionen für den Linux-Kernel bereitstellt. Doch PaX wurde nie Teil des offiziellen Linux-Kernels. Mit der Version 2.6.12 führte Linux eine eigene Implementierung von ASLR ein. Doch das Problem dabei: In vielen Fällen greift diese überhaupt nicht. Während unter Windows, Mac OS X, Android und iOS ASLR inzwischen Standard ist, wird es unter Linux nach wie vor nur mangelhaft genutzt.

Der Hintergrund ist, dass nicht jedes Programm automatisch an beliebige Speicherbereiche geladen werden kann. Klassischerweise können Sprungbefehle in Software auf feste Adressen verweisen. Damit der Code an beliebige Speicherbereiche geladen werden kann, muss dies bereits bei der Kompilierung berücksichtigt werden. Der gcc-Compiler bietet hierfür die Option -fpic (pic steht für "Position Independent Code"), für den Linker muss die Option -pie (für "Position Independent Executable") angegeben werden. Und genau hier hapert es: Alle großen Distributionen nutzen standardmäßig noch Programme, die nicht mit den entsprechenden Optionen für positionsunabhängigen Code kompiliert wurden.

PaX liefert eine deutlich bessere Speicherrandomisierung als der Standard-Linux-Kernel. (Bild: PaX)

Artikel: ASLR Speicher-Randomisierung unter Linux mangelhaft
Inhalt: Firefox hat ASLR nach Problemen wieder deaktiviert
Datum: 8.12.2014, 16:00
Autor: Hanno Böck
Themen: Linux, Sicherheitslücke, Mozilla, Technologie, Applikationen, Open Source, Security

Geringe Auswirkungen auf die Leistungen

Die Nutzung von positionsunabhängigem Code hat Auswirkungen auf die Performance. Insbesondere auf alten PC-Systemen mit 32 Bit ist das ein Problem, denn hier ist die Zahl der Prozessorregister knapp und für den positionsunabhängigen Code wird ein zusätzliches Register benötigt. Auf 64-Bit-Systemen sind die Performanceeinbußen hingegen sehr gering. Bei einem Test von uns mit der Codierung eines Videos mit dem Programm *ffmpeg* betrug der Unterschied etwa 1,5 Prozent. Es gibt Patches für den gcc-Compiler und Binutils, welche die Leistungseinbußen noch weiter reduzieren und die in den kommenden Versionen der entsprechenden Tools enthalten sein werden.

Auch ohne positionsunabhängigen Code ist die Adressrandomisierung nicht völlig nutzlos. Der Stack- und der Heap-Speicher landen trotzdem an zufälligen Adressen und Bibliotheken werden generell mit positionsunabhängigem Code kompiliert. Aber für einen wirklichen Schutz reicht das nicht. Insbesondere um vor sogenannten Return-Oriented-Programming-Angriffen zu schützen, ist eine Randomisierung des eigentlichen Programmcodes wichtig.

Firefox hat ASLR nach Problemen wieder deaktiviert

Mozilla hatte vor kurzem versucht, Firefox für Linux mit den entsprechenden Optionen zu kompilieren. Dabei trat ein unerwartetes Problem auf: Der GNOME-Dateimanager Nautilus erkannte die entsprechend kompilierten ausführbaren Dateien nicht als solche und Firefox ließ sich über den Dateimanager nicht starten. Firefox schaltete daraufhin die entsprechende Funktion wieder ab.

Der Grund für die Nautilus-Probleme, die bei einem Test von Golem.de unter dem KDE-Dateimanager Dolphin in genau derselben Form auftraten: Der Dateimanager greift zur Erkennung von ausführbaren Dateien auf die Bibliothek libmagic zurück, die Teil des Tools file ist. Die libmagic-Bilbiothek wiederum kann positionsunabhängige Linux-Binaries nicht von Bibliotheken unterscheiden und liefert den MIME-Type für Bibliotheken zurück. Sowohl Binaries als auch Bibliotheken verwenden unter Linux das Elf-Dateiformat.

Chrome wird standardmäßig mit Adressrandomisierung ausgeliefert, ebenso der auf Firefox basierende Tor-Browser. Anders als Mozilla liefern diese beiden Browser ein Shellskript zum Starten mit, sie sind somit von dem Problem in den Dateimanagern nicht betroffen.

In Linux-Distributionen kein Standard

Bei den Linux-Distributionen ist die Situation in Sachen ASLR sehr gemischt. Fedora und Debian aktivieren das Feature nur für einzelne Tools, die als besonders sicherheitskritisch gelten. Gleiches gilt auch für andere auf Debian basierende Distributionen wie Ubuntu. Selbst Tails, ein auf Datenschutzeinstellungen und Sicherheit getrimmtes Linux-System, nutzt ASLR nicht standardmäßig.

Es gibt auch immer wieder generelle Probleme mit der ASLR-Implementierung von Linux. Mitglieder von Google's Projekt Zero entdeckten beim Versuch, eine Glibc-Sicherheitslücke auszunutzen, dass man zumindest unter 32-Bit-Systemen die Speicherrandomisierung von Suid-Binaries mit Hilfe des Befehls ulimit weitgehend deaktivieren kann.

Videos

E-Fan fliegt über den Ärmelkanal - Airbus

Verwandte Artikel

ENTERPRISE-LINUX
CentOS bringt monatliche Rolling-Releases

PaX liefert eine deutlich bessere Speicherrandomisierung als der Standard-Linux-Kernel. (Bild: PaX)

Artikel: ASLR Speicher-Randomisierung unter Linux mangelhaft

Inhalt: Firefox hat ASLR nach Problemen wieder deaktiviert

Datum: 8.12.2014, 16:00

Autor: Hanno Böck

Themen: Linux, Sicherheitslücke, Mozilla, Technologie, Applikationen, Open Source, Security

Teilen: 5 8 18 5

Tools: Drucken

offset2lib-Schwäche entdeckt

Zuletzt hatten die Sicherheitsforscher Hector Marco-Gisbert und Ismael Ripoll auf der Deepsec-Konferenz in Wien eine ausführliche Analyse des ASLR-Konzepts von Linux vorgestellt und ein weiteres Problem entdeckt, das sie offset2lib getauft haben: Linux legt zwar den Programmcode an einer zufälligen Stelle im Speicher ab, aber der Hauptprogrammcode und der Code von nachgeladenen Bibliotheken wird immer im selben Abstand abgelegt. Das bedeutet, dass ein Angreifer, der im Hauptprogramm aufgrund eines Fehlers möglicherweise Kenntnis von einer Speicheradresse erlangt, damit eine Sicherheitslücke in einer Bibliothek ausnutzen kann.

Android ist von der offset2lib-Schwäche ebenfalls betroffen. Anders als unter gängigen Linux-Distributionen kommt unter Android in aller Regel auch Adressrandomisierung zum Einsatz. Nicht betroffen sind Linux-Systeme, die Pax benutzen. Die Forscher haben einen Patch vorgelegt, der zur Zeit auf der Kernel-Mailingliste diskutiert wird.

Solange die meisten Linux-Distributionen aber keine Dateien mit positionsunabhängigem Code ausliefern, hilft das alles nicht viel. Die Distributionen sollten hier dringend handeln und die Speicherrandomisierung mittels ASLR auch unter Linux zum Standard machen. •

1 2

ASLR: Speicher-Randomisierung unter Linux mangelhaft

http://oe1.orf.at/programm/390557
matrix - computer & neue medien

Datum: 30.11. 2014

Autor: Sarah Kriesche

1. Hacker-Training Die DeepSec 2014
2. Ist Privatsphäre wirklich so wichtig? Über Bürgerrechte und Lippenbekenntnisse

EPA/PETER STEFFEN

Menschen vor einem bunten Weltkartenbild

1. Die im September geleakten Nacktbilder von US-Prominenten, die aus dem Online-Speicherdienst iCloud gestohlen wurden, zeigen ein weiteres Mal, dass im Netz nichts und niemand sicher ist. Manchmal sind es nur zu einfach gesetzte Passwörter, die es Kriminellen leicht machen, Fotos, Kreditkartendetails oder ganze Identitäten zu stehlen.
Um die Sicherheits-Herausforderungen der IT zu beleuchten und aus den Fehlern der Vergangenheit zu lernen, holt die "DeepSec"-Konferenz auch dieses Jahr internationale Vortragende Ende November nach Wien. Ein erklärtes Ziel dieser Internationalen Konferenz ist es, Akademiker, Regierungs- und Wirtschaftsvertreter, sowie die Hacking-Community zusammenzubringen und den Dialog rund um das Thema Sicherheit zu intensivieren, wie Sarah Kriesche berichtet.

2. Wie stehen die Europäerinnen und Europäer zum Thema Überwachung, Privatsphäre und Regulierung des Internet? Das wollte die EU-Kommission wissen und initiierte drei Bürgerbeteiligungsprojekte namens SURPRISE, PRISMS und PACT. Mitte November trafen sich Expertinnen und Experten auf Einladung des Instituts für Technikfolgenabschätzung ITA an der Akademie der Wissenschaften in Wien, um die Ergebnisse zu diskutieren. Entgegen allen Klischees sorgen sich junge Leute zum Beispiel mehr um die Privatsphäre als ältere. Mariann Unterluggauer war dabei und hat die Anwesenheit von Gästen wie Ben Hayes von Statewatch und Peter Hustinx, ehemals Datenschutzbeauftragter in der Barroso-Kommission, dazu genutzt, um der Frage nachzugehen, warum es so schwer ist, das Bedürfnis der Bevölkerung nach Datenschutz, Privatheit und Kommunikationsfreiheit politisch umzusetzen.

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

matrix - computer & neue medien

Sonntag
30. November 2014
22:30

1. Hacker-Training Die DeepSec 2014
2. Ist Privatsphäre wirklich so wichtig? Über Bürgerrechte und Lippenbekenntnisse

EPA/PETER STEFFEN

1. Die im September geleakten Nacktbilder von US-Prominenten, die aus dem Online-Speicherdienst

iCloud gestohlen wurden, zeigen ein weiteres Mal, dass im Netz nichts und niemand sicher ist. Manchmal sind es nur zu einfach gesetzte Passwörter, die es Kriminellen leicht machen, Fotos, Kreditkartendetails oder ganze Identitäten zu stehlen.
Um die Sicherheits-Herausforderungen der IT zu beleuchten und aus den Fehlern der Vergangenheit zu lernen, holt die "DeepSec"-Konferenz auch dieses Jahr internationale Vortragende Ende November nach Wien. Ein erklärtes Ziel dieser Internationalen Konferenz ist es, Akademiker, Regierungs- und Wirtschaftsvertreter, sowie die Hacking-Community zusammenzubringen und den Dialog rund um das Thema Sicherheit zu intensivieren, wie Sarah Kriesche berichtet.

2. Wie stehen die Europäerinnen und Europäer zum Thema Überwachung, Privatsphäre und Regulierung des Internet? Das wollte die EU-Kommission wissen und initiierte drei Bürgerbeteiligungsprojekte namens SURPRISE, PRISMS und PACT. Mitte November trafen sich Expertinnen und Experten auf Einladung des Instituts für Technikfolgenabschätzung ITA an der Akademie der Wissenschaften in Wien, um die Ergebnisse zu diskutieren. Entgegen allen Klischees sorgen sich junge Leute zum Beispiel mehr um die Privatsphäre als ältere. Mariann Unterluggauer war dabei und hat die Anwesenheit von Gästen wie Ben Hayes von Statewatch und Peter Hustinx, ehemals Datenschutzbeauftragter in der Barroso-Kommission, dazu genutzt, um der Frage nachzugehen, warum es so schwer ist, das Bedürfnis der Bevölkerung nach Datenschutz, Privatheit und Kommunikationsfreiheit politisch umzusetzen.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Dezember
Gestern
Morgen
Heute
Wissen Downloads

Social Media

Zwei Klicks für mehr Datenschutz: Erst wenn Sie dieses Feld durch einen Klick aktivieren, werden die Buttons aktiv, und Sie können Ihre Empfehlung an Facebook, Twitter und Google+ senden. Schon beim Aktivieren werden Informationen an diese Netzwerke übertragen und dort gespeichert. Näheres erfahren Sie durch einen Klick auf das i.

- nicht mit Facebook verbundenSocial-Media-Dienste aktivieren
- nicht mit Twitter verbunden
- nicht mit Google+ verbunden

http://oe1.orf.at/programm/390226

Digital.Leben

Datum: 27. 11 2014

Autor: Frank Zeller

Hacker mit Ethos

Moderation und Redaktion: Franz Zeller

EPA/JOCHENLUEBKE

Frau hält Laptop

Sicherheitsexperten haben oft etwas Paranoides an sich - sie wittern allerorts Überwachung. Und das häufig zu Recht: Webseiten versuchen mit Cookies unser Surf-Verhalten aufzuzeichnen, Fitnessgadgets speichern unseren Körperzustand - und melden ihn weiter.

Mit Themen wie diesen beschäftigte sich letzte Woche die Sicherheitskonferenz "Deepsec" in Wien. Der Nachwuchs in der IT-Sicherheitsszene konnte sich tags darauf bei den sogenannten B-Sides austoben. Sarah Kriesche hat dort einen "ethischen Hacker" zum Interview getroffen.

zur Sendereihe

Standort: oe1.ORF.at

Navigation

Digital.Leben

Donnerstag
27. November 2014
16:55

Hacker mit Ethos
Gestaltung: Sarah Kriesche

Moderation und Redaktion: Franz Zeller

EPA/JOCHENLUEBKE

Sicherheitsexperten haben oft etwas Paranoides an sich - sie wittern allerorts Überwachung. Und das häufig zu Recht: Webseiten versuchen mit Cookies unser Surf-Verhalten aufzuzeichnen, Fitnessgadgets speichern unseren Körperzustand - und melden ihn weiter.

Mit Themen wie diesen beschäftigte sich letzte Woche die Sicherheitskonferenz "Deepsec" in Wien. Der Nachwuchs in der IT-Sicherheitsszene konnte sich tags darauf bei den sogenannten B-Sides austoben. Sarah Kriesche hat dort einen "ethischen Hacker" zum Interview getroffen.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Dezember
Gestern
Morgen
Heute
Wissen Downloads

Social Media

http://ananalyticalapproach.blogspot.co.at/2014/11/thoughts-on-irisscon-and-deepsec.html

Thoughts on #IRISSCON and #DeepSec

Datum: 24.11.2014

Autor: Josh Goldfarb

Last week, I was fortunate to have the opportunity to speak at both #IRISSCON and #DeepSec in Dublin and Vienna respectively. Both conferences were extremely well run, with a great crowd and interesting dialogue to go along with them. My conversations and observations at the conferences indicate to me that the paradigm shift from a focus solely on prevention to a mix between prevention and detection/response is indeed well under-way. Each conference I speak at, I find more and more people who are interested in better understanding the subject of incident response.

This is a good thing in my opinion. It shows that we as an industry are trending in the correct direction. People ask me many questions, but one of the most common is: "Where can I go to get good educational materials on incident response?" This is a tough question to answer because, while there are many, many good materials on the subject, there are unfortunately, quite a few not so good materials out there. Generally, I recommend finding a few trusted sources (I would be flattered if you would consider this blog one of them) as a beginning point. As time allows, sources can be expanded, perhaps with the help of a seasoned incident response veteran.

Those of us who have experience in incident response should continue to share our knowledge with those that are new to the field. Together, we can help organizations improve the state of their security operations function and their overall security posture. I am glad that the community is becoming more interested in what has for a long time been a very niche field. Let's continue to keep the knowledge and exchange of ideas flowing, while hopefully minimizing the influence of #FUD and bad ideas.

An Analytical Approach

MONDAY, NOVEMBER 24, 2014

Thoughts on #IRISSCON and #DeepSec

Last week, I was fortunate to have the opportunity to speak at both #IRISSCON and #DeepSec in Dublin and Vienna respectively. Both conferences were extremely well run, with a great crowd and interesting dialogue to go along with them. My conversations and observations at the conferences indicate to me that the paradigm shift from a focus solely on prevention to a mix between prevention and detection/response is indeed well underway. Each conference I speak at, I find more and more people who are interested in better understanding the subject of incident response.

This is a good thing in my opinion. It shows that we as an industry are trending in the correct direction. People ask me many questions, but one of the most common is: "Where can I go to get good educational materials on incident response?" This is a tough question to answer because, while there are many, many good materials on the subject, there are unfortunately, quite a few not so good materials out there. Generally, I recommend finding a few trusted sources (I would be flattered if you would consider this blog one of them) as a beginning point. As time allows, sources can be expanded, perhaps with the help of a seasoned incident response veteran.

Those of us who have experience in incident response should continue to share our knowledge with those that are new to the field. Together, we can help organizations improve the state of their security operations function and their overall security posture. I am glad that the community is becoming more interested in what has for a long time been a very niche field. Let's continue to keep the knowledge and exchange of ideas flowing, while hopefully minimizing the influence of #FUD and bad ideas.

Posted by Josh Goldfarb at 3:51 AM

No comments:

Post a Comment

http://fm4.orf.at/stories/1749883/

Freie Programme gegen "Staatstrojaner"

Datum: 23. 11. 2014

Autor: Erich Möchel

Neben neuen Verschlüsselungsprogrammen sind auch ein Tool gegen Staatstrojaner und eine mächtige Netzwerksuite zur Abwehr von Angriffen nun frei verfügbar.

Die Ankündigung von WhatsApp, ihr populäres, aber bis dato kaum gesichertes Chatprogramm künftig zu verschlüsseln, markiert den ersten Höhepunkt eines Trends, der seit Monaten sichtbar ist. Sichere Protokolle und Methoden, die aus der Hackersphäre stammen und nur von einer Minderheit benutzt wurden, ziehen in weit verbreitete Anwendungen ein. Im Falle von WhatsApp wurde das Protokoll von TextSecure übernommen, das Chats so verschlüsselt, dass auch der Betreiber selbst nicht mitlesen kann.

Zu einer großen Anzahl neuer, einfach zu bedienender Chat-Verschlüsselungsprogramme wie TextSecure oder Cryptocat kommen nun auch spezialisierte und komplexere Anwendungen. Am Donnerstag wurde mit "Detekt" der erste, auf sogenannte "Staatstrojaner" spezialisierte Virenscanner veröffentlicht. Derartige Schadsoftware wird von Firmen vor allem aus der EU den USA für Geheimdienste und Polizeibehörden produziert und auch an Diktaturen geliefert, die damit Oppositionelle ausspionieren. Zur Früherkennung von Angriffen auf Netzwerke generell wird mit der freien "Suricata"-Suite auch ein mächtiges Abwehrinstrument für fortgeschrittene Anwender benutzbar, das sich mit teuren kommerziellen Produkten für Unternehmensnetze messen kann.

Immer mehr einfach zu bedienende, neue und freie Kryptoprogramme kommen als bloße Plug-ins für gängige Webbrowser daher. Prototypisch für diese Entwicklung steht Cryptocat, das auch als iPhone-App und bald auch für Android erhältlich ist.

Die Gemeinsamkeiten

Diese drei, von ihren Funktionen völlig unterschiedlichen Tools weisen jedoch eine ganze Reihe von Gemeinsamkeiten auf. Zum einen liegt bei allen der Quellcode offen, denn nur dann lässt sich von unabhängiger Seite überprüfen, ob der Code auch wirklich keine Hintertüren enthält. Zweitens stammen all diese Programme von Entwicklergemeinschaften, die ihre Arbeit über Stiftungen und Spenden finanzieren.

TextSecure wurde von einer Gruppe von Open-Source-Programmierern rund um den bekannten Hacker Moxie

Marlinspike entwickelt. TextSecure bietet sicher verschlüsselten Chat sowohl für Androids und iPhones und ist aber mit mehreren, anderen Chatprogrammen - etwa Pidgin (Windows, Linux) oder Adium (Mac) - kompatibel, die ebenfalls das "Off the Record"-Protokoll beherrschen. Daneben haben Marlinspike und Co auch die Redphone-App für verschlüsselte Telefonate entwickelt. RedPhone nützt das von Kryptopionier Phil Zimmermann entwickelte ZRTP-Protokoll zur Sprachverschlüsselung. Wie TextSecure hat auch Redphone in allen Sicherheitstests bis dato hervorragend abgeschnitten.

Scorecard sicherer ChatEFF

Die Tabelle der Electronic Frontier Foundation zeigt noch den derzeitigen Unterschied an Sicherheit zwischen Text-Secure und WhatsApp

Macht durch Offenheit

Die neuen Services, für die auch die Anbieter keine Nachschlüssel haben, veranlasste die Behörden bereits zur Beschwörung "dunkler, dunkler Zeiten". Anlass für diese Unkenrufe war, dass die neuen iPhones mit Passwortschutz ausgeliefert werden

Die eigentliche Macht dieser Programme liegt in der Offenheit ihres Quellcodes begründet. Da die berühmte "Kette der Sicherheit" insgesamt nur so stark ist, wie ihr schwächstes Glied, lässt sie sich nur dann auch lückenlos überprüfen. Am sichersten ist sie natürlich, wenn darunter ein Betriebssystem werkt, dessen Quellcode ebenfalls offenliegt, doch auch unter Windows oder Mac ist der Sicherheitsgewinn für die Benutzer beträchtlich.

Wer diese TextSecure-Server auch betreibt, hat weder eine Möglichkeit, die Konversationen mitzuschneiden, noch kann er Schlüssel an Behörden herausgeben, weil die Schlüssel nicht auf dem Server, sondern auf den Clients der Benutzer gespeichert sind. Dasselbe gilt bald auch für die weltweit auf 600 Millionen geschätzten Nutzer von WhatsApp.

Wachsame Erdmännchen

Während TextSecure gerade in kommerzielle Anwendungen für Endbenutzer wie WhatsApp integriert werden, wird die quelloffene "Suricata"-Suite schon seit geraumer Zeit in Firmen eingesetzt. Anders als TextSecure ist Suricata kein Tool für Endanwender, vielmehr wurde es für Administratoren entwickelt, die damit Angriffe auf ihr Netz frühzeitig erkennen können. Die Entwicklung von Suricata wurde bereits vor sieben Jahren begonnen, ein eigenes graphisches Benutzerinterface hatte dabei keine besondere Priorität. Offenbar war das Projekt von den Sponsoren (siehe unten) zur Integration in eigene Benutzeroberflächen vorgesehen.

"Natürlich gibt es da einiges zu konfigurieren, so müssen etwa die Parameter des jeweiligen Netzes - Gateways, Routeradressen usw. - eingegeben werden, damit sich Suricata orientieren kann", sagte Victor Julien, der Entwicklungschef von Suricata zu ORF.at. "Wir arbeiten im Moment vor allem daran, die Konfigurierbarkeit zu vereinfachen und Prozesse, bei denen dies auch möglich ist, zu automatisieren." Ziel sei es dabei, sagte Julien, dass Suricata auch von weniger geübten Administratoren oder auch fortgeschrittenen Usern eingesetzt werden könne. Die Software läuft auf allen drei großen Betriebssystemen, für den Betrieb genügt ein einfacher PC.

Die Entwickler von Suricata hielten auf der DeepSec Konferenz, die am Freitag in Wien zu Ende ging, Suricata-Workshops für Nutzer aus Industrie und Behörden ab. Dieselbe Suricata-Suite ist allerdings als Tool für die Kommandozeile in allen Linuxdistributionen schon enthalten.

Mächtiges Verteidigungsinstrument

Damit steht auch kleineren Firmen wie finanzschwachen Organisationen ein mächtiges Instrument zu Überwachung ihrer eigenen Netze auf Angriffe von außen zur Verfügung. Anders als bei Virenscannern werden hier nicht bloß Dateien auf die jeweils charakteristischen Zeichenfolgen bekannter Schadsoftware durchsucht. Vielmehr werden die Vorgänge im gesamten Datenverkehr beobachtet und nach Mustern gesucht, die auf einen Angriff von außen hinweisen.

Screenshot von SuricataCC Suricata

Im Grunde macht Suricata ganz genau dasselbe, wie alle kommerziellen - und entsprechend teuren - "Intrusion Detection Suites" für Netzwerke von Großkonzernen. In den Netzen von Geheimdiensten und Militärs gehören solche Softwaretools seit jeher zum Sicherheitsstandard und genau von dort kommt Suricata eigentlich her, von der "dunklen Seite der Macht".

Heimatschutz und Sternenkrieger

Die Stiftung, die diese Suite zur Identifikation und Abwehr von Angriffen finanziert, gehört zum "Homeland Open Security Program" des US-Ministeriums für Heimatschutz und dem "Space and Naval Warfare Systems Command" (SPAWAR) der US Navy. Das erscheint paradox, hat aber dennoch einen völlig rationalen Hintergrund.

Dass nur quelloffene Sicherheitssysteme vertrauenswürdig, weil auch überprüfbar sind, gilt im Militärbereich schon weitaus länger als in der Sphäre ziviler Kommunikation. Zudem sind Open-Source-Systeme viel schneller zu entwickeln, wenn nämlich andere Interessenten für dieselbe Art von Software dazustoßen. Obendrein hängt der Sicherheitsgrad noch völlig davon ab, wieviele Coder mit entsprechender Erfahrung den Quellcode laufend

überprüfen. Gerade im Sicherheitsbereich geht der Trend fast unaufhaltsam in Richtung Open Source, der NSA-Spionageskandal hat hier natürlich einen entscheidenden Schub geliefert.

Detekt AlarmmeldungCC

Staatstrojaner und ihre Lieferanten

Die Veröffentlichung von "Detekt" ist natürlich auch als politischer Akt zu sehen. Das Programm ist dazu angetan, die Kosten für die Entwicklung bestimmter Spionage-Suites in die Höhe zu treiben

Mit Amnesty International, Privacy International, der Digitalen Gesellschaft und der Electronic Frontier Foundation stehen hinter dem Staatstrojaner-Scanner "Detekt" ebenfalls gemeinnützige Organisationen. Die erste Version von "Detekt" ist ein vergleichsweise einfaches, aber hochspezialisiertes Tool, das eine selektive Zielgruppe bedient. Es richtet sich an Menschen, die wichtige Gründe haben, derartige staatliche Angriffe auf ihre Kommunikation zu befürchten.

Detekt soll in erster Linie Dissidenten und Journalisten schützen, die von Geheimdiensten und politischer Polizei in nichtdemokratischen Staaten angegriffen werden. Die bekanntesten dieser Spionagesuites sind die Produkte der deutsch-britischen Gamma International namens "FinFisher", sowie jene der italienischen Hacking Team RCS, die ebenfalls Behörden rund um die Welt mit Schadsoftware beliefert.

Aktivisten, Journalisten

Seit März läuft in Großbritannien ein von Privacy International und anderen unterstützter Prozess gegen Gamma International und Hacking Team RSC. Die Anzeige selbst stammt von einem britischen Staatsbürger, der aus Bahrain stammt.

Die Spionagesuites dieser beiden Firmen waren während des Arabischen Frühlings wiederholt aufgefallen, weil sie von den regierenden Diktatoren gegen Oppositionelle eingesetzt wurden. Der Zeitpunkt der Veröffentlichung von "Detekt" direkt vor den ersten Wahlen in Bahrain nach dem Volksaufstand von 2011 am Samstag war nicht zufällig. Eines der ersten nachgewiesenen Opfer von FinFisher war eine Aktivistin aus der Demokratiebewegung in Bahrain, auf deren Rechner Spuren der deutsch-britischen Spionagesoftware FinFisher gefunden wurden.

Die Zielgruppe von Detekt ist allerdings nicht auf autoritär regierte Staaten wie Bahrain beschränkt. Am Freitag hatte AP gemeldet, die britische Journalistengewerkschaft habe Klage gegen die Londoner Metropolitan Police und das britische Innenministerium eingereicht. Anfragen von Journalisten nach dem Gesetz zur Informationsfrei-

heit hatten ergeben, dass eine ganze Reihe britischer Journalisten systematisch und jahrelang in ihrem persönlichen Umfeld bespitzelt wurde.

SPAWAR, TOR

Warum fördern das Außenministerium der USA, die See- und Sternenkrieger der US Navy, zu der auch die NSA gehört und weniger auffällige Stiftungen aus den USA Projekte wie etwa TOR? Zum einen, weil Bürger und Armeen der Weltmacht USA auch rund um die Welt sichere Kommunikation benötigen. Zum anderen muss man als Supermacht führend dabei sein, weil sich dieser ebenso globale wie mächtige Trend zur quelloffenen sicheren Verschlüsselung ohnehin nicht stoppen lässt.

Erstellt am: 23. 11. 2014 - 19:22 Uhr

Freie Programme gegen "Staatstrojaner"

Neben neuen Verschlüsselungsprogrammen sind auch ein Tool gegen Staatstrojaner und eine mächtige Netzwerksuite zur Abwehr von Angriffen nun frei verfügbar.

Die Ankündigung von WhatsApp, ihr populäres, aber bis dato kaum gesichertes Chatprogramm künftig zu verschlüsseln, markiert den ersten Höhepunkt eines Trends, der seit Monaten sichtbar ist. Sichere Protokolle und Methoden, die aus der Hackersphäre stammen und nur von einer Minderheit benutzt wurden, ziehen in weit verbreitete Anwendungen ein. Im Falle von WhatsApp wurde das Protokoll von TextSecure übernommen, das Chats so verschlüsselt, dass auch der Betreiber selbst nicht mitlesen kann.

Zu einer großen Anzahl neuer, einfach zu bedienender Chat-Verschlüsselungsprogramme wie TextSecure oder Cryptocat kommen nun auch spezialisierte und komplexere Anwendungen. Am Donnerstag wurde mit "Detekt" der erste, auf sogenannte "Staatstrojaner" spezialisierte Virenscanner veröffentlicht. Derartige Schadsoftware wird von Firmen vor allem aus der EU den USA für Geheimdienste und Polizeibehörden produziert und auch an Diktaturen geliefert, die damit Oppositionelle ausspionieren. Zur Früherkennung von Angriffen auf Netzwerke generell wird mit der freien "Suricata"-Suite auch ein mächtiges Abwehrinstrument für fortgeschrittene Anwender benutzbar, das sich mit teuren kommerziellen Produkten für Unternehmensnetze messen kann.

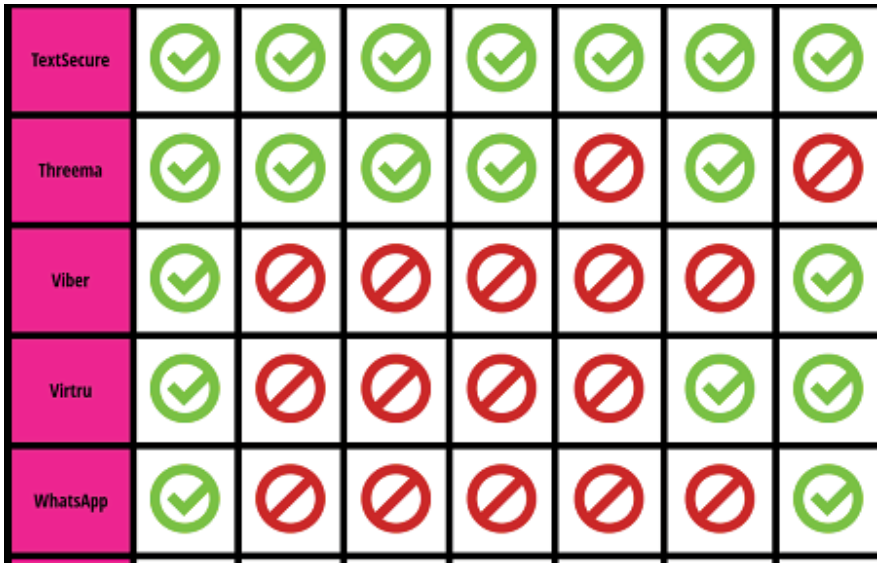
Immer mehr einfach zu bedienende, neue und freie Kryptoprogramme kommen als bloße Plug-ins für gängige Webbrowser daher. Prototypisch für diese Entwicklung steht Cryptocat, das auch als iPhone-App und bald auch für Android erhältlich ist.

Die Gemeinsamkeiten

Diese drei, von ihren Funktionen völlig unterschiedlichen Tools weisen jedoch eine ganze Reihe von Gemeinsamkeiten auf. Zum einen liegt bei allen der Quellcode offen, denn nur dann lässt sich von unabhängiger Seite überprüfen, ob der Code auch wirklich keine Hintertüren enthält. Zweitens stammen all diese Programme von Entwicklergemeinschaften, die ihre Arbeit über Stiftungen und Spenden finanzieren.

TextSecure wurde von einer Gruppe von Open-Source-Programmierern rund um den bekannten Hacker Moxie Marlinspike entwickelt. TextSecure bietet sicher verschlüsselten Chat sowohl für Androids und iPhones und ist aber mit mehreren, anderen Chatprogrammen - etwa Pidgin (Windows, Linux) oder Adium (Mac) - kompatibel, die ebenfalls das "Off the Record"-Protokoll beherrschen. Daneben haben Marlinspike und Co auch die Redphone-App für verschlüsselte Telefonate entwickelt. RedPhone nützt das von Kryptopionier Phil Zimmermann entwickelte ZRTP-Protokoll zur Sprachverschlüsselung. Wie TextSecure hat auch Redphone in allen Sicherheitstests bis dato hervorragend abgeschnitten.

Die Scorecard der EFF für sichere Chats (https://www.eff.org/de/secure-messaging-scorecard)



EFF

Die Tabelle der Electronic Frontier Foundation zeigt noch den derzeitigen Unterschied an Sicherheit zwischen TextSecure und WhatsApp

Macht durch Offenheit

Die neuen Services, für die auch die Anbieter keine Nachschlüssel haben, veranlasste die Behörden bereits zur Beschwörung "dunkler, dunkler Zeiten". Anlass für diese Unkenrufe war, dass die neuen iPhones mit Passwortschutz ausgeliefert werden

Die eigentliche Macht dieser Programme liegt in der Offenheit ihres Quellcodes begründet. Da die berühmte "Kette der Sicherheit" insgesamt nur so stark ist, wie ihr schwächstes Glied, lässt sie sich nur dann auch lückenlos überprüfen. Am sichersten ist sie natürlich, wenn darunter ein Betriebssystem werkt, dessen Quellcode ebenfalls offenliegt, doch auch unter Windows oder Mac ist der Sicherheitsgewinn für die Benutzer beträchtlich.

Wer diese TextSecure-Server auch betreibt, hat weder eine Möglichkeit, die Konversationen mitzuschneiden, noch kann er Schlüssel an Behörden herausgeben, weil die Schlüssel nicht auf dem Server, sondern auf den Clients der Benutzer gespeichert sind. Dasselbe gilt bald auch für die weltweit auf 600 Millionen geschätzten Nutzer von WhatsApp.

Wachsame Erdmännchen

Während TextSecure gerade in kommerzielle Anwendungen für Endbenutzer wie WhatsApp

integriert werden, wird die quelloffene "Suricata"-Suite schon seit geraumer Zeit in Firmen eingesetzt. Anders als TextSecure ist Suricata kein Tool für Endanwender, vielmehr wurde es für Administratoren entwickelt, die damit Angriffe auf ihr Netz frühzeitig erkennen können. Die Entwicklung von Suricata wurde bereits vor sieben Jahren begonnen, ein eigenes graphisches Benutzerinterface hatte dabei keine besondere Priorität. Offenbar war das Projekt von den Sponsoren (siehe unten) zur Integration in eigene Benutzeroberflächen vorgesehen.

Sara&Joachim&Mebe / CC BY-SA 2.0

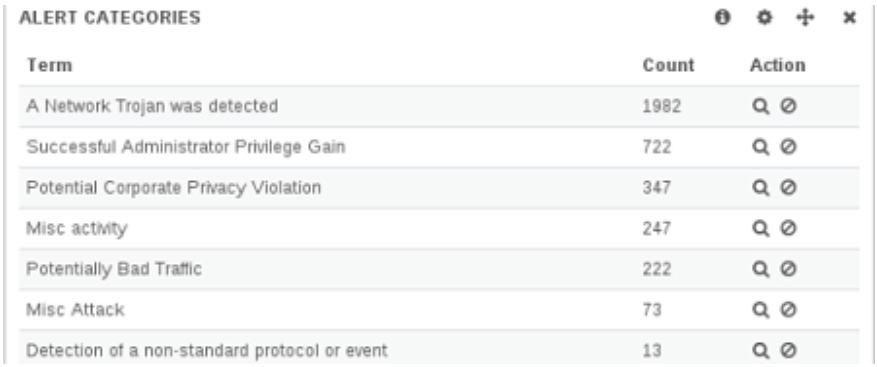
Die Wachsamkeit der Erdmännchen (lat. Suricata suricata) hat die Namensgebung von Suricata inspriert (CC BY-SA 2.0 (https://creativecommons.org/licenses/by-sa/2.0/))

"Natürlich gibt es da einiges zu konfigurieren, so müssen etwa die Parameter des jeweiligen Netzes - Gateways, Routeradressen usw. - eingegeben werden, damit sich Suricata orientieren kann", sagte Victor Julien, der Entwicklungschef von Suricata zu ORF.at. "Wir arbeiten im Moment vor allem daran, die Konfigurierbarkeit zu vereinfachen und Prozesse, bei denen dies auch möglich ist, zu automatisieren." Ziel sei es dabei, sagte Julien, dass Suricata auch von weniger geübten Administratoren oder auch fortgeschrittenen Usern eingesetzt werden könne. Die Software läuft auf allen drei großen Betriebssystemen, für den Betrieb genügt ein einfacher PC.

Die Entwickler von Suricata hielten auf der DeepSec Konferenz, die am Freitag in Wien (https://deepsec.net) zu Ende ging, Suricata-Workshops für Nutzer aus Industrie und Behörden ab. Dieselbe Suricata-Suite (https://redmine.openinfosecfoundation.org/projects/suricata/wiki) ist allerdings als Tool für die Kommandozeile in allen Linuxdistributionen schon enthalten.

Mächtiges Verteidigungsinstrument

Damit steht auch kleineren Firmen wie finanzschwachen Organisationen ein mächtiges Instrument zu Überwachung ihrer eigenen Netze auf Angriffe von außen zur Verfügung. Anders als bei Virenscannern werden hier nicht bloß Dateien auf die jeweils charakteristischen Zeichenfolgen bekannter Schadsoftware durchsucht. Vielmehr werden die Vorgänge im gesamten Datenverkehr beobachtet und nach Mustern gesucht, die auf einen Angriff von außen hinweisen.



ALERT CATEGORIES

Term	Count	Action
A Network Trojan was detected	1982	
Successful Administrator Privilege Gain	722	
Potential Corporate Privacy Violation	347	
Misc activity	247	
Potentially Bad Traffic	222	
Misc Attack	73	
Detection of a non-standard protocol or event	13	

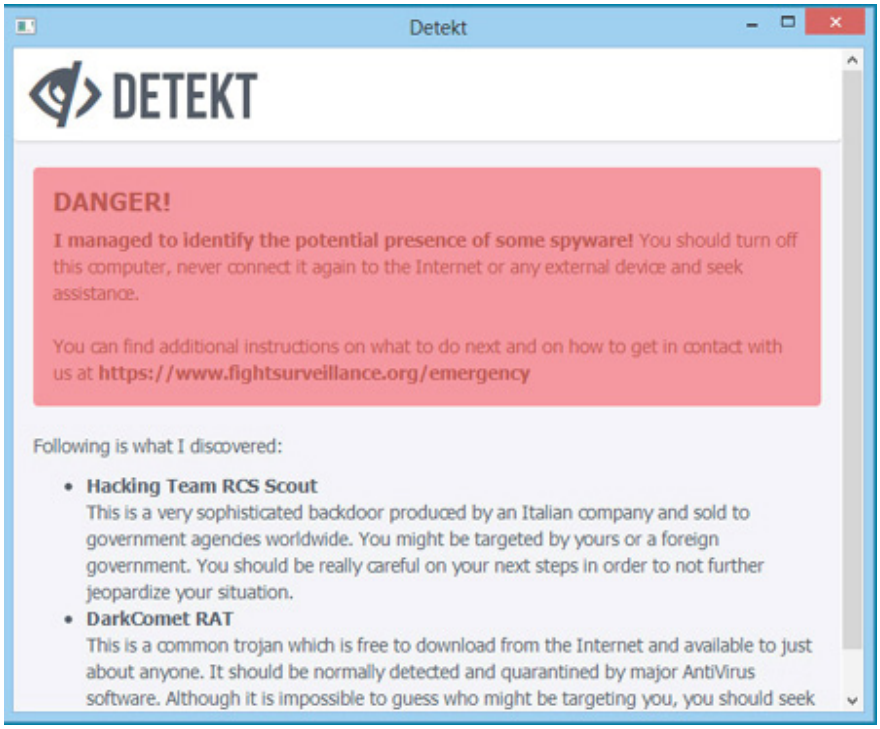
CC Suricata

Im Grunde macht Suricata ganz genau dasselbe, wie alle kommerziellen - und entsprechend teuren - "Intrusion Detection Suites" für Netzwerke von Großkonzernen. In den Netzen von Geheimdiensten und Militärs gehören solche Softwaretools seit jeher zum Sicherheitsstandard und genau von dort kommt Suricata eigentlich her, von der "dunklen Seite der Macht".

Heimatschutz und Sternenkrieger

Die Stiftung, die diese Suite zur Identifikation und Abwehr von Angriffen finanziert, gehört zum "Homeland Open Security Program" des US-Ministeriums für Heimatschutz und dem "Space and Naval Warfare Systems Command" (SPAWAR) der US Navy. Das erscheint paradox, hat aber dennoch einen völlig rationalen Hintergrund.

Dass nur quelloffene Sicherheitssysteme vertrauenswürdig, weil auch überprüfbar sind, gilt im Militärbereich schon weitaus länger als in der Sphäre ziviler Kommunikation. Zudem sind Open-Source-Systeme viel schneller zu entwickeln, wenn nämlich andere Interessenten für dieselbe Art von Software dazustoßen. Obendrein hängt der Sicherheitsgrad noch völlig davon ab, wieviele Coder mit entsprechender Erfahrung den Quellcode laufend überprüfen. Gerade im Sicherheitsbereich geht der Trend fast unaufhaltsam in Richtung Open Source, der NSA-Spionageskandal hat hier natürlich einen entscheidenden Schub geliefert.



CC

Staatstrojaner und ihre Lieferanten

Die Veröffentlichung von "Detekt" ist natürlich auch als politischer Akt zu sehen. Das Programm ist dazu angetan, die Kosten für die Entwicklung bestimmter Spionage-Suites in die Höhe zu treiben (`https://resistsurveillance.org/`)

Mit Amnesty International, Privacy International, der Digitalen Gesellschaft und der Electronic Frontier Foundation stehen hinter dem Staatstrojaner-Scanner "Detekt" ebenfalls gemeinnützige Organisationen. Die erste Version von "Detekt" ist ein vergleichsweise einfaches, aber hochspezialisiertes Tool, das eine selektive Zielgruppe bedient. Es richtet sich an Menschen, die wichtige Gründe haben, derartige staatliche Angriffe auf ihre Kommunikation zu befürchten.

Detekt soll in erster Linie Dissidenten und Journalisten schützen, die von Geheimdiensten und politischer Polizei in nichtdemokratischen Staaten angegriffen werden. Die bekanntesten dieser Spionagesuites sind die Produkte der deutsch-britischen Gamma International namens "FinFisher", sowie jene der italienischen Hacking Team RCS, die ebenfalls Behörden rund um die Welt mit Schadsoftware beliefert.

Aktivisten, Journalisten

Seit März läuft in Großbritannien ein von Privacy International und anderen unterstützter Prozess gegen Gamma International und Hacking Team RSC. Die Anzeige selbst stammt von einem britischen Staatsbürger, der aus Bahrain stammt.

Die Spionagesuites dieser beiden Firmen waren während des Arabischen Frühlings wiederholt aufgefallen, weil sie von den regierenden Diktatoren gegen Oppositionelle eingesetzt wurden. Der Zeitpunkt der Veröffentlichung von "Detekt" direkt vor den ersten Wahlen in Bahrain nach dem Volksaufstand von 2011 am Samstag war nicht zufällig. Eines der ersten nachgewiesenen Opfer von FinFisher war eine Aktivistin aus der Demokratiebewegung in Bahrain, auf deren Rechner Spuren der

deutsch-britischen Spionagesoftware FinFisher gefunden wurden.

Die Zielgruppe von Detekt ist allerdings nicht auf autoritär regierte Staaten wie Bahrain beschränkt. Am Freitag hatte AP gemeldet, die britische Journalistengewerkschaft habe Klage gegen die Londoner Metropolitan Police und das britische Innenministerium eingereicht. Anfragen von Journalisten nach dem Gesetz zur Informationsfreiheit hatten ergeben, dass eine ganze Reihe britischer Journalisten systematisch und jahrelang in ihrem persönlichen Umfeld bespitzelt wurde.

SPAWAR, TOR

Warum fördern das Außenministerium der USA, die See- und Sternenkrieger der US Navy, zu der auch die NSA gehört und weniger auffällige Stiftungen aus den USA Projekte wie etwa TOR? Zum einen, weil Bürger und Armeen der Weltmacht USA auch rund um die Welt sichere Kommunikation benötigen. Zum anderen muss man als Supermacht führend dabei sein, weil sich dieser ebenso globale wie mächtige Trend zur quelloffenen sicheren Verschlüsselung ohnehin nicht stoppen lässt.

http://futurezone.at/netzpolitik/white-hat-hacking-ist-nicht-lukrativ-genug/98.211.388

DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

Datum: 21.11.14

Autor: Florian Christof

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

Die OpenSSL-Lücke Heartbleed bestand zwei Jahre, bis sie von der Öffentlichkeit entdeckt wurde. Der Shellshock-Bug, der Apple-, Linux- und Unix-Nutzer gefährdete, blieb überhaupt mehr als 20 Jahre unentdeckt. Dies sind nur zwei Beispiele, die Linus Neumann, ein Sprecher des Chaos Computer Clubs, bei der Pressekonferenz der Sicherheitskonferenz DeepSec in Wien für den katastrophalen Zustand der IT-Security anführte.
Problemfelder dabei sieht Neumann gleich an mehreren Orten und über verschiedene Ebenen verteilt. Ein wesentlicher Punkt ist, dass es für White Hat Hacker einfach nicht lukrativ genug sei, gefundene Sicherheitslücken offen zu legen.

Anreize für White Hats schaffen

"Bei den Bug-Bounties werden meist nur ein paar tausend Euro ausgeschrieben. Wer eine Schwachstelle entdeckt, kann sie allerdings am Schwarzmarkt um ein Vielfaches verkaufen", bemängelt Neumann. "Um Anreize zu schaffen, müssten die Prämien für das Aufspüren von Sicherheitslücken massiv erhöht werden, ganz besonders bei Open-Source-Software." Dabei sieht Neumann auch die Politik sowie branchen- und unternehmensübergreifende Initiativen gefordert.
Einen unüberbrückbaren Interessenskonflikt sieht Neumann in der Tatsache, dass IT-Sicherheitsthemen allesamt im Innenministerium angesiedelt sind. "Einerseits sind die Behörden mit Bewusstseinsarbeit, Aufklärung und Verbrechensaufdeckung beschäftigt und andererseits kauft dasselbe Ressort Zero Day Exploits um Schwachstellen, etwa für Spionage oder Überwachungstätigkeiten ausnutzen zu können", kritisiert Neumann. "Mit einer solchen Vorgehensweise kann man nicht für nachhaltige IT-Sicherheit sorgen."

BND will Zero Day Exploits kaufen

Für diesen Kauf von Zero Day Exploits hat der deutsche Bundesnachrichtendienst nach Informationen des Spiegel für die kommenden fünf Jahre 4,5 Millionen Euro budgetiert. Bis 2014 hatte die deutsche Bundesregierung einen

Vertrag mit dem französischen Sicherheitsunternehmen Vupen, das auf den Handel mit Zero-Day-Schwachstellen spezialisiert ist.

Neumann kritisiert, dass Vupen-Mitarbeiter etwa bei Bug-Bounty-Events auftreten, Sicherheitslücken zeigen, aber die Schwachstellen weder dokumentieren noch erklären. "Nachdem sie ihren Hack gezeigt haben, packen sie zusammen und gehen, ohne sich ein Preisgeld abzuholen", sagt Neumann. Ein solches Verhalten signalisiere, dass woanders weit mehr Geld mit dem Aufdecken von Sicherheitslücken zu machen ist, wodurch auch der Handel mit Sicherheitslücken extrem angeheizt wird.

Daher forderte der CCC auch Anfang November, dass der Kauf von Zero Day Exploits durch deutsche Behörden verboten wird: "Sicherheitslücken gehören nach der Entdeckung geschlossen und nicht verkauft und geheim gehalten, solange es irgendwie geht."

Die Frage nach der Haftung

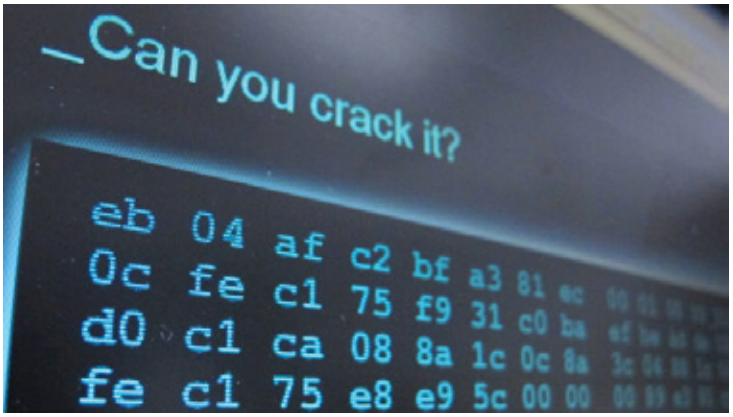
Abschließend stellte Neumann eine Frage in den Raum, die allerdings noch durchdiskutiert gehöre: "Warum haften Softwarehersteller eigentlich nicht für die Sicherheit ihres Produkts?" In keiner anderen Branche sei es möglich, ein Produkt zu verkaufen und dafür keine Haftung zu übernehmen. Wenn bei Fahrzeugen etwa Probleme mit den Bremsen auftreten, kann es sein, dass die komplette Serie zurückgerufen wird. Bei Software gebe es so etwas nicht. "Sollte nicht ein kommerzieller Anbieter für Sicherheitslücken haften", mutmaßt Neumann.(FUTUREZONE)

ERSTELLT AM 21.11.2014, 11:24

DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

von Florian Christof 21.11.14, 11:24 FlorianChristof Mail an Autor



Für White Hat Hacking sollten die Anreize massiv erhöht werden - Foto: AP/Cassandra Vinograd

DEEPSEC
"White Hat Hacking ist nicht lukrativ genug"
KOMMENTARE (2)
MEHR ZUM THEMA

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

SICHERHEITSLÜCKE, HACKER, CCC, IT-SECURITY, DEEPSEC, IT-SICHERHEIT

Die OpenSSL-Lücke Heartbleed bestand zwei Jahre, bis sie von der Öffentlichkeit entdeckt wurde. Der Shellshock-Bug, der Apple-, Linux- und Unix-Nutzer gefährdete, blieb überhaupt mehr als 20 Jahre unentdeckt. Dies sind nur zwei Beispiele, die Linus Neumann, ein Sprecher des Chaos Computer Clubs, bei der Pressekonferenz der Sicherheitskonferenz DeepSec in Wien für den katastrophalen Zustand der IT-Security anführte.

Problemfelder dabei sieht Neumann gleich an mehreren Orten und über verschiedene Ebenen verteilt. Ein wesentlicher Punkt ist, dass es für White Hat Hacker einfach nicht lukrativ genug sei, gefundene Sicherheitslücken offen zu legen.

Anreize für White Hats schaffen

"Bei den Bug-Bounties werden meist nur ein paar tausend Euro ausgeschrieben. Wer eine Schwachstelle entdeckt, kann sie allerdings am Schwarzmarkt um ein Vielfaches verkaufen", bemängelt Neumann. "Um Anreize zu schaffen, müssten die Prämien für das Aufspüren von Sicherheitslücken massiv erhöht werden, ganz besonders bei Open-Source-Software." Dabei sieht Neumann auch die Politik sowie branchen- und unternehmensübergreifende Initiativen gefordert.

Einen unüberbrückbaren Interessenskonflikt sieht Neumann in der Tatsache, dass IT-Sicherheitsthemen allesamt im Innenministerium angesiedelt sind. "Einerseits sind die Behörden mit Bewusstseinsarbeit, Aufklärung und Verbrechensaufdeckung beschäftigt und andererseits kauft dasselbe Ressort Zero Day Exploits um Schwachstellen, etwa für Spionage oder Überwachungstätigkeiten ausnutzen zu können", kritisiert Neumann. "Mit einer solchen Vorgehensweise kann man nicht für nachhaltige IT-Sicherheit sorgen."

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

BND will Zero Day Exploits kaufen

Für diesen Kauf von Zero Day Exploits hat der deutsche Bundesnachrichtendienst nach Informationen des Spiegel für die kommenden fünf Jahre 4,5 Millionen Euro budgetiert. Bis 2014 hatte die deutsche Bundesregierung einen Vertrag mit dem französischen Sicherheitsunternehmen Vupen, das auf den Handel mit Zero-Day-Schwachstellen spezialisiert ist.

Neumann kritisiert, dass Vupen-Mitarbeiter etwa bei Bug-Bounty-Events auftreten, Sicherheitslücken zeigen, aber die Schwachstellen weder dokumentieren noch erklären. "Nachdem sie ihren Hack gezeigt haben, packen sie zusammen und gehen, ohne sich ein Preisgeld abzuholen", sagt Neumann. Ein solches Verhalten signalisiere, dass woanders weit mehr Geld mit dem Aufdecken von Sicherheitslücken zu machen ist, wodurch auch der Handel mit Sicherheitslücken extrem angeheizt wird.

Daher forderte der CCC auch Anfang November, dass der Kauf von Zero Day Exploits durch deutsche Behörden verboten wird: "Sicherheitslücken gehören nach der Entdeckung geschlossen und nicht verkauft und geheim gehalten, solange es irgendwie geht."

Die Frage nach der Haftung

Abschließend stellte Neumann eine Frage in den Raum, die allerdings noch durchdiskutiert gehöre: "Warum haften Softwarehersteller eigentlich nicht für die Sicherheit ihres Produkts?" In keiner anderen Branche sei es möglich, ein Produkt zu verkaufen und dafür keine Haftung zu übernehmen. Wenn bei Fahrzeugen etwa Probleme mit den Bremsen auftreten, kann es sein, dass die komplette Serie zurückgerufen wird. Bei Software gebe es so etwas nicht. "Sollte nicht ein kommerzieller Anbieter für Sicherheitslücken haften", mutmaßt Neumann.

(FUTUREZONE) ERSTELLT AM 21.11.2014, 11:24

SICHERHEITSLÜCKE, HACKER, CCC, IT-SECURITY, DEEPSEC, IT-SICHERHEIT

Kommentare (2)

Ihr Kommentar
Bitte loggen Sie sich ein

Einloggen / Registrieren

ABSENDEN

a190 vor 7 monaten permalink | melden 0 0

Ich denke nicht, dass es notwendig ist, überhaupt "Prämien" für White Hacking zu zahlen.

Im Gegenteil: Wer eine Sicherheitslücke findet und diese verkauft, ist natürlich strafrechtlich voll in der Scheiße, wenn damit ein Schaden verursacht wird, und - zumindest teilweise - für den Schaden auch haftbar. Existenz, baba! Wer's nicht glaubt, versuche mal, die Information über eine versehentlich offene Tür an eine Einbrecherbande zu verkaufen.

Und Haftung für Software gibt's generell nicht. Dazu ist Software zu komplex, und auch zu abhängig von anderen Softwarekomponenten, Hardwaresystemen und zu vernetzt. Wo ist nun wirklich die Ursache für einen Schaden, und zu welchem Prozentsatz ist die Softwarelücke schuld? Diese Frage kann im Normalfall kein Gericht zweifelsfrei beantworten.

Haftung für Software wäre so: Ein Auto fährt durch ein Schlagloch; der Reifen platzt. Nun wäre der Autohersteller haftbar, weil er kein Schlaglochwarnsystem eingebaut hat, nicht etwa der Straßenerhalter oder der Lenker, der zu unaufmerksam war.

antworten

rhsraphael vor 7 monaten permalink | melden 0 0

Für Software wird viel zu wenig bezahlt, als dass man dann noch dafür haften könne...

antworten

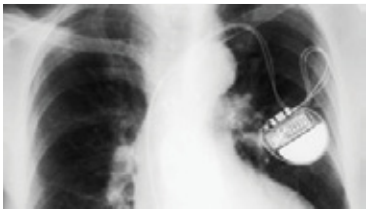
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

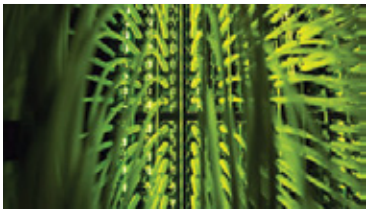
von Barbara Wimmer



SICHERHEITSKONFERENZ

DeepSec: Vom Herzschrittmacher-Hack bis zum Profiling

Zur Sicherheitskonferenz DeepSec, die von 19. bis 22. November in Wien stattfindet, kommt unter anderem der IT-Sicherheitspionier Marcus J. Ranum.



KRITIK

CCC: Sicherheitslücken-Kauf durch Behörden verbieten

Der Chaos Computer Club kritisiert das Vorgehen der deutschen Bundesregierung scharf. Der Zukauf von "Zero Day Exploits" durch den Bund heize den Markt unnötig an.

Netzpolitik

15.07.2015 13:31 Uhr

JAHRESBERICHT 1

Europarat beklagt Zunahme von Hassreden im Internet

Laut Europarat gab es im Vorjahr eine "beunruhigenden Tendenz zu Hassreden und Ausländerfeindlichkeit im Internet", auch dank der Wahlerfolge populistischer Parteien.

SCHIKANE 1

Snowden-Dokumentarfilmerin Poitras verklagt US-Behörden

Die Filmschaffende verlangt von den US-Behörden Auskunft darüber, warum sie so häufig bei der Einreise in die USA zur Überprüfung festgehalten worden ist.

SICHERHEIT 8

US-Senator fordert Haftung für Verschlüsselung

Der demokratische Senator Sheldon Whitehouse fordert, dass Opfer eines Verbrechens Unternehmen verklagen können, sollte deren Verschlüsselung jemandem Schaden.

POLITIK 2

Hashtag #ThisIsACoup: Heftige Kritik an Griechenland-Deal

Die Forderungen der Gläubiger haben Kritik im Internet ausgelöst. Unter dem Hashtag #ThisIsACoup wurde vor allem über die Rolle Deutschlands in harschen Worten diskutiert.

EU 2

"Die Netzneutralität wird de facto abgeschafft"

Die geplanten EU-Regeln zur Gleichbehandlung aller Daten und Dienste im Internet stoßen auf harsche Kritik.

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

Die Hier-Box, ein kleines Gerät zum Nachrüsten, kann bei einem Autounfall selbstständig einen Notruf absetzen. Die Reaktionszeit der Rettung soll so stark verkürzt werden.

von David Kotrba

REPORTAGE

http://www.golem.de/news/messenger-keine-kommunikation-zwischen-whatsapp-und-textsecure-1411-110718.html

Messenger

Keine Kommunikation zwischen Whatsapp und Textsecure

Datum: 21.11.2014

Autor: Jörg Thoma

Textsecure-Nutzer werden auch künftig nicht mit Whatsapp-Anwendern kommunizieren können. Textsecure soll als eigenständiges Produkt bestehen bleiben. Eine weitere Zusammenarbeit soll es dennoch geben.

Textsecure-Benutzer sollen auch künftig nicht direkt mit Whatsapp-Nutzern verschlüsselt kommunizieren können. Es gebe keine Pläne, das von Open Whispers Systems entwickelte und in Whatsapp integrierte Axolotl-Protokoll gemeinsam zu nutzen. Das sagte Christine Corbett von Open Whisper Systems zu Golem.de am Rande der IT-Sicherheitskonferenz Deepsec 2014 in Wien.

Technisch sei es zwar durchaus möglich, dass die Nutzer beider Messenger direkt kommunizieren könnten, es bestehe aber diesbezüglich von beiden Seiten kein Interesse. Open Whisper Systems wolle sein Axolotl-Protokoll weiterentwickeln und diese Änderungen nicht in Whatsapp erzwingen. Geplant sei jedoch, dass in Whatsapp auch der Gruppenchat künftig verschlüsselt wird. Daran arbeitet Open Whispers Systems gegenwärtig mit seinen etwa neun Kernentwicklern um Moxie Marlinspike.

Die Überraschung bei der Ankündigung, Whatsapp verwende jetzt das von Open Whisper Systems entwickelte Verschlüsselungsprotokoll, sei geplant. Dessen Integration habe bereits vor Monaten begonnen. Die Kryptographie sei aber so gut umgesetzt, dass es niemand gemerkt habe. Es habe keine Fehlermeldung durch Benutzer während der Umstellung gegeben, sagte Corbett.

Open Whisper Systems arbeite gerade vornehmlich an der Version von Textsecure in iOS. Wenn sie fertig ist, wird sie in Signal für iOS integriert. In Signal werden künftig der Messenger Textsecure und die verschlüsselte VoIP-Lösung Redphone vereint. Für Android wird es auch eine Version von Signal geben.

Von der Integration in Whatsapp habe Open Whisper Systems viel Erfahrung über die Skalierbarkeit seines Protokolls gesammelt. Sie soll künftig auch in weitere Funktionen einfließen. So sei beispielsweise geplant, die gegenwärtige Abhängigkeit von externen Cloud-Lösungen abzuschaffen. Das sei einer der größten Wünsche aus der Com-

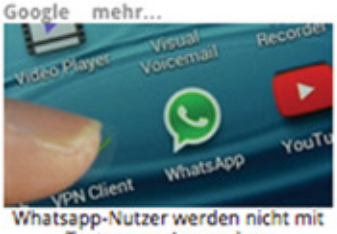
munity, habe wegen Personalmangel aber aktuell nur eine niedrige Priorität.

Bislang ist der Markt der mobilen Messenger sehr zersplittert, in aller Regel sind die verschiedenen Systeme nicht miteinander kompatibel. Den Versuch, verschiedene Messenger-Systeme miteinander kompatibel zu gestalten, gab es bereits einmal: Jabber und das dahinterstehende Protokoll XMPP. Doch zuletzt hat Jabber einiges an Unterstützung eingebüßt. In Sachen Verschlüsselung kann das XMPP-Protokoll mit modernen Lösungen wie Textsecure nicht mithalten.

MESSENGER

Keine Kommunikation zwischen Whatsapp und Textsecure

Textsecure-Nutzer werden auch künftig nicht mit Whatsapp-Anwendern kommunizieren können. Textsecure soll als eigenständiges Produkt bestehen bleiben. Eine weitere Zusammenarbeit soll es dennoch geben.



Whatsapp-Nutzer werden nicht mit Textsecure-Anwendern kommunizieren können. (Bild: Stan Honda/AFP/Getty Images)

Datum: 21.11.2014, 12:15
Autor: Jörg Thoma
Themen: Whatsapp, Facebook, Instant Messenger, Jabber, Soziales Netz, Verschlüsselung, VoIP, XMPP, Applikationen, Internet

Textsecure-Benutzer sollen auch künftig nicht direkt mit Whatsapp-Nutzern verschlüsselt kommunizieren können. Es gebe keine Pläne, das von Open Whispers Systems entwickelte und in Whatsapp integrierte Axolotl-Protokoll gemeinsam zu nutzen. Das sagte Christine Corbett von Open Whisper Systems zu Golem.de am Rande der IT-Sicherheitskonferenz Deepsec 2014 in Wien.

Technisch sei es zwar durchaus möglich, dass die Nutzer beider Messenger direkt kommunizieren könnten, es bestehe aber diesbezüglich von beiden Seiten kein Interesse. Open Whisper Systems wolle sein Axolotl-Protokoll weiterentwickeln und diese Änderungen nicht in Whatsapp erzwingen. Geplant sei jedoch, dass in Whatsapp auch der Gruppenchat künftig verschlüsselt wird. Daran arbeitet Open Whispers Systems gegenwärtig mit seinen etwa neun Kernentwicklern um Moxie Marlinspike.

Die Überraschung bei der Ankündigung, Whatsapp verwende jetzt das von Open Whisper Systems entwickelte Verschlüsselungsprotokoll, sei geplant. Dessen Integration habe bereits vor Monaten begonnen. Die Kryptographie sei aber so gut umgesetzt, dass es niemand gemerkt habe. Es habe keine Fehlermeldung durch Benutzer während der Umstellung gegeben, sagte Corbett.

Open Whisper Systems arbeite gerade vornehmlich an der Version von Textsecure in iOS. Wenn sie fertig ist, wird sie in Signal für iOS integriert. In Signal werden künftig der Messenger Textsecure und die verschlüsselte VoIP-Lösung Redphone vereint. Für Android wird es auch eine Version von Signal geben.

Von der Integration in Whatsapp habe Open Whisper Systems viel Erfahrung über die Skalierbarkeit seines Protokolls gesammelt. Sie soll künftig auch in weitere Funktionen einfließen. So sei beispielsweise geplant, die gegenwärtige Abhängigkeit von externen Cloud-Lösungen abzuschaffen. Das sei einer der größten Wünsche aus der Community, habe wegen Personalmangel aber aktuell nur eine niedrige Priorität.

Bislang ist der Markt der mobilen Messenger sehr zersplittert, in aller Regel sind die verschiedenen Systeme nicht miteinander kompatibel. Den Versuch, verschiedene Messenger-Systeme miteinander kompatibel zu gestalten, gab es bereits einmal: Jabber und das dahinterstehende Protokoll XMPP. Doch zuletzt hat Jabber einiges an Unterstützung eingebüßt. In Sachen Verschlüsselung kann das XMPP-Protokoll mit modernen Lösungen wie Textsecure nicht mithalten. •

Link: http://derstandard.at/2000008419083/Das-Versagen-der-Politik-in-Fragen-IT-Sicherheit

Deepsec: Das Versagen der Politik bei IT-Sicherheit

Datum: 20. November 2014

Name: Andreas Proschofsky

CCC-Sprecher Neumann attestiert fatalen Interessenskonflikt zwischen Schutzfunktion und Begehrlichkeiten der Geheimdienste

Zum mittlerweile achten Mal wird dieser Tage die IT-Sicherheitskonferenz Deepsec in Wien abgehalten. Neben vielen Fachvorträgen spielen dabei auch grundlegende Themen eine wichtige Rolle. So betont Linus Neumann, Sprecher des Chaos Computer Club, in einem Pressegespräch die gesellschaftspolitische Dimension.

Widerspruch

Durch ihr ambivalentes Verhältnis stünde die Politik der IT-Sicherheit derzeit eher im Wege als sie zu befördern. So sei es bezeichnend, dass dieser Bereich üblicherweise in den Innenministerien angesiedelt ist - und damit exakt dort, wo auch massive Anstrengungen unternommen werden, jegliche Computersicherheit zu unterwandern.

Finanzierung

Ein Beispiel: Der deutsche Bundesnachrichtendienst hat gerade erst angekündigt, in den kommenden Jahren 4,5 Millionen Euro für Zero-Day-Exploits zu Spionagezwecken ausgeben zu wollen. Damit werden aber genau jene Kreise finanziert, die solche Lücken aus finanziellen Motiven gezielt zurückhalten.

Selbstleger. Eine Doppelstrategie in IT-Sicherheitsfragen funktioniere aber schlicht nicht. Wer willentlich Sicherheitslücken in Kauf nehme, um einen Spionagevorteil zu haben, gefährde damit auch die eigene Infrastruktur. Ähnlich verhalte es sich mit Hintertüren wie jene zur "Lawful Interception" bei Telekomunternehmen: Jeder Angreifer wisse, dass es diese gebe, also sei sie ein lohnendes Ziel, da man an einem Punkt garantiert alle Daten bekomme.

Alternativen

Dabei könnten Staaten auch ganz anders agieren. Etwa indem mit öffentlichen Geldern Bug Bounties ausgeschrieben werden, um Sicherheitsforschern einen Anreiz zu geben, diese zu melden, anstatt sie gewinnbringend am Schwarzmarkt zu verkaufen. Immerhin werden aktuell bereits tausende Euros für Zero-Day-Exploits geboten. Den Wert einer Lücke wie Heartbleed würde Neumann gar ab einer Viertel Million Euro beziffern.

Fehlernder Wille

Hohe Preise für Bug Bounties würden zwar zweifellos auch die Preise am Schwarzmarkt steigen lassen, trotzdem zeigt sich der Sicherheitsexperte von den positiven Auswirkungen einer solchen Initiative überzeugt. Immerhin gebe es genügend Personen, die keine bösen Absichten hegen, und lieber auf diesem Weg ihr finanzielles Aus-

kommen finden. Derzeit scheint aber der politische Wille für solche eine proaktive Sicherheitspolitik zu fehlen.

Investitionen

Zumindest ortet Neumann zarte Fortschritte im Unternehmensbereich. Nach dem "Super-GAU" mit Hearbleed und Shellshock hätten endlich die ersten Firmen damit begonnen in die Sicherheit von weit verbreiteten Open-Source-Programmen zu investieren. Aber auch hier gibt es natürlich noch viel Luft nach oben.

(apo, derStandard.at, 20.11.2014)

Deepsec: Das Versagen der Politik bei IT-Sicherheit

ANDREAS PROSCHOFSKY
20. November 2014, 14:02

foto: flickr.com/111692634@n04 (CC-Lizenz)

CCC-Sprecher Neumann attestiert fatalen Interessenskonflikt zwischen Schutzfunktion und Begehrlichkeiten der Geheimdienste

Zum mittlerweile achten Mal wird dieser Tage die IT-Sicherheitskonferenz Deepsec in Wien abgehalten. Neben vielen Fachvorträgen spielen dabei auch grundlegende Themen eine wichtige Rolle. So betont Linus Neumann, Sprecher des Chaos Computer Club, in einem Pressegespräch die gesellschaftspolitische Dimension.

Widerspruch

Durch ihr ambivalentes Verhältnis stünde die Politik der IT-Sicherheit derzeit eher im Wege als sie zu befördern. So sei es bezeichnend, dass dieser Bereich üblicherweise in den Innenministerien angesiedelt ist - und damit exakt dort, wo auch massive Anstrengungen unternommen werden, jegliche Computersicherheit zu unterwandern.

Finanzierung

Ein Beispiel: Der deutsche Bundesnachrichtendienst hat gerade erst angekündigt, in den kommenden Jahren 4,5 Millionen Euro für Zero-Day-Exploits zu Spionagezwecken ausgeben zu wollen. Damit werden aber genau jene Kreise finanziert, die solche Lücken aus finanziellen Motiven gezielt zurückhalten.

Selbstleger

Eine Doppelstrategie in IT-Sicherheitsfragen funktioniere aber schlicht nicht. Wer willentlich Sicherheitslücken in Kauf nehme, um einen Spionagevorteil zu haben, gefährde damit auch die eigene Infrastruktur. Ähnlich verhalte es sich mit Hintertüren wie jene zur "Lawful Interception" bei Telekomunternehmen: Jeder Angreifer wisse, dass es diese gebe, also sei sie ein lohnendes Ziel, da man an einem Punkt garantiert alle Daten bekomme.

Alternativen

Dabei könnten Staaten auch ganz anders agieren. Etwa indem mit öffentlichen Geldern Bug Bounties ausgeschrieben werden, um Sicherheitsforschern einen Anreiz zu geben, diese zu melden, anstatt sie gewinnbringend am Schwarzmarkt zu verkaufen. Immerhin werden aktuell bereits tausende Euros für Zero-Day-Exploits geboten. Den Wert einer Lücke wie Heartbleed würde Neumann gar ab einer Viertel Million Euro beziffern.

Fehlernder Wille

Hohe Preise für Bug Bounties würden zwar zweifellos auch die Preise am Schwarzmarkt steigen lassen, trotzdem zeigt sich der Sicherheitsexperte von den positiven Auswirkungen einer

solchen Initiative überzeugt. Immerhin gebe es genügend Personen, die keine bösen Absichten hegen, und lieber auf diesem Weg ihr finanzielles Auskommen finden. Derzeit scheint aber der politische Wille für solche eine proaktive Sicherheitspolitik zu fehlen.

Investitionen

Zumindest ortet Neumann zarte Fortschritte im Unternehmensbereich. Nach dem "Super-GAU" mit Hearbleed und Shellshock hätten endlich die ersten Firmen damit begonnen in die Sicherheit von weit verbreiteten Open-Source-Programmen zu investieren. Aber auch hier gibt es natürlich noch viel Luft nach oben. (apo, derStandard.at, 20.11.2014)

Link

Deepsec

Aktuelle Spiele finden Sie unter Rätsel & Sudoku

http://futurezone.at/netzpolitik/it-sicherheit-ist-kein-rein-technisches-thema/98.164.615

"IT-Sicherheit ist kein rein technisches Thema"

Datum: 20.11.14

Autor: Florian Christof

Auf der Sicherheitskonferenz DeepSec wird diagnostiziert, dass IT-Security darniederliegt. Das Thema gehöre breiter diskutiert und an Schulen vermittelt, so ein Vorschlag.

Die IT-Security liegt am Boden und kaum jemanden scheint es zu kümmern. Das war der Tenor bei der Pressekonferenz der diesjährigen Sicherheitskonferenz DeepSec in Wien. Um der IT-Sicherheit auf die Beine zu helfen, schlägt Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung vor, das Thema breiter zu diskutieren und es als Allgemeinbildung im Lehrplan zu verankern.

Er ist der Ansicht, es sei ein Fehler, zu glauben, IT-Security sei eine durch und durch technische Angelegenheit. Ein Grund für den katastrophalen Zustand der IT-Sicherheitsbranche sei daher, dass meist nur technische Details diskutiert werden, ohne nach langfristigen Lösungen zu suchen.

IT-Security breiter diskutieren

"Nur wenn man aus dem rein technischen Eck herauskommt und IT-Security breiter angeht, um psychologische, pädagogische, politische sowie soziologische Gesichtspunkte erweitert und mit Aspekten des Social Engineering verknüpft, kann es gelingen, nachhaltige Konzepte zu erarbeiten", sagte Schumacher. Daher setzt er sich dafür ein, dass IT-Sicherheit endlich auf wissenschaftlicher Ebene, Disziplin übergreifend diskutiert wird.

Dies sei für Schumacher auch der Ausgangspunkt dafür, dass Informatik im Allgemeinen und IT-Security im Speziellen, als Allgemeinbildung an den Schulen vermittelt wird. "Der heutige Informatikunterricht beschränkt sich meist auf ein bisschen MS Word erklären und eine bunte PowerPoint-Präsentation zu erstellen", kritisiert Schumacher, "Dabei wäre es höchst an der Zeit an den Schulen ein Verständnis für Informatik zu schaffen. Es müsste Grundlegendes gelehrt werden, etwa wie Computer und Netzwerke funktionieren und es müssten dringend auch netzpolitische Themen wie Datenschutz und Privacy vermittelt werden."

Kein Interesse vorhanden

Allerdings vermisst Schumacher dafür den politischen Willen und die Bereitschaft der Lehrer: "In Sachsen-Anhalt wollten wir bereits mehrfach eine Lehrerfortbildung für IT-Vermittlung im Schulunterricht anbieten. Leider ist diese Veranstaltung noch nie zustande gekommen, da das Interesse der Lehrpersonen einfach nicht vorhanden war."

(FUTUREZONE) ERSTELLT AM 20.11.2014, 13:44

DEEPSEC

"IT-Sicherheit ist kein rein technisches Thema"

von Florian Christof 20.11.14, 13:44 FlorianChristof Mail an Autor

Bei IT-Sicherheit gehe es nicht nur um Bits und Bytes - Foto: GETTY IMAGES/ISTOCKPHOTO
ISTOCKPHOTO/PN_Photo/thinkstock

Auf der Sicherheitskonferenz DeepSec wird diagnostiziert, dass IT-Security darniederliegt. Das Thema gehöre breiter diskutiert und an Schulen vermittelt, so ein Vorschlag.

SCHULE, IT-SECURITY, IT-SICHERHEIT

Die IT-Security liegt am Boden und kaum jemanden scheint es zu kümmern. Das war der Tenor bei der Pressekonferenz der diesjährigen Sicherheitskonferenz DeepSec in Wien. Um der IT-Sicherheit auf die Beine zu helfen, schlägt Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung vor, das Thema breiter zu diskutieren und es als Allgemeinbildung im Lehrplan zu verankern.

Er ist der Ansicht, es sei ein Fehler, zu glauben, IT-Security sei eine durch und durch technische Angelegenheit. Ein Grund für den katastrophalen Zustand der IT-Sicherheitsbranche sei daher, dass meist nur technische Details diskutiert werden, ohne nach langfristigen Lösungen zu suchen.

IT-Security breiter diskutieren

"Nur wenn man aus dem rein technischen Eck herauskommt und IT-Security breiter angeht, um psychologische, pädagogische, politische sowie soziologische Gesichtspunkte erweitert und mit Aspekten des Social Engineering verknüpft, kann es gelingen, nachhaltige Konzepte zu erarbeiten", sagte Schumacher. Daher setzt er sich dafür ein, dass IT-Sicherheit endlich auf wissenschaftlicher Ebene, Disziplin übergreifend diskutiert wird.

Dies sei für Schumacher auch der Ausgangspunkt dafür, dass Informatik im Allgemeinen und IT-Security im Speziellen, als Allgemeinbildung an den Schulen vermittelt wird. "Der heutige Informatikunterricht beschränkt sich meist auf ein bisschen MS Word erklären und eine bunte PowerPoint-Präsentation zu erstellen", kritisiert Schumacher, "Dabei wäre es höchst an der Zeit an den Schulen ein Verständnis für Informatik zu schaffen. Es müsste Grundlegendes gelehrt werden, etwa wie Computer und Netzwerke funktionieren und es müssten dringend auch netzpolitische Themen wie Datenschutz und Privacy vermittelt werden."

Kein Interesse vorhanden

FEATURED

VERKEHR
Hier-Box holt bei Autounfällen automatisch Hilfe

REPORTAGE
Buffalo: „Stadt des Lichts" kämpft gegen den Rost

AKTION
Facebook-Video zeigt waghalsige Aktion im AKW Zwentendorf

Allerdings vermisst Schumacher dafür den politischen Willen und die Bereitschaft der Lehrer: "In Sachsen-Anhalt wollten wir bereits mehrfach eine Lehrerfortbildung für IT-Vermittlung im Schulunterricht anbieten. Leider ist diese Veranstaltung noch nie zustande gekommen, da das Interesse der Lehrpersonen einfach nicht vorhanden war."

(FUTUREZONE) ERSTELLT AM 20.11.2014, 13:44

SCHULE, IT-SECURITY, IT-SICHERHEIT

Kommentare ()

Ihr Kommentar
Bitte loggen Sie sich ein

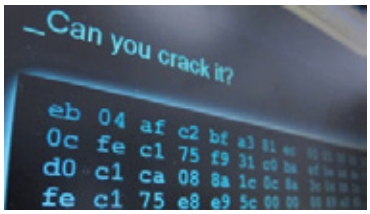
Mehr zum Thema

DEEPSEC

Forscher zeigt: So leicht lassen sich Medizingeräte hacken

Die IT-Sicherheit kommt bei vielen Medizingeräten zu kurz. Bei der Konferenz Deep Sec demonstrierte der Forscher Florian Grunow, wie man einen Patientenmonitor manipuliert.

von Barbara Wimmer



DEEPSEC

"White Hat Hacking ist nicht lukrativ genug"

Bei der DeepSec-Konferenz forderte Linus Neumann vom CCC, Anreize für das Aufdecken von Schwachstellen massiv zu erhöhen und sieht Interessenskonflikte im Innenministerium.

von Florian Christof

IT-SICHERHEIT

"Firmen müssen akzeptieren, dass Netzwerke knackbar sind"

Die IT-Infrastruktur von Firmen ist neuen Herausforderungen ausgesetzt. Thomas Hackner erläutert beim Security Forum des Hagenberger Kreises der FH Oberösterreich ...

von Markus Keßler

Netzpolitik

15.07.2015 13:38 Uhr

SICHERHEIT 8

US-Senator fordert Haftung für Verschlüsselung

Der demokratische Senator Sheldon Whitehouse fordert, dass Opfer eines Verbrechens Unternehmen verklagen können, sollte deren Verschlüsselung jemandem Schaden.

TELEKOM-PAKET

Kritik: Roaming-Abschaffung ist nur Formalität

EU-Parlamentarier der SPÖ, Grüne und ÖVP zeigen sich am Mittwoch - wenn auch aus unterschiedlichen Gründen - enttäuscht über die Entwicklungen bei Roaming und ...

SCHIKANE 1

Snowden-Dokumentarfilmerin Poitras verklagt US-Behörden

Die Filmschaffende verlangt von den US-Behörden Auskunft darüber, warum sie so häufig bei der Einreise in die USA zur Überprüfung festgehalten worden ist.

Featured

VERKEHR

Hier-Box holt bei Autounfällen automatisch Hilfe

Die Hier-Box, ein kleines Gerät zum Nachrüsten, kann bei einem Autounfall selbstständig einen Notruf absetzen. Die Reaktionszeit der Rettung soll so stark verkürzt werden.

von David Kotrba

http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/106898-sicherheitskonferenz-deep-sec-legt-fokus-auf-kommunikation-und-wissen/

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

Datum: 03.11.2014

Autor: Rudolf Felser

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security.

Die Konferenz DeepSec versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt. Wie kann man sich solch eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

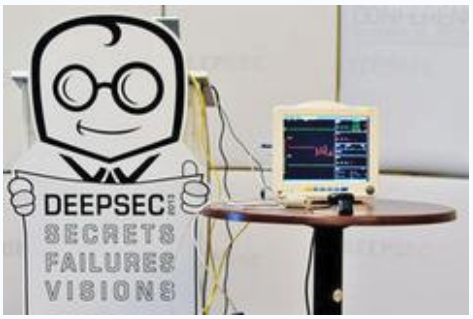
Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. (pi)

Computerwelt: Aktuelle IT-News Osterreich

03.11.2014 *pi/Rudolf Felser*

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security.



DeepSec: Vortrag zu Schwachstellen medizinischer Geräte
© Joanna Pianka

Die Konferenz DeepSec versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt. Wie kann man sich solch eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. (pi)

Sponsored Links:

http://oe1.orf.at/programm/372733

Radiokolleg - Schutz durch Spionage?

Datum: 19. 05.2014

Autor: Sonja Bettel

Die Macht der Geheimdienste

René Pfeiffer, Dienstleister und Lektor für die Sicherheit von Informationstechnologien und Organisator der Wiener Sicherheitskonferenz DeepSec, über Angriffsmöglichkeiten durch Geheimdienste und Möglichkeiten und Grenzen des Schutzes vor Überwachung.

Zwischen Stasi und NSA

Viele Menschen lieben Bücher und Filme über Geheimdienste und vor allem über ihre Protagonisten, die Spione. Sie sind lässige Womanizer wie James Bond, eiskalte Killer wie Jason Bourne und überleben die schlimmsten Anschläge, wie Ethan Hunt in "Mission: Impossible". Spezialwaffen, schöne Frauen, schnelle Autos, Flugzeuge, versteckte Kameras und Tonbandgeräte, ein gestählter Körper und alle Psycho-Tricks der Welt sind selbstverständlich inbegriffen.Doch wie sieht das Leben von Agenten und Agentinnen im wirklichen Leben aus? Warum und seit wann gibt es Geheimdienste und wie sind sie organisiert? Und was leisten sie überhaupt?

Nach den Snowden-Enthüllungen über die NSA, die National Security Agency der USA, die lange Zeit so geheim war, dass sie ihre eigene Existenz leugnete, stellen sich dazu viele Fragen. Denn das Bild, das durch die Enthüllungen entstand, ist eher jenes von gelangweilten Beamt/innen, die in Hochsicherheitsgebäuden Computerprogramme und Server betreuen, die jeden Tag mehrere Petabyte an Kommunikationsdaten aus aller Welt absaugen, durchsuchen und speichern.In den vergangenen Jahren sind aber auch Bilder von Geheimdiensten entstanden, die Menschen aus westlichen Demokratien entführen und in Diktaturen auf Auftrag foltern und verschwinden lassen. Es drängen sich unweigerlich Vergleiche auf zwischen der teils gefürchteten und teils belächelten Stasi der ehemaligen DDR und dem riesigen Überwachungs- und Spionageapparat der heutigen USA.

Sind Geheimdienste unvermeidlich? Können wir sie kontrollieren? Und wie viel "intelligence" liefern sie überhaupt angesichts der Datenflut heutiger elektronischer Kommunikation?

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

Radiokolleg - Schutz durch Spionage?

Montag
19. Mai 2014
09:05

Die Macht der Geheimdienste (1). Gestaltung: Sonja Bettel

(c) Schimmer, ORF

Audio als mp3

AUDIO 19:54
Externer Player

René Pfeiffer, Dienstleister und Lektor für die Sicherheit von Informationstechnologien und Organisator der Wiener Sicherheitskonferenz DeepSec, über Angriffsmöglichkeiten durch Geheimdienste und Möglichkeiten und Grenzen des Schutzes vor Überwachung.

Zwischen Stasi und NSA

Viele Menschen lieben Bücher und Filme über Geheimdienste und vor allem über ihre Protagonisten, die Spione. Sie sind lässige Womanizer wie James Bond, eiskalte Killer wie Jason Bourne und überleben die schlimmsten Anschläge, wie Ethan Hunt in "Mission: Impossible". Spezialwaffen, schöne Frauen, schnelle Autos, Flugzeuge, versteckte Kameras und Tonbandgeräte, ein gestählter Körper und alle Psycho-Tricks der Welt sind selbstverständlich inbegriffen.

Doch wie sieht das Leben von Agenten und Agentinnen im wirklichen Leben aus? Warum und seit wann gibt es Geheimdienste und wie sind sie organisiert? Und was leisten sie überhaupt? Nach den Snowden-Enthüllungen über die NSA, die National Security Agency der USA, die lange Zeit so geheim war, dass sie ihre eigene Existenz leugnete, stellen sich dazu viele Fragen. Denn das Bild, das durch die Enthüllungen entstand, ist eher jenes von gelangweilten Beamt/innen, die in Hochsicherheitsgebäuden Computerprogramme und Server betreuen, die jeden Tag mehrere Petabyte an Kommunikationsdaten aus aller Welt absaugen, durchsuchen und speichern.

(c) Gebert, DPA

In den vergangenen Jahren sind aber auch Bilder von Geheimdiensten entstanden, die Menschen aus westlichen Demokratien entführen und in Diktaturen auf Auftrag foltern und verschwinden lassen. Es drängen sich unweigerlich Vergleiche auf zwischen der teils gefürchteten und teils belächelten Stasi der ehemaligen DDR und dem riesigen Überwachungs- und Spionageapparat der heutigen USA.

Sind Geheimdienste unvermeidlich? Können wir sie kontrollieren? Und wie viel "intelligence" liefern sie überhaupt angesichts der Datenflut heutiger elektronischer Kommunikation?

zurück

Gestaltung: Sonja Bettel · zur Sendereihe

Kategorie: Wissen

http://fm4.orf.at/stories/1737330/

Der neueste Unsicherheitsstandard der NSA

Datum: 21.04.2014

Autor: Erich Möchel

Der aktuell beim Gremium für Internetstandards IETF eingereichte Entwurf der NSA für verschlüsselte Internettelefonie ist an Dreistigkeit kaum zu überbieten.

Langsam zeichnet sich hinter dem Agieren der NSA-Techniker in Standardisierungsgremien wie der "Internet Engineering Task Force" (IETF) eine Methodik ab. Die ist verblüffend einfach, geradlinig und strukturell ganz ähnlich auch in anderen Entwürfen der NSA anzutreffen. Auch der neueste Standardentwurf, den ein mittlerweile bekannter NSA-Techniker namens Kevin Igoe am 1. April 2014 bei der IETF eingereicht hatte, zeigt ein solches Muster.

Dieser aktuelle NSA-Entwurf betrifft das Protokoll zur Verschlüsselung von Internettelefonie. Der dafür vorgesehene Blockchiffre-Modus namens "Galois Counter Mode" (GCM) aber wurde bereits 2005 von einem namhaften Kryptografie-Eperten von Microsoft als generell angreifbar bezeichnet und vernichtend kritisiert. Speziell und eindringlich wurde davor gewarnt, diese Chiffre für Echtzeit-Protokolle einzusetzen, als negatives Praxisbeispiel dafür wurde die Verschlüsselung von Internettelefonie angeführt.

Die Methodik der NSA

Neun Jahre danach schlägt die NSA nun genau jenen Chiffriermodus GCM als Kernelement eines internationalen Verschlüsselungstandards für Internettelefonie vor. Und das, obwohl mehrere andere Chiffriermodi für diesen Zweck zur Verfügung stehen, die gerade diese Schwächen nicht aufweisen. Das entspricht der darunterliegenden, grundlegenden Methodik der NSA, die potentiell verheerende Wirkung dieser Vorgehensweise wurde von einem internationalen Forscherteam erst Ende März in der Praxis nachgewiesen.

TextCC IETF

Stets sind es zwei oder mehr verschiedene Komponenten des Verschlüsselungsvorgangs, die ihre Wirkung erst in ihrer Kombination entfalten. Und stets war mindestens eines dieser Elemente bereits davor in die Kritik der Fachwelt geraten, was die NSA jedoch nicht davon abgehalten hat, "verbesserte" Versionen davon erneut aufs Tapet zu bringen. Im Praxistest des Kryptografenteams, der nur einen Tag vor der Einreichung des aktuellen NSA-Standardvorschlags für verschlüsselte VoIP-Telefonie veröffentlicht wurde, wird dieses Muster ersichtlich.

Der aktuelle IETF-Entwurf für SRTP mit dem Blockchiffriermodus "Galois Counter Mode"

Wenn zwei Faktoren zusammentreffen

Der Test betraf den Zufallszahlengenerator "Dual EC DRBG", der von der NSA stammt und seit Anbeginn im Verdacht stand, letztlich berechenbare "Zufallszahlen" zu erzeugen. Mit der Qualität, also dem Grad der Zufälligkeit dieser Zahlen, aber steht und fällt jeder Verschlüsselungsvorgang. Ein im Vergleich zu NSA-Equipment mickriger Angriffsrechner mit 14 Prozessoren, der von den Forschern eingesetzt wurde, benötigte zwischen einer und drei Stunden um diesen in die BSAFe-Suite der Firma RSA integrierten Zahlengenerator zu knacken.

Im Rahmen des "Bullrun"-Programms, das gerade unter Netzwerkern für besondere Empörung gesorgt hat, schleusen NSA-nahe Techniker möglichst plausible Erweiterungen in bestehende Verschlüsselungsprotokolle ein, um diese auszuhebeln. Die Kombination von "Dual EC DRBG" und "Extended Random" im Detail.

Das eigentlich Verblüffende aber passierte, als in dieses Set-Up noch eine Erweiterung des für alle möglichen Arten von Verschlüsselung verwendeten Protokolls TLS/SSL integriert wurde. Diese ebenfalls von der NSA stammende Protokollerweiterung namens "Extended Random" beschleunigte den Entschlüsselungsvorgang um den Faktor 65.000. Damit dauerte es gerade noch vier Sekunden, um den Output von "Dual EC DRBG" zu berechnen.

Knackpunkt Chiffriermodus

Der neueste Entwurf der NSA bei der IETF weist strukturell ganz ähnliche Züge auf, auch wenn der Knackpunkt hier ein ganz anderes Element des Verschlüsselungsvorgangs betrifft, nämlich Blockchiffre-Modi und ihre Verkettung. Der aktuelle Entwurf Igoes bezieht sich auf Verschlüsselung und Authentifizierung im "Secure Real Time Protocol" (SRTP). Das ist die verschlüsselte Variante der herkömmlichen Internettelefonie (VoIP), die das RTP-Protokoll benutzt.

Das "Bullrun"-Projekt der NSA-Projekt sieht dem "Cloud-Überwachungsstandard" des European Telecom Standards Institute frappierend ähnlich. Erst seit den Enthüllungen Edward Snowdens sind Name und Mission dieses Projekts von NSA und GCHQ bekannt

Dabei soll nach dem Willen der NSA der "Galois Counter Mode" (GCM) als Modus zum Einsatz kommen, der als besonders schlank und schnell gilt und einen hohen Datendurchsatz verspricht. GCM hat deshalb bei Cloud-Anwendungen Verbreitung, als Vorteil wird dabei hervorgehoben, dass GCM für Parallel-Computing gut geeignet ist. Ebenso ist ein Einsatz in rechenschwachen Umgebungen, also "Embedded"-Geräten denkbar. GCM hat also dur-

chaus dort Meriten, wo Rechen- und Datendurchsatzzeiten absolut kritische Faktoren sind. Dafür wurde der Modus nämlich entwickelt. Die Schnelligkeit din diesem Chiffriermodus wird freilich dadurch erzielt, dass Authentifizierung und Verschlüsselung mit einer einzigen Funktion abgewickelt werden.

Zwei Anwendungen in einer

"Bei Anwendungen, die robuste Sicherheit verlangen, ist das unüblich", sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at, "Man hat diese beiden Funktionen immer schon deshalb getrennt gehalten, weil Angriffe dadurch erschwert werden." Die durch die Schlankheit von GCM gewonnene Rechengeschwindigkeit könne bei VoIP-Telefonie so eher einem Angreifer zu Gute kommen, so Kafka weiter, während sich der Vorteil von GCM für die Abwicklung gerade von Internettelefonie in marginalen Grenzen halte.

Anders als etwa beim Cloud-Computing, wo gewaltige Datenmengen ver- und entschlüsselt werden müssen, nehmen sich die bei VoIP-Telefonie anfallenden Daten nachgerade verschwindend aus. Angesichts der Leistungsfähigkeit der Prozessoren in heute gängigen Smartphones falle dieser Gewinn an Performance deshalb in der Praxis überhaupt nicht mehr ins Gewicht, sagte Kafka.

"Galois Counter Mode"

Der grundsätzliche Vorteil der "Galois Counter Mode"-Methode, nämlich Effizienz und hoher Datendurchsatz kommt unter diesen Voraussetzungen also eben nicht zum Tragen, während sich die Nachteile gerade bei einem Echtzeitprotokoll wie SRTP multiplizieren. Auch hier gibt es auffällige Parallelen zum Fall des anrüchigen Zahlengenerators "Dual EC DRBG".

Eine 2008 von der NSA eingereichte Erweiterung des TLS/SSL-Protokolls namens "Extended Random" war von den in der IETF vertretenen, großteils zivilen Technikern letzlich deshalb abgelehnt worden, weil keine praktischen Vorteile dafür erkennbar waren. Wie der Feldversuch der Forscher nun zeigte, hatte "Extended Random" nur einen einzigen "Vorteil": Ein Angriff der NSA auf den Verschlüsselungsvorgang wurde um den Faktor 65.000 beschleunigt.

Negatives Musterbeispiel anno 2005

Bereits 2005 hatte der bekannte Kryptograf Niels Ferguson von Microsoft zwei grundlegende Schwächen gegenüber Angriffen in "Galois Counter Mode" nachgewiesen und vor dem Einsatz von GCM als universellem Modus für kryptografische Blockchiffren gewarnt. Als negatives Musterbeispiel dafür führte Ferguson damals den möglichen Einsatz von GCM bei verschlüsselter Internettelefonie an.

TextMicrosoft

Das Gutachten Niels Fergusons im Volltext: "Authentication weaknesses in GCM"

Weil die Schwäche besonders eklatant zu Tage tritt, wenn zu kurze "Authentifizierungs-Tags" verwendet werden, riet Ferguson: "Wenn man umständehalber gezwungen ist, GCM einzusetzen, sollte man den Modus ausschließlich mit 128-Bit langen Tags benützen." Grundsätzlich riet der holländische Kryptograf vom Einsatz dieses Modus überhaupt ab und empfahl andere Blockchiffre-Modi zu benützen, die diese Schwächen eben nicht aufwiesen.

Wie GCM zum NIST-Standard wurde

2007 wurde GCM dennoch durch die US-Standardisierungsbehörde NIST in den Rang eines nationalen Standards erhoben, sieben Jahre danach, am 1. April 2014 schlug nun die NSA "Galois Counter Mode" ausgerechnet für jene Anwendung vor, für die man GCM laut Ferguson und einer Reihe anderer Fachleute auf keinen Fall einsetzen sollte.

Galois Counter Mode, NIST-Standard SP 800-38D

Wie auf dem Screenshot des aktuellen NSA-Entwurfs nun zu sehen ist, sind auch nicht wie 2005 empfohlen, ausschließlich 128-Bit sondern auch 64-Bit lange Tags für die Authentifizierung vorgesehen. Was auf den ersten Blick nur doppelt so viel ist, ergibt bei einer Exponentialrechnung doch deutlich mehr. "Der Unterschied zwischen 64 und 128 langen Tags ergibt eine Zahl mit 20 Nullen vor dem Komma. Ein solcher Faktor im Trillionenbereich macht dann doch einen gewaltigen Unterschied, wenn angegriffen wird" sagte Kafka.

TabelleCC IETF

Michael Kafka ist internationaler Sicherheitsexperte und Mitveranstalter der Wiener Deepsec-Konferenz deren Motto ist "Bleeding Edge Security"

Unangebrachte Schlüsse

Der aktuelle Entwurf für diesen internationalen Standard bei der IETF verzeichnet neben dem NSA-Mann Kevin Igoe noch einen zweiten Namen, nämlich den des Cisco-Technikers David McGrew. Die vorschnelle Annahme, dass sich da Cisco mit der NSA zusammengetan hätte, um sichere Verschlüsselung zu sabotieren, wäre jedoch grundverkehrt.

Wie die Praxis in den Arbeitsgruppen der IETF zeigt, wird (nicht nur) bei kryptografiebezogenen Einreichungen

dem jeweiligen Vertschlüsselungsexperten auch ein Spezialist für die Ebene der Protokolle beigestellt. Heißt die einreichende Partei dann NSA kommt eben auch ein ziviler Techniker zum Handkuss, der mit der Einreichung selbst eigentlich nichts zu tun hat, außer sie in die Protokolle zu integrieren. Im Falle von "Extended Random" kam zum Beispiel ein Protokollspezialist der Mozilla Foundation zur zweifelhaften Ehre, als Koautor einer Einreichung der hochrangigen NSA-Technikerin Margaret Salter zu firmieren.

Wie Techniker unter Druck geraten

Im Falle von McGrew erwies sich diese Vorgangsweise, die von der NSA benützt wird, als besonders perfid. McGrew ist nämlich Koautor von "Galois Counter Mode", um dessen Einsatz sich der gesamte NSA-Entwurf ja dreht. Hier sieht man, unter welchen Druck der weltweit insgesamt recht kleine Kreis von Verschlüsselungsspezialisten durch die NSA geraten ist. Im Dezember hatte einer Reihe ziviler Techniker in der IETF gegen diese Art von Einflussnahme durch die NSA rebelliert und die Absetzung Kevin Igoes als zweiten Vorsitzenden der IETF-Forschungsgruppe für Kryptografie gefordert.

Die Forderung nach Absetzung Igoes auf der Mailing-Liste, samt dem Thead mit den Antworten der anderen Techniker

Igoe hatte einen Entwurf für ein passwortbasiertes Protokoll zum Schlüsselaustausch namens "Dragonfly" präsentiert, das er als einziger, der in der Forschungsgruppe versammelten Techniker für gut befunden hatte. Während der Konsens dort lautete, Dragonfly sei "ein schlampig gearbeitetes und unseriöses Protokoll" hatte Igoe versucht, es der übergeordneten TLS-Arbeitsgruppe in der IETF als Konsens der Kryptospezialisten zu verkaufen.

Die Dreistigkeit der NSA

Mit dem aktuellen Vorschlag, ausgerechnet "Galois Counter Mode" für verschlüsselte Internettelefonie zu verwenden hat Igoe seine damalige Vorgangsweise an Dreistigkeit noch übertroffen. Den Kopf mit dafür hinhalten muss nun Cisco-Techniker McGrew, der GCM für völlig andere Zwecke miterfunden hat.

Dass vordergründige Konspirationsthesen hier überhaupt nicht greifen, zeigt die Erwähnung McGrews in der Expertise des Microsoft-Technikers Niels Ferguson. Unter der Handvoll von Experten, bei denen sich Ferguson für die technische Unterstützung bei seiner vernichtenden Analyse von "Galois Counter Mode" bedankte, war auch der Koautor von GCM, David McGrew.

Parallelen zu SSH

Der finnische Kryptograf Markku-Juhani Saarinen hatte 2012 auf der Sicherheitskonferenz FSE 2012 in Washington ebenfalls vor dem Einsatz der Blockchiffre gewarnt. Gerade bei Echtzeitprotokollen wie Secure Shell für Virtual Private Networks sei von GCM dringend abzuraten. "Wenn tatsächlich rationale Gründe für den Einsatz von GCM vorlägen, etwa in Hochgeschwindigkeits-VPNs" dann sollte das nur geschehen, wenn vorher eine Risikoabschätzung stattgefunden haben, hieß es in Saarinens Vortrag.

RFC 5647 der IETF CC IETF 2009

Die NSA-Techniker Kevin Igoe und Jerry Salinas waren von solchen Überlegungen offenbar nicht geplagt. Im Frühjahr 2009 wurde von beiden der Entwurf RFC 5647 bei der IETF eingereicht und im August dort durchgewunken. Der Titel: "Galois Counter Mode" für das Secure Shell Layer Protocol".

Der Vortrag Saarinens auf der FSE-Konferenz 2009 und der RFC 5647 der IETF

Das Bombardierkäfer-Prinzip

Niels Ferguson wiederum war einer der beiden Microsoft-Spezialisten, die bereits 2007 vor dem anrüchigen NSA-Zufallszahlengenerator "Dual EC DRBG" gewarnt hatten. Eine wirklich verheerende Wirkung entfaltete der erst in Kombination mit der Erweiterung "Extended Random" von 2008. Der Wiener Sicherheitsexperte Michael Kafka nennt dies das "Bombardierkäfer-Prinzip".

Der Bombardierkäfer in der Wikipedia

Der Abwehrmechanismus dieser Laufkäferart besteht darin, zwei jeweils für sich gesehen harmlose Flüssigkeiten getrennt im Körper vorzuhalten. Wenn sie jedoch vermischt und ausgespritzt werden, erhitzt sich diese Mischung plötzlich auf etwa 100 Grad wobei sie obendrein noch stark ätzend wirkt.

Erstellt am: 21. 4. 2014 - 19:00 Uhr

Der neueste Unsicherheitsstandard der NSA

Der aktuell beim Gremium für Internetstandards IETF eingereichte Entwurf der NSA für verschlüsselte Internettelefonie ist an Dreistigkeit kaum zu überbieten.

Langsam zeichnet sich hinter dem Agieren der NSA-Techniker in Standardisierungsgremien wie der "Internet Engineering Task Force" (IETF) eine Methodik ab. Die ist verblüffend einfach, geradlinig und strukturell ganz ähnlich auch in anderen Entwürfen der NSA anzutreffen. Auch der neueste Standardentwurf, den ein mittlerweile bekannter NSA-Techniker namens Kevin Igoe am 1. April 2014 bei der IETF eingereicht hatte, zeigt ein solches Muster.

Dieser aktuelle NSA-Entwurf betrifft das Protokoll zur Verschlüsselung von Internettelefonie. Der dafür vorgesehene Blockchiffre-Modus namens "Galois Counter Mode" (GCM) aber wurde bereits 2005 von einem namhaften Kryptografie-Eperten von Microsoft als generell angreifbar bezeichnet und vernichtend kritisiert. Speziell und eindringlich wurde davor gewarnt, diese Chiffre für Echtzeit-Protokolle einzusetzen, als negatives Praxisbeispiel dafür wurde die Verschlüsselung von Internettelefonie angeführt.

Die Methodik der NSA

Neun Jahre danach schlägt die NSA nun genau jenen Chiffriermodus GCM als Kernelement eines internationalen Verschlüsselungstandards für Internettelefonie vor. Und das, obwohl mehrere andere Chiffriermodi für diesen Zweck zur Verfügung stehen, die gerade diese Schwächen nicht aufweisen. Das entspricht der darunterliegenden, grundlegenden Methodik der NSA, die potentiell verheerende Wirkung dieser Vorgehensweise wurde von einem internationalen Forscherteam erst Ende März in der Praxis nachgewiesen.

Network Working Group D. McGrew
Internet Draft Cisco Systems, Inc.
Intended Status: Standards Track K. Igoe
Expires: October 03, 2014 National Security Agency
April 01, 2014

AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)
draft-ietf-avtcore-srtp-aes-gcm-11

CC IETF

Stets sind es zwei oder mehr verschiedene Komponenten des Verschlüsselungsvorgangs, die ihre Wirkung erst in ihrer Kombination entfalten. Und stets war mindestens eines dieser Elemente bereits davor in die Kritik der Fachwelt geraten, was die NSA jedoch nicht davon abgehalten hat, "verbesserte" Versionen davon erneut aufs Tapet zu bringen. Im Praxistest des Kryptografenteams, der nur einen Tag vor der Einreichung des aktuellen NSA-Standardvorschlags für verschlüsselte VoIP-Telefonie veröffentlicht wurde, wird dieses Muster ersichtlich.

Der aktuelle IETF-Entwurf für SRTP mit dem Blockchiffriermodus "Galois Counter Mode" (http://tools.ietf.org/html/draft-ietf-avtcore-srtp-aes-gcm-11)

Wenn zwei Faktoren zusammentreffen

Der Test betraf den Zufallszahlengenerator "Dual EC DRBG", der von der NSA stammt und seit Anbeginn im Verdacht stand, letztlich berechenbare "Zufallszahlen" zu erzeugen. Mit der Qualität, also dem Grad der Zufälligkeit dieser Zahlen, aber steht und fällt jeder Verschlüsselungsvorgang. Ein im Vergleich zu NSA-Equipment mickriger Angriffsrechner mit 14 Prozessoren, der von den Forschern eingesetzt wurde, benötigte zwischen einer und drei Stunden um diesen in die BSAFe-Suite der Firma RSA integrierten Zahlengenerator zu knacken.

Im Rahmen des "Bullrun"-Programms, das gerade unter Netzwerkern für besondere Empörung gesorgt hat, schleusen NSA-nahe Techniker möglichst plausible Erweiterungen in bestehende Verschlüsselungsprotokolle ein, um diese auszuhebeln. Die Kombination von "Dual EC DRBG" und "Extended Random" im Detail.

Das eigentlich Verblüffende aber passierte, als in dieses Set-Up noch eine Erweiterung des für alle möglichen Arten von Verschlüsselung verwendeten Protokolls TLS/SSL integriert wurde. Diese ebenfalls von der NSA stammende Protokollerweiterung namens "Extended Random" beschleunigte den Entschlüsselungsvorgang um den Faktor 65.000. Damit dauerte es gerade noch vier Sekunden, um den Output von "Dual EC DRBG" zu berechnen.

Knackpunkt Chiffriermodus

Der neueste Entwurf der NSA bei der IETF weist strukturell ganz ähnliche Züge auf, auch wenn der Knackpunkt hier ein ganz anderes Element des Verschlüsselungsvorgangs betrifft, nämlich Blockchiffre-Modi und ihre Verkettung. Der aktuelle Entwurf Igoes bezieht sich auf Verschlüsselung und Authentifizierung im "Secure Real Time Protocol" (SRTP). Das ist die verschlüsselte Variante der herkömmlichen Internettelefonie (VoIP), die das RTP-Protokoll benutzt.

Das "Bullrun"-Projekt der NSA-Projekt sieht dem "Cloud-Überwachungsstandard" des European Telecom Standards Institute frappierend ähnlich. Erst seit den Enthüllungen Edward Snowdens sind Name und Mission dieses Projekts von NSA und GCHQ bekannt

Dabei soll nach dem Willen der NSA der "Galois Counter Mode" (GCM) als Modus zum Einsatz

kommen, der als besonders schlank und schnell gilt und einen hohen Datendurchsatz verspricht. GCM hat deshalb bei Cloud-Anwendungen Verbreitung, als Vorteil wird dabei hervorgehoben, dass GCM für Parallel-Computing gut geeignet ist. Ebenso ist ein Einsatz in rechenschwachen Umgebungen, also "Embedded"-Geräten denkbar. GCM hat also durchaus dort Meriten, wo Rechen- und Datendurchsatzzeiten absolut kritische Faktoren sind. Dafür wurde der Modus nämlich entwickelt. Die Schnelligkeit din diesem Chiffriermodus wird freilich dadurch erzielt, dass Authentifizierung und Verschlüsselung mit einer einzigen Funktion abgewickelt werden.

Zwei Anwendungen in einer

"Bei Anwendungen, die robuste Sicherheit verlangen, ist das unüblich", sagte der Wiener Sicherheitsexperte Michael Kafka zu ORF.at, "Man hat diese beiden Funktionen immer schon deshalb getrennt gehalten, weil Angriffe dadurch erschwert werden." Die durch die Schlankheit von GCM gewonnene Rechengeschwindigkeit könne bei VoIP-Telefonie so eher einem Angreifer zu Gute kommen, so Kafka weiter, während sich der Vorteil von GCM für die Abwicklung gerade von Internettelefonie in marginalen Grenzen halte.

Anders als etwa beim Cloud-Computing, wo gewaltige Datenmengen ver- und entschlüsselt werden müssen, nehmen sich die bei VoIP-Telefonie anfallenden Daten nachgerade verschwindend aus. Angesichts der Leistungsfähigkeit der Prozessoren in heute gängigen Smartphones falle dieser Gewinn an Performance deshalb in der Praxis überhaupt nicht mehr ins Gewicht, sagte Kafka.

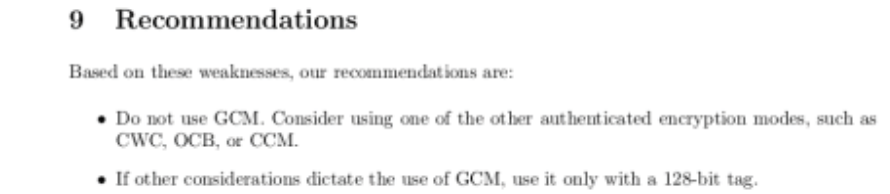
"Galois Counter Mode"

Der grundsätzliche Vorteil der "Galois Counter Mode"-Methode, nämlich Effizienz und hoher Datendurchsatz kommt unter diesen Voraussetzungen also eben nicht zum Tragen, während sich die Nachteile gerade bei einem Echtzeitprotokoll wie SRTP multiplizieren. Auch hier gibt es auffällige Parallelen zum Fall des anrüchigen Zahlengenerators "Dual EC DRBG".

Eine 2008 von der NSA eingereichte Erweiterung des TLS/SSL-Protokolls namens "Extended Random" war von den in der IETF vertretenen, großteils zivilen Technikern letzlich deshalb abgelehnt worden, weil keine praktischen Vorteile dafür erkennbar waren. Wie der Feldversuch der Forscher nun zeigte, hatte "Extended Random" nur einen einzigen "Vorteil": Ein Angriff der NSA auf den Verschlüsselungsvorgang wurde um den Faktor 65.000 beschleunigt.

Negatives Musterbeispiel anno 2005

Bereits 2005 hatte der bekannte Kryptograf Niels Ferguson von Microsoft zwei grundlegende Schwächen gegenüber Angriffen in "Galois Counter Mode" nachgewiesen und vor dem Einsatz von GCM als universellem Modus für kryptografische Blockchiffren gewarnt. Als negatives Musterbeispiel dafür führte Ferguson damals den möglichen Einsatz von GCM bei verschlüsselter Internettelefonie an.



9 Recommendations

Based on these weaknesses, our recommendations are:

- Do not use GCM. Consider using one of the other authenticated encryption modes, such as CWC, OCB, or CCM.
- If other considerations dictate the use of GCM, use it only with a 128-bit tag.

Microsoft

Das Gutachten Niels Fergusons im Volltext: "Authentication weaknesses in GCM" (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf)

Weil die Schwäche besonders eklatant zu Tage tritt, wenn zu kurze "Authentifizierungs-Tags" verwendet werden, riet Ferguson: "Wenn man umständehalber gezwungen ist, GCM einzusetzen, sollte man den Modus ausschließlich mit 128-Bit langen Tags benützen." Grundsätzlich riet der holländische Kryptograf vom Einsatz dieses Modus überhaupt ab und empfahl andere Blockchiffre-Modi zu benützen, die diese Schwächen eben nicht aufwiesen.

Wie GCM zum NIST-Standard wurde

2007 wurde GCM dennoch durch die US-Standardisierungsbehörde NIST in den Rang eines nationalen Standards erhoben, sieben Jahre danach, am 1. April 2014 schlug nun die NSA "Galois Counter Mode" ausgerechnet für jene Anwendung vor, für die man GCM laut Ferguson und einer Reihe anderer Fachleute auf keinen Fall einsetzen sollte.

Galois Counter Mode, NIST-Standard SP 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

Wie auf dem Screenshot des aktuellen NSA-Entwurfs nun zu sehen ist, sind auch nicht wie 2005 empfohlen, ausschließlich 128-Bit sondern auch 64-Bit lange Tags für die Authentifizierung vorgesehen. Was auf den ersten Blick nur doppelt so viel ist, ergibt bei einer Exponentialrechnung doch deutlich mehr. "Der Unterschied zwischen 64 und 128 langen Tags ergibt eine Zahl mit 20 Nullen vor dem Komma. Ein solcher Faktor im Trillionenbereich macht dann doch einen gewaltigen Unterschied, wenn angegriffen wird" sagte Kafka.

Parameter	Value
Master key length	128 bits
Master salt length	96 bits
Key Derivation Function	AES_CM_PRF [RFC3711]
Default key lifetime (SRTP)	2^48 packets
Default key lifetime (SRTCP)	2^31 packets
Cipher (for SRTP and SRTCP)	AEAD_AES_128_GCM_8
AEAD authentication tag length	64 bits

CC IETF

Michael Kafka ist internationaler Sicherheitsexperte und Mitveranstalter der Wiener Deepsec-Konferenz deren Motto ist "Bleeding Edge Security" (https://deepsec.net)

Unangebrachte Schlüsse

Der aktuelle Entwurf für diesen internationalen Standard bei der IETF verzeichnet neben dem NSA-Mann Kevin Igoe noch einen zweiten Namen, nämlich den des Cisco-Technikers David McGrew. Die vorschnelle Annahme, dass sich da Cisco mit der NSA zusammengetan hätte, um sichere Verschlüsselung zu sabotieren, wäre jedoch grundverkehrt.

Wie die Praxis in den Arbeitsgruppen der IETF zeigt, wird (nicht nur) bei kryptografiebezogenen Einreichungen dem jeweiligen Vertschlüsselungsexperten auch ein Spezialist für die Ebene der Protokolle beigestellt. Heißt die einreichende Partei dann NSA kommt eben auch ein ziviler Techniker zum Handkuss, der mit der Einreichung selbst eigentlich nichts zu tun hat, außer sie in die Protokolle zu integrieren. Im Falle von "Extended Random" kam zum Beispiel ein Protokollspezialist der

Mozilla Foundation zur zweifelhaften Ehre, als Koautor einer Einreichung der hochrangigen NSA-Technikerin Margaret Salter zu firmieren.

Wie Techniker unter Druck geraten

Im Falle von McGrew erwies sich diese Vorgangsweise, die von der NSA benützt wird, als besonders perfid. McGrew ist nämlich Koautor von "Galois Counter Mode", um dessen Einsatz sich der gesamte NSA-Entwurf ja dreht. Hier sieht man, unter welchen Druck der weltweit insgesamt recht kleine Kreis von Verschlüsselungsspezialisten durch die NSA geraten ist. Im Dezember hatte einer Reihe ziviler Techniker in der IETF gegen diese Art von Einflussnahme durch die NSA rebelliert und die Absetzung Kevin Igoes als zweiten Vorsitzenden der IETF-Forschungsgruppe für Kryptografie gefordert.

Die Forderung nach Absetzung Igoes auf der Mailing-Liste, samt dem Thead mit den Antworten der anderen Techniker (http://www.ietf.org/mail-archive/web/cfrg/current/msg03554.html)

Igoe hatte einen Entwurf für ein passwortbasiertes Protokoll zum Schlüsselaustausch namens "Dragonfly" präsentiert, das er als einziger, der in der Forschungsgruppe versammelten Techniker für gut befunden hatte. Während der Konsens dort lautete, Dragonfly sei "ein schlampig gearbeitetes und unseriöses Protokoll" hatte Igoe versucht, es der übergeordneten TLS-Arbeitsgruppe in der IETF als Konsens der Kryptospezialisten zu verkaufen.

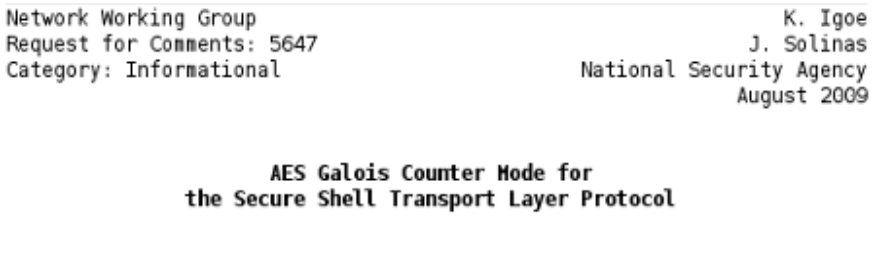
Die Dreistigkeit der NSA

Mit dem aktuellen Vorschlag, ausgerechnet "Galois Counter Mode" für verschlüsselte Internettelefonie zu verwenden hat Igoe seine damalige Vorgangsweise an Dreistigkeit noch übertroffen. Den Kopf mit dafür hinhalten muss nun Cisco-Techniker McGrew, der GCM für völlig andere Zwecke miterfunden hat.

Dass vordergründige Konspirationsthesen hier überhaupt nicht greifen, zeigt die Erwähnung McGrews in der Expertise des Microsoft-Technikers Niels Ferguson. Unter der Handvoll von Experten, bei denen sich Ferguson für die technische Unterstützung bei seiner vernichtenden Analyse von "Galois Counter Mode" bedankte, war auch der Koautor von GCM, David McGrew.

Parallelen zu SSH

Der finnische Kryptograf Markku-Juhani Saarinen hatte 2012 auf der Sicherheitskonferenz FSE 2012 in Washington ebenfalls vor dem Einsatz der Blockchiffre gewarnt. Gerade bei Echtzeitprotokollen wie Secure Shell für Virtual Private Networks sei von GCM dringend abzuraten. "Wenn tatsächlich rationale Gründe für den Einsatz von GCM vorlägen, etwa in Hochgeschwindigkeits-VPNs" dann sollte das nur geschehen, wenn vorher eine Risikoabschätzung stattgefunden haben, hieß es in Saarinens Vortrag.



Network Working Group — K. Igoe
Request for Comments: 5647 — J. Solinas
Category: Informational — National Security Agency
August 2009

AES Galois Counter Mode for the Secure Shell Transport Layer Protocol

Die NSA-Techniker Kevin Igoe und Jerry Salinas waren von solchen Überlegungen offenbar nicht geplagt. Im Frühjahr 2009 wurde von beiden der Entwurf RFC 5647 bei der IETF eingereicht und im August dort durchgewunken. Der Titel: "Galois Counter Mode" für das Secure Shell Layer Protocol".

Der Vortrag Saarinens (http://fse2012.inria.fr/SLIDES/36.pdf) auf der FSE-Konferenz 2009 und der RFC 5647 der IETF (https://tools.ietf.org/html/rfc5647)

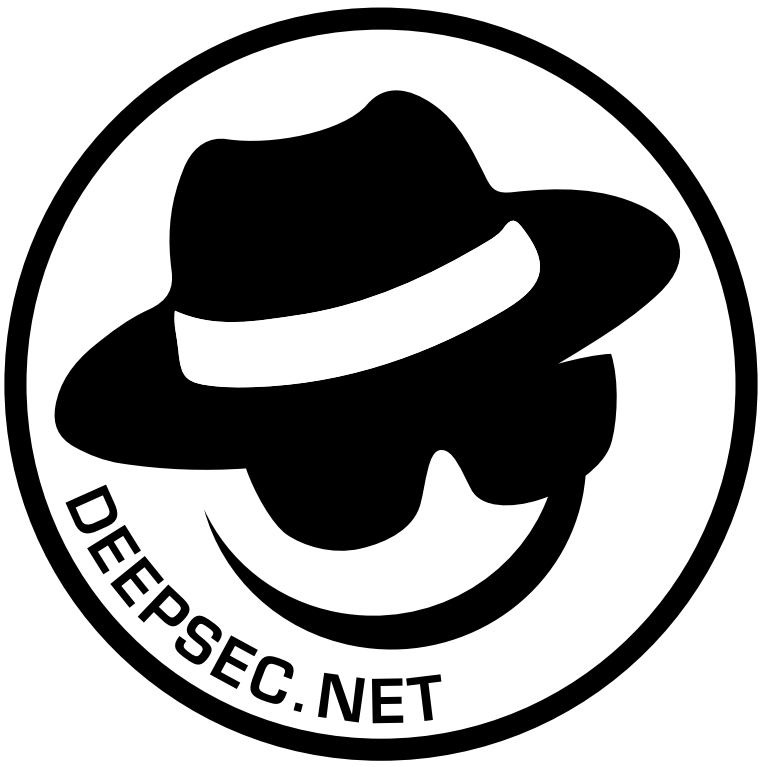
Das Bombardierkäfer-Prinzip

Niels Ferguson wiederum war einer der beiden Microsoft-Spezialisten, die bereits 2007 vor dem anrüchigen NSA-Zufallszahlengenerator "Dual EC DRBG" gewarnt hatten. Eine wirklich verheerende Wirkung entfaltete der erst in Kombination mit der Erweiterung "Extended Random" von 2008. Der Wiener Sicherheitsexperte Michael Kafka nennt dies das "Bombardierkäfer-Prinzip".

Der Bombardierkäfer in der Wikipedia (http://de.wikipedia.org/wiki/Bombardierk%C3%A4fer)

Der Abwehrmechanismus dieser Laufkäferart besteht darin, zwei jeweils für sich gesehen harmlose Flüssigkeiten getrennt im Körper vorzuhalten. Wenn sie jedoch vermischt und ausgespritzt werden, erhitzt sich diese Mischung plötzlich auf etwa 100 Grad wobei sie obendrein noch stark ätzend wirkt.

press releases 2014



http://www.pressetext.com/news/20141103007

Sicherheitskonferenz DeepSec legt Fokus auf Kommunikation und Wissen
Moderne Netzwerke lassen sich nur mit Information verteidigen

Datum: 03.11.2014

Autor: René Pfeiffer

Wien (pts007/03.11.2014/08:15) -Wie kann man sich eine internationale IT-Sicherheitskonferenz vorstellen? "Die DeepSec funktioniert wie eine große Börse, auf der Lösungen und Abhilfe für brennende Sicherheitsprobleme diskutiert und ausgetauscht werden", so René Pfeiffer, Sicherheitsexperte und einer der Organisatoren der Konferenz. "Alles dreht sich um Informationen und Informationstechnologie: Man erhält kompetente Antworten von Experten, gepaart mit Demonstrationen von Schwachstellen, auf die Unternehmen reagieren müssen."

Gedankenaustausch und Aufklärungsarbeit

Bereits zum achten Mal versammelt die internationale Sicherheitskonferenz DeepSec (https://deepsec.net) vom 18. bis 21. November 2014 in Wien die Weltelite aus den Bereich der IT-Security. Die Konferenz versteht sich als neutrale Plattform die Hacker-Community, IT-/Security Unternehmen, Behördenvertreter sowie Forscher in Vorträgen und Workshops zum Gedanken- und Erfahrungsaustausch zusammenbringt.

Die Highlights des Programms thematisieren Hintertüren in Serverhardware, Schwachstellen in kryptographischen Anwendungen, Schwächen im Internetprotokoll der nächsten Generation (IPv6), Aufspüren von Schadsoftware und neue Wege vernetzte Systeme zu kompromittieren. Teile der Inhalte haben ihre Premiere zur DeepSec und wurden bisher noch nicht öffentlich diskutiert.

Sicherheit ist vielen ein Begriff, ganz besonders wenn es um Computer und Netzwerke geht. Leider wissen zuwenig Unternehmen was ihnen in der Wildnis "da draußen" wirklich passieren kann. Die internationale DeepSec Konferenz möchte diese Lücke schließen und Experten und Nutzer zusammenbringen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind: "Vielen geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Erst dann können sie geschlossen werden", erklärt René Pfeiffer.

Informationen aus erster Hand

Vor der Konferenz finden zweitägige Workshops statt, in denen Trainer mit den Teilnehmern ausgewählte Inhalte durchgehen. Die Trainings sind nicht nur passive Vorlesungstage sondern Unterricht zum Anfassen und Ausprobieren. Bedrohungen sind schließlich keine Theorie. Alle Teilnehmer lernen persönlich betreut an Beispiele aus der realen Welt. An den zwei darauf folgenden Tagen findet die eigentliche Konferenz statt. Über 30 Vorträgen zeigen aktuellen Bedrohungen im Bereich der Informationstechnologie und darüber hinaus. Man hat damit die einmalige Gelegenheit aus erster Hand zu erfahren wie erfahrene Experten mit Risiken umgehen und welche Gegenmaßnah-

Contact

René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390

DeepSec GmbH

c/o Mr. René Pfeiffer

Bräuhausgasse 32

1050 Vienna, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635