



Insecurity? It's just a matter of Time

Alexey Kachalin
(Advanced Monitoring)





Me.About

- Computer science & math education, network/analysis (av/ids) software design
- Head of security research company
 - Taking care of customers
 - Set goals/dig into problems with the team
- Found myself being “interpreter” from geek to human (business) and back
- Seeking for efficient ways to prove value of security to stakeholders

Thanks to my team and all who helped with reallife stories!



•

Meeting Minutes



- Introducing our services, or
- Presenting report
 - We saw our DB could be leaked - but that is not damaging our business, right?



- All the way IT/CSO solving problems with purchase of Security System



- Let's talk
 - Numbers
 - Time
 - Controls and business processes

- Образец текста
 - Второй уровень
 - Третий уровень
 - Четвертый уровень
 - Пятый уровень
- Update and AV!!!
- ©FX





Back story of this talk:



Vuln/days

Vendor	Vulns in 7 months 2012 jan-jul	Days to fix
Apple	17	190
IBM	12	185
Microsoft	9	129
Mozilla	4	88
HP	12	218
Novell	5	146
Symantec	3	172
Oracle	12	90

Total: **128**

Days : **177**

Days to fix: **158**

* Patch lag is not included

**0-day time is not included

Back story of this talk 2.

Meeting notes



- First meeting on Project
 - IT security goals
 - IT security - rough reality
 - Security Baseline, goals
 - Documented IT system state
 - Known state - interviews
 - Real - ptest etc.
- Second meeting – few months later
 - Goals got bigger
 - We want stuff we wanted
 - ... and we want more ...
 - IT security got worse



e.g. Documents are not really up to date



- Got progress

- 2011 Federal Law on Personal Data Processing #152 changed
- 2012 more changes of #152 – penalties for violators

The answer is
~~42~~ 152

- SomeOrganization.ru – got worried

- 10 offices in the city, over 1000 PCs, own servers
- Pretty large stack of technology: DBs, VoIP, Custom SW for processing

Last consistent documentation on IT – **1987**





What's happening over time with security of IT System?

- Externally

- New threats - i.e. phishing schemes
- New vulnerabilities - component properties change without any action or observable effect

- Internally

- System growth
- Business requirements drive the change
- ... with sudden changes in changes
- Staff changes - fired/hired/assigned/reassigned/moved
- ... and doing some work
- ... and not only work - unwanted HW/SW, browsing
- Components broke, upgraded/updated, removed





Problem

- Subject: complex system security
- If everybody doing everything **right** why security issues occure
 - How and when security issues and causes for them occurs
 - Why security of IT system getting worse with time and to what extent



- Approach

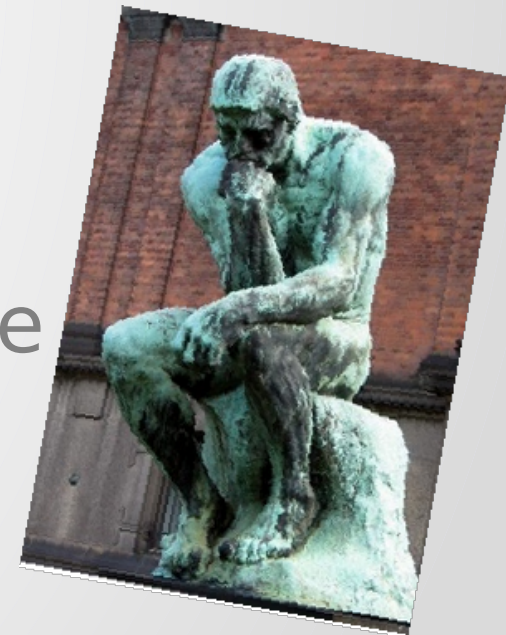
- Examples to extend and prove model
- Thinking model to avoid chaos





Problem description – assumptions and limitations

- Some entirely wrong situations proved to exist by practice due to:
 - Physical laws, government regulation
 - Business environment – fast changes, fast forward to goal skipping required steps, time to market race, growth and reorganization etc.
 - Human nature
- Those are hardly changeable, but could be analyzed to figure what causes them
-

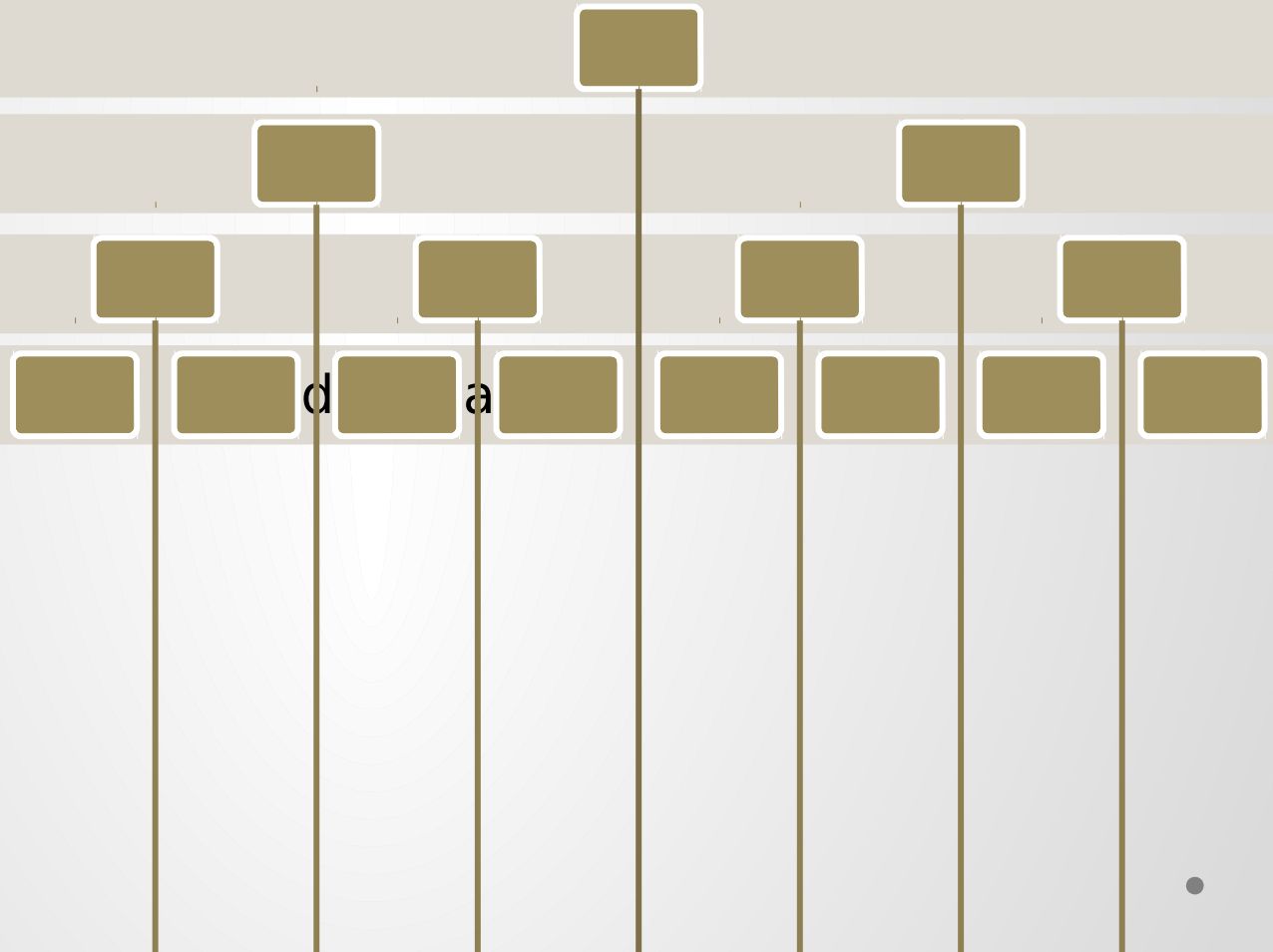




Complex systems are complicated



Global



Comfort Time frames hypothesis



Years

Months

Days

Minutes

Countries
algorithms

Companies
architecture

Departments
product

Groups
release version

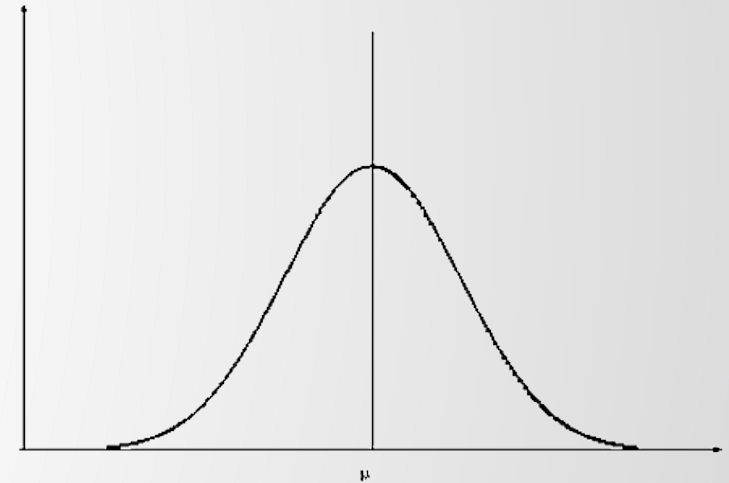
Individuals
installed copy





Extremum cases

- Timing attacks – cryptography, blind SQLi
- Event frequency - not enough randomness in clouds
 - Time as a source of randomization fails
 - Predictable user behavior
- Microsoft certificates
 - Valid for 10 years
 - Enough time to build CA infrastructure dependant on certificates
 - Enough time to write and publish a paper and POC/Virus developed compromising certificates





Forgotten actions



- OnNew
 - Check existing
- OnDispose
- OnTime
 - E-mail binded to web-service registration got deleted due to inactivity
- Lost “Temporary” in “Temporary Solution”
 - Temporary Internet access (3g-modems + ext IP) temporary whitelisted on Big Corporate Firewall, temporary given to ... save somebody’s life probably
 - Found during external scan In other company nearby
- Rare activities vs Frequent activities
 - Automation should have limited use
- Action integrity
 - AD-User deleted, “Contact” - not



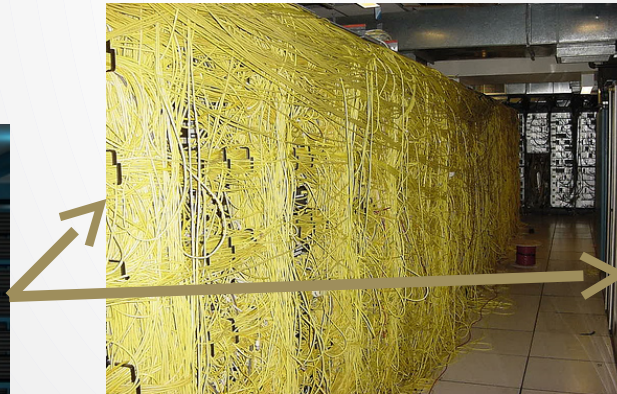
Abandoned stuff

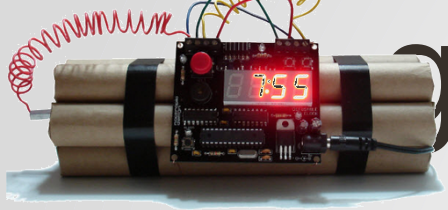
- Physically lost vs. Lost&Updated
 - Spreadsheet@Internet website updated by some temporary script with passwords
- Data
 - Backups
 - Admin scripts with passwords hardcoded
- Accounts
 - Read corporate mail 2 years after quitting company
 - Clouds: now you can just lose IT. All of IT
- Services
 - Abandoned Site
 - Abandoned Site CMS Installation Process. With DB creds
 - Abandoned company CRM. But readonly. But from Internets
 - Alternate AD
 - Abandoned Server – last updated 2005, walled-in old server room
- Corporate File Dump



Changes?

- Incremental system change
 - Scalability has its limits
 - Exceeding limits causes trouble
- Are changes tracked?
 - Offline actions as well?
- Any plan on rolling back changes?
- Definition of Done?





g. Proxy Mi-mi-mi-gration



- New shiny Proxy planned to be put into system next month
- Maintenance of old proxy ceases few months before - it's going to be switched off anyway so who cares
- Discovered while swithing: not ready to get rid of Old Proxy ... yet
 - "some critical service" could become unavailable
 - Both proxies are operating
- Internet content policies were enforced on New Proxy
 - But if You really need something forbidden - could voluntarily use old Proxy
- Situation left this way for a year
 - Get new proxy running and enforce policy - DONE



Time for Human vulnerability



- Stupidity – situation doesn't improve over time
- Laziness => Delays => Never happens
 - “Will do for system X next time when I fix Y”
 - Who needs this checklists, documentation, etc. anyway?
- Impatience
 - Captcha is annoying => Browser bar that removes captcha
 - Time for security operation optimizations
- Chaotic actions
 - Mixing private (own) and job activities=> Social Engineer's heaven
 - Hiring from social network accounts with employer e-mail
 - Mentioning this e-mail in services with dates and details
 - Mentioning private cell #



e.g. it get's boring instantly



- Telephony>AutoPay>E-mail notification
- Admin got bored with “You have put \$ on Your Phone Account via AutoPay”
- Automation!
- E-mail notifications are moved from Inbox to Inbox/IT/Services/ForAccountants/PaymentsForTelephony
- Friday night bad things started (admin observed Inbox on weekend)
- Discovered next week
-



Staff dynamics over time



- Accounting issues

- Details in procedures are important
- OnHire = OnSwitch position?
- OnLeave = OnFire?
- OnSwitchPosition = ?
- Roles
- Who's doing X OnAbsence of responsible?
- ... and how responsible person will know later the status?

- Pissed off staff

- Fired Admin: tear off all the tags from patches/ports servers etc.
- Programmer adds time/logic bombs
- DTMF parsing as stored procedure in CCM DB
- ... removes infrequent used fuzzy-logic script/hack
- Printer encoding twick checking OS type and version



Exceptions better be exceptionally traced



- VIP got special set of rules in Firewall (allow*)
 - Over time got more devices, exception for them
 - VIP moves away – some rules got revoked, some not
 - Person and devices leave, configs don't
 - ... comments “WTF is this rule for?” in ACL
 - Few months later company get public wifi hotspots

... welcome: public WiFi router with allow*



Only rule #34
Has No exceptions

Backups – go back in time!



- Essential security mechanism. Many ways to do it wrong!
- Backup security
 - on USB Harddrive
 - With network sharing on
 - Harddrive contained previous backups
- Backup frequency
 - Automated backups – ok, checked consistency and backup cleaning is made
 - Regular made by hand – lags, errors
 - Rare backups
- Backup corrupted at unknown point
- Backup stolen
 - Thieves Steal Backup Tapes with Billing Records of 2.2 Million Patients



bring some time issues. For sure!



- Company.ru

Vladivostok GMT+10
Krasnoyarsk GMT+7
Moscow GMT+3

- Finance day closing operations

- Moscow and other regions. Is made with no users logged in
- Started closing DB in Moscow at 22-00 Msk
- Got some problems, took longer then ussialy
- Then Krasnoyarsk
- At 4-00 Msk started processing of Vladivostok
- Kick hung users, started scripts
- ...but they were not that hung (11-00 Vlad. Time)





Uncontrolled afterlife

- After being used hardware is ~~disposed~~ sold or thrown away
- Laptops
 - Afghanistan military secrets sold for £18.87 on eBay after army officer dumped laptop in a skip
- ATMs
 - Used ATMs with CC logs
 - ATM-hardware for rent?



АРЕНДА БАНКОМАТА

Компания предлагает в аренду: Банкоматы



Micromanagement from macrolevel



Good cause - Zapret-info.gov.ru - report sites for CP, drugs, suicide provoking content. Active since 2012-11-01 by federal law

- 3 governmental institution would make a decision on submission to ban a site
 - appeal could be made in court
- First day
 - Over 3000 submittions
 - Over 1100 need to be analysed
 - Decision on 6 sites
- First month
 - Microsoft MSDN temporary unavailable
 - Banned YouTube (mistake)
 - Captcha cracked

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)

ЕДИНЫЙ РЕЕСТР
доменных имен, указателей страниц сайтов в сети "Интернет"
и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет",
содержащие информацию, распространение которой
в Российской Федерации запрещено


[Просмотр реестра](#) | [Прием сообщений](#) | [Провайдерам хостинга](#) | [Операторам связи](#)

Через форму, опубликованную ниже, вы можете получить данные о нахождении в Едином реестре доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

Искомый ресурс:

1.2.3.4 (для IP адреса)
domain-xxx.ru (для доменного имени)
http://www.domain-xxx.ru/news/?id=2 (для URL адреса)

Защитный код:



• [Перечень информации, предоставляемой из Единого реестра](#)



Software Development

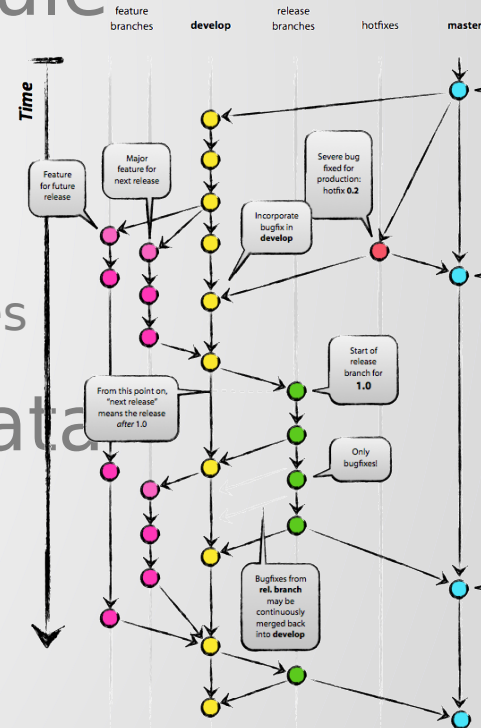
- Industry-grade process?
 - What's methodology of development of every GPL library your product depend on
- Lifecycle
 - Design
 - Implementation
 - Testing
 - Release
 - Support
 - End of life





e.g. parallel dev

- 3 teams are working in branches of version control system
- Team1: added functionality module
 - Evolved addresses/logins/passwords
- Team2: refactored logging
 - Convenient logging for all intro-module exchanges
- Team3: worked on networking data exchange
 - Security enhancement - network logging!



e.g. dev us more CYBER sec!



- Network device firmware password auth -ok!
- Firmware is running on *nix, ssh access - secure!
- Password from firmware on setup is put to passwd - sweet, no default-pass backdoor!
- In next release: Token auth for firmware
- Most secure token only - vulnerable to default password





Security Solutions

- Scanners
 - Infinite time to complete scan (system changes too fast)
- Monitors
 - Inbound buffer issues
 - Limited time-frame of observation
- Both
 - Avoid being analyzed with given time/resources limitations
 - Detect/avoid race
 - Knowledge base outdate/being cut to optimise performance





Outro: Security&Time

- Events got duration
 - Expect something going on behind your back
- All events which make impact could not be observed
 - And never will be with event correlation engine of any complexity
- Besides event itself consider frequency of events
 - Rare events, regular, frequent – should be dealt in different way

Comfort Time frames hypothesis



Years

Months

Days

Minutes

Countries
algorithms

Companies
architecture

Departments
product

Groups
release version

Individuals
installed copy



Bonus track: meeting cheatsheet



- Is there a link of controls from highest to lowest level?
 - Policy =>Requirements=>Instructions=>Automation means
- Are this controls appropriate to time
 - Rare events governed
 - Frequent events handling automated
 - Extreme cases overthought
 - Events/actions with significant duration got interruptions handled
 - Periodical checks. System Consistency?!
- Are there controls over controls?
 - Controls sanity check
 - Changes of controls
- Tracking of changes and clear definition of done





Thanks for Your time!

Few minutes for questions



@kchIn

Advanced Monitoring





Insecurity? It's just a matter of Time

Alexey Kachalin
(Advanced Monitoring)





Me.About

- Computer science & math education, network/analysis (av/ids) software design
- Head of security research company
 - Taking care of customers
 - Set goals/dig into problems with the team
- Found myself being “interpreter” from geek to human (business) and back
- Seeking for efficient ways to prove value of security to stakeholders

Thanks to my team and all who helped with reallife stories!



•

Meeting Minutes



- Introducing our services, or
- Presenting report
 - We saw our DB could be leaked - but that is not damaging business, right?



- All the way IT/CSO solving problems with purchase of Security System



- Let's talk
 - Numbers
 - Time
 - Controls and business processes

- Образец
◦ Второй уровень
◦ Третий уровень
◦ Четвертый
Update and AV!!!
©FX





Back story of this talk:

Vuln/days



Vendor	Vulns in 7 months 2012 jan-jul	Days to fix
Apple	17	190
IBM	12	185
Microsoft	9	129
Mozilla	4	88
HP	12	218
Novell	5	146
Symantec	3	172
Oracle	12	90

Total: **128**

Days : **177**

Days to fix: **158**

* Patch lag is not included

**0-day time is not included

Back story of this talk 2

Meeting notes



- First meeting on Project
 - IT security goals
 - IT security - rough reality
 - Security Baseline, goals
 - Documented IT system state
 - Known state - interviews
 - Real - ptest etc.
- Second meeting - few months later
 - Goals got bigger
 - We want stuff we wanted
 - ... and we want more ...
 - IT security got worse



e.g. Documents are not really up to date



- Got progress

- 2011 Federal Law on Personal Data Processing #152 changed
- 2012 more changes of #152 - penalties for violators

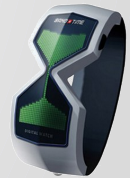
The answer is
~~42~~ 152

- SomeOrganization.ru - got worried

- 10 offices in the city, over 1000 PCs, own servers
- Pretty large stack of technology: DBs, VoIP, Custom SW for processing



Last consistent documentation on IT - **1987**



What's happening over time with security of IT System?



- Externally

- New threats - i.e. phishing schemes
- New vulnerabilities - component properties change without any action or observable effect

- Internally

- System growth
- Business requirements drive the change
- ... with sudden changes in changes
- Staff changes - fired/hired/assigned/reassigned/moved
- ... and doing some work
- ... and not only work - unwanted HW/SW, browsing
- Components broke, upgraded/updated, removed





Problem

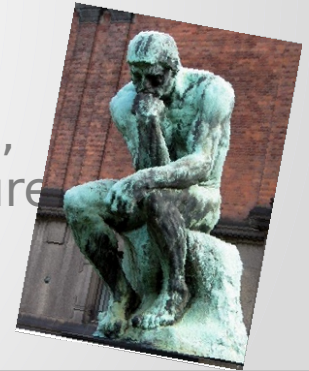
- Subject: complex system security
- If everybody doing everything **right** why security issues occur
 - How and when security issues and causes for them occur
 - Why security of IT system getting worse with time and to what extent
- Approach
 - Examples to extend and prove model
 - Thinking model to avoid chaos

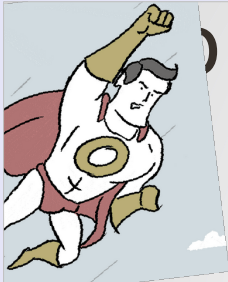


Problem description – assumptions and limitations



- Some entirely wrong situations proved to exist by practice due to:
 - Physical laws, government regulation
 - Business environment – fast changes, fast forward to goal skipping required steps, time to market race, growth and reorganization etc.
 - Human nature
- Those are hardly changeable, but could be analyzed to figure out what causes them

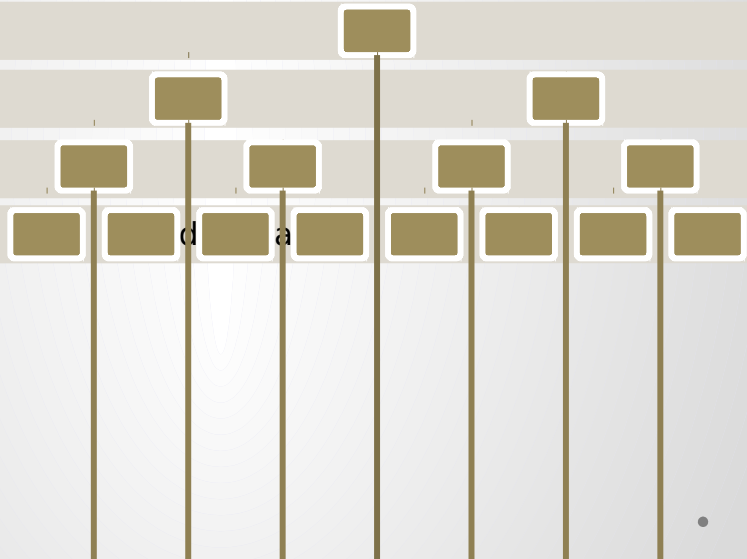




Complex systems are complicated



Global



•

•

Comfort Time frames hypothesis



Years Months Days Minutes

Countries
alogrithm

Companies
architecture

Departments
prouct

Groups
release version

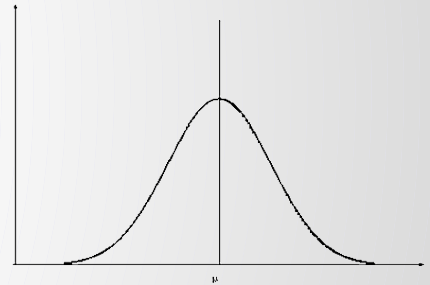
Individuals
installed copy





Extremum cases

- Timing attacks – cryptography, blindn SQLi
- Event frequency - not enough randomness in clouds
 - Time as a source of randomization fails
 - Predictible user behavior
- Microsoft certificates
 - Valid for 10 years
 - Enough time to build CA infrastructure dependad on certificates
 - Enough time to write and publish a paper and POC/Virus developed compromising certificates



•

•



Forgotten actions



- OnNew
 - Check existing
- OnDispose
- OnTime
 - E-mail binded to web-service registration got deleted due to inactivity
- Lost “Temporary” in “Temporary Solution”
 - Temporary Internet access (3g-modems + ext IP) temporary whitelisted on Big Corporate Firewall, temporary given to ... save somebody's life probably
 - Found during external scan In other company nearby
- Rare activities vs Frequent activities
 - Automation should have limited use
- Action integrity
 - AD-User deleted, “Contact” - not





Abandoned stuff

- Physically lost vs. Lost&Updated
 - Spreadsheet@Internet website updated by some temporary script with passwords
- Data
 - Backups
 - Admin scripts with passwords hardcoded
- Accounts
 - Read corporate mail 2 years after quitting company
 - Clouds: now you can just lose IT. All of IT
- Services
 - Abandoned Site
 - Abandoned Site CMS Installation Process. With DB creds
 - Abandoned company CRM. But readonly. But from Internets
 - Alternate AD
 - Abandoned Server - last updated 2005, walled-in old server room
- Corporate File Dump



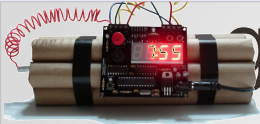


Changes?

- Incremental system change
 - Scalability has its limits
 - Exceeding limits causes trouble
- Are changes tracked?
 - Offline actions as well?
- Any plan on rolling back changes?
- Definition of Done?



•



9. Proxy Mi-mi-mi-gration



- New shiny Proxy planned to be put into system next month
- Maintenance of old proxy ceases few months before - it's going to be switched off anyway so who cares
- Discovered while swithing: not ready to get rid of Old Proxy ... yet
 - "some critical service" could become unavailable
 - Both proxies are operating
- Internet content policies were enforced on New Proxy
 - But if You really need something forbidden - could voluntarily use old Proxy
- Situation left this way for a year
 - Get new proxy running and enforce policy - DONE





Time for Human vulnerability



- Stupidity - situation doesn't improve over time
- Laziness => Delays => Never happens
 - "Will do for system X next time when I fix Y"
 - Who needs this checklists, documentation, etc. anyway?
- Impatience
 - Captcha is annoying => Browser bar that removes captcha
 - Time for security operation optimizations
- Chaotic actions
 - Mixing private (own) and job activities=> Social Engineer's heaven
 - Hiring from social network accounts with employer e-mail
 - Mentioning this e-mail in services with dates and details
 - Mentioning private cell #



e.g. it get's boring instantly



- Telephony>AutoPay>E-mail notification
- Admin got bored with “You have put \$ on Your Phone Account via AutoPay”
- Automation!
- E-mail notifications are moved from Inbox to Inbox/IT/Services/ForAccountants/PaymentsForTelephony
- Friday night bad things started (admin observed Inbox on weekend)
- Discovered next week



Staff dynamics over time



- Accounting issues

- Details in procedures are important
- OnHire = OnSwitch position?
- OnLeave = OnFire?
- OnSwitchPosition = ?
- Roles
- Who's doing X OnAbsence of responsible?
- ... and how responsible person will know later the status?



- Pissed off staff

- Fired Admin: tear off all the tags from patches/ports servers etc.
- Programmer adds time/logic bombs
- DTMF parsing as stored procedure in CCM DB
- ... removes infrequent used fuzzy-logic script/hack
- Printer encoding twick checking OS type and version



Exceptions better be exceptionally traced



- VIP got special set of rules in Firewall (allow*)
 - Over time got more devices, exception for them
 - VIP moves away - some rules got revoked, some not
 - Person and devices leave, configs don't
 - ... comments "WTF is this rule for?" in ACL
 - Few months later company get public wifi hotspots



welcome: public WiFi router with allow*

Only rule **#34**
Has No exceptions

Backups – go back in time!



- Essential security mechanism. Many ways to do it wrong!
- Backup security
 - on USB Harddrive
 - With network sharing on
 - Harddrive contained previous backups
- Backup frequency
 - Automated backups – ok, checked consistency and backup cleaning is made
 - Regular made by hand – lags, errors
 - Rare backups
- Backup corrupted at unknown point
- Backup stolen
 - Thieves Steal Backup Tapes with Billing Records of 2.2 Million Patients



bring some time issues. For sure!



- Company.ru

Vladivostok GMT+10
Krasnoyarsk GMT+7
Moscow GMT+3



- Finance day closing operations

- Moscow and other regions. Is made with no users logged in
- Started closing DB in Moscow at 22:00 Msk
- Got some problems, took longer than usual
- Then Krasnoyarsk
- At 4:00 Msk started processing of Vladivostok
- Kick hung users, started scripts
- ...but they were not that hung (11:00 Vlad. Time)





Micromanagement from macrolevel



Good cause - Zapret-info.gov.ru - report sites for CP, drugs, suicide provoking content. Active since 2012-11-01 by federal law

- 3 governmental institution would make a decision on submission to ban a site
 - appeal could be made in court
- First day
 - Over 3000 subinitous
 - Over 1100 need to be analysed
 - Decision on 6 sites
- First month
 - Microsoft MSDN temporary unavailabe
 - Banned YouTube (mistake)
 - Captcha cracked

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
(РОССОМНАДЗОР)

ЕДИНЫЙ РЕЕСТР
доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено

[Просмотр реестра](#) | [Приним сообщения](#) | [Провайдерам хостинга](#) | [Операторам связи](#)

Через форму, опубликованную ниже, вы можете получить данные о нахождении в Едином реестре доменного имени, указателя страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено

Искомый ресурс:

1.2.3.4 (для IP-адреса)
domain-xxx.ru (для доменного имени)
http://www.domain-xxx.ru/news/?id=2 (для URL-адреса)

Защитный код:

• [Перечень информации, предоставляемой из Единого реестра](#)



Software Development

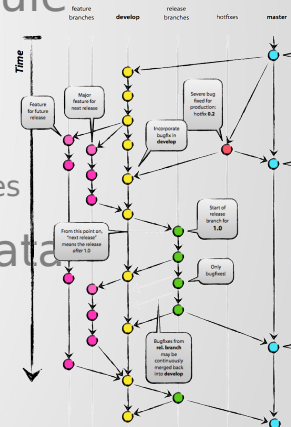
- Industry-grade process?
 - What's methodology of development of every GPL library your product depend on
- Lifecycle
 - Design
 - Implementation
 - Testing
 - Release
 - Support
 - End of life





e.g. parallel dev

- 3 teams are working in branches of version control system
- Team1: added functionality module
 - Evolved addresses/logins/passwords
- Team2: refactored logging
 - Convenient logging for all intro-module exchanges
- Team3: worked on networking data exchange
 - Security enhancement - network logging!



e.g. dev us more CYBER sec!



- Network device firmware password auth -ok!
- Firmware is running on *nix, ssh access - secure!
- Password from firmware on setup is put to passwd - sweet, no default-pass backdoor!
- In next release: Token auth for firmware
- Most secure token only - vulnerable to default password





Security Solutions

- Scanners
 - Infinite time to complete scan (system changes too fast)
- Monitors
 - Inbound buffer issues
 - Limited time-frame of observation
- Both
 - Avoid being analyzed with given time/resources limitations
 - Detect/avoid race
 - Knowledge base outdate/being cut to optimise performance





Outro: Security&Time

- Events got duration
 - Expect something going on behind your back
- All events which make impact could not be observed
 - And never will be with event correlation engine of any complexity
- Besides event itself consider frequency of events
 - Rare events, regular, frequent - should be dealt in different way

•

•

Comfort Time frames hypothesis



Years Months Days Minutes

Countries
alogrithm

Companies
architecture

Departments
prouct

Groups
release version

Individuals
installed copy



Bonus track: meeting cheatsheet



- Is there a link of controls from highest to lowest level?
 - Policy =>Requirements=>Instructions=>Automation means
- Are this controls appropriate to time
 - Rare events governed
 - Frequent events handling automated
 - Extreme cases overthought
 - Events/actions with significant duration got interruptions handled
 - Periodical checks. System Consistency?!
- Are there controls over controls?
 - Controls sanity check
 - Changes of controls
- Tracking of changes and clear definition of done



