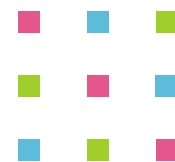
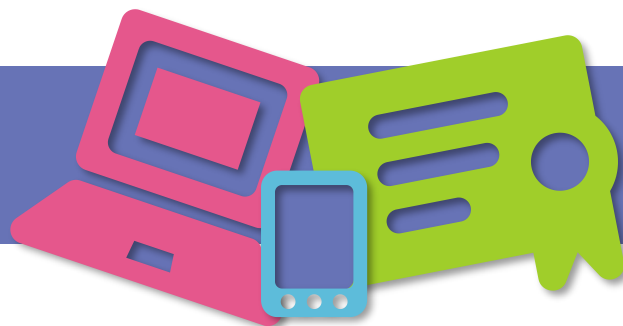


SECURITY 2015



23. ročník konference o bezpečnosti v ICT



Bezpečnost mobilních aplikací v praxi

Lukáš Bláha

AEC, spol. s r.o.



OWASP Mobile Top Ten



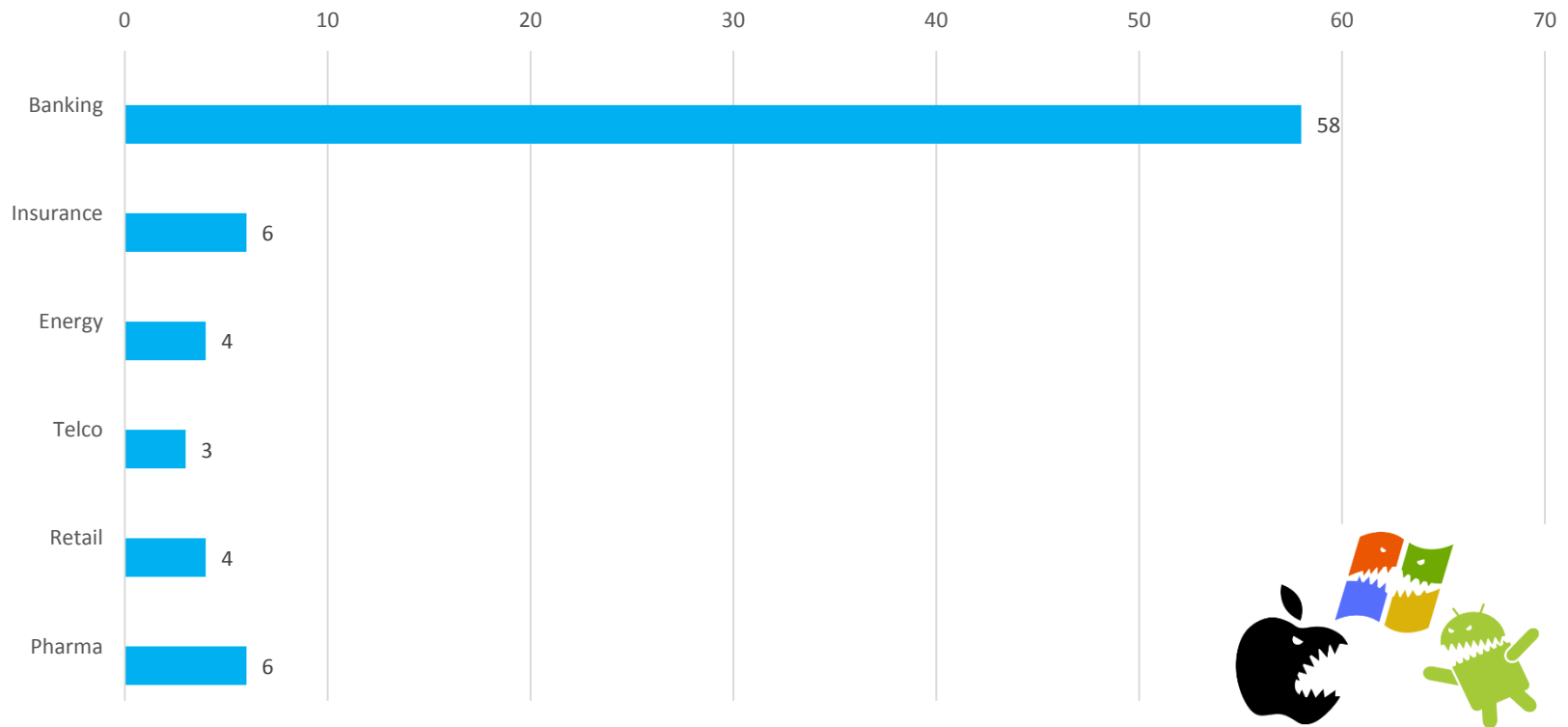


AEC Mobile Top Eleven



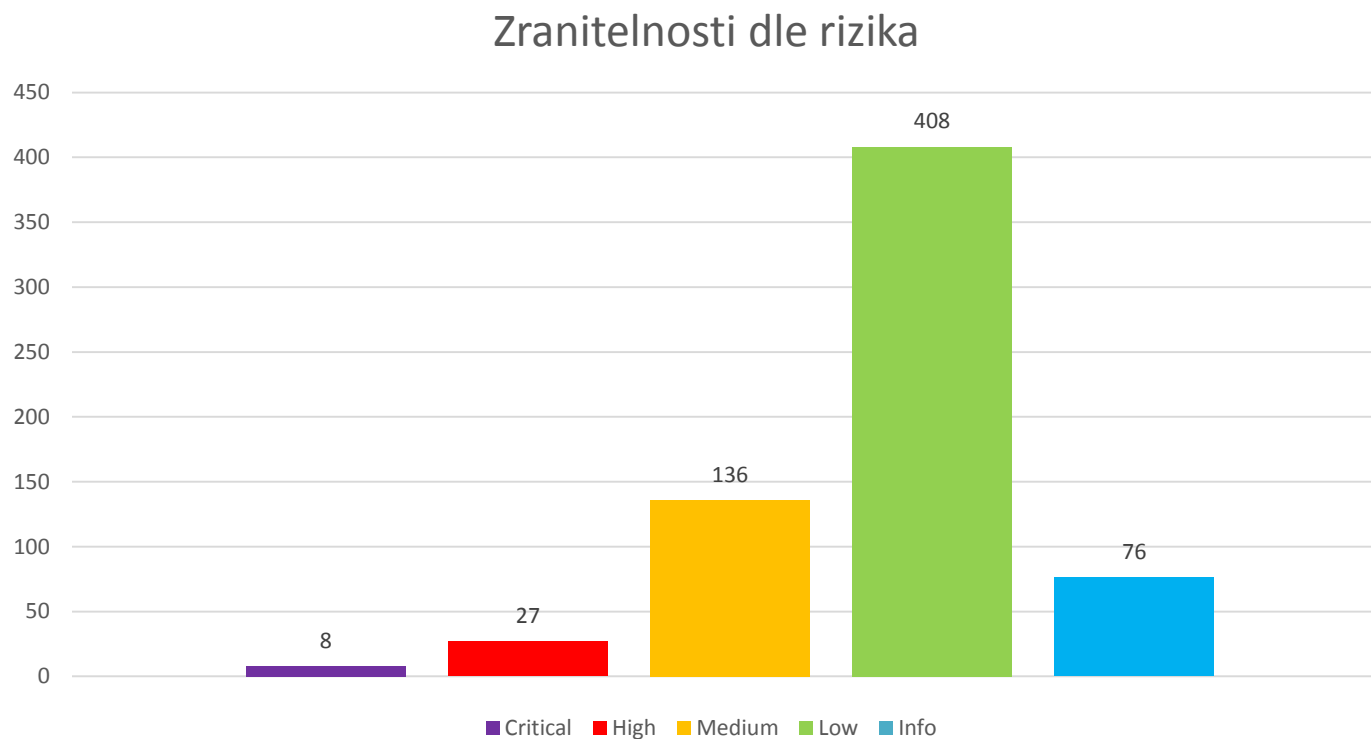
Statistiky za rok 2014

Oblasti testovaných aplikací



Celkový počet aplikací: 81

Statistiky za rok 2014



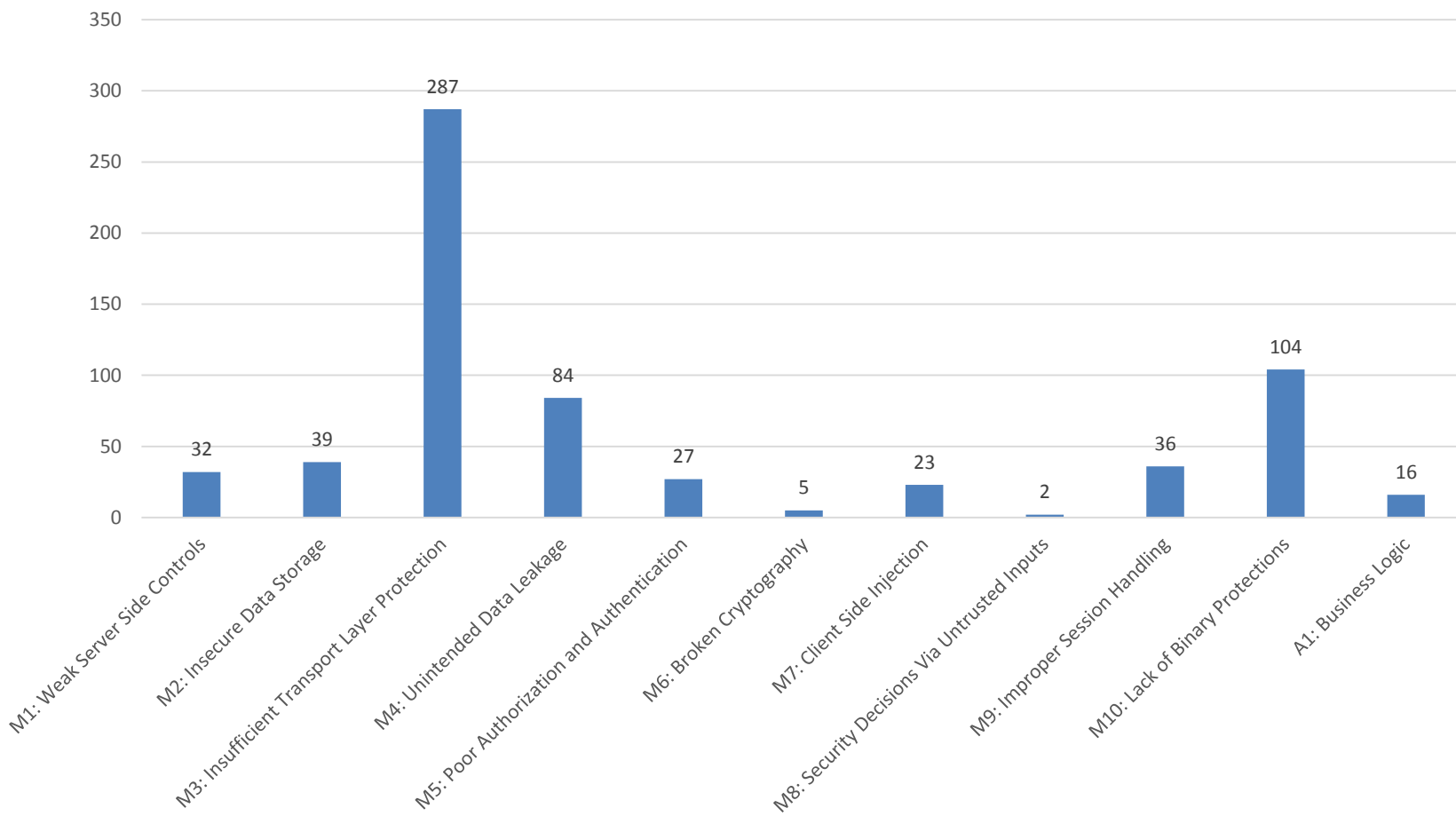
655 zranitelností

81 aplikací

V průměru 8 zranitelností na aplikaci

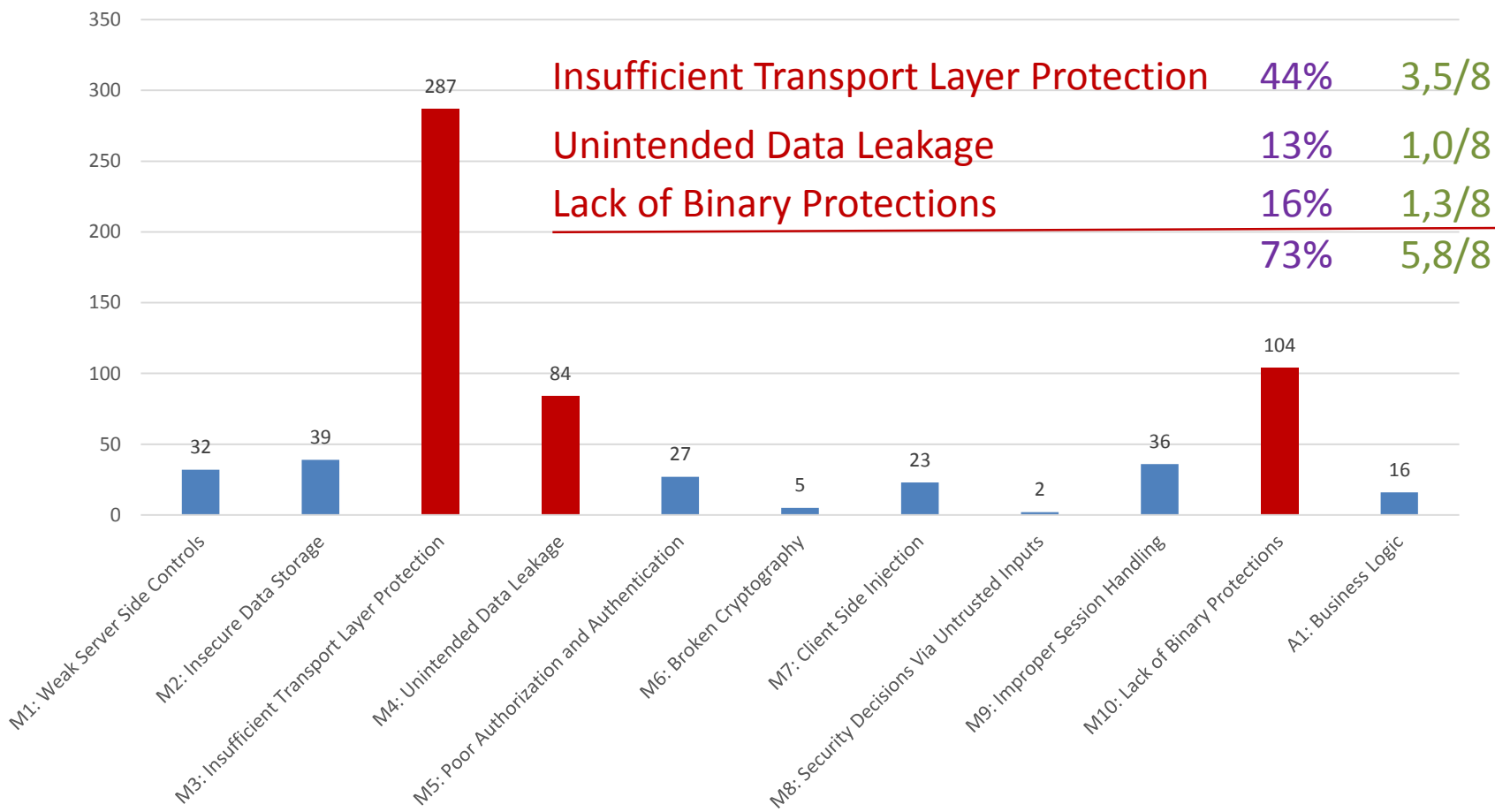
Statistiky za rok 2014

Rozdělení dle kategorií



Statistiky za rok 2014

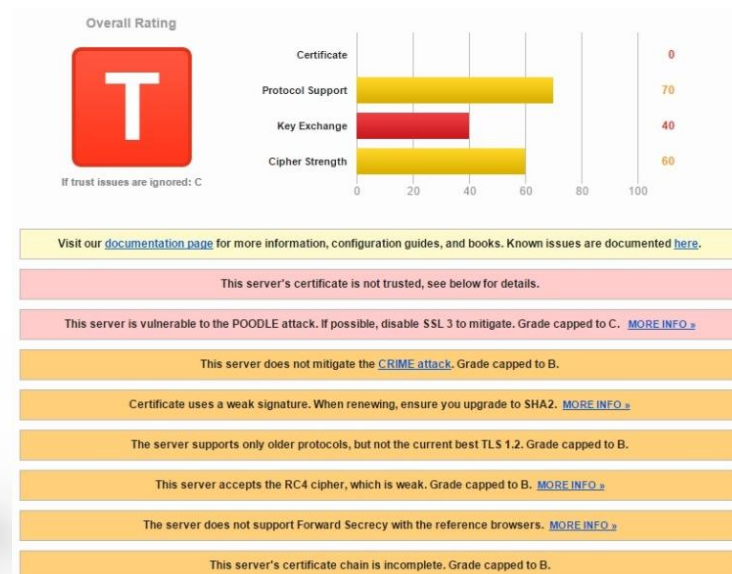
Rozdělení dle kategorií





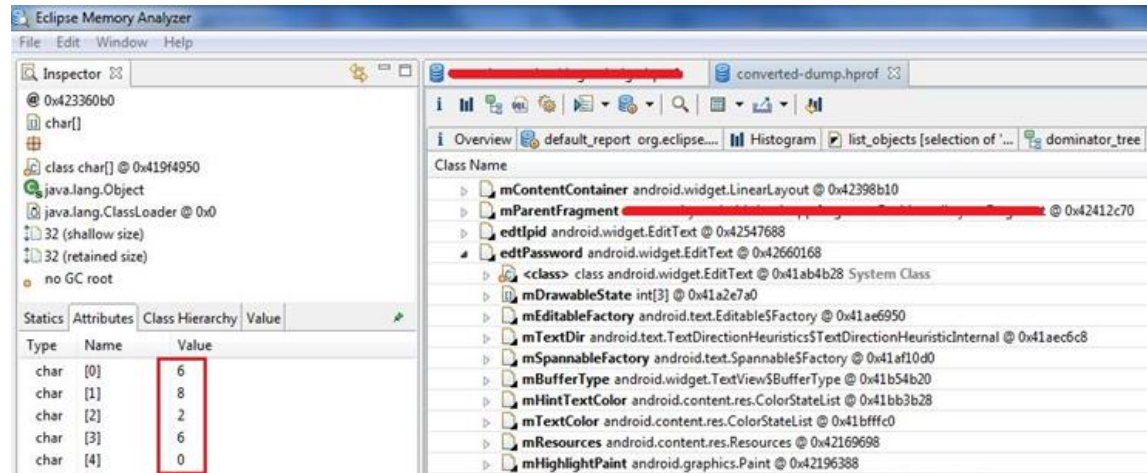
Insufficient Transport Layer Protection

- Špatná konfigurace serveru
 - Únik informací (HTTP Headers, Error Pages, ...)
 - Zastaralé verze technologií
- Špatná konfigurace SSL/TLS
 - Verze, certifikáty, algoritmy, klíče
 - Certificate Pinning
 - SSL Strip (HSTS)
- Injection
 - SQL
 - XML/XXE



Unintended Data Leakage

- Cache
- Logs
- Debug mode
- GPS
- RAM
- Crash logs
- Screenshots
- Keyboard cache
- Copy & Paste



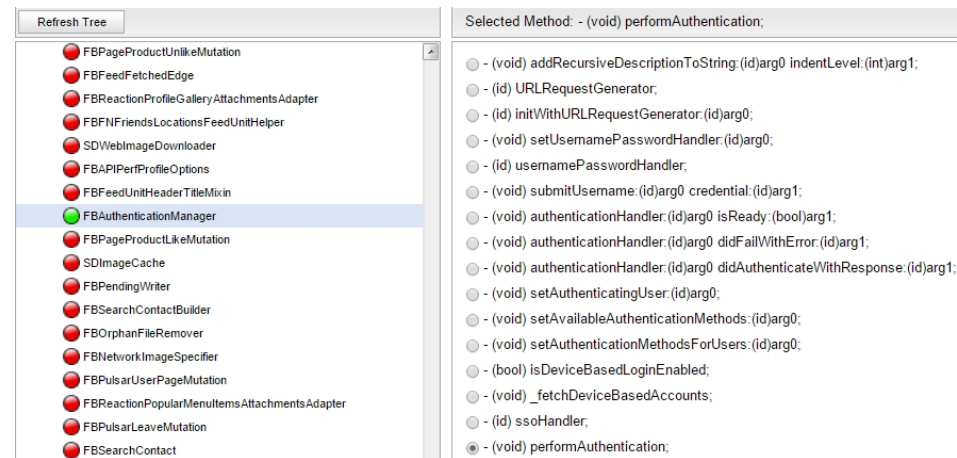
```
D/Login (13029): sessionId: aaUGmqBIy3T5own22tFetEEW5eYaN5KK
D/Login (13029): PetiServer: peti-10.kocquitas.ru
D/Login (13029): PetiServerPort: 80
D/Login (13029): etcgiURL: 
D/Login (13029): BeerDaemonHost: 
D/Login (13029): BeerDaemonPath: 
D/Login (13029): BeerDaemonSecure: true
D/Login (13029): ControlHost: 
D/Login (13029): ControlPath: 
D/ArDaemon (13029): Disconnecting...
D/ArDaemon (13029): Connecting.
```

```
1B0 6A62 6B75 626F 7562 6F75 6E6F 6A6E 6F6A jbkuboubounojno
1C0 686F 756E 6C6A 6E6C 6A6E 6B6A 626B 6A6E houn1jnljnkjbk
1D0 006A 6800 6D6E 006D 6E6B 6A6E 6B6A 626B .jh.mn.mnkjnkj
1E0 6A62 6B75 626B 6A62 6B68 6200 6D6E 006D jbkubkjkbkhb.m
1F0 006D 6E00 6A6E 6B6A 6E6B 6A6E 6B6A 6A62 .mn.jnkjnkjnkj
200 6B6A 626B 6A6E 6B6A 6200 6A6E 006A 6876 kjbkjnkjb.jn.j
210 6876 6868 006A 6A6A 0068 7970 6F6F 0068 hvhh.jjj.
220 7970 6F6F 0063 7A7A 0000 0000 0000 0000 
230 4701 0061 0001 0061 6563 0001 0061 7070 G...aec...app
```

Lack of Binary Protections

- Zdrojové kódy
 - Obfuskace kódu
 - Hardcoded informace
- Aplikační balík
 - Nastavení kompilátoru
 - Citlivé/testovací soubory
- Anti-tamper techniky
 - Debuggers Restricting
 - Trace Checking
 - Binaries Stripping
 - Integrity Checks (checksums, signatures)
- Root/Jailbreak detekce
- Vlastní klávesnice

```
public class EmailSender extends Authenticator
{
    private String mailhost = "██████████";
    private String password = "██████████";
    private Session session;
    private String user = "██████";
}
```





Z čeho chyby nejčastěji plynou?

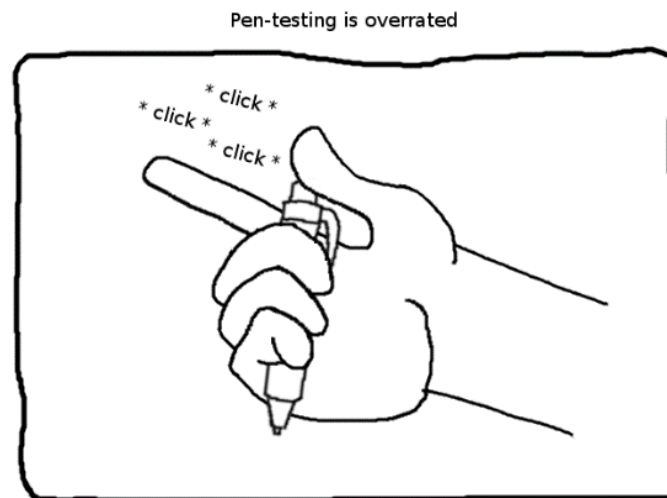
- Rychlost uvedení produktu na trh
- Neznalost bezpečnostních specifik
 - jednotlivých jazyků
 - SDK
 - platforem či nových verzí OS
- Neexistence, špatná kvalita nebo nedodržování metodik pro bezpečný vývoj
- Mylný předpoklad, že mobilní OS nese plnou odpovědnost za bezpečnost
- Outsourcing vývoje – kontrola třetí strany
- Nižší budget pro vývoj/bezpečnost mobilních aplikací
- Využití frameworků, které nedbají na bezpečnost





Jak to tedy vylepšit?

- Zahrnutí bezpečnostních specialistů již do návrhu
- Metodiky pro bezpečný vývoj
 - Vytvoření / aktualizace
 - Vynucování jejich dodržování
- Vzdělávání vývojářů
 - Školení



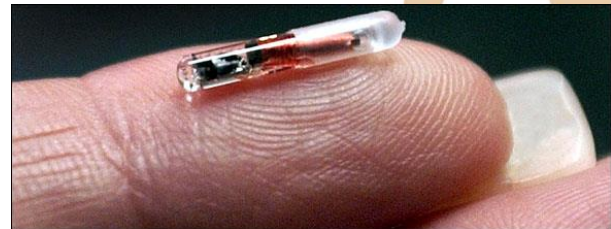
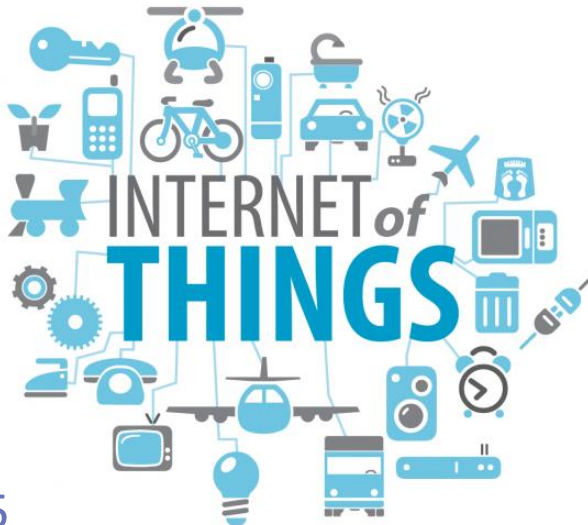
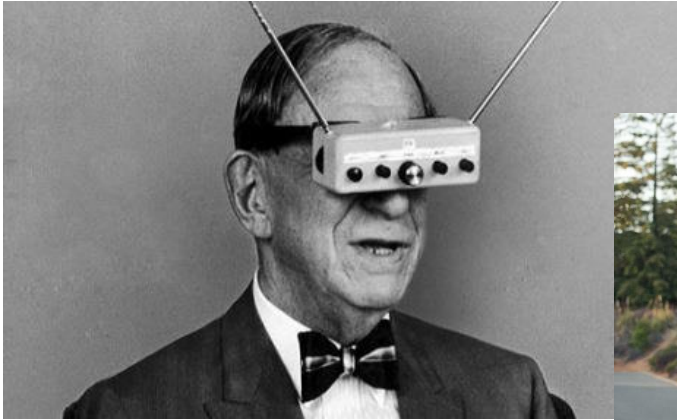
-
- Penetrační testy
 - Quick Scan

v průběhu vývoje?

- Source Code Review



Budoucnost?



18. února 2015

SECURITY 2015



SECURITY 2015



23. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Lukáš Bláha

AEC, spol. s r.o.

lukas.blaha@aec.cz

