Agentúra
Ministerstva školstva, vedy, výskumu a športu SR
pre štrukturálne fondy EÚ

Operačný program
VZDELÁVANIE

Európska únia
Európsky sociálny fond

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

# PRÍPRAVA ŠTÚDIA MATEMATIKY A INFORMATIKY NA FMFI UK V ANGLICKOM JAZYKU

ITMS: 26140230008

DOPYTOVO – ORIENTOVANÝ PROJEKT

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je spolufinancovaný zo zdrojov EÚ

# Security incidents, weaknesses and vulnerabilities

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Security of IT infrastructure (2014/15)

# Content

General discussion

Examples – security failures

- Randomness of cryptographic keys
- Heartbleed
- Timing attacks on comparisons
- Adobe password encryption
- WPS (WiFi Protected Setup)
- Encrypted USB drives
- Hash tables collisions
- Apple “goto” fail

Other incidents

# Introduction

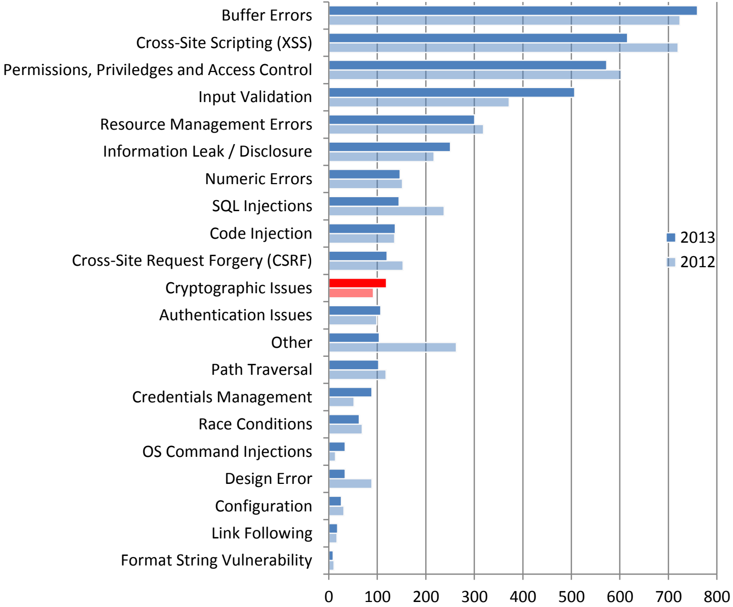
Security incidents and failures

- various causes (or their combination): human factor, criminal activities, technical vulnerabilities etc.
- impact: “nothing” happened, loss of reputation, cost of repair/replacement of data and systems, direct financial loss, bankruptcy etc.

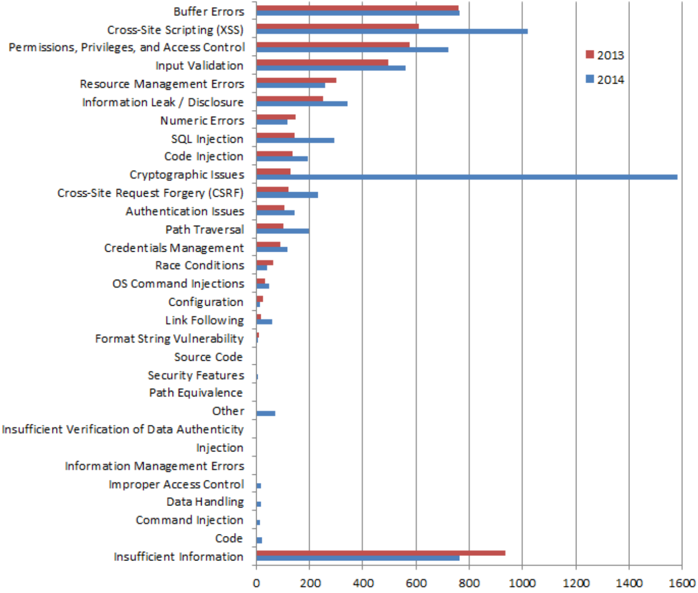
mostly technical failures/vulnerabilities in this lecture

- just examples …reality is worse
- National Vulnerability Database (nvd.nist.gov)
- vulnerabilities published (data collected 15/02/2015):
  5278 (2012), 5174 (2013), 7903 (2014)
- classification (categories, severity etc.)
- “Insufficient information” not shown on the following chart

# NVD – vulnerabilities published in 2012 and 2013



# NVD – vulnerabilities published in 2013 and 2014



# Strange number of “Cryptographic Issues” in 2014

- January – August: 125 vulnerabilities
- September: 674 vulnerabilities
- October: 712 vulnerabilities
- November – December: 22 vulnerabilities

- *The … application for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.*
- (?) nogotofail tool released by Google in November 2014

# Authentication Issues

- CVE-2014-8522: The MySQL database in McAfee Network Data Loss Prevention (NDLP) does not require a password, which makes it easier for remote attackers to obtain access.
- CVE-2014-3053: An undisclosed vulnerability can allow unauthorized users to login to the Local Management Interface of the IBM Security Access Manager for Mobile appliance / IBM Security Access Manager for Web appliance with invalid credentials.
- CVE-2014-0643: RSA NetWitness and RSA Security Analytics each contain a security fix for an authentication bypass vulnerability that could potentially be exploited to compromise the affected system. When PAM for Kerberos is enabled, an attacker can authenticate to the vulnerable system with a valid user name and without specifying a password.

# Buffer overflow

- CVE-2014-0160 The TLS and DTLS implementations in OpenSSL do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, aka the *Heartbleed* bug.
- CVE-2014-4100, CVE-2014-4104, CVE-2014-4105, … Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka “Internet Explorer Memory Corruption Vulnerability”

# Credentials Management & Command Injection

- CVE-2014-0329 ZTE ZXV10 W300 router contains hardcoded credentials that are useable for the telnet service on the device. The username is “admin” and the password is “XXXXairocon” where “XXXX” is the last four characters of the device’s MAC address. The MAC address is obtainable over SNMP with community string public.
- CVE-2014-7208 Gparted does not properly sanitize strings before passing them as parameters to an OS command. Those commands are executed using root privileges.

# Other classifications of vulnerabilities

- Common Weaknesses Enumeration (cwe.mitre.org)
  - Common Attack Pattern Enumeration and Classification (capec.mitre.org)
- Open Web Application Security Project (OWASP, www.owasp.org)
  - primarily for web applications – vulnerabilities, attacks, risks
  - Testing Guide (v4, 2014)
- more detailed classifications, description, examples, additional information

# Real world – surveys and analyses

[1] EY's Global Information Security Survey 2014 (October 2014)

[2] Websense Security Predictions for 2015

[3] DataLossDB Statistics (datalossdb.org)

[4] Verizon 2014 Data Breach Investigations Report (2014)

…etc.

# Data breaches

2014 – the most frequent types of data breaches (DataLossDB.org):

1. Hack – Computer-based intrusion, data may or may not be publicly exposed (37%)
2. Fraud or scam (usually insider-related), social engineering (9%)
3. Web – Data typically available to the general public via search engines, public pages, etc. (7%)
4. Stolen Laptop (generally specified as a laptop in media reports) (5%)
5. Other – Breach type was disclosed but no formal classification (5%)
6. Unknown or unreported breach type (4%)
7. Discovery of documents not disposed properly (4%)
8. Documents either reported or known to have been stolen by a third party (4%)
9. Email communication exposed to unintended third party (4%)

…other causes

# Data breaches – examples (1)

1. University of Veterinary Medicine and Pharmacy in Košice
    - January 2014
    - leaked personal data of 1500 students
    - addresses, ID card numbers, personal identification numbers, …
    - published PDF in Central register of contracts
    - “blacked out” personal data … still there, can be copied (selected)
2. Anthem (USA, managed health care company)
    - December 2014 – January 2015
    - leaked personal data of 80 million customers
    - names, dates of birth, SSN, health care ID numbers, home addresses, email addresses, employment information, income data
    - attack vector unknown/not published (“sophisticated attack”)

# Data breaches – examples (2)

3. Target (USA, retail)
    - December 2013
    - 40 million credit and debit cards information
      + additional 70 million personal information
    - card information
      + names, mailing addresses, phone numbers, email addresses
    - malware installed on POS devices
    - entry using authentication credentials stolen from a heating, ventilation, and air-conditioning subcontractor
4. JPMorgan Chase (USA, banking)
    - discovered in July 2014
    - names, addresses, phone numbers and e-mail addresses of 83 million account holders
    - initial assumption: 0-day web server exploit (?)
    - reality: stolen credentials (password), 2nd factor not enabled on one server
    - 90 servers compromised when detected

# Data breaches – examples (3)

3. Home Depot (USA, retail)
   - breach started in April 2014, undetected for 5 months
   - 56 million customer credit and debit card accounts
     + 53 million customer email addresses
   - malware on self-checkout registers
   - initial step: credentials stolen from a third-party vendor
4. Sony Pictures (USA, entertainment)
   - 100 terabytes of data (?)
   - discovered in November 2014
   - personal information about employees, e-mails, salaries, copies of unreleased Sony films
   - North Korea vs. current/former employees (?)
   - the White House reacts

# …and finally – stealing money

- Kaspersky Lab published their findings (February 2015)
- Carbanak (malware)
- more than 100 banks in 30 countries (Russia, Japan, USA, …)
- more than 300 million USD stolen
- initial vector: spear phishing attacks

# Factors of risk exposure

- EY's Global Information Security Survey 2014
- global survey, 1825 organizations
- Top 2 vulnerabilities:
  1. Outdated information security controls or architecture
  2. Careless or unaware employees
- Top 2 threats:
  1. Cyber attacks to disrupt or deface the organization
  2. Cyber attacks to steal financial information (credit card numbers, bank information, etc.)

## Security failures/vulnerabilities …

examples

# Randomness of cryptographic keys

- 2008 – Debian
- modification of openssl source code
  - the use of uninitialized memory
  - broken initialization of pseudorandom generator …initialized by PID only
  - at most 98301 unique initialization values overall (depending on particular platform)
- impact:
  - predictable keys for SSH, OpenVPN, DNSSEC, X.509 certificates, session keys in SSL/TLS, …
  - using library just for a single DSA signing …compromised private key
  - similar problem with randomness in Sony Playstation 3 (ECDSA signatures, 2010)

# Later …in openssl 1.0 source code

```
/* DO NOT REMOVE THE FOLLOWING CALL TO MD_Update()! */
MD_Update(&m,buf,j);
/* We know that line may cause programs such as
   purify and valgrind to complain about use of
   uninitialized data.  The problem is not, it's
   with the caller.  Removing that line will make
   sure you get really bad randomness and thereby
   other problems such as very insecure keys. */
```

- Correct and secure implementation of cryptography is not easy
  - 10 vulnerabilities in openssl (NVD, published in 2010–2014) with severity High, not including the Heartbleed bug (with severity Medium)

# Heartbleed

- probably the most important vulnerability in 2014
- problem in implementation of heartbeat extension (RFC6520) in OpenSSL
- the attacker can read the memory of the server

  request (as intended): send me this 6 byte payload “abcdef”
  response: “abcdef”

  request (attack): send me this 20003 byte payload “abc”
  response: “abc” + 20000 bytes of server’s memory

# Timing attacks on comparisons (Google, Sun, …)

- 2009 – Keyczar (Google), Java (Sun), …
- common scenario: server compares received HMAC with calculated one
- attacker's goal: to get correct HMAC for his own message ("authentic")
- What is wrong with this code (Python)?

```
return self.Sign(msg) == sig_bytes
```

# What is wrong with this code (Java)?

```java
public static boolean
isEqual(byte digesta[], byte digestb[]) {
  if (digesta.length != digestb.length)
    return false;

  for (int i = 0; i < digesta.length; i++) {
    if (digesta[i] != digestb[i])
      return false;
  }
  return true;
}
```

# HMAC reconstruction

How long does it take for server to answer/react to incorrect HMAC

- if the first 0, 1, 8 or 15 bytes are correct?
- HMAC reconstruction based on time-variance of responses
- 4th byte:

**71 A0 89** 00 00 . . . 00

**71 A0 89** 01 00 . . . 00

. . .

**71 A0 89** 4A 00 . . . 00 longer time to process?

. . .

**71 A0 89** FF 00 . . . 00

- usually multiple measures required for a single value (noise)
- statistical evaluation of measurements

# Constant-time comparison (Java)

```
public static boolean
isEqual(byte[] digesta, byte[] digestb) {
  if (digesta.length != digestb.length)
    return false;

  int result = 0;
  for (int i = 0; i < digesta.length; i++) {
    result |= digesta[i] ^ digestb[i];
  }
  return result == 0;
}
```

# Adobe password encryption

- 2013, Adobe
- data breach, 38 million *active* users account information exposed
- 150 million user accounts overall
- passwords are encrypted (the key was not leaked)
  …using 3DES (block cipher with 8 B block) in ECB mode
- result:
  - equal password substring [1-8], [9-16] easily identifiable
  - guess using password hits (part of account information), e.g.
    “numbers 123456”, “c’est 123456”
    “1*6”, “sixones”
    “q w e r t y”, “6 long qwert”

# The most frequent passwords from Adobe’s database

| | | |
|---|---|---|
| 1. | 123456 | (≈ 1,9 million) |
| 2. | 123456789 | (≈ 446 thousand) |
| 3. | password | (≈ 345 thousand) |
| 4. | adobe123 | (≈ 211 thousand) |
| 5. | 12345678 | |
| 6. | qwerty | |
| 7. | 1234567 | |
| 8. | 111111 | |
| 9. | photoshop | |
| 10. | 123123 | |
| 11. | 1234567890 | |
| 12. | 000000 | |
| 13. | abc123 | |
| 14. | 1234 | |
| 15. | adobe1 | |
| 16. | macromedia | |
| 17. | azerty | |
| 18. | iloveyou | |
| 19. | aaaaaa | |
| 20. | 654321 | |

# The most frequent passwords

source: Splashdata, based on leaked passwords (2014 and comparison with 2013)

| | | |
|---|---|---|
| 1. | 123456 | |
| 2. | password | |
| 3. | 12345 | (+ 17) |
| 4. | 12345678 | (– 1) |
| 5. | qwerty | (– 1) |
| 6. | 123456789 | |
| 7. | 1234 | (+ 9) |
| 8. | baseball | (new) |
| 9. | dragon | (new) |
| 10. | football | (new) |
| 11. | 1234567 | (– 4) |
| 12. | monkey | (+ 5) |
| 13. | letmein | (+ 1) |
| 14. | abc123 | (– 9) |
| 15. | 111111 | (– 8) |
| 16. | mustang | (new) |
| 17. | access | (new) |
| 18. | shadow | |
| 19. | master | (new) |
| 20. | michael | (new) |
| 21. | superman | (new) |
| 22. | 696969 | (new) |
| 23. | 123123 | (– 12) |
| 24. | batman | (new) |
| 25. | trustno1 | (– 1) |

# WPS (WiFi Protected Setup)

- 2011
- goal: easy (and secure) method to add a device to network
- implementation:
  - 8 digit PIN code authentication (printed on a sticker)
  - theoretically $10^8$ possibilities
  - practically: response to incorrect PIN leaks an information whether the first half of the PIN is wrong
    last digit is a checksum
  - $10^4 + 10^3$ possibilities
- WPS can't be turned off in some WiFi routers

# Encrypted USB drives

- 2010; Kingstone, SanDisk, Verbatim
- FIPS 140-2 Level 2 certification; AES-256 encryption
- reality:
  - encryption key does not depend on user's password
  - USB key unlocks if some expected string (fixed, password- and device-independent) is received

# Hash tables collisions

- 2011; Oracle, Microsoft, PHP, Apache Tomcat, …
- analogous problem found originally in 2003; Perl, Squid
- hash table – data structure for storing (key/data) pairs
  - average complexity $O(n)$ for inserting/deleting/finding $n$ elements
  - worst case complexity $O(n^2)$ for $n$ elements (when keys collide)
- problem: colliding keys can be generated easily
- parameters of HTTP POST requests are parsed into hash table automatically
- DoS attack on web server:
  $\sim$70-100kbits/s ⇒ one i7 core busy (2011, PHP)

# Hashing for hash tables

- Java 6 (java.lang.String, method public int hashCode())
  - 32-bit arithmetic (int), $s_i$ denotes an $i$-th character of an ($s_{1,\ldots,n}$):

$$\sum_{i=1}^{n} 31^{n-i} \cdot s_i$$

- PHP 5 (algorithm DJBX33A, 32-bit arithmetic), $s_0$ is constant 5381

$$\sum_{i=0}^{n} 33^{n-i} \cdot s_i$$

- ASP.NET (algorithm DJBX33X), $s_0$ is constant 5381

$$\bigoplus_{i=0}^{n} 33^{n-i} \cdot s_i$$

- easy to find large multicollisions

# Solutions

- limit the size of POST requests, limit CPU for single request, etc.
- better hash function
  - for example randomized hashing – the function dependent on randomly chosen parameter (when process starts)

# Apple “goto” fail (2014)

```
SSLVerifySignedServerKeyExchange(...)
{
  OSStatus  err;
  ...
  if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
  if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
  if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
    ...
    err = sslRawVerify(...)

  fail:
    ...
    return err;
}
```

# Other incidents (1)

- NSA
  - 2013; approx. 1.7 million files
  - Showden (contractor)
  - gradual publication of documents and files, global surveillance programs
    - tools and methods, e.g. see Tailored Access Operations (TAO) catalog
    - identities of cooperating companies and governments
    - identities of ISPs and platforms that NSA has penetrated or attempted to penetrate
    - foreign officials and systems that NSA has targeted
- Associated Press
  - April 2013
  - AP Twitter account hacked:
    *Breaking: Two Explosions in the White House and Barack Obama is Injured.*
  - 136 billion USD from the S&P's 500 Index in two minutes

# Other incidents (2)

- Network Time Protocol – DoS attacks
  - NTP amplification attack (amplification factor 19)
  - single 234-byte request … 10 packets response (total 4 460 bytes).
  - MONLIST command (IP addresses of the last 600 machines interacting with an NTP server)
  - February 2014 … reported DDoS attack with 400 Gbps traffic

- BMW
  - ConnectedDrive technology (since 2010)
  - more than 50 models affected (BMW, Mini, Rolls Royce)
  - features: emergency call, remote unlocking and unlocking, auxiliary heating, etc.
  - analysis in 2014, published in 2015
  - the same symmetric keys in all cars
  - some services do not encrypt messages between the car and BMW's servers
  - device is not tamper-proof, etc.

# Other incidents (3)

- RSA (1)
  - 2011; targeted attack on RSA (part of EMC)
  - SecurID tokens (one-time passwords, two-factor authentication), market leader
  - replacing 40 million tokens
- NIST, RSA
  - 2013
  - NIST standard includes Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG)
  - Dual EC DRBG proposed by NSA
  - RSA: Dual EC DRBR default in BSAFE toolkit
  - RSA: 10 million USD deal with NSA (Reuters)
  - trapdoor in Dual EC DRBR