Security incidents, weaknesses and vulnerabilities

Martin Stanek

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

Security of IT infrastructure (2016/17)

Content

Vulnerabilities

Statistics, surveys, predictions, controls

Real-world security incidents

Data breaches

Other incidents

Examples of vulnerabilities – technical details

Introduction

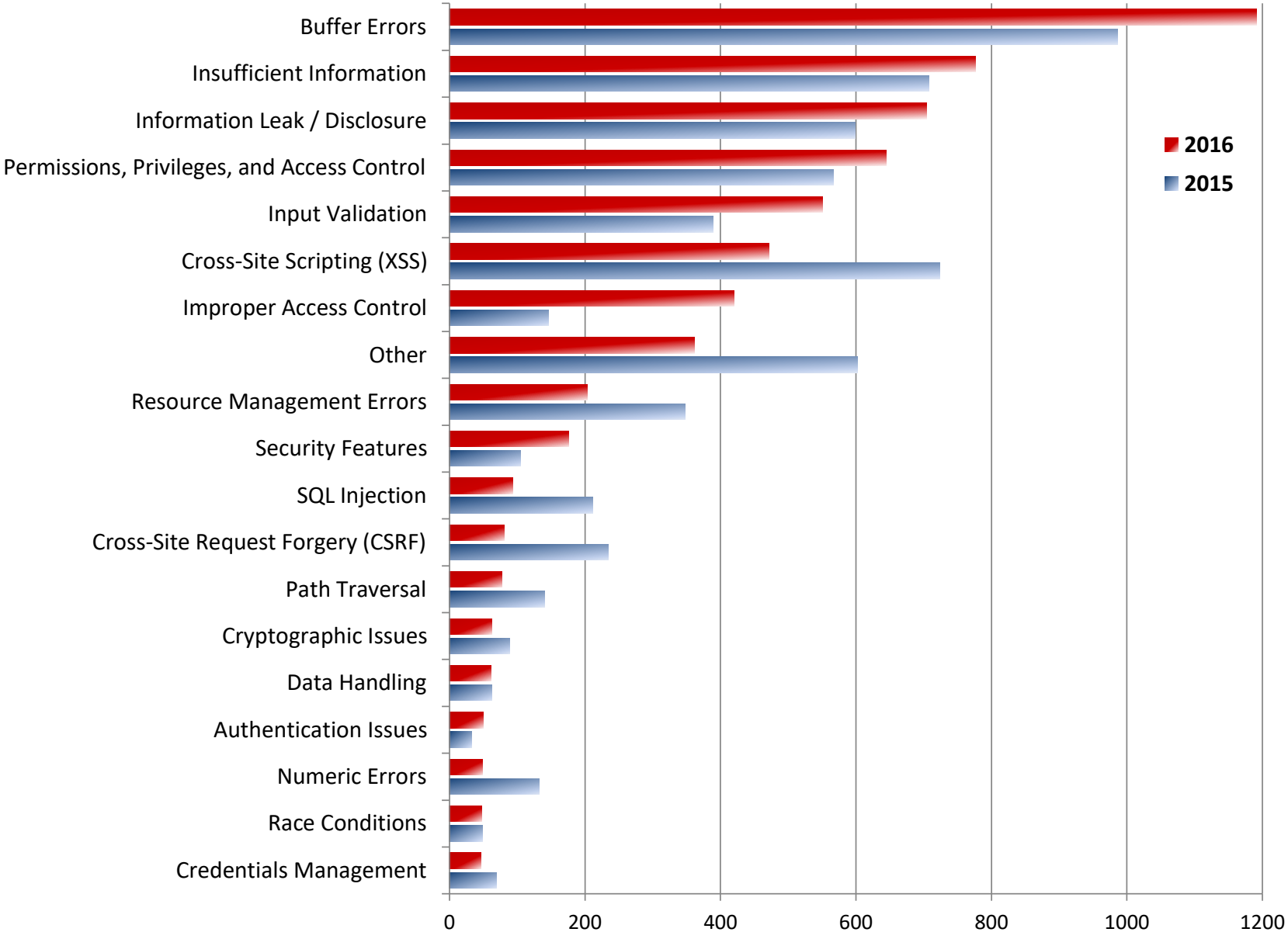
Security incidents and failures

- 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 reality is worse (unpublished vulnerabilities, weak passwords, misconfiguration, etc.)
- National Vulnerability Database (nvd.nist.gov)
- vulnerabilities (software flaws) published:
  5278 (2012), 5174 (2013), 7903 (2014), 6453 (2015), 6449 (2016)
- classification (categories, severity etc.)

NVD – vulnerabilities published in 2015 and 2016



Examples . . . (1)

Authentication Issues (CVE-2015-7755):
Juniper ScreenOS 6.2.0r15 through 6.2.0r18, . . . , and 6.3.0r20 before 6.3.0r21 allows remote attackers to obtain administrative access by entering an unspecified password during a (1) SSH or (2) TELNET session.
user: auth_admin_internal, password: `<<< %s(un='%s') = %u`

Buffer Errors (CVE-2016-0946):
Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and ... on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0945.

Examples . . . (2)

Credentials Management (CVE-2015-7283):
The web administration interface on ZyXEL NBG-418N devices with firmware 1.00(AADZ.3)C0 has a default password of 1234 for the admin account, which allows remote attackers to obtain administrative privileges by leveraging a LAN session.

Cryptographic Issues (CVE-2015-2233):
Lenovo System Update (formerly ThinkVantage System Update) before 5.06.0034 does not properly validate CA chains during signature validation, which allows man-in-the-middle attackers to upload and execute arbitrary files via a crafted certificate.

Improper Access Control (CVE-2015-3306):
The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands. (without authentication)

Examples . . . (3)

SQL Injection (CVE-2015-5308):
Multiple SQL injection vulnerabilities in cs_admin_users.php in the wp-championship plugin 5.8 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) user, (2) isadmin, (3) mail service, (4) mailresceipt, (5) stellv, (6) champtipp, (7) tippgroup, or (8) userid parameter.

Security Features (CVE-2016-0019):
The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka “Windows Remote Desktop Protocol Security Bypass Vulnerability.”

Other classifications of vulnerabilities

- MITRE:
  - Common Vulnerabilities and Exposures (cve.mitre.org)
  - 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
  - OWAPSP Top 10 (most critical web application security risks, 2013)
  - Testing Guide (v4, 2014)
- more detailed classifications, description, examples, additional information

Real world – surveys, analyses, predictions

- EY's Global Information Security Survey 2016-17
- Verizon's Data Breach Investigations Report 2016
- PwC's The Global State of Information Security Survey 2017
- Various Security Predictions for 2017:
  - Symantec, Forcepoint, McAfee, Trend Micro, IBM, Kaspersky, ...

EY's Global Information Security Survey 2016-17

- 1735 respondents (CISO, CIO, etc.)
- 87% of board members and C-level executives lack confidence in their organization's level of cybersecurity
- top two threats: phishing, malware
- top three security areas to address in the coming 12 months:
  1. Business continuity/disaster recovery resilience
  2. Data leakage/data loss prevention
  3. Security awareness and training

Verizon – 2016 Data Breach Investigations Report

- summary of 2015, 82 countries represented
- 64.199 security incidents, 2.260 confirmed data breaches
- top 10 vulnerabilities ~ 85% of the successful exploits
- patterns:

	incidents	breaches
Web App Attacks	8.3%	40.2%
POS Intrusions	0.8%	23.2%
Miscellaneous Errors	17.7%	8.7%
Privilege Misuse	16.3%	7.6%
Cyber-espionage	0.4%	6.9%
Everything Else	13.8%	5.5%
Payment Card Skimmers	0.2%	3.8%
Physical Theft/Loss	15.1%	2.5%
Crimeware	12.4%	2.2%
Denial-of-Service	15.0%	0.0%

Trend Micro Security Predictions 2017

- Ransomware growth will plateau in 2017, but attack methods and targets will diversify.
- IoT devices will play a bigger role in DDoS attacks; IIoT (Industrial IoT) systems in targeted attacks.
- The simplicity of Business Email Compromise attacks will drive an increase in the volume of targeted scams in 2017.
- Business Process Compromise will gain traction among cybercriminals looking to target the financial sector.
- Adobe and Apple will outpace Microsoft in terms of platform vulnerability discoveries.
- Cyberpropaganda will become a norm.
- General Data Protection Regulation (GDPR) implementation and compliance will raise administrative costs across organizations.
- Threat actors will come up with new targeted attack tactics that circumvent current anti-evasion solutions.

SANS: Critical Security Controls (1)

https://www.sans.org/critical-security-controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability

SANS: Critical Security Controls (2)

https://www.sans.org/critical-security-controls

11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

UK: Cyber Essentials Scheme

https://www.cyberaware.gov.uk/cyberessentials/

Requirements for basic technical protection from cyber attacks

1. Boundary firewalls and internet gateways
2. Secure configuration
3. User access control
4. Malware protection
5. Patch management

Data breaches – examples

Data breaches – examples (1)

1. Office of Personnel Management
   - detected: April 2015, started: March 2014
   - 21.5 million records
   - attackers with valid user credentials / contractors
   - names, SSNs, dates and places of birth, addresses, security-clearance information
   - 5.6 million sets of fingerprints
2. Anthem (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: some tech employees had their credentials compromised
   - detection: noticing suspicious queries

   Similar breach: Premera (11 million people)

Data breaches – examples (2)

3. Ashley-Madison
   - data breach announced in July 2015 (“Impact Team”)
   - 10GB + 19GB compressed data
   - $\sim$ 37 million customer records
   - e-mail addresses, names, credit card transactions, …
   - source code, e-mails
   - suicides, blackmailing, bcrypt + MD5
4. Friend Finder Network
   - October 2016
   - 412 million accounts (Adult Friend Finder, Cams.com, Penthouse.com, Stripshow.com …)
   - addresses, passwords, dates of last visits, browser information, IP addresses and site membership status
   - not the first time (May 215, 4 million users)
   - plaintext and SHA-1 password (lowercase)
   - over 99% paswords cracked

Data breaches – examples (3)

5. Hacking Team
   - selling offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations
   - data breach announced: July 2015
   - 400GB (customers, e-mails, 0-day exploits, source code, ...)
   - weak passwords, e.g. “P4ssword”, “HTPassw0rd”, “wolverine”
6. IRS (Internal Revenue Service)
   - detected: too many old tax returns (May 2015)
   - stolen credentials (probably from other data breaches, e.g. Anthem)
   - 334 thousand people
   - 15,000 falsified documents processed ... 50 million USD in refunds

Data breaches – examples (2)

7. 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
8. 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)

9. 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
10. Sony Pictures (USA, entertainment)
   - 100TB of data (?)
   - discovered in November 2014
   - personal information about employees, e-mails, salaries, copies of unreleased Sony films
   - North Korea (?)
   - the White House reacts

Other security incidents

Other security incidents (1)

- stealing money
  - Bangladesh Bank (March 2016)
  - operator's SWIFT credentials, malware
  - bank transfers from Bangladesh Bank's account in Federal Reserve Bank of New York to Philippines and Sri Lanka
  - 81 million USD (only a typo prevented 1 billion USD transfer)
- Ukrainian Power Grid
  - December 2015
  - BlackEnergy trojan
  - black-out (for few hours): 103 cities complete 184 cities partial
  - blocked call centers

Other security incidents (2)

- 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 security incidents (3)

- 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
- DynDNS and Mirai
  - October 2016
  - DDoS attack ~ 1.2Tbps
  - primary source of the attack: Mirai botnet
  - Mirai: IoT devices – routers, DVRS and CCTV cameras (> 60 common default usernames and passwords)
  - September 2016 (KrebsOnSecurity, 620Gbps)

Other security incidents (4)

- Ransomware
  - 172% increase in new ransomware families in first half of 2016
  - ransomware modifications: 2.900 Q1 → 32.091 Q2 (Kaspersky)
  - threefold increase in attacks between January and September 2016
  - victims – anybody, but also healthcare and education sectors
    The Hollywood Presbyterian Medical Center (paid 40 BTC),
    The University of Calgary (paid 45 BTC)
  - Ransomware-as-a-Service
  - diversifying targets: KeRanger (OS X, 2016), Linux.Encoder.1 (Linux, 2015), MongoDB databases (2017)

Security failures/vulnerabilities ...

examples

The most frequent passwords

source: Splashdata, based on leaked passwords (2016 and comparison with 2015)

1.	123456	
2.	password	
3.	12345	(+ 2)
4.	12345678	(− 1)
5.	football	(+ 2)
6.	qwerty	(− 2)
7.	1234567890	(+ 5)
8.	1234567	(+ 1)
9.	princess	(+ 12)
10.	1234	(− 2)
11.	login	(+ 9)
12.	welcome	(− 1)
13.	solo	(+ 10)
14.	abc123	(− 1)
15.	admin	(new)
16.	121212	(new)
17.	flower	(new)
18.	passw0rd	(+ 6)
19.	dragon	(− 3)
20.	sunshine	(new)
21.	master	(− 4)
22.	hottie	(new)
23.	loveme	(new)
24.	zaq1zaq1	(new)
25.	password1	(new)

How to verify the certificates for TLS

- 76 iOS applications from App Store vulnerable to MITM attacks (January 2017)
- not a new issue:
  - CVE-2016-6231: Kaspersky Safe Browser iOS before 1.7.0 does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to obtain sensitive information via a crafted certificate.
  - CVE-2016-3664: Trend Micro Mobile Security for iOS before 3.2.1188 does not verify the X.509 certificate of the mobile application login server, which allows man-in-the-middle attackers to spoof this server and obtain sensitive information via a crafted certificate.
  - many others ...
- $\sim$ 1.400 Android applications (2014):

  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.

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)?

```
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”

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:
  ~70-100kbits/s $\Rightarrow$ 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;
}
```