Security incidents, weaknesses and vulnerabilities

Martin Stanek

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

Security of IT infrastructure (2018/19)

Content

Global DNS Hijacking

- reported by FireEye in January 2019
- various activities observed since 2017
- manipulation of DNS records
- techniques
  - manipulating DNS A record
  - manipulating DNS NS record
  - using DNS Redirector
- targets:
  - telecoms, ISPs, government agencies, etc.
  - Middle East, North Africa, Europe and North America
- impact
  - redirected and intercepted web and mail traffic
  - possibly other network services

Global DNS Hijacking – DHS reaction

- Department of Homeland Security
- Cybersecurity and Infrastructure Security Agency
- an emergency directive issued
- multiple federal agencies affected by the attack
- 10 business days for three actions:
  1. audit all public DNS records on all authoritative and secondary DNS servers
  2. update passwords for all accounts on systems that can make changes to DNS records
  3. implement multi-factor authentication for all those accounts
  4. monitor Certificate Transparency logs

Marriott breach

- large hospitality company (hotels)
- data leak involving a guest reservation database
- unauthorized access since 2014, detected in September 2018
- 500 million guests
- leaked data - some combination of
  - name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences
  - payment card numbers (encrypted) and payment card expiration dates
- updated numbers from January 2019:
  - 8.6 million unique payment card numbers (encrypted)
  - 5.25 million unique unencrypted passport numbers
  - 20.3 million encrypted passport numbers

PEAR supply-chain attack

- PHP Extension and Application Repository
- published in 2019 (breached for 6 months)
- infected package manager file on the project's web site
- malicious backdoor – reverse shell on infected hosts
- similar problems:
  - PyPI repository typosquatting (2017): bzip (original bz2file), crypt (crypto), setup-tools (setuptools), django-server (django-server-guardian-api), etc.
  - Node.js NPM event-stream (2018), targeting a bitcoin wallet
  - CCleaner (2017) - 2.27 million users infected

“Unexpected” vulnerabilities

- IE vulnerability (CVE-2018-8653), remote code execution, actively exploited by attackers . . . emergency update
- Apple: FaceTime group chat (eavesdropping)
- 14 years old bug in WinRAR (CVE-2018-20253): absolute path traversal leading to code execution
- . . .
- your custom web application

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)
- various other sources exist
  - more sources and vulnerabilities covered, faster publication, additional detail (e.g. how to fix), . . .

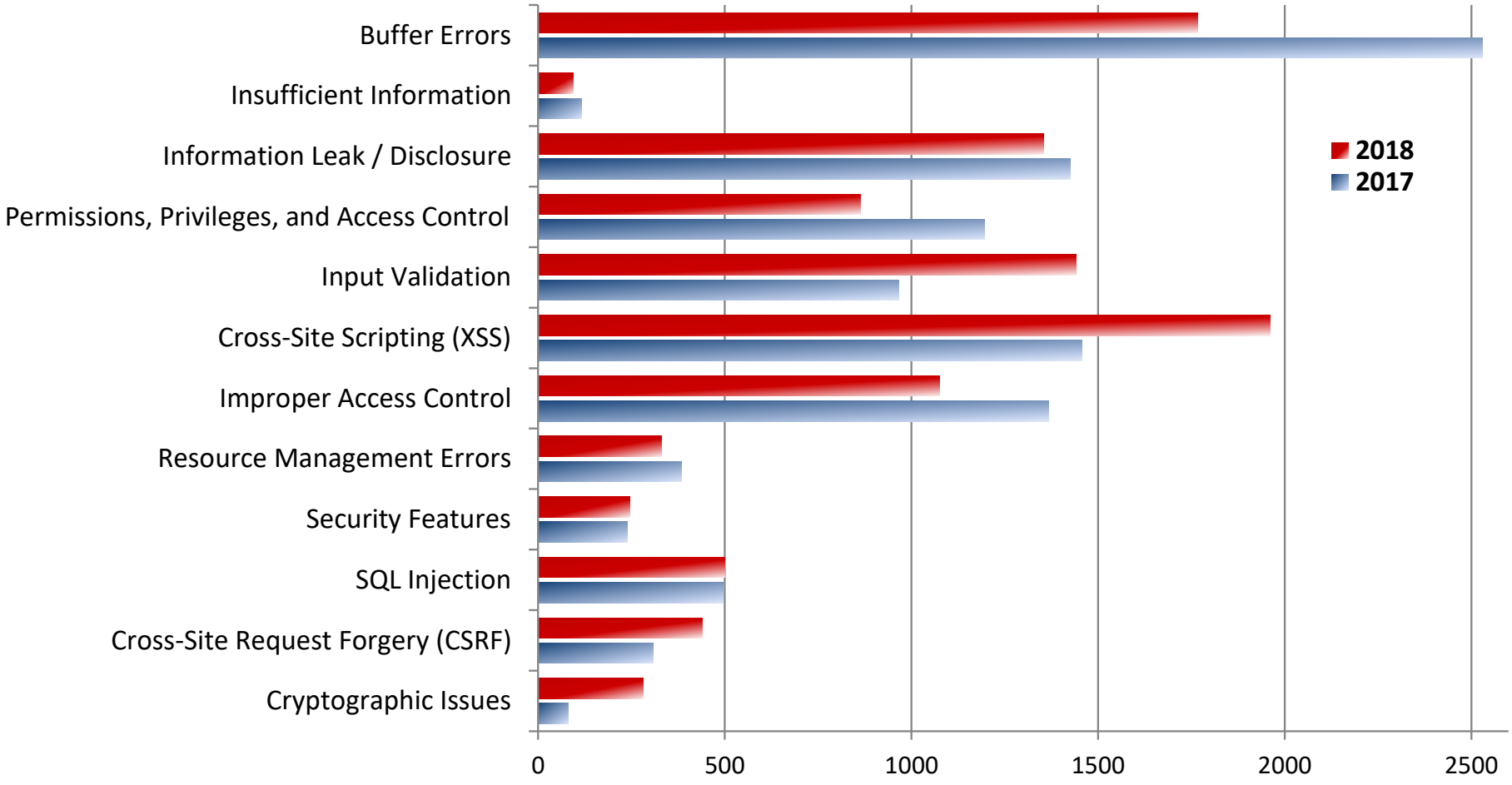
NVD

- operated by NIST
- vulnerabilities (software flaws) published:

year	2013	2014	2015	2016	2017	2018
count	5174	7903	6453	6449	14646	16517

- the rise – “organizational changes and increased vulnerability research”
- includes classification (categories, severity etc.)
- for more detailed analysis, see e.g.
  Skybox Security: Vulnerability and Threat Trends Report 2019 (Analysis of current vulnerabilities, exploits and threats in play)

NVD – selected vulnerabilities published in 2017 and 2018



Examples . . . (1)

Authentication Issues (CVE-2017-13872):
Apple macOS High Sierra before Security Update 2017-001 . . . It allows attackers to obtain administrator access without a password via certain interactions involving entry of the root user name.

Buffer Errors (CVE-2018-8653):
A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10. This CVE ID is unique from CVE-2018-8643.

Examples . . . (2)

Cryptographic Issues (CVE-2017-[12373, 13099, 13098, 6168, . . .]):
Cisco, Citrix, F5, WolfSSL, Bouncy Castle , Radware, . . . Return Of Bleichenbacher's Oracle Threat (ROBOT)

Input Validation (CVE-2017-5638) . . . *Equifax*:
The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Examples . . . (3)

Credentials Management (CVE-2017-3192):
D-Link DIR-130 firmware version 1.23 and DIR-330 firmware version 1.12 do not sufficiently protect administrator credentials. The tools_admin.asp page discloses the administrator password in base64 encoding in the returned web page. A remote attacker with access to this page (potentially through a authentication bypass such as CVE-2017-3191) may obtain administrator credentials for the device.

Improper Access Control (CVE-2018-1000628):
Battelle V2I Hub 2.5.1 could allow a remote attacker to bypass security restrictions, caused by the direct checking of the API key against a user-supplied value in PHP's GET global variable array using PHP's strcmp() function. By adding "[]" to the end of "key" in the URL when accessing API functions, an attacker could exploit this vulnerability to execute API functions.

Examples . . . (4)

SQL Injection (CVE-2017-16510):
WordPress before 4.8.3 is affected by an issue where $wpdb->prepare() can create unexpected and unsafe queries leading to potential SQL injection (SQLi) in plugins and themes, as demonstrated by a “double prepare” approach, a different vulnerability than CVE-2017-14723.

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
  - OWASP Top 10 (most critical web application security risks, 2017)
  - Testing Guide (v4, 2014)
  - OWASP Application Security Verification Standard (v3.0.1, new version Q1/2019)
- more detailed classifications, description, examples, additional information

Real world – surveys, analyses, predictions

- EY's Global Information Security Survey 2018-19
- Verizon's Data Breach Investigations Report 2018
- Skybox Security: Vulnerability and Threat Trends Report 2019
- Various Security Predictions for 2019:
  - Symantec, Kaspersky, Forcepoint, FireEye, Trend Micro, McAfee, ...

Some findings from global surveys

- EY's Global Information Security Survey 2018-19
  - approx. 1.400 respondents (CISO, CIO, etc.)
  - 8% – information security function meets the organization's needs
  - 15% – information security reporting meets the needs
  - top two threats: phishing (22%), malware (20%)
    (no change from the previous survey)
  - the most valuable info: customer data
  - top two vulnerabilities: careless/unaware employees, outdated security controls

Verizon – 2018 Data Breach Investigations Report (1)

- summary of 2017, global coverage
- Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach: An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party
- datasets contributed by various security vendors
- 43.308 security incidents, 2.216 confirmed data breaches

Verizon – 2018 Data Breach Investigations Report (2)

- patterns:

	incidents	breaches
Web App Attacks	9.1%	18.7%
Cyber-espionage	0.7%	7.7%
Privilege Misuse	20.0%	12.5%
Miscellaneous Errors	4.0%	15.7%
POS Intrusions	0.6%	14.6%
Everything Else	1.4%	13.9%
Payment Card Skimmers	0.3%	5.0%
Physical Theft/Loss	7.4%	6.5%
Crimeware	16.6%	6.3%
Denial-of-Service	40.2%	0.0%

- the report provides details for 8 industries

Skybox Security: Vulnerability and Threat Trends Report 2019

- the report *"examines new vulnerabilities published in 2018, newly developed exploits, new exploit–based malware and attacks, current threat tactics and more"*
- top malware attacks: 27% cryptomining, 14% remote access, 13% botnet
- ransomware decline: 13% (28% in 2017)
- more web browsers vulnerabilities
- operational technology attacks on rise

What to do – regulatory and compliance frameworks

- NIST SP 800-53 (Rev. 4) Recommended Security Controls for Federal Information Systems and Organizations
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls
- Australian Signals Directorate: Strategies to Mitigate Cyber Security Incidents
- Australian Government Information Security Manual – Executive Companion / Principles / Guidelines
- ISACA: COBIT 2019 Framework
- CIS Controls (V7, 2018)
- Payment Card Industry – Data Security Standard version 3.2.1 (PCI DSS)

CIS Controls V7 – Basic (1-6)

https://www.cisecurity.org/controls/

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

- Foundational (7-16)
- Organizational (17-20)

CIS Controls V7 – (7-20)

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration 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. Implement a Security Awareness and Training Program
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. Secure your Internet connection (Boundary firewalls and internet gateways)
2. Secure your devices and software (Secure configuration)
3. Control access to your data and services (User access control)
4. Protect from viruses and other malware (Malware protection)
5. Keep your devices and software up to date (Patch management)

Data breaches – examples

Data breaches – examples (1)

1. Equifax
   - detected: July 2017, started: May 2017
   - 143 million people affected
   - attackers used unpatched Apache Struts vulnerability (CVE-2017-5638)
   - names, SSNs, birth dates, addresses
   - in some instances, driver's license numbers, credit card numbers
   - December 2018: House Oversight Committee report
2. Uber
   - October 2016, revealed: November 2017
   - leaked personal data of 50 million customers and 7 million drivers
   - names, email addresses, phone numbers
   - attack: AWS (Amazon Web Services) logon credentials accessible on GitHub
   - Uber paid the attackers $100.000 to delete data and keep quiet
   - September 2018: $148 million penalty

Data breaches – examples (2)

3. 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
4. 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 (3)

5. Ashley-Madison
   - data breach announced in July 2015 (“Impact Team”)
   - 10GB + 19GB compressed data
   - $\sim$ 37 million records (customers)
   - e-mail addresses, names, credit card transactions, …
   - source code, e-mails
   - suicides, blackmailing, bcrypt + MD5
6. 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 2015, 4 million users)
   - plaintext and SHA-1 password (lowercase)
   - over 99% paswords cracked

Data breaches – examples (4)

7. 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”
8. British Airways
   - detected: airline’s partner
   - 21 August – 5 September 2018
   - 380 thousand booking transactions
   - names, email addresses and credit card numbers, expiry dates and CVV codes
   - compromised website (modified javascript)

Data breaches – examples (5)

9. 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
10. 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 (6)

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)
  - recent example: Russian Central Bank (6 million USD, 2017)
- 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)

- 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
- 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 (3)

- Crypto-ransomware
  - May 2017 WannaCry
    - 4 days, 200.000 computers, 150 countries
    - EternalBlue exploit (developed by NSA, leaked by Shadow Brokers in April 2017)
  - October 2017 Bad Rabbit
    - fake Adobe Flash update
    - EternalRomance exploit (developed by NSA, leaked by Shadow Brokers)
  - August 2018 TSMC (Taiwan)
    - WannaCry variant; installation of infected software
    - more than 10 thousand systems affected (multiple sites)
    - day-long halt of production
    - (similar problem: Boeing, March 2018)

Appendix

The most frequent passwords

source: Splashdata, based on leaked passwords (2018 and comparison with 2017)

1.	123456	
2.	password	
3.	123456789	(+ 3)
4.	12345678	(− 1)
5.	12345	
6.	111111	(new)
7.	1234567	(+ 1)
8.	sunshine	(new)
9.	qwerty	(− 5)
10.	iloveyou	
11.	princess	(new)
12.	admin	(− 1)
13.	welcome	(− 1)
14.	666666	(new)
15.	abc123	
16.	football	(− 7)
17.	123123	
18.	monkey	(− 5)
19.	654321	(new)
20.	!@#$%^&*	(new)
21.	charlie	(new)
22.	aa123456	(new)
23.	donald	(new)
24.	password1	(new)
25.	qwerty123	(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.

certificates verification (cont.)

- CVE-2018-16395: An issue was discovered in the OpenSSL library in Ruby ... When two OpenSSL::X509::Name objects are compared using ==, depending on the ordering, non-equal objects may return true. When the first argument is one character longer than the second, or the second argument contains a character that is one less than a character in the same position of the first argument, the result of == will be true. This could be leveraged to create an illegitimate certificate that may be accepted as legitimate and then used in signing or encryption operations.
- CVE-2018-16875 The crypto/x509 package of Go ... does not limit the amount of work performed for each chain verification, which might allow attackers to craft pathological inputs leading to a CPU denial of service. Go TLS servers accepting client certificates and TLS clients are affected.