

EWD - Security part

Setting the scene



Security part of module: main topics

- Introduction
 - Threats, attacks, vulnerabilities; Security services
- Cryptography
 - Symmetric encryption
 - Public key cryptography
 - Authentication and integrity
 - Key management and certificates
- Web application threats and vulnerabilities
 - Common vulnerabilities
 - Penetration testing
 - Threat modelling
- Web application protection
 - Input validation
 - Web authentication schemes
 - Secure key and password storage

Security news stories...

News Brief: Mexico Earthquake

www.npr.org/2017/09/08/549373719/news-brief-mexico-earthquake-florida-evacuates-equifax-data-breach

npr change station? news arts & life music programs shop  

ON AIR NOW
NPR 24 Hour Program Stream

OUR PICKS LIVE RADIO SHOWS

U.S.

News Brief: Mexico Earthquake, Florida Evacuates, Equifax Data Breach

10:21 + Queue

Download Embed Transcript

September 8, 2017 · 5:15 AM ET Heard on [Morning Edition](#)

GREG ALLEN 

 Reporter Emily Green talks about a massive earthquake off the coast of Mexico. Also, the latest on Hurricane Irma, and TechCrunch writer John Mannes talks about a massive data breach at Equifax.

Transcript

DAVID GREENE, HOST:

We're covering a couple natural disasters on this morning. Let's begin with this powerful earthquake that toppled houses and damaged schools and hospitals in the south of Mexico.

MARY LOUISE KELLY, HOST:



ENDEAVOUR SEASON FOUR
AVAILABLE AT 



Security news stories...

← → C ⌂ <https://komonews.com/news/local/personal-data-of-nearly-1-million-uw-medicine-patients-exposed-online>

≡ **KOMONEWS** NEWS WEATHER SPORTS Refined CHIME IN WATCH

Personal data of nearly 1 million UW Medicine patients exposed online

by Tammy Mutasa | KOMO News | Wednesday, February 20th 2019



Security news stories...

Microsoft spots Russian hacking x +

https://news.sky.com/story/microsoft-spots-russian-hacking-campaign-ahead-of-eu-elections-11642702

sky news Watch Live

Home UK World Politics US Ocean Rescue Science & Tech Business Ents & Arts Offbeat More ▾

Biz Expo.ie IRELAND'S LARGEST SME & BUSINESS EXPO

5

Security news stories...

A screenshot of a web browser showing a news article from Extra.ie. The title of the article is '‘THIRD PARTY DATA BREACHES’ LEAD BANK OF IRELAND TO RESTRICT DEBIT CARDS'. The article is by George Morahan on 11/01/2019. It includes social sharing buttons for Facebook, Twitter, Email, and WhatsApp. Below the article, there is a paragraph about Bank of Ireland restricting debit card use due to third-party data breaches. A sidebar on the right shows a Ford INNOV8 advertisement.

Third Party Data Breaches' Lead Bank of Ireland to Restrict Debit Cards

By **George Morahan** - 11/01/2019

Bank of Ireland has restricted the use of some customers' debit cards amid ongoing concerns about fraud.

Affected customers will be prevented from using their cards for online and contactless transactions until they receive their new cards, which have been issued as a precaution.

The bank's decision stems from what it said was an 'increase in third party data breaches', citing breaches at Ticketmaster and the Marriott Hotel Group.

Bank of Ireland

Security news stories...

The screenshot shows a web browser window with the following details:

- Tab:** Ireland's Privacy Watchdog Pro
- Address Bar:** Information Security Media Group, Corp. [US] | https://www.bankinfosecurity.com/irelands-privacy-watchd...
- Header:** Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾ Jobs ▾
- Header Icons:** f (Facebook), t (Twitter), in (LinkedIn), r (RSS), m (Email), q (Search)
- Trending:** Webinar | Beyond Managed Security Services: SOC-as-a-Service for Financial Institutions
- Text:** Breach Notification , Data Breach , General Data Protection Regulation (GDPR)
- Section Header:** Ireland's Privacy Watchdog Probes Facebook Data Breaches
- Text:** 6.8 Million Users' Private Photos Exposed, Triggering GDPR Investigation
- Text:** Mathew J. Schwartz (@euroinfosec) • December 17, 2018 • 2 Comments
- Share Buttons:** Email, Print, LinkedIn, Facebook, Twitter, Credit Eligible, Get Permission
- Form:** GET DAILY EMAIL UPDATES (Email address: Submit
- Text:** Covering topics in risk management, compliance, fraud, and information security.
- Text:** By submitting this form you agree to our Privacy & GDPR Statement
- Image:** A smartphone displaying a "Help Center" screen with a search bar and the text "Important information about your".
- Advertisement:** THE RESULTS ARE IN FOR THE WORLD'S BEST CYBERSECURITY. SEE FOR YOURSELF. SOPHOS

Security news stories...

Yahoo's 2013 Data Breach Aff X

Secure | <https://mobileidworld.com/yahoo-data-breach-three-billion-accounts-010045/>

Yahoo's 2013 Data Breach Affected Three Billion Accounts

Posted on October 4, 2017 by Alex Peralta

"There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database."

Yahoo's 2013 data breach affected three billion accounts, the company has now revealed.

It is yet another upsizing of the damage on Yahoo's part, with the company initially having announced that the credentials of 200 million users had appeared for sale online, and later admitting that [half a billion accounts](#) had been compromised. Its latest revelation is the result, the company says, of collaboration with independent forensic investigators.

There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database. The other is that the data leaked didn't include personal information such as names, addresses, and birth dates.



Security news stories...

A screenshot of a web browser window showing a news article from The Washington Post. The title of the article is "Hacked Dropbox data of 68 million users is now for sale on the dark Web". The article is dated September 7 at 3:40 PM and was written by Karen Turner. Above the article, there is a banner for Gartner's Magic Quadrant for Business Intelligence & Analytics, with a call-to-action button labeled "GET THE REPORT". The browser interface includes a search bar, sections menu, and user profile "Jimmy".

wp Hacked Dropbox data of 68 mi X Jimmy

Sections

The Washington Post

Sign In Subscribe

GARTNER MAGIC QUADRANT FOR
BUSINESS INTELLIGENCE & ANALYTICS

GET THE REPORT

The Switch

Hacked Dropbox data of 68 million users is now for sale on the dark Web

By Karen Turner September 7 at 3:40 PM



9

Security news stories...

WannaCry attacks prompt Microsoft to release Windows updates for older versions

The company typically releases security updates for operating systems it still supports - but in wake of serious cyber-attack it has reassessed the policy

BOMGAR Provide remote support to any system or mobile device, anywhere.

FREE TRIAL

sign in become a supporter subscribe search jobs dating more International edition

UK world sport football opinion culture business lifestyle fashion environment tech travel all sections

home > tech

Windows WannaCry attacks prompt Microsoft to release Windows updates for older versions

This article is 2 months old

267

Alex Hern @alexhern

Wednesday 14 June 2017 12.26 BST

Microsoft Windows XP

PURINA Bakers Taste good every day NOW WITH NO ADDED ARTIFICIAL COLOURS, FLAVOURS OR PRESERVATIVES

SAME GREAT Taste

PURINA Your Pet. Our Passion.

Security news stories...

The screenshot shows a web browser window on a Mac OS X system. The title bar says 'F Just One Photo Can Silently Hack Millions Of Androids'. The address bar shows the URL 'www.forbes.com/sites/thomasbrewster/2016/09/06/google-android-one-photo-hack/#15ab50961555'. The page content is from Forbes under the 'Security / #CyberSecurity' section. It features a headline 'Just One Photo Can Silently Hack Millions Of Androids' by Thomas Fox-Brewster. Below the headline is a large image of a smartphone displaying a Google search interface with the text 'Ok Google... Make a call'. To the right of the phone is an advertisement for the 'efus™A7UL' chip, which is described as an 'NXP i.MX 6UltraLite' with 'Low Power WiFi/Bluetooth Linux Windows Embedded' capabilities. The chip is shown on a green printed circuit board. The date 'SEP 6, 2016 @ 03:47 PM' and '10,503 VIEWS' are visible. A sidebar on the left includes social sharing icons for Facebook, Twitter, and LinkedIn, and a 'SHARE >' button. A sidebar on the right contains the same 'efus™A7UL' advertisement and a 'More Info' button.

F Just One Photo Can Silently Hack Millions Of Androids

www.forbes.com/sites/thomasbrewster/2016/09/06/google-android-one-photo-hack/#15ab50961555

Forbes / Security / #CyberSecurity

efus™A7UL

NXP i.MX 6UltraLite Low Power eMMC

WiFi/Bluetooth Linux Windows Embedded

Made in Germany

SEP 6, 2016 @ 03:47 PM 10,503 VIEWS

The Little Black Book of Billionaire Secrets

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. [FULL BIO](#)

SHARE >

efus™A7UL

NXP i.MX 6UltraLite WiFi/Bluetooth eMMC

Low Power Linux Windows Embedded

Made in Germany

More Info

Security news stories...

The screenshot shows a web browser window displaying an article from CNN Tech. The URL in the address bar is money.cnn.com/2017/10/16/technology/wi-fi-flaw-krack-security/index.html. The page header includes the CNN logo and navigation links for BUSINESS, CULTURE, GADGETS, FUTURE, and STARTUPS. Social sharing icons for Facebook, Twitter, and LinkedIn are also present.

The main headline reads: "Wi-Fi network flaw could let hackers spy on you". Below the headline is a sub-headline: "Cyber-Safe". The author is listed as Selena Larson (@selenalarson), and the publication date is October 16, 2017, at 3:49 PM ET. To the right of the article are social sharing buttons for Facebook, Email, Twitter, LinkedIn, and a more options button.

The central image of the article is a close-up photograph of a person's hands connecting carabiners, symbolizing security or safety. Overlaid on this image is the text: "How to protect yourself from hackers".

At the bottom of the article, there is a video player showing a progress bar at 0:00 / 0:30. A red banner at the bottom of the video player says "Your video will play in 00:30".

To the right of the article, there is a sidebar titled "Social Surge - What's Trending" featuring three news items:

- "Goodell: NFL players aren't trying to be 'disrespectful to the flag'" (with a thumbnail image of a football team)
- "Doctors in Puerto Rico: 'Reality here is post-apocalyptic'" (with a thumbnail image of a doctor)
- "Trump's net worth drops \$600 million on Forbes' rich list, falls 92 spots" (with a thumbnail image of Donald Trump)

At the very bottom of the page, there is a small advertisement for a Samsung product.

Security news stories...

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Security news stories...

The screenshot shows a web browser window with the following details:

- Title Bar:** Revealed: how US and UK spy agencies defeat internet privacy and security
- Address Bar:** www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
- Page Header:** theguardian
- Page Navigation:** News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | Tech News > World news > The NSA files
- Text:** Series: Glenn Greenwald on security and liberty
- Main Article Title:** Revealed: how US and UK spy agencies defeat internet privacy and security
- Article Summary:** A bulleted list of findings:
 - NSA and GCHQ unlock encryption used to protect emails, banking and medical records
 - \$250m-a-year US program works covertly with tech companies to insert weaknesses into products
 - Security experts say programs 'undermine the fabric of the internet'
 - Q&A: submit your questions for our privacy experts
- Share Buttons:** Facebook Share (2882), Twitter Tweet (10.9K), Google +1 (3.4k), Pinterest Pin it, LinkedIn Share (742), Email
- Follow Button:** Follow Julian Borger by email (BETA)
- Author Information:** James Ball, Julian Borger and Glenn Greenwald, Guardian Weekly, Friday 6 September 2013
- Comments:** Jump to comments (4146)
- Article History:** Article history
- Page Footer:** World news

Security news stories...

Screenshot of a web browser displaying a security news article from eSecurityPlanet.com.

The browser window title is "Stuxnet Malware May Have Taken Out 1,000 Centrifuges" and the URL is "www.esecurityplanet.com/headlines/article.php/3919111/article.htm".

The page header includes a date "January 17, 2011", "Hot topics" (Desktop Security, Network Security, Trojans, Malware, Wpa Sec), and "Free Newsletters" (Security Daily).

The main content area features a sidebar advertisement for "Outlook PST Backup Solution for the Enterprise" and the main article headline:

Stuxnet Malware May Have Taken Out 1,000 Centrifuges

January 4, 2011
By eSecurityPlanet Staff
[Submit Feedback](#) »
[More by Author](#) »

A recent report from the [Institute for Science and International Security \(ISIS\)](#) states that the Stuxnet worm likely took out approximately 1,000 centrifuges at Iran's Natanz uranium enrichment plant.

"In late 2009 or early 2010, Iran decommissioned and replaced 1000 IR-I centrifuges at Natanz," [according to Infosecurity](#).

The article continues: "The ISIS said that quarterly safeguard reports by the International Atomic Energy Agency (IAEA) support the possibility that Stuxnet was responsible for the Natanz centrifuges' disruption," the article states.

Click [here](#) to read the Infosecurity article.

Right-hand sidebar advertisements include:

- Trend Micro Enterprise Security for Endpoints and Mail Servers \$54.99
- CDW
- DEFEND YOUR NETWORK THE LATEST SECURITY
- Free Trial: ESET NOD32 Antivirus 4
- 10 Ways to Dodge Cyber Bullets

Security news stories...

The screenshot shows a web browser window with the following details:

- Title Bar:** "FREAK: Another day, another serious SSL security hole" - www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/
- Toolbar:** Includes links for G.ie, Gmail, Maps, Drive, Print, Wiki, Moodle, Moodle Edge, WIT, AWS, TSSG, Tech, Media, Pers, Other, Temp, and Other Bookmarks.
- Header:** EDITION: UK, ZDNet logo, search icon, navigation icons, and links for CXO, HARDWARE, MICROSOFT, STORAGE, INNOVATION, HARDWARE, APPLE, MORE, NEWSLETTERS, ALL WRITERS, and user profile.
- Text Area:** JUST IN: APPLE LAUNCHES IPAD PRO: PROMISES DESKTOP PERFORMANCE IN TABLET
- Main Article Title:** **FREAK: Another day, another serious SSL security hole**
- Text Below Title:** More than one third of encrypted Websites are open to attack via the FREAK security hole.
- Author Information:** By Steven J. Vaughan-Nichols for Networking | March 3, 2015 -- 22:19 GMT (22:19 GMT) | Topic: Security
- Advertisement:** Key Encryption Solutions, Simple & Secure Cryptography Tools. Free Key Encryption Whitepaper, with a green button labeled →.
- Share Buttons:** Icons for messaging, Facebook, Twitter, LinkedIn, Email, and a bell.
- Text Summary:** It seemed like such a good idea in the early 90s. Secure-Socket Layer (SSL) encryption was brand new and the National Security Agency (NSA) wanted to make sure that they could read "secured" web traffic by foreign nationals. So, the NSA got Netscape to agree to deploy 40-bit cryptography in its International Edition while saving the more secure 128-bit version for the US version. By 2000, the rules changed and [any browser could use higher security](#)
- NSAI Advertisement:** NSAI provides a complete range of standards, as well as certification. NSAI logo.

Security news stories...

The screenshot shows a web browser window with the following details:

- Title Bar:** "Extremely critical crypto flaw in iOS may also affect fully patched Macs" at arstechnica.com
- Header:** MAIN MENU, MY STORIES: 25, FORUMS, SUBSCRIBE, JOBS
- Article Summary:** "Extremely critical crypto flaw in iOS may also affect fully patched Macs" by Dan Goodin - Feb 22 2014, 7:45pm GMT
- Left Sidebar:** Shows an email from Ashkan Soltani to himself, titled "Mail.app #gotofail test". It contains the text: "Ashkan Soltani <ashkan.soltani@gmail.com> To: Ashkan Soltani <ashkan.soltani@gmail.com> Mail.app #gotofail test". Below it is a message titled "Testing Mail.app iFrame issue" with the text: "If you can see this message then you are probably affected by CVE-2014-1266! See https://www.http://support.apple.com/kb/HT6147 for the iOS patch."
- Code Block:** A large block of C code related to SSL/TLS handling. A red oval highlights two consecutive "goto fail;" statements within a loop.

```
hashOut.length = SSL_SHA1_DIGEST_LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
    goto fail;

if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

    err = sslRawVerify(ctx,
                        ctx->peerPubKey,
                        dataToSign,
                        dataToSignLen,
                        signature,
                        signatureLen);
    if(err) {
        sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify
                    "returned %d\n", (int)err);
        goto fail;
    }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
```

Anything wrong with this?

The screenshot shows an email client interface with a message from Tesco.ie. The message details are as follows:

From: online@tesco.ie [Hide](#)
Subject: Tesco.ie Password Reminder
Date: 5 September 2014 22:15:24 GMT+01:00
To: jmcmcibney@gmail.com

Dear Mr McGibney

Please find below a reminder of your password as requested from the Tesco.ie website. We take security very seriously and this message has been sent only to the e-mail address given in your account details.

Your password is [REDACTED]

Kind regards,

Tesco.ie

This is an email from Tesco Ireland Limited (Company Number 19542). Registered in Ireland. Registered Office: Gresham House, Marine Road, Dun Laoghaire, Co Dublin.

Anything wrong with this?

The screenshot shows an email client interface with a message from Tesco.ie. The message details are as follows:

From: online@tesco.ie [Hide](#)
Subject: Tesco.ie Password Reminder
Date: 5 September 2014 22:15:24 GMT+01:00
To: jmcmcibney@gmail.com

Dear Mr McGibney

Please find below a reminder of your password as requested from the Tesco.ie website.

We take security very seriously and this message has been sent only to the e-mail address given in your account details.

Your password is [REDACTED]

Kind regards,

Tesco.ie

This is an email from Tesco Ireland Limited (Company Number 19542). Registered in Ireland. Registered Office: Gresham House, Marine Road, Dun Laoghaire, Co Dublin.

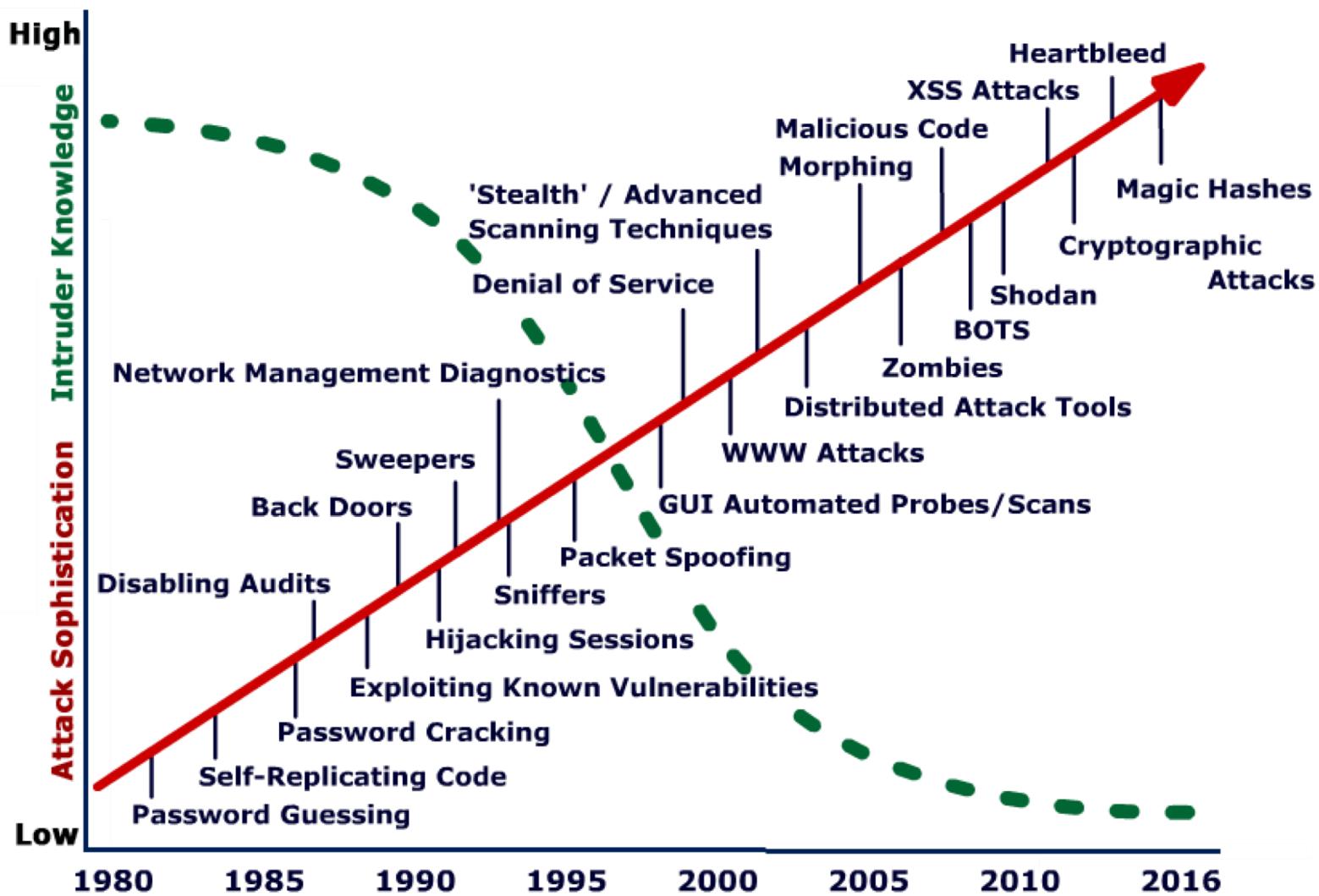
Security in context

- Increasing reliance on IT & networks for just about everything:
 - Communications (phone, email, social networks)
 - Finance
 - Supply chain (e.g. food on supermarket shelves)
 - Electricity generation & distribution
 - Industrial control systems
 - Water supply
 - Transportation
- How long could we cope without these?

SecurityFocus.com – new vulnerabilities snapshot

- 19-02-2019 LibVNCServer Incomplete Fix Multiple Heap **Buffer Overflow** Vulnerabilities
- 19-02-2019 Elasticsearch Logstash CVE-2019-7612 Information Disclosure Vulnerability
- 19-02-2019 WordPress CVE-2019-8943 Directory Traversal Vulnerability
- 19-02-2019 WordPress CVE-2019-8942 Remote Code Execution Vulnerability
- 19-02-2019 Horner Automation Cscape CVE-2019-6555 **Arbitrary Code Execution** Vulnerability
- 19-02-2019 Delta Industrial Automation CNCSoft CVE-2019-6547 **Denial of Service** Vulnerability
- 20-02-2019 Drupal Core CVE-2019-6340 Arbitrary PHP Code Execution Vulnerability
- 20-02-2019 Cisco Unity Connection CVE-2019-1685 **Cross Site Scripting** Vulnerability
- 20-02-2019 Cisco HyperFlex CVE-2019-1667 Arbitrary File Overwrite Vulnerability
- 20-02-2019 Microsoft Windows HTTP/2 SETTINGS Frames Denial of Service Vulnerability
- 20-02-2019 Cisco IoT Field Network Director CVE-2019-1698 **XML External Entity** Vulnerability
- 20-02-2019 Cisco Prime Infrastructure **SSL Certificate Validation Security Bypass** Vulnerability
- 21-02-2019 Opencontainers runc CVE-2019-5736 Local Command Execution Vulnerability
- 21-02-2019 WPA2 Key Reinstallation Multiple Security Weaknesses
- 21-02-2019 Intel Data Center Manager SDK CVE-2019-0110 Information Disclosure Vulnerability
- 21-02-2019 Intel Data Center Manager SDK Multiple **Privilege Escalation** Vulnerabilities
- 21-02-2019 Microsoft .NET Framework and Visual Studio CVE-2019-0657 **Spoofing** Vulnerability
- 21-02-2019 Microsoft Windows Device Guard CVE-2019-0627 Local Security Bypass Vulnerability

Attack Sophistication vs. Intruder Technical Knowledge



Main Players in Information Security

- Standards Bodies
 - IETF (Internet Engineering Task Force)
 - Internet standards, IPsec, SSL/TLS, ...
 - ISO (International Standards Organisation)
 - OSI model; ISO 27000 series of security standards; "Common Criteria" in ISO 15408
 - ITU (International Telecoms Union)
 - Recommendation X.800 on security services
 - NIST (US Nat'l Institute of Standards & Technology)
 - Official US standards (called FIPS); many on security
 - IEEE (Inst of Electrical & Electronics Engineers)
 - Communication standards, most notably IEEE 802 series:
Ethernet (802.3), WiFi (802.11), Authentication (802.1x), ...
 - Industry domain-specific standards and regulations
 - FDA, PCI DSS, etc

Main Players (continued)

- Government agencies
 - NSA - National Security Agency (US)
 - in the news a lot in recent years
 - Dept of Homeland Security (US)
 - Data Protection authorities (powerful in EU countries)
- The industry
 - Software and equipment vendors, web services
 - Microsoft, Apple, Google, Cisco, Facebook, ...
 - Security vendors, outsourcers, consultants
 - Symantec, McAfee, RSA Security, Trend Micro, IBM, HP, ...
 - Open source community
 - OpenSSL, Kali Linux, GPG, OWASP, ...
 - Certificate authorities
 - VeriSign, DigiCert, Comodo, GeoTrust, GoDaddy, ...