

# Security part

---

## 13.1. 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...

The screenshot shows a web browser window with the URL [money.cnn.com/2017/10/16/technology/wi-fi-flaw-krack-security/index.html](https://money.cnn.com/2017/10/16/technology/wi-fi-flaw-krack-security/index.html). The page is from the CNN Tech section, featuring a banner for BOMGAR INSIGHT Remote Camera Sharing for iOS & Android. The main headline is "Wi-Fi network flaw could let hackers spy on you" by Selena Larson (@selenalarson) on October 16, 2017, at 3:49 PM ET. The article includes a video thumbnail showing a person's hands holding a carabiner and a yellow strap, with the text "How to protect yourself from hackers". To the right, there is a sidebar titled "Social Surge - What's Trending" with links to other news stories: "Goodell: NFL players aren't trying to be 'disrespectful to the flag'", "Doctors in Puerto Rico: 'Reality here is post-apocalyptic'", and "Trump's net worth drops \$600 million on Forbes' rich list, falls 92 spots". At the bottom, there is an advertisement for a Samsung washing machine.

Wi-Fi network flaw could let hackers spy on you

by Selena Larson @selenalarson

October 16, 2017: 3:49 PM ET

How to protect yourself from hackers

Social Surge - What's Trending

- Goodell: NFL players aren't trying to be 'disrespectful to the flag'
- Doctors in Puerto Rico: 'Reality here is post-apocalyptic'
- Trump's net worth drops \$600 million on Forbes' rich list, falls 92 spots

AddWash with EcoBubble technology

# 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  
amazon

PBS

# 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 | **the guardian** | all sections

home > tech

**Windows** 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

 Microsoft Windows XP

This article is 2 months old

267

Alex Hern

@alexhern

Wednesday 14 June 2017 12.26 BST

**PURINA Bakers** **NOW WITH NO ADDED ARTIFICIAL COLOURS, FLAVOURS OR PRESERVATIVES** **SAME GREAT TASTE**

PURINA. Your Pet. Our Passion.

# Security news stories...

Yahoo's 2013 Data Breach Aff... 

## **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 company didn't disclose the names of their victims. If you're one of the three billion people who have been compromised, you won't know if your account was breached or not.



# Security news stories...

A screenshot of a web browser window displaying 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 categorized under "The Switch". The author is Karen Turner, and it was published on September 7 at 3:40 PM. There is a link to "GET THE REPORT".

The Washington Post

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 [✉](#)

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

# Security news stories...

US to announce new sanctions x Jimmy

www.cnbc.com/2016/12/28/us-to-announce-new-sanctions-against-russia-in-response-to-election-hacking.html

POLITICS

POLITICS | ELECTIONS | PRESIDENTIAL DEBATES 2016 | WHITE HOUSE | CONGRESS | LAW | TAXES

## US to announce new sanctions against Russia in response to election hacking

Christine Wang | @christiiineeee

Wednesday, 28 Dec 2016 | 4:06 PM ET

CNBC



ALEXEI DRUZHININ | AFP | Getty Images

Russian President Vladimir Putin (L) meets with his US counterpart Barack Obama on the sidelines of the G20 Leaders Summit in Hangzhou on September 5, 2016.

The White House is preparing to announce retaliatory measures against

2.6K SHARES

Discover how Digital High Performers are reinventing their business.

> Learn more

accentureconsulting

FROM THE WEB

Sponsored Links by Taboola ▶



# 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' module, which is described as 'NXP i.MX 6UltraLite' with 'Low Power WiFi/Bluetooth Linux Windows Embedded'. The module is shown on a printed circuit board with a red diagonal banner that says 'from \$29'. The date 'SEP 6, 2016 @ 03:47 PM' and '10,503 VIEWS' are visible. A sidebar on the left has social sharing icons for Facebook, Twitter, and LinkedIn, and a 'SHARE >' button. The right sidebar includes a 'The Little Black Book of Billionaire Secrets' link 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 >

Google

Ok Google... Make a call

efus™A7UL

NXP i.MX 6UltraLite WiFi/Bluetooth eMMC

Low Power Linux Windows Embedded

Made in Germany

More Info

# Security news stories...

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

The browser title bar shows "Stuxnet Malware May Have T..." and the URL "www.esecurityplanet.com/headlines/article.php/3919111/article.htm".

The page header includes "January 17, 2011", "Hot topics : Desktop Security Network Security Trojans Malware Wpa Sec", "Free Newsletters : Security Daily", and navigation links for "eSecurityPlanet.com", "Security Headlines From Around the Web", and "All Security Headlines From Around the Web»".

A sidebar advertisement for Trend Micro Enterprise Security for Endpoints and Mail Servers is displayed, featuring the text "With customized security solutions, we can help keep you protected." and a price of "\$54.99".

The main content features a large headline "Stuxnet Malware May Have Taken Out 1,000 Centrifuges". Below it, a summary states: "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." A quote from Infosecurity follows: "In late 2009 or early 2010, Iran decommissioned and replaced 1000 IR-I centrifuges at Natanz," according to Infosecurity.

Text at the bottom left discusses the IAEA's support for the possibility of Stuxnet's responsibility.

At the bottom, a link encourages reading the full Infosecurity article.

Advertisement banners for CDW and ESET NOD32 Antivirus 4 are also visible.

# Security news stories...

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

- Title Bar:** FREAK: Another day, another serious SSL security hole
- Address Bar:** 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 menu options like 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 Content:**

## FREAK: Another day, another serious SSL security hole

More than one third of encrypted Websites are open to attack via the FREAK security hole.

By Steven J. Vaughan-Nichols for Networking | March 3, 2015 -- 22:19 GMT (22:19 GMT) | Topic: Security
- Call-to-Action:** Key Encryption Solutions (Simple & Secure Cryptography Tools. Free Key Encryption Whitepaper) with a green button containing a white arrow pointing right.
- Social Sharing:** Buttons for sharing the article on various platforms: a red speech bubble, blue Facebook, light blue Twitter, dark blue LinkedIn, a white envelope, and a white bell.

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](#)



# Security news stories...

A screenshot of a web browser window displaying an article from FCW (The Business of Federal Technology). The article is titled "Huge Heartbleed data theft logged". The page includes navigation links for Trending, Policy, Management, Exec Tech, Who & Where, The Hill, Agencies, Opinion, Resources, and Events. Social sharing buttons for LinkedIn, Facebook, Twitter, and Google+ are present. A sidebar on the right features an advertisement for SAS Analytics.

FCW Huge Heartbleed data theft

fcw.com/articles/2014/09/02/heartbleed-health-data-theft.aspx

About Us Advertise Contact Us Subscribe

Rising Star 2013 NSA Cyber Workforce FY2015

TRENDING: Rising Star 2013 NSA Cyber Workforce FY2015

in Share Like 16 Tweet g+1

Cybersecurity

## Huge Heartbleed data theft logged

By Mark Rockwell Sep 02, 2014

The FBI has warned health care providers and health IT device makers that they have been targeted in what appears to be one of the largest disclosed cyberattacks based on the Heartbleed Open SSL vulnerability that was uncovered last spring.

The FBI issued an unclassified but restricted warning to health care providers in mid-August in

FCW Huge Heartbleed data theft

fcw.com/articles/2014/09/02/heartbleed-health-data-theft.aspx

About Us Advertise Contact Us Subscribe

Rising Star 2013 NSA Cyber Workforce FY2015

TRENDING: Rising Star 2013 NSA Cyber Workforce FY2015

in Share Like 16 Tweet g+1

Cybersecurity

## Huge Heartbleed data theft logged

By Mark Rockwell Sep 02, 2014

The FBI has warned health care providers and health IT device makers that they have been targeted in what appears to be one of the largest disclosed cyberattacks based on the Heartbleed Open SSL vulnerability that was uncovered last spring.

The FBI issued an unclassified but restricted warning to health care providers in mid-August in

**sas** THE POWER TO KNOW.

### Analytics

Text analysis greatly improves the speed, efficiency and quality of government programs.

Read the paper

A photograph of a man in a dark suit and tie, sitting at a desk and working on a computer monitor. He is looking down at the screen. The background shows an office environment.

# Security news stories...

The screenshot shows a web browser window with the title "Extremely critical crypto flaw in iOS may also affect fully patched Macs" from arstechnica.com. The page content discusses a coding blunder that exposed sensitive data. On the right side of the page, there is a snippet of C code related to SSL/TLS handling. A red oval highlights two consecutive "goto fail;" statements in the code.

```
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;
```

**A critical iOS vulnerability that Apple patched on Friday gives a**

# 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

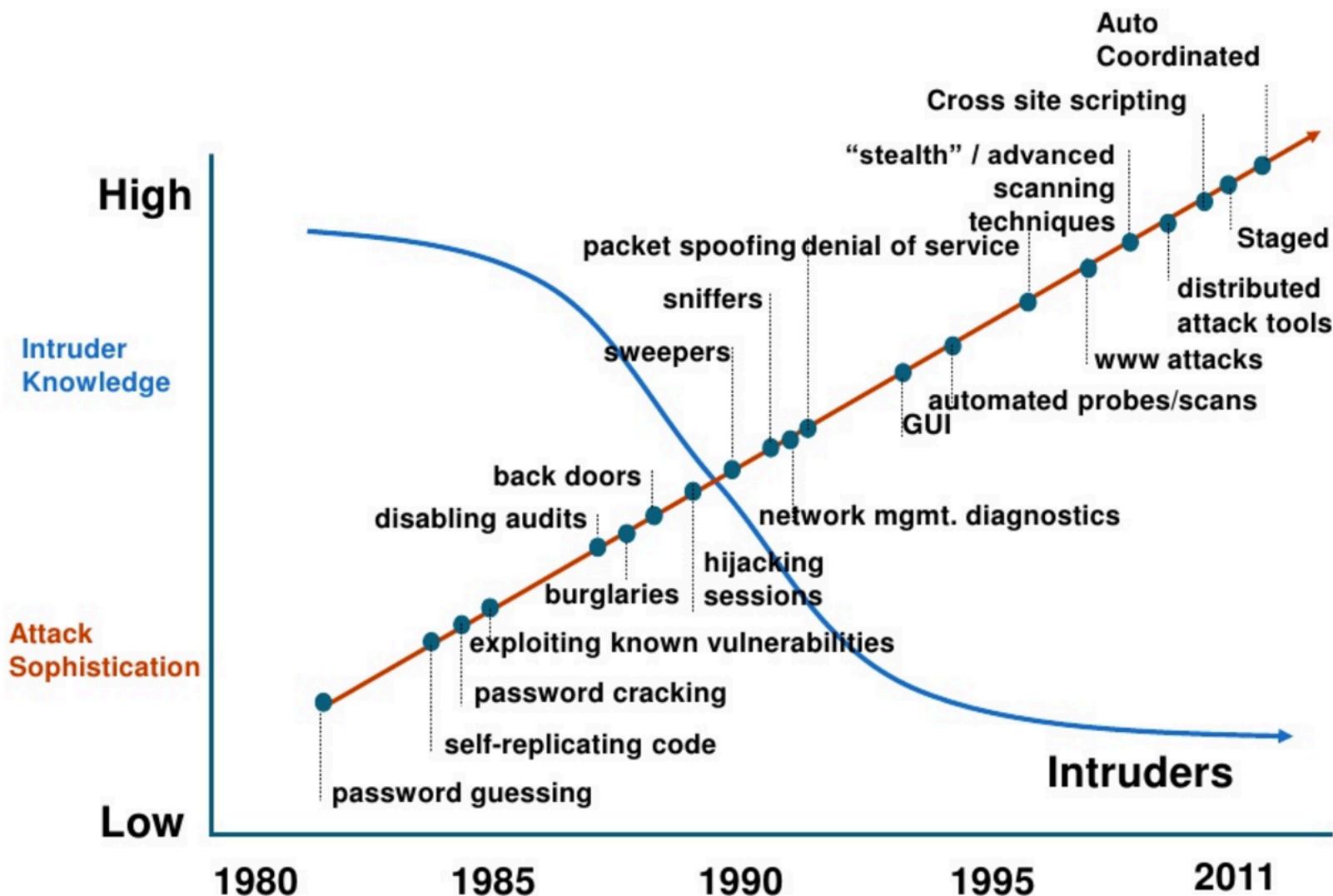
---

- 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

- 
- 2017-08-10 HP Client Automation Remote Code Execution and Stack **Buffer Overflow** Vulnerabilities
  - 2017-08-10 Microsoft Windows Server Service RPC Handling **Remote Code Execution** Vulnerability
  - 2017-08-10 Microsoft Internet Information Services CVE-2017-7269 Buffer Overflow Vulnerability
  - 2017-08-10 Oracle Java SE CVE-2017-10081 Remote Security Vulnerability
  - 2017-08-10 GNU Binutils 'bfd/elf.c' Remote Buffer Overflow Vulnerability
  - 2017-08-10 Mercurial Remote Command Injection and Symlink **Directory Traversal** Vulnerabilities
  - 2017-08-10 Git CVE-2017-1000117 Remote **Command Injection** Vulnerability
  - 2017-08-10 Apache Tomcat CVE-2017-7674 Security Bypass Vulnerability
  - 2017-08-10 RedHat CVS CVE-2017-12836 Command Injection Vulnerability
  - 2017-08-10 PostgreSQL CVE-2017-7546 **Authentication Bypass** Vulnerability
  - 2017-08-10 VMware NSX-V Edge CVE-2017-4920 **Denial of Service** Vulnerability
  - 2017-08-10 PostgreSQL CVE-2017-7547 **Information Disclosure** Vulnerability
  - 2017-08-10 Linux Kernel CVE-2017-1000111 Local **Privilege Escalation** Vulnerability
  - 2017-08-10 Apache Tomcat CVE-2017-7675 Directory Traversal Vulnerability
  - 2017-08-10 IBM Sterling B2B Integrator CVE-2017-1174 Unspecified **SQL Injection** Vulnerability
  - 2017-08-10 Symantec Messaging Gateway CVE-2017-6328 **Cross Site Request Forgery** Vulnerability
  - 2017-08-10 Microsoft ChakraCore CVE-2017-8658 Scripting Engine **Remote Memory Corruption**
- + more (on this day alone)

# Attack Sophistication vs. Intruder Technical Knowledge



---

# Main players in information security

# 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 recently
  - 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, ...