

# 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...

The image is a screenshot of a web browser displaying a CNN Tech article. The browser's address bar shows the URL: `money.cnn.com/2017/10/16/technology/wi-fi-flaw-crack-security/index.html`. The page header includes the CNN Tech logo and navigation links for BUSINESS, CULTURE, GADGETS, FUTURE, and STARTUPS. A social media sharing bar is visible with icons for Facebook, Twitter, Instagram, and Pinterest. Below the header is a BOMGAR advertisement for 'INSIGHT Remote Camera Sharing for iOS & Android' with a 'TRY FREE' button. The main article title is 'Wi-Fi network flaw could let hackers spy on you', with a sub-header 'Cyber-Safe'. The author is identified as Selena Larson (@selenalarson) and the article is dated October 16, 2017, at 3:49 PM ET. A video player is embedded in the article, showing a person's hands using a red and silver padlock. The video title is 'How to protect yourself from hackers'. To the right of the video is a 'Social Surge - What's Trending' section with three items: '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 of the page, there is a Samsung advertisement for 'AddWash with EcoBubble technology'.

Wi-Fi network flaw could let hackers spy on you

Cyber-Safe

by Selena Larson @selenalarson

October 16, 2017: 3:49 PM ET

Recommend 1.1K

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

How to protect yourself from hackers

0:00 / 0:30

Your video will play in 00:30

AddWash with EcoBubble technology

# Security news stories...

The screenshot shows a web browser window displaying an NPR news article. The address bar shows the URL: [www.npr.org/2017/09/08/549373719/news-brief-mexico-earthquake-florida-evacuates-equifax-data-breach](http://www.npr.org/2017/09/08/549373719/news-brief-mexico-earthquake-florida-evacuates-equifax-data-breach). The page features a video player with a play button icon and a duration of 10:21. Below the video player are options for '+ Queue', 'Download', 'Embed', and 'Transcript'. The article title is 'News Brief: Mexico Earthquake, Florida Evacuates, Equifax Data Breach', dated September 8, 2017, at 5:15 AM ET, and is attributed to Greg Allen. The main text of the article begins with '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.' Below the text is a 'Transcript' section, which starts with '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.' On the right side of the page, there is a promotional banner for the TV show 'Endeavour: Season Four', available on Amazon, and a PBS logo at the bottom.

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

U.S.

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:

ON AIR NOW  
NPR 24 Hour Program Stream

OUR PICKS | LIVE RADIO | SHOWS

ENDEAVOUR  
SEASON FOUR  
AVAILABLE AT  
amazon

PBS.

# Security news stories...

The screenshot shows a web browser window with the address bar displaying the URL: <https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for...>. The page features a navigation bar with links for 'sign in', 'become a supporter', 'subscribe', 'search', 'jobs', 'dating', 'more', and 'International edition'. The main navigation menu includes categories like 'UK', 'world', 'sport', 'football', 'opinion', 'culture', 'business', 'lifestyle', 'fashion', 'environment', 'tech', and 'travel'. The article title is 'WannaCry attacks prompt Microsoft to release Windows updates for older versions'. The sub-headline reads: 'The company typically releases security updates for operating systems it still supports - but in wake of serious cyber-attack it has reassessed the policy'. The article is by Alex Hern, dated Wednesday 14 June 2017, 12.26 BST. There are social media sharing icons and a note that the article is 2 months old. An advertisement for BOMGAR is visible at the top, and another for Purina Bakers dog food is at the bottom right.

Advertisement

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

theguardian

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

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

This article is 2 months old

< 267

Alex Hern

@alexhern

Wednesday 14 June 2017 12.26 BST

Advertisement

Bakers NOW WITH NO ADDED ARTIFICIAL COLOURS, FLAVOURS OR PRESERVATIVES

SAME GREAT Taste

PURINA Your Pet, Our Passion.

# Security news stories...



The image is a screenshot of a web browser window. The address bar shows the URL <https://mobileidworld.com/yahoo-data-breach-three-billion-accounts-010045/>. The page title is "Yahoo's 2013 Data Breach Affected Three Billion Accounts". The article is posted on October 4, 2017, by Alex Perala. The main text includes a quote: "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." Below this, the article states that Yahoo's 2013 data breach affected three billion accounts. It also mentions that the company initially announced that 200 million users' credentials had appeared for sale online, and later admitted that half a billion accounts had been compromised. The article concludes by stating that there are silver linings, one being that the breach represents the entire account database.

Yahoo's 2013 Data Breach Affected Three Billion Accounts

Posted on October 4, 2017 by Alex Perala

**“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 illustration shows a central globe with several circular avatars of people's faces around it. Dotted lines connect the avatars to each other and to the globe, suggesting a network or data flow. The background is a light blue color with some faint binary code (0s and 1s) visible at the bottom.

# Security news stories...

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

- Browser Tab:** "wp Hacked Dropbox data of 68 mil x"
- Address Bar:** "https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million..."
- Page Header:** "The Washington Post" logo, a search icon, "Sections" menu, a notification bell, "Sign In", and "Subscribe" buttons.
- Advertisement:** A banner for Tableau with the text "GARTNER MAGIC QUADRANT FOR BUSINESS INTELLIGENCE & ANALYTICS" and a "GET THE REPORT" button.
- Section Header:** "The Switch" in blue, followed by the main headline "Hacked Dropbox data of 68 million users is now for sale on the dark Web" in large black font.
- Text:** "By Karen Turner September 7 at 3:40 PM" with an email icon.
- Image:** A close-up photograph of a smartphone screen, which is mostly blank and blue.

# 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

2.6K SHARES

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

Discover how Digital High Performers are reinventing their business.

> Learn more

accentureconsulting

### FROM THE WEB

Sponsored Links by Taboola





# Security news stories...

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

## Just One Photo Can Silently Hack Millions Of Androids

**Thomas Fox-Brewster**, FORBES STAFF  
*I cover crime, privacy and security in digital and physical forms.* [FULL BIO](#)



efus™ A7UL  
NXP i.MX 6UltraLite  
WiFi/Bluetooth eMMC  
Low Power Linux  
Windows Embedded  
Made in Germany

 [More Info](#)

cookies on Forbes

# Security news stories...

The screenshot shows a web browser window with the address bar displaying [www.esecurityplanet.com/headlines/article.php/3919111/article.htm](http://www.esecurityplanet.com/headlines/article.php/3919111/article.htm). The page title is "Stuxnet Malware May Have Taken Out 1,000 Centrifuges". The article is dated January 4, 2011, and is written by eSecurityPlanet Staff. The main text states that a report from the Institute for Science and International Security (ISIS) indicates that the Stuxnet worm likely disabled approximately 1,000 centrifuges at Iran's Natanz uranium enrichment plant. A quote from the report is provided: "In late 2009 or early 2010, Iran decommissioned and replaced 1000 IR-1 centrifuges at Natanz," according to Infosecurity. The article also mentions that the ISIS report supports the possibility that Stuxnet was responsible for the Natanz centrifuges' disruption. A link is provided to read the full Infosecurity article.

January 17, 2011 Hot topics : Desktop Security Network Security Trojans Malware Wpa Sec

eSecurityPlanet.com Security Headlines From Around the Web All Security Headlines From Around the Web

**Outlook PST Backup Solution for the Enterprise:** Fast, secure, incrementally backs up PST files even if Outlook is open. Click here to learn more and get your free trial download for EdgeSafe PST2PST Backup now.

## 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-1 centrifuges at Natanz," [according to Infosecurity](#).

"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.

Free Newsletters : Security Daily

With customized security solutions, we can help you protected.

Trend Micro Enterprise Security for Endpoints and Mail Servers  
**\$54.99**

TREND MICRO

[Shop CDW »](#)

DEFEND YOUR NETWORK THE LATEST SECURITY

**Free Trial: ESET NOD32 Antivirus 4**  
ESET NOD32 Antivirus 4 protects your business by creating system slowdowns that negatively impact productivity. It is effective against emerging Internet threats as they are released, not hours later. Request your free trial today. >>

**10 Ways to Dodge Cyber Bullets**

# Security news stories...

The screenshot shows a web browser window with the URL [www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/](http://www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/). The browser's address bar and tabs are visible at the top. The ZDNet logo is in the top left corner of the page. A navigation bar contains links for CXO, HARDWARE, MICROSOFT, STORAGE, INNOVATION, APPLE, MORE, NEWSLETTERS, and ALL WRITERS. A 'JUST IN' banner at the top reads 'APPLE LAUNCHES IPAD PRO: PROMISES DESKTOP PERFORMANCE IN TABLET'. The main article title is 'FREAK: Another day, another serious SSL security hole'. Below the title is a sub-headline: 'More than one third of encrypted Websites are open to attack via the FREAK security hole.' The author is identified as Steven J. Vaughan-Nichols for Networking, with a date of March 3, 2015. A promotional banner for 'Key Encryption Solutions' is positioned below the article text, featuring a green arrow button. At the bottom of the page, there is a row of social media sharing icons (comment, Facebook, Twitter, LinkedIn, email, and a bell icon). The article text begins with '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'. A red sidebar advertisement for NSA is visible on the right side of the page.

EDITION: UK

ZDNet

CXO HARDWARE MICROSOFT STORAGE INNOVATION HARDWARE APPLE MORE NEWSLETTERS ALL WRITERS

JUST IN APPLE LAUNCHES IPAD PRO: PROMISES DESKTOP PERFORMANCE IN TABLET

## 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

Key Encryption Solutions

Simple & Secure Cryptography Tools. Free Key Encryption Whitepaper

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

NSA provides a complete range of standards, as well as certification.

NSAI

# Security news stories...

Huge Heartbleed data theft

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

FCW  
THE BUSINESS OF FEDERAL TECHNOLOGY

About Us Advertise Contact Us Subscribe

TRENDING: Rising Star 2013 NSA Cyber Workforce FY2015

POLICY MANAGEMENT EXEC TECH WHO & WHERE THE HILL AGENCIES OPINION RESOURCES EVENTS

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

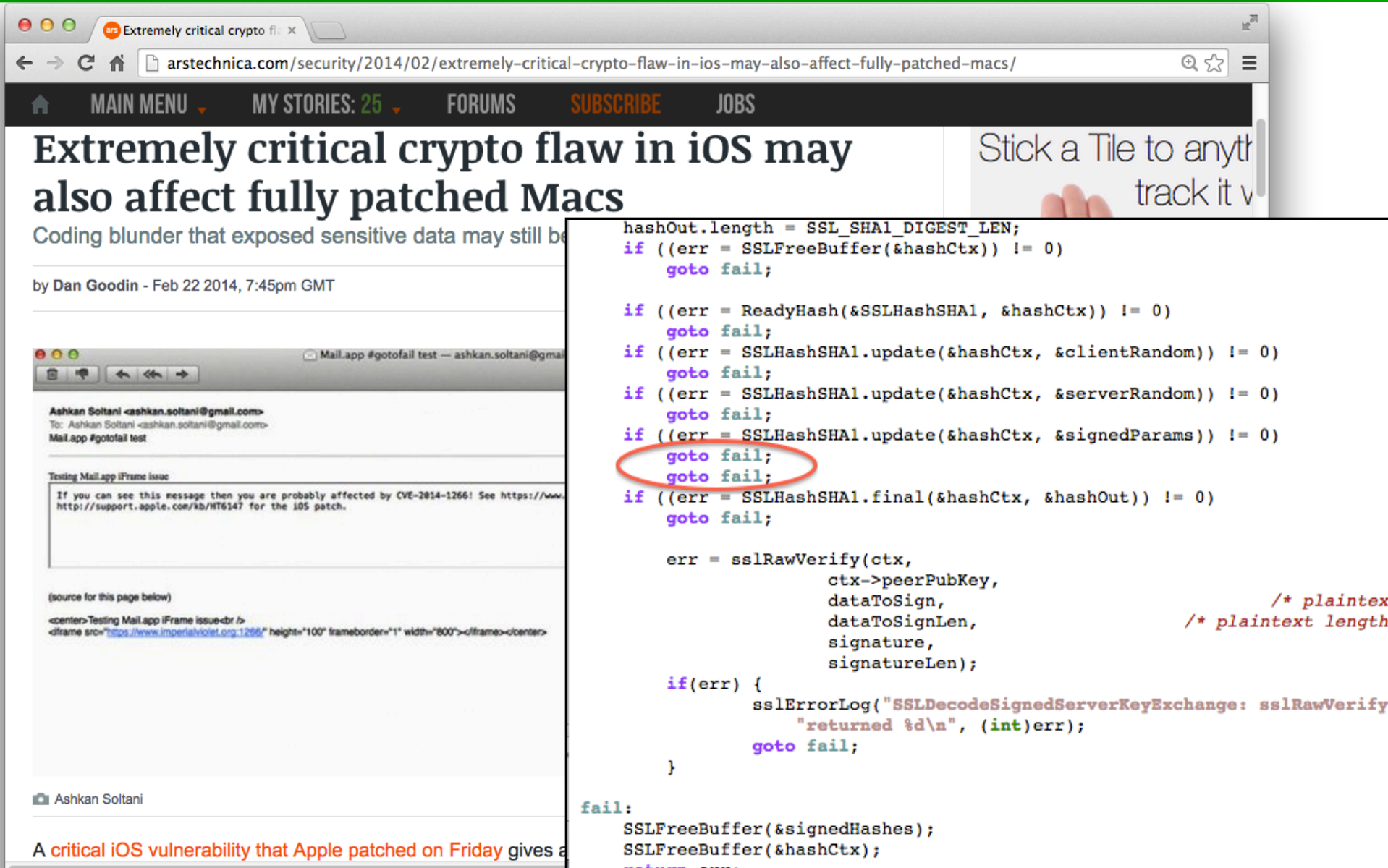
**sas** THE POWER TO KNOW.

### Analytics

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

Read the paper

# Security news stories...



The image shows a browser window with the URL `arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/`. The article title is "Extremely critical crypto flaw in iOS may also affect fully patched Macs". The author is Dan Goodin, dated Feb 22 2014, 7:45pm GMT. The article content includes a link to an email from Ashkan Soltani and a code snippet from a source file.

**Extremely critical crypto flaw in iOS may also affect fully patched Macs**  
Coding blunder that exposed sensitive data may still be

by Dan Goodin - Feb 22 2014, 7:45pm GMT

Ashkan Soltani <ashkan.soltani@gmail.com>  
To: Ashkan Soltani <ashkan.soltani@gmail.com>  
Mail.app #gotofail test

Testing Mail.app iFrame issue

If you can see this message then you are probably affected by CVE-2014-1266! See <https://www.imperialviolet.org/2014/02/22/apple/> or <http://support.apple.com/kb/HT6147> for the iOS patch.

(source for this page below)

```
<center>Testing Mail.app iFrame issue<br />
<iframe src="https://www.imperialviolet.org/2014/02/22/apple/" height="100" frameborder="1" width="800"></iframe></center>
```

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

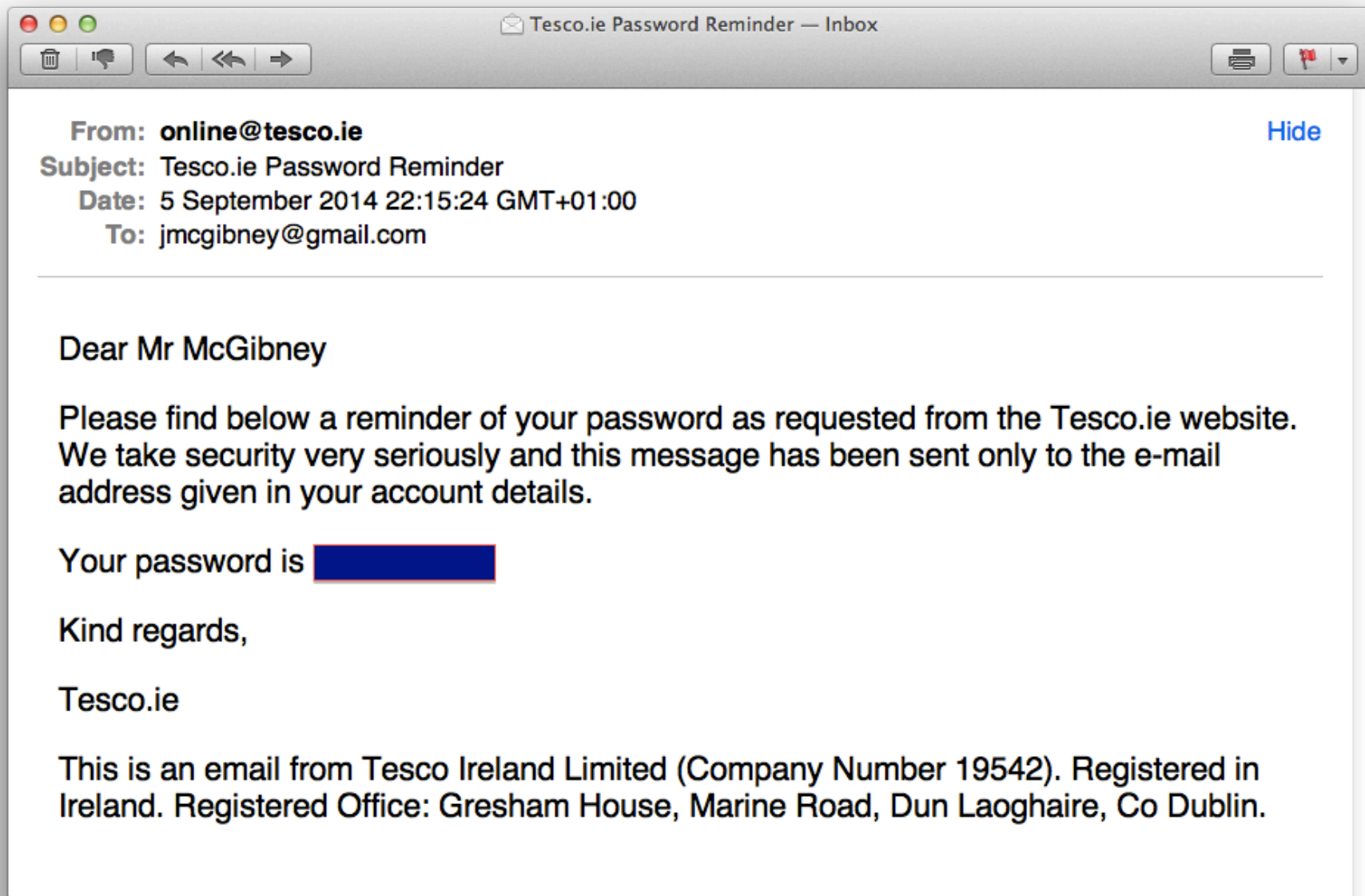
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
if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

err = sslRawVerify(ctx,
                  ctx->peerPubKey,
                  dataToSign,
                  dataToSignLen,
                  signature,
                  signatureLen);
/* plaintext
/* plaintext length

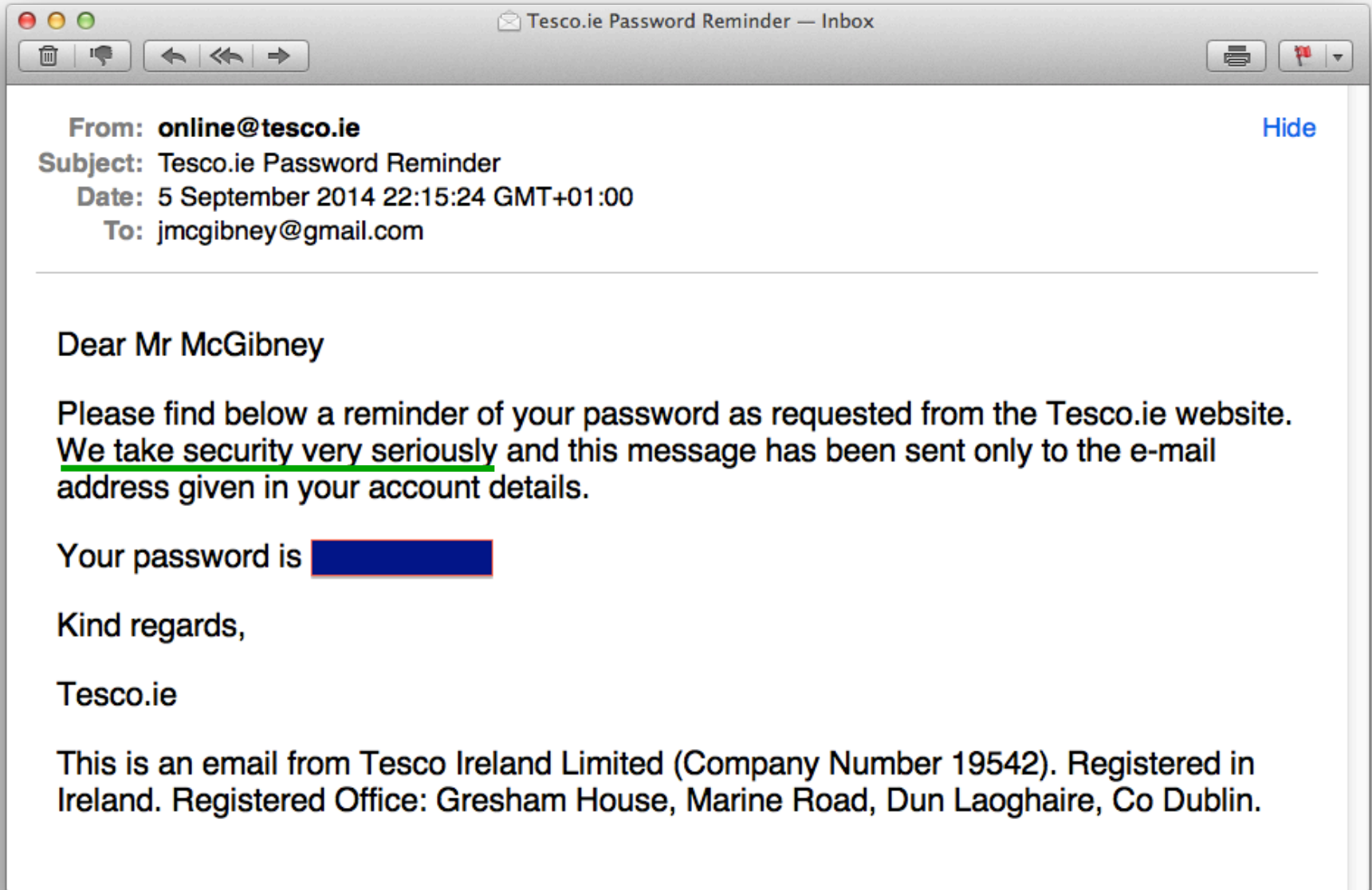
if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify
                "returned %d\n", (int)err);
    goto fail;
}

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

# Anything wrong with this?



# Anything wrong with this?



# 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

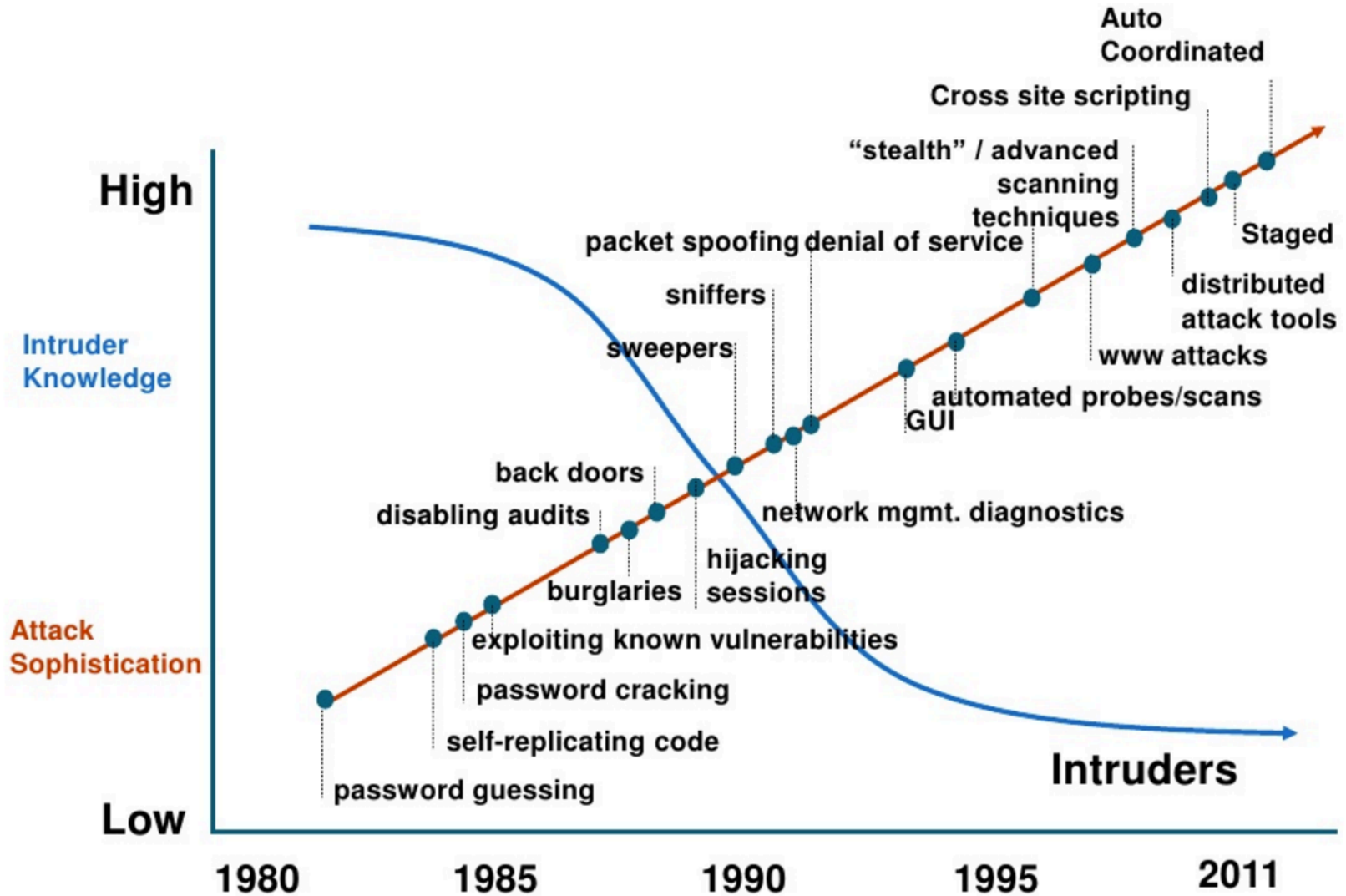
2017-08-10 IBM Sterling B2B Integrator CVE-2017-1174 Unspecified **SQL Injection** Vulnerability

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, ...