

Security part

1. Introduction to Security

Security part: 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

Setting the scene

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. The page is from the CNN Tech section, featuring a prominent advertisement for BOMGAR INSIGHT Remote Camera Sharing for iOS & Android. The main headline reads "Wi-Fi network flaw could let hackers spy on you" by Selena Larson (@selenalarson) on October 16, 2017, at 3:49 PM ET. A video player at the bottom indicates a duration of 00:30. To the right, there's a sidebar titled "Social Surge - What's Trending" with links to other news stories.

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

0:00 / 0:30

Your video will play in 00:30

BOMGAR INSIGHT Remote Camera Sharing for iOS & Android TRY FREE

Cyber-Safe

Facebook Recommend 1.1K Email Facebook Twitter LinkedIn More

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 SAMSUNG

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

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

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... 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 company didn't disclose the names of their victims. If you're one of the three billion people who have been affected, 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

[Twitter](#) [Facebook](#) [Reddit](#) [LinkedIn](#) [Email](#) [Print](#)

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 main content area is a Forbes article by Thomas Fox-Brewster. The article title is 'Just One Photo Can Silently Hack Millions Of Androids'. Below the title is a photo 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. The module is described as 'NXP i.MX 6UltraLite' with 'Low Power WiFi/Bluetooth', 'Linux', and 'Windows Embedded'. It is also noted as 'eMMC' and 'Made in Germany'. The advertisement includes a 'More Info' button and the F+S logo. On the left side of the article, there is a sidebar with social sharing icons for Facebook, Twitter, and LinkedIn, and a 'SHARE >' button.

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](#) ▾

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

F+S

SHARE >

Just One Photo Can Silently Hack Millions Of Androids

10

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 Taken Out 1,000 Centrifuges" 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, showing a price of \$54.99 and a "TREND MICRO" logo.

A second sidebar advertisement for CDW features a "Shop CDW" button.

The main content area features a large headline: "Stuxnet Malware May Have Taken Out 1,000 Centrifuges". Below the headline is a summary text: "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." To the left of this text is a sidebar with author information: "January 4, 2011 By eSecurityPlanet Staff Submit Feedback » More by Author »".

Below the summary text is a quote: "In late 2009 or early 2010, Iran decommissioned and replaced 1000 IR-I centrifuges at Natanz," according to Infosecurity.

At the bottom of the page, there is a statement: "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.

At the very bottom, a link reads: "Click here to read the Infosecurity article."

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/. The page is from ZDNet, with a navigation bar including links for CXO, HARDWARE, MICROSOFT, STORAGE, INNOVATION, HARDWARE, APPLE, MORE, NEWSLETTERS, ALL WRITERS, and a user profile. A banner at the top reads "JUST IN APPLE LAUNCHES IPAD PRO: PROMISES DESKTOP PERFORMANCE IN TABLET". The main headline is "FREAK: Another day, another serious SSL security hole". Below it, a sub-headline states "More than one third of encrypted Websites are open to attack via the FREAK security hole." The author is Steven J. Vaughan-Nichols, and the date is March 3, 2015. At the bottom of the article, there are social sharing icons for comments, Facebook, Twitter, LinkedIn, email, and a 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, looking at a computer monitor. He is wearing glasses and has short hair. The monitor is white and appears to be a flat-panel screen. The background is slightly blurred, showing an office environment.

Security news stories...

The screenshot shows a web browser window with the title bar "Extremely critical crypto fl...". The address bar contains the URL "arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/". The page content includes a main menu, forums, subscribe, and jobs links. The main headline is "Extremely critical crypto flaw in iOS may also affect fully patched Macs". Below the headline is a sub-headline "Coding blunder that exposed sensitive data may still be" and a byline "by Dan Goodin - Feb 22 2014, 7:45pm GMT". To the right of the headline is a sidebar with the text "Stick a Tile to anyth..." and "track it v".

On the left side of the page, there is a screenshot of a Mac Mail application window. It shows an email message from "Ashkan Soltani <ashkan.soltani@gmail.com>" to "Ashkan Soltani <ashkan.soltani@gmail.com>". The subject is "Mail.app #gotofail test". The message body contains the text "Testing Mail.app iFrame issue" and "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." Below the message is a note "(source for this page below)" and a center tag containing "Testing Mail.app iFrame issue
<iframe src='https://www.imperialviolet.org/1266/' height='100' frameborder='1' width='800'></iframe></center>".

On the right side of the page, there is a large block of C code. A red oval highlights two consecutive "goto fail;" statements:

```
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.

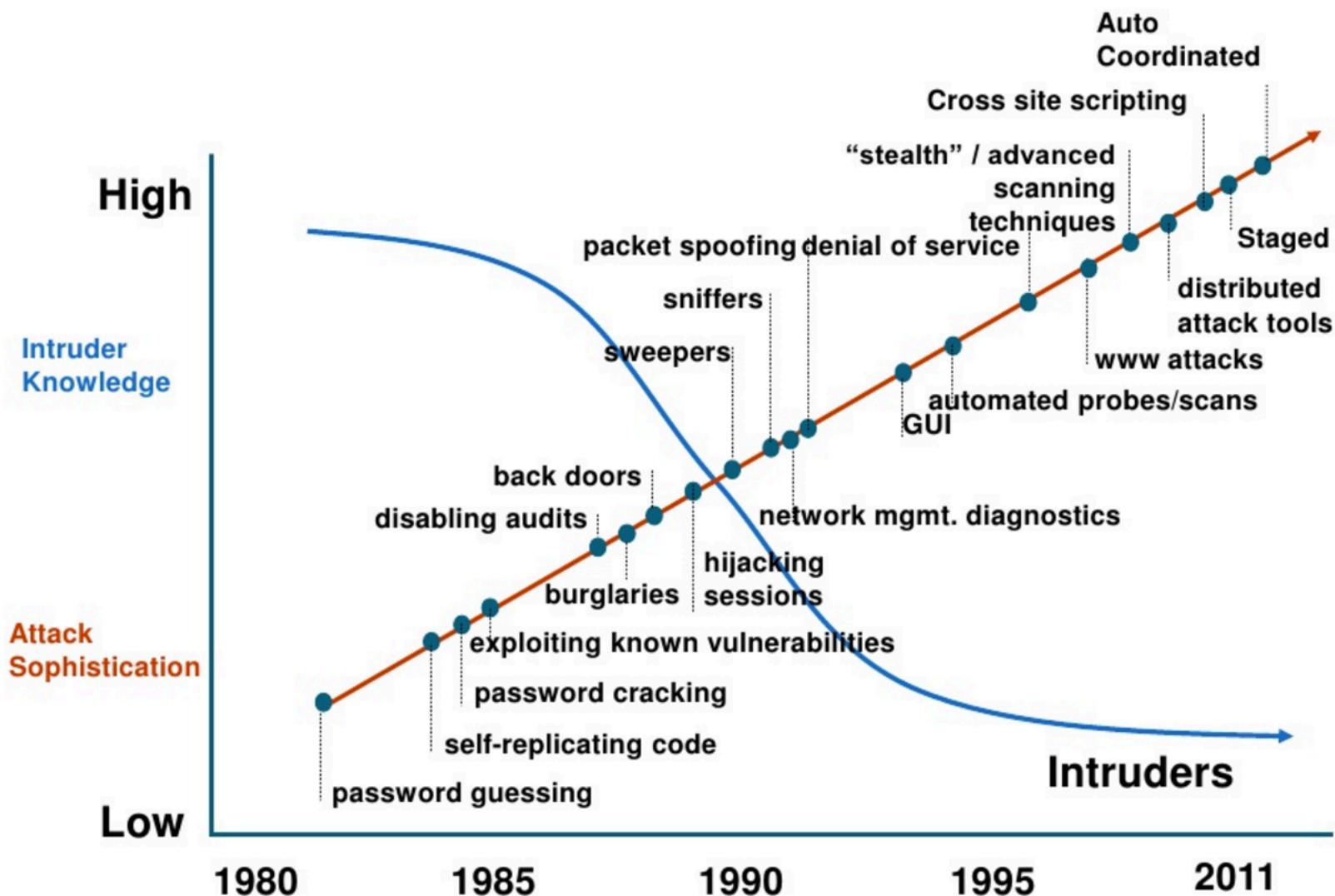
Security in context

- 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

-
- 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



Vulnerabilities & Attacks

Vulnerabilities

- Vulnerabilities appear everywhere in the stack
 - Modern systems are very large and complex
 - Impossible to test all possible use cases in advance
- Long history of
 - Network protocol vulnerabilities
 - OS vulnerabilities
 - Application vulnerabilities
 - Browsers, web servers, database mgmt systems, mail programs
 - Web apps (see OWASP Top 10)
 - Mobile apps
- Also non-technical vulnerabilities”
 - Social engineering
 - Illness, loss of personnel
 - Power failure, comms problems, fire, flood, earthquake, ...

Human vulnerabilities (Social Engineering)

- Social engineering is the practice of manipulating legitimate users
- Users are tricked into providing passwords or other secrets or allowing the attacker to bypass security
- Can be very effective
 - Typically tried in bulk on a large number of users in the hope that a few users will fall for it
 - Sometimes very subtle
- Best defence is security awareness training
 - See SANS "Securing the Human" project:
 - <http://securingthehuman.sans.org/>

Malware: risks from insecure programs

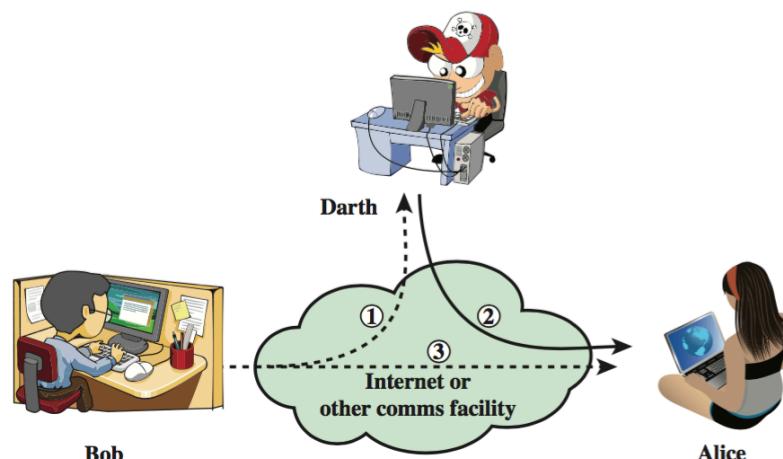
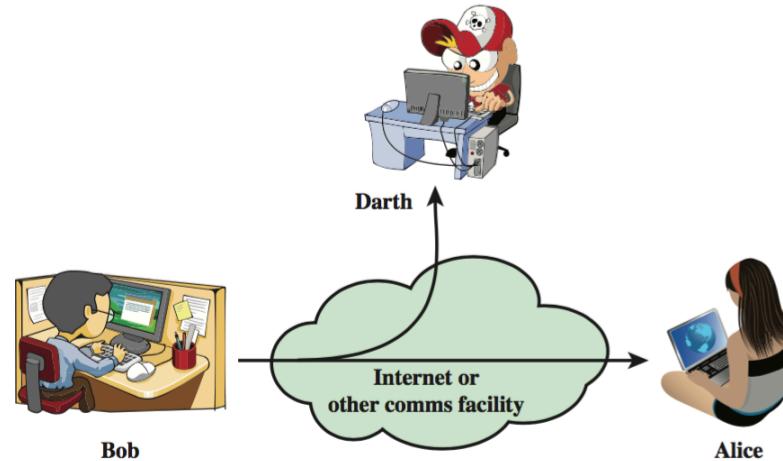
- Anything that can be executed on a machine may have all the rights and privileges of the user who is (directly or indirectly) executing it
- This may include
 - Read/write/modify/create/delete files or data
 - Reading from input devices (e.g. keyboard)
 - Writing to output devices
 - Interacting with the user
 - Administrative tasks like creating user accounts, opening/closing ports, launching other programs
 - Connection to other networked machines, file transfer, send emails, etc

Types of Attackers

- Opportunists
 - Typically scan wide range of addresses looking for system to exploit
 - For fun; to vandalise; to store pirated movies, music, etc
- Professionals
 - Industrial espionage; Fraud; Spam
- Activists
 - Political or social motivation
- Disgruntled current and former employees and contractors
 - May be able to bypass security measures – via legitimate accounts, accounts left open, back doors, etc
- Worms and automated agents
 - Malicious software

Classification of Attacks

- **Passive Attack**
 - Eavesdropping or monitoring to:
 - Obtain message contents, or
 - Monitor traffic flows
- **Active Attack**
 - Modification of data stream to:
 - Masquerade as someone else
 - Replay previous messages
 - Modify messages in transit
 - Denial of service
 - Break into system



Passive attack: Sniffing

- Sniffing on a network
 - Easy to do on broadcast LAN if attacker can get physical access to network point
 - Wireless LANs often have no encryption or broken encryption (e.g. WEP)
 - WAN security varies
- Keystroke logging
 - Keystroke logging software may be installed by virus or directly by attacker.
 - Alternatively, can insert small piece of hardware between keyboard and computer

KeyGhost USB KeyLogger : M X

www.keyghost.com/USB-Keylogger.htm

KEY GHOST

THE HARDWARE KEYLOGGER



Interface Security



We welcome

VISA

MasterCard

AMERICAN EXPRESS

Home - Site Map

[Home](#)

[Products](#)

[Reviews](#)

[Demonstration](#)

[Testimonials](#)

[Photos](#)

[Specifications](#)

[FAQ](#)

[Press releases](#)

[Download](#)

[Legal Disclaimer](#)

[Affiliates](#)

[Distributors](#)

KeyGhost USB Keylogger

World's first keylogger for Mac and PC USB keyboards.
Simply plug it in and record keystrokes.
Works with 100% of all USB keyboards!

NEW! TimeDate USB/HUB KeyGhost device released.

High-capacity and compact.
NEW! Plug-style USB KeyGhost devices released.

KeyGhost devices are always designed in consultation with leading law enforcement and government officials.

You can be certain that a KeyGhost product will always work as described.

NATO Classification Information
KeyGhost LTD (NATO supplier) NCAGE Code E1969

The plug-style KeyGhost USB devices look similar to USB Thumb Drives and record all keystrokes typed on any USB keyboard (Mac or PC).

NEW! QIDO - Qwerty to Dvorak USB Adapter.



Our latest development in



KeyGhost Headlines



KeyGhost USB Keylogger

"Customer satisfaction guaranteed" 12-Month Manufacturers Warranty.

[Order now](#)

27

Stages of an active attack – the five Ps

- Probe
- Penetrate
- Persist
- Propagate
- Paralyse

Stages of an attack – Probe

- Reconnaissance
 - Public information – Whois, DNS, target company website, search engines
 - Maltego
 - “Google hacking”
 - Social engineering
- Sniffing & scanning
 - Listen on broadcast (W)LANs; NetStumbler, Wireshark
 - Key logging
 - Network mapping
 - Port scanning; Nmap
 - Software version mapping
 - Vulnerability scanning

Stages of an attack – Penetrate

- **Finding secrets**
 - Password guessing & grinding (brute force cracking)
 - Malware (virus, Trojan, rootkit, etc)
- **Spoofing**
 - IP address / MAC address
- **Session hijacking**
- **DNS cache poisoning**
- **Malformed input**
 - Buffer overflows, format string attacks, ...
- **Web app attacks**
 - SQLi, XSS, CSRF, ...
- **All of the above; Metasploit framework**

Stages of an attack – Persist

- Having gone to the trouble of breaking in, the attacker wants to get back in easily
- Back door for remote control
 - Install small service listening on port and providing access (e.g a shell)
 - or else a small client that “dials out”
- Trojan horse
 - Malicious software often disguised as something innocuous
- Rootkit
 - Trojan suite that hides itself by suppressing logging and monitoring tools
- Covert channels
- Steganography

Stages of an attack – Propagate

- Use newly compromised system as the source of further attacks – more sniffing and scanning (see “Probe”)
- Map internal network from compromised machine.
- Often internal resources are configured to trust each other, making it easier to attack.

Stages of an attack – Paralyse

- The attacker does some damage – stealing or destroying data, bringing systems down, etc.
- Access confidential data
 - By sniffing, malformed input, web app attacks, etc (see “Probe”, “Penetrate”)
- Integrity breach
 - Modify/corrupt data
- Denial of Service (DoS)
 - where one user takes up so much of a shared resource that little or none of the resource is left for others.
 - These resources can be CPU time, disk space, OS processes, network bandwidth, or even someone’s time.
 - Examples: Amplifier attacks, Distributed DoS

Security Services

Understanding security

- For clear thinking, it is useful to separate the following:

Threat (potential security breach)



Service (measure to deal with this threat)



Mechanism (means to provide a service)



Technology (implementation of mechanism)



Deployment (configuration)



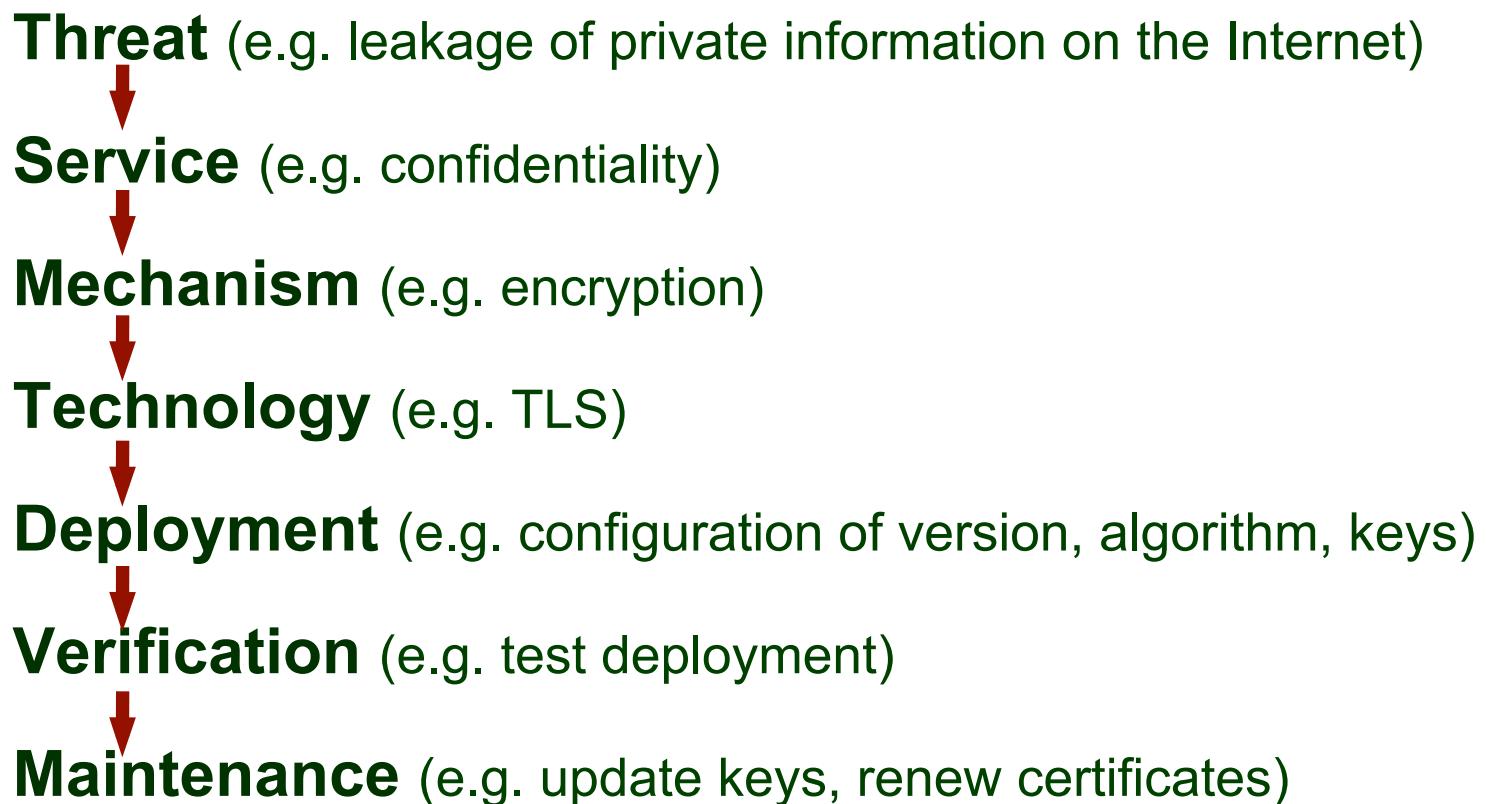
Verification (test if it works)



Maintenance (support & keep up to date)

Understanding security

- For clear thinking, it is useful to separate the following:



Security Services

- **Authentication**
 - Correct identification of entity or source of data
- **Access control**
 - Who can access what; in what way
- **Data confidentiality**
 - Non-disclosure to external parties
- **Data integrity**
 - “Correctness” of data
- **Non-repudiation**
 - Proof that communication or transaction took place
- **Availability**
 - Ensuring system available to users when required

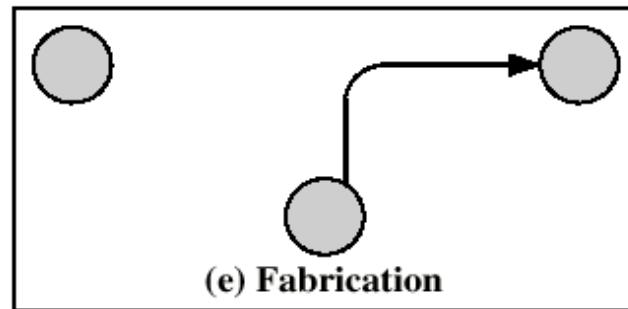
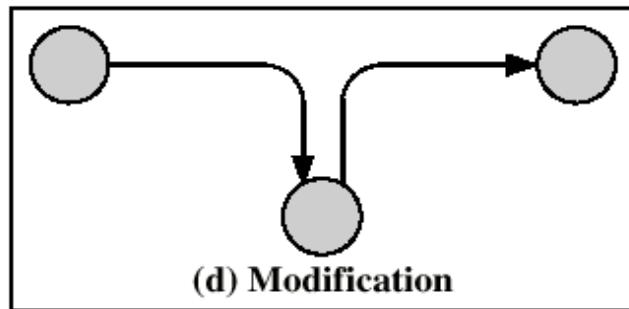
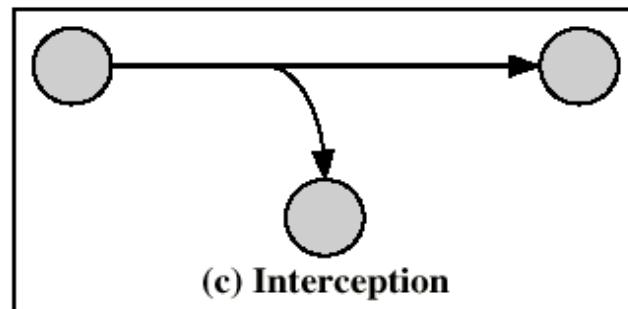
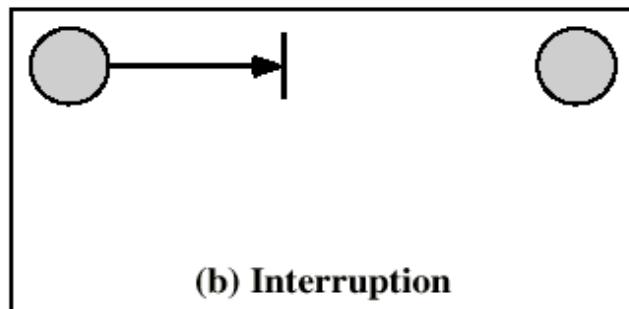
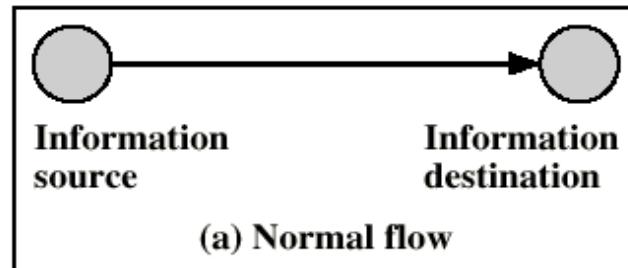
Mechanisms supporting services (examples)

- Authentication
 - Passwords; biometrics
- Access control
 - File permissions
- Data confidentiality
 - Encryption; traffic padding
- Data integrity
 - Message digests; checksums
- Non-repudiation
 - Digital signatures
- Availability
 - Replication of data and services; Backup systems

Attacks on Communications

- Interruption
 - Cutting a communication line
- Interception
 - Unauthorised party gains access
- Modification
 - Unauthorised party gains access and tampers
- Fabrication
 - Unauthorised party masquerades as an authorised party

Attacks on Communications



Exercise

- Consider the 4 communications security attack types shown on the previous 2 slides (interruption, interception, modification, fabrication)
- Match each of these four attack types with a security service designed to prevent it.
- Also suggest a mechanism/technology that would realise this service

Main players

Main Players in Computer 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, ...