

# 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...

Yahoo says 500 million accounts stolen

by Seth Fiegerman @sfiegerman

September 23, 2016: 10:39 AM ET

**Yahoo says information from at least 500 million accounts has been stolen**

Yahoo (YHOO, Tech30) confirmed on Thursday data "associated with at least 500 million user accounts" have been stolen in what may be one of the largest cybersecurity breaches ever.

The company said it believes a "state-sponsored actor" was behind the data breach, meaning an individual acting on behalf of a government. The breach is said to have occurred in late 2014.

**CNN Money Transfers**  
IT'S THE FAST, EASY,  
**SECURE**  
WAY TO SEND MONEY

Jimmy

Log In

THE DESTINATION INDONESIA www.indonesia.travel wonderful indonesia

20K

Social Surge - What's Trending

Trump campaign launches nightly 'newscast' on Facebook

New York Times buying The Wirecutter, and a new revenue stream

Nearly 10,000 people in China apply for one job

4

# 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 categorized under "The Switch". The author is Karen Turner, and it was published on September 7 at 3:40 PM. There is a "GET THE REPORT" button with a Gartner Magic Quadrant for Business Intelligence & Analytics advertisement above the article.

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

By Karen Turner September 7 at 3:40 PM

GARTNER MAGIC QUADRANT FOR BUSINESS INTELLIGENCE & ANALYTICS

GET THE REPORT

# Security news stories...

BI Pegasus, from NSO Group, is s x

uk.businessinsider.com/pegasus-nso-group-iphone-2016-8?r=US&IR=T

Jimmy

BUSINESS INSIDER UK TECH

Q

## Inside 'Pegasus,' the impossible-to-detect software that hacks your iPhone

Paul Szoldra [✉](#) [Ñ](#) [%](#) [RSS](#) [Twitter](#) [g+](#)  
Aug. 26, 2016, 9:51 PM [4,506](#)

[FACEBOOK](#) [LINKEDIN](#) [TWITTER](#) [✉](#) [⎙](#)

---

- [Irish People Born Between 1941 an...](#) (Survey Compare)
- [The Secret You Need to Know Abo...](#) (BookBub)
- [See Why MVMT Is The Hottest Selli...](#) (MVMT)
- [Cheap Travel Insurance. Stop Payi...](#) (Excite Insurance)

Sponsored Links



### Popular Articles

by Taboola

---



Here's What The Average American Man Looks Like Compared To Men In Other...

---



Bill Gates made these 15 predictions in 1999 — it's scary how accurate he was

# Security news stories...

The screenshot shows a web browser window with the title bar "CSC Blackmail rising from Ashley" and the URL "www.csionline.com/article/2980631/data-breach/blackmail-rising-from-ashley-madison-breach.html". The page is from CSO magazine, featuring a large image of various letters from different sources. The main headline is "Blackmail rising from Ashley Madison breach". Below the headline is a quote: "Cyber criminals, always adaptable, are still attacking enterprises. But when the opportunities arise, they are getting personal as well". The author's name is Taylor Armerding.

Jimmy

www.csionline.com/article/2980631/data-breach/blackmail-rising-from-ashley-madison-breach.html

CSO

Most read:

Home > Data Protection > Data Breach

FEATURE

## Blackmail rising from Ashley Madison breach

Credit: [Keith Hall/modified](#)

Cyber criminals, always adaptable, are still attacking enterprises. But when the opportunities arise, they are getting personal as well

By [Taylor Armerding](#) | Follow

CSO | Sep 8, 2015 10:44 AM PT

MORE LIKE THIS

- Ashley Madison still a top lure for scammers and crooks
- Ashley Madison hack linked to suicide, spam, and public outrage
- Are your biggest security threats on the inside?
- If I buy a Chromebook and can't get to grips with OS can I convert to windows?

7

# Security news stories...

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

- Title Bar:** "Even NASA Got Infected W X" and "Jimmy".
- Address Bar:** "motherboard.vice.com/read/even-nasa-got-infected-with-cryptolocker-ransomware".
- Header:** "MOTHERBOARD" logo, "Watch" dropdown, "Sections" dropdown, search icon, and social sharing icons for Facebook, Twitter, and YouTube.
- Main Content:**
  - Section Header:** "Even NASA Got Infected With 'CryptoLocker' Ransomware"
  - Text:** "Written by LORENZO FRANCESCHI-BICCHIERAI" and "June 5, 2015 // 11:33 AM EST".
  - Text Content:** "Between September 2013 and June 2014, a virus known as CryptoLocker infected around 500,000 computers around the world. Designed to lock data on a victim's computer and hold it for ransom, it ended up extorting an estimated \$3 million from victims who agreed to pay rather than lose their files."
  - Text Content:** "Among those victims of Cryptolocker were two NASA computers, according to an internal document obtained by Motherboard."
  - Text Content:** "The ransomware virus infected a computer at the NASA Ames Research Center in California on October 23, 2013, resulting in the loss of access to NASA data," according to the document. It also hit another computer at the visitor center of the Kennedy Space Center in Florida two days later."

# 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".

The article 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." It also quotes: "In late 2009 or early 2010, Iran decommissioned and replaced 1000 IR-I centrifuges at Natanz," according to Infosecurity."

The bottom of the article summary includes a note: "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 bottom of the page, there is a call to action: "Click here to read the Infosecurity article."

On the right side of the page, there are two advertisements:

- A Trend Micro advertisement for "Enterprise Security for Endpoints and Mail Servers" priced at \$54.99, featuring the Trend Micro logo.
- A CDW advertisement with the text "Shop CDW ▶" and the CDW logo.

At the very bottom, there is a banner for ESET NOD32 Antivirus 4 with the text: "DEFEND YOUR NETWORK WITH THE LATEST SECURITY", "Free Trial: ESET NOD32 Antivirus 4", and "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
- 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 links for CXO, HARDWARE, MICROSOFT, STORAGE, INNOVATION, HARDWARE, APPLE, MORE, NEWSLETTERS, ALL WRITERS, and user profile.
- Section Header:** 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:** Red speech bubble, blue Facebook, light blue Twitter, dark blue LinkedIn, white envelope, and white 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...

A screenshot of a web browser window displaying a news article from FCW (The Business of Federal Technology). The title of the article is "Huge Heartbleed data theft logged". The article is by Mark Rockwell, dated Sep 02, 2014. The text discusses the FBI warning health care providers and IT device makers about a targeted cyberattack using the Heartbleed SSL vulnerability. A large red heart icon with a liquid dripping down is overlaid on the bottom left of the article. On the right side of the page, there is a sidebar advertisement for SAS Analytics, featuring a man in a suit working at a computer.

FCW Huge Heartbleed data theft

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

**TRENDING:** Rising Star 2013 NSA Cyber Workforce FY2015

About Us Advertise Contact Us Subscribe

in | in | f | g+ | t

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

A photograph of a man in a dark suit and tie, sitting at a desk and looking at a computer monitor. He is positioned next to a vertical advertisement for SAS Analytics.

# Security news stories...

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

- Title Bar:** "Extremely critical crypto fl..." (partially visible), "Extremely critical crypto fl...", "arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/", search, star, menu.
- Header:** MAIN MENU, MY STORIES: 25, FORUMS, SUBSCRIBE, JOBS.
- Main Content:** Article title "Extremely critical crypto flaw in iOS may also affect fully patched Macs", subtext "Coding blunder that exposed sensitive data may still be", author "by Dan Goodin - Feb 22 2014, 7:45pm GMT".
- Right Sidebar:** "Stick a Tile to anyth..." (partially visible).
- Code Block:** A large block of C-like code is displayed on the right side of the page. A red oval highlights two consecutive "goto fail;" statements at the beginning of a loop iteration. The code is as follows:

```
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);
    /* plaintext length */
```

**Left Side:** A sidebar shows a screenshot of the Mail.app interface with an email message from Ashkan Soltani. The message body contains a link to a test page: "Testing Mail.app iFrame issue<br /><iframe src='https://www.imperialviolet.org:1286/' height='100' frameborder='1' width='800'></iframe></center>". Below the message, it says "(source for this page below)" and "A critical iOS vulnerability that Apple patched on Friday gives a".

# 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 Header Links:** News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | Tech
- Breadcrumbs:** 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:** • 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'
- Share Buttons:** Facebook Share (2882), Twitter Tweet (10.9K), Google +1 (3.4k), 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
- Comment Link:** Jump to comments (4146)
- Article History:** Article history
- Page Footer:** World news

# 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

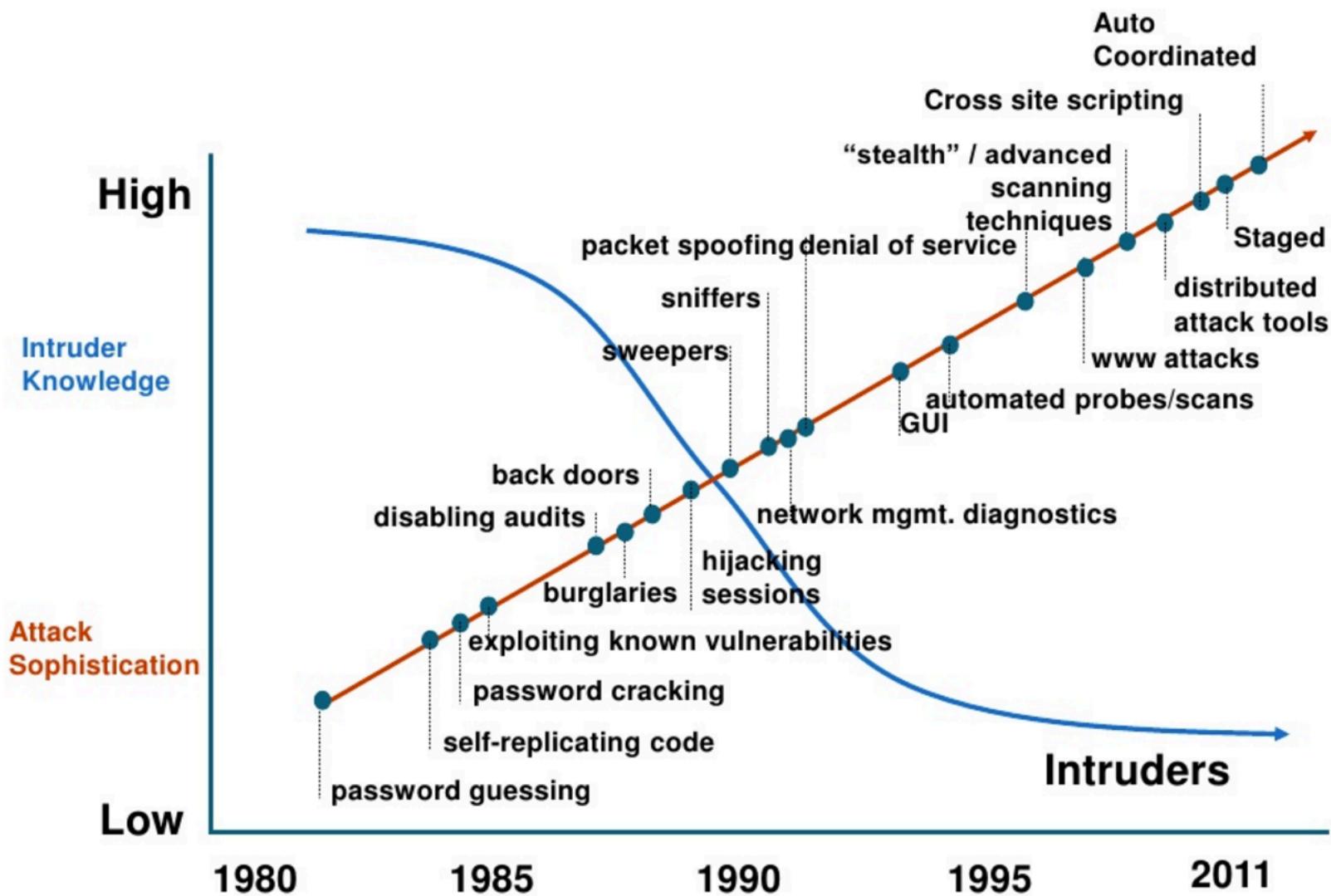
---

- 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

- 2016-09-06 Multiple IBM DB2 Products CVE-2016-0211 **Denial of Service** Vulnerability
- 2016-09-06 Apache Xerces-C CVE-2016-0729 **Buffer Overflow** Vulnerability
- 2016-09-06 OpenSSL Padding Oracle Incomplete Fix **Information Disclosure** Vulnerability
- 2016-09-06 Siemens EN100 Ethernet Module CVE-2016-7112 **Authentication Bypass** Vulnerability
- 2016-09-06 NTP CVE-2016-1550 **Local Security Bypass** Vulnerability
- 2016-09-06 NTP Symmetric Key Encryption Authentication Security Bypass Vulnerability
- 2016-09-06 Mozilla Network Security Services **Use After Free** Remote Code Execution Vulnerability
- 2016-09-06 SSL/TLS Protocol CVE-2016-2183 Information Disclosure Vulnerability
- 2016-09-06 cURL/libcURL CVE-2016-5420 **Certificate Validation Security Bypass** Vulnerability
- 2016-09-06 Inspircd SSL **Certificate Spoofing** Vulnerability
- 2016-09-06 Google Android CVE-2016-3875 Local **Privilege Escalation** Vulnerability
- 2016-09-06 Google Android libutils CVE-2016-3861 **Arbitrary Code Execution** Vulnerability
- 2016-09-06 Open Dental CVE-2016-6531 **Hardcoded Credentials** Security Bypass Vulnerability
- 2016-09-06 Dentsply Sirona CDR DICOM Hardcoded Credentials Security Bypass Vulnerability
- 2016-09-06 Multiple Kaspersky Products CVE-2016-4329 Local Denial of Service Vulnerability
- 2016-09-06 Red Hat JBoss BPMS CVE-2016-7033 Multiple HTML Injection Vulnerabilities
- 2016-09-06 Red Hat JBoss BPMS CVE-2016-7034 **Cross Site Request Forgery** Vulnerability
- 2016-09-06 cURL/libcURL CVE-2016-7141 Certificate Validation Security Bypass Vulnerability
- 2016-09-06 ADOdb CVE-2016-4855 **Cross Site Scripting** Vulnerability

# 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

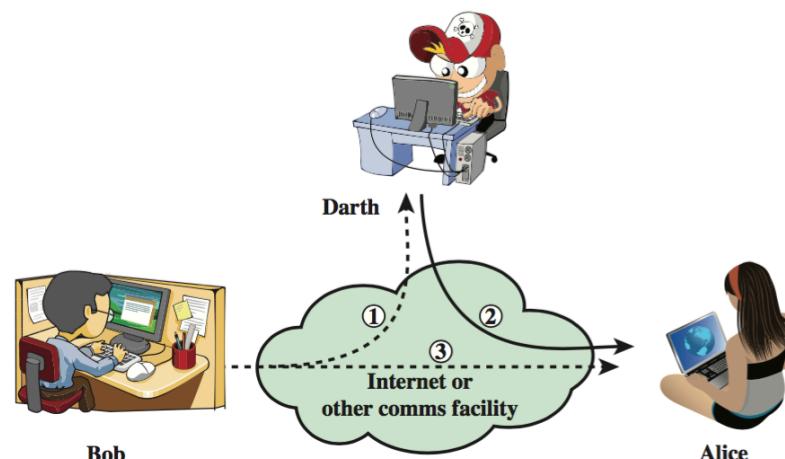
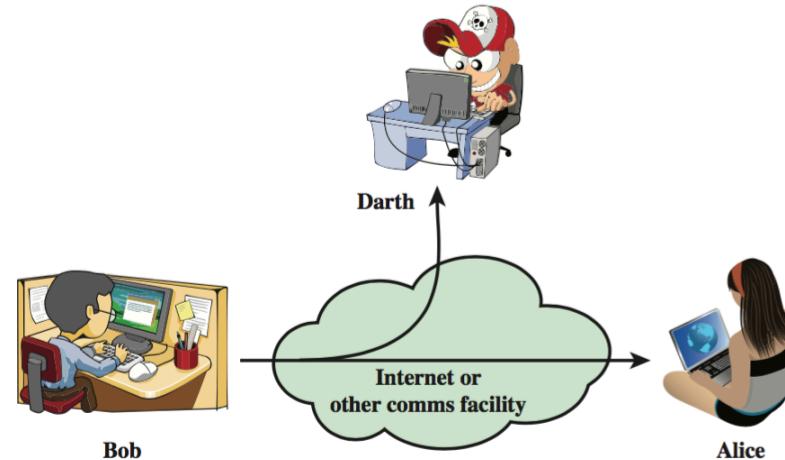
# Types of Attackers

---

- 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

[Ordering](#) [Customer Support](#) [Products](#) [Company Info](#) [Links](#) [Helpdesk](#)

We welcome

[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](#)

26

# 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)



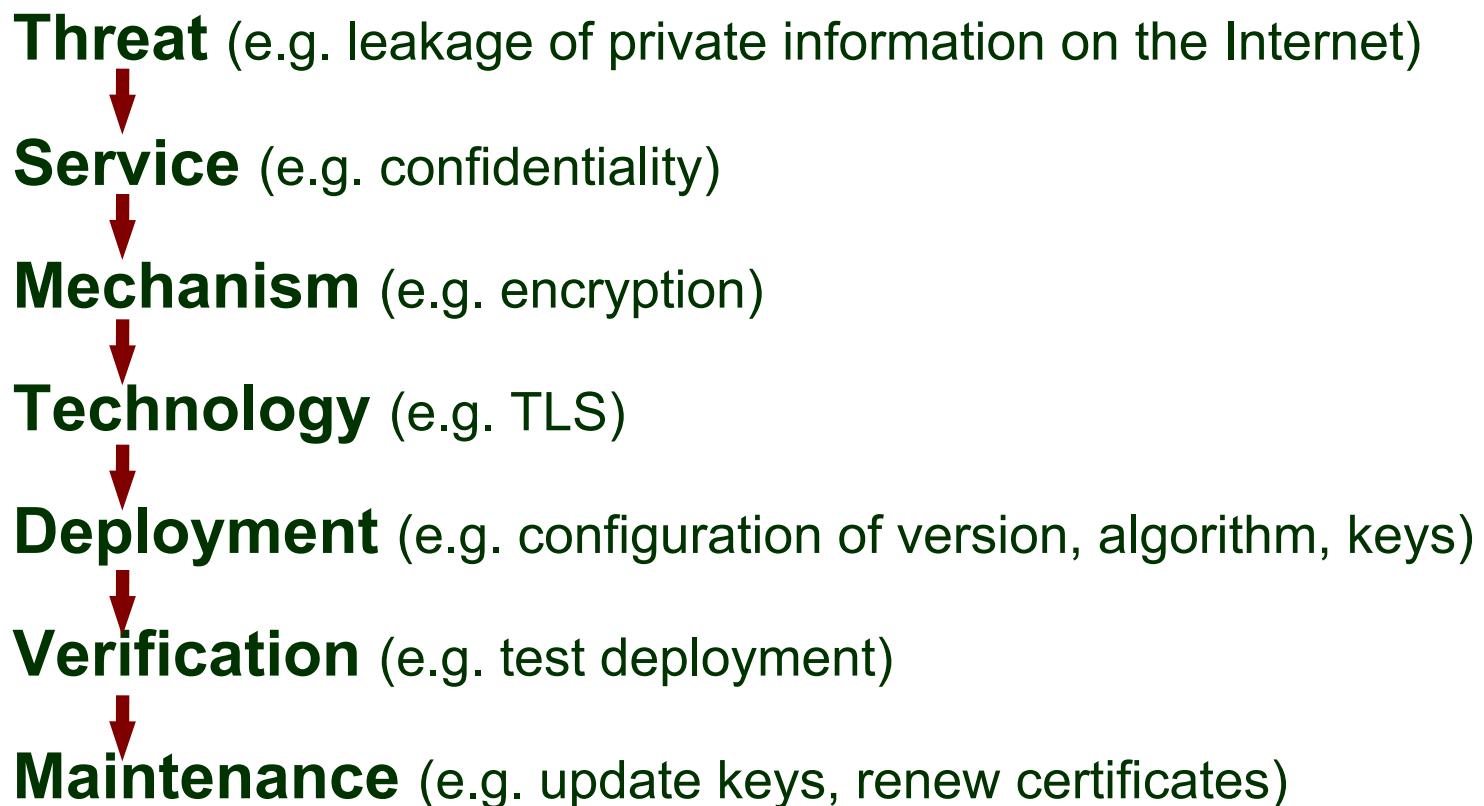
**Verification** (test if it works)



**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

# Exercise

---

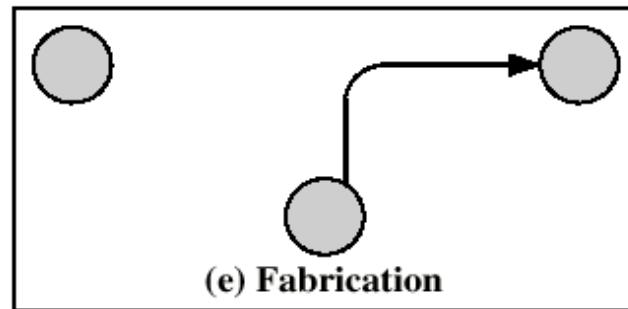
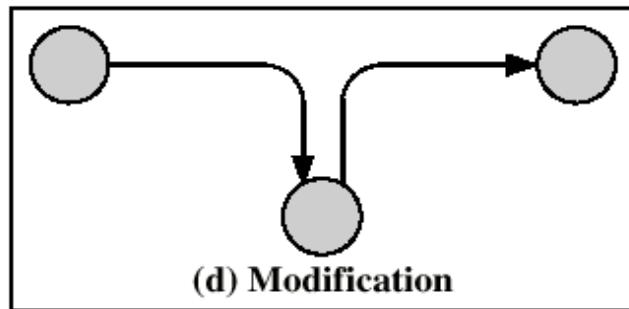
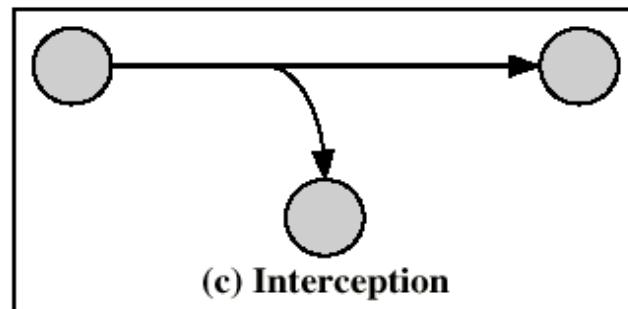
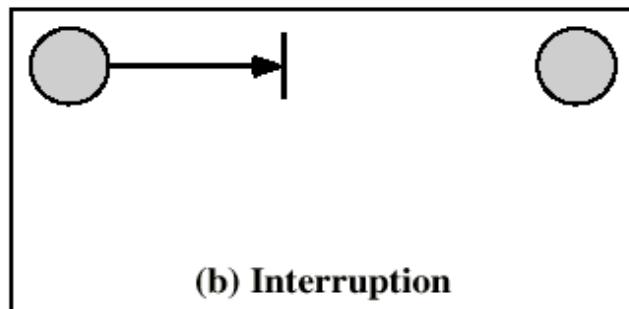
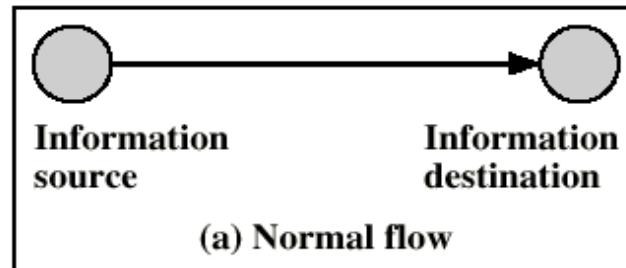
- Consider the 4 communications security attack types shown on the next 2 slides (interruption, interception, modification, fabrication)
- Match each of these four attack types with a security service designed to prevent it.
- Also suggest a mechanism/technology that would realise this service

# 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



---

# 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, ...