Security part

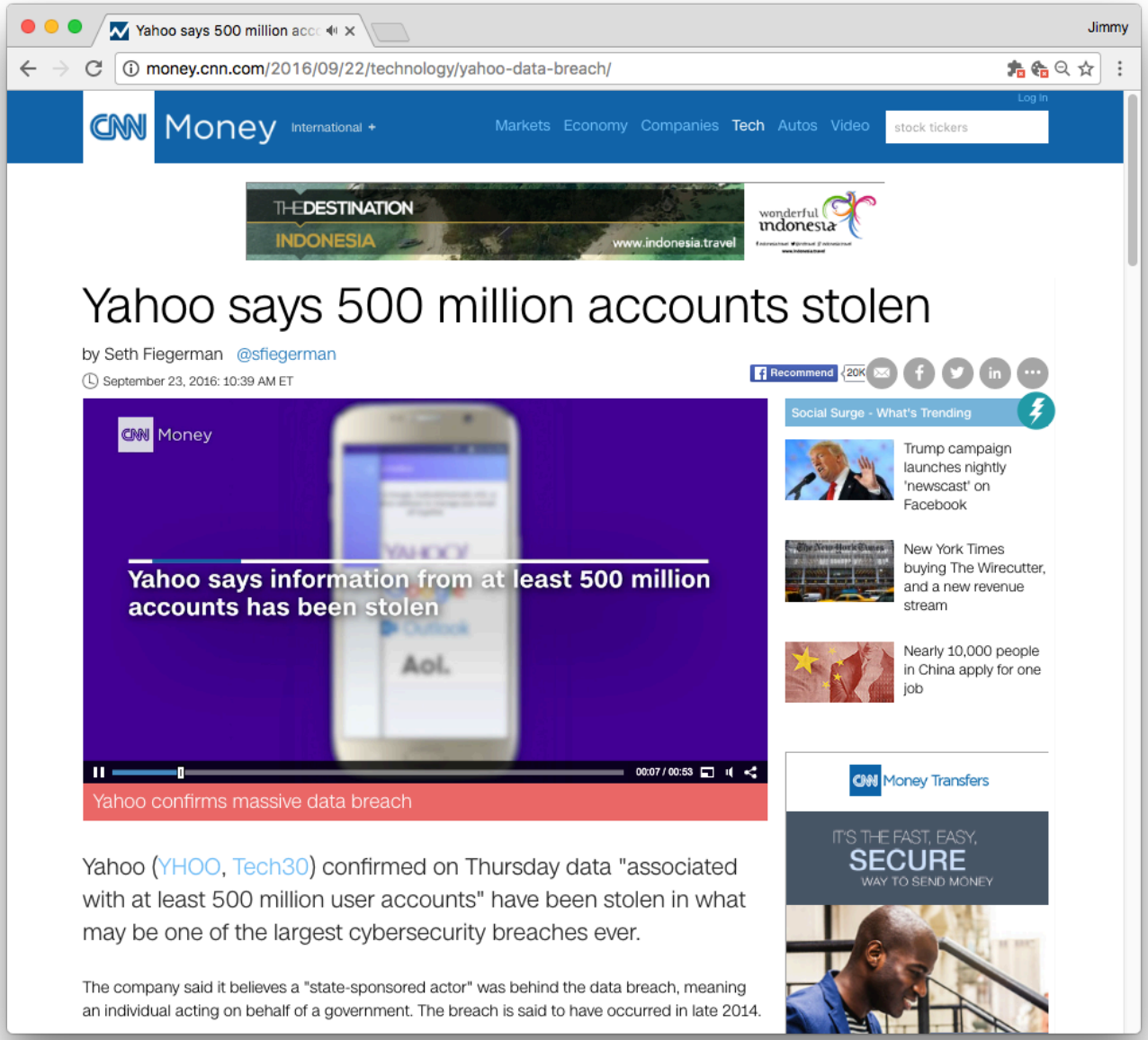
1. Introduction to Security

Security part: main topics

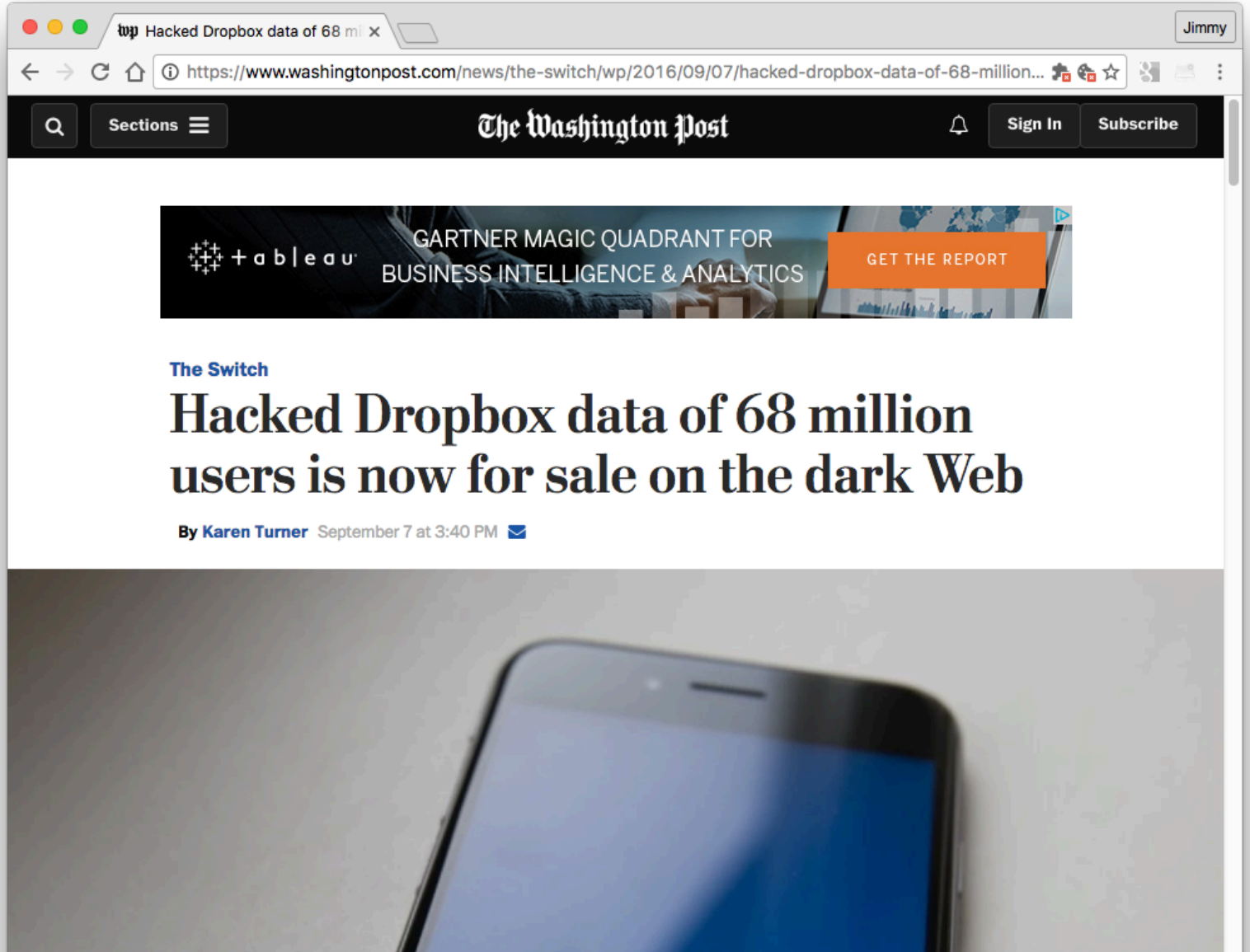
- Introduction
  - Threats, attacks, vulnerabilities; Security services
- Cryptography
  - Symmetric encryption
  - Public key cryptography
  - Authentication and integrity
  - Key management and certificates
- Web application threats and vulnerabilities
  - Common vulnerabilities
  - Penetration testing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

Setting the scene

Security news stories…



Security news stories…



Security news stories…

Pegasus, from NSO Group, is s

Jimmy

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

BUSINESS INSIDER UK TECH

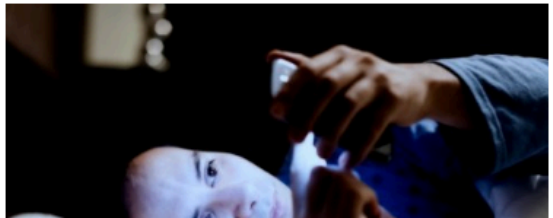
Inside 'Pegasus,' the impossible-to-detect software that hacks your iPhone

Paul Szoldra

Aug. 26, 2016, 9:51 PM 4,506

FACEBOOK LINKEDIN TWITTER

The hacking software that completely takes over an Apple iPhone and turns it into a mobile surveillance device is pretty terrifying.



Security news stories…

Blackmail rising from Ashle ×

Jimmy

www.csoonline.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

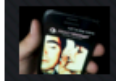
Credit: Keith Hall/modified

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

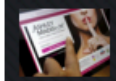
By Taylor Armerding | Follow

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

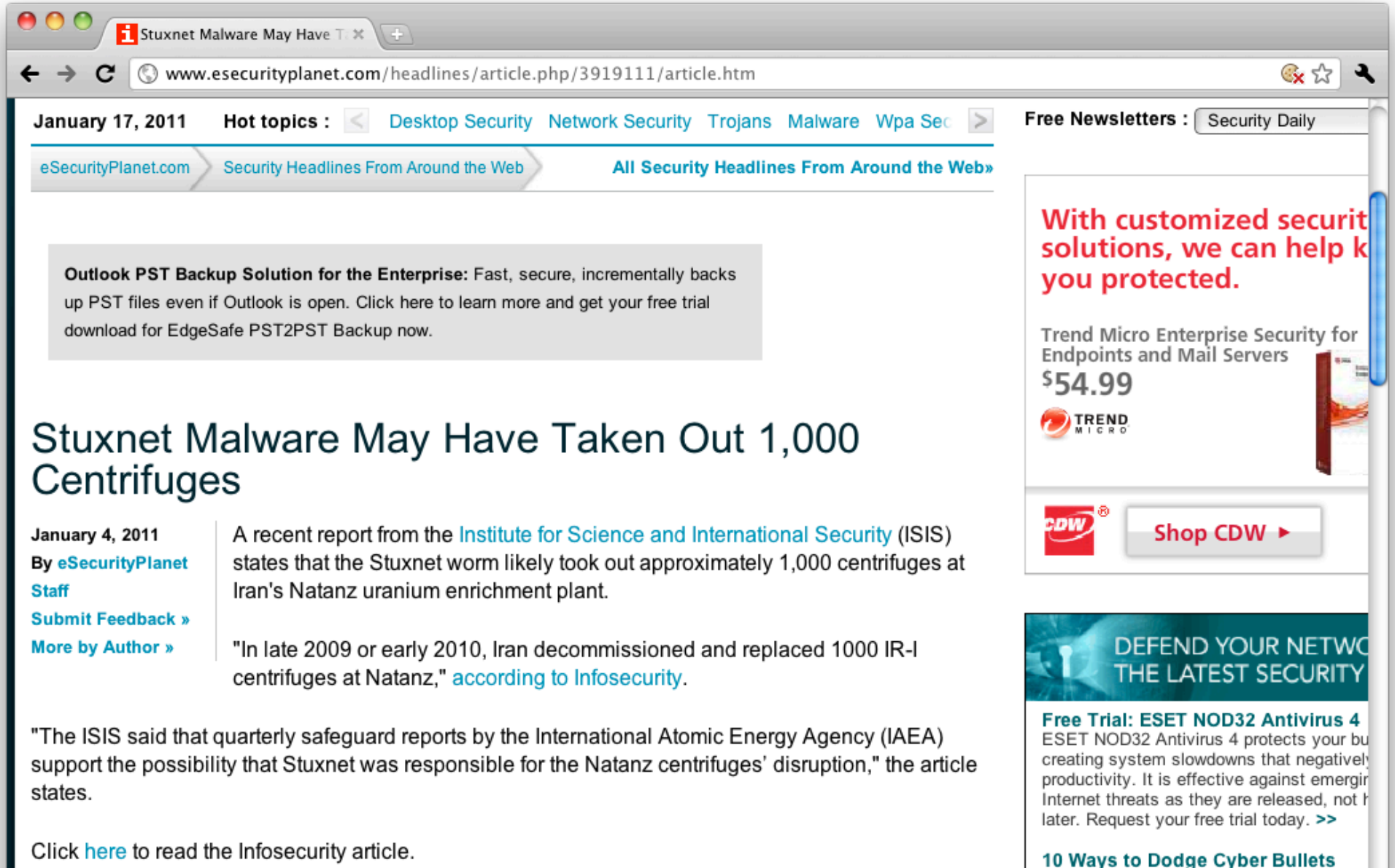
Are your biggest security threats on the inside?

on IDG Answers

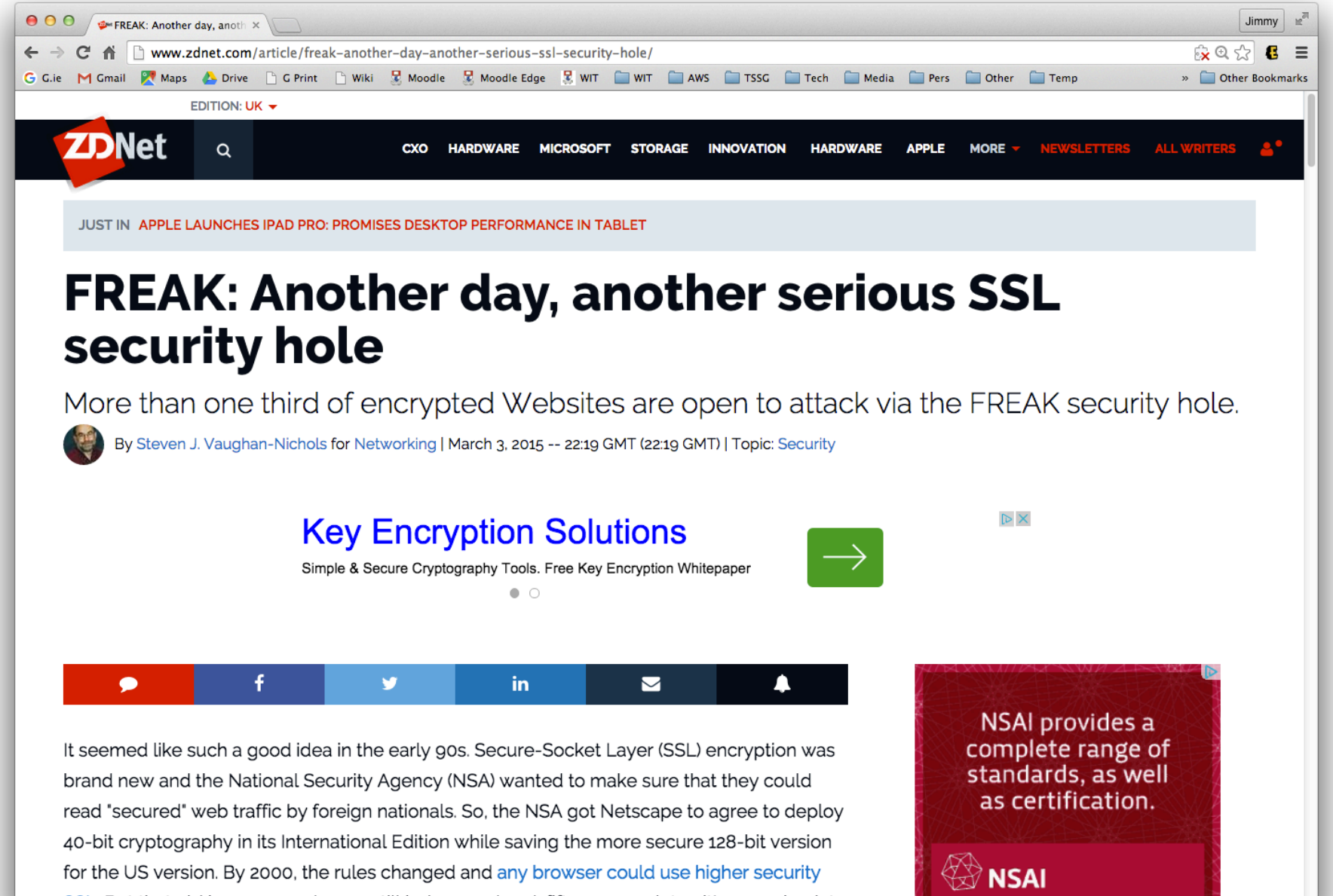
If I buy a Chromebook and can't get to grips with OS can I convert to windows?

Security news stories…

Security news stories…



Security news stories…



FREAK: Another day, anoth ×

Jimmy

www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/

G.ie Gmail Maps Drive G Print Wiki Moodle Moodle Edge WIT WIT AWS TSSG Tech Media Pers Other Temp Other Bookmarks

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

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…

Huge Heartbleed data thef ×

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

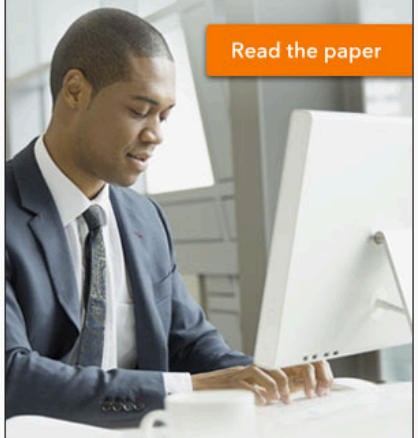
Cybersecurity

Huge Heartbleed data theft logged

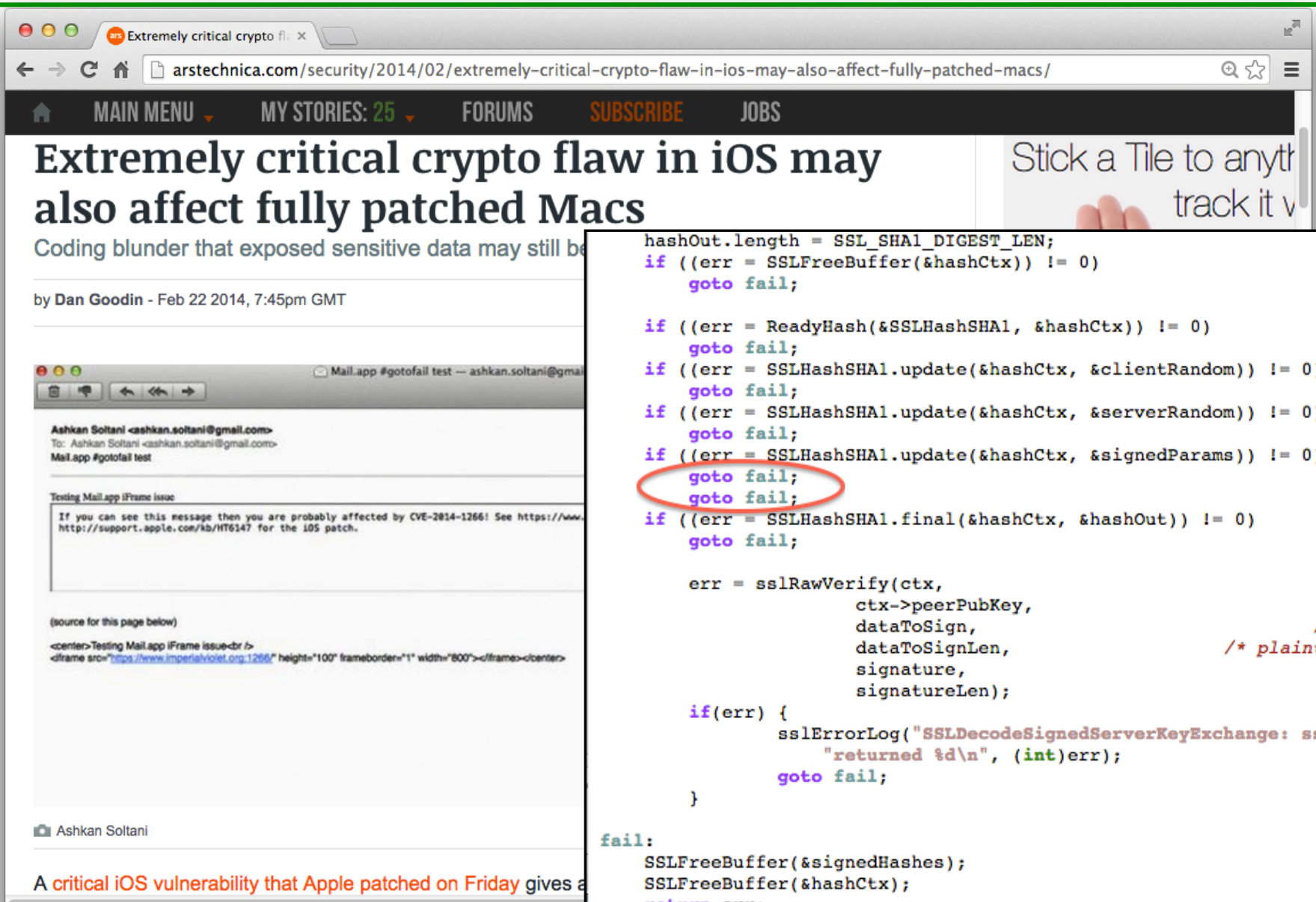
By Mark Rockwell Sep 02, 2014

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

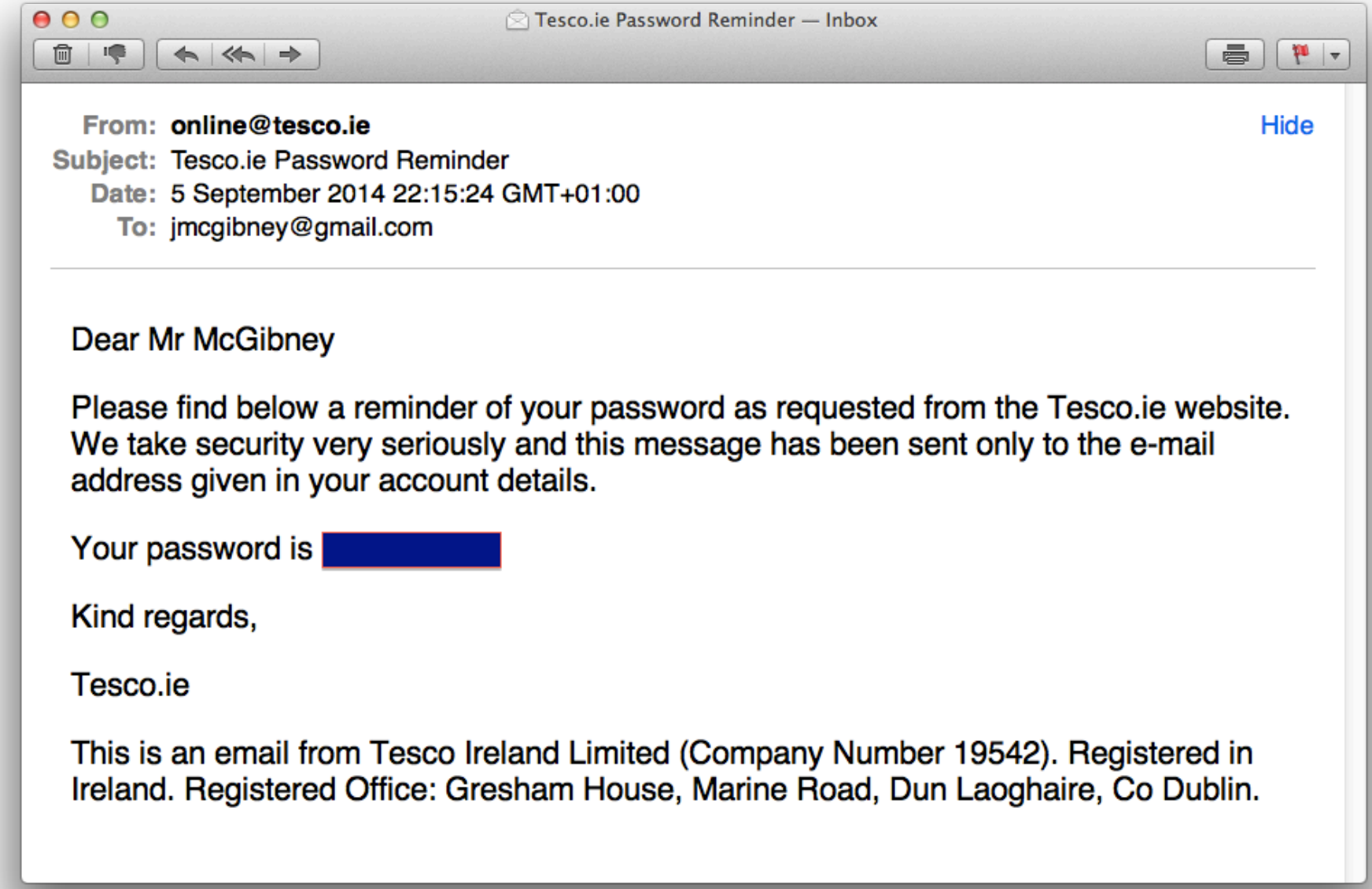


Security news stories…

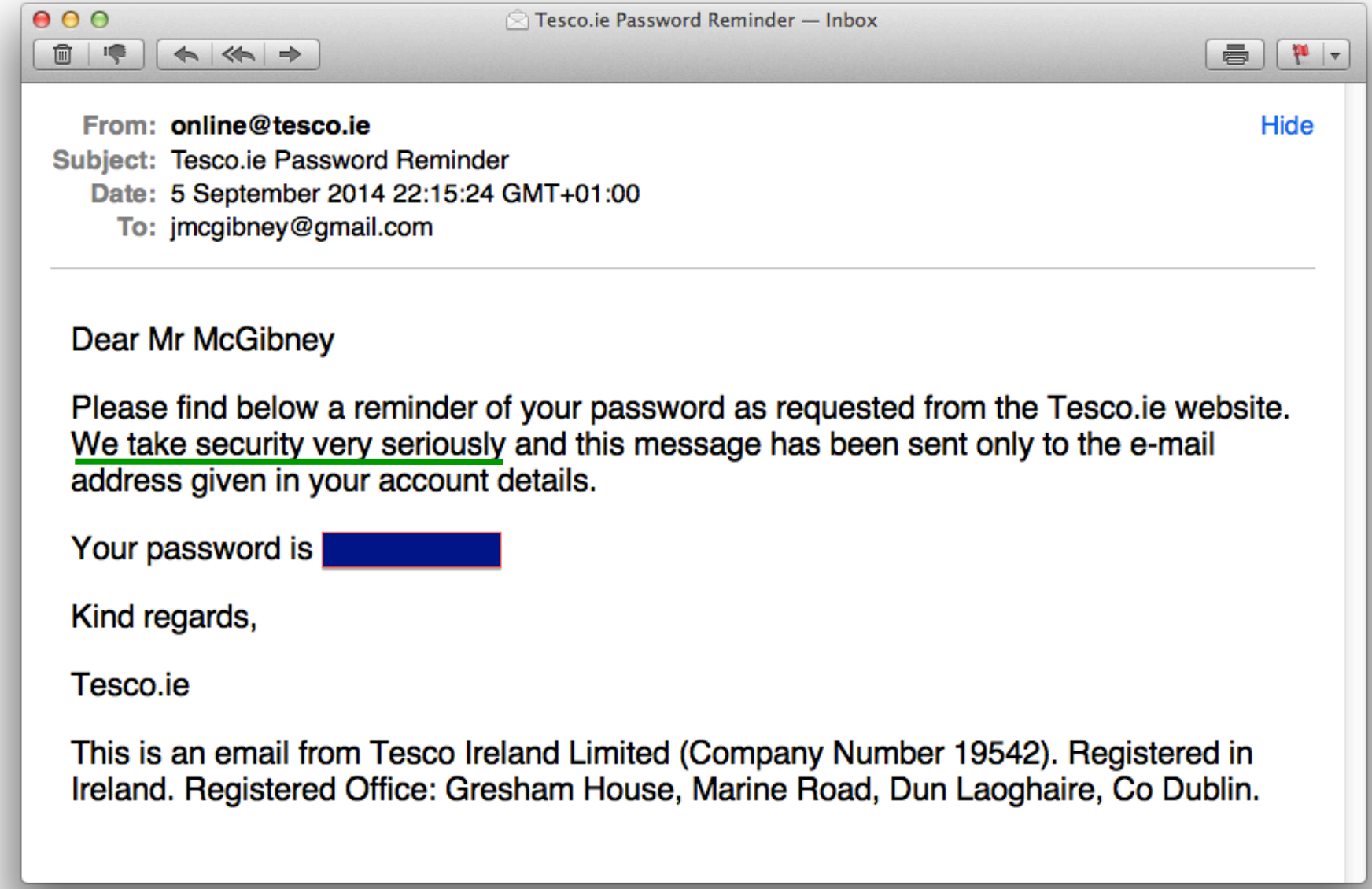


Security news stories…

Anything wrong with this?



Anything wrong with this?



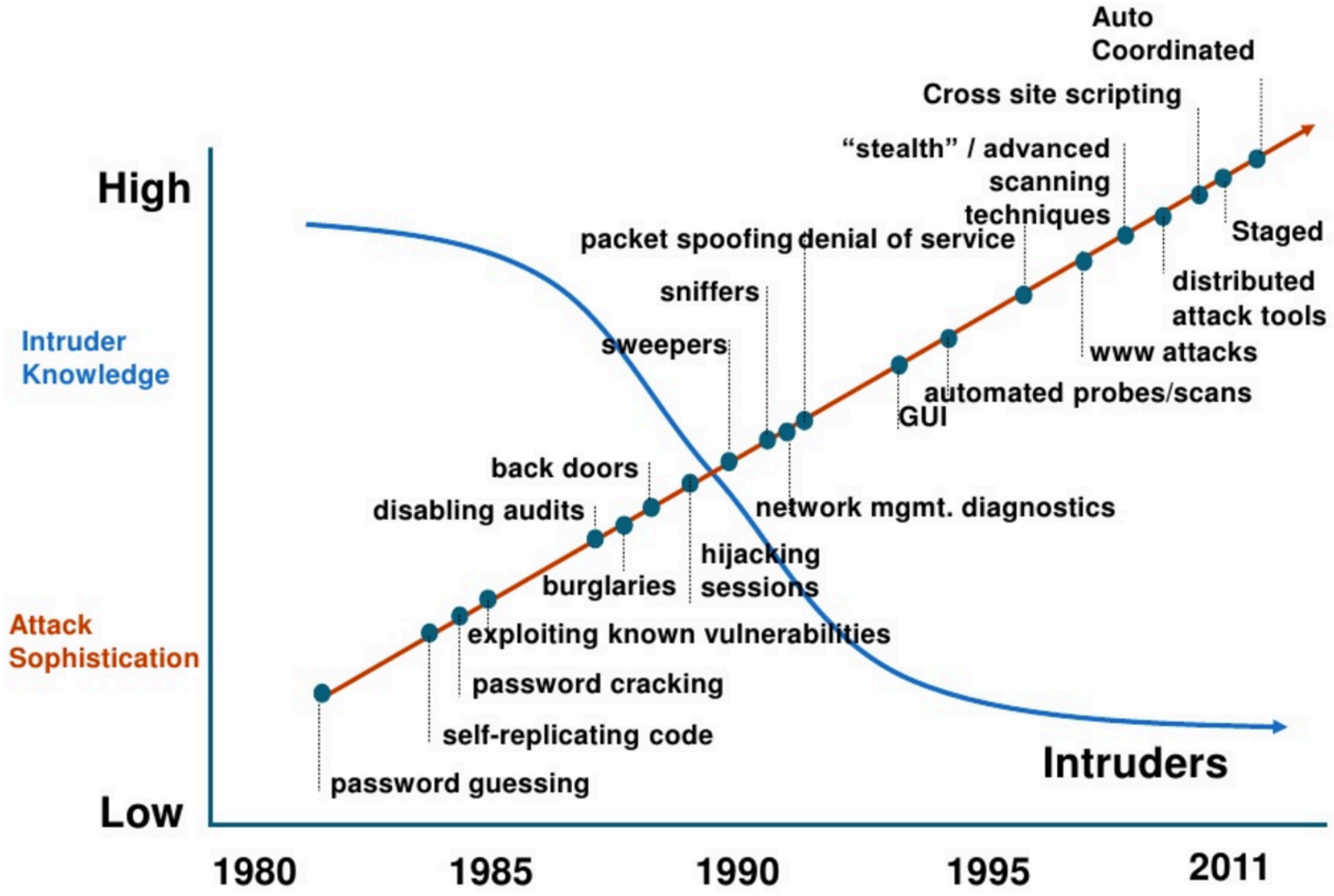
Security in context

- 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

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



Source: CERT Coordination Center, Pittsburgh

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

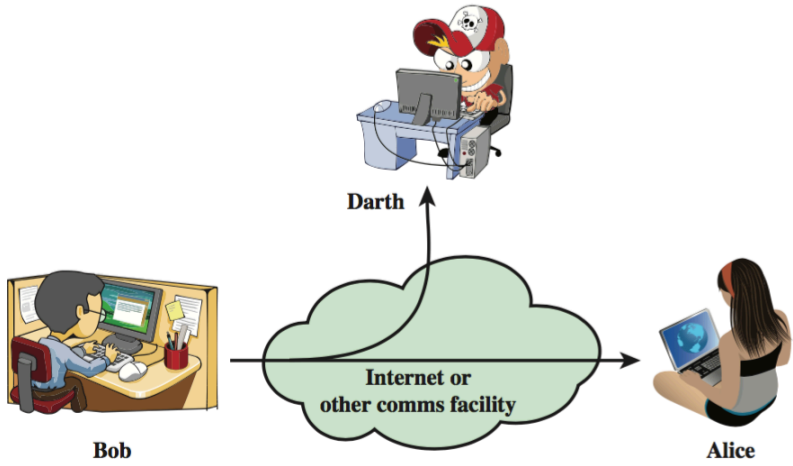
- Anything that can be executed on a machine may have all the rights and privileges of the user who is (directly or indirectly) executing it
- This may include
  - Read/write/modify/create/delete files or data
  - Reading from input devices (e.g. keyboard)
  - Writing to output devices
  - Interacting 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

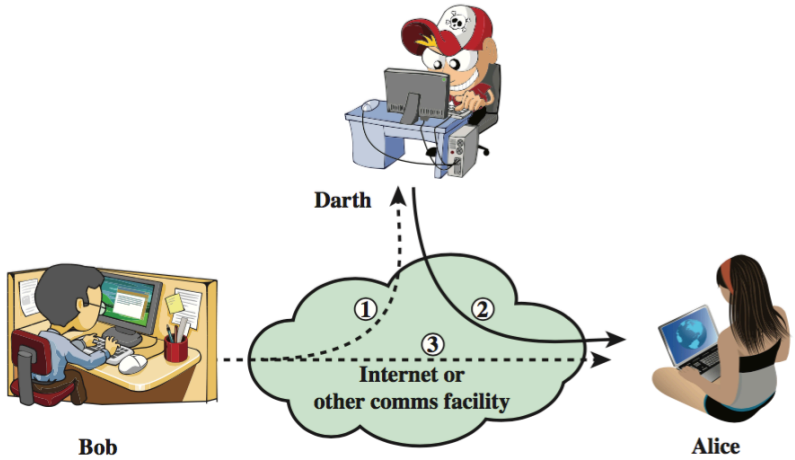
- Opportunists
  - Typically scan wide range of addresses looking for system to exploit
  - For fun; to vandalise; to store pirated movies, music, etc
- Professionals
  - Industrial espionage; Fraud; Spam
- Activists
  - Political or social motivation
- Disgruntled current and former employees and contractors
  - 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

www.keyghost.com/USB-Keylogger.htm

KEY GHOST
THE HARDWARE KEYLOGGER

Interface Security

THAWTE Authentic Site Secured by SSL

Ordering | Customer Support | Products | Company Info | Links | Helpdesk

We welcome

VISA

MasterCard AMERICAN EXPRESS

Home - Site Map

- Home
- Products
- Reviews
- Demonstration
- Testimonials
- Photos
- Specifications
- FAQ
- Press releases
- Download
- Legal Disclaimer
- Affiliates
- Distributors

NEW! QIDO - Qwerty to Dvorak USB Adapter.

QIDO
Qwerty-In > Dvorak-Out

Our latest development in

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).

KeyGhost Headlines

KeyGhost USB Keylogger
"Customer satisfaction guaranteed" 12-Month Manufacturers Warranty.
Order now

Stages of an active attack – the five Ps

- Probe
- Penetrate
- Persist
- Propagate
- Paralyse

Stages of an attack – Probe

- Reconnaisance
  - 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:

Threat (e.g. leakage of private information on the Internet)

↓

Service (e.g. confidentiality)

↓

Mechanism (e.g. encryption)

↓

Technology (e.g. TLS)

↓

Deployment (e.g. configuration of version, algorithm, keys)

↓

Verification (e.g. test deployment)

↓

Maintenance (e.g. update keys, renew certificates)

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

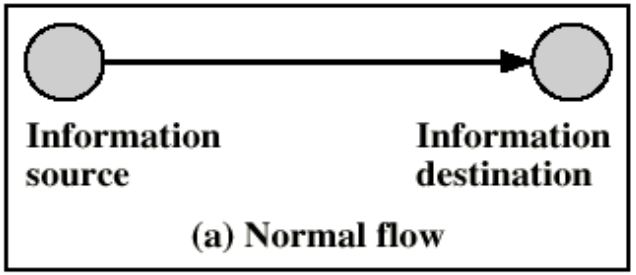
Exercise

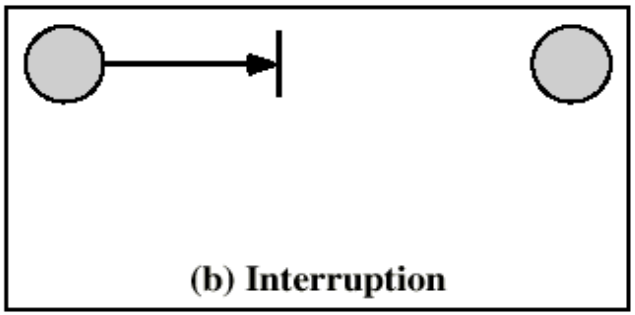
- Consider the 4 communications security attack types shown on the next 2 slides (interruption, interception, modification, fabrication)
- Match each of these four attack types with a security service designed to prevent it.
- Also suggest a mechanism/technology that would realise this service

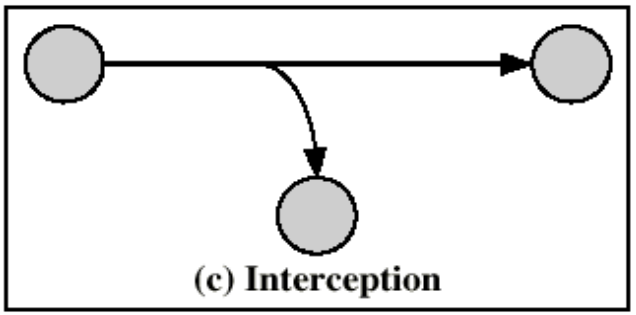
Attacks on Communications

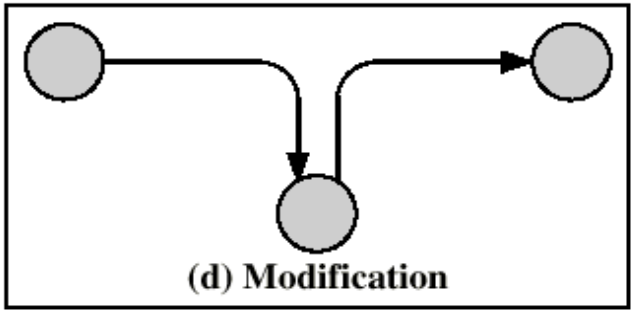
- Interruption
  - Cutting a communication line
- Interception
  - Unauthorised party gains access
- Modification
  - Unauthorised party gains access and tampers
- Fabrication
  - Unauthorised party masquerades as an authorised party

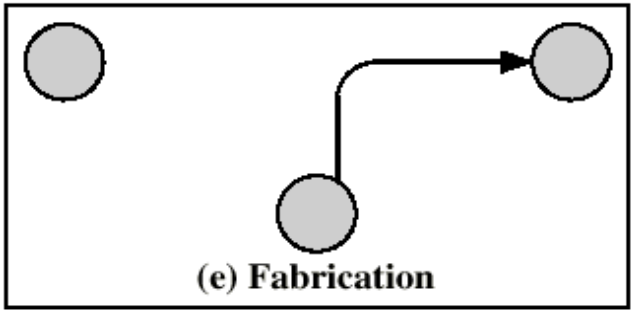
Attacks on Communications











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, …