Security part

1. Introduction to Security

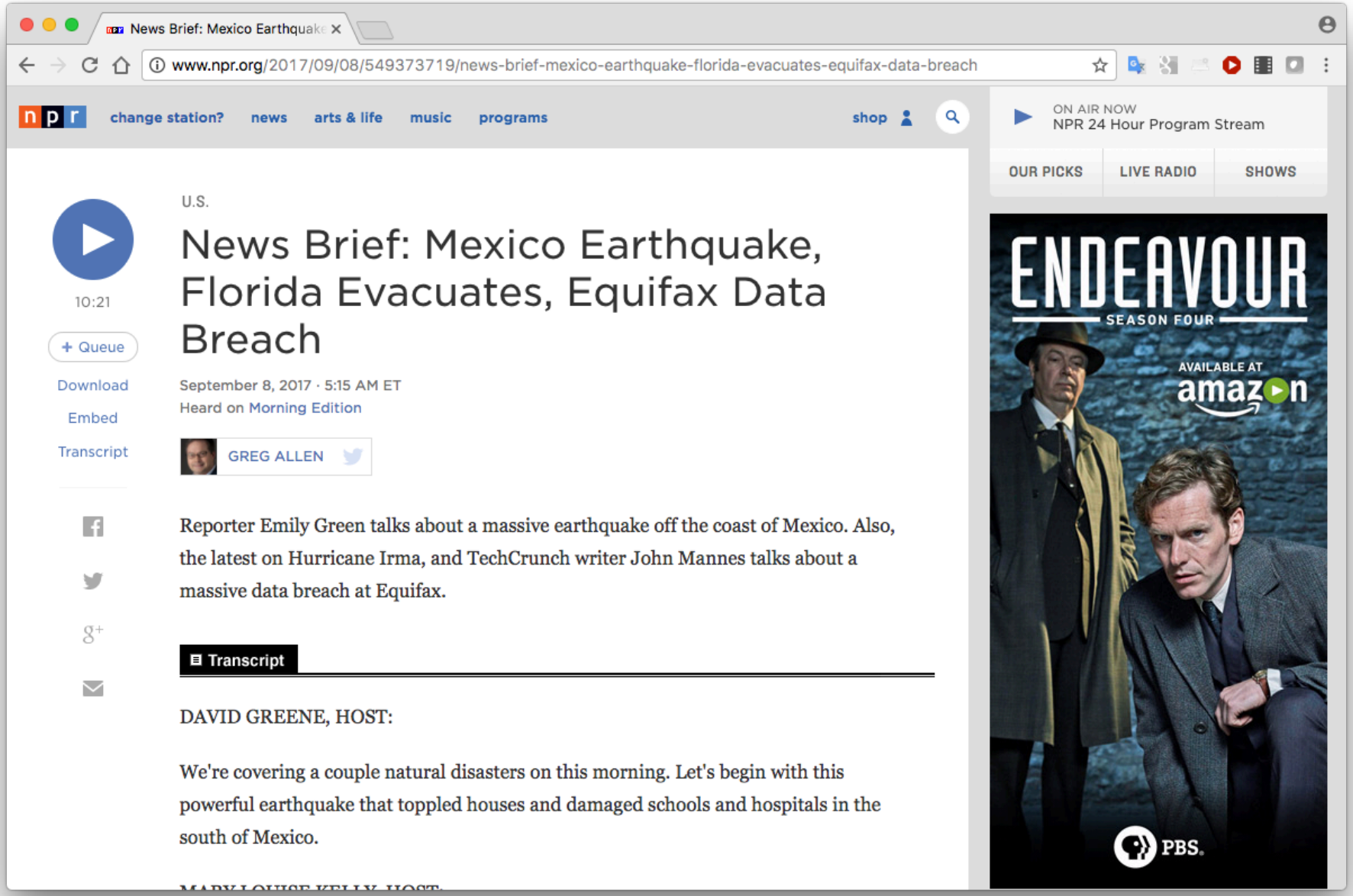
Security part: main topics

- 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…

WannaCry attacks prompt Mic

Secure | https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for...

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

Security news stories…

Yahoo's 2013 Data Breach Affected Three Billion Accounts

Posted on October 4, 2017 by Alex Perala

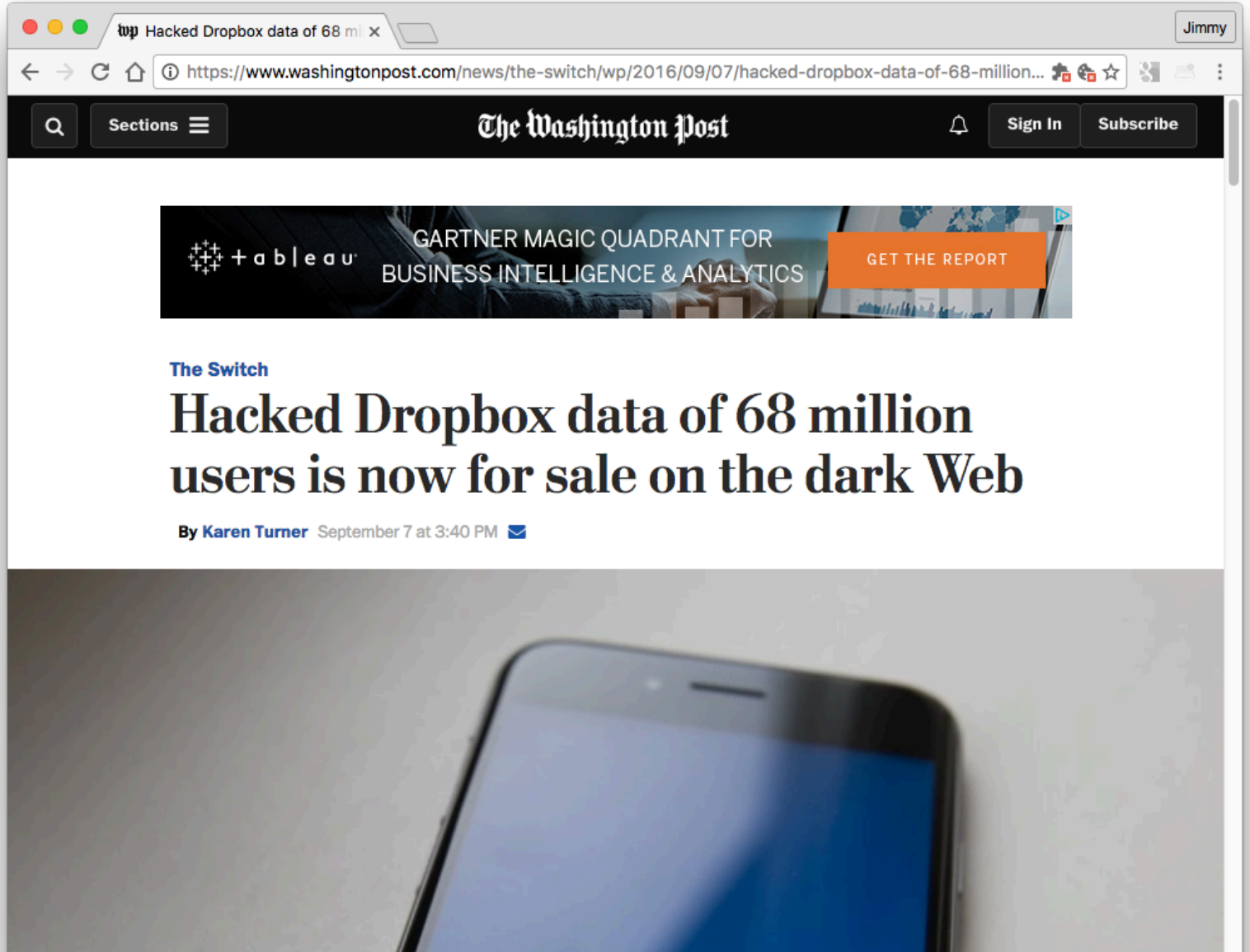
> **"There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database."**

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

Security news stories…



Security news stories…

US to announce new sanctions

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

Security news stories…

Just One Photo Can Silently Ha ×

Jimmy

www.forbes.com/sites/thomasbrewster/2016/09/06/google-android-one-photo-hack/#15ab50961555

Forbes / Security / #CyberSecurity

SEP 6, 2016 @ 03:47 PM 10,503 VIEWS

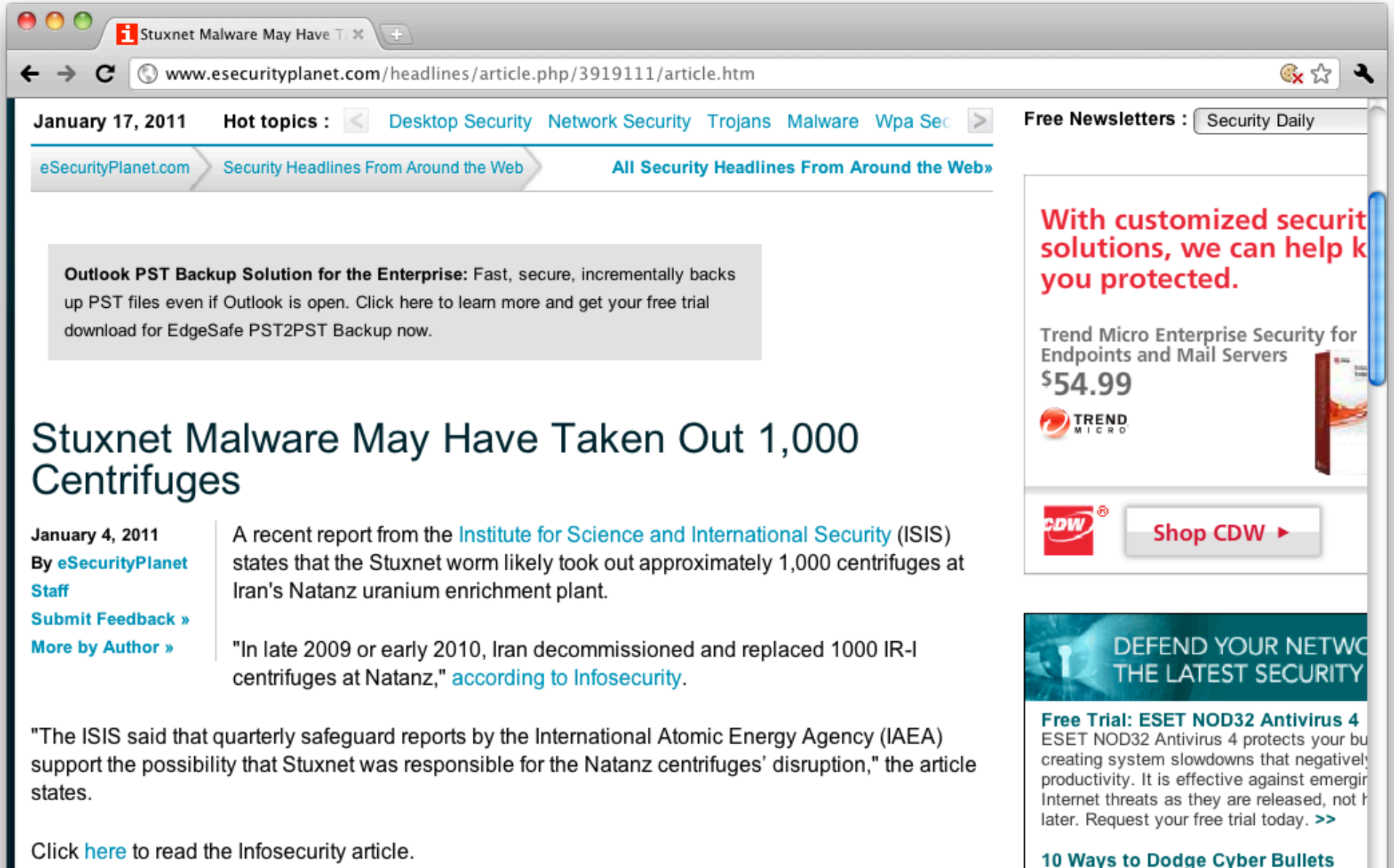
The Little Black Book of Billionaire Secrets

Just One Photo Can Silently Hack Millions Of Androids

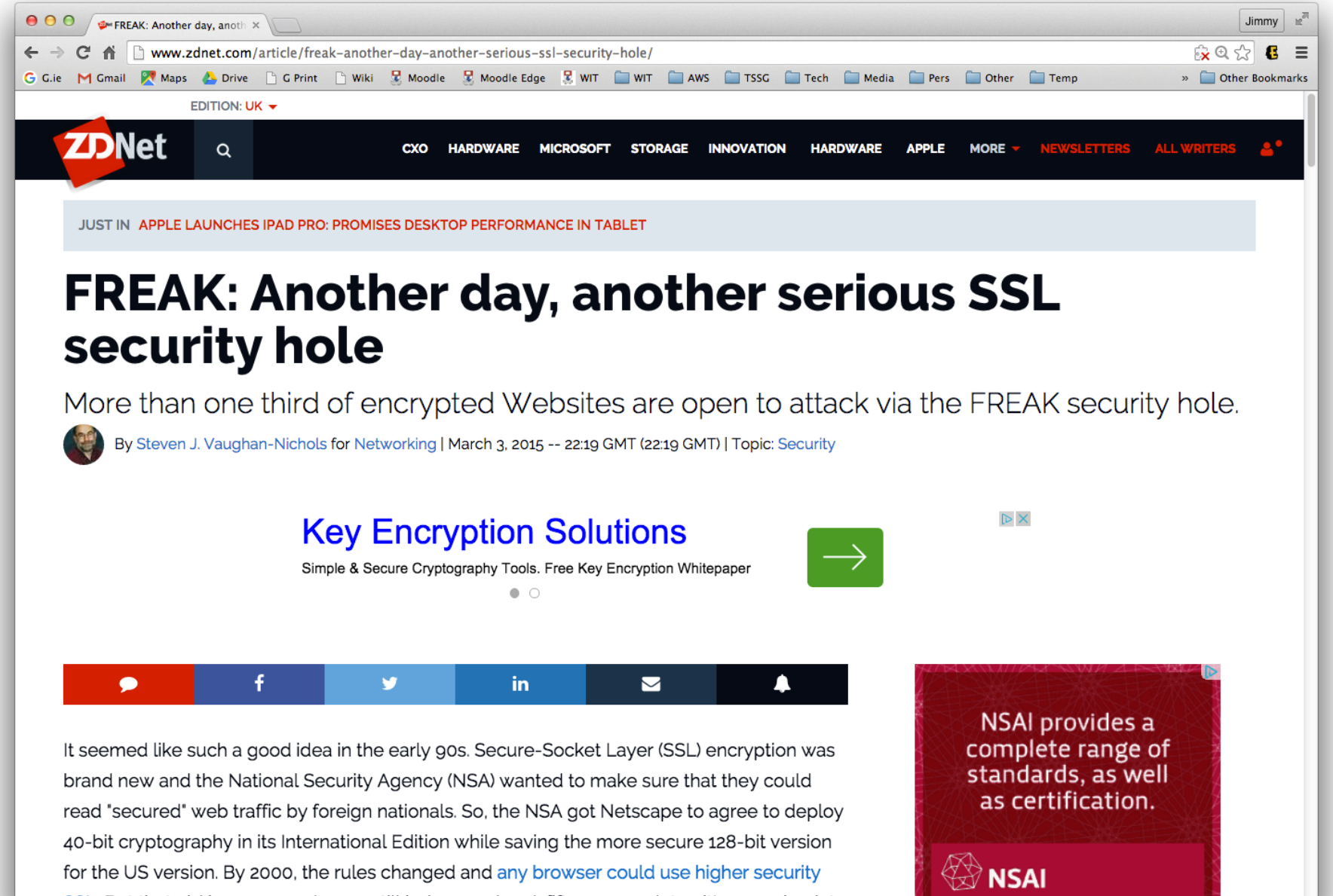
Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

SHARE

Security news stories…



Security news stories…



Security news stories…

Security news stories…

Extremely critical crypto fl ×

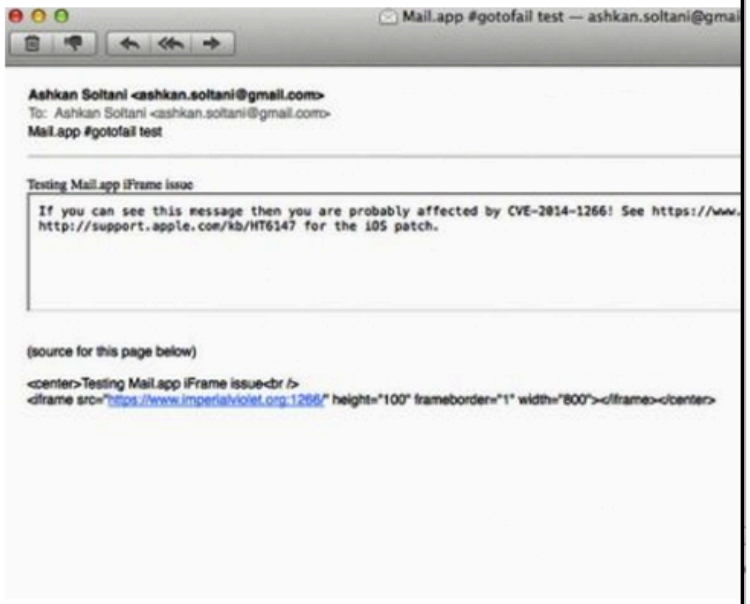
arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS

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

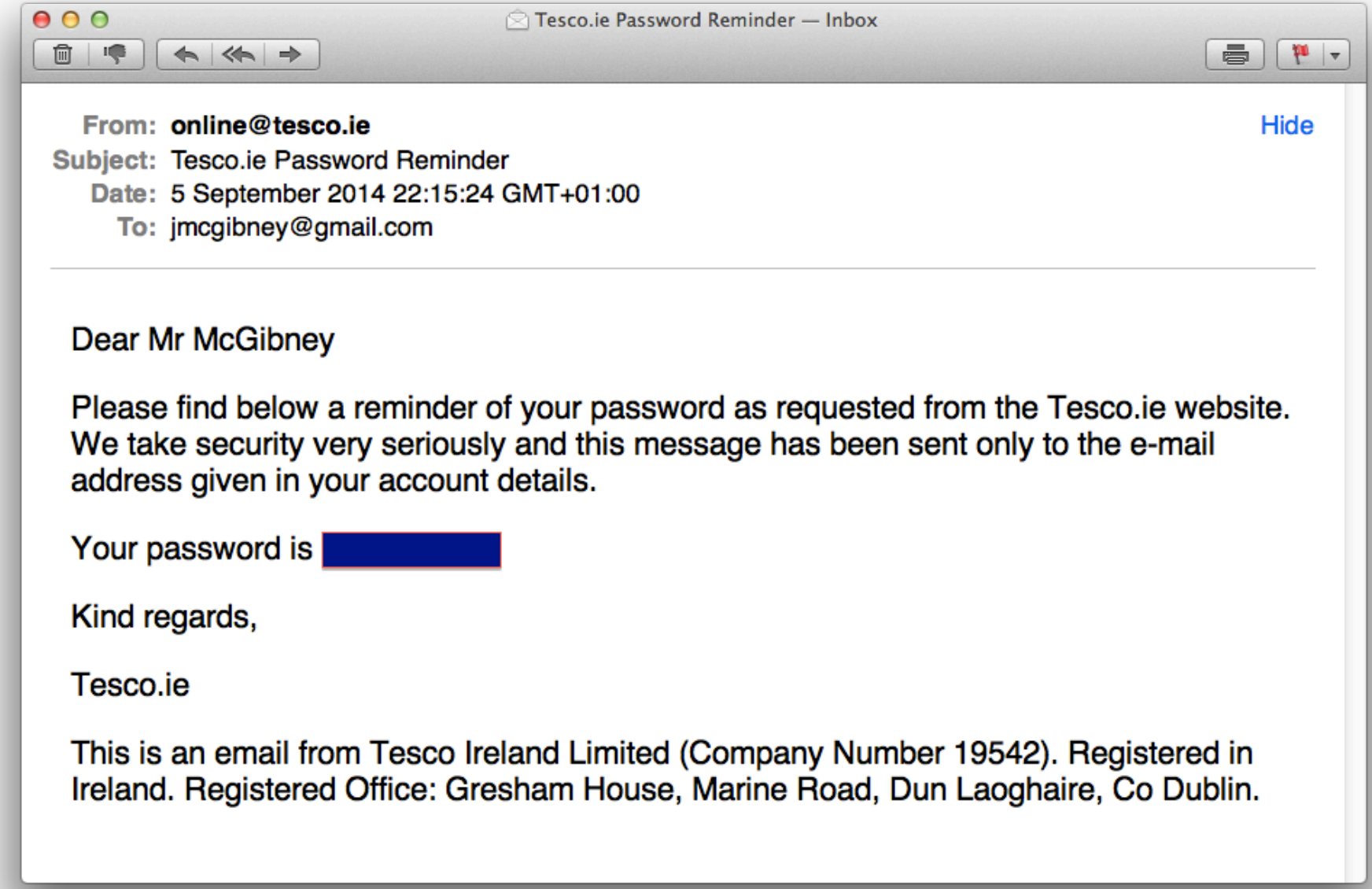


Ashkan Soltani

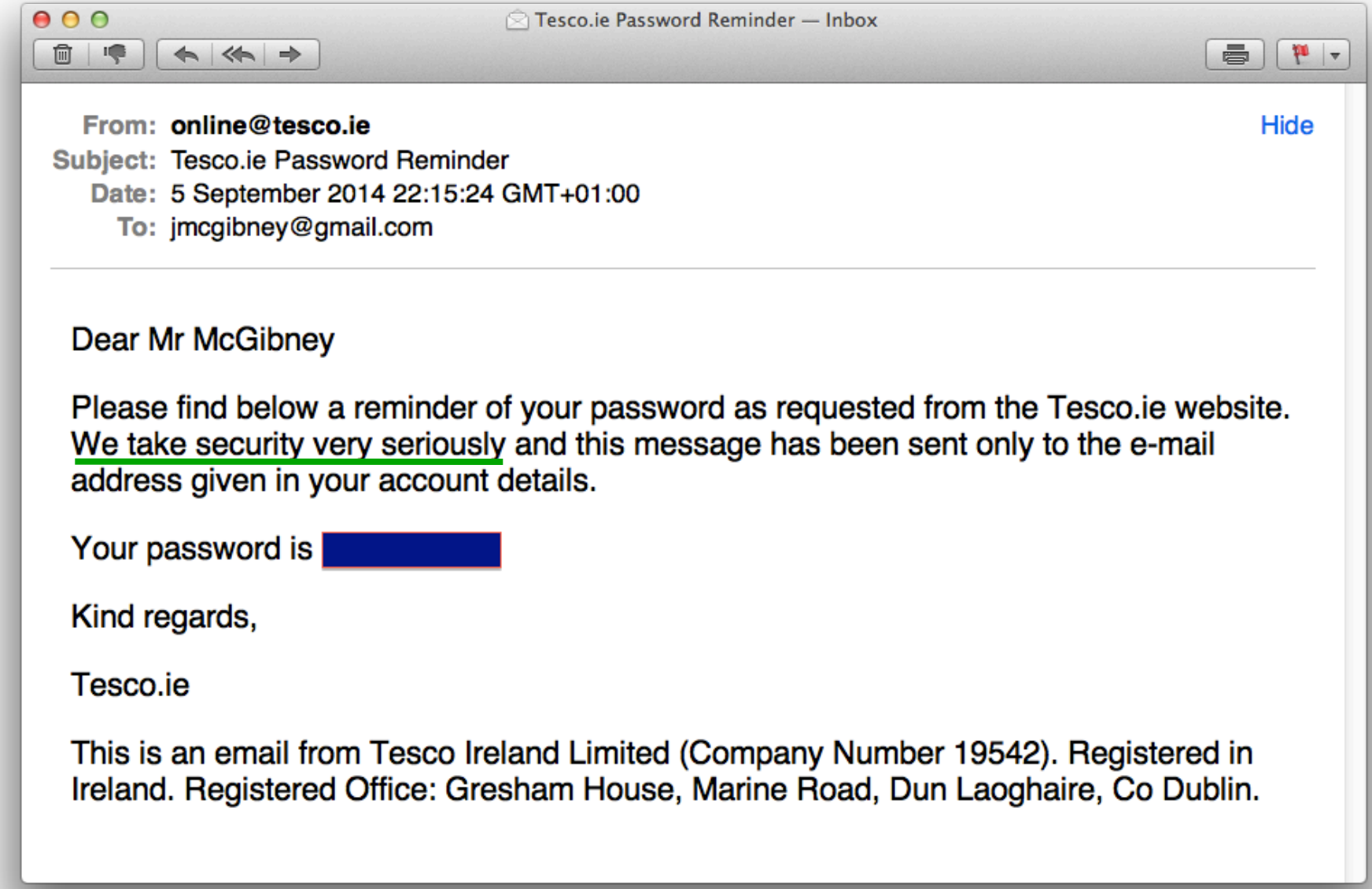
A critical iOS vulnerability that Apple patched on Friday gives a


```
    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;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,                /* plaintex
                           dataToSignLen,             /* plaintext length
                           signature,
                           signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify
                    "returned %d\n", (int)err);
                goto fail;
        }

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

Anything wrong with this?



Anything wrong with this?



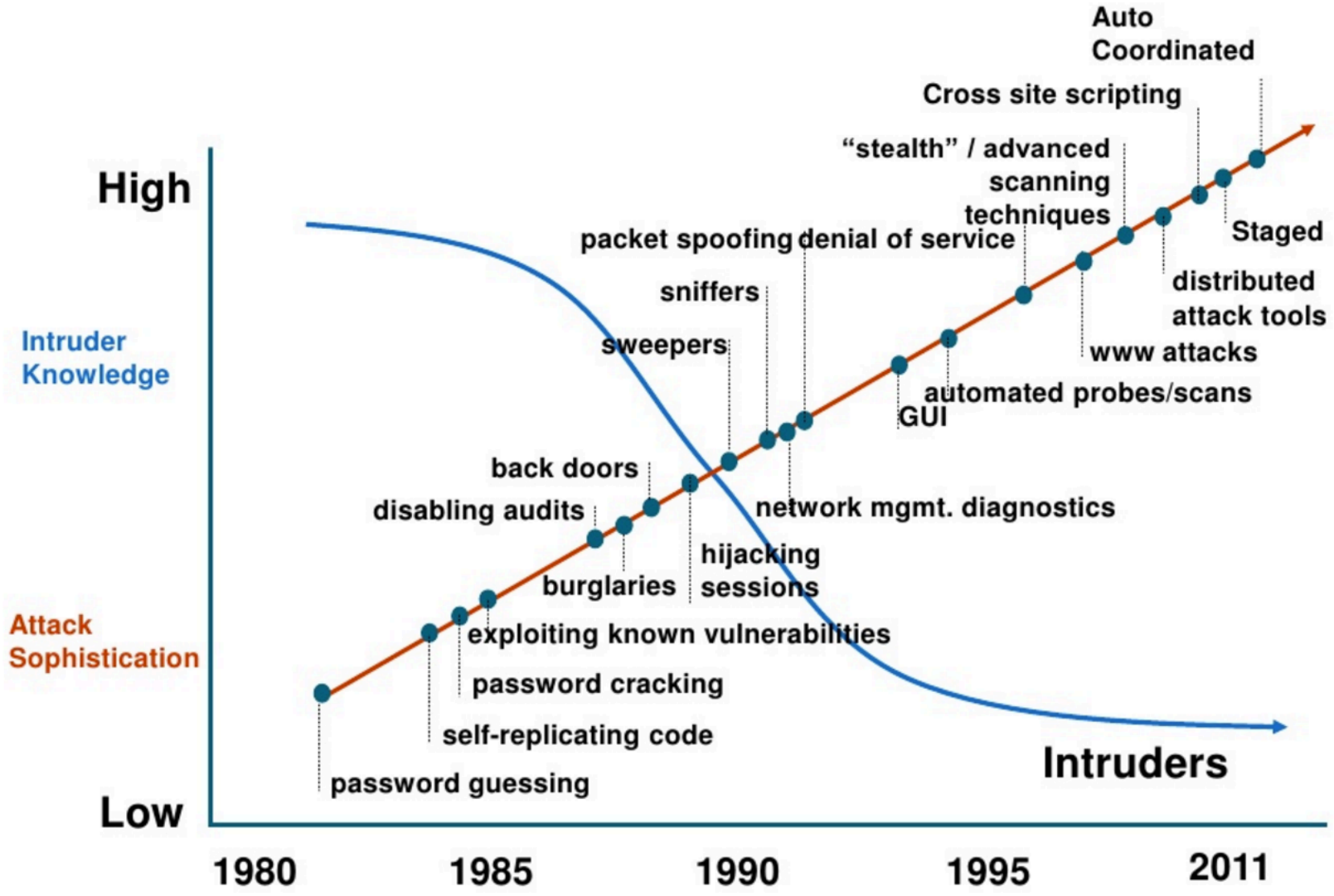
Security in context

- 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



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

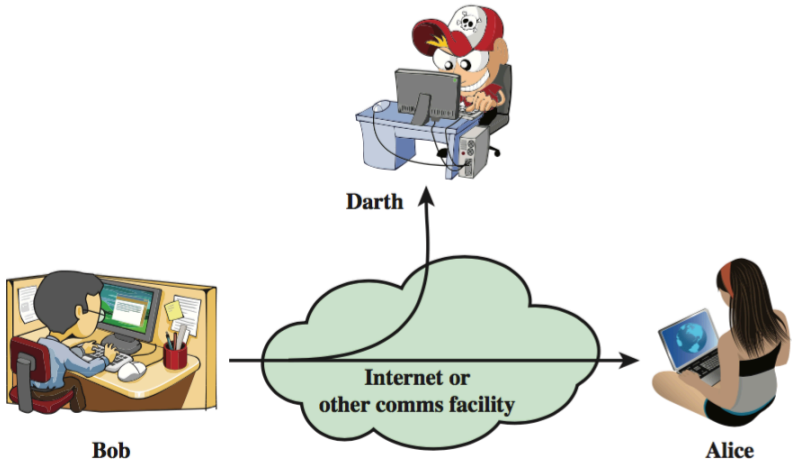
- Anything that can be executed on a machine may have all the rights and privileges of the user who is (directly or indirectly) executing it
- This may include
  - Read/write/modify/create/delete files or data
  - Reading from input devices (e.g. keyboard)
  - Writing to output devices
  - Interacting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

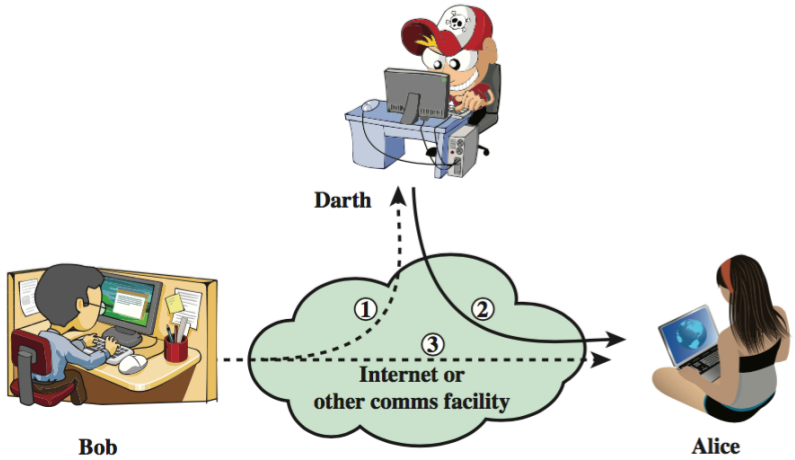
- Opportunists
  - Typically scan wide range of addresses looking for system to exploit
  - For fun; to vandalise; to store pirated movies, music, etc
- Professionals
  - Industrial espionage; Fraud; Spam
- Activists
  - Political or social motivation
- Disgruntled current and former employees and contractors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

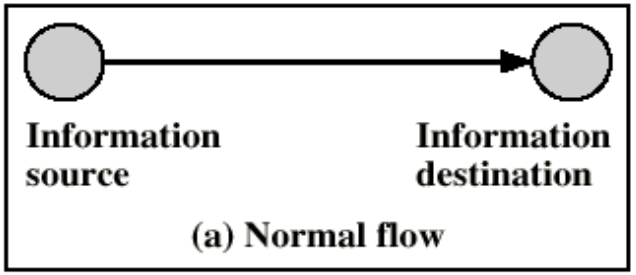
Mechanisms supporting services (examples)

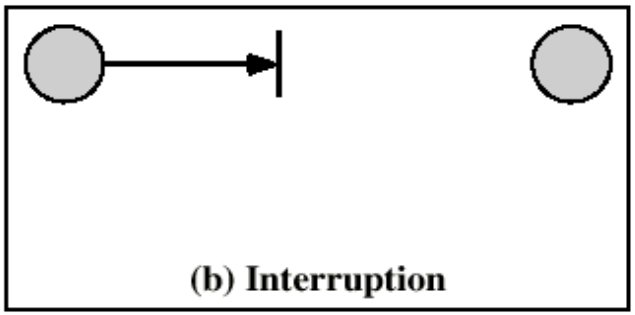
- Authentication
  - Passwords; biometrics
- Access control
  - File permissions
- Data confidentiality
  - Encryption; traffic padding
- Data integrity
  - Message digests; checksums
- Non-repudiation
  - Digital signatures
- Availability
  - Replication of data and services; Backup systems

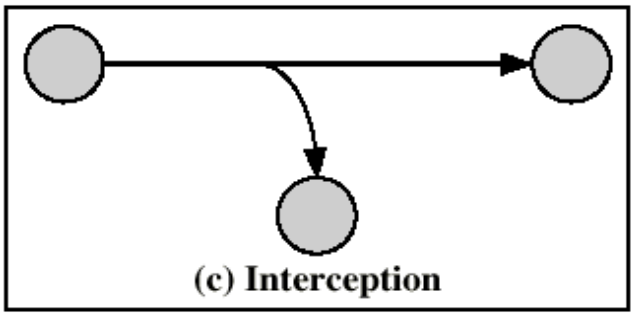
Attacks on Communications

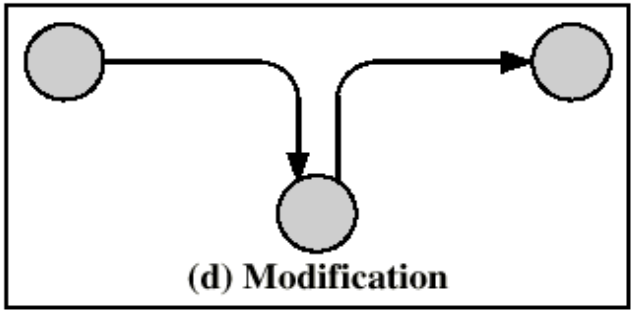
- Interruption
  - Cutting a communication line
- Interception
  - Unauthorised party gains access
- Modification
  - Unauthorised party gains access and tampers
- Fabrication
  - Unauthorised party masquerades as an authorised party

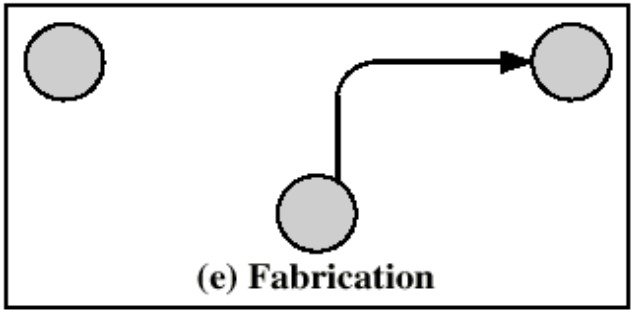
Attacks on Communications











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, …