Security part

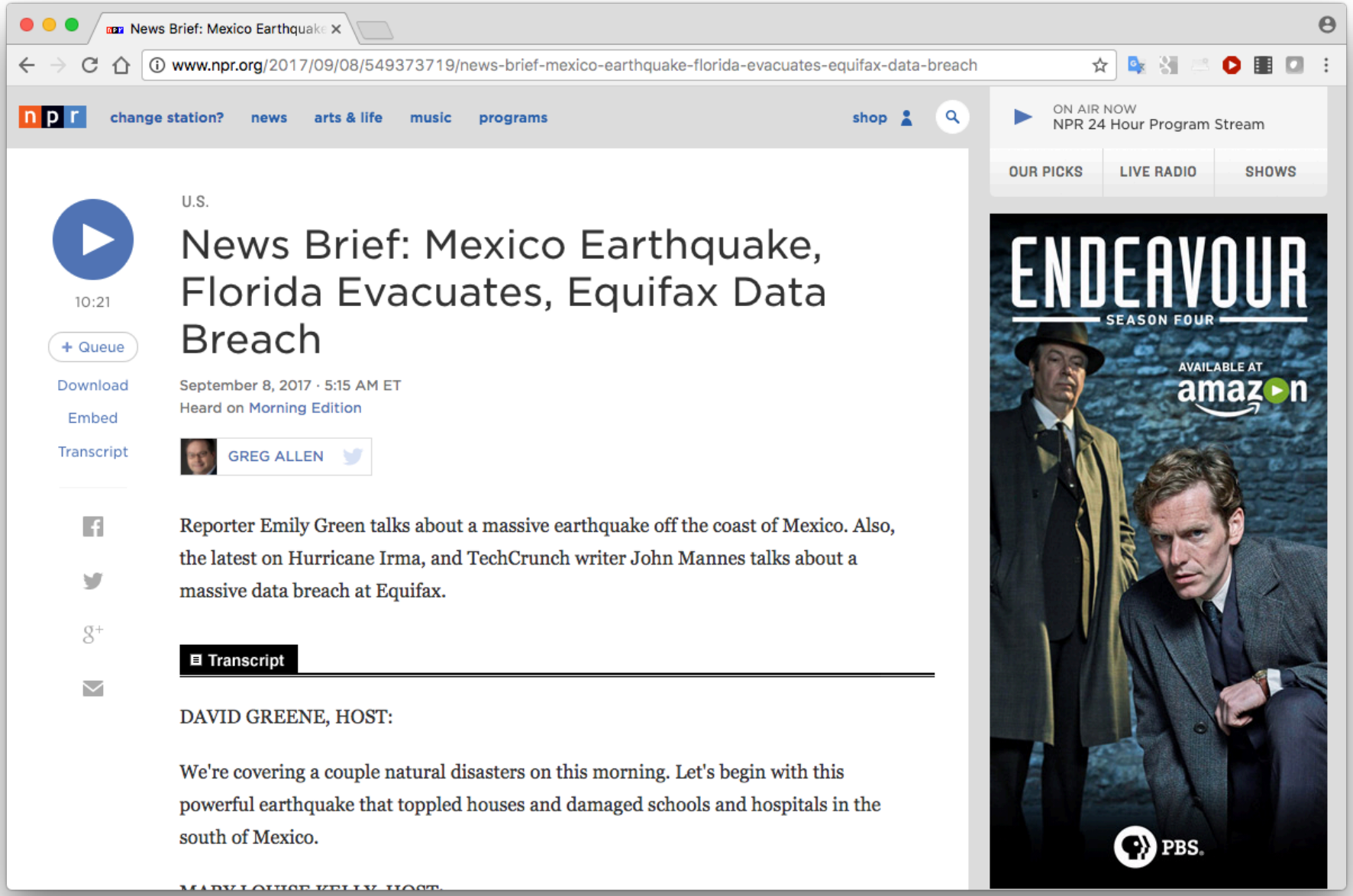
13.1. Setting the scene

Security part of module: main topics

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

Security news stories…

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

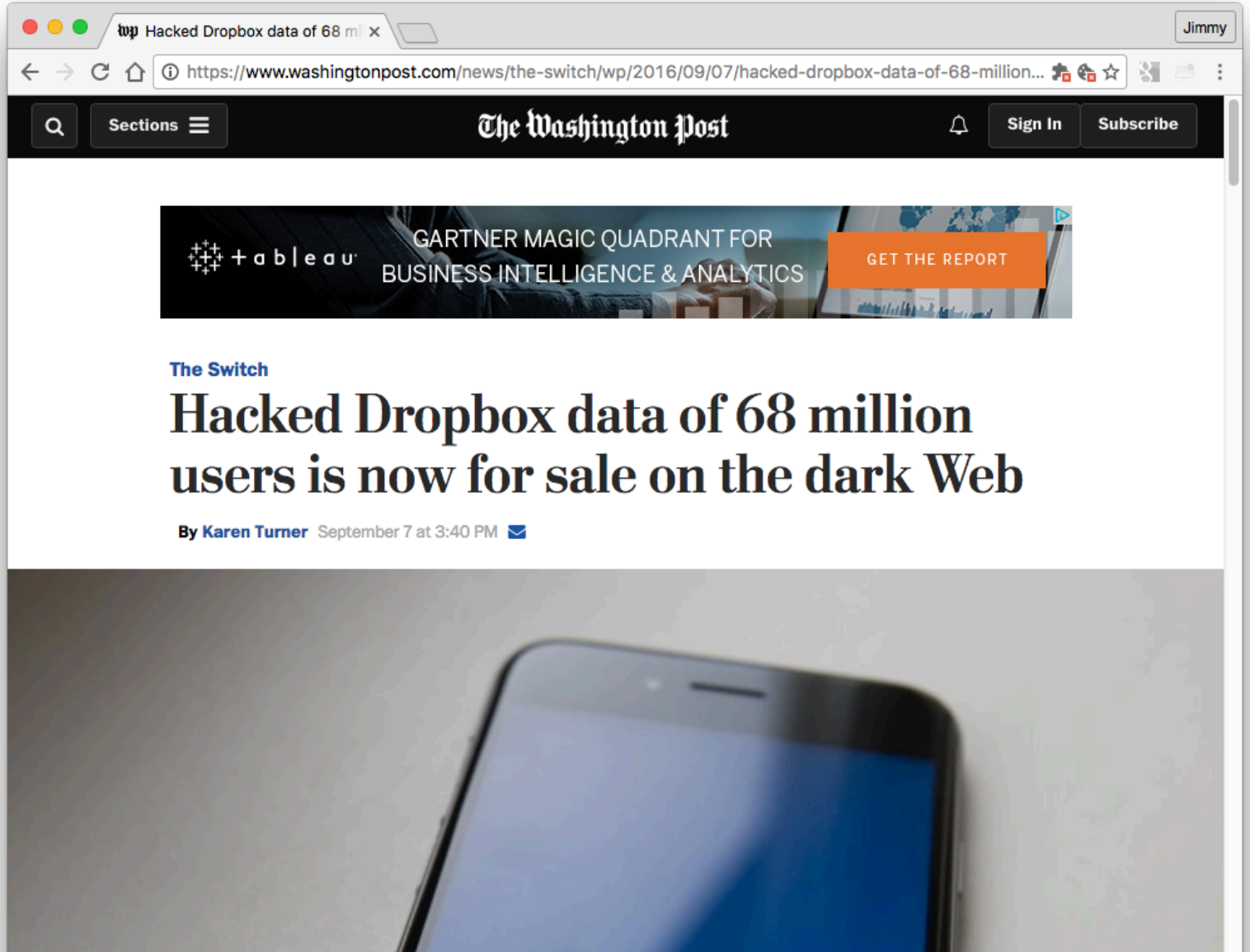
> **"There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database."**

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

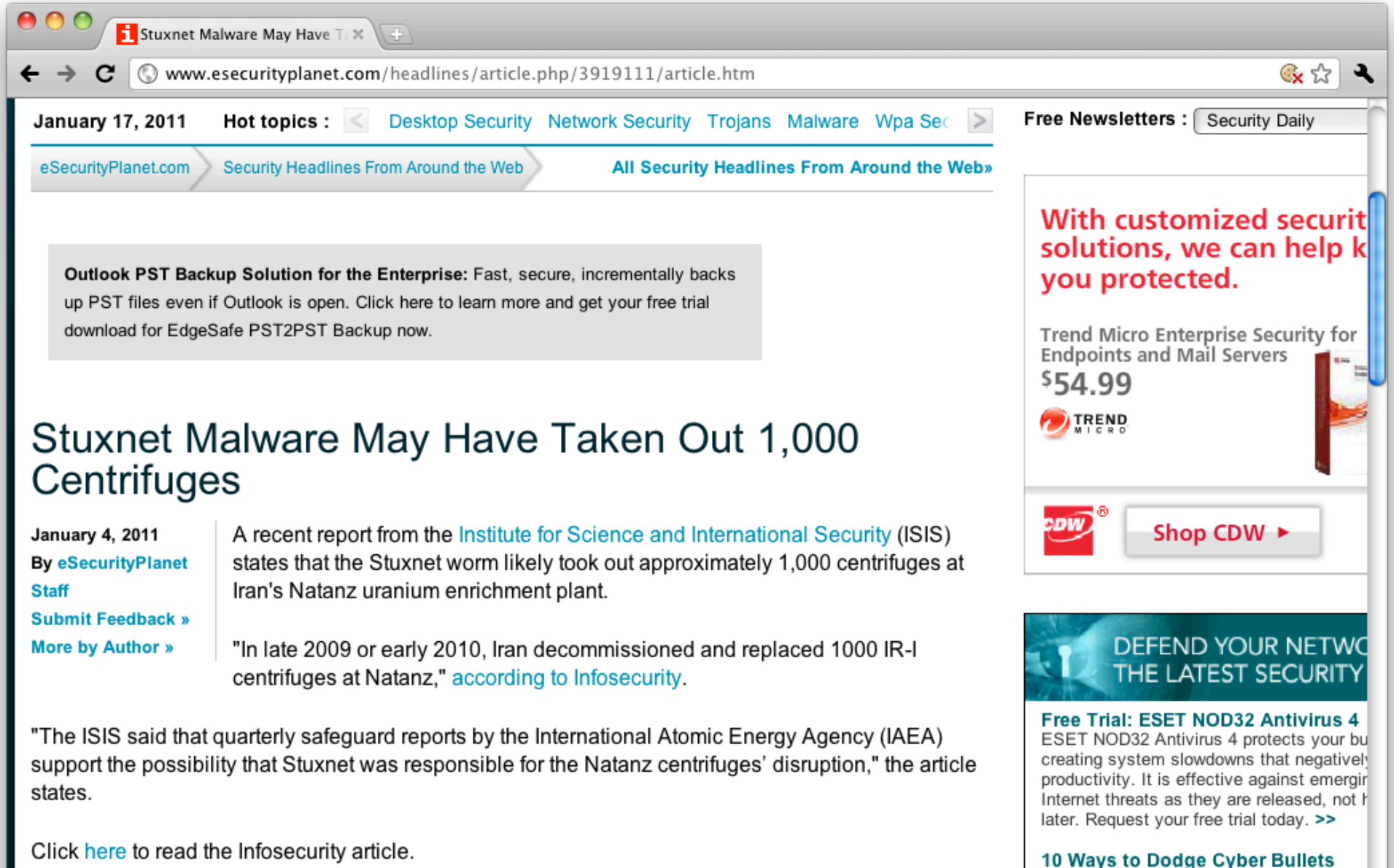
The Little Black Book of Billionaire Secrets

Just One Photo Can Silently Hack Millions Of Androids

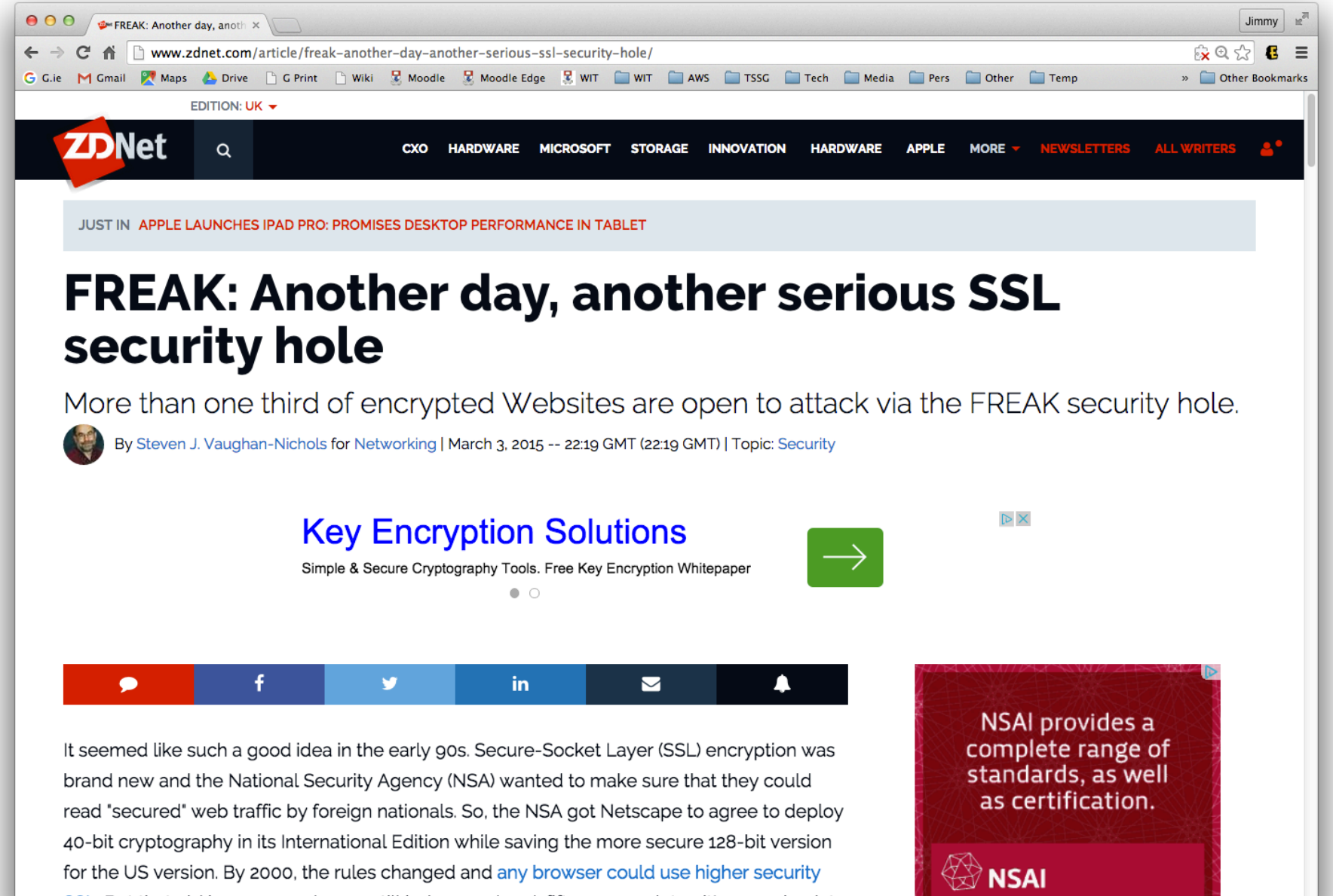
Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

SHARE

Security news stories…



Security news stories…



Security news stories…

Security news stories…

Extremely critical crypto fl ×

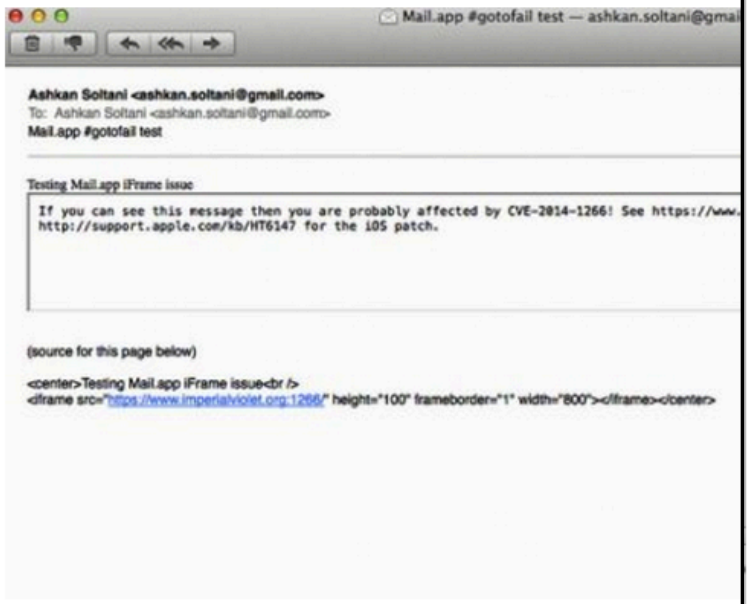
arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/

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

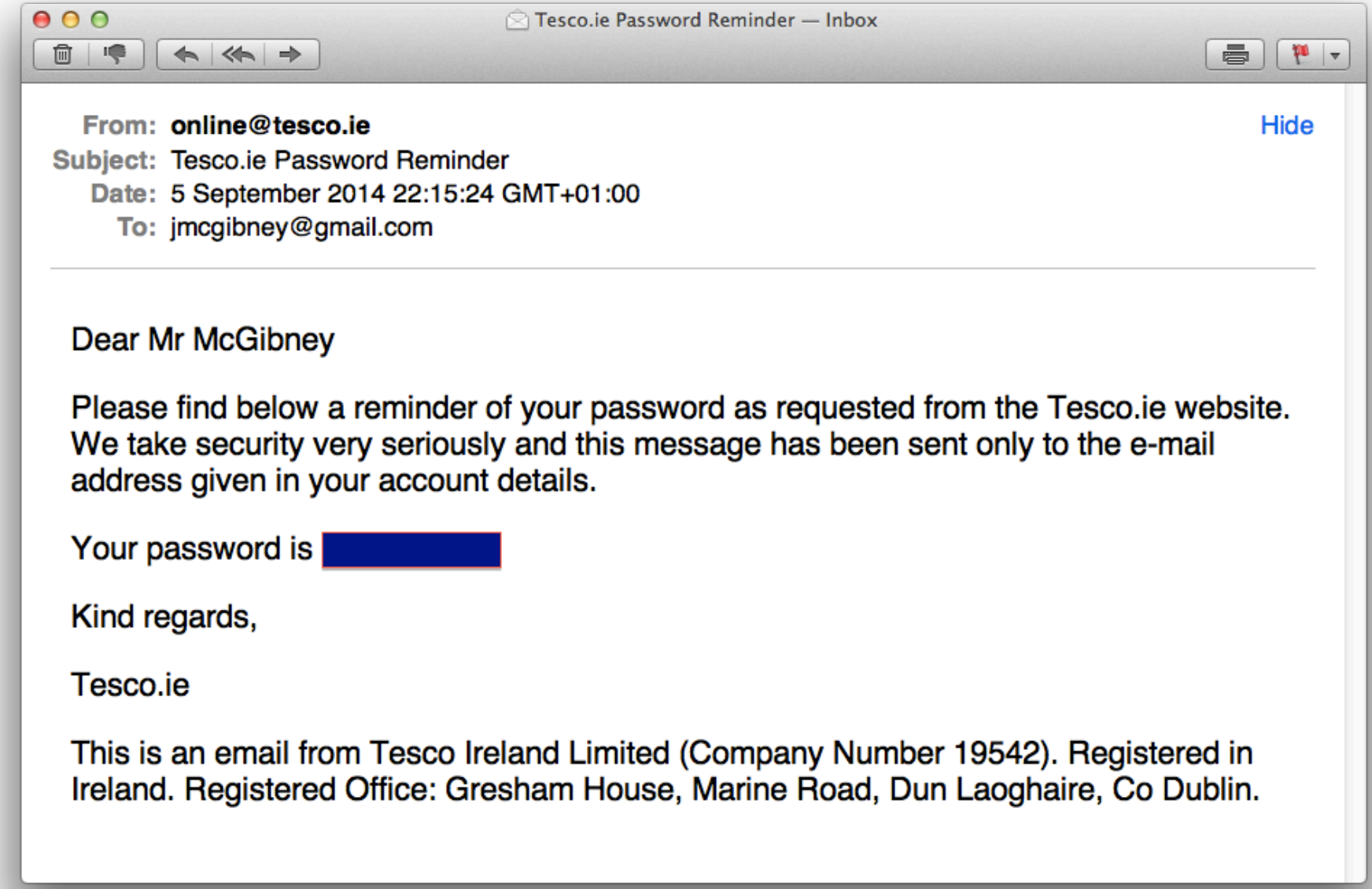


Ashkan Soltani

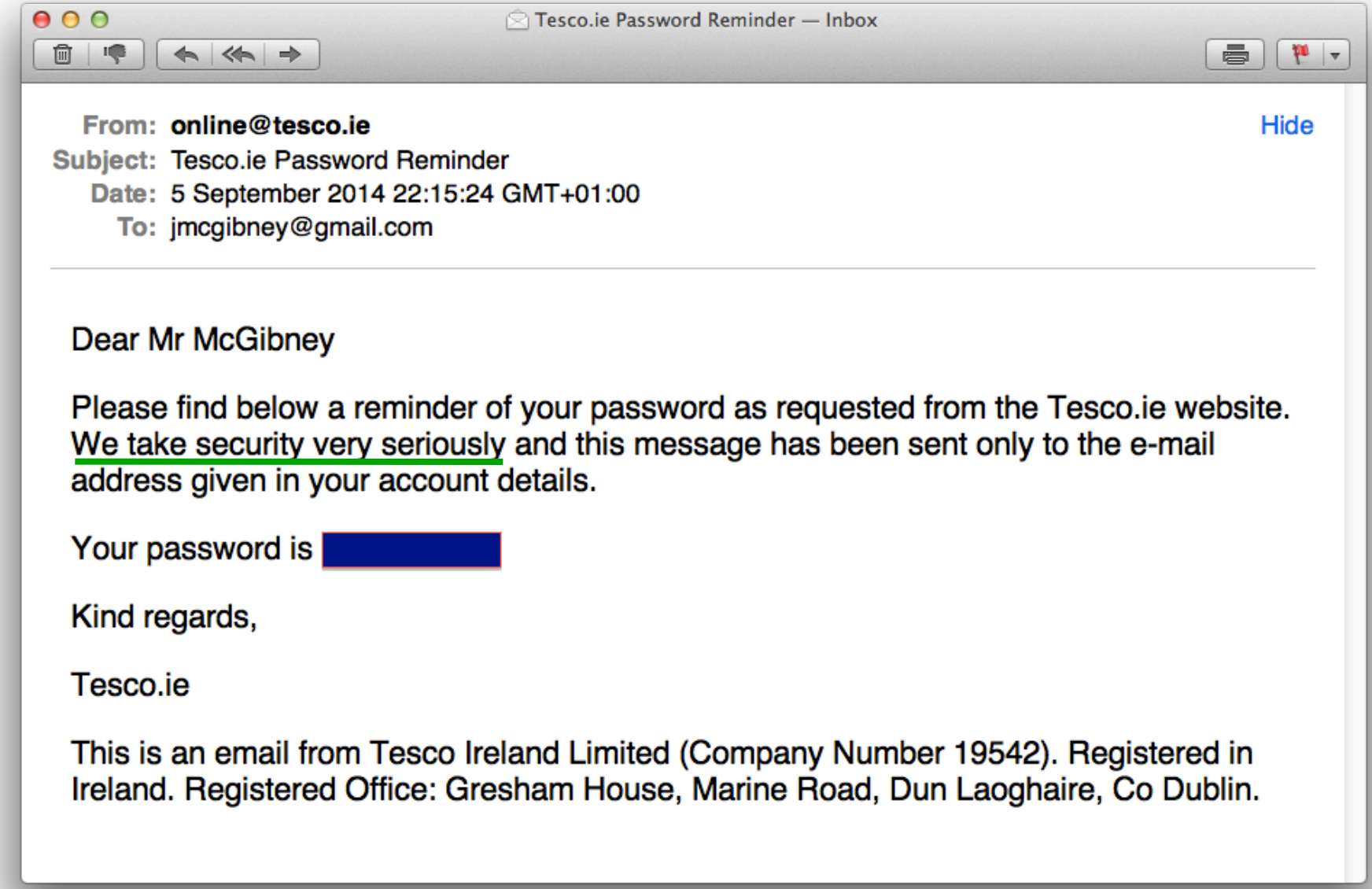
A critical iOS vulnerability that Apple patched on Friday gives a


```
    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?



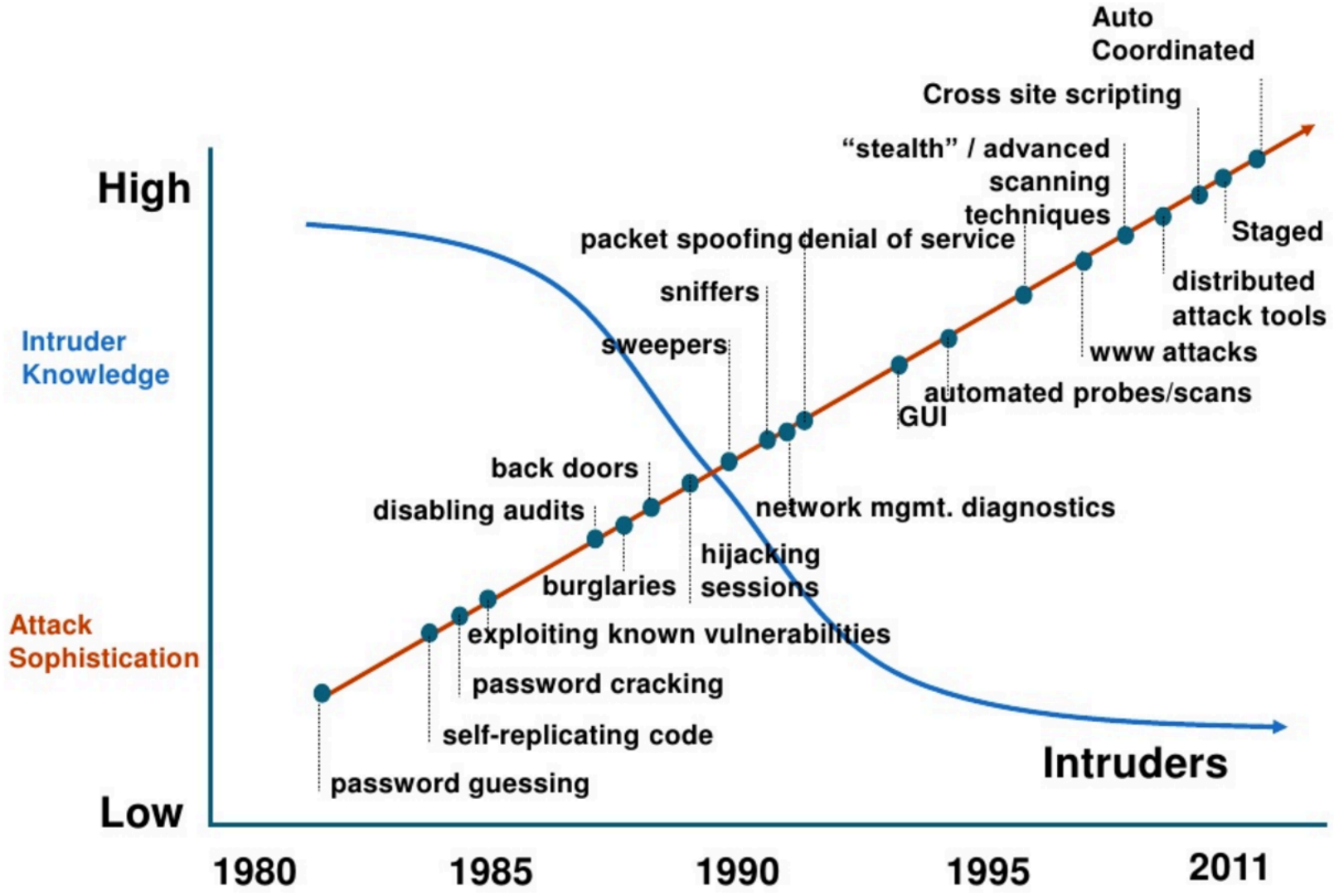
Security in context

- 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

Main players in information security

Main Players in Information Security

- Standards Bodies
  - IETF (Internet Engineering Task Force)
    - Internet standards, IPsec, SSL/TLS, …
  - ISO (International Standards Organisation)
    - OSI model; ISO 27000 series of security standards; "Common Criteria" in ISO 15408
  - ITU (International Telecoms Union)
    - Recommendation X.800 on security services
  - NIST (US Nat'l Institute of Standards & Technology)
    - Official US standards (called FIPS); many on security
  - IEEE (Inst of Electrical & Electronics Engineers)
    - Communication standards, most notably IEEE 802 series: Ethernet (802.3), WiFi (802.11), Authentication (802.1x), …
  - Industry domain-specific standards and regulations
    - FDA, PCI DSS, etc

Main Players (continued)

- Government agencies
  - NSA - National Security Agency (US)
    - in the news a LOT recently
  - Dept of Homeland Security (US)
  - Data Protection authorities (powerful in EU countries)
- The industry
  - Software and equipment vendors, web services
    - Microsoft, Apple, Google, Cisco, Facebook, …
  - Security vendors, outsourcers, consultants
    - Symantec, McAfee, RSA Security, Trend Micro, IBM, HP, …
  - Open source community
    - OpenSSL, Kali Linux, GPG, OWASP, …
  - Certificate authorities
    - VeriSign, DigiCert, Comodo, GeoTrust, GoDaddy, …