The State of Cyber Security

Don Thomas, CISSP, CISA

February 21, 2018

IEEE Buenaventura Computer Society

is Challenging

- Cyber Security just got more interesting…
- Exponential growth in exploitation… and it's only going to get worse.
- Attacks are coming from all side and players
  - Organized Crime – driven by money
  - State Sponsored attacks – for intelligence, chaos and disruption
  - Script kiddies – e.g. Autosploit
- Protection of systems are getting better, but keeping up with security is a challenge
- 2017 – The year of wake-up calls on cybersecurity

Let's take a look at some recent fails and trends

- Shadow Brokers
- Wannacry
- Equifax
- Uber
- City of Dallas
- Maersk Shipping
- Krack
- Strava Fitness
- Meltdown & Spetre

Shadow Brokers

Known for leaking allegedly NSA cyber weapons on 5 separate occasions to the internet.

- 1. Equation Group Cyber Weapons Auction – invitation”
- 2. Trick or Treat
- 3. Black Friday / Cyber Monday Sale
- 4. Don’t forget your base
- 5. Lost in translation – 4/14/17 – The most damaging release of exploits.
  - Dumped on the Internet the NSA tools and exploitation code
    - EternalBlue (10 times worse than Heartbleed)
    - Windows SMB exploits (Microsoft pushed out patches one month earlier, including a patch to XP)

      Known malware that used EternalBlue, WannaCry, Petya, NotPetya Ransomware

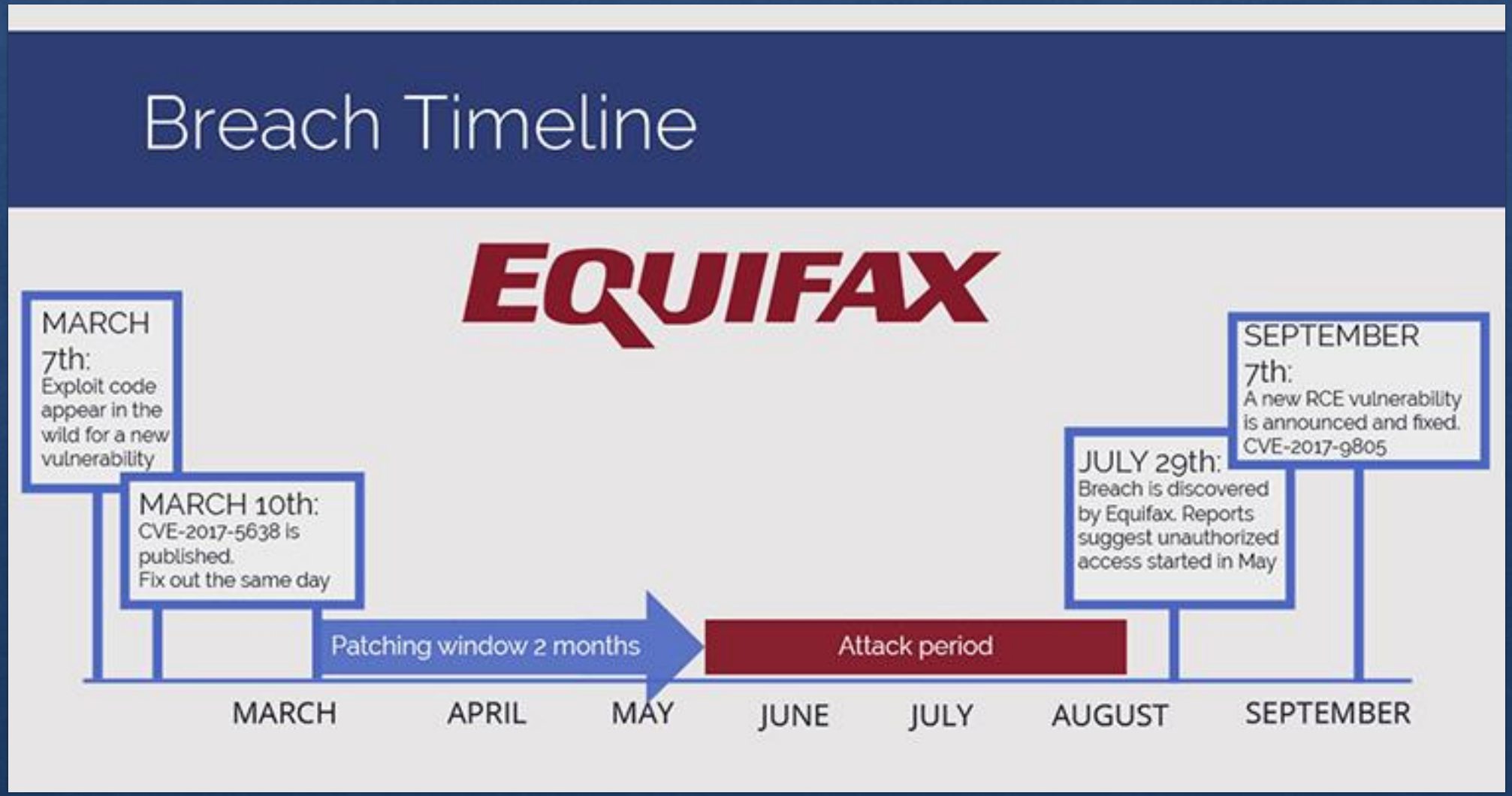
Wannacry

- Ransomware attack began Friday May 12, 2017, worldwide.
- Initial infection was in Asia through a vulnerable SMB port via EternalBlue exploit.
- Infected over 230,000 systems in 150 countries.
- Hit The National Health Service Hospitals in England and Scotland ~ 70,000 systems
- Nissan Motor Manufacturing, halted production
- Researcher Marcus Hutchins accidentally discovered the kill switch domain hardcoded in the malware
- Dec 2017 – several agencies confirm the Wannacry attack was organized by North Korea

Equifax

- 2016 – Had advanced warning of insecure systems and lack of security.
  - E.g. – Employee Only Portal open to the internet
- March 2017 – Data Breach, in September Equifax announced breach (Apache Struts)
  - 140 Million customers personal data breached.
    - Social Security Numbers, Date of Birth, etc…
    - American Salary Data
  - 15.2 Million UK customers records compromised and 569K had sensitive Personal Identifiable Information (PII) exposed.
  - Exposure of Argentinian consumer data (admin/admin)
- CEO – Richard Smith – Retired / ? Fired
- CISO - Susan Mauldin – Retired / Fired
- CIO - Dave Webb – Retired / Fired

Equifax


Breach Timeline
EQUIFAX
MARCH 7th:
Exploit code appear in the wild for a new vulnerability
MARCH 10th:
CVE-2017-5638 is published.
Fix out the same day
Patching window 2 months
Attack period
JULY 29th:
Breach is discovered by Equifax. Reports suggest unauthorized access started in May
SEPTEMBER 7th:
A new RCE vulnerability is announced and fixed.
CVE-2017-9805
MARCH
APRIL
MAY
JUNE
JULY
AUGUST
SEPTEMBER

Equifax – Letter from the FTC

September 8, 2017
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies. . . . The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too.

There are steps to take to help protect your information from being misused. Visit Equifax's website, www.equifaxsecurity2017.com.

https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Uber

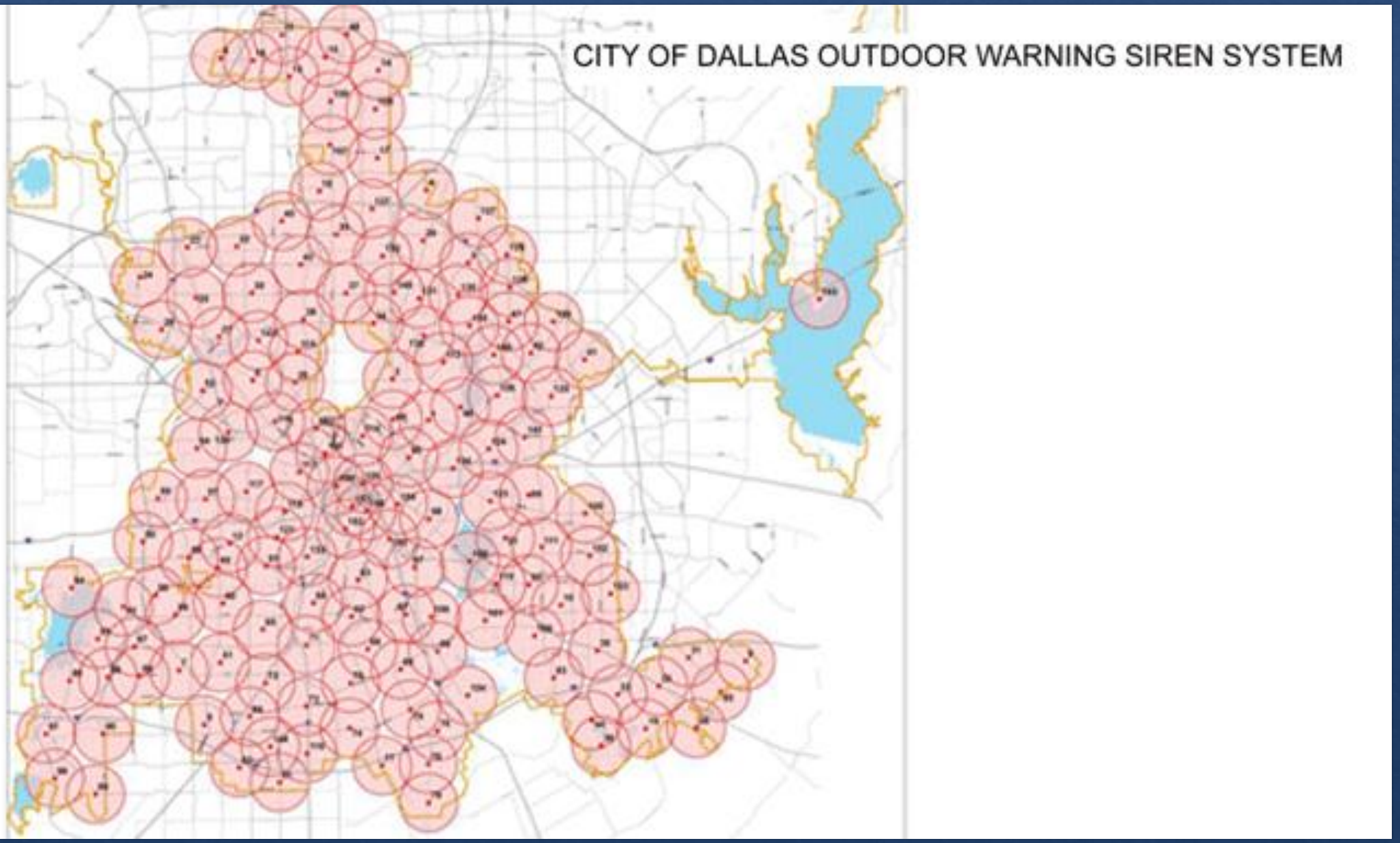
- October 2016 - Data Stolen on 57 Million subscribers
- Uber paid $100,000 to hackers demands and asked hackers to delete the stolen data
- Stolen data was not disclosed until November 21, 2017
- Nov 2017 - CISO – Fired – for covering up the breach and paying the ransom

City of Dallas

- City of Dallas - 156 outdoor emergency sirens -
  - installed in 2007
  - 700Mhz reserved for public safety
  - Radio replay attack DTMF -
  - No use of Signal Authentication or encryption.
  - City voted to pay $100k to retrofit the system with security.

https://thehackernews.com/2017/04/emergency-tornado-siren-hack.html

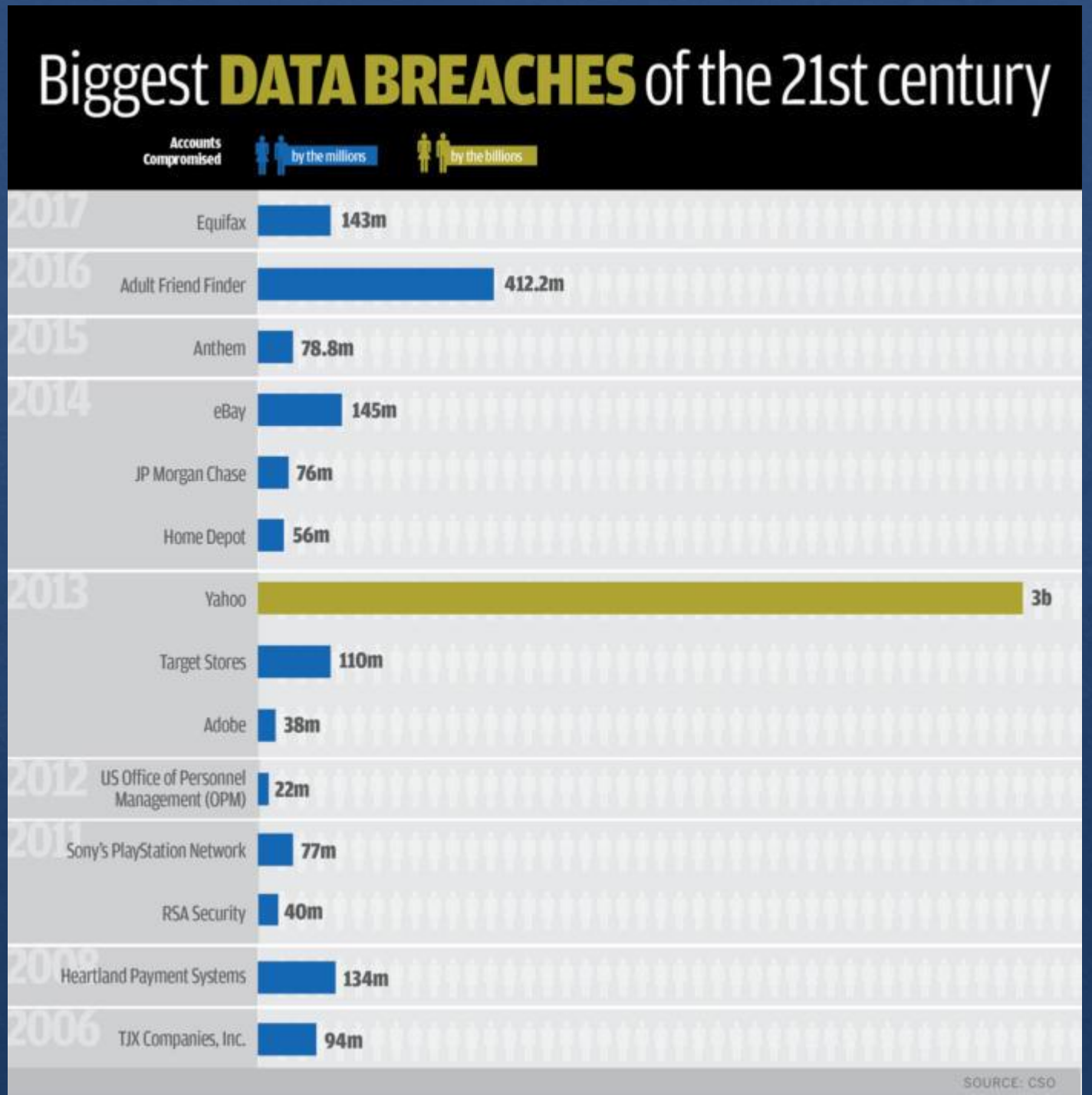
https://forum.level1techs.com/t/infosec-dallas-emergency-alert-system-hack/114889


CITY OF DALLAS OUTDOOR WARNING SIREN SYSTEM

Maersk shipping line

- 45,000 PC's and 4,000 servers hit with NotPteya Ransomware
- Est. $300,000,000 in damages to recover.
- Known damages to others impacted by it exceeded $1 billion.
- All PC, Servers and Application were replaced in 10 days

The name Petya is a reference to the 1995 James Bond film GoldenEye, wherein Petya is one of two weapon satellites that carries a "Goldeneye" – an atomic bomb detonated in low Earth orbit to produce an electromagnetic pulse. NotPetya is a variant of Petya, which propagates via the EternalBlue exploit.


Biggest DATA BREACHES of the 21st century
Accounts Compromised
by the millions
by the billions
2017
Equifax
143m
2016
Adult Friend Finder
412.2m
2015
Anthem
78.8m
2014
eBay
145m
JP Morgan Chase
76m
Home Depot
56m
2013
Yahoo
3b
Target Stores
110m
Adobe
38m
2012
US Office of Personnel Management (OPM)
22m
2011
Sony's PlayStation Network
77m
RSA Security
40m
2009
Heartland Payment Systems
134m
2006
TJX Companies, Inc.
94m
SOURCE: CSO

Krack

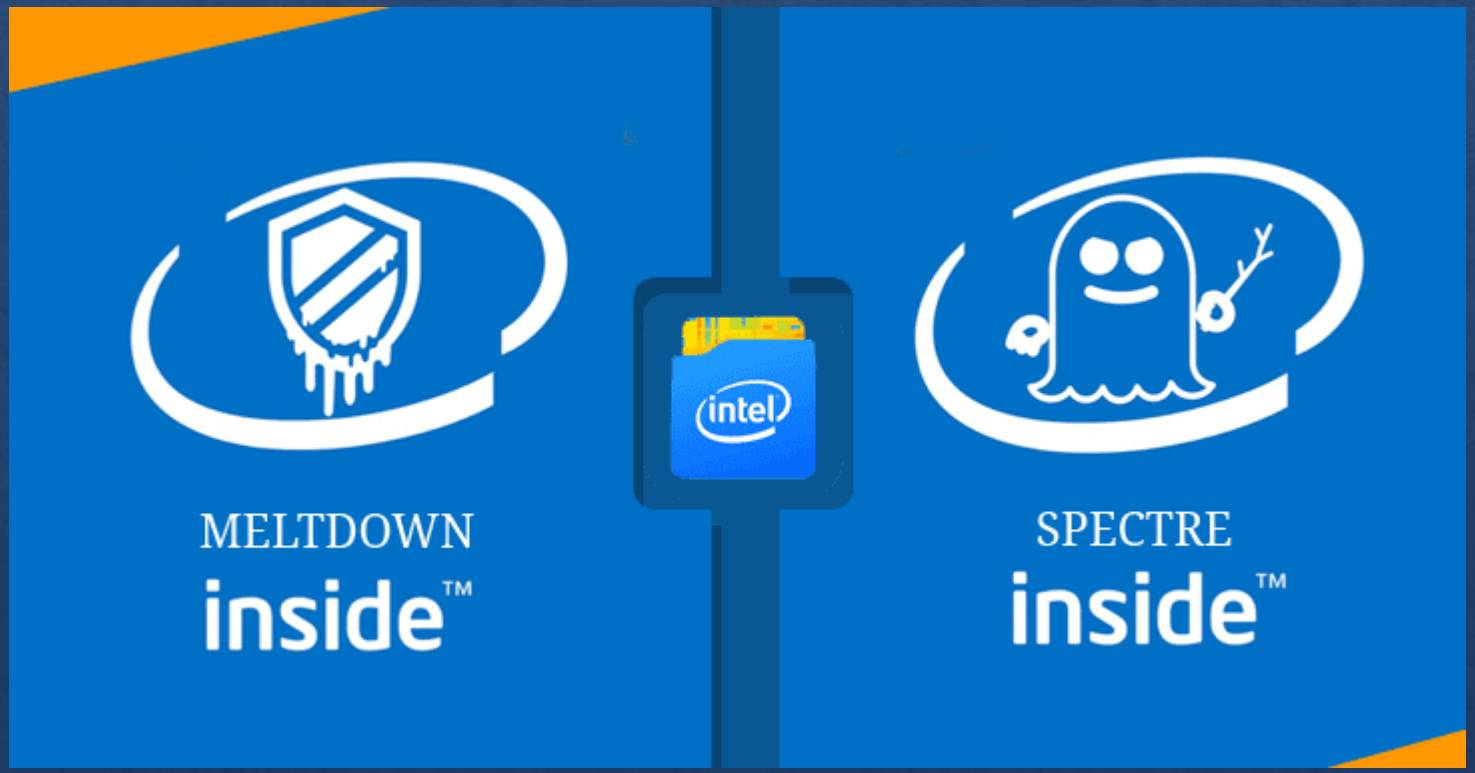
- Breaking WPA2 by forcing nonce reuse
- Key Reinstallation Attack – Inject / Replay WPA2 key – Totally transparent to end user.
- Ability to intercept and decrypt packets sent by clients
- Does not require knowledge of the WPA2 password.
- An Attacker can hijack TCP connections.
  - Fixed by Firmware updates
  - https://www.krackattacks.com/

Strava Fitness

- Strava is a website and mobile app used to track athletic activity via satellite navigation
- Styled as a "Social Network for Athletes", it can be used for a number of sporting activities however the most popular activities tracked using the software are cycling and running.
- Records fitness data and insecurely publishes personal training sessions into the cloud
- Strava user location data has been seen in remote locations in developing countries corresponding with the presence of western military personnel utilizing the service whilst on deployment. Some data showed known US bases in Syria, forward operating bases in Afghanistan and a trace from someone in Area 51
- Congressional investigation on why Strava published heat maps and what data it is collecting.
  - https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Strava%20Briefing%20Request.2018.01.31.pdf

https://en.wikipedia.org/wiki/Strava

Meltdown & Spectre



Meltdown

- Meltdown exploits a race condition, inherent in the design of many modern Intel, IBM and ARM CPUs. This occurs between memory access and privilege checking during instruction processing combined with a cache side-channel attack; this vulnerability allows a process to bypass the normal privilege checks that isolate the process from accessing data belonging other running processes.
- Since many operating systems map physical memory, Meltdown effectively makes it possible for a rogue process to read physical memory, regardless of whether it should be able to do so.
- The vulnerability is viable on any operating system in which privileged data is mapped into virtual memory for unprivileged processes—which includes many present-day operating systems. Meltdown could potentially impact a wider range of computers than presently identified, as there is little to no variation in the microprocessor families used by these computers.
- A Meltdown attack cannot be detected if it is carried out.

Meltdown

- "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems" published at the 1995 IEEE Symposium on Security and Privacy warned against a covert timing channel in the CPU cache and translation lookaside buffer (TLB).
- On August 8, 2016, Anders Fogh and Daniel Gruss presented "Using Undocumented CPU Behavior to See Into Kernel Mode and Break KASLR in the Process" at the Black Hat 2016 conference.
- On December 27, 2016, at 33C3, Clémentine Maurice and Moritz Lipp of TU Graz presented their talk "What could possibly go wrong with <insert x86 instruction here>? Side effects include side-channel attacks and bypassing kernel ASLR" which outlined already what is coming.
- On February 1, 2017, the CVE numbers 2017-5715, 2017-5753 and 2017-5754 were assigned to Intel
- On February 27, 2017, Bosman et al. of Vrije Universiteit Amsterdam published their findings how address space layout randomization (ASLR) could be abused on cache-based architectures at the NDSS Symposium.

Meltdown

- In July 2017, CyberWTF website by security researcher Anders Fogh outlined the use of a cache timing attack to read kernel space data by observing the results of speculative operations conditioned on data fetched with invalid privileges.

  Meltdown was discovered independently by Jann Horn from Google's Project Zero, Werner Haas and Thomas Prescher from Cyberus Technology, as well as Daniel Gruss, Moritz Lipp, Stefan Mangard and Michael Schwarz from Graz University of Technology.[41] The same research teams that discovered Meltdown also discovered a related CPU security vulnerability now called Spectre.

- July 28, 2017, hardware and software vendors were made aware of the vulnerabilities and made public jointly, on January 3, 2018, several days ahead of the coordinated release date of January 9, 2018 as news sites started reporting about commits to the Linux kernel and mails to its mailing list. As a result, patches were not available for some platforms, such as Ubuntu, when the vulnerabilities were disclosed.
- On January 28, 2018, Intel was reported to have shared news of the Meltdown and Spectre security vulnerabilities with Chinese technology companies before notifying the U.S. government of the flaws.
- The security vulnerability was called Meltdown because "the vulnerability basically melts security boundaries which are normally enforced by the hardware."

Meltdown & Spectre

- 1/10/18 – ZDnet – Windows update crashing AMD systems
- 1/23/18 – Wired – Meltdown and Spectre Patching has been a total train wreck
- 1/29/18 - Microsoft issues emergency Windows update to disable Intel's buggy Spectre fixes
- 2/16/18 - Verge - Intel facing 32 lawsuits over Meltdown and Spectre CPU security flaws

Intel Newsroom

- By Date:
  Jan. 3, 2018: Intel Responds to Security Research Findings
  Jan. 4, 2018: Intel Issues Updates to Protect Systems from Security Exploits
  Jan. 4, 2018: Industry Testing Shows Recently Released Security Updates Not Impacting Performance in Real-World Deployments
  Jan. 8, 2018: Intel CEO Addresses Security Research Findings during 2018 CES Keynote Address
  Jan. 9, 2018: Intel Offers Security Issue Update
  Jan. 10, 2018: Intel Security Issue Update: Initial Performance Data Results for Client Systems
  Jan. 11, 2018: Intel's Security-First Pledge
  Jan. 11, 2018: Intel Security Issue Update: Addressing Reboot Issues
  Jan. 17, 2018: Firmware Updates and Initial Performance Data for Data Center Systems
  Jan. 22, 2018: Root Cause of Reboot Issue Identified; Updated Guidance for Customers and Partners
  Feb. 7, 2018: Security Issue Update: Progress Continues on Firmware Updates
  Feb. 14, 2018: Expanding Intel's Bug Bounty Program: New Side Channel Program, Increased Awards
- Feb. 20, 2018: Latest Intel Security News: Updated Firmware Available for 6th, 7th and 8th Generation Intel Core Processors, Intel Xeon Scalable Processors and More

Spectre

- Spectre Vulnerability
  - Branch prediction and speculative execution
  - Affects Intel, AMD, ARM and IBM

enisa

THE EU CYBERSECURITY AGENCY

VULNERABILITY	MELTDOWN	SPECTRE
Processors affected	Intel	Intel, AMD, ARM, (ARM based chips from Apple, Samsung, and Qualcomm)
Method	Out-of-order execution	Speculative execution, branch prediction
Attack vector	The attacker must be able to execute code on the target system.	The attacker must be able to execute code on the target system. Remote exploitation is possible through web-based attack using JavaScript, e.g. to attack browsers.
Impact	Reads kernel memory and physical memory from the user space (privilege escalation), i.e. the attacker can read secret data on the system. In cloud systems, the attack can give access to secret data of other tenants.	Reads the memory of a target/victim process running on the system, i.e. the attacker can leak process specific secret data. The attack needs to be tailored for the target process. A variant of the attack can be used in virtualised environments.
Solution	Operating system patch specific to Meltdown. Hardware-level fixes in future products.	Software patches for vulnerable processes, e.g. browsers. Bios/firmware updates. Hardware-level fixes in future products.

Spectre & Meltdown

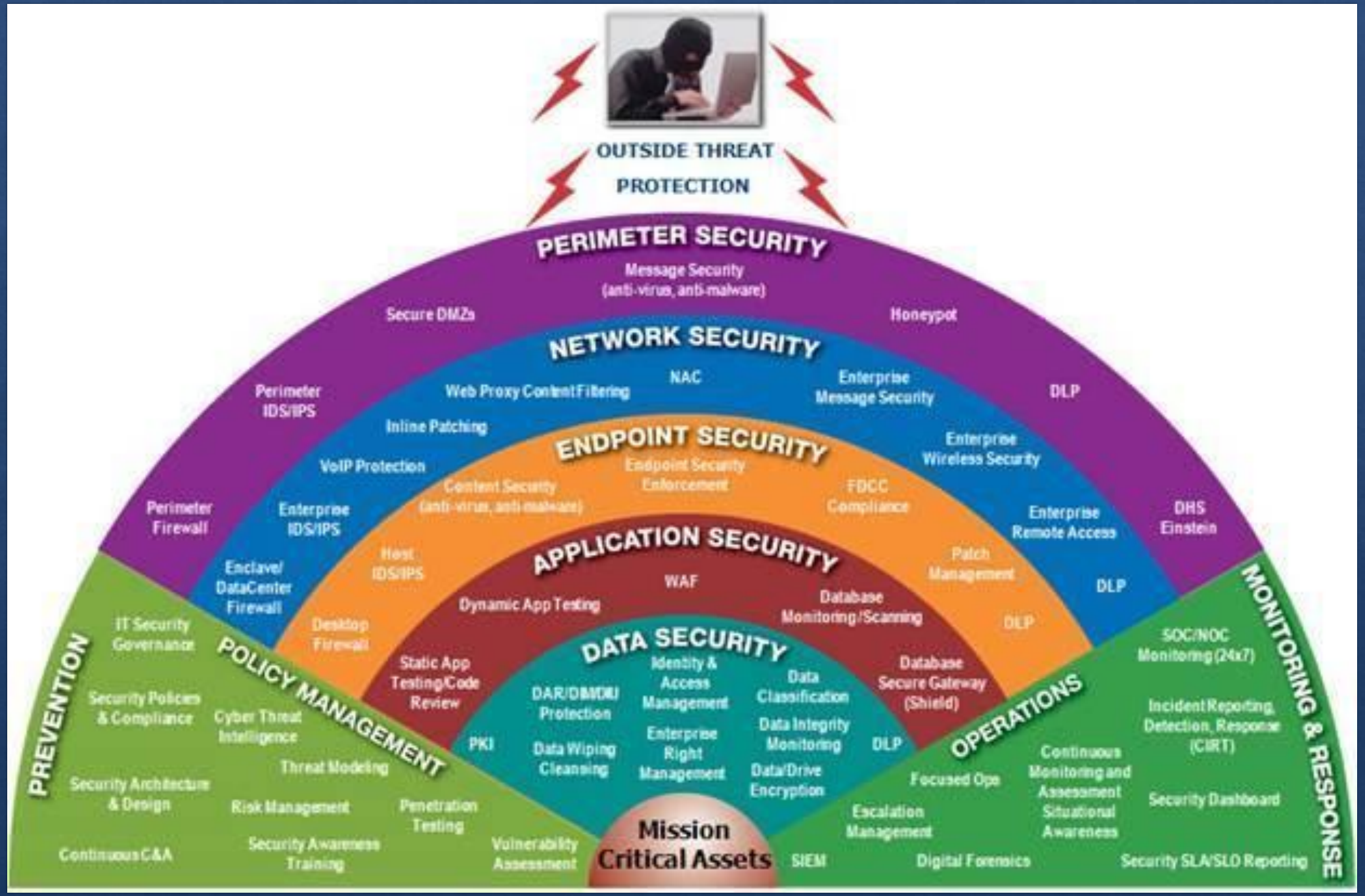
The basic difference between Spectre and Meltdown is that Spectre can be used to manipulate a process into revealing its own data. On the other hand, Meltdown can be used to read privileged memory in a process's address space which even the process itself would normally be unable to access (on some unprotected OS's this includes data belonging to the kernel or other processes).

The Meltdown paper distinguishes the two vulnerabilities thus: "Meltdown is distinct from the Spectre Attacks in several ways, notably that Spectre requires tailoring to the victim process's software environment, but applies more broadly to CPUs and is not mitigated by KAISER."

	Meltdown	Spectre
CVE	CVE-2017-5754	CVE-2017-5175 CVE-2017-5753
Impact	Easy to exploit	Difficult to exploit
Chipsets	Intel, IBM, ARM	Intel, AMD, ARM
Mitigation	OS level Patch and Firmware updates	Only browser solutions. No firmware solution yet.

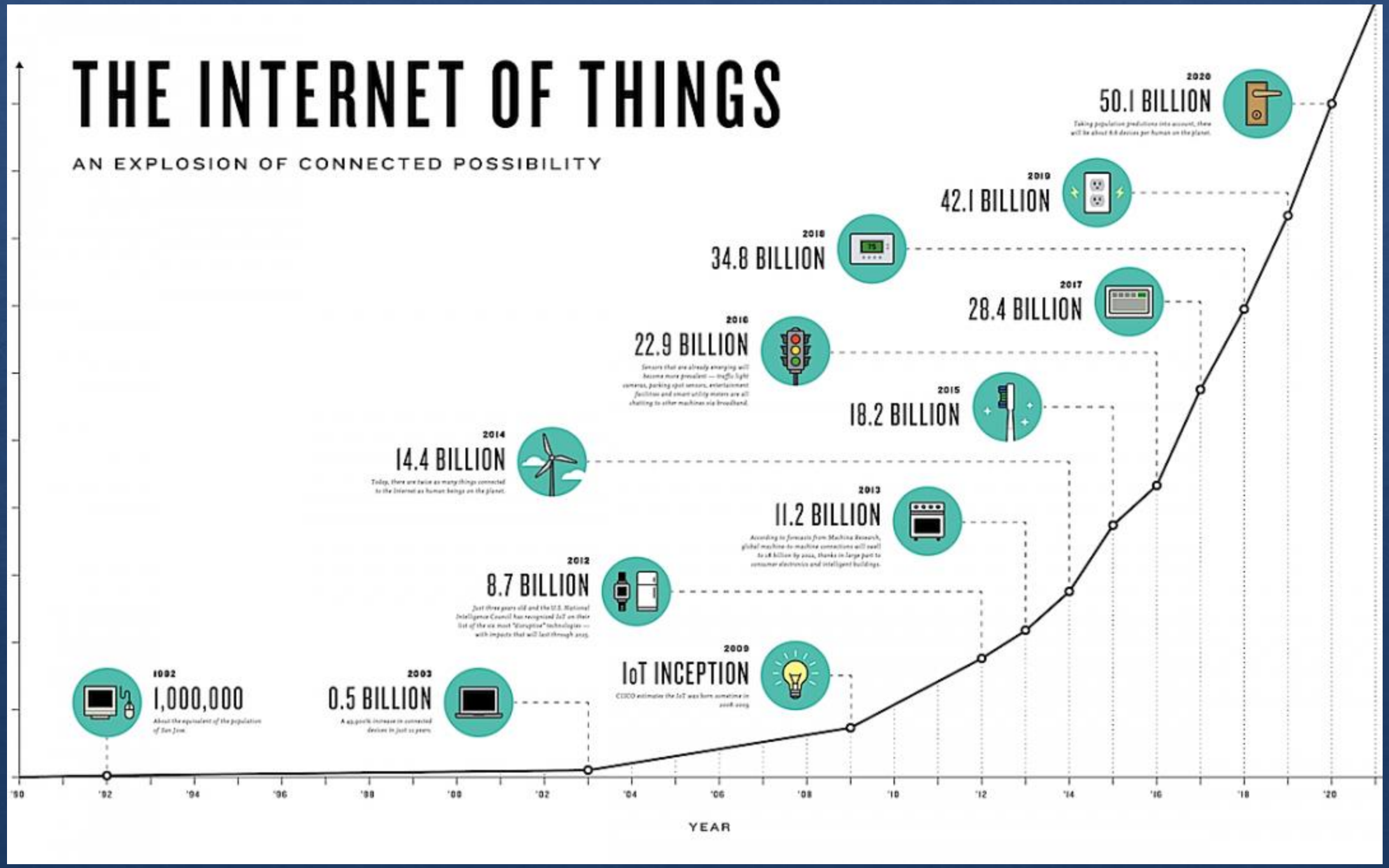
Current Trend

- Attacks are getting exponentially more sophisticated, and it is expected to get worse.
- Cloud attacks are on the rise with no end in sight.
- There are currently close to 200 researchers (professional hackers) working on exploits of Meltdown and Spectre.
- Attacks are coming from all sides and players
  - Organized Crime – driven by money
  - State Sponsored attacks – for intelligence, chaos and disruption
  - Script kiddies – e.g. Autosploit - now almost anyone can automate an attack on a system
  - Advertisers are mining crypto currencies in your browser. (i.e. Salon Magazine)
- 2017 – The year of wake-up calls on cybersecurity


OUTSIDE THREAT
PROTECTION
PERIMETER SECURITY
Message Security
(anti-virus, anti-malware)
Secure DMZs
Honeypot
NETWORK SECURITY
Perimeter
IDS/IPS
Web Proxy Content Filtering
NAC
Enterprise
Message Security
DLP
Inline Patching
ENDPOINT SECURITY
Endpoint Security
Enforcement
Enterprise
Wireless Security
VoIP Protection
Content Security
(anti-virus, anti-malware)
FDCC
Compliance
Perimeter
Firewall
Enterprise
IDS/IPS
Enterprise
Remote Access
DHS
Einstein
APPLICATION SECURITY
Host
IDS/IPS
Patch
Management
Enclave/
DataCenter
Firewall
WAF
DLP
Dynamic App Testing
Database
Monitoring/Scanning
Desktop
Firewall
DLP
DATA SECURITY
Static App
Testing/Code
Review
Identity &
Access
Management
Data
Classification
Database
Secure Gateway
(Shield)
DAR/DIM/DIU
Protection
PKI
Data Wiping
Cleaning
Enterprise
Right
Management
Data Integrity
Monitoring
DLP
Data/Drive
Encryption
PREVENTION
IT Security
Governance
POLICY MANAGEMENT
Security Policies
& Compliance
Cyber Threat
Intelligence
Threat Modeling
Security Architecture
& Design
Risk Management
Penetration
Testing
Continuous C&A
Security Awareness
Training
Vulnerability
Assessment
Mission
Critical Assets
OPERATIONS
SOC/NOC
Monitoring (24x7)
Incident Reporting,
Detection, Response
(CIRT)
Focused Ope
Continuous
Monitoring and
Assessment
Situational
Awareness
Security Dashboard
Escalation
Management
SIEM
Digital Forensics
Security SLA/SLO Reporting
MONITORING & RESPONSE

What to expect in the near future

- Increase in ransomware attacks.
  - Backup your systems Daily
- Increase in cryptocurrency theft and fraud.
  - Use a password safe, and don't reuse passwords. (remember Yahoo & LinkedIn breaches)
  - Use two factor authentication where you can. (i.e. Yubikey)
- Increase in targeted email attacks
  - Don't click on anything you didn't ask for or can not confirm
- Cloud Breaches will increase dramatically
- The good news is that Microsoft's latest OS is making headways with combating most of the common attacks.
- Protection of systems are getting better, but keeping up with security will always be a challenge
- Open Source Tools and analytics are competing head to head with Legacy Security tools.


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 49,900% increase in connected devices in just 10 years.
2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008-2009.
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
'90
'92
'94
'96
'98
'00
'02
'04
'06
'08
'10
'12
'14
'16
'18
'20
YEAR

Where all this is heading

- Expect US legislation / regulation similar to GDPR and/or NYDFS for all companies

GDPR:

Companies that collect data on citizens in European Union (EU) countries will need to comply with strict new rules around protecting customer data by May 25. The General Data Protection Regulation (GDPR) is expected to set a new standard for consumer rights regarding their data.

- Privacy violation or leakage of EU Personal Information can result in Fines up to 4% of annual worldwide turnover or 20MM Euros whichever is greater.
- EU Citizens have the right to be forgotten.

Recommendations

- Paranoia is a good thing.
- Use a Password safe, don’t reuse passwords between vendors or merchants. Use 20 character randomly generated Password or Pass phrases with non-alpha’s in-between phrases.
  - The Password crackers now use the “4” for “A” and “3” for “E” in the iterations and concatenate words and complex phrases.
- Don’t click on anything unless you asked for it or can verify it’s authenticity.
- Use Chrome or Firefox w/ Extensions or Add-ons (i.e Ublock Origin & NoScript)
- Use a DNS that will filter out the bad websites
  - (e.g. OpenDNS.com is Free for personal use)
- Use a PO Box for your financial mail.
- Shred all mail with you name on it before tossing it out in the trash.

Bonus

- https://www.youtube.com/watch?v=F78UdORll-Q

The

END