SENG 460 / ECE 574
Practice of Information Security and Privacy

Week 7:

Architecture, Cloud Operations,

Network Communications

IoT, Mobile

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Architecture

- translate business requirements into solutions that provide security for key assets
- system components (e.g. processors, storage, peripherals, OS)
- multitasking, multiprocessing, multithreading
- security zones

Architecture

- architecture
  - fundamental organization of a system embodied in its components, their relationships to each other and to the environment and the principles guiding its design and evolution
- architecture = what you need to have
- design = how you do it
- system architecture, computer architecture, CPU architecture (structure & security)
- operating system architecture (eg. monolithic, layered, microkernel, hybrid microkernel)

Architecture

- build security in from the ground up; security by design (good)
  - easier, simpler, faster, cheaper, more effective
- “bolt on” security after the fact (bad)
  - more difficult, slower, causes delay, expensive, less effective
- security policy
  - expresses what the security level should be by setting the security mechanisms are supposed to accomplish
  - foundation for specifications of a system and provides baseline for evaluating system

Architecture

- Enterprise Architecture
  - SABSA — Sherwood Applied Business Security Architecture
    business-driven, based on risk, relies on others (e.g. COBIT) for actual controls
    create top-down architecture for every requirement, control, process
    6 layers: contextual, conceptual, logical, physical, component, and
    Security Service Management Architecture (vertical)
  - TOGAF — the open group architecture framework
    defines architecture goals, benefits/vision, sets up projects to reach goals

University of Victoria

Architecture

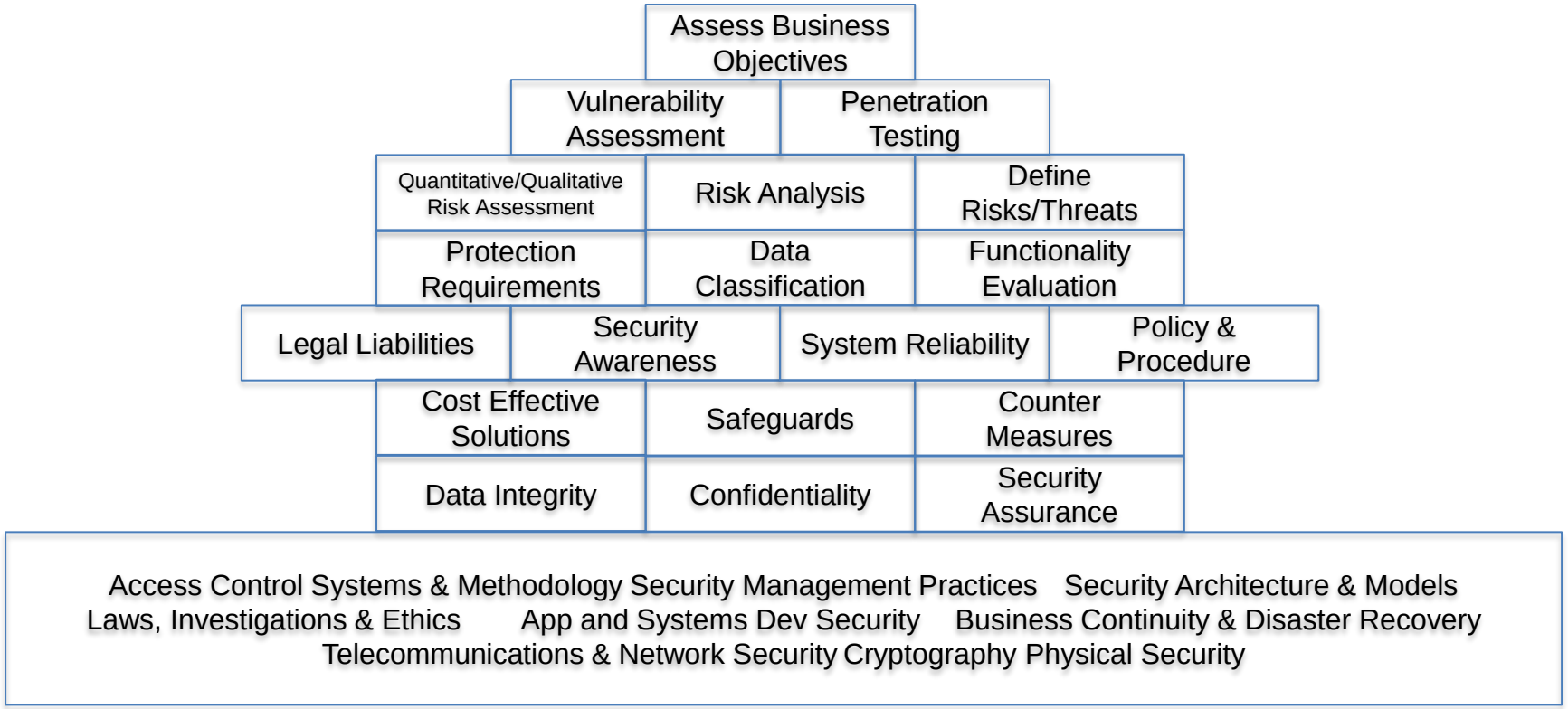
	SABSA (Sherwood Applied Business Security Architecture)	**TOGAF** (the open group architecture framework)	
Operational Layer	Contextual Layer	Business Architecture	describes processes business uses to meet goals
	Conceptual Layer		
	Logical Layer	Application Architecture	describes how applications are designed & how they interact with each other
	Physical Layer	Data Architecture	describes how data stores are organized/accessed
	Component Layer	Technical Architecture	describes hardware & software infrastructure that supports applications and interactions

University of Victoria

Information Security Journal: A Global Perspective, 21:47–54, 2012

Architecture

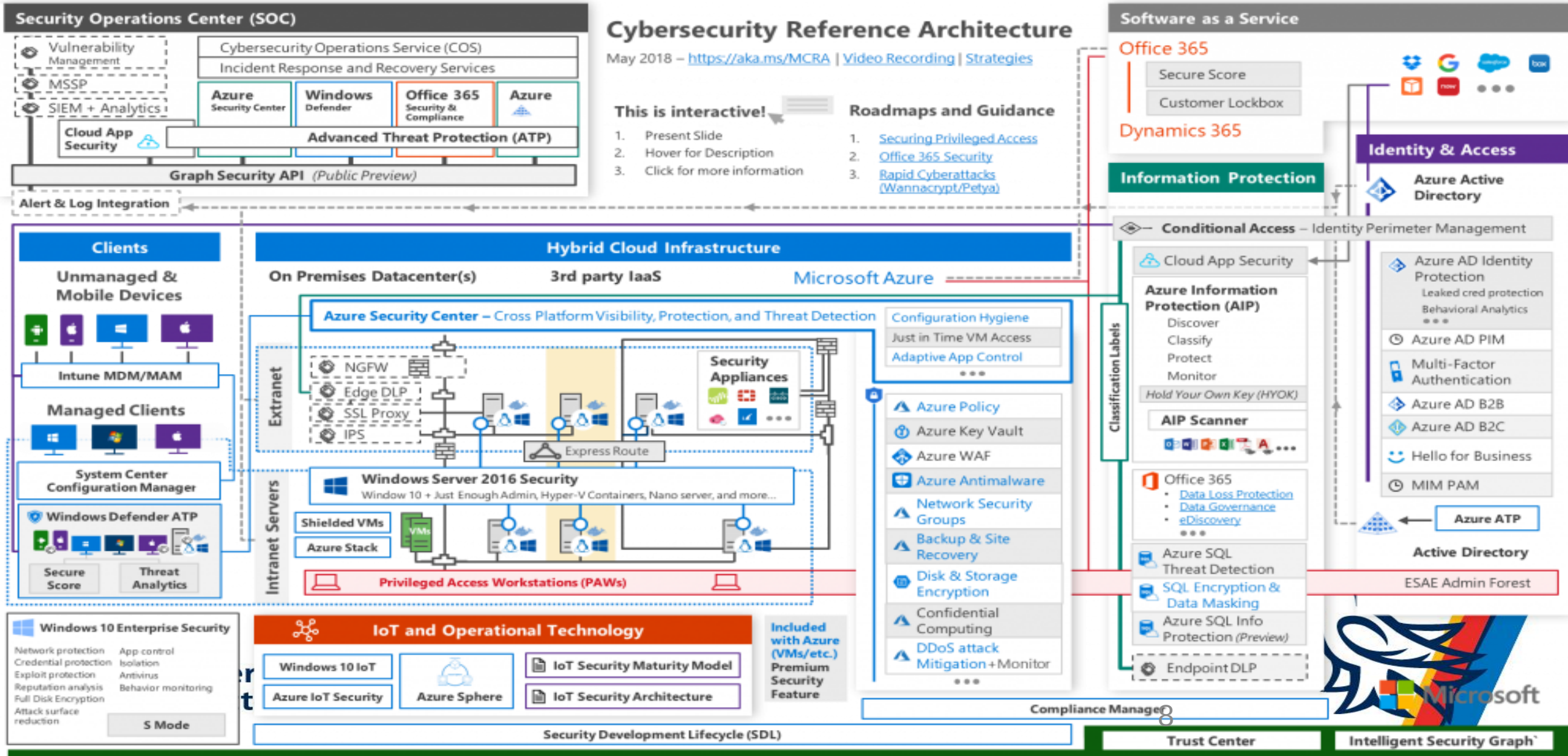
- another interpretation



University of Victoria

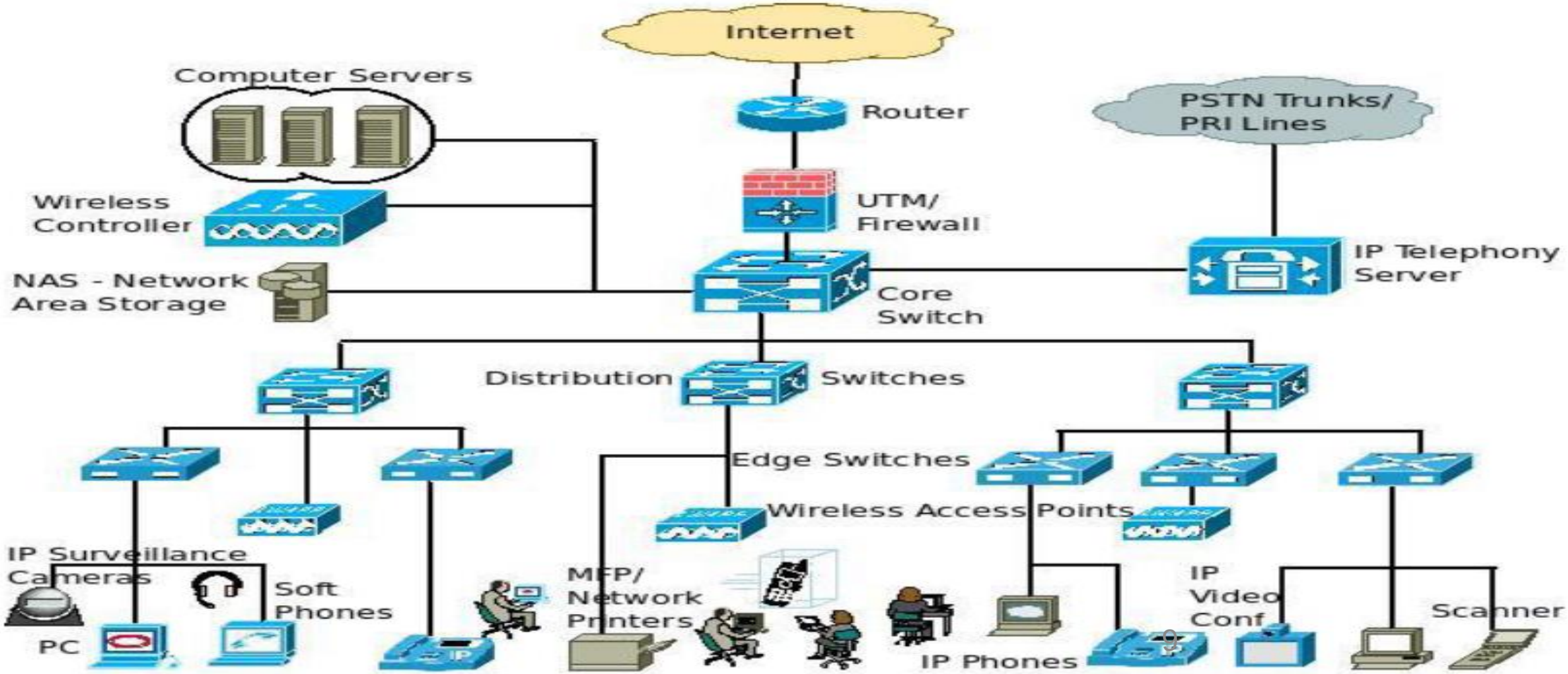
CISSP, Shon Harris

Architecture



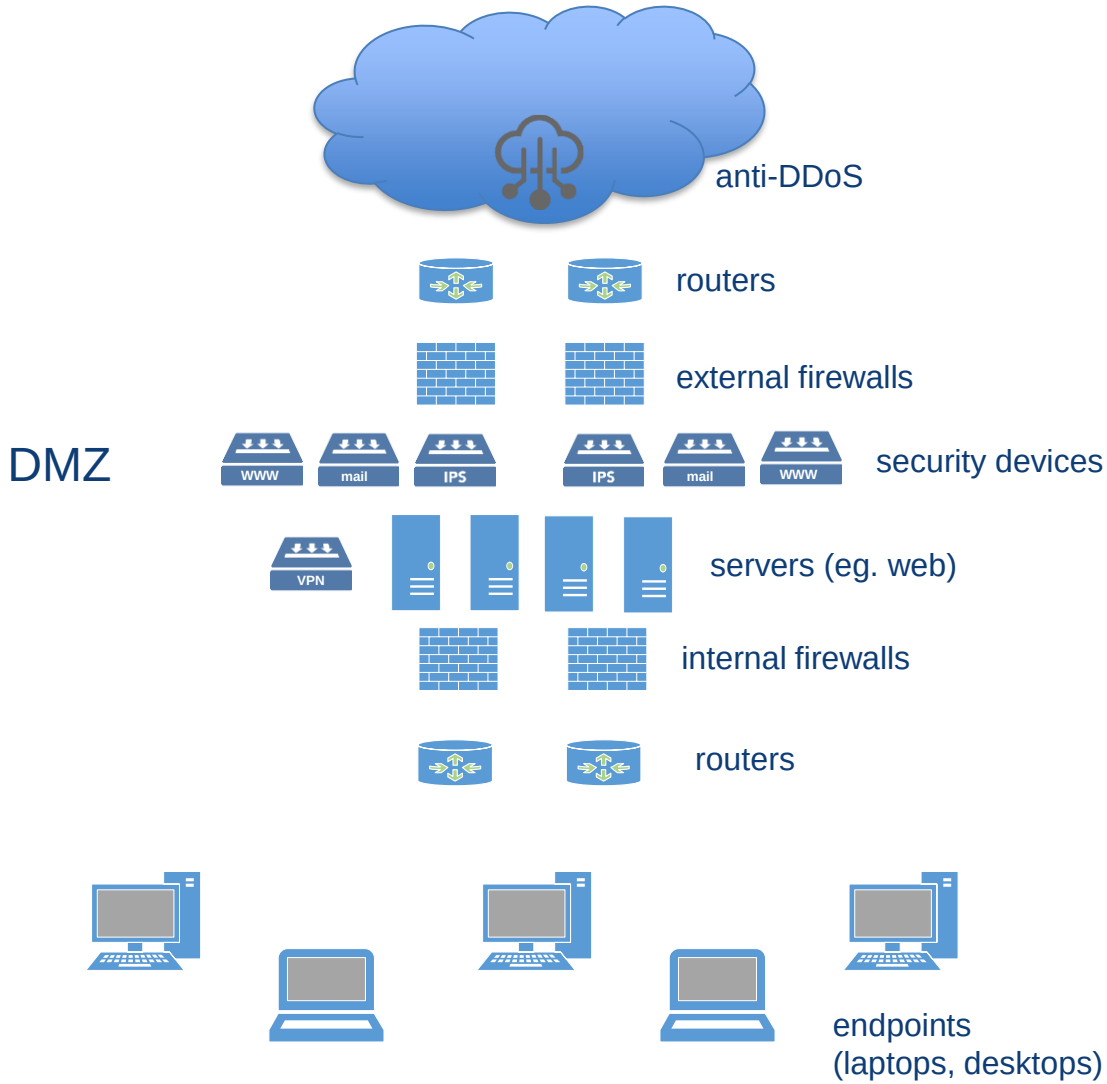
Architecture

- network architecture



Sample Network Diagram

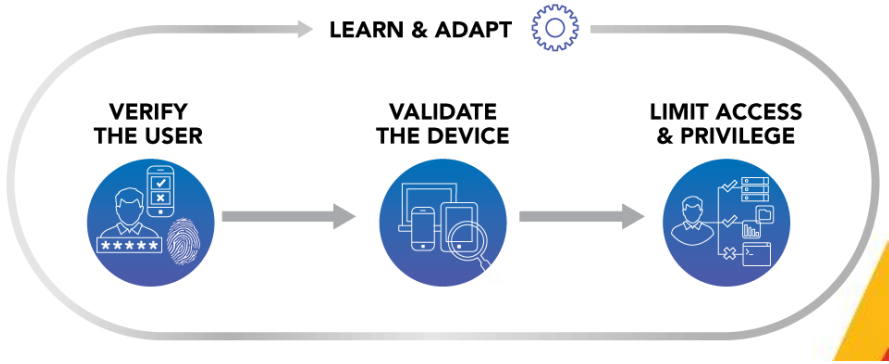
- cloud vs. traditional hosted services vs. client internet
- traffic paths in and out
- challenges examining encrypted traffic

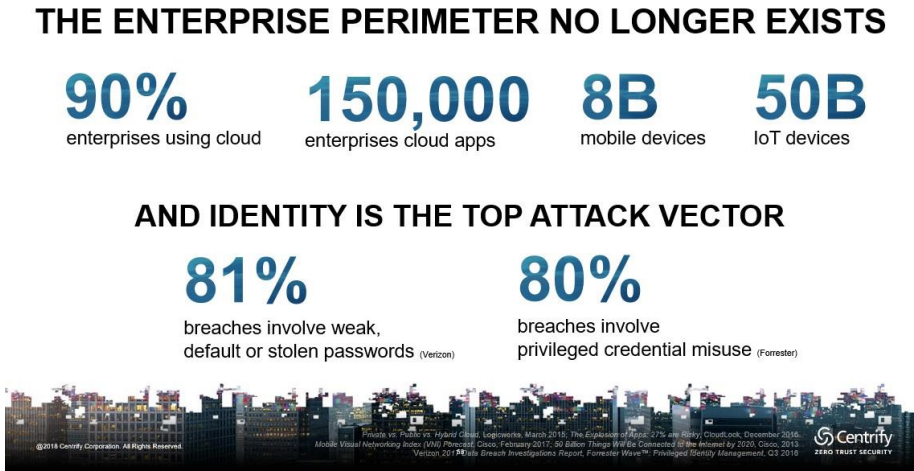


University of Victoria

Zero Trust

- concept that castle and moat doesn't work
- can't count on keeping bad guys out
- proposes to not trust anything
- no-one is trusted by default
- verification is required for everyone



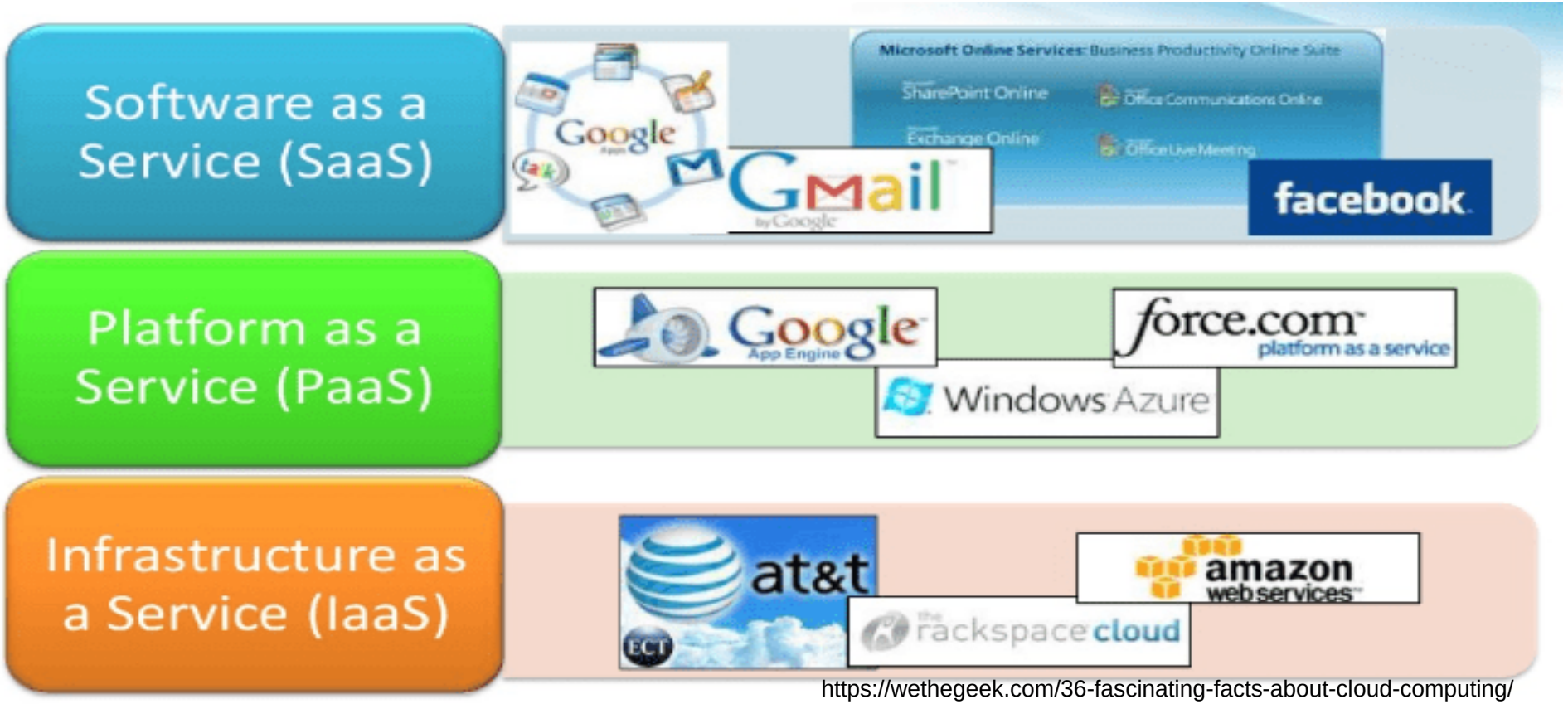


University of Victoria

Cloud Security

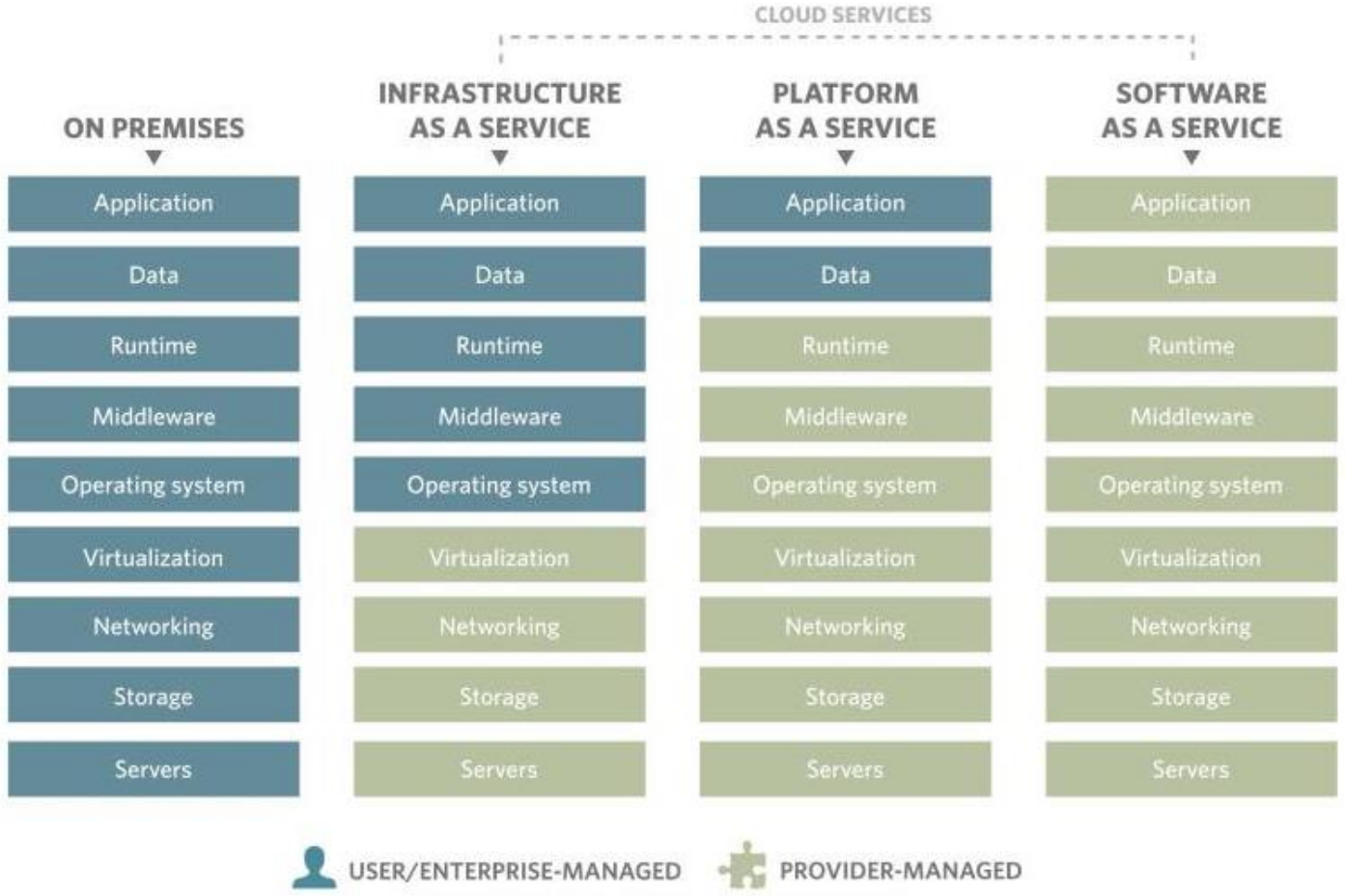
Cloud

- delivering hosted services over the internet
- three common types: SaaS, PaaS, IaaS

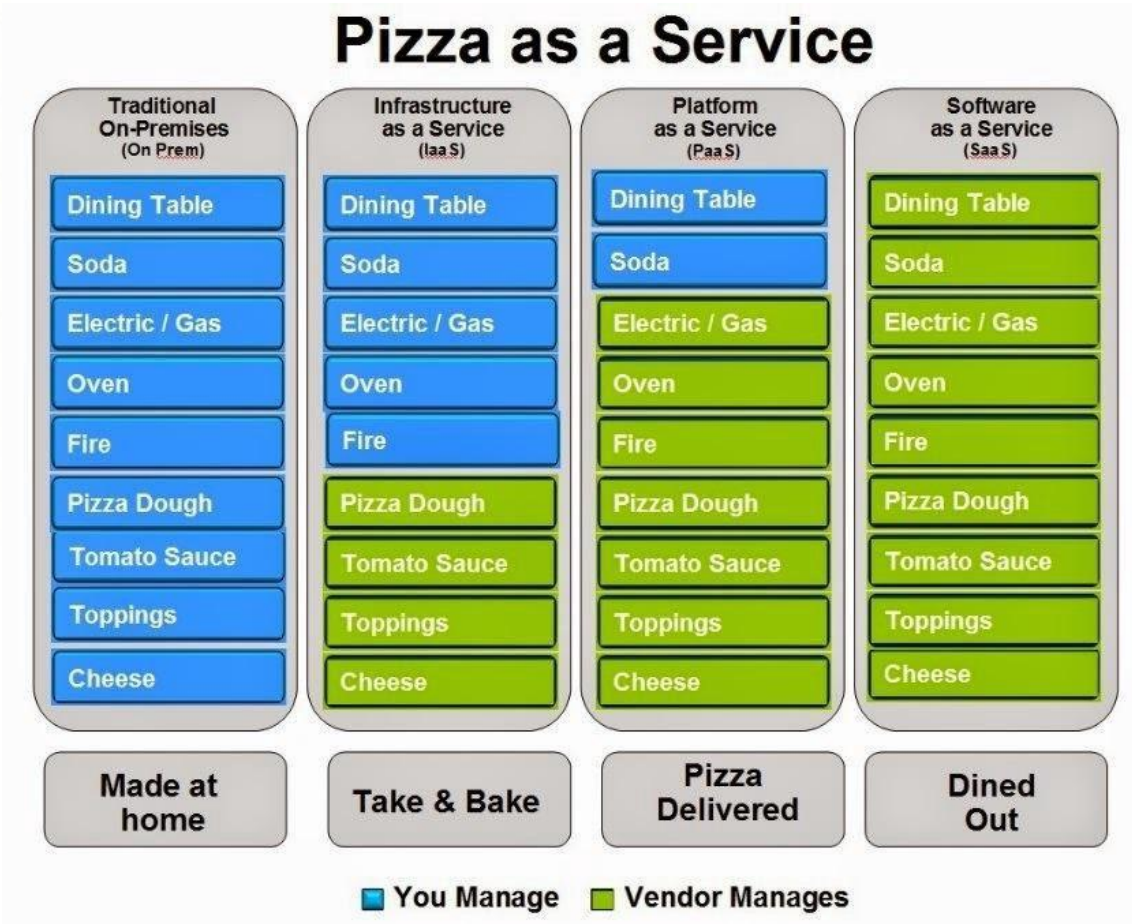


https://wethegeek.com/36-fascinating-facts-about-cloud-computing/

Cloud



University of Victoria



Cloud

- confusion and hype, real cloud vs. fake cloud
- adopting for wrong reasons
  - save money vs. flexibility vs. focus on core business
- absence of responsible adoption of the cloud
- unclear roles and responsibilities
  - who does investigations? incident response?
- cloud can have greater security
  - scale and ability to invest
  - requires customer to utilize the controls available

Cloud

- data classification is key
- data security in cloud
- encryption and access control
- who has the encryption keys?

University of Victoria

Cloud Security

- contracts
  - whose ‘paper’? (contract terms)
  - inability to customize agreements (e.g. ref Gartner*)
  - are there any “teeth” (penalties) in the contract?
- standards-based approach?
  - 3 cloud security standards/frameworks:
    - CSA Cloud Controls Matrix (CCM)
    - ISO 27017
    - NIST 800-53

Cloud Security

- consider traditional defence in depth
- consider traditional audit approaches often look for ‘air gaps’ between machines
  - air gap means the webserver and database are on two separate pieces of hardware
  - this is not the way things are done in cloud
- cloud security requires “east-west” controls as well as “north-south”
  - securing the hypervisor
  - defence in depth applied at a VM level
  - controls should follow VM around

University of Victoria

east-west: internal to internal
north-south: external to internal, internal to external

Cloud Examples

Microsoft's Cloud Email Breach Is a Cause for Concern

By: Sean Michael Kerner | April 15, 2019

NEWS ANALYSIS: Potentially millions of Microsoft email users on Outlook, Hotmail and MSN mail had their email information exposed after a Microsoft support person was breached, exposing a wider issue of risks that cloud services represent.

Microsoft has admitted that it suffered a data breach involving its web-based email services including Outlook.com, MSN.com and Hotmail.com that lasted for three months before it was detected and remediated.

Microsoft has not fully publicly disclosed how many customer accounts were impacted, and the company did not immediately respond to a request for comment from *eWEEK* on April 15. That said, Microsoft did send out an email late on April 12 to the unknown number of impacted users that was publicly posted on Reddit.

"We have identified that a Microsoft support agent's credentials were compromised, enabling individuals outside Microsoft to access information within your Microsoft email account," the Microsoft notice stated. "Upon awareness of this issue, Microsoft immediately disabled the compromised credentials, prohibiting their use for any further unauthorized access."

Microsoft claims in its advisory that the unauthorized access could have enabled an attacker to access email account information including the subject lines of emails and the names of contacts. The breach, according to Microsoft, lasted from Jan. 1 until March 28.

According to Microsoft, user email login credentials were not directly impacted by the incident, though out of an abundance of caution it is still suggesting that users reset their email passwords.

Further reading

Why You Don't Need to Change Passwords So Often

How Software-Defined Perimeter Mitigates Common Security...

Analysis

While breaches of any type and size are always a cause of concern, the method by which Microsoft's email services were breached is particularly troubling. This was not a breach of individual user passwords via some form of credential stuffing attack, where passwords stolen in other breaches were used again to gain access. Neither was it a new zero-day vulnerability in the email platforms that Microsoft provides.

This was a relatively simple attack, with very broad and surprising consequences. By Microsoft's own admission, a single Microsoft support agent's credentials were compromised. There is no official disclosure at this time about how the support agent's credentials were stolen, but there are any number of ways that a single user can have their credentials stolen—that's not the issue.

The issue is that a single set of user credentials enabled an attacker to see information from potentially tens of millions of Microsoft email users. This one single Microsoft support agent had access to the user accounts, representing what in a very real sense is a single point of failure.

It's not clear if the Microsoft support agent had two-factor authentication enabled, which potentially might have made it more difficult for an attacker to gain access to the email system. It's also not clear if Microsoft had some form of user behavior analytics that might have flagged a suspicious access pattern from the support agent. What is clear is that the attacker got access because the single support agent had access.

Microsoft is not alone in enabling its support staff to have seemingly broad access to user information. Amazon has recently been scrutinized for allowing some of its staff access to user information from its Alexa personal assistant service. And Facebook admitted on March 21 that it had left hundreds of millions of user accounts unencrypted in an internal system that was apparently used for auditing purposes. Google routinely had been looking in at some of its Google Cloud Platform (GCP) public cloud user accounts when maintenance was needed as well. In Google's case, however, the company has recently announced an effort to be more transparent and alert users when it wants access.

Headlines

Microsoft data breach exposes 250 million customer service and support records

Graham Cluley
1:55 pm, January 22, 2020

Such information could clearly be useful to a scammer posing as a genuine Microsoft support technician.

Microsoft is clearly embarrassed by the goof:

> *"Misconfigurations are unfortunately a common error across the industry. We have solutions to help prevent this kind of mistake, but unfortunately, they were not enabled for this database. As we've learned, it is good to periodically review your own configurations and ensure you are taking advantage of all protections available."*
>
> *"We want to sincerely apologize and reassure our customers that we are taking it seriously and working diligently to learn and take action to prevent any future reoccurrence. We also want to thank the researcher, Bob Diachenko, for working closely with us so that we were able to quickly fix this misconfiguration, investigate the situation, and begin notifying customers as appropriate."*

Microsoft says its investigation into the security breach has "found no malicious use" of the data, but that it has begun to notify customers whose data was present in the unsecured database.

Microsoft has admitted that between December 5th-31st 2019, a misconfiguration of the security rules for (what should have been) an internal customer support database left it exposed for anyone to access — no password required.

According to researcher Bob Diachenko, who discovered the database was accessible to anyone capable of running a web browser, the nearly 250

Headlines

Severe ‘Perfect 10.0’ Microsoft Flaw Confirmed: ‘This Is A Cloud Sec Nightmare’

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

AFP VIA GETTY IMAGES

‘This is a cloud security nightmare,” Check Point’s Yaniv Balmas tells me. “It undermines the concept of cloud security. You can’t prevent it, you can’t protect yourself. The only one who can is the cloud provider.” In this case that’s Microsoft, provider of the hyper scale Azure. Check Point is on a roll—a string of disclosures for vulnerabilities detected and disclosed in recent months. We’ve had

There are two vulnerabilities here. The first is a modest software bug that can be pushed hard to crash a system and escalate that crash to secure user privileges. And the second in a lack of security on a relatively arbitrary shared service that can be manipulated to break out of a user’s own part of the cloud infrastructure and onto the common shared hardware. That great advantage of the cloud, using only what you need, just when you need it, means you are a tenant in a server version of an apartment block. Check Point’s exploit built a master key for all the other apartments in that block.

Balmas fills in the gaps in terms of what this means. “We can break the isolation of Azure’s functions—now I can see everybody else’s functions. Anyone using Azure will be impacted—that means millions of users.” In addition to storing vast volumes of data in those isolated chambers, the cloud also runs countless programs. As a user, or “tenant,” you drop your code onto your cloud resource and it does the rest, running the program to order. Breaking that isolation enabled Check Point to access other tenants’ code running on any shared Azure server on which it was a tenant.

Microsoft quickly fixed the vulnerability when Check Point approached them in the fall, and customers who have patched their . The vulnerability is as punchy as it gets, “a s says, referring to the CVE score on Microsoft’s r. “It’s huge—I can’t even start to describe how for the hyperbole is that Balmas says his team e code execution (RCE) exploit on a major cloud ould break the cloud isolation separating rs, intercepting code, manipulating programs. basis of cloud security, enabling the safe sharing e.

when Microsoft patched the flaw, just a short er who successfully exploited this vulnerability vileged function run by the user to execute said at the time, “thereby escaping the Sandbox.” This week, Microsoft confirmed Check Point’s report, telling me that “we released updates to address these issues in 2019.” The spokesperson added that “customers who have applied the updates are protected,” as covered at CVE-2019-1372 and CVE-2019-1234.

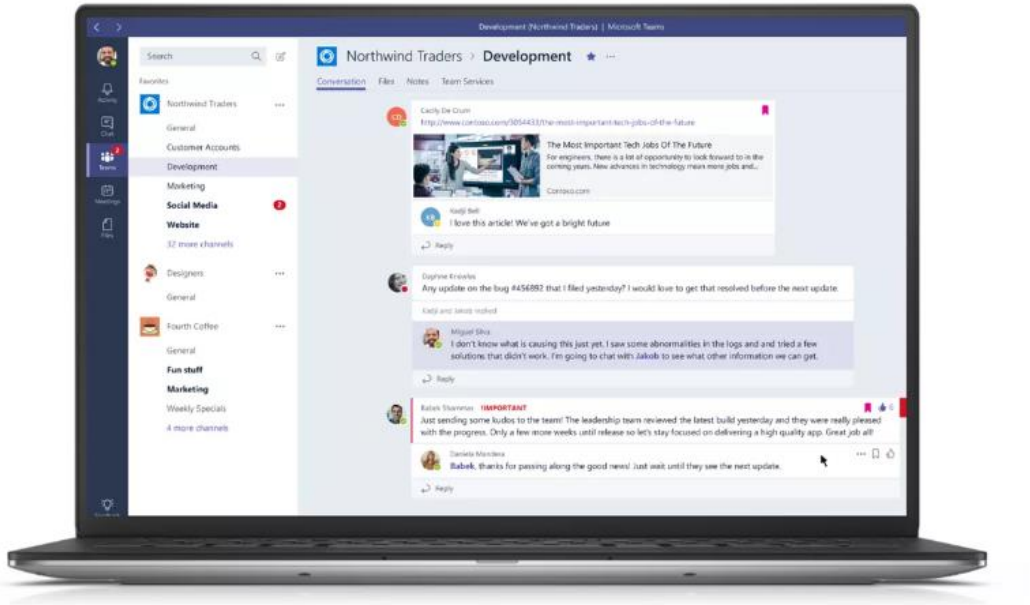
Headlines

Microsoft Teams suffers outage due to expired certificate, company says

The business communication platform was down for about three hours.

Shelby Brown February 3, 2020 11:04 AM PST

LISTEN - 00:30



Microsoft flubbed on its Teams app today.

Microsoft

Microsoft Teams experienced an outage on Monday after Microsoft failed to renew its authentication certificate. The tool was down for about three hours while Microsoft investigated and updated the certificate, according to the company's Twitter account. By noon ET, the service was working for most users. Microsoft didn't immediately respond for comment.

Microsoft 365 Status
@MSFT365Status

We're investigating an issue where users may be unable to access Microsoft Teams. We're reviewing systems data to determine the cause of the issue. More information can be found in the Admin center under TM202916

♡ 696 6:19 AM - Feb 3, 2020

673 people are talking about this

Microsoft Teams is a communication platform for businesses that offers chat, video meetings, file storage and more. It offers an alternative to Slack, another workplace collaboration app.

Microsoft 365 Status @MSFT365Status · 6h
We successfully deployed the fix to the affected infrastructure and conducted additional remediation actions to resolve the issue. More information can be found under TM202916.

8 24 67

Show this thread

Microsoft 365 Status @MSFT365Status · 11h
We've initiated the deployment of the updated certificate and are monitoring service health as the fix progresses. Additional information can be found under TM202916 in the admin center.

45 82 171

Show this thread

Microsoft 365 Status @MSFT365Status · 12h
We've determined that an authentication certificate has expired causing, users to have issues using the service. We're developing a fix to apply a new certificate to the service which will remediate impact. Further updates can be found under TM202916 in the admin center.

188 408 716

Show this thread

Cloud Examples

Zyng
Milli

By Kevin McLaugh

A hacker claim
to store user a
218 million us

The report she
in which it rev
accessed by ou
law enforceme

Now the quest
data centers o
commenting b
didn't respond

Zynga, an earl
private data ce
2015 and curr
services.

While it's not
misconfigurati
Capital One ac
gain access to
stored on AWS

How d
Amaz
bucke

Amazon launched
as a platform for
S3 buckets have
for everything fro
Netflix, Reddit, an
security principals

The issue of S3 b
prominent data b
United States Dep
common factor –
misconfigured se
wondering how th
security defaults

To Amazon's cred
by default. Admin
the public, and ot
hasn't always bee
bucket. It's possib
restricted permis
public access.

Imper
AWS

Imperva said it

By Catalin Cim

0

Cyber-security firm
mortem report of a
months ago, in Aug

The company blan
Services (AWS) AP
that was left acces

The post-mortem
the series of event
below:

AWS s
data b

Amazon Web Se
according to a M
passengers, incl

By Eileen Yu for

0

All Amazon Web Se
secured "with no fu
statement from the
security breach tha
Malindo's sister cor

Forensic and data
infrastructure, focu
a statement Thursc
financial institution

The airline reminde
unsolicited calls as
verification of their

The Malaysian carr
statement confirmi
hosted on AWS' clc
The cloud vendor,
GoQuo, had begun

Over
on ex

Leak originate

By Catalin Cim

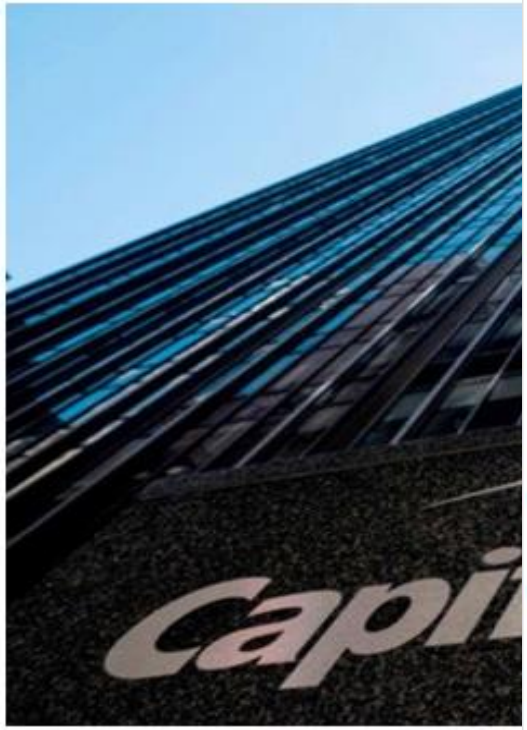
9

Data breach hunte
storing over 540 m
been collected by
affected users is b
of millions.

Capital One hac
investigation for
breaches

By Malcolm Owen
Thursday, August 15, 2019, 12:18 pm PT (03:1

The Seattle hacker behind the major
organizations, with authorities claimi
entities in other thefts from Amazon



Amazon hit with major
before Black Friday

Customers' names and email addresses posted on website, tech giant confirms

▲ Amazon said it has contacted customers that have been affected. Photograph: Alamy

Amazon has suffered a major data breach that caused customer names and email addresses to be disclosed on its website, just two days ahead of Black Friday.

The e-commerce giant said it has emailed affected customers but refused to give any more details on how many people were affected or where they are based.

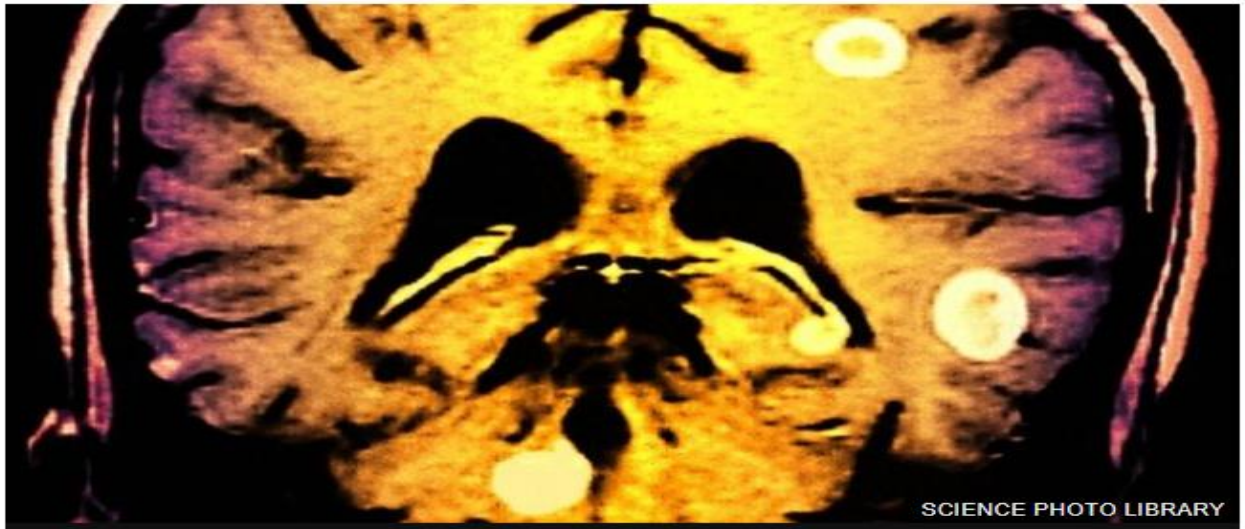
The firm said the issue was not a breach of its website or any of its systems, but a technical issue that inadvertently posted customer names and email addresses to its website.

In a short statement, Amazon said: "We have fixed the issue and informed customers who may have been impacted."

Headlines

Computer virus alters cancer scan images

4 April 2019 Share



The experimental malware could add fake tumours and other signs of disease to scans

A computer virus that can add fake tumours to medical scan images has been created by cyber-security researchers.

In laboratory tests, the malware altered 70 images and managed to fool three radiologists into believing patients had cancer.

The altered images also managed to trick automated screening systems.

The team from Israel developed the malicious software to show how easy it is to get around security protections for diagnostic equipment.

The program was able to convincingly add fake malignant growths to images of lungs taken by MRI and CT scanning machines.

A computer virus that can add fake tumours to medical scan images has been created by cyber-security researchers.
In laboratory tests, the malware altered 70 images and managed to fool three radiologists into believing patients had cancer.
The altered images also managed to trick automated screening systems.
The team from Israel developed the malicious software to show how easy it is to get around security protections for diagnostic equipment.
The program was able to convincingly add fake malignant growths to images of lungs taken by MRI and CT scanning machines.

Images and scans were vulnerable, said the researchers, because the files were generally not digitally signed or encrypted. This means any changes would be hard to spot.

Ensuring privacy and security guardrails

Free Training!

Everyone involved with cloud should take the following 2 courses:

1) AWS Cloud Practitioner Essentials (Course – 6 hours)

- https://www.aws.training/Details/Curriculum?id=27076
- This course covers the following concepts: Cloud Concepts Introduction, AWS Core Services, AWS Enhanced Services, AWS Architecting, Security, Pricing and Support

2) Azure Fundamentals (Course – 10 hours)

- https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals
- This course covers cloud concepts such as High Availability, Scalability, Elasticity, Agility, Fault Tolerance, and Disaster Recovery and understand the benefits of cloud computing
- Also compare and contrast basic strategies for transitioning to the Azure cloud and explore the services available in Azure including compute, network, storage and security

University of Victoria

Amazon AWS

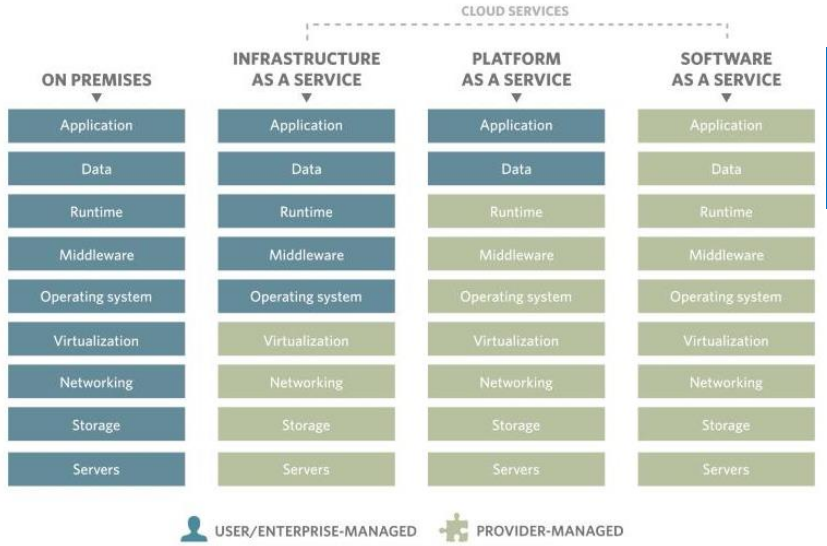
AWS Shared Responsibility Model (5 mins)	Introduction to AWS Marketplace	Introduction to Cloud Adoption Framework	Job Roles in the Cloud	Introduction to AWS Management Console
AWS Security Fundamentals	Introduction to Data Encryption	Introduction to AWS Security Hub	AWS Cloud Practitioner Essentials: AWS Security	AWS Security Fundamentals
Network Ninja to Cloud Ninja	Introduction to AWS Identity and Access Management	AWS Certified Security	AWS Certified Advanced Networking	

University of Victoria

Microsoft Azure

Cloud Concepts - Principles	Microsoft runs on trust	Foundations of cloud computing for admins	Cloud Services – Introduction to Azure	Implement network security in Azure	Secure your cloud applications in Azure	Create security baselines
Create an Azure account	Manage security operations in Azure	Secure your cloud data	Implement VM security in Azure	Manage identity and access in Azure	Improve incident response w/ alerting on Azure	Intro to App Centre
Secure Azure AD users with MFA	Manage users and groups in Azure AD	Resolve security threats with Azure Security	Configure security policies to manage data	Identify security threats with Azure Security	Protect identity and access with MS 365	Strengthen Auth w/ MS 365
MS Cloud Adoption Framework for Azure	Overview of IAM in MS 365	Simplify Access and Identity Provisioning	Analyze your Azure infrastructure using logs	Provision and manage cloud services	See Azure in action	Secure your Azure resources with conditional access
Azure fundamentals	Cloud concepts – Principles of Cloud	Intro to Azure virtual machines	Top 5 security items to consider	Design for security in Azure	Security, responsibility, and trust	

Summary



- on-premises
  - you do everything
- three common types of Cloud:
  - Software as a Service (SaaS) – they do (almost) everything
  - Platform as a Service (PaaS) – they do everything but application/data
  - Infrastructure as a Service (IaaS) – they do some things
- cloud can have better security than traditional hosted services given scale and level of investment
  - **however you have to use the controls available to you**

University of Victoria

Summary

- three cloud standards/frameworks
  1. CSA CCM
  2. ISO 27017 (security) & ISO 27018 (privacy)
  3. NIST 800-53

- terms:
  - North-South traffic is in and out of the data centre
  - East-West traffic is within the data centre

- examples:
  - SaaS: Salesforce, Dropbox
  - PaaS: AWS Elastic Beanstalk, Heroku, Force.com
  - IaaS: Amazon AWS, Microsoft Azure

Network Communications

University of Victoria

OSI Model (Open Systems Interconnection)

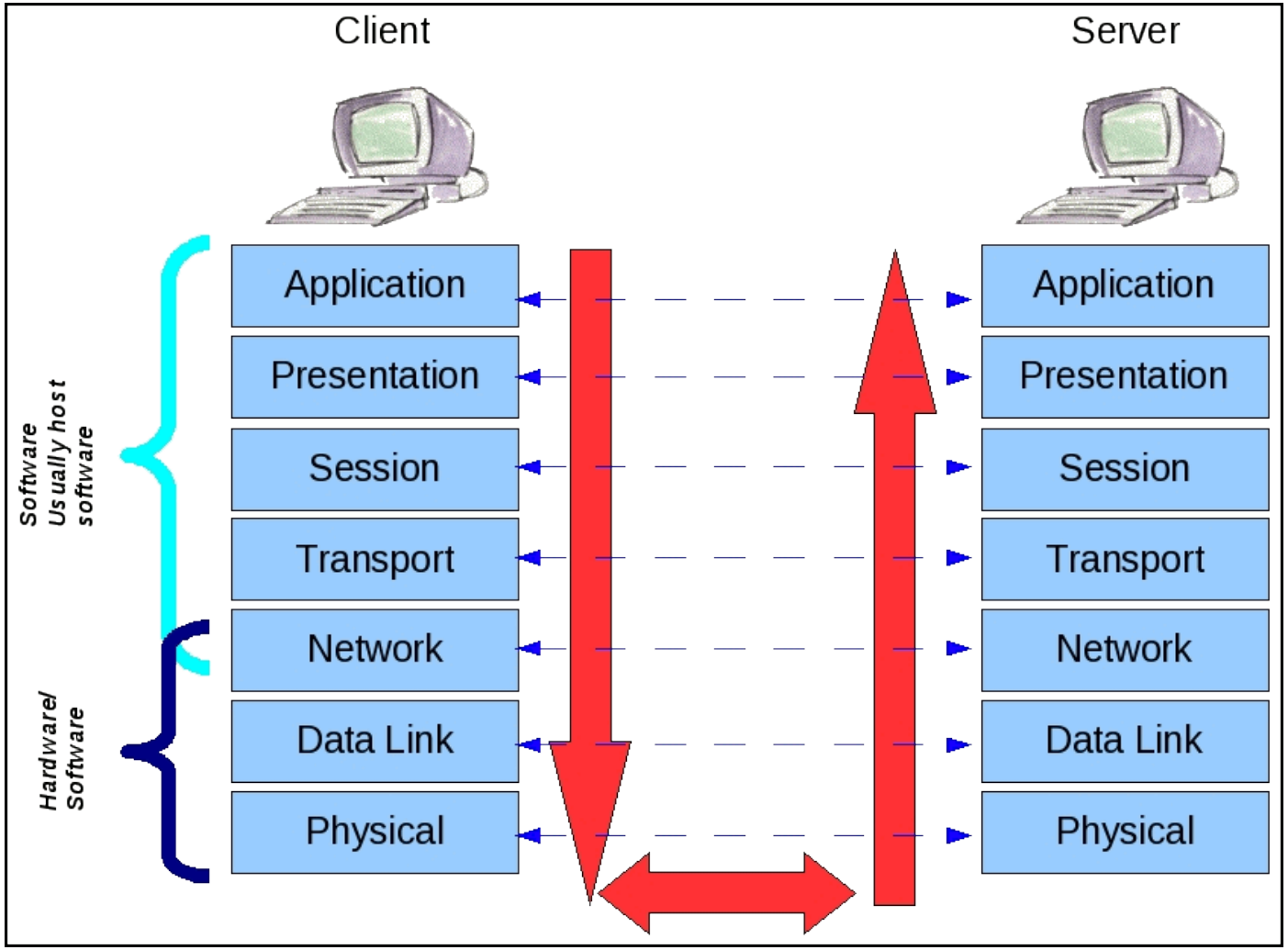
#	Layer	Purpose	Examples	DOD Model
7	Application	end user layer	SMTP, HTTP, FTP	Application
6	Presentation	encryption, decryption	JPEG, GIF	
5	Session	session management	logical ports RPC, SQL, NFS	
4	Transport	flow control	TCP, UDP	Transport
3	Network	router	IP, ICMP packets	Internet
2	Data Link	switch	frames	Network
1	Physical	hub/repeater	volts, bits	

PDNTSPA

also unofficial Layers 8, 9, and 10

University of Victoria

OSI Model (Open Systems Interconnection)



https://osimultimedia.weebly.com/how-the-osi-model-works.html

University of Victoria

Ports

- used for communicating between systems
- 65,535 TCP ports and 65,535 UDP ports

Port	Purpose
20/21	FTP
22 ✓	SSH
23	Telnet
25	SMTP
53	DNS
67/68 (U)	DHCP

Port	Purpose
69 (U)	TFTP
80	HTTP
110	POP
143	IMAP
443 ✓	HTTPS
1433	SQL

Port	Purpose
0-1023	well-known
1024-49,151	registered
49,152-65,535	dynamic / private

Certification

- different modes of communication
  - simplex data sent one direction only
  - half-duplex data sent in either direction but only one at a time
  - full-duplex data sent in both directions simultaneously (separate wires for each)
- broadcast domains part of network where broadcasts are forwarded

  e.g. all ports on hub/switch
- collision domains part of network where collisions can occur

  two devices send packet at same time

  e.g. affects hubs

University of Victoria

Certification

- ICMP — internet control message protocol
  (used by routers to send error messages)
- MPLS — multiprotocol label switching
  - LSP — label switched path – tunnel between pair of routers
  - LER — label edge router – router that first encapsulates a packet
  - LSR — label switch router – does MPLS switching in middle of LSP
  - egress node — final router at end of LSP
- VOIP — Voice-over-IP
  - SIP — session initiation protocol

University of Victoria

Certification

- identify elements used for network profiling
  - total throughput
  - session duration
  - ports used
  - critical asset address space

- identify these elements used for server profiling
  - listening ports
  - logged in users/service accounts
  - running processes
  - running tasks
  - applications

Certification

- WiFi
  - encryption — WEP WPA WPA2 TKIP LEAP
  - evil twin — setting up a fake WiFi access point to get users to connect through the attacker
  - rogue AP — rogue access point – evil twin is an example
  - jamming — deliberately blocking or interfering with authorized WiFi access point
  - deauth — using wireless network sniffing to get victim MAC address and send a disconnect

- Wireless Standards
  - 802.11b — bandwidth up to 11Mbps at 2.4 GHz
  - 802.11a — bandwidth up to 54 Mbps at 5 GHz
  - 802.11g — bandwidth up to 54 Mbps at 2.4 GHz
  - 802.11d — to emulate 802.11b for countries where 2.4 GHz is not available
  - 802.11f — improves 802.11 handover mechanism to maintain connection while roaming
  - 802.11h — improves on 802.11a by adding better control over channel selection and transmission
  - 802.11i — deals with security based on AES
  - 802.11j — changes to 5GHz signaling capabilities to support Japan's regulatory requirements
  - 802.11n — bandwidth 100+ Mbps

- worth noting
  - LAN — local area network
  - WAN — wide area network
  - WLAN — wireless local area network
  - **802.1x** — **standard for port-based Network Access Control (PNAC)**
    provides authentication for devices looking to connect to a LAN or WLAN

Certification

- security terms
  - pass the hash — obtaining hash of target user accounts and replaying it on a target system
  - honeypots — system with the purpose of detecting, deflecting, or counteracting unauthorized use of a system may intentionally have vulnerabilities
  - honeynets — network set up with intentional vulnerabilities to invite attack to study attacker's methods
  - tarpit — system that purposely delays incoming malicious or nuisance traffic
  - faraday bag — enclosure to block electromagnetic fields
  - faraday cage — grounded metal screen to exclude electrostatic and electromagnetic influences
  - fuzzing — testing to discover errors and vulnerabilities by sending invalid, unexpected, or random data (called fuzz) to a system to make it crash or be exploited
  - wardialing — dialing every number to gather information and identify vulnerable systems (also demon dialing)
  - wardriving — searching for WiFi networks by a person in a moving vehicle
  - warwalking — searching for WiFi networks by a person who is walking
- security programs (historical)
  - ToneLoc — popular wardialing computer program from the 90's
  - SATAN — security administrator tool for analyzing networks developed in the 90's
  - COPS — computer oracle and password system (vulnerability scanner) – 12 scanners in one (80's, 90's)
  - Cain & Abel — password recovery tool for Windows (dictionary attacks, brute force, and cryptanalysis)
  - L0phtCrack — password auditing and recovery application for Windows

Certification

- implement and manage engineering processes using secure design principles
- understand the fundamental concepts of security models
- select controls based upon systems security requirements
- understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- assess and mitigate vulnerabilities in web-based systems
- assess and mitigate vulnerabilities in mobile systems
- assess and mitigate vulnerabilities in embedded devices
- apply cryptography
- apply security principles to site and facility design
- client-based systems
- server-based systems
- database systems
- cryptographic systems
- Industrial Control Systems (ICS)
- cloud-based systems
- distributed systems
- Internet of Things (IoT)

Certification

- understand and apply fundamental concepts of networking
- OSI and TCP/IP models
- network topographies (e.g., ring, star, bus, mesh, tree)
- network relationships (e.g., peer to peer, client server)
- transmission media types (e.g., fiber, wired, wireless)
- commonly used ports and protocols
- understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)
- manage network access controls
- network access control and monitoring (e.g., remediation, quarantine, admission)
- network access control standards and protocols (e.g., IEEE 802.1X, Radius, TACACS)
- remote access operation and configuration (e.g., thin client, SSL VPN, IPSec VPN, telework)
- manage network security
- logical and physical placement of network devices (e.g., inline, passive)
- segmentation (e.g., physical/logical, data/control plane, VLAN, ACLs)
- secure device management
- operate and configure network-based security devices
- firewalls and proxies (e.g., filtering methods)
- network intrusion detection/prevention systems
- routers and switches
- traffic-shaping devices (e.g., WAN optimization, load balancing)

Certification

- operate and configure wireless technologies (e.g., bluetooth, NFC, WiFi)
- transmission security
- wireless security devices (e.g.,WIPS, WIDS)
- implement secure design principles in network architectures
- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking
- implications of multilayer protocols
- converged protocols
- software-defined networks (SDN)
- wireless networks
- secure network components
- operation of hardware
- transmission media
- Network Access Control (NAC) devices
- endpoint security
- content-distribution networks (CDN)
- implement secure communication channels according to design
- voice
- multimedia collaboration

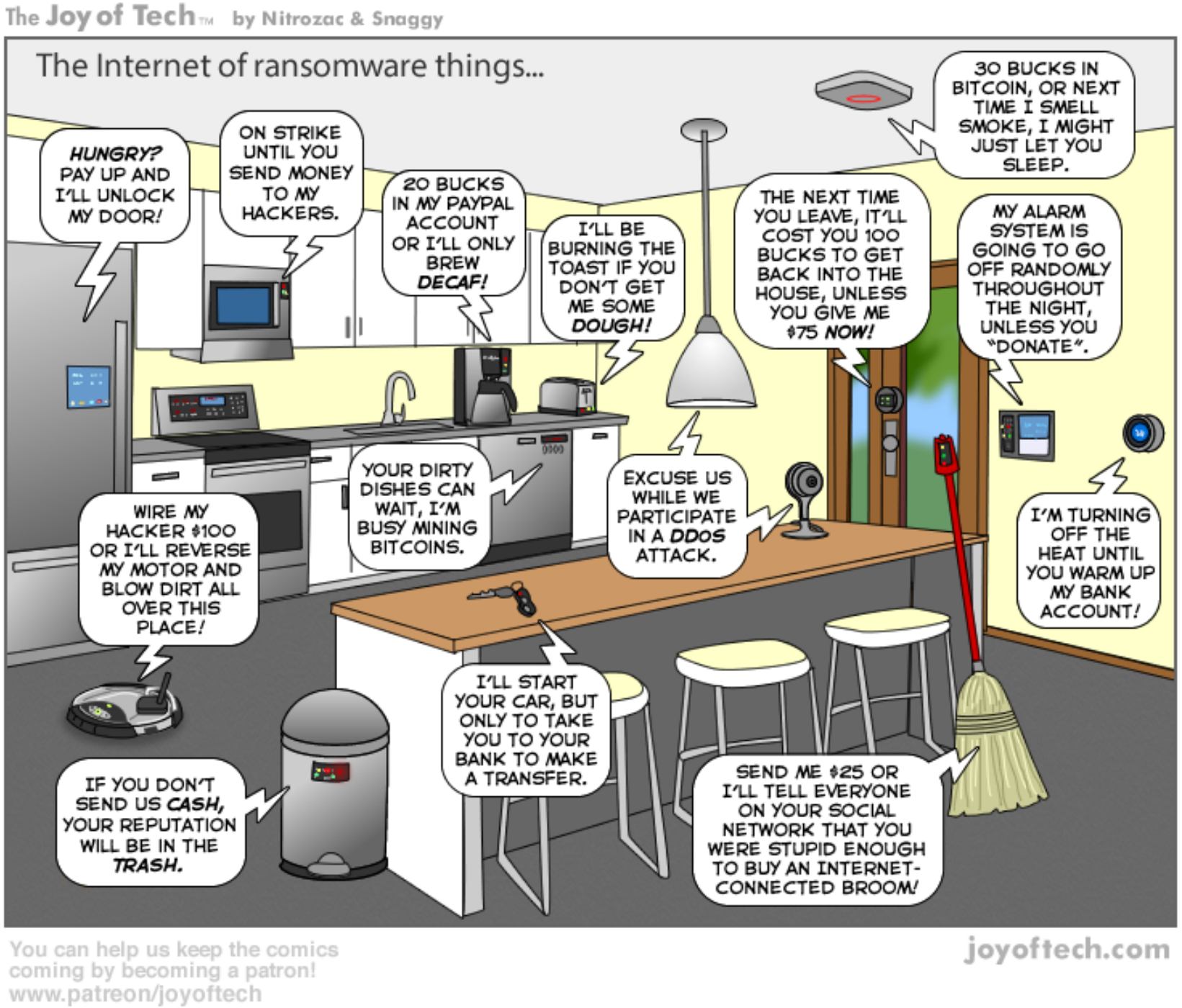
Certification

- remote access
- data communications
- virtualized networks
- implement and operate endpoint device security and host-based sysems (HIDS, host-based firewalls)
- application white listing
- endpoint encryption
- Trusted Platform Module (TPM)
- secure browsing (e.g., sandbox)
- operate and configure mobile device security
- Mobile Device Management (MDM) (e.g., COPE, BYOD)
- operate and configure Internet of Things (IoT)
- Internet of Things security
- Operate and configure ICS/SCADA Security
- Operational Technology (OT) security
- Operate and configure cloud security
- Deployment models (e.g., public, private, hybrid, community)
- Service models (e.g., IaaS, PaaS and SaaS)
- Virtualization (e.g., hypervisor)

Internet of Things

- aka Internet of Everything

- aka Internet of Vulnerabilities



University of Victoria

Headlines

Are you watching your TV – or is your TV watching you?

Net Results: There's a reason why modern, feature-packed smart TVs are so cheap

Thu, Jan 17, 2019, 05:30

Karlin Lillington

1

Senior vice-president of Samsung Electronics America Dave Das showcases the QLED 8K smart television during CES in Las Vegas. Photograph: David McNew/AFP/Getty Images

There's a reason why those big, feature-packed televisions are so affordable, even the cutting-edge new ones shown off this month at the annual Las Vegas mega-electronics show CES.

I know what you are thinking: it's some TV variation on Moore's Law. The chips and electronics inside the big-screened behemoths keep growing more powerful as the costs of components drop. As with computers, so with TVs.

But that's not it. The real reason is that the TVs can access your data – your screen time, what you watch, what you subscribe to and, in some cases, what you say.

Because, in yet another example of the invisible creep of corporate surveillance – so subtle that you were probably not aware it was happening – your TV now monetises you. And your data is so valuable to TV manufacturers that it is the predominant influence on the cost of your television.

How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight

A detail from a slide from a marketing presentation by Samba TV looking at how it can analyze what viewers are watching, determine how many connected devices they have in the house and then target them with ads.

Headlines

The chief technology officer of major TV maker Vizio discussed this new paradigm in a Verge podcast from CES. Podcast host Nilay Patel notes that **"companies like Vizio would have to charge higher prices for hardware if they didn't run content, advertising and data businesses".** Oh. You can turn off this data business surveillance "feature" on your Vizio TV, notes Baxter, and Patel says "Baxter told me that he thinks Vizio is the industry leader in disclosing what tracking is happening and letting users opt in or out during set-up."

But this is only because the company was forced to do so last year as part of a $2.2 million settlement with the US Federal Trade Commission, after Vizio was accused of "monitoring what customers are viewing on 11 million smart televisions", according to the Courthouse News Service.

Your phone and TV are tracking you, and political campaigns are listening in

By EVAN HALPER FEB 20, 2019 | 4:00 AM | WASHINGTON

Smartphones and related devices have become ubiquitous in people's lives. They've also become potent tracking devices that data brokers can use to learn a person's whereabouts — information valuable to political campaigns. (Oli Scarff / Getty Images)

It was a crowded primary field and Tony Evers, running for governor, was eager to win the support of officials gathered at a Wisconsin state Democratic Party meeting, so the candidate did all the usual things: He read the room, he shook hands, he networked.

Then he put an electronic fence around everyone there.

The digital fence enabled Evers' team to push ads onto the iPhones and Androids of all those attending the meeting. Not only that, but because the technology pulled the unique identification numbers off the phones, a data broker could also use the digital signatures to follow the devices home. Once there, the campaign could use so-called cross-device tracking technology to find associated laptops, desktops and other devices to push even more ads.

Internet of Things

FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

By Charlie Osborne for Zero Day | August 30, 2017 -- 10:31 GMT (03:31 PDT) | Topic: Security

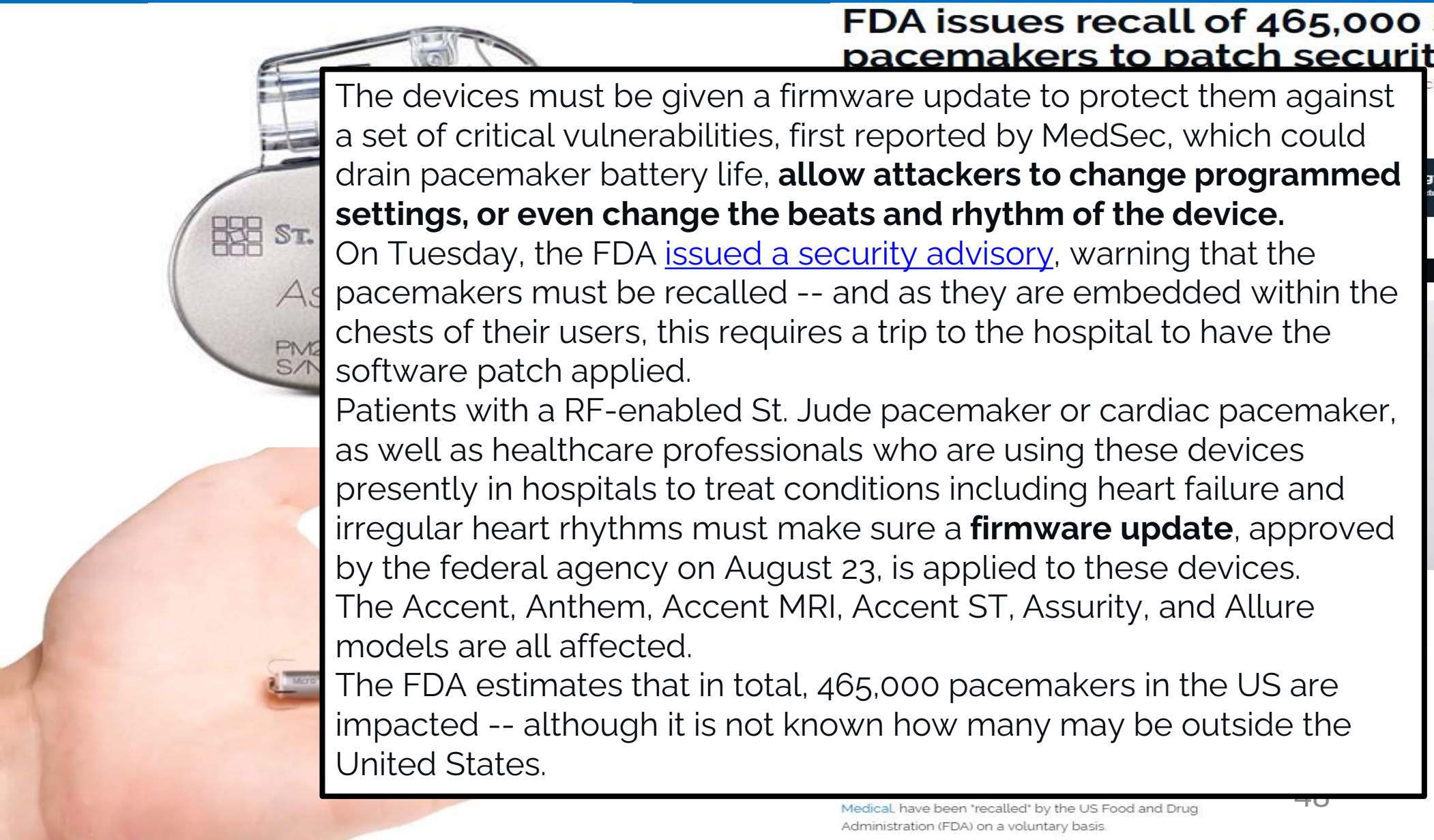
File photo

In what may be a first, patients with heart conditions that are using particular pacemaker brands will have to visit their doctors for firmware updates to keep their embedded devices safe from tampering.

It seems such an odd concept at first, but with many kinds of pacemakers now "smarter," with connections to mobile devices and diagnostic systems, the avenue has been carved for these medical devices to potentially be tampered with, should a threat actor choose.

In particular, Abbott's pacemakers, formerly of St. Jude Medical, have been "recalled" by the US Food and Drug Administration (FDA) on a voluntary basis.

Internet of Things



The devices must be given a firmware update to protect them against a set of critical vulnerabilities, first reported by MedSec, which could drain pacemaker battery life, **allow attackers to change programmed settings, or even change the beats and rhythm of the device.**

On Tuesday, the FDA [issued a security advisory](), warning that the pacemakers must be recalled -- and as they are embedded within the chests of their users, this requires a trip to the hospital to have the software patch applied.

Patients with a RF-enabled St. Jude pacemaker or cardiac pacemaker, as well as healthcare professionals who are using these devices presently in hospitals to treat conditions including heart failure and irregular heart rhythms must make sure a **firmware update**, approved by the federal agency on August 23, is applied to these devices.

The Accent, Anthem, Accent MRI, Accent ST, Assurity, and Allure models are all affected.

The FDA estimates that in total, 465,000 pacemakers in the US are impacted -- although it is not known how many may be outside the United States.

FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

...ched for the "voluntary" recall -- but

...gy ...tures, and the Download Now

RECOMMENDED FOR YOU

Endpoint Detection and Response: Automatic Protection Against Advanced Threats

White Papers provided by CrowdStrike

DOWNLOAD NOW

MORE FROM CHARLIE OSBORNE

Security
OceanLotus adopts public exploit code to abuse Microsoft Office software

Security
MyPillow and Amerisleep wake up to Magecart card theft nightmare

Security
Global threat group Fin7 returns with new SQLRat malware

Security
CUJO Smart Firewall vulnerabilities exposed home networks to critical attacks

Medical have been "recalled" by the US Food and Drug Administration (FDA) on a voluntary basis.

Review

- **IoT raises significant security and privacy concerns**
- devices were not created with security or privacy in mind
- *“often privacy and security are not ahead but often in the rearview mirror in danger of catching up” GP*
- *saying things are a “game changer” is often overused but Internet of Things is truly a game changer for privacy and security (so are big data and AI) GP*
- explosion of devices, significant number in the 10’s of billions
- “70% of IoT devices contain security vulnerabilities”

briankrebs
@briankrebs

Follow

vulnerabilities
passwords
security on IoT in general

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

3:02 AM - 21 Sep 2016

Brian Krebs site hit with 665 Gbps DDoS attack; Largest Internet has ever seen

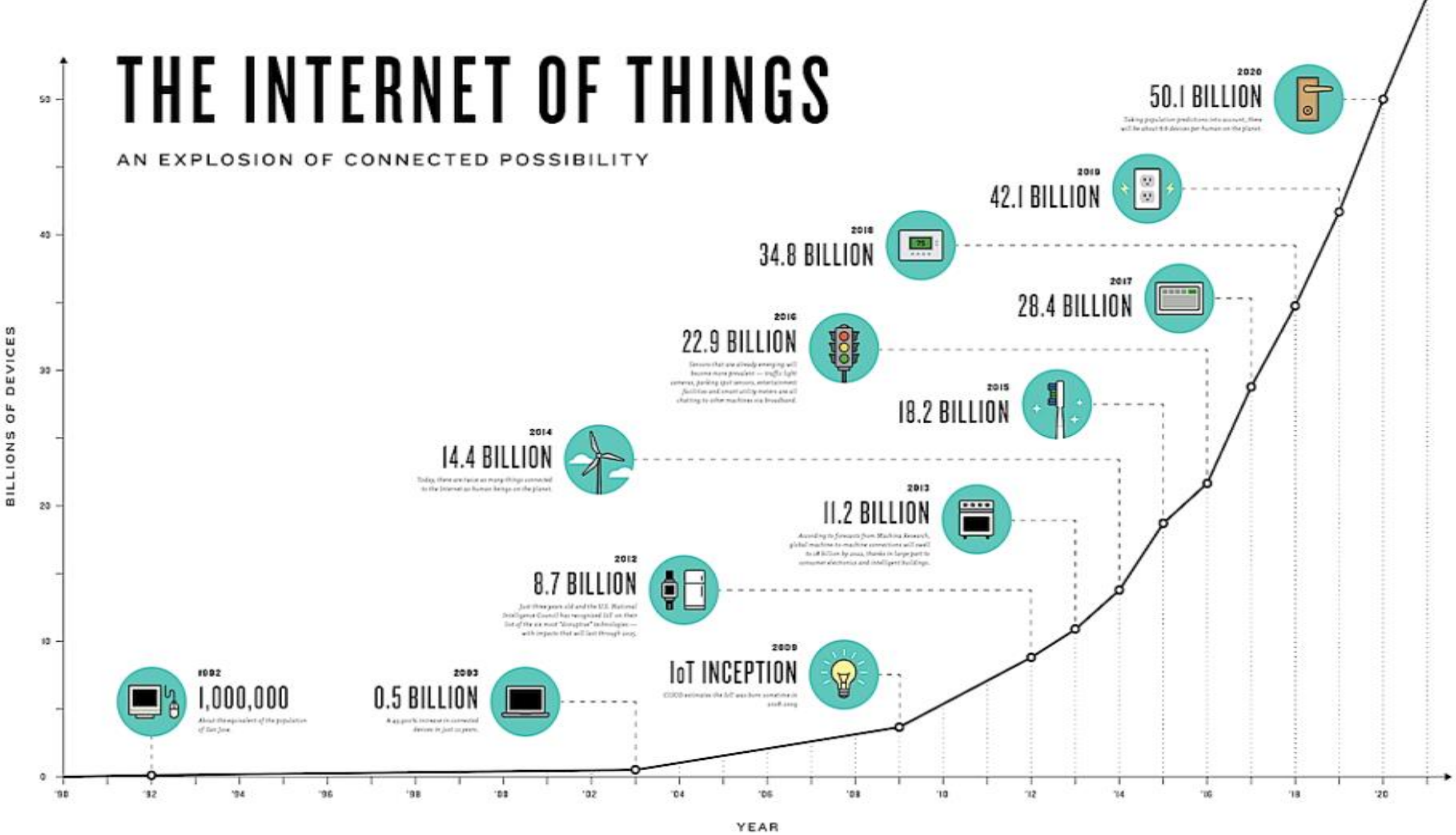
Colossal 1 terabyte per second DDoS attack hits French tech firm

Armies of hacked IoT devices launch unprecedented DDoS attacks

DDoS attacks got a power boost thanks to hundreds of thousands of insecure IoT devices

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY




05.06.40
PERSONAL
NUTRITION
SUGGESTED
ANALYSIS
15°C

LIFX

Live a more illuminated life

COLOR
1000

Couleur 1000/Farbe 1000

1055 LUMENS
75 WATT EQUIVALENT

1055 Lumens/équivalents 75 Watts
1055 Lumen/Equivalente a 75 Watt
1055 Lumen/75 Watt Äquivalent
1055 lúmenes/equivalente a 75 vatios

works with nest

WI-FI LED SMART BULB
MILLIONS OF COLORS AND WHITES

Ampoule LED Wi-Fi intelligente - Des millions de couleurs et de blancs
Lampadina LED Wi-Fi intelligente - Milioni di colori e sfumature di bianco
WLAN-LED Intelligente Glühlampe - Millionen von Farb- und Weißtönen
Bombilla inteligente LED con wifi - Millones de colores y blancos

ilumi

UNLOCK THE POWER OF LUXURY LIGHTING

Let your lighting be so much more than just light. Let it enhance your life. Improve your sleep, complement your mood, ramp up your music and connect your whole home.

A World of Color and Whites
Perfect atmosphere. From the warmest & coolest whites to any color under the rainbow.

Detect Your Presence
AUTO
Sensing your phone, your lights can turn on & off without hitting a switch. It's alive! Sort of.

Wellness Lighting
Tune your body's natural rhythm by replicating the sun's daily color cycle. Namaste.

Light Your Routine
Schedule a sunrise. Dine in candlelight. Shake your phone for a nightlight. Convenient? Yup.

Vacation Security
Hey, you're home! Or are you? Have your lights turn on & off randomly while you're away.

Music's New Best Friend
Sync your music and watch your Smartbulbs move to the beat of your fancy dancing feet.

The Internet of Things: a Surveillance State in Disguise

BY JOHN C. DVORAK MAY 27, 2015 26 COMMENTS

The Internet of Things is just bringing us closer to a 24/7 surveillance state.

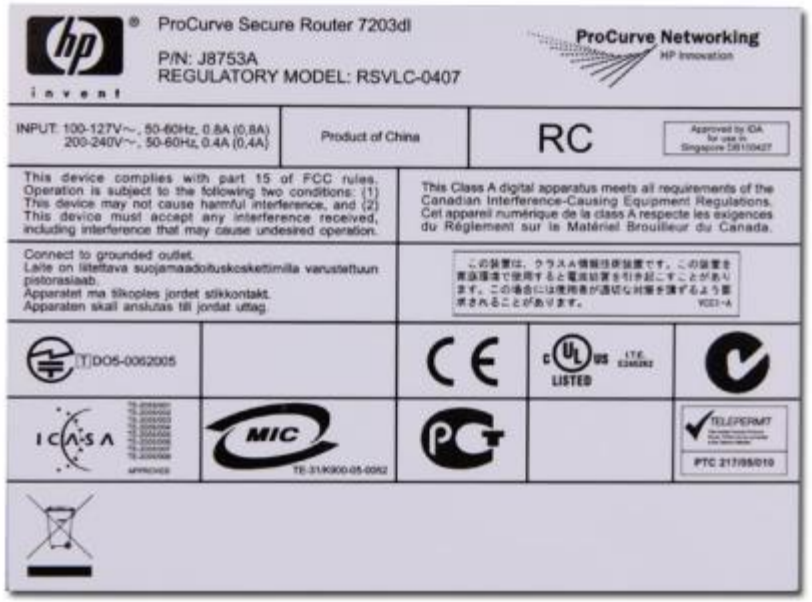
Internet of Things

If it’s connected to the internet it can be hacked.

Everything is being connected to the internet.

Therefore everything can be hacked.

Standards



https://www.csagroup.org/documents/resources-insights/gcmp-special-tech/CSA_Group_Protecting_Connected_Devices_Against_Cyber_Attack_Whitepaper.pdf

Rules for IoT devices

1) Be able to turn it off

2) Be able to disconnect it

3) Be able to update/patch it

Internet of Things (IoT)

- IoT devices were popularized by thermostats, fridges, and lightbulbs
- didn’t stop there – it’s so cheap to add connectivity they put it in and decide whether to use it later
  - eg. cars, locks, crockpots, baby monitors, fitbits
- most IoT devices can surveil you
  - detect presence, monitor communications
- those that can’t can be used against others

University of Victoria

Internet of Things (IoT)

- IoT are not designed with security and privacy in mind
- sold by companies that don’t understand privacy & security
- may use protocols that are not secure
- may use no password, passwords with low complexity, or hardcoded passwords
- may have default, generic, or undocumented accounts

Top IoT Vulnerabilities

- weak, guessable/predictable, or hardcoded passwords
- insecure network services
- insecure ecosystem interfaces (eg. web, api)
- lack of secure update mechanism
- insecure or outdated components
- insufficient privacy protection
- insecure data transfer and storage
- lack of device management
- insecure default settings
- lack of physical hardening

- inability to turn on/off
- inability to update/patch
- insufficient privacy
- integration with cloud

University of Victoria

Internet of Things (IoT)

- IoT devices are often are low cost, low margin
  - purpose built with few extras
  - revenue trumps security
  - usability and first to market
- may be so cheap they are designed to be disposable
  - throw them away, may keep working
  - imagine if so ubiquitous our oceans are filled with them as are the skies and the sewers
  - could be so small you excrete them

Internet of Things (IoT)

- sold online by companies that may not have a reputation or may not have a good reputation
- may have additional inputs, outputs that were not necessary
- vendors want to capture as much data as possible

Internet of Things (IoT)

- Internet of Things (IoT) devices have no relevant standards
- IoT devices have no privacy and security requirements
- no way for consumers to discern
- would people be willing to pay $5 extra for one with a badge/certification that says it respects privacy/security?
  - what percentage of the purchase price are people willing to pay?

Internet of Things (IoT)

How the IoT Cybersecurity Improvement Act Impacts You

As the world trends toward more internet-connected devices, security is playing catch-up. Standards need to exist or we're all at risk. The IoT Cybersecurity Improvement Act may be a step in the right direction.

Verifications

Any vendor selling an internet-connected device would have to affirm the following about the device:

- Does not contain any known security vulnerabilities
- Uses industry-standard technology for security and communication
- Can be securely accessed and updated by the vendor
- Doesn't have any fixed or hard-coded credentials

Mandatory Behaviors

After the device is provided to the government, the vendor would be required to do the following:

- Notify the government if they later learn of a vulnerability
- Update devices to ensure their security
- Repair or replace devices, should there come a security need
- Provide information on continuing security support, including a support timeline and notification when support ceases

California just became the first state with an Internet of Things cybersecurity law

By Adi Robertson | @thedextriarchy | Sep 28, 2018, 6:07pm EDT

SHARE

California Governor Jerry Brown has signed a cybersecurity law covering "smart" devices, making California the first state with such a law. The bill, SB-327, was introduced last year

New IoT Security Bill: Third Time's the Charm?

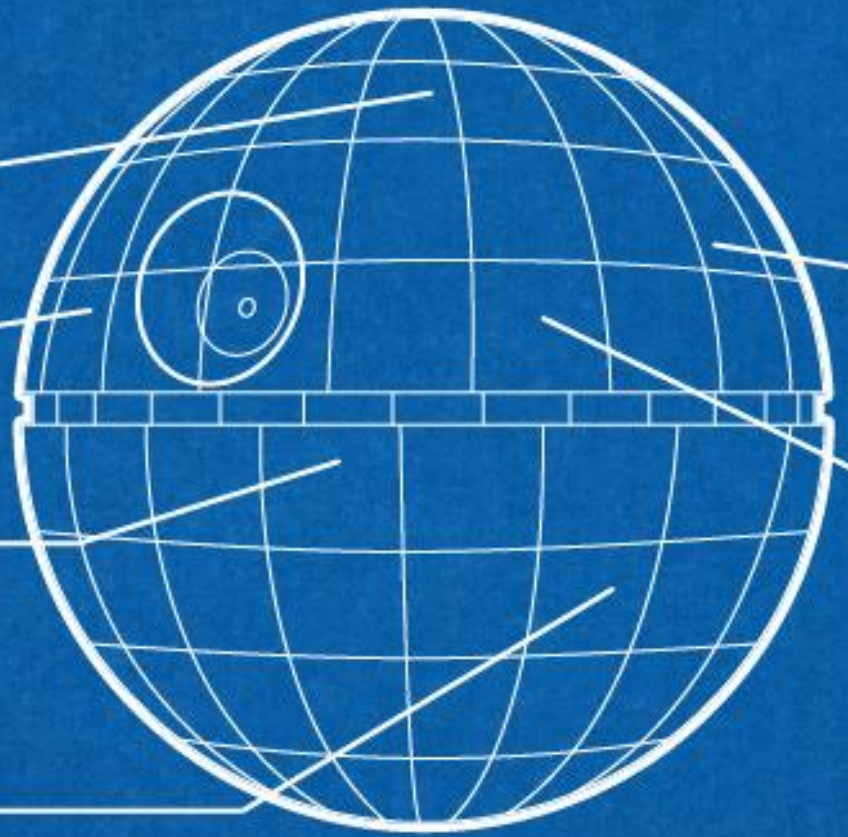
The latest bill to set security standards for connected devices sold to the US government has fewer requirements, instead leaving recommendations to the National Institute of Standards and Technology.

For the third time in as many years, lawmakers have introduced a bill that would require Internet of Things (IoT) products sold by federal contractors and vendors to abide by government guidelines to ensure a baseline of cybersecurity.

Internet of Things (IoT)

- is it reasonable to expect these organizations to respect security and privacy?
- why are people buying and implementing these devices with little to no care for security
- are they assuming they are secure?
- do they think the likelihood is low?
- do they think the impact is low?

THE DEATH STAR'S DEMISE:
CAN YOU TRUST YOUR IoT VENDORS?



Trash Compactor

Hair Bun Dryer

Bantha Milk Chiller

Light Saber Charger

Dejarik Gaming Table

Droid Polisher

tripwire.com/blog

IoSWT

(Internet of Star Wars Things)

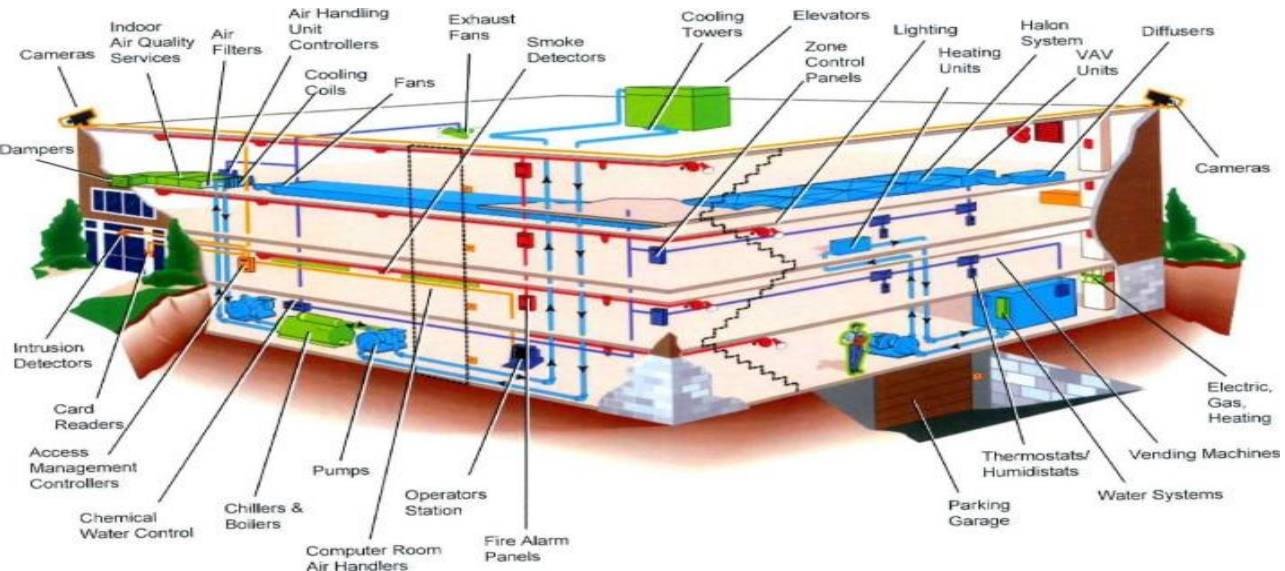
Solutions

- have to know what is there first
  - surprising how many devices
- if you don’t need it connected then don’t
  - examine what features it supports (wired, WiFi, infrared, Bluetooth)
  - if WiFi is it a client, access point, how many of each?
- use reputable vendors – watch out for the apps
- do your research – what features does the device have?

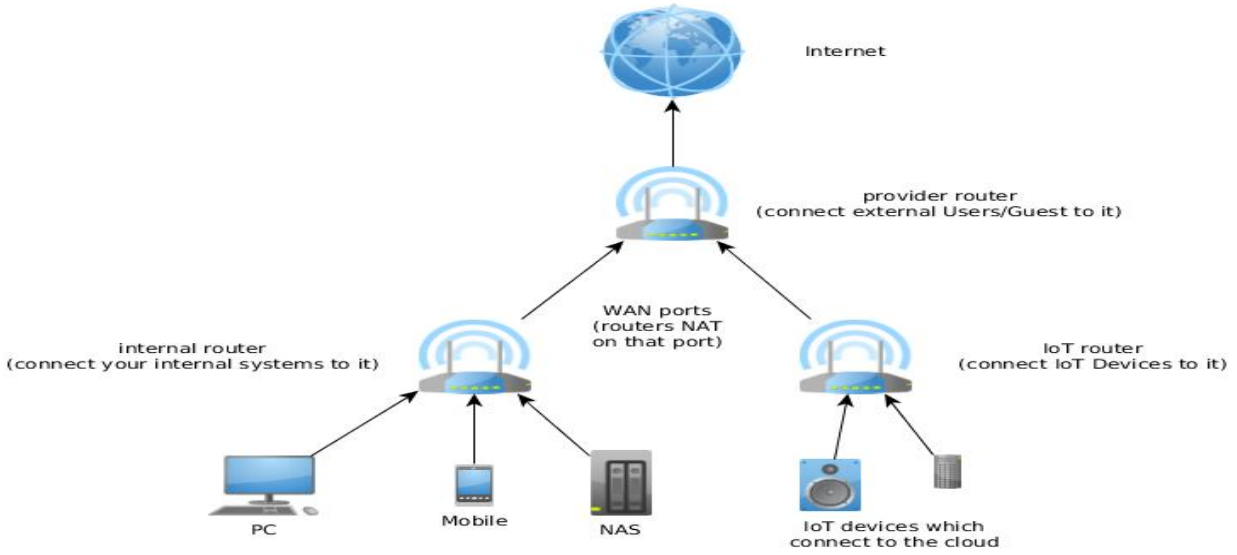
Solutions

- update products regularly, patch them
- protect them with firewalls
- put them on a different VLAN or SSID
- monitor the activity (logs or traffic)

business



home

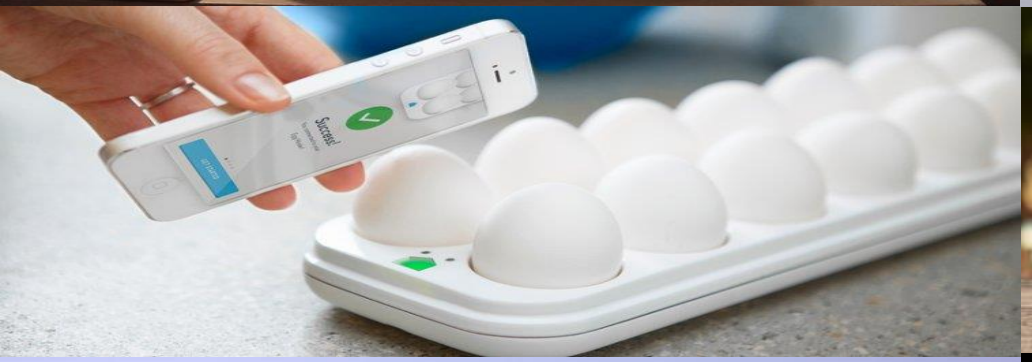


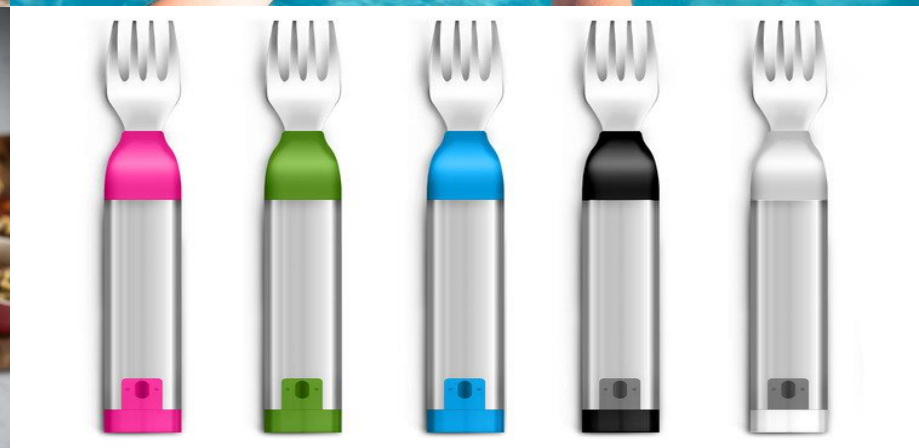
Internet of Things

University of Victoria

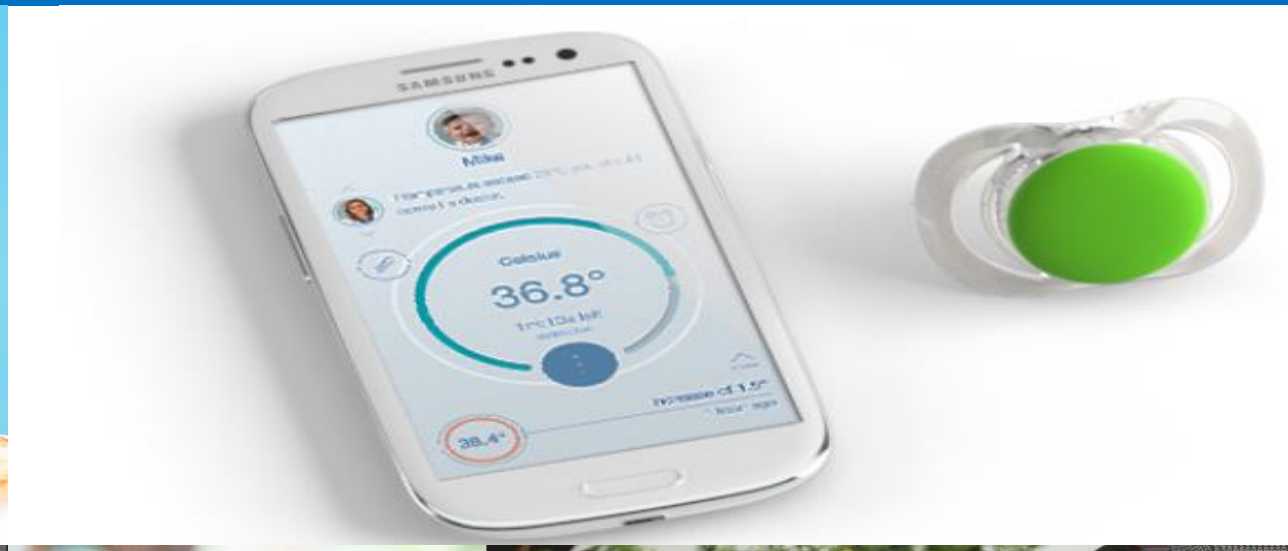
Internet of Things

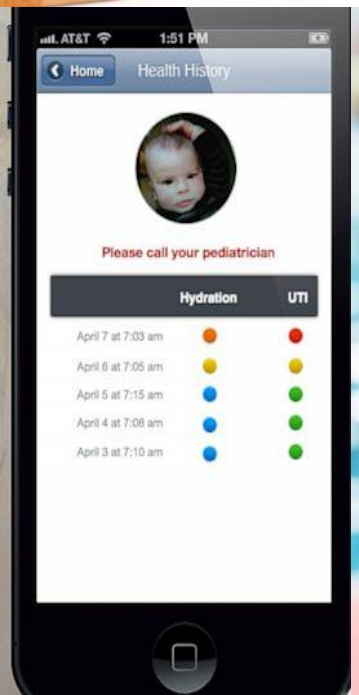
Internet of Things



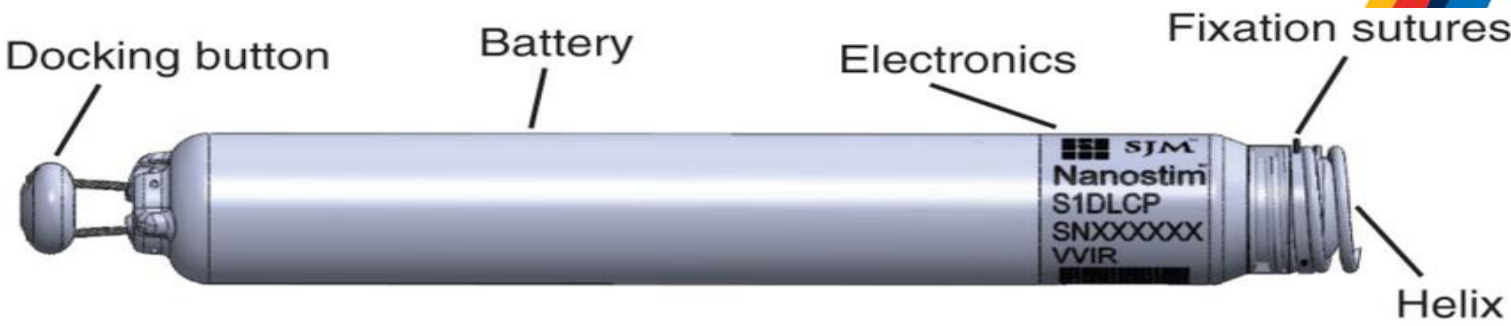


Internet of Things

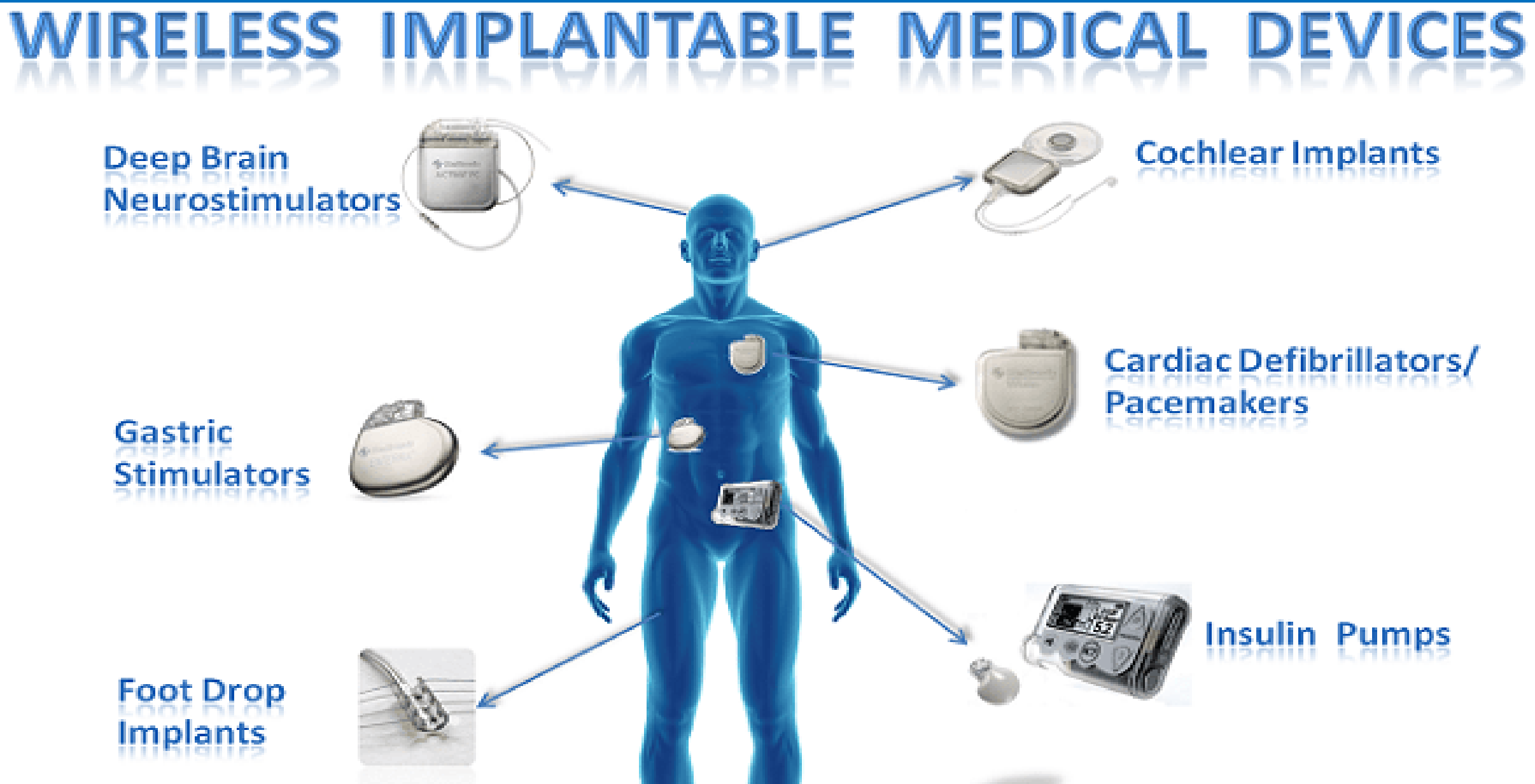




Internet of Things



Internet of Things



This is the newest version (v1.3) with camera connector.
For the Wireless version (Zero W) please click here.

Please carefully check the description and the related products requirements and recommendations below.

$6.99

Add to basket

Examples

Bluetooth Smart Watch DZ09 Smartwatch GSM SIM Card With Camera For Android IOS Black

★★★½☆ 6 reviews Kanstar

$13.15

Free shipping

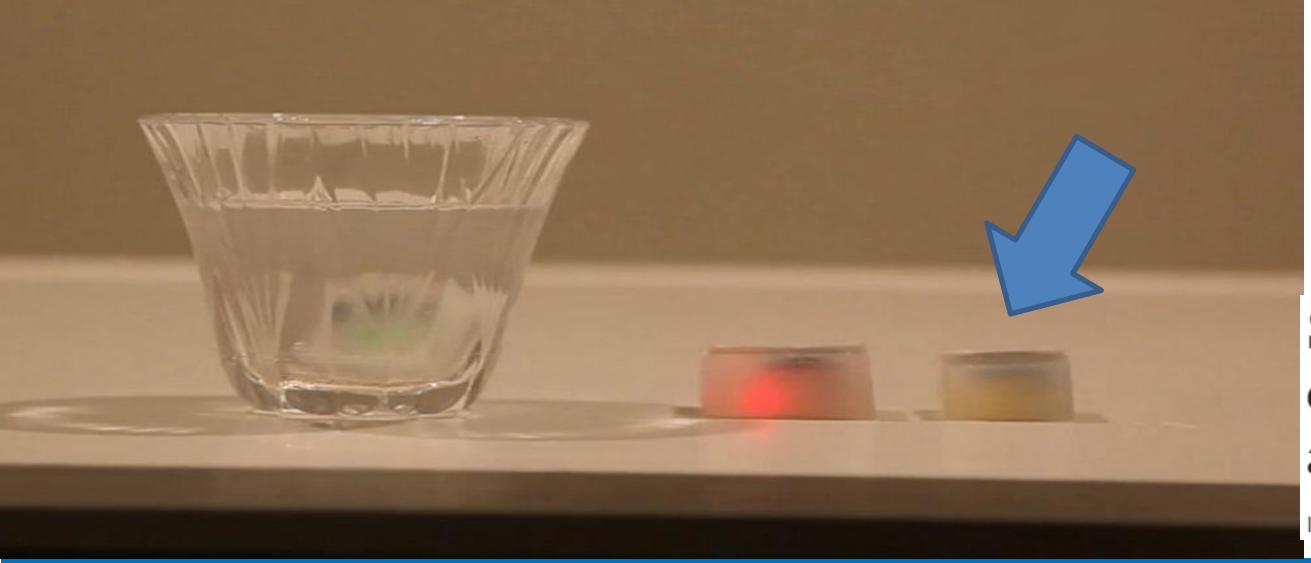
Arrives by Wednesday, Apr 3

Or get it by Mon, Mar 25 with faster shipping Options

Qty: 1

Add to Cart

Pickup not available



The cubes glow and beat to the ambient music, but more importantly, they know how fast and how much you are drinking, and they change color from green to orange to finally red as you reach your safe limit. If things go too far, the ice cubes can connect to your smartphone and send a text message for a friend come get you. Of course, you have to remember not to swallow them.

Smart ice cube knows when your drink is running low and automatically orders you another

It could also be used to detect when drinks have been tampered with

Examples

Spy cams found in South Korean motel rooms

Early Start

About 1,600 people have been secretly filmed in motel rooms in South Korea, with the footage live-streamed online for paying customers to watch, police said. Source: CNN

Hydro and Smart Meters

Opposition grows, but BC Hydro installing smart meters

By Andrew Mitchell

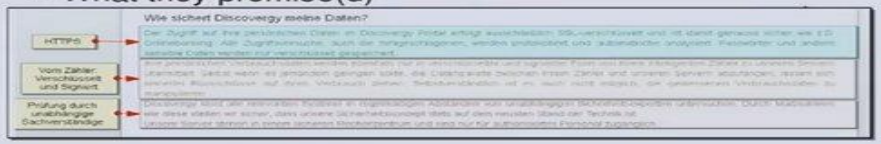
CLICK TO ENLARGE

According to BC Hydro, the meters are only active for a total of a minute per day. Over the 20-year life of the meters they claim that the meters will emit the same amount of radiation as a 30-minute cell phone call. As well, the signals are lower than the lowest safety thresholds in the world — 2.0 microwatts per square centimetre versus 4.5 in Swiss schools and hospitals.

Smart meter hacking can disclose which TV shows and movies you watch

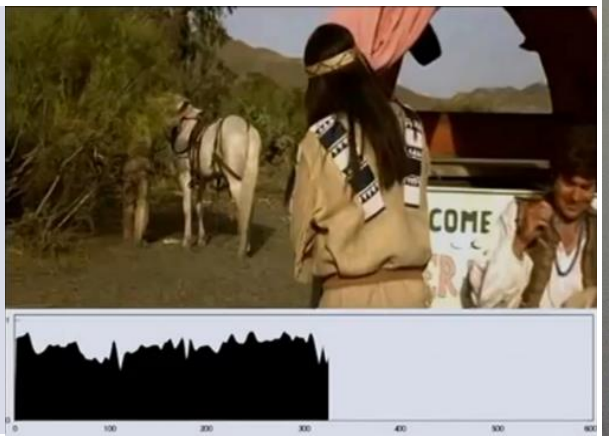
Hacking Discovergy

- What they promise(d)



- Web-based GUI: HTTPS
- Communication smart meter to server
  - Encrypted (provides confidentiality)
  - Signed (provides authenticity and integrity
- Inspected by independent experts

22



Videos

How hackers could use smart home devices to spy on you (Marketplace)
https://www.youtube.com/watch?v=-P0rSnt2HSU

IoT in Healthcare
https://vimeo.com/173521227

“IoT is the backbone of SmartCities”

University of Victoria

Threats to Critical Infrastructure

Mobile Device Security

University of Victoria

Mobile Devices

- iPhone, Android, Windows, BlackBerry
- which is most secure? why?

Mobile Devices

- enforcing controls
  - BES (BlackBerry Enterprise Server)
  - ActiveSync
  - Mobile Device Management (MDM)
  - Enterprise Mobility Management

Mobile Devices

- weak or no authentication
- what are you protecting?
- jailbreaking, rooting devices
- side-loading apps
- whitelisting, blacklisting apps
- Allowlisting
- etc

Mobile Devices

- containerization
  - where to authenticate?
- device ownership
  - personal device
  - employer device
- common models
  - BYOD: bring your own device
  - CYOD: choose your own device
  - HYOD: here’s your own device

University of Victoria

Review

- How do companies enforce security policies on mobile devices?
  - Mobile Device Management (MDM) or now Enterprise Mobility Management (EMM)
    - Examples: AirWatch, MaaS 360, MobileIron

- These tools provide organizations ability to enforce security settings like:
  - password complexity, history, aging, encryption, detection of jailbroken devices, remote wipe

University of Victoria

Assigned Reading

- read Chapters 16-18 for next time
- **quiz next week!**
- lab is optional (RegEx)


University
of Victoria