



NATIONAL CYBER SECURITY AWARENESS MONTH

October is scary not just because of Halloween

Dr. Ray Klump
Chair and Professor, Computer & Mathematical Sciences
Director, Master of Science in Information Security



National Cyber Security Awareness Month (NCSAM)

- Annual campaign to raise awareness about cyber security
- Educate public and private sector through events that increase awareness



Each week of NCASM has a theme.



October 3 – 7:

Everyday Steps Towards Online Safety
with **Stop. Think. Connect.**



October 10 – 14:

Cyber from the Break Room to the
Board Room



October 17 – 21:

Recognizing and Combating Cybercrime



October 24 – 28:

Our Continuously Connected Lives:
What's Your 'App'-titude?



October 31

Building Resilience in Critical Infrastructure



Why do we need a month for cyber security awareness?



The problem is bigger now than ever.

Yahoo 'state' hackers stole data from 500 million users

23 September 2016 | Technology



Yahoo says "state-sponsored" hackers stole data on about 500 million users in what could be the largest publicly disclosed cyber-breach in history.

The breach included swathes of personal information, including names and emails, as well as "unencrypted security questions and answers".

The hack took place in 2014 but has only now been made public.

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy **Business** Tech Markets Opinion Arts Life Real Estate



Digital Ad Doubts
Rise Over New
Revelations



Yahoo Executives
Detected a Hack Tied
to Russia in 2014



Salesforce
Considers Takeover
of Twitter



WSJ. MAGAZINE
Snapchat
Releases First
Hardware ...



BUSINESS

Anthem: Hacked Database Included 78.8 Million People

Health insurer says data breach affected up to 70 million Anthem members



Most Popular Video

1. Video Release
Charlotte Pol
Shooting
2. Best Moment
Presidential I
History
3. Great Wall of
Repairs Provo
Outrage
4. Fix iOS 10's
Frustrating L
Screen
5. Police Release
Footage of De
Tulsa Shootin



Why do hackers do this?



Successful hacks raise a lot of money

- \$11 per birthdate-name-address
- \$20 per health insurance record
- \$30 per SSN
- \$300 per bank account number
- \$1,200 per full identity kit



Successful attacks cause tremendous loss to an organization.

- Average cost of breach: \$674K
- Average cost of a healthcare breach: \$1.3 million
- Median per-record cost of losing a record: \$13
- Average # of records lost: 3.2 million



Most popular causes of attacks

- employee errors
- privilege misuse
- physical theft / loss
- denial of service
- crimeware
- web app attacks
- POS intrusions
- cyber espionage
- payment card skimmers



All together ...

- 31 % of cyber loss caused by hackers
- 14% by malware
- 11% by human error



Who's the target?



Organizations of all shapes and sizes face cyber challenges

- In 2015, 60% of attacks were targeted toward small and medium-sized businesses (SMBs)
- 1 in 2 businesses surveyed in 2014 reported being victim of cyber attack
- 3 out of 4 spear-phishing attacks in August 2015 targeted small businesses with 250 employees or less.
- 60% of SMB cybercrime victims go out of business within 6 months of an attack.



To cope, you need to ...

- Recognize that there is a problem
- Break down the problem
- Acquire the expertise
 - *Currently more than 200,000 cyber jobs are unfilled*
- Acquire the resources to carry out your plan
 - *60% see buy-in as the number one obstacle*
 - *Need to make the case*
- Counteract inertia



Phishing is one of the biggest threats

- We click on duplicitous emails
- Anti-phishing software is getting more popular

Phishing Protection across the Entire Organization

With more than 90% of breaches attributed to successful phishing campaigns, it's easy for organizations to point to the everyday employee as the root cause – as the problem to be solved. We disagree. PhishMe believes employees – humans – should be empowered as part of the solution to help strengthen defenses and gather real-time attack intelligence to stop attacks in progress.

Learn More PhishMe's Human Phishing Defense Solutions.



Recognize

Phishing attacks like ransomware and business email compromise (BEC) target people – so when a phish gets through your technology, your employees need to be able to recognize the attempt.

[LEARN MORE](#)



Research

Not all intelligence sources are the same. PhishMe focuses on phishing-specific threats and provides human-vetted analysis of phishing and ransomware campaigns and the malware they contain. Easily integrated across multiple security solutions – you can confirm and respond to real threats in less time.

[LEARN MORE](#)



Report

It's not enough to delete a bad email. Employees are your last line of defense and your best source of knowledge. Engaging them to report attacks in progress can significantly decrease time to respond to developing threats and attacks in progress.

[LEARN MORE](#)



Respond

Security Operations and Incident Response teams have the daunting and thankless job of sorting through alarms and reports to determine what's real and what isn't. PhishMe helps to significantly speed the collection, analysis and response to real phishing threats.

[LEARN MORE](#)

And you need to encrypt ... everywhere

- Data that needs to remain secret must be encrypted
- Encrypt data at rest and in transit
- Encrypt on all devices where the data resides



And you need to require more than just a password

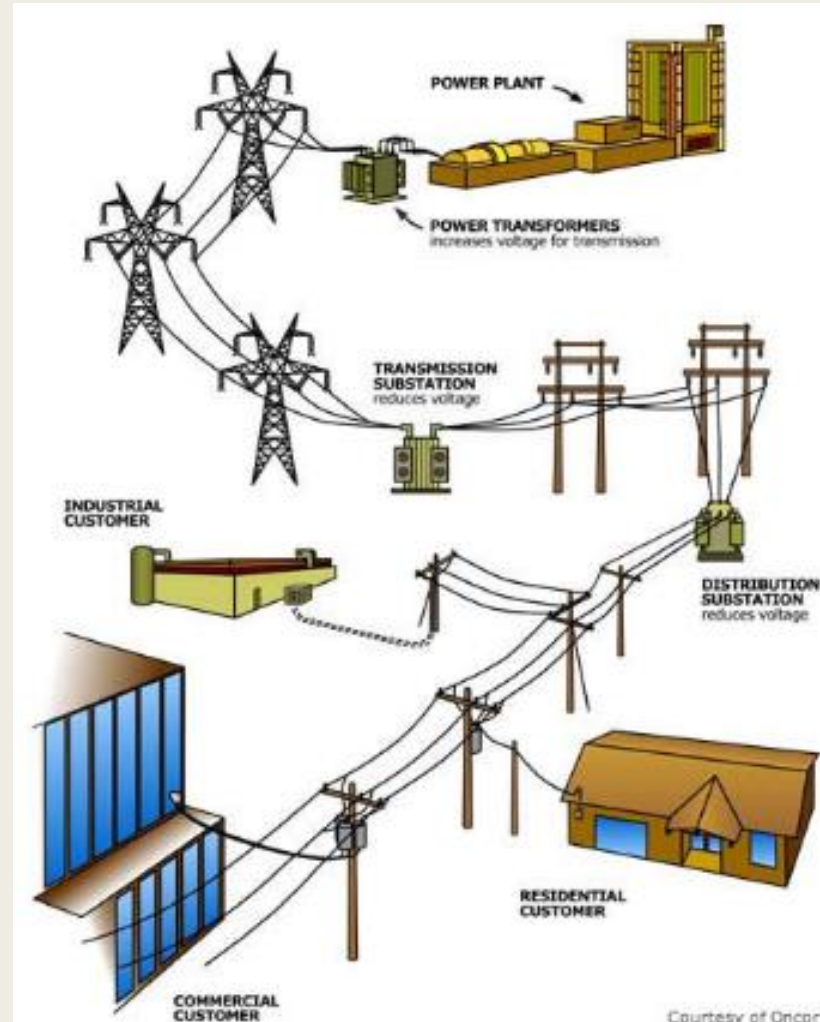
- Multifactor authentication is very important today



As if this weren't enough, critical infrastructures are increasingly at risk.

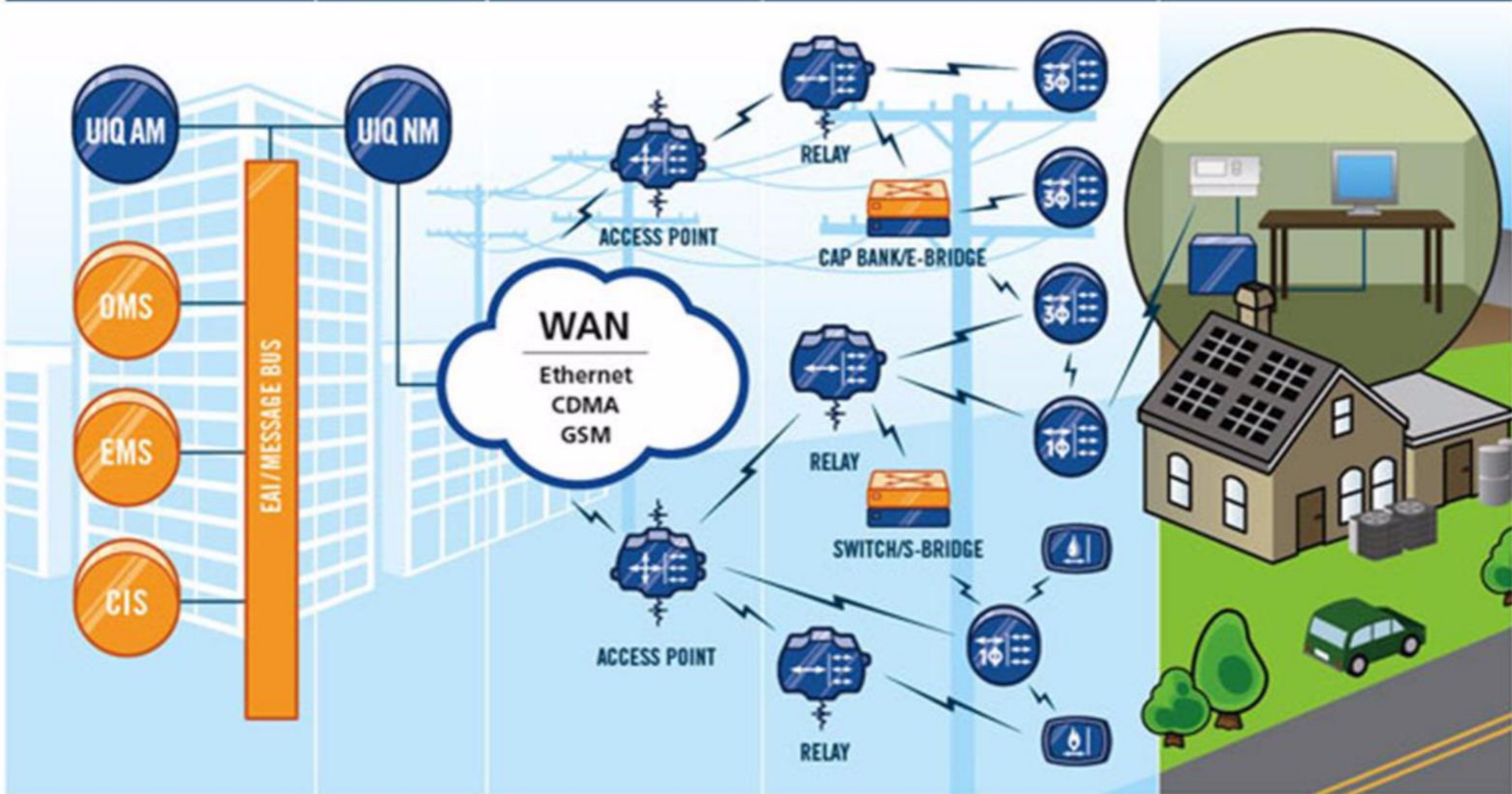


Today's Power System

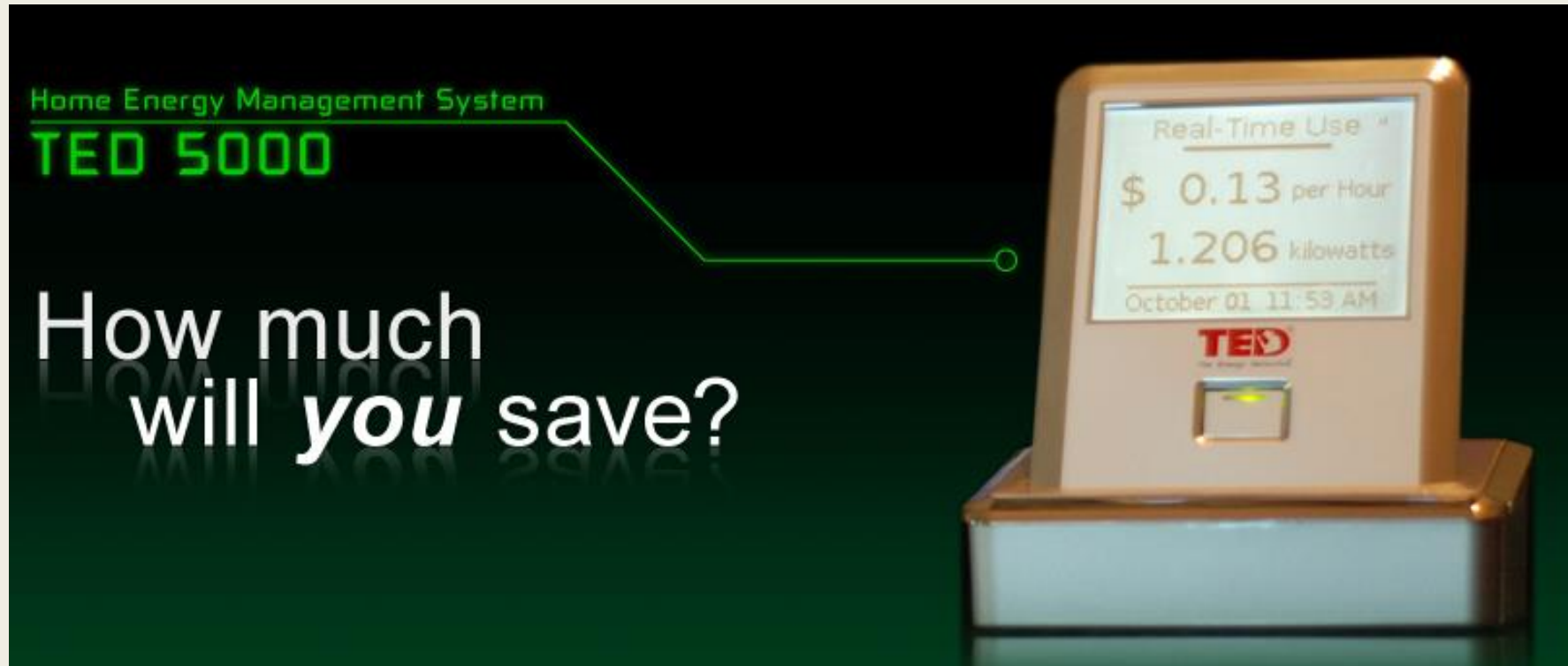




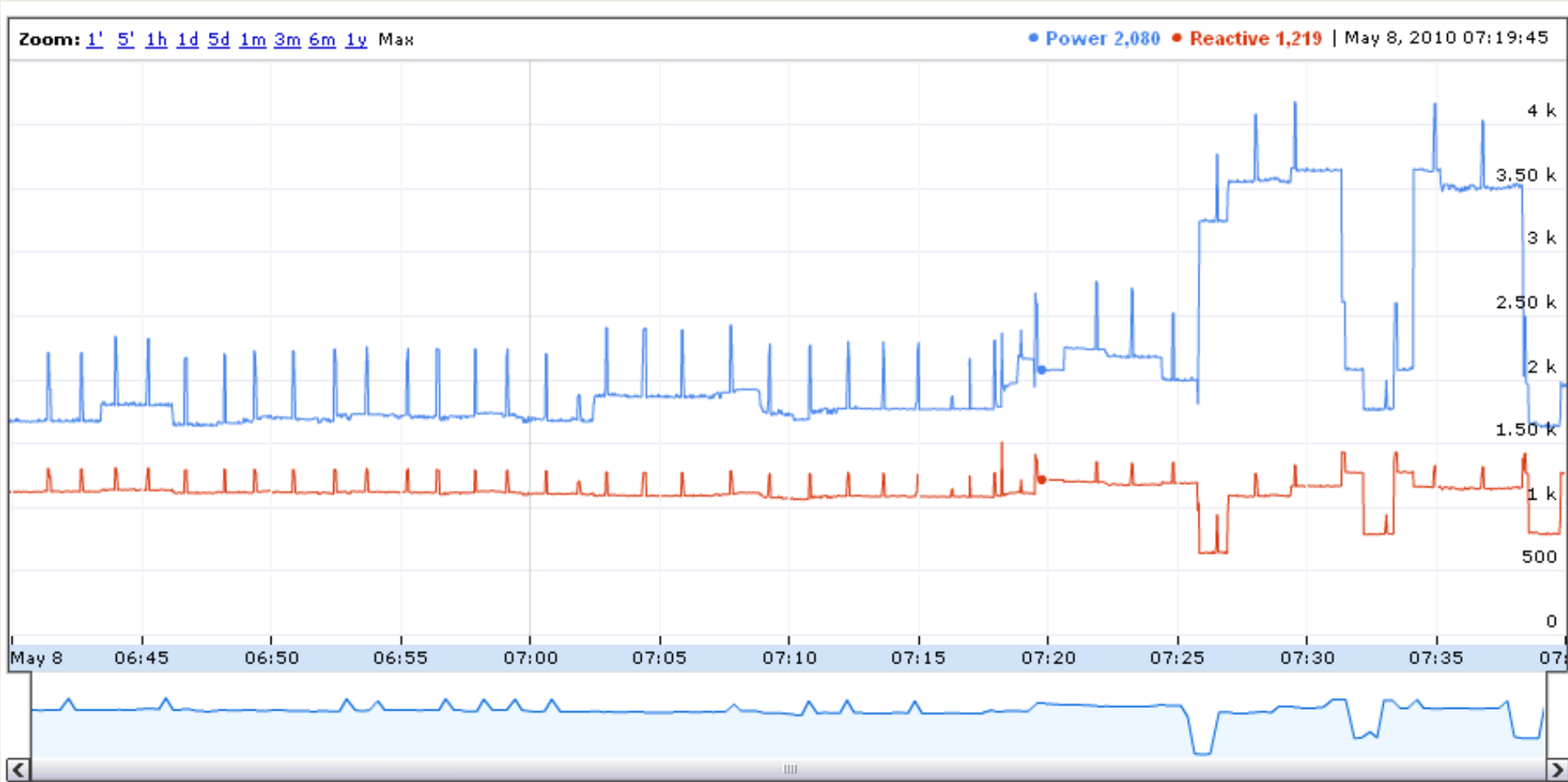
BACK OFFICE	NETWORK OPERATING CENTER	SMART GRID NETWORK	SMART GRID DEVICES	SMART HOME
-------------	--------------------------	--------------------	--------------------	------------



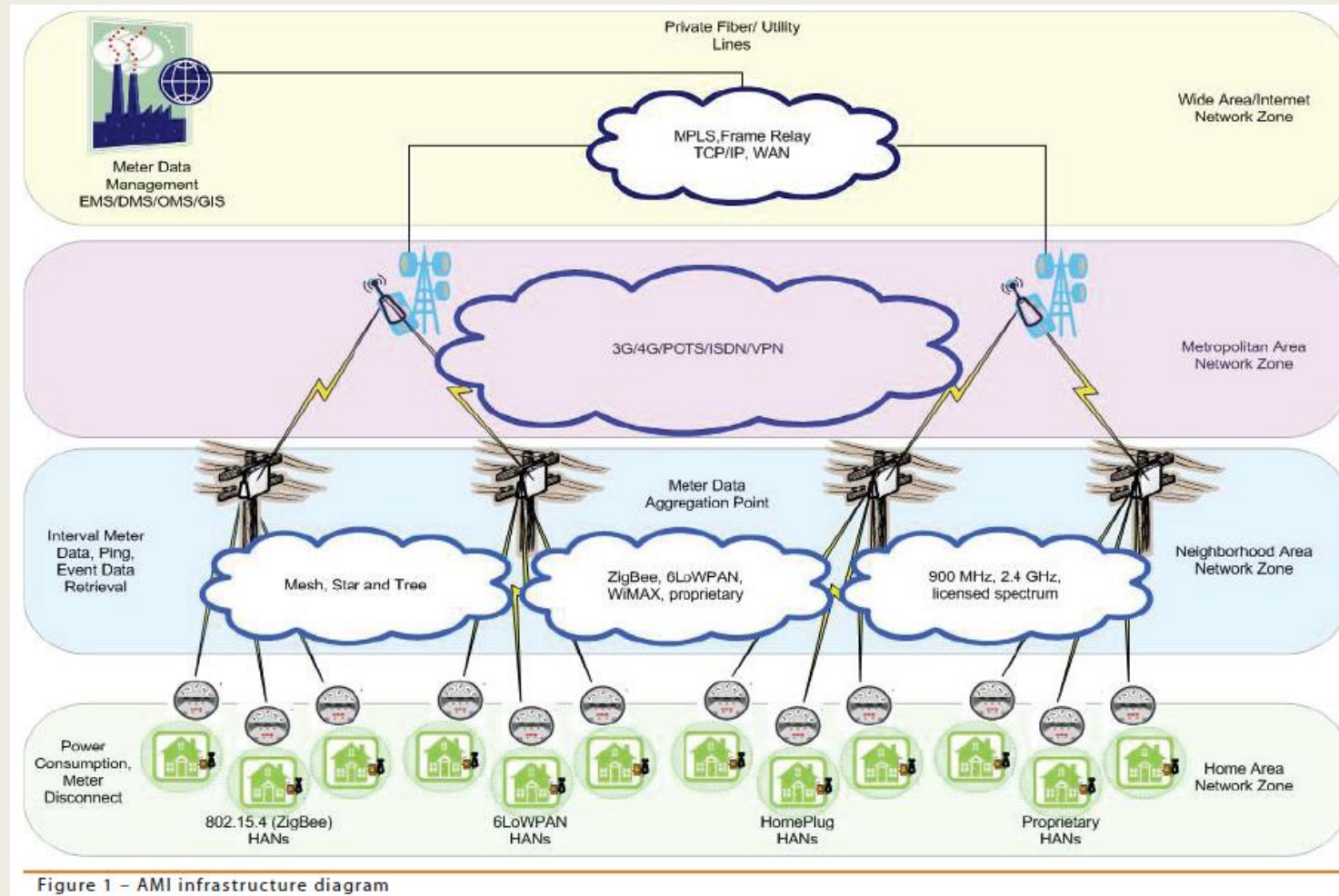
Smart Grid in the Home



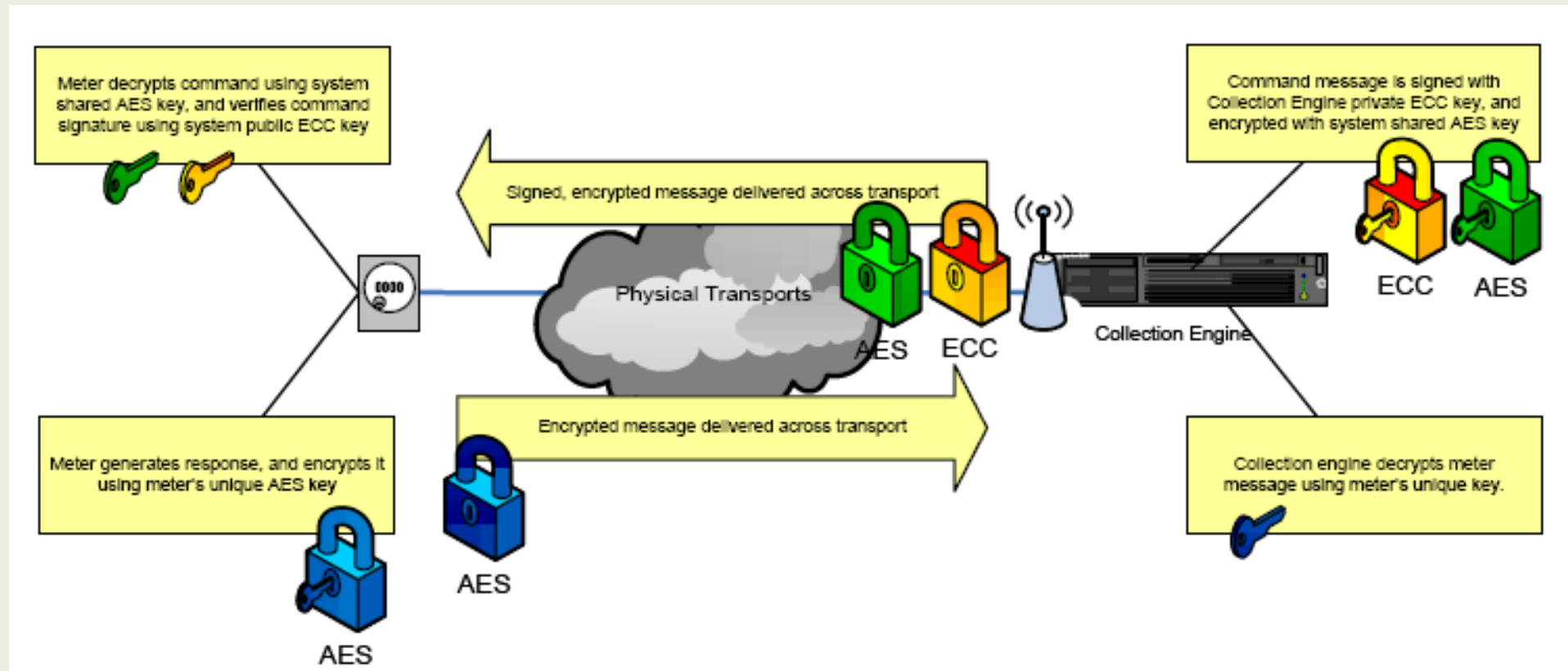
Data in Your Home



Data Everywhere



Where Security Fits In



Challenges

Confidentiality

Integrity

Authentication

Availability

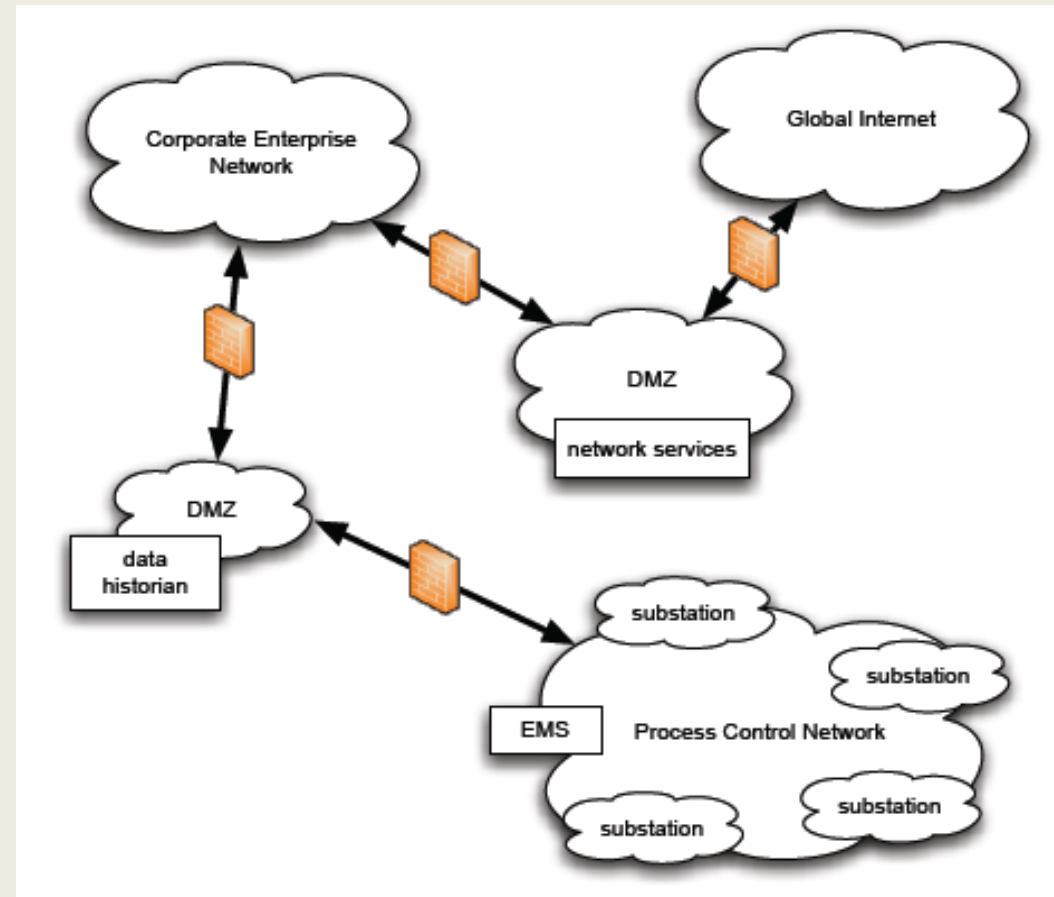
Collection

Storage

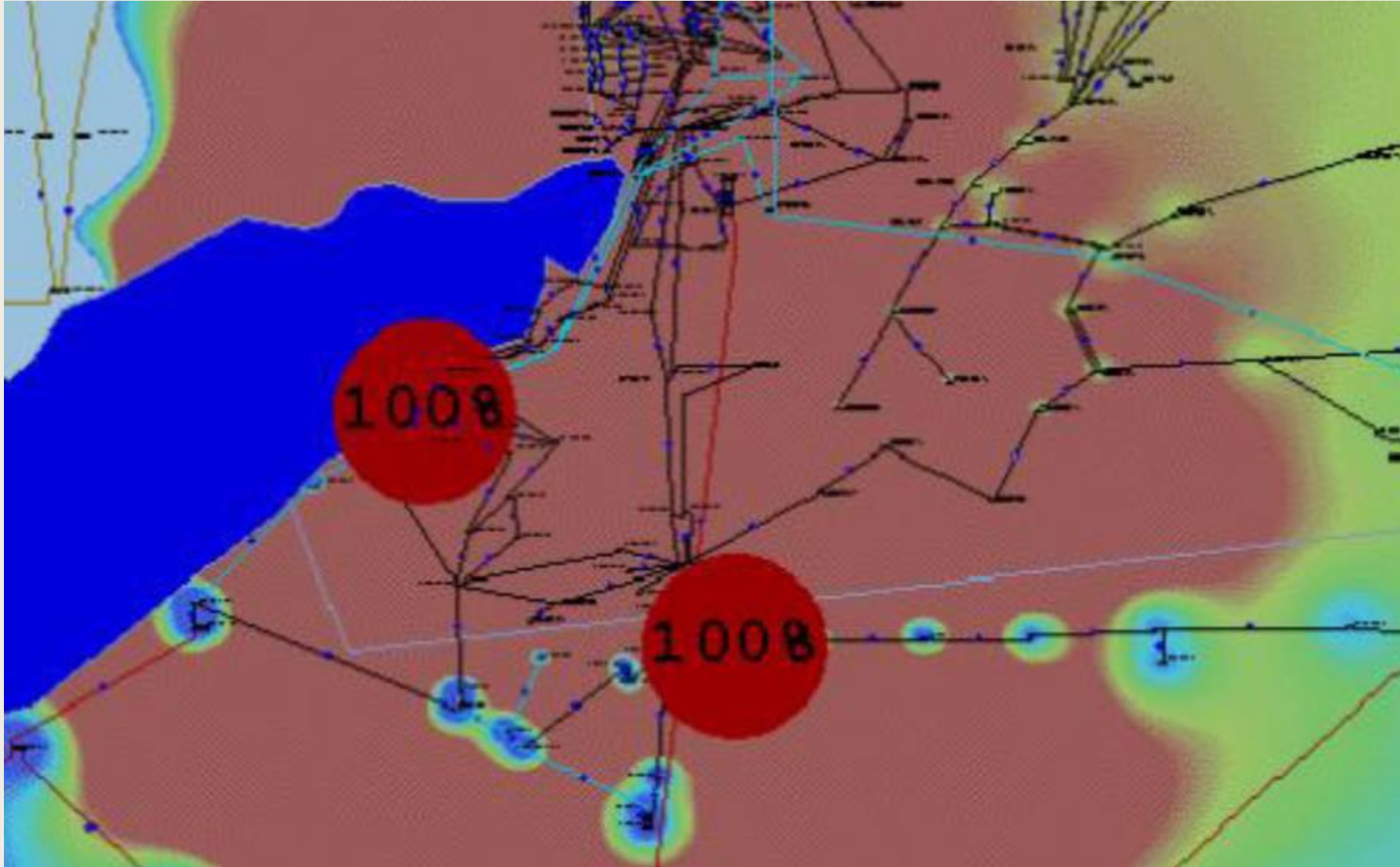
Interpretation



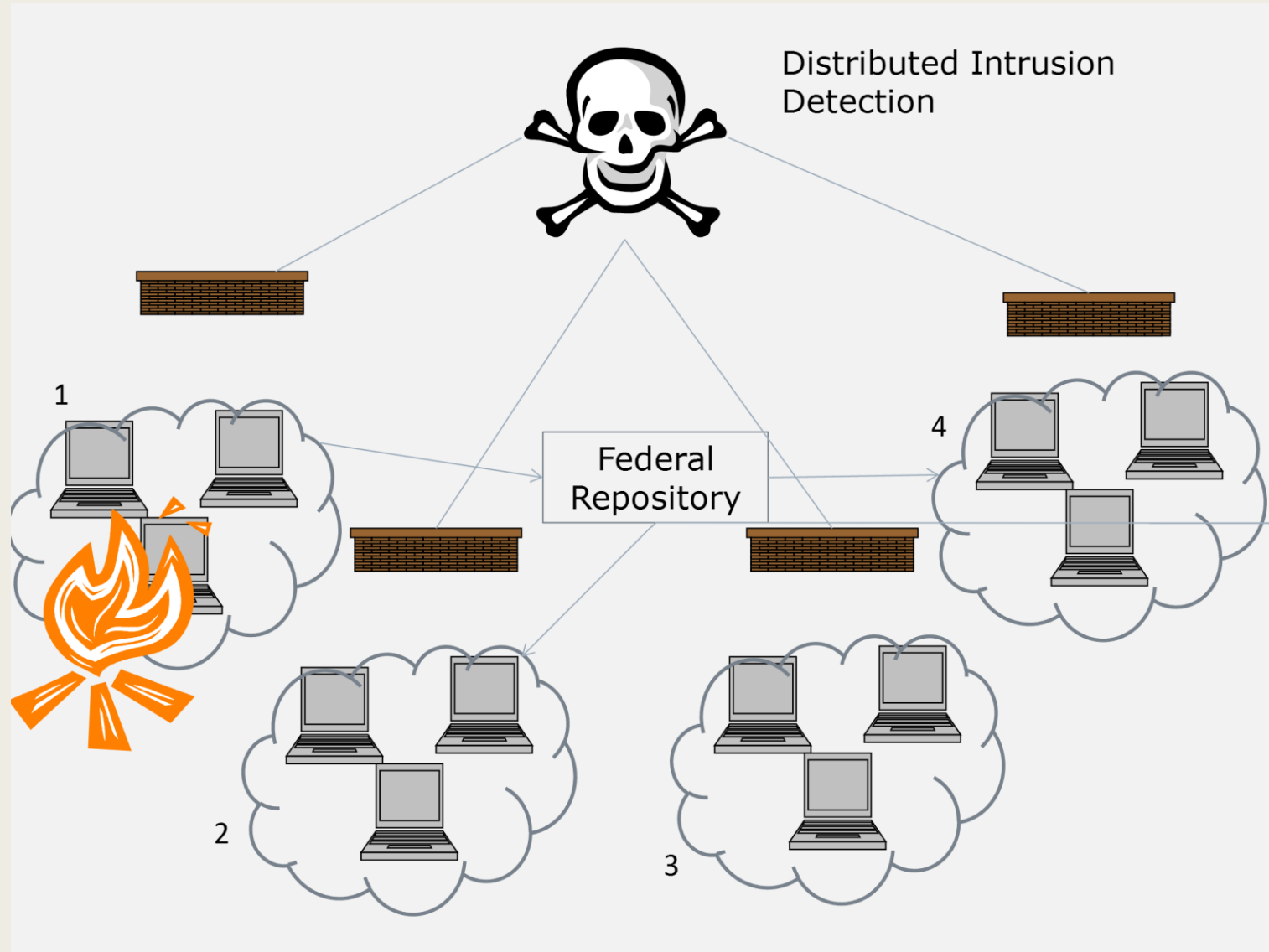
Real Consequences



Overload results



The need to work together



So, cyber *in*security wreaks havoc on both small and large scales.



But, cyber security starts with us.



Stop. Think. Connect.

- National public awareness campaign aimed at
 - *Increasing our understanding of cyber threats*
 - *Empowering the American public to be safer and more secure online*



Stop. Think. Connect.

- Cyber security is a shared responsibility.
- Advocates simple steps makes the Internet safer for everyone.
- Provides lots of resources for a variety of Internet users.
- <https://www.dhs.gov/stopthinkconnect-toolkit>



For example: Smartphone security checklist

- <https://www.fcc.gov/smartphone-security>



Another example: Social Media

- https://www.dhs.gov/sites/default/files/publications/Social%20Media%20Guide_3.pdf
- Telling stats:
 - *64% of teens make their tweets public*
 - *19% of teens have posted something they regret*
 - *Only 18% of adults are comfortable with what their friends post about them online*



Beware of what you post online

- Don't post things that could be used to steal your identity (e.g. your birthday)
- Don't post anything you wouldn't want a future employer to see
- Don't post your location
- Remember that there is no DELETE button on the Internet



Beware of public wifi

- Be careful when you connect
- Avoid conducting sensitive activities
- Use your mobile network connection instead
 - *Or use a VPN*



Be cautious even when you're not using
a “computer”

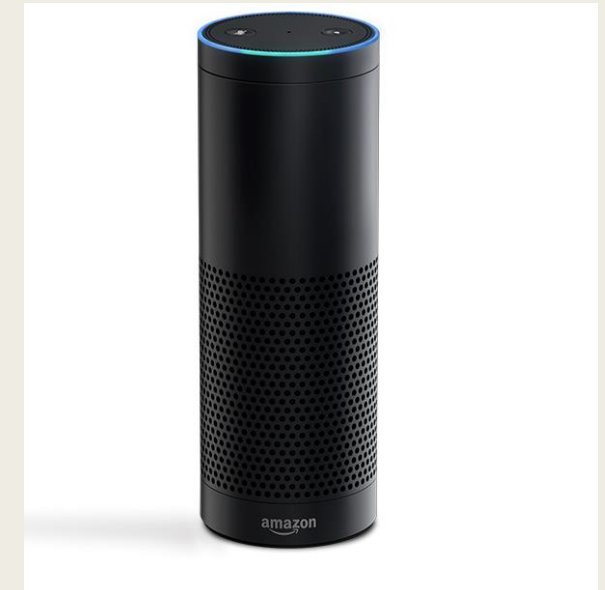


Internet of things

- Non-traditional computing devices provide computing services to us
 - *Often collaborating with other such devices*
- Communicate over wifi
- These share information about us
- Systems you don't usually think of as computers are
 - *Your car*
 - *Your appliances*
- By 2019: 20 billion to 40 billion connected devices
- They must be kept constantly patched



Examples



Who are interested in these devices?

- Criminals
- Law enforcement
- Device manufacturers



Free and open-source can capture the data from these devices

- Wireshark
- FATXplorer
- FTK Imager
- The Sleuth Kit
- Rooting software
- Coolgear USB 3.0 Multifunctional Commutator



Nest

- Reveals a regular traffic pattern when the house is unoccupied

NestWiresharkAwaySetting.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 2 Expression... Clear Apply Save

802.11 Channel: Channel Offset: FCS Filter: All Frames Wireshark Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Length	Info
111	19.635301000	192.168.1.118	107.22.11.173	TCP	74	38537→9543 [SYN] Seq=0 win=4380 Len=0 MSS=1460 SACK
114	19.689535000	107.22.11.173	192.168.1.118	TCP	74	9543→38537 [SYN, ACK] Seq=0 Ack=1 win=17898 Len=0 M
115	19.791741000	192.168.1.118	107.22.11.173	TCP	66	38537→9543 [ACK] Seq=1 Ack=1 win=4380 Len=0 TSval=2
116	19.800126000	192.168.1.118	107.22.11.173	TCP	583	38537→9543 [PSH, ACK] Seq=1 Ack=1 win=4380 Len=517
118	19.853651000	107.22.11.173	192.168.1.118	TCP	66	9543→38537 [ACK] Seq=1 Ack=518 win=19072 Len=0 TSva
119	19.854162000	107.22.11.173	192.168.1.118	TCP	259	9543→38537 [PSH, ACK] Seq=1 Ack=518 win=19072 Len=1
120	19.894120000	192.168.1.118	107.22.11.173	TCP	66	38537→9543 [ACK] Seq=518 Ack=194 win=5452 Len=0 TSv
121	19.899549000	192.168.1.118	107.22.11.173	TCP	173	38537→9543 [PSH, ACK] Seq=518 Ack=194 win=5452 Len=
122	19.990417000	107.22.11.173	192.168.1.118	TCP	66	9543→38537 [ACK] Seq=194 Ack=625 win=19072 Len=0 TS
123	20.098751000	192.168.1.118	107.22.11.173	TCP	732	38537→9543 [PSH, ACK] Seq=625 Ack=194 win=5452 Len=
124	20.154250000	107.22.11.173	192.168.1.118	TCP	66	9543→38537 [ACK] Seq=194 Ack=1291 win=20352 Len=0 T
125	20.166931000	107.22.11.173	192.168.1.118	TCP	508	9543→38537 [PSH, ACK] Seq=194 Ack=1291 win=20352 Le
126	20.206527000	192.168.1.118	107.22.11.173	TCP	151	38537→9543 [PSH, ACK] Seq=1291 Ack=636 win=6524 Len=
127	20.206950000	192.168.1.118	107.22.11.173	TCP	66	38537→9543 [FIN, ACK] Seq=1376 Ack=636 Win=6524 Len=
128	20.263657000	107.22.11.173	192.168.1.118	TCP	151	9543→38537 [PSH, ACK] Seq=636 Ack=1376 win=20352 Le
130	20.267946000	107.22.11.173	192.168.1.118	TCP	66	9543→38537 [FIN, ACK] Seq=721 Ack=1377 win=20352 Le
131	20.303604000	192.168.1.118	107.22.11.173	TCP	60	38537→9543 [RST] Seq=1376 win=0 Len=0
132	20.303936000	192.168.1.118	107.22.11.173	TCP	60	38537→9543 [RST] Seq=1377 win=0 Len=0

< >

Frame 116: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0

Ethernet II, Src: BelkinIn_a4:24:f3 (b4:75:0e:a4:24:f3), Dst: Cisco-Li_07:4c:8a (58:6d:8f:07:4c:8a)

Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 107.22.11.173 (107.22.11.173)

Transmission Control Protocol, Src Port: 38537 (38537), Dst Port: 9543 (9543), Seq: 1, Ack: 1, Len: 517

Data (517 bytes)

```
0000  58 6d 8f 07 4c 8a b4 75 0e a4 24 f3 08 00 45 00  Xm...u...$....E.
0010  02 39 c7 05 40 00 40 06 38 d8 c0 a8 01 76 6b 16  .9...@. 8....yk.
0020  0b ad 96 89 25 47 8d ec 9c f3 2a a4 00 9d 80 18  ....%G...".
0030  08 8e 67 61 00 00 01 01 08 0a 00 04 5c 07 35 0a  .ga....\..5.
0040  47 31 16 03 01 02 00 01 00 01 fc 03 03 05 aa e7  G1.....
0050  7b dd 8b cd b2 4b ff 2c 06 c6 57 23 6e 73 59 d2  {...K...wfnY.
0060  9b f5 67 54 4e 70 cc d8 56 d9 63 a5 78 20 56 43  .gTnp...V.C.X VC
0070  3f a5 79 33 7e 8c 28 c0 19 74 a1 85 6d 71 f5 98  ?y3~(. .t..mq...
0080  68 1b 7a 6f 13 76 5d 4f d7 b0 be 53 05 af 00 94  h.20.vjo...S...
0090  c0 3d c0 2c c0 28 c0 24 c0 14 c0 0a 00 a3 00 9f  .0...($.....
```

File: "C:\Users\Doug\Desktop\DiskImages\N... Packets: Profile: Default



Amazon Echo

- Voice requests
- When voice requests were issued



Xbox – Data saved under gamer id

```
Hex Strings Metadata Results Text Media
Matches on page: 1 of 1 Match Page: 1 of 1 Page
m9k@|
l~|Q~
&JBXML
PlayerProfile
uint64value690359770530896007nameProfileID
stringvaluexCountryCloudxnameGamerID
uint64value1879831248namesavegame_user_id
uint32value1nameauto_save
uint32value1namedifficulty
uint32value0nameassist_p2_braking
uint32value0nameassist_p2_ABS
uint32value0nameassist_p2_traction_control
uint32value0namep2_transmission_type
uint32value0nameassist_p2_dynamic_racing_line
uint32value0nameassist_p2_pit_limiter
uint32value0nameassist_p2_pit_box_control
uint32value4nameassist_race_braking
uint32value0nameassist_race_ABS
uint32value0nameassist_race_traction_control
uint32value0nameassist_race_dynamic_racing_line
```



Xbox usage data

- Youtube app
- Netflix app
- Xbox Live search app
- Accessed email
- Purchased and downloaded games



Emails on the Xbox

Feature Filter ☐ Match case
sattui

Feature File domain.txt

46964975	www.vsattui.com
46965359	www.vsattui.com
46965743	www.vsattui.com
46966127	www.vsattui.com
46966511	www.vsattui.com
46966895	www.vsattui.com
46967279	communicate.vsattui.com
46967663	www.vsattui.com

Referenced Feature File None
Referenced Feature None

Image File Xbox2.E01
Feature File domain.txt
Forensic Path 46966511
Feature www.vsattui.com

Image

46960640	Wine-of-the-Month-Club-banner[1].jpg....d.....W.....Gn.[Gn.[
46960704	WOM-monthly-newsletter[1].jpg.....Y....."Gn.[Gn.[
46960768	Gift-Card-banner[1].jpg.....W.....s.....Gn.[Gn.[
46960832	Gift-Card-image[1].jpg.....V.....t.....Gn.\Gn.\
46960896	dt[1].gif.....I.....v.....+Gn.\Gn.\
46960960	dt[1].gif.....I.....{.....+Gn.cGn.c
46961024	dt[1].gif.....I.....+Gn.iGn.i
46961088	QB057NSM.....Gn..Gn..
46961152	mbcsc[1].....Gn.iGn.i
46961216	mbcsc[1].....Gn.iGn.i
46961280	banner[2].htm.....M.....sGn.jGn.j
46961344	get-user-id[1].js.....Q.....Gn.jGn.j
46961408	clk[1].js.....I.....Gn.jGn.j
46961472	6910866308792112351[1].htm.....Z.....`Gn.jGn.j
46961536	02Fdx1a_02F2-8-9_02Fhtml_02F-sf11.htmh Gn.kGn.k

☒ Text ☐ Hex



To protect yourself

- Patch your devices
- Don't click on links in emails or documents
- Avoid using services you could use on traditional computers on non-traditional ones
- Use multi-factor authentication
- Avoid public wifi
- Keep personal information personal
- Educate each other
- Report problems when they occur



If you are a victim of cyber crime

- Notify local authorities immediately
- File a complaint with the Internet Crime Complaint Center www.ic3.gov



We will never eliminate attacks, but we can take steps to limit their frequency and impact..



Thank you!

