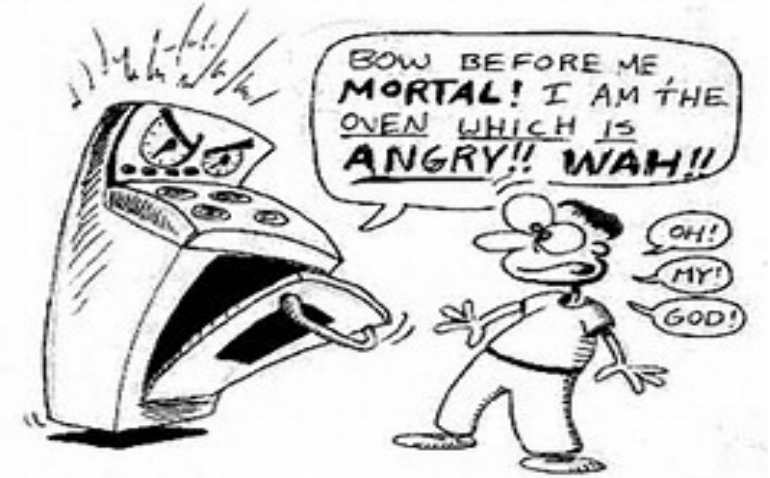
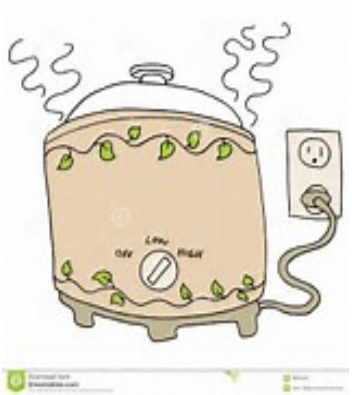
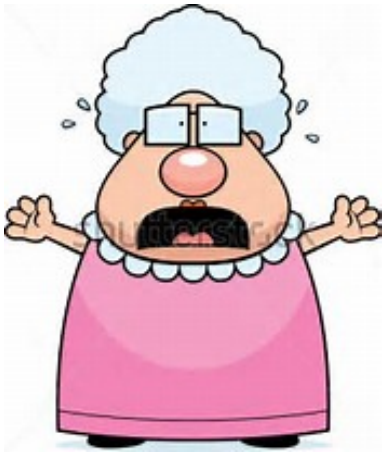
The IoT of Things

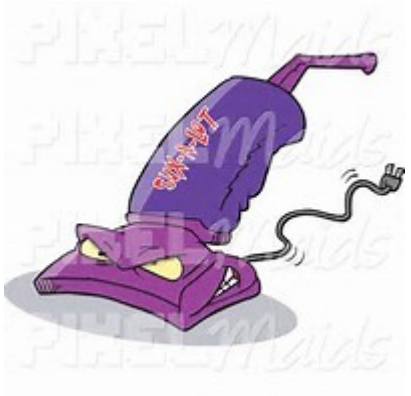
or...



Mama Got Attacked by the Home Appliances!







First...Some Background...

1975 - X10 connectivity system developed utilizing home power lines... not really practical...

1985 - AT&T creates and markets “Fiber to the Home” and “SmartHouse” (w/NAHB) technologies

1990 - John Romkey creates first internet connected (remote on/off) toaster using TCP/IP

...and then...

1998 - Mark Weiser creates water fountain whose flow & height mimicked the stock market

2000 - LG announces plans to design an internet connected refrigerator

...and then...

2010 - Tony Fadell (creator of the iPod) creates “Nest”, a more agile platform

2012 -Launch of “Smart Things” app - over 10,000 hubs shipped by 2013

...and in 2013...

Belkin launches its “WeMo” platform using a smart plug between the wall socket and the device...

Microsoft launches the “Lab of Things” to encourage connectivity development...

Linux Foundation launches “AllSeen Alliance” - an open source software backed by twenty-three (23) manufacturers...

...and then, in 2014...

LG launched a line of appliances using the “HomeChat” mobile messaging app...

Ben Kaufman (creator of “Quirky”) launched “Wink” - small networks controlled by one app...

Samsung acquired SmartThings – Samsung “Smart Home” app connects multiple home devices...

Google acquired Nest Labs for $3.2B and focuses on re-inventing home automation...

...and even MORE in 2014...

Apple announced “HomeKit” which allows control of lights, locks, cameras, doors, etc....

Samsung, Dell, & Intel joined forces to create the “Open Interconnect Consortium” standard...

Nest, Samsung, & others launched “Thread” – an IP-based wireless network protocol...

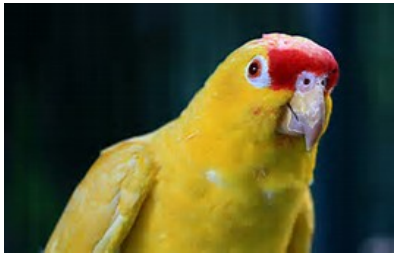
...and in 2015...

Belkin introduced room motion sensors, window/door sensors, water usage sensors, etc.

Nest announced its “Works with Nest” open source capability - Whirlpool, LG, Jawbone, UniKey, and others plan to incorporate it

Samsung CEO B.K. Yoon reiterates company's intent to integrate all products (90% by 2017)

...and MORE in 2015...



“Parrot Pot” – Self-monitoring/self-watering plant pot … (huh?)...

Keen SmartVent – Allows remote control of individual HVAC ventilator settings...so your self-watering plant doesn't get chilled ???

Sony “Life Space” UX – Allows remote control of lights, speakers, projections, SmartLights, etc...so your self-watering plant gets plenty of light ???

Examples of Attacks – Jan 2014

Proofpoint Inc. reports first proven IoT cyber attack using “smart” appliances

Attack perpetrated **via botnet** of “zombie” devices (100,000+) active 12/23/13 through 1/15/14

- Penetration of home network routers, multi-media centers, TVs, and at least *one refrigerator*

- Originated malicious spam and phishing emails, usually w/o the owner's knowledge

Jan 2014 (cont'd)

- Waves of malicious emails – 750,000 total, sent in batches of 100,000, three times per day

- More than 25% of the volume was sent by “things” that were not laptops, desktops, etc.

- No more than 10 emails were initiated by *any single device!*

Examples of Attacks – Feb 2014

Belkin devices remotely commandeered using their “WeMo” firmware update mechanism

Devices **exposed password & crypto signing key** used for updates (AO Active)

Devices *also* **failed to validate SSL certificates** when connecting to Belkin servers

Examples of Attacks – Nov 2014

"Network World" reports an on-line site linked to 73,011 unsecured security camera user locations

Locations included 256 countries including: USA (11,046), S. Korea (6,536), & China (4,770)

Devices manufactured by Foscam, LinkSys, Panasonic, Avtec, Hikvision, & others

Access path was via **default passwords**

Examples of Attacks - Apr 2015

Reported in “Network World”- A new method of attack through an *alternate* vulnerability path

Devices purchased from retail store stock, **exploit mechanism loaded** in by hacker ***at home***, and then **returned to the retail outlet** for re-sale

- Synack researchers purchased several popular IP cameras to test attack methodology...

Apr 2015 (cont'd)

- Synack researchers altered the test devices and re-wrapped them in original packaging

- Co-workers *could not* identify which units had been opened and altered

a] Hacker buys and alters device

b] Hacker returns device to store for credit

c] Unknowing victim buys compromised device

d] Hacker accesses compromised device

Examples of Attacks – Aug 2015

“Network World” reports story from “The Register”

“Pen Test Partners” found flaw during exercise at “Def Con” conference in August, 2015

Unit impacted – Samsung model RF28HMELBSR

Aug 2015 (cont'd)

Vector was via the **user's "Gmail Calendar"**, which is incorporated into the unit's display functionality

Device **did not validate SSL certificates**, allowing access to the network AND user credentials

Attack was essentially a "Man in the Middle" exploit, but other vulnerabilities are possible

Examples of Attacks – Oct 2016

"KrebsonSecurity" reports massive "Mirai" (Japanese for "future") exploit

Mirai primarily exploits **default credentials** to create botnets

Internet infrastructure provider "Dyn" was a primary target of this exploit

Impacted users included: Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix

Examples of Attacks – Oct 2016

"KrebsonSecurity" reports massive "Mirai" (Japanese for "future") exploit

Mirai primarily exploits **default credentials** to create botnets

Internet infrastructure provider "Dyn" was a primary target of this exploit

Impacted users included: Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix

Oct 2016 (cont'd)

Attack vectored though **DVRs and IP cameras** manufactured by XiongMai Technologies

XiongMai products have been used in *multiple* manufacturers' consumer end-products

Per Zach Wikholm of “Flashpoint” - User **cannot change passwords**, which are *hard-coded* in the device

“Flashpoint” scanned internet in October 2016 and found 515,000+ vulnerable devices

Potential Points of Vulnerability

- Coffee makers
- Crock pots
- Refrigerators
- Dishwashers
- Thermostats
- Garage door openers
- Webcams
- Baby monitors
- Smart TVs
- Adjustable beds
- Heart monitors
- Breathing ventilators

...Additional Unique Risk Factors...

This market is driven by consumers who *DO NOT* associate IT risk with their purchases

Susceptible device vendors are led by executives focused on sales, profit margin, and market share – *NOT IT Security*

This market sector has *little or no* experience with, knowledge of, or sensitivity to... IT Security

Potential Damage

Theft and exploitation of banking and credit card account numbers and logins

Theft and exploitation of business information, including information corruption

Utilization of access and credentials to proliferate spam & DoS attacks via home appliance botnets

Utilization of access to alter IoT device settings, *including medical devices*

Violation of user privacy, including access to baby monitors

Add'l Threat Information

Per “Massive Media” 10/31/16 – Other Mirai exploits have since been identified

Universal Plug & Play (UPnP) poses a security risk:

- *NO* form of user authentification is required

- *ANY* app can ask the router to forward a port over UPnP – probably *NOT* secure...

Firmware updates delivered through WeMo-paired devices commonly use *non-encrypted* channels

So, Where Do We Stand?

NO federal laws, policies, or guidelines exist

Vendor efforts are focused primarily on providing "legalese" disclaimers...*protecting THEM*

Third-party components in products may constitute a significant – *and HIDDEN* – threat

It may *NOT BE POSSIBLE* to change passwords in some products *OR* disable the IoT features

IoT capable devices *CAN BE SUSCEPTIBLE* to tampering, return, re-sale, and exploitation by hackers

What Can We Do?

VERIFY the IoT capabilities and associated risks with ALL existing ...and new...products

Consider MOVING AWAY from devices which CANNOT be readily or practically secured

MONITOR THE MEDIA for information about IoT exploits and risks

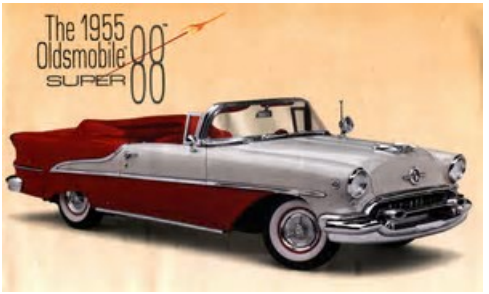
Investigate products such as “Dojo” to block access and “Shodan” to monitor devices

Be careful DISPOSING OF IoT appliances – Remember what we all learned about printers ???

...Worst Case Scenario...

- Your “smart” bed folds up and traps you...
- The thermostat drives up the temperature...
- The IoT vacuum cleaner blocks the door...
- Your SmartPhone answers that you are “out”...
- Your webcam broadcasts the whole thing while the coffee pot, the crock pot, and the microwave bubble over and celebrate in the kitchen while the garage door happily opens and closes...

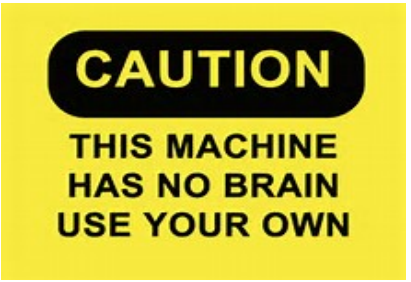
...Other Options..



Buy a 1955 Oldsmobile...

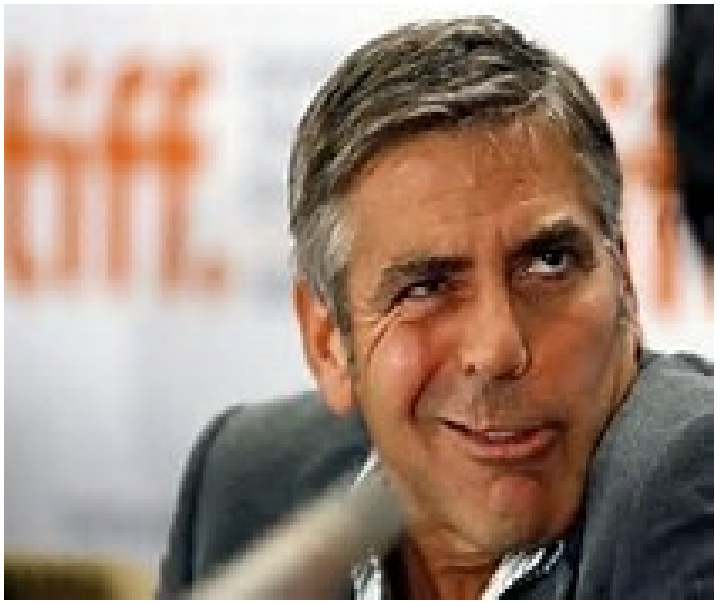
Learn to cook over a campfire...

Learn to love “dumb” devices - some of us can relate to them pretty easily...



NEVER leave your IoT devices together in the dark where they can conspire against you!

Questions or Comments?



Sources

http://mashable.com/2015/01/08/smart-home-tech-ces/

https://phys.org/news/2014-01-cyberattack-hacked-refrigerator.html

https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/internet-of-things-cyberattack/

http://www.massivealliance.com/2016/10/31/mirai-malware-protect-internet-things-iot-exploit/

http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html

http://www.massivealliance.com/2016/10/31/mirai-malware-protect-internet-things-iot-exploit/

https://arstechnica.com/security/2014/02/password-leak-in-wemo-devices-makes-home-appliances-susceptible-to-hijacks/

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html

http://www.sfgate.com/business/article/Smart-devices-have-confusing-policies-may-be-6234557.php

http://www.bankingexchange.com/news-feed/item/5770-5-hacks-into-your-internet-of-things-devices

https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices