**What is IoT?**

* The **Internet of Things** (**IoT**) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.
* British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers - referring to a global network of Radio-frequency identification (RFID) connected objects).[10] Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications.[11] The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid,[12] and expanding to the areas such as smart cities.
* Cisco Systems refers to IoT as the “Internet of Everything”…
* Bruce Schinerer recently referred to two new colloquial terms – World Spanning Robot and Benign Organization. There is also the term “Skynet” in reference to the Terminator movies that is frequently discussed in Blog and online postings/jargon.

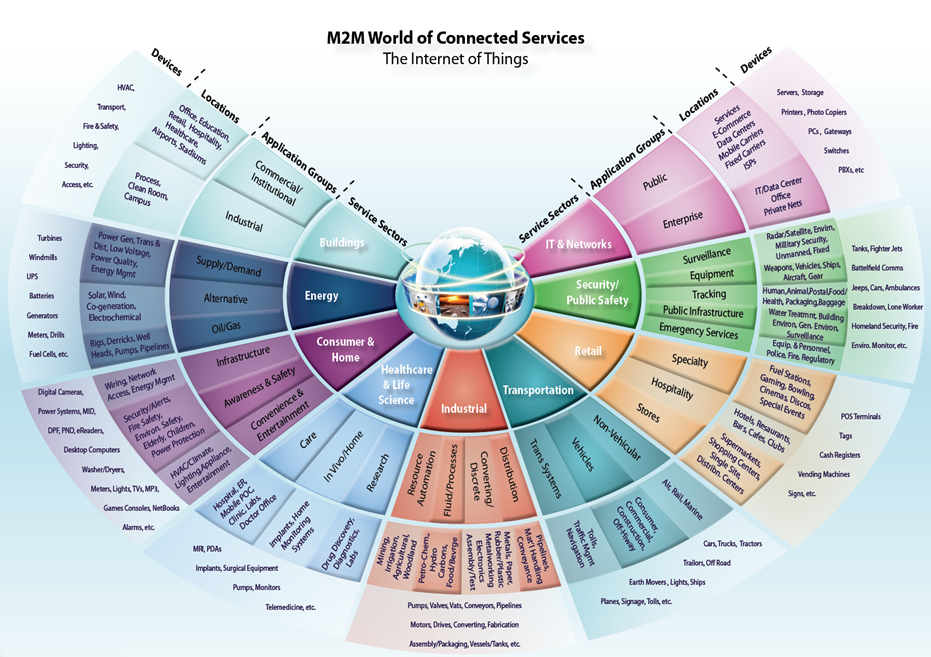
**Where is IoT?**

* IoT is everywhere! (Audience Participation)

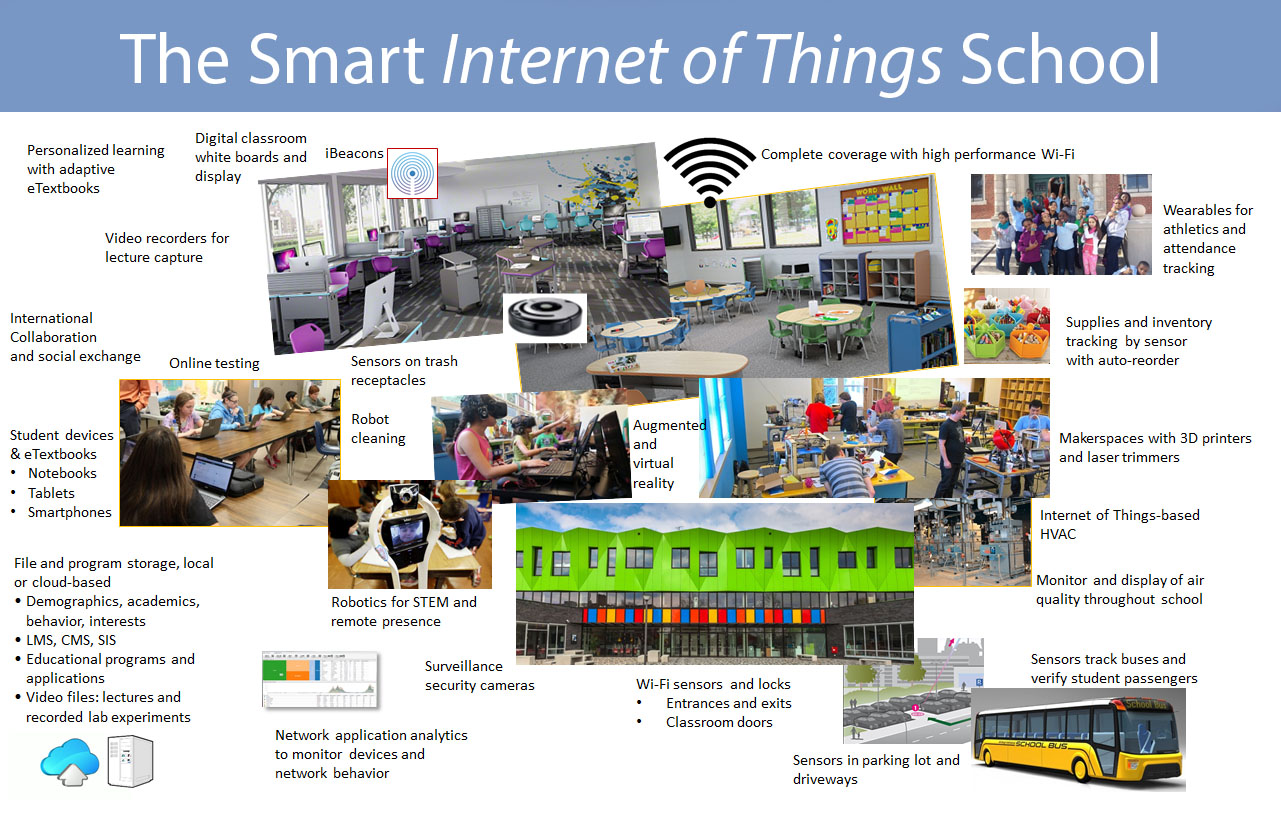
In our daily lives, we have become more reliant on IoT with our wearable tech, appliances, our cars, how we receive health care.

**M2M/IoT Sector Map :: Beecham Research**

The following graphic from Beecham Research depicts how the Internet of Things may interact with various service sectors within the public/private sectors and ordinary consumers. Public sector entities (such as universities) may have some level of involvement and interaction within all service sectors depicted; ranging from the operation and industry elements of buildings, to levels of research, retail entities, transportation, and IT/Networks. \*\*Place emphasis on service sectors, that it is likely that at least one example of devices may be found within university networks.



And in our institutions of higher learning, IoT is prevalent in the operational and research initiatives…



Lund, D., Turner, V., MacGillivray, C., & Morales, M. (2014, May). Worldwide and Regional Internet of Things (IoT) 2014 – 2020 Forecast: A Virtuous Circle of Proven Value and Demand. Retrieved January 25, 2016, from http://www.business.att.com/content/article/IoT-worldwide\_regional\_2014-2020-forecast.pdf

The following describes the “moderate forecasts” concerning growth of the IoT markets over the next several years. More extensive forecasts by Cisco Systems project 50 billion units by 2020.

The Internet of Things marketplace is expected to see increased adoption and revenue growth through the year 2020. Moderate expectations of such growth will span across business, government entities and consumers. Business is expected is expected to show the strongest gains, while consumer growth and adoption will be lower, despite more IoT marketing of devices to consumers.

**Why be concerned about IoT?**

Like all new technology, the Internet of Things brings both a beneficial and disruptive element. With the concept of “always-on”, such technology will require a change in mindset when considering implementation of products and services related to IoT. Since IoT is more and more an element in the daily lives of individuals and organizations, maintaining both privacy, security and business operations/opportunities will be more of a priority both today and in the future.

**Does IoT add additional risk?**

How visible will IoT devices be considering identification through network vulnerability scans?

What defines a network perimeter or “edge”

How are consumer devices thorough BYOD policies used in sensitive areas?

Since IoT is more and more an element in the daily lives of individuals and organizations, maintaining both privacy, security and business operations/opportunities will be more of a priority both today and in the future. : IoT are not generic items or auxiliary services like those that have been prevalent in business for years; rather, IoT devices should be considered as unique devices, each with a distinct set of security risks. Both security controls as well as security training necessary to effectively manage IoT devices may not yet be fully developed.

**Attacking IoT**

Issues that is common when attacking IoT infrastructure is similar to current levels of attacks that are currently experienced today. The avenue of how attacks may occur may however be through untraditional methods:

It may be more often to find default, weak, and hardcoded credentials (usernames passwords) within IoT devices

The issue of upgrading firmware to counter vulnerabilities may be dependent both upon how devices are designed during development; issues may occur that upgrading may break functionality. For this reason, vendors may be hesitate or refuse to render support in product lines and make adjustments during the next design phase of projects.

Certain IoT devices with embedded web services may also be subject to the same vulnerabilities that commonly plague web server platforms today; also with the premise that updating such functionality may run into the same issues such as

Buffer overflows are quite common vulnerabilities within technology infrastructure, with IoT no exception.

Devices may also at times use protocols that transmit credentials in the clear, in addition to having open ports

DOS/DDOS attacks may be the results in hacking or hijacking IoT devices on network(s); it also possible that through misconfigurations of IoT devices that such “attacks” may be false positives and cause business disruption

The issue of physical attacks of IoT devices may result in tampering to inject malicious code or make hardware modifications to IoT devices. In addition, impersonating or counterfeiting devices may be issues when safeguards are not in place to protect physical security.

Infiltration through non-traditional communication protocols; such as Bluetooth, Zigbee, Zwave, Sigfox, NFC, 6LowPAN, and other types of non-traditional wireless communication outside of Wifi. communication protocols as well that may not be within scope through common incident and forensic management tools.

Cross-site scripting – certain IoT devices may have embedded web server technology, putting them at risk

Buffer overflows – design flaws that may not be immediately corrected because of patching mechanisms, developmental issues during the SDLC process

Open ports – common issue on device ports that are not locked down and may be used via reconnaissance.

**Case Study: Trane**

Trane Case Study emphasis points:

3 vulnerabilities noted by Cisco Talos and company notified

Fixes occur for least severe vulnerabilities nearly a year later in firmware update, no notification given to public or Trane customers

CERT involved, no response

Firmware update released to fix most severe vulnerability, no release of information to public again or Trane customers

Cisco Talos releases full disclosures of vulnerabilities and patching requirements

Time taken from reporting to disclosure: 22 months.

**Case Study: Lessons Learned**

When it comes to vulnerabilities with IoT, expect them! Vendors may not inform the public about critical issues in their products. Since products at times may be updated or new lines come out, vendors may not necessarily invest in maintaining the security of existing products. The issue of patching mechanism may also be a factor, where they might not even exist for some products as well as layman/technical issues installing patches or firmware updates in Iot products. Larger organizations may also have issues scaling to patch/update IoT related devices, given the size of organization and number of units effected.

**Recommendations**

How do current UT165 and institutional policies, standards, and procedures take into account IoT? Are they sufficient to address areas of confidentiality of data? Does current BYOD policies address wearable tech items? Concerning the present might these policies also BYOx?

bring your own device (BYOD)

bring your own apps (BYOA)

bring your own encryption (BYOE)

bring your own identity (BYOI)

bring your own technology (BYOT)

bring your own network (BYON)

bring your own wearables (BYOW)

Awareness building for IoT will involve similar approaches currently developed in University training.

Relationship building with those departments, vendors and academia/research entities will perpetuate dialogue concerning the subject of IoT; whether within the marketing/sales/procurement of IoT devices and services and/or when internal development occurs, as in the case of research. Building relationships also assists in the awareness in the areas of privacy (both of data and individuals), what is logged when it comes to data and other transactional information, the reasons why items need to be logged (local, State, Federal laws and acts, industry-specified compliance requirements.)

Training initiatives may need to be rethought in the areas of IoT; do University partners as well as Information Technology/Information Security

How we assess for risk may change in certain retrospect. We may need to go “dig deeper” on our current risk assessments of networks, data centers, departments; to include how we assess in the areas of legal and regulatory requirements (e.g. HIPPA, PCI-DSS, FERPA). Considerations must be taken into account when system owners assume or transfer risk in relation to IoT. Different measurements may need to be considered when considering both risk formulation as well as risk acceptance when considering IoT; for system owners and data owners risk acceptance may involve additional measures IT and Security staffs must take to protect information/data.

Security controls must be in place to leverage such risk acceptance in the overall network.

There is the need to consider how we scan for vulnerabilities; while certain IoT Devices may show up on scans, others types of IoT devices may not.

Forensic approach to IoT may require some retooling in the areas as to whether local Security staffs are equipped and trained to deal with incidents when they occur, as well forensics capabilities in the situations with forensics may be outsourced/required of by third party entities.

With the incorporation of IoT in today’s networks, there will be an increase in the need for logging and monitoring capabilities

Increasing need for log storage

“Needle in a bigger haystack” will make incident response and forensics more challenging, are current capabilities sufficient?

Logging in regards to compliance may involve a number of factors; to include storage of logs, relevance of logs, privacy concerns when dealing with University partners of logging.

Considerations for the redesign of networks may come as more demand for traditional IPv4 addresses, with the contingency on planning for further IPv6 implementations in regards to IoT. Planning of network design may also require changes on how bandwidth as consumed, quality of service, and prioritizing network traffic through new designs. And further, the redesign of networks may also take into account of how firewalls and IDS/IPS may handle IoT traffic when considering IPv6

**Threat vs. Opportunity**

In closing, while, how we as security professionals work, support, and provide the security expertise for Higher Education business initiatives is crucial to success in the scope of IoT.

**Just what is this?**

**Its components are:**

**A Raspberry Pi, an external hard drive, a wireless router, a GSM device, a battery backup.**

**What does it do, what is it for?**

**An IoT mystery….**

**References:**

* [**http://www.utsystem.edu/offices/board-regents/uts165-standards**](http://www.utsystem.edu/offices/board-regents/uts165-standards)
* [**https://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/**](https://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/)
* [**http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx**](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx)
* [**https://www.owasp.org/images/7/71/Internet\_of\_Things\_Top\_Ten\_2014-OWASP.pdf**](https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf)
* [**https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf**](https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf)
* [**http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html**](http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html)
* [**http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability/#**](http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability/)
* [**http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about**](http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about)
* [**https://thenewstack.io/tutorial-prototyping-a-sensor-node-and-iot-gateway-with-arduino-and-raspberry-pi-part-1**](https://thenewstack.io/tutorial-prototyping-a-sensor-node-and-iot-gateway-with-arduino-and-raspberry-pi-part-1)
* [**http://www.business.att.com/content/article/IoT-worldwide\_regional\_2014-2020-forecast.pdf**](http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf)
* [**http://blog.talosintel.com/2016/02/trane-iot.html**](http://blog.talosintel.com/2016/02/trane-iot.html)
* [**http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/**](http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/)
* [**http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/**](http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/)