Internet of Things

David Fletcher

Introduction

The Internet of Things (IoT) got its start in 1999 with the founding of the MIT Auto-ID Center. The goal of the Auto-ID Center was to develop a broad class of identification technologies for use in industry to support automation, reduce errors, and increase efficiency. The cornerstone of this technology was the Radio Frequency Identification (RFID) tag. The RFID tag allows one to uniquely identify any tagged object and discover details regarding the object via a centralized service. This initial work culminated in the launch of the EPC Network in 2003. This network demonstrated that computers could be used to automatically identify and track man-made objects through the production, distribution, and delivery processes. It also opened the door to realizing new efficiencies in manufacturing and distribution. Now, production objects could be tracked in mass to identify bottlenecks in production, reduce the amount of human labor required, and deter item theft [1].

After the EPC Network demonstration, the Auto-ID Center was split into Auto-ID Labs and EPCglobal. The purpose of Auto-ID Labs was to develop the hardware, software, and languages that could be integrated into the current internet in order to realize the IoT. In contrast, EPCglobal was charged with commercialization of IoT. Since this time, advancements in wireless communication and embedded computing have broadened the scope of IoT to include virtually any device that can be used to sense and communicate across the internet [1].

This broadening of scope has caused a fair amount of confusion regarding the definition of the IoT. A sampling of definitions includes:

- The capability to connect, communicate, and remotely manage a number of networked, automated devices via the Internet [2].

D. Fletcher (✉)
e-mail: david.fletcher.6@us.af.mil

M. Blowers (ed.), *Evolution of Cyber Technologies and Operations to 2035*,
Advances in Information Security 63, DOI 10.1007/978-3-319-23585-1_2

- The point in time when more "things or objects" are connected to the Internet than people [3].
- A world-wide network of interconnected objects uniquely addressable based on standard communication protocols [4].
- The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data [5].

Each of these definitions paints a very broad picture of the internet of things and each includes the common characteristic of an objects' ability to communicate. In fact, it is this ability for objects to communicate that delivers the power of the IoT. This power is found in the form of data. Through arrays of sensors, each IoT device is predicted to generate of a waterfall of data that can be used to increase the collective knowledge and wisdom of the human race. More data captured results in a greater level and fidelity of knowledge and wisdom for mankind [3].

The size and scale of the Internet of Things is expected to be monumental. Various predictors of IoT scale have estimated that as many as 100 billion devices will be connected to the internet by the year 2020 [1, 3, 6]. This number does not account for traditional internet devices such as computers, tablets, and smart phones. In addition, the number of devices that will have indirect connections to the internet (typically sensors) will number in the trillions by that same date [7, 8]. If these predictions come to pass, then the number of machine to machine communication sessions will be 30 times that of human to human communication on the internet [1]. In addition, given a population estimate of 7.6 billion people in 2020 each person will be associated with six directly connected IoT devices, over 130 sensors, and innumerable embedded objects [8].

Gartner conservatively estimates that in 2020 there will be 25 billion IoT devices connected to the internet [6]. Analysis of the growth trend presented in the study indicates that the IoT grows by roughly 35 % year over year. Extrapolating this trend out to the year 2035 results in an IoT device count of 2.2 trillion devices. Because of the sheer number of devices and their pervasive deployment in our surrounding environment the Gartner study goes on to describe the IoT as disruptive across all industries and areas of society [6]. This sentiment has been echoed by several other sources including a National Intelligence Council study conducted in 2008 [9, 10].

Future Benefits

There is almost unimaginable potential for the sensing, processing, informing, and decision making power of the Internet of Things. This potential is so widely recognized that industries have begun creating their own terms that embody the intent of the IoT within their particular markets. Terms like Industrial Internet, Industry 4.0, Smart

Planet, Smart Grid, and Smart Home attempt to restrict the focus of IoT technology to a specific vertical industry. Examples of Internet of Things research can be found in nearly every industry.

At the consumer level, the Internet of Things is being developed in the form of home automation. Through this technology, individuals will be able to create efficiencies based on information that typical home appliances generate. For instance, a refrigerator will maintain a full inventory of its contents in addition to product expiration information to better inform the homeowner to support product ordering and waste minimization. This information could be further correlated with favorite recipes to determine available ingredients and potentially re-supply. Orders would be automatically transmitted to a grocery store with pick-up or delivery being the only remaining task. Gartner predicts that the efficiencies realized by the connected kitchen will reduce consumer cost by 15 % [6]. This example is a single instance of IoT in the home. Other offerings include connected televisions, entry control and alarm systems, light switches, light bulbs, etc. An almost endless array of products will exist to support the efficient management of the home.

In retail stores, RFID is poised to change the way that we shop dramatically. Once all of the products in a retail outlet are tagged and the facility is equipped with reader technology it becomes effortless to manage stock and operate with much lower overhead than today. These efficiencies will be realized in many different ways. First, the reliance on human labor will be reduced as instant inventory becomes possible. Second, shoppers will have reduced wait times to complete purchases as reader technology can be used to instantly inventory and tally their purchases for checkout. Finally, by observing consumption trends, better estimates of product demand can be made to eliminate overstock situations and reduce requirements for stock on hand [11].

Efficiencies in the delivery of these goods and services to retailers can be realized through IoT integration into supply chain logistics. An example of this activity can be seen in the Port of Hamburg which has deployed a system of sensors into the roads, parking spaces, and trucks. Drivers get real-time information in their vehicles to aid in navigating the port and delivering goods for transport to their final destination. These concepts have in-turn been applied to management of waterway and rail traffic [12]. Cascading retail efficiencies with supply chain efficiencies could allow stock on hand to be distributed to reach a wider population while potentially reducing overall cost. This is possible due to efficiencies gained in delivery of goods and reduction of stock on hand based on consumption trends. This surplus stock will consequently be available for distribution rather than being stored in a stock room or spoiling on the shelf.

In the facilities sector, efficiencies are already being realized with the inclusion of industrial control systems for everything from heating, ventilation, and air conditioning control to ambient light sensing and adjustment. These capabilities allow facility operating costs to be slashed by adjusting temperature and lighting based on occupancy. In addition, through data collection, trends for energy consumption can be developed and

monitored to support problem diagnosis. However, this is just the beginning of the Internet of Things revolution for facilities. From a facility maintenance perspective, smart devices such as emergency lighting and smoke detectors can alert maintenance staff proactively when problems occur. Mundane tasks like monitoring soap levels in washrooms can also be automated to reduce staff levels and decrease response time [13]. Other technologies such as smart elevators promise to more efficiently manage resource use and minimize wait times for users by predicting peak usage and positioning cars strategically for response [14].

With intelligence embedded into individual facilities the next evolution becomes the realization of smart cities. The smart city is a superset of the smart facility concept and is used to more efficiently manage and instrument public resources. Public buildings are instrumented as described above to increase efficiency in utility monitoring and consumption. Offerings such as smart parking, lighting, waste management, traffic management, and environmental monitoring improve the effectiveness of urban infrastructure while decreasing the overall operating costs of municipalities [15].

In the realm of agriculture, smart sensors will be used to monitor and communicate soil composition and irrigation conditions to enable real-time adjustment. This information, coupled with weather forecasts, temperature, and humidity readings can be used to more accurately manage resources. Watering of crops can occur at a more accurate rate to limit the cost and environmental impact of irrigation while conserving this critical natural resource. Livestock will also be tagged and monitored to proactively manage health of the herd and farm implements will include sensing devices to provide fleet diagnostics to farmers [16].

The automotive industry also holds great promise for the Internet of Things. In addition to features such as entertainment and navigation, the automotive industry will integrate a vast array of sensors into new automobiles. These sensors will provide advanced diagnostic information as well as features such as collision avoidance and traffic management sensors. This array of features will not only revolutionize consumer vehicles but entire fleets of commercial vehicles in every industry. The ability to collect diagnostic information will allow proactive management of the fleet and reduce maintenance and overhead costs [16].

The IoT adds value to the medical field as well. Initiatives in smart medicine include technologies that support proactive rather than reactive medicine. Through wearable (such as our clothes) and implantable (artificial organs and sensors) technology as well as tele healthcare devices our physicians can get a more complete picture of our overall health rather than relying on a snapshot in time. This activity is already being observed as more and more people employ fitness bands to manage their personal health and behavior [17]. Medical breakthroughs such as the artificial pancreas will make management of diseases such as diabetes almost transparent to the sufferer while more effectively managing the effects of the disease. In addition, smart pills and nano-scale robotics will allow doctors to eliminate many of the most invasive procedures by fighting diseases like cancer where they manifest themselves [18].

Challenges

Despite all of the potential benefits outlined above, realization of the IoT faces several challenges. These challenges may result in slower than expected adoption of IoT technologies or may negate any or all of the identified benefits. A literature review reveals the following challenges to full scale deployment and adoption of the Internet of Things.

The Internet of Things relies on internet connectivity in order to transmit and receive data from the embedded processors and sensors. Currently, the public routable Internet Protocol version 4 address space is fully saturated. Evans predicts that IoT adoption and growth will be highly dependent upon deployment of the next generation Internet Protocol. Internet Protocol version 6 provides ample address space to handle the immense number of devices that IoT promises [3].

A large population of the IoT will require energy to operate. Many of these devices will also be deployed in locations that do not have energy readily available. Examples include wearable technology, retrofitted sensors, and technologies such as smart roads. This leaves two options for powering devices; energy harvesting and battery power. Without advanced power saving schemes and overall reduced consumption it may be economically unfavorable to adopt IoT technologies as the cost to operate devices may outweigh any efficiencies gained [3, 19, 20].

The Internet of Things will rely heavily on wireless communication. Another shortfall in physical capacity is the availability of wireless spectrum. A myriad of wireless technologies are poised to support IoT such as near field communication, zigbee, zwave, Bluetooth, wi-fi and others. As more and more devices are added to the IoT there will be an increasing amount of interference due to proximity of devices. This leaves just a few solution choices; either devices must become increasingly more resilient to interference, more spectrum must be added, or new protocols must be developed [21, 20].

The large number of devices deployed in the IoT will generate a mountain of data that must be collected, analyzed and responded in a timely fashion. This will create several challenges that will affect the future of IoT. First, big data analytics must mature to the point that this data can be processed in a timely fashion [9]. Second, data centers must be prepared to receive and store this data. Third, policy must be developed regarding the judicious use and retention of data that may be sensitive in nature [22].

The IoT must also be supported with standards in order to ease complexity involved in deployment of products and promote interoperability among vendors. These standards must be applied across the spectrum of capability to include policy, protocols, and architecture. Focus on the greater landscape of IoT must be achieved to maximize return on investment. Currently, research on IoT exhibits a fragmented approach with focus on single application domains and technologies [20]. Recent activity by the Federal Trade Commission and congress also highlights the need to address policy regarding security and privacy [22]. While IoT specific protocols have been developed it is likely that there is much work to be done to unify the field [23].

Privacy is a serious issue for the future of the Internet of Things. Through the technology employed IoT will collect mountains of data that are both mundane and extremely intimate in nature. In order to promote IoT adoption, vendors and service providers must exercise due care in developing and deploying technology. In addition, data that is generated by the IoT must be scrutinized to ensure that the appropriate access controls are in place, data is protected at rest and in transit, data is effectively anonymized, and that data is destroyed when it is no longer useful [22]. These concerns are underscored by recent data breaches at retailers such as Target, Home Depot, and Anthem [24]. To make matters worse, all of these requirements must be levied on hardware and software platforms that are typically resource-constrained [25].

Just as important as privacy is security for the devices that make up the Internet of Things. A lack of forward thought and attention to security leads to the types of breaches identified above. Hardware designers must ensure that their devices can support security enhancing features and that security is considered during up-front device design [25]. Software and firmware developers must likewise employ security best practice in design and consider the mechanics of vulnerability discovery and remediation. Finally, those deploying IoT technology must pay careful attention to ensure that sensors, devices, and services are installed with available security enhancing features enabled and properly configured [26].

Another challenge that accompanies security is cost. With a great deal of interest in the Internet of Things there will be a large amount of competition. Consumers (both individual and corporate) must be educated to understand the security differences between products. In many cases, purchase of a product comes down to cost comparison [19]. This behavior will likely be more prevalent in individual consumer purchases. When it comes to a commodity device like a light bulb the consumer may not look beyond cost in making a purchase. This brings a whole new aspect to the buying process as these devices will likely remain in service for an extended period of time with little or no support [27].

Current State of IoT Security and Privacy

Of all of the challenges identified above, none has a greater ability to influence IoT adoption than security and privacy [22]. Unfortunately, users seldom have a full understanding of the impact of security until after a breach has occurred. However, given recent security breaches that have led to compromise of privacy, consumers' appetites for poor security are waning. Unfortunately, there is an abundance of evidence to indicate that security in the IoT is lagging behind and in many cases repeating cyber security history [28]. This concern has become so great that Congress and the Federal Trade Commission have begun taking an interest in order to provide greater consumer protection [22, 29].

In recent security reviews conducted by the HP Fortify [30] and Veracode [31] teams, consumer-grade IoT devices have not fared well. In addition, research conducted by

Miller and Valasek [32] has indicated a great deal of vulnerability in modern automotive systems, which are projected to number 250 million by the year 2020 [6]. Finally, a session titled "The Internet of Fails" at the annual DEFCON conference in Las Vegas exposed a handful of these failures which has served to illustrate the pervasiveness of the problem [26]. One element that each of these studies have in common is that the security problems that are being exhibited are well known security issues that are present or have been eliminated in other more typical information technology domains. The problem is bad enough that the Open Web Application Security Project (OWASP) has created an Internet of Things Top 10 list of security oversights [33]. The findings of the HP Fortify report are directly correlated to this list [30].

"Internet of Fails" describes a confluence of several factors that has led to poor security in consumer-level IoT devices [26]. Low-cost development platforms such as Arduino and Raspberry Pi have increased accessibility for experimentation. These low-cost platforms typically require a minimum of skill to configure and program which has, in turn, led to a larger developer pool that is not typically familiar with secure device configuration and secure programming practices. These developers also may not understand the implications that lack of inherent security controls means for their potential user base.

In addition to typical revenue streams, such as venture capital, non-standard streams of revenue have appeared to answer the call for innovation. Crowd sourcing applications such as GoFundMe [34] and Kickstarter [35] have generated funding for a wide range of products. Since this funding is user-supplied much of the rigor of the risk-reward equation has been boiled down to functional demand. Where crowd sourced funding for a product is tight innovators must make trade-offs between cost, functionality, time to market and security. In this equation, security typically loses out. Especially when there is market competition and profit margins are slim [26].

Some of the basic security issues identified in the IoT studies above include the following:

- Support – It is projected that some IoT devices will be expected to be in service for up to 20 years [27]. With the burgeoning nature of the IoT market buyers must make wise investments in viable technology companies or risk having to purchase the same device multiple times. It is reasonable to expect that some IoT start-ups will fail over this period of time [26]. Without making this risk evaluation it can be expected that a number of devices will remain in service and unsupported. Reluctance to accept the end of life announcement for Microsoft Windows XP serves to illustrate resistance to replacement products despite increased risk when that product is still functionally capable [36].
- Maintenance – The internet of Things represents a vast expansion in the number and types of devices connected to the internet (directly or indirectly). As consumers and businesses adopt IoT technologies they must also consider the requirement to perform updates on these devices. While an auto-update infrastructure is desirable, this infrastructure carries its own security concerns such as the possibility for watering hole attacks and firmware modification in transit [26].

- Lack of Physical Device Security – Embedded systems, especially development platforms, have hardware debugging interfaces [26]. If these interfaces are not properly protected or physically disabled then malicious actors may be able to extract and reverse engineer firmware installed on the device. Since IoT devices must be cost conscious it is trivial for a malicious user to purchase these devices. Compromise of a single device may lead to device class level compromise due to commonality or the nature of the vulnerability.
- Lack of Encryption – In order to be useful, Internet of Things devices must communicate information. This information is typically transmitted to a gateway device or web service and in-turn viewed by the user using a typical computer or mobile platform. This can lead to a large number of communication paths that, if not properly secured, may be intercepted or manipulated by an attacker [30]. Even more important is protection of key material. The "Internet of Fails" DEFCON presentation identified situations where private keys could be extracted from firmware updates [26]. Use of hard coded key material in this fashion should be avoided at all cost. Once a key has been compromised communication should be presumed to be unprotected and subject to interception.
- Lack of User-Level Security – Users and their passwords have been the weakest link in security since the dawn of the internet. This concept remains true in Internet of Things devices. In the HP Fortify [30] report several of the devices that the team tested had a user interface that did not require passwords of sufficient length or complexity to adequately protect the users' information. In addition, "Internet of Fails" exposed passwords that were hard-coded in firmware that could be easily discovered in downloaded updates [26].

IoT Security and Privacy Concerns

If the current protective posture of IoT does not improve the internet will be rife with targets for attack and abuse. Many researchers are addressing difficult topics such as next generation capabilities to support Confidentiality, Integrity, and Availability [2, 20, 27]. However, a vast amount of vulnerability typically lies in the details of implementation, configuration, and administration. Due to the resource-constrained nature of IoT devices, it is likely that security will remain a variable in the time, functionality, and cost equation for some time to come [8, 25]. In addition, consumer-grade devices are likely to receive less rigor than commercial-grade devices from a security perspective [19]. This does not bode well because in the internet we have learned that a risk assumed by one is a risk to all. As illustrated in the Target breach, one compromise can lead to another where one party inherently assumes risk that another takes [37]. Many small businesses employ consumer-grade devices in their networks as a cost saving measure. This becomes increasingly important as more devices incorporate functionality to affect our physical environment.

Because of resource constraints, IoT devices will be particularly susceptible to Denial of Service (DoS) attacks [8]. These classes of attack serve to exhaust resources

on a particular device in order to deny service to its operator. This can have a systemic effect in the IoT as other devices that rely on information produced by the targeted device will be denied this information. In turn, the information produced by upstream processors and sensors may therefore be denied or skewed based on the activity [30].

In addition, through compromise, IoT devices become excellent targets to stage a Distributed Denial of Service attack. While the IoT in general is expected to be largely heterogeneous there will be environments and classes of devices that are homogeneous or employ the same underlying technology. If an attacker is able to take advantage of this and compromise a large swath of devices they may be used to launch an asymmetric attack against a target entity and overwhelm it. The compromised devices may also pose a challenge to diagnose as they typically don't have a standard user interface and are expected to generate a large volume of continuous communication.

The Internet of Things also offers opportunities for re-envisioning attacks such as resource denial, resource exhaustion, physical safety, and pervasive surveillance attacks. While none of these concepts are new, the wide distribution of IoT devices and internet connectivity allows an attacker to pursue them from a distance and with relative anonymity and impunity. In addition, once vulnerability is found it becomes trivial to perform mass discovery thanks to services like Shodan HQ [38] which provides search engine functionality for finding internet connected devices.

Resource denial can be approached in the same fashion that recent banking Trojans have. In this situation, attackers may compromise and control access to devices or services in return for ransom from legitimate users. Once IoT devices have become integrated into an environment it may be impossible to continue operation without them. A recent example of resource denial is that of an IoT adopter who fully automated his home. One of the devices in his home automation system malfunctioned to the point that he could no longer control any of its constituent systems. It turned out that the culprit was a malfunctioning lightbulb that created an internal denial of service on his network [39]. A question to consider is whether a typical home user would be able to solve this problem. In addition, consider the types of resource denial attacks that might be carried out by a malicious actor. This could include access denial to automation systems or disabling smart meters delivering gas, water, or electricity.

A slightly different spin on resource denial is resource exhaustion. Instead of disabling service, though, the attacker may adjust set points on appliances such as heating, ventilation and air conditioning to waste energy. On a micro scale, the objective of this type of attack may be simply to burn resources or increase operating cost. On a macro scale, the attacker may target multiple businesses or homes within a specific geographical area with the objective of increased strain on the resource provider [19]. This activity could potentially result in infrastructure damage causing widespread outages such as the blackout of 2003 in the Midwest United States [40].

As we integrate more capability to control the physical world around us physical safety becomes an issue for the IoT. The Aurora [41] project and Stuxnet [42] worm have served to illustrate that vulnerability in cyber-physical systems can have dire

consequences. A recent cyber-attack on a German steel mill caused massive damage by disrupting the control systems on a blast furnace. While there was no indication of injury, the potential was evident given that the blast furnace could not be properly shut down. Industrial control systems can be found across many industries employed in various safety critical functions [43].

Another potential threat to physical safety is integration of advanced sensing and controls within automobiles. Security researchers Charlie Miller and Chris Valasek demonstrated this type of attack through the on-board diagnostic port inside the vehicle. Their report illustrated the ability to command advanced vehicle control systems such as electronic steering, acceleration, and braking through this access method [32]. A follow-on report to their original 2013 work included an architectural review of a number of vehicles with the same types of features demonstrating the same types of vulnerabilities [44]. As mentioned earlier, Gartner expects 250 million vehicles to be connected to the internet by 2020. Implementations lacking security could allow these types of attacks to occur over the internet rather than requiring physical access to the vehicle.

Even if physical access is necessary, researchers have demonstrated other weaknesses that may grant easier access to the vehicle for implantation of malware. For instance, one researcher identified a flaw in the BMW smartphone application that rendered 2.2 million vehicles vulnerable to unauthorized access by way of unlocking the vehicle [45]. This research also revealed suspected dealer unlock codes that worked multiple times across multiple vehicles of the same make and model.

The prospect of physical access brings us to the connected home. Many home security systems allow the homeowner to control access to their residence through a smartphone application. Some systems provide the ability to not only alarm the home but control other physical aspects such as entry door locks, garage doors, lighting, and water [46, 47]. HP Fortify and Veracode security researchers surveyed several of these types of consumer devices and found an alarming number of vulnerabilities [30, 31]. The prospect of gaining physical access to a residence brings a new level of power to common burglary. Through sensors connected to these same systems attackers may be able to identify presence of the homeowner [19]. After presence is determined, an attacker may be able to take advantage of one of these vulnerabilities to obtain physical access to the premises with little risk over the internet.

The final concern that we will discuss is pervasive surveillance. Many researchers warn against the loss of privacy due to massive integration of technology into our environment. This concern is not without merit. With full adoption of the Internet of Things there will be an endless stream of data regarding our location, medical history, preferences, etc. from a vast array of devices that each may be used to uniquely identify us as individuals. Once a device is associated with an individual identity, it is likely that additional device associations can be inferred.

Some examples of current day privacy issues in the Internet of Things follow. Recently, Samsung received criticism over the privacy agreement for its smart television software. The privacy agreement warned users that any sensitive information discussed may be transmitted to a third party for translation [48]. This revelation

startled users but these same people are likely surrounded by recording devices like microphones and cameras in many of the devices they own. These devices include common items such as laptops, smartphones, and televisions but may also extend to uncommon items such as children's toys and baby monitors [49].

In addition, it is possible to read unprotected RFID tag information without the owner being aware that the tag has been read or that it even exists [50]. This activity has been demonstrated by passively cloning devices such as passports and driver's license [51]. Once RFID tags have been used to identify the majority of consumer devices and embedded into clothing and documents privacy and attribution become a serious issue if not properly protected.

Conclusion

The Internet of Things holds a great deal of promise for improving our collective lives. Knowledge gained will allow us to realize efficiencies in nearly every aspect of human life. However, rapid adoption of Internet of Things technologies may lead to long-term problems given the current state of the industry. Unless standards, interoperability, and developer/user education and practices improve there may be significant negative consequences. In addition, there must be equality between consumer grade and commercial grade product offerings with regard to security.

The number of devices expected to be deployed to support the Internet of Things underscores the requirement for adequate security and privacy. IoT adoption represents an exponential growth in the attack surface of the internet and may bring with it new and unimagined attacks as a result. Since the IoT will also connect the virtual world with the physical world, security concerns turn into safety concerns.

Privacy in the internet of things is just as important and depends on adequate security measures to be in place. The implications of the Internet of Things may in reality be the trading of functionality and efficiency for the personal privacy that we have enjoyed as a free society. The sheer number of uniquely identifiable devices associated with an individual may mean that association of any single device with that individual may lead to further associations through simple observation. This may become so pervasive that privacy is unattainable. The result may be a surveillance society like something out of George Orwell's 1984.

Bibliography

1. Santucci G (2010) The internet of things: between the revolution of the internet and the metamorphosis of objects. [Online]. Available: http://ec.europa.eu/information_society/policy/rfid/documents/iotrevolution.pdf. Accessed Apr 2015
2. Leo M, Battisti F, Carli M, Neri A (2014) A federated architecture approach for internet of things security. Euro Med Telco conference 2014, Naples, 2014

3. Evans D (2011) CISCO Internet Business Solutions Group (IBSG). [Online]. Available: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed Apr 2015
4. I. o. T. i. 2020 (2008) European technology platform on smart systems integration. [Online]. Available: http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf. Accessed Mar 2015
5. Oxford Dictionary (2015) Oxford English Dictionary online. Oxford University Press, Oxford
6. Rivera J, van der Meulen R (2014) Gartner Newsroom, Gartner, 11 Nov 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2905717. Accessed Feb 2015
7. Bryzek J, Cooper B (2013) TSensors Summits. [Online]. Available: http://www.tsensorssummit.org/Resources/TSensors%20Roadmap%20v1.pdf. Accessed Feb 2015
8. Covington MJ, Carskadden R (2013) Threat implications of the internet of things. International Conference on Cyber Conflict, Tallinn, 2013
9. Kott A, Swami A, McDaniel P (2014) Security outlook: six cyber game changes for the next 15 years. Computer 47(12):104–106
10. SRI Consulting Business Intelligence (2008) Disruptive civil technologies. United States National Intelligence Council, Washington, DC
11. Griffin J, Deuty S (2014) RFID arena. NORDIC ID, 15 May 2014. [Online]. Available: http://www.rfidarena.com/2014/5/15/rfid-shopping-cart-level-checkout-is-possible-with-technology-that-is-available-today.aspx. Accessed Feb 2015
12. CISCO Systems Inc. (2014) Internet of everything. [Online]. Available: http://internetofeverything.cisco.com/sites/default/files/pdfs/Hamburg_Jurisdiction_Profile_final.pdf. Accessed Feb 2015
13. Lakovidis V Intelligent buildings. Arqiva. [Online]. Available: http://www.arqiva.com/overviews/internet-of-things/facilities-management/. Accessed 08 06 2015
14. Kaplan M (2012) Intelligent elevators answer vertical challenges. ZDNet, 17 July 2012. [Online]. Available: http://www.zdnet.com/article/intelligent-elevators-answer-vertical-challenges/. Accessed Feb 2015
15. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet of Things Journal 1(1):22–32
16. James R (2014) The internet of things: a study in hype, reality, disruption and growth. Raymond James & Associates, Saint Petersburg
17. Greussner V (2015) Wearable device adoption revolutionizes patient monitoring. mHealth Intelligence, 29 April 2015. [Online]. Available: http://mhealthintelligence.com/news/wearable-device-adoption-revolutionizes-patient-monitoring. Accessed May 2015
18. de Medici L (2014) Top 10 implantable wearables soon to be in your body. WT VOX, 20 Oct 2014. [Online]. Available: https://wtvox.com/2014/10/top-10-implantable-wearables-soon-body/. Accessed Mar 2015
19. Koopman P (2004) Embedded system security. Embedded Computing Magazine 37(7):95–97
20. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: vision, applications, and research challenges. Ad Hoc Networks 10:1497–1516
21. Kleeman M (2011) Point of view: wireless point of disconnect. Global Information Industry Center, San Diego
22. Federal Trade Commission Staff (2015) Internet of things: privacy & security in a connected world. Federal Trade Commission, Washington, DC
23. Schneider S (2013) Understanding the protocols behind the internet of things. Electronic Design, 9 Oct 2013. [Online]. Available: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things. Accessed Feb 2015
24. Granville K (2015) 9 Recent cyberattacks against big businesses. The New York Times, 5 Feb 2015. [Online]. Available: http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0. Accessed Mar 2015
25. Ukil A, Sen J, Koilakonda S (2011) Embedded security for internet of things. Emerging Trends and Applications in Computer Science, Meghalaya, 2011

26. Stanislav M, Lanier Z (2014) The internet of fails – where IoT has gone wrong. DEFCON Conference,24Aug2014.[Online].Available:https://www.youtube.com/watch?v=WHdU4LutBGU. Accessed Jan 2015
27. Abomhara M, Koien GM (2014) Security and privacy in the internet of things: current status and open issues. Privacy and Security in Mobile Systems, Aalborg, 2014
28. Lyne J (2015) Hacking the internet of things. Sophos Labs, 5 Mar 2015. [Online]. Available: https://www.youtube.com/watch?v=wKHDyhhgSXc. Accessed Mar 2015
29. Kelly E (2015) Congress sees security risk in 'internet of things. USA Today, 9 Feb 2015. [Online]. Available: http://www.usatoday.com/story/news/politics/2015/02/09/internet-of-things-house-caucus-senate-hearing/22927075/. Accessed Feb 2015
30. Smith C, Miessler D (2014) Internet of things research study. Hewlett Packard Fortify Team
31. Carlson J, Creighton B, Meyer D, Montgomery J, Reiter A (2015) The internet of things: security research study. 15 April 2015. [Online]. Available: https://www.veracode.com/sites/defafiles/Resources/Whitepapers/internet-of-things-whitepaper.pdf?mkt_tok=3RkMMJWWfF9wsRogv63BZKXonjHpfsX87+8tWKW+lMI/0ER3fOvrPUfGjI4IScdlI+SLDwEYGJlv6SgFTbnFMbprzbgPUhA=. Accessed Apr 2015
32. Valasek C, Miller C (2014) Adventures in automotive networks and control units. [Online]. Available: http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf. Accessed Feb 2015
33. Open Web Application Security Project (OWASP). OWASP internet of things top ten project. OWASP. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project. Accessed Feb 2015
34. GoFundMe. GoFundMe. [Online]. Available: www.gofundme.com. Accessed Feb 2015
35. Kickstarter. Kickstarter. [Online]. Available: www.kickstarter.com. Accessed Feb 2015
36. Pritchard S (2014) Windows XP: why is the enterprise so reluctant to let it go? IT Pro, 5 June 2014. [Online]. Available: http://www.itpro.co.uk/operating-systems/22409/windows-xp-why-is-the-enterprise-so-reluctant-to-let-it-go. Accessed Mar 2015
37. Krebs B (2014) Target hackers broke in via HVAC company. Krebs On Security, Feb 2014. [Online]. Available: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. Accessed 08 06 2015
38. Shodan HQ. Shodan HQ. [Online]. Available: www.shodanhq.com. Accessed Mar 2015
39. Hill K (2015) Internet of dumb things. Fusion, 3 Mar 2015. [Online]. Available: http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/. Accessed Mar 2015
40. Wald M (2013) The blackout that exposed flaws in the grid. The New York Times, 11 Nov 2013. [Online]. Available: http://www.nytimes.com/2013/11/11/booming/the-blackout-that-exposed-the-flaws-in-the-grid.html. Accessed Feb 2015
41. Schneier B (2007) Staged attack causes generator to self-destruct. Schneier On Security, 2 Oct 2007. [Online]. Available: https://www.schneier.com/blog/archives/2007/10/staged_attack_c.html. Accessed Mar 2015
42. Kushner D (2013) The real story of Stuxnet. IEEE Spectrum, 26 Feb 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed Mar 2015
43. BBC Technology News Staff (2014) Hack attack causes 'massive damage' at steel works. BBC, 22 Dec 2014. [Online]. Available: http://www.bbc.com/news/technology-30575104. Accessed Feb 2015
44. Valasek C, Miller C (2014) Survey of remote attack surfaces. [Online]. Available: http://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces. Accessed Mar 2015
45. Behrmann E (2015) BMW cars found vulnerable to being unlocked by hackers. 30 Jan 2015. [Online]. Available: http://www.bloomberg.com/news/articles/2015-01-30/bmw-cars-found-vulnerable-to-being-unlocked-by-hackers. Accessed Feb 2015
46. AT&T. AT&T digital life. AT&T. [Online]. Available: https://my-digitallife.att.com/learn/. Accessed Mar 2015
47. Cox Communications. Cox HomeLife. Cox Communications. [Online]. Available: https://homelife.cox.com. Accessed Mar 2015

48. Gibbs S (2015) Samsun smart TVs send unencrypted voice recognition data across internet. The Guardian, 19 Feb 2015. [Online]. Available: http://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet. Accessed Mar 2015
49. Needle D (2015) New threats range from ‘dribbling breached data' to IoT and toys. E Week, 26 Apr 2015. [Online]. Available: http://www.eweek.com/security/new-threats-range-from-dribbling-breached-data-to-iot-and-toys.html. Accessed Apr 2015
50. Weber RH (2010) Internet of things – new security and privacy challenges. Computer Law & Security Review 26(1):23–30
51. Koscher K, Juels A, Brajkovic V, Kohno T (2009) EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. ACM conference on Computer and Communications Security, Chicago, 2009