Overview of Security and Privacy Issues in the Internet of Things

Chris Lu, chris.lu (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract:

The Internet of Things is the idea that everything around us from cars to ovens can be connected. If everything around us is linked and collecting information, these networks must be able to provide security and privacy to the end-user particularly in low-power lossy networks. Certain features including energy conservation and automation differentiate low-power lossy networks from the standard Internet. This paper examines how these qualities affect implementations of security and privacy.

Keywords:

IoT, PANA, LLN, IKEv2, HIP, EAP, ROLL, Security, Privacy, LLN, RPL

Table of Contents

1. Introduction

As more devices become connected to the Internet, networks between devices, especially sensors, will become more prominent. The data collected and communicated over these networks may contain user-sensitive information such as health data. It is important to ensure the security and privacy of the users of these networks. These networks of autonomous devices connected to each other, the Internet of Things (IoT), have already been deployed for many uses and are looking to transform the way we live.

1.1 What is the Internet of Things?

By 2015, the Federal Trade Commission (FTC) believes that there will be twenty-five billion things or devices connected to the Internet. By 2020, the FTC estimates fifty billion things [FTC13]. Almost anything can have a sensor attached to it and have it connected to a network.

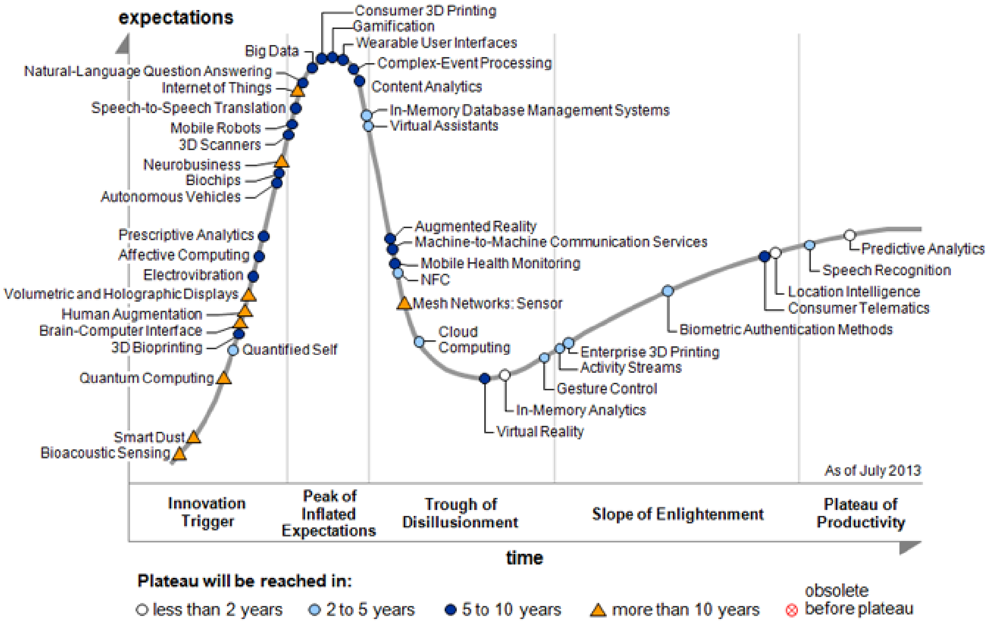


Figure 1: Gartner's 2013 Hype Cycle for Emerging Technologies

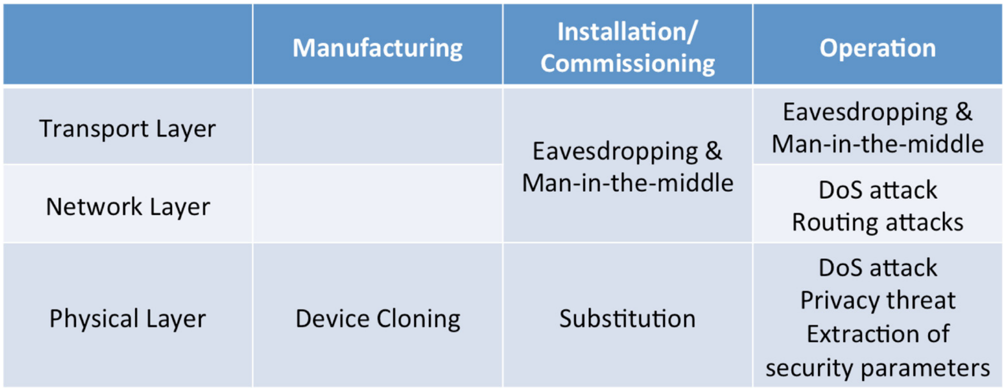
This idea, the Internet of Things, has a multitude of applications to benefit users. IoT is being used to monitor health, automate homes, and much more. Already, there are over three billion sensors and the number is increasing rapidly. According to Gartner's 2013 Hype Cycle for Emerging Technologies as seen in Figure 1, the Internet of Things has just reached the Peak of Inflated Expectations and can be expected to reach the Plateau of Productivity in over ten years [Gartner13]. At this current phase with high future expectations, security and privacy for users become important concerns.

1.2 Differences between IoT and traditional Internet

Internet of Things has several key differences from the traditional Internet. Many times, IoT is deployed differently than the standard Internet. Many IoT networks are deployed on low-power lossy networks (LLN) while others have highly dynamic topologies depending on the application, e.g. vehicular networks and medical devices. LLNs are networks constrained by energy, memory, and processing power. Many times, LLNs experience high data loss. These distinctions change the approach needed for security and privacy [RFC6550]. For many mobile or wearable sensors, which are deployed in low-power lossy networks, resource conservation becomes a serious consideration. LLNs require nodes to be autonomous and conserve energy. This results in nodes that sleep or enter power-saving modes. These aspects have not been considered for the standard Internet.

2. Lifecycle of a "thing"

Even though there are a high variety of uses and deployments of the Internet of Things, this paper will focus on security and privacy for low power and lossy networks. A device or thing goes through several stages in its lifetime [Garcia13]. At each stage, there are different security and privacy concerns to address. Most things cycle through the same three phases manufacturing, installation, and operational.



	Manufacturing	Installation/ Commissioning	Operation
Transport Layer		Eavesdropping & Man-in-the-middle	Eavesdropping & Man-in-the-middle
Network Layer			DoS attack Routing attacks
Physical Layer	Device Cloning	Substitution	DoS attack Privacy threat Extraction of security parameters

Figure 2: Threats throughout lifecycle

As seen in Figure 2, there are various attacks that can be carried out during the lifecycle of a thing . The rest of this section discusses these attacks in more detail.

2.1 Manufacturing

With the many applications of IoT, devices tend to be tailored towards very specific tasks. As a result, it is unlikely a network will contain nodes created by the same manufacturer. An attack that could occur during this phase would involve an untrustworthy manufacturer that clones the device. In the best-case scenario, the cloned device is sold for a cheaper price but functions the same as a genuine device. In the worst-case scenario, the software may be changed to implement harmful features such as a backdoor [Garcia13]. As a result, there exists an implicit user trust of vendors and their manufacturers.

2.2 Installation

The commissioning and installation phase for a thing entails providing device identity and secret keys which will be used for communication during the operational phase. An untrustworthy installer may substitute a device for a lower quality one. This attack would save the installer money and can be profitable if the genuine device is resold [Garcia13]. Once again, there exists an implicit user trust of the installers. Other attacks that may occur during the installation stage involve obtaining the secret keys when the installer provides them to the device [Shipley13]. If attackers are successful in obtain the secret keys, then the network communications are compromised.

2.3 Operational

Most of this paper is focused on attacks during the operational phase. These attacks can vary from eavesdropping to active routing attacks to denial-of-service attacks. These attacks can be separated into a few categories, physical capture, disrupt, degrade, deny, or destroy a part of the network, manipulation attacks, and eavesdropping attacks [Covington13]. This paper will return to these attacks and their countermeasures in Section 4.

3. Architecture of IoT

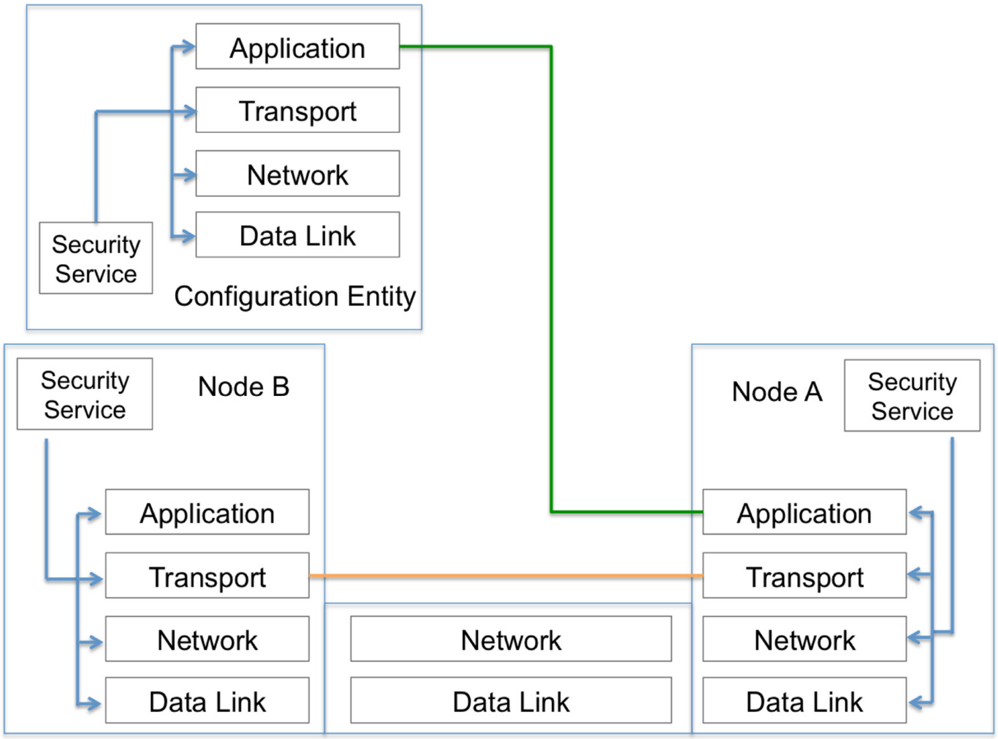


Figure 3: Security Mechanisms Overview

3.1 Centralized

Even though there are a multitude of uses for IoT, Figure 3 shows a general overview of a centralized security mechanism. For the IoT, the most common architectures are completely centralized mainly due to security. For ZigBee, there is a trust center. For 6LoWPAN/CoRE, the 6LoWPAN Border Router is the central entity [IEEE802.15.4k]. A centralized architecture simplifies the task of device and key management but represents a distinct point of failure. Another factor to consider is that for low-power lossy networks, nodes will sometimes sleep, thus complicating authentication and the synchronization of security states [Tsao13].

3.2 Bootstrapping

Bootstrapping refers to the process of securely connecting a thing to the Internet of Things. Currently, there are a few protocols which help authenticate nodes. Protocol for Carrying Authentication for Network Access (PANA) is an UDP-based, network-layer transport for Extensible Authentication Protocol (EAP) [RFC5191]. EAP is a two-party protocol, which generates keying material. An important difference between IoT and the standard Internet protocols is that the Internet protocols assume the identity of a host is always available. The design of IoT and its aspects as a low-power lossy network affects this assumption. After EAP authenticates the node, configuration parameters are sent via Internet Key Exchange version 2 (IKEv2), Host Identity Protocol (HIP), Transport Layer Security (TLS), or Datagram Transport Layer Security (DTLS) [Tsao13]. As privacy becomes a bigger issue, these protocols built in privacy protection. TLS and DTLS allow the option of only authenticating the responding host. This feature prevents eavesdroppers from discovering the initiating host's identity [RFC5246]. HIP and IKEv2 have public-key identities, which are used to authenticate the initiating host [RFC5282]. Both of these protocols encrypt the packets sent. Diet-HIP, which is based off of HIP but aims to reduce the computation and energy usage involved in encryption, does not provide a similar privacy feature due to computational limits.

4. Attacks and Countermeasures

To examine the security threats and possible attacks, this paper will survey security at the physical and network layers. The IoT has to protect against attacks from the following categories: authentication, access control, confidentiality, integrity, and availability.

Authentication involves the mutual verification of routing peers before they share route information and ensures shared data origin is accurate. In the IoT, authentication has to be strong and highly automated. Access control is the prevention of unauthorized node use, i.e. making sure nodes are not compromised. Confidentiality is the protection of information, especially when shared over a publicly accessible medium such as air for wireless. Integrity involves the protection of data and confirms no unauthorized modifications occur. Availability, which is specific to IoT, ensures that information is available when required [Tsao13]. When examining these threats, this paper is specifically examining LLNs, which face energy and connectivity constraints.

4.1 Physical Layer

Commonly, the Internet of Things networks are centralized with many remote nodes. Many of these nodes are in distant locations and may not have adequate protection from being captured. Attackers can seize and extract security information, keys, etc. from the device. They may even re-program the device for their own needs. If a group key is used throughout the network, this sort of attack can compromise the entire network. If unique keys are used, this attack is not as damaging [Garcia13]. Networks can also experience denial-of-service attacks at a physical layer if the attacker uses jamming or interference equipment. This sort of attack aims to disrupt communications and can be hard to detect.

4.2 Network Layer

The routing protocols used in the network layer of IoT are similar to the network layer of standard Internet; however, the network layer of IoT is specified towards low-power and lossy networks.

Failure to Authenticate Attacks: Node impersonation occurs when an attack gains access to a network as a legitimate node. It would be able to carry attacks, which involve reporting false data or readings, provide bad control messages, or control/affect the traffic flow of the network. A dummy node is when the attack pretends to be a legitimate node. Many times, it can carry out the same attacks as an impersonated node [Tsao13].

Node resource spam occurs when an attacker continuously joins a network to drain the resources of the network. The attacker would aim to fill up storage memory and potentially take down a portion of the network [Tsao13].

Confidentiality Attacks: At the network layer, confidentiality attacks aim to expose routing information or routing exchange data. A deliberate exposure attack happens when a routing entity allows the information to be exposed to an outside entity either due to misconfiguration or by an attack. To prevent against this exposure attack, all communicating nodes should be authenticated. The communication between nodes should also be peer-to-peer, which ensures that neither node is sending information without knowledge of both peers [Tsao13]. This does not thoroughly prevent an attack, but requires a compromised node to take more action to expose routing information.

Passive wiretapping attacks listen in on information being sent between nodes. By analyzing traffic, the attacker can learn about the network. These attacks can be countered by encrypting all data used for routing. It is mandatory to implement Advanced Encryption Standard (AES)-128 in Counter with CBC-MAC (CCM) mode for low-power lossy networks [RFC6550]. CCM combines the counter mode for encryption and the cipher block chaining message authentication code technique for authentication. For example, ZigBee specifies use of CCM, PANA, and EAP-TLS for management of keys. It is believed CCM is secure against almost all brute force attacks [Tsao13]. Some deployments including ZigBee do not specify a network layer encryption but use similar security for the data link layer. These networks are immune to passive wiretapping, but they are more vulnerable to attacks through compromised nodes [Tsao13].

Attackers can also learn information by analyzing traffic flow through a network. This attack relies on the fact that data link layer and network layer routing information has to remain unencrypted. By analyzing source and destination addresses, attackers can map the network and flow patterns [Garcia13]. Allowing multi-path routing counters this attack, however, many low-power lossy networks do not allow for multi-path. Another way to counter this attack is through encapsulation which hides information about the transmission. This is done automatically for data link layer security that uses encryption.

Integrity Attacks: Unauthorized modification attacks are when attackers change information in a message or in stored data. This attack can be easily countered by adding access controls for storage and by implementing data integrity services for messages.

Overclaiming and misclaiming attacks aim to change the topology and routing data by creating false routes. This attack can be countered by determining bad routes by reviewing old data and by designing the network with restricted realizable network topologies.

Identity attacks, also known as spoofing, happen when an attacker tries to gain access to a device by masquerading as someone else. Sybil attacks are when the attacker has multiple of these identities. The attacker can create false routing information and disrupt normal routing operations [Garcia13]. These attacks can be countered by using either a public key based authentication for the network layer, or use data link layer security with authentication controls like PANA.

Routing information replay attacks occur when the attacker records messages sent over the network and replays them to the network in an effort to disrupt operations. The IETF routing over low-power lossy networks (ROLL) is designed to counter this sort of attack. Older messages will be ignored and multiple versions of the message would not affect normal operations [RFC6550].

Byzantine routing information attacks are when a node is compromised by an attacker but still contains a valid identity and security credentials. This attack is hard to defend against and address. Authentication cannot completely counter this attack. Distance vector protocols like the IETF ROLL do not provide much protection for this attack and would require a separate implementation to analyze and validate routing information to counter it [Tsao13].

Availability Attacks: Selective forwarding attacks affecting routing paths and aim to disrupt communications. As seen in Figure 4, a compromised node within the network may choose to randomly filter packets causing confusion within the network. If the node drops all the packets it receives, it is called a black hole attack [Garcia13]. This attack can be countered by having either multipath routing of the same message over disjoint paths, or having each node randomly select the next hop from a set of potential hops. The multipath method requires more energy, thus not used for low-power lossy networks.

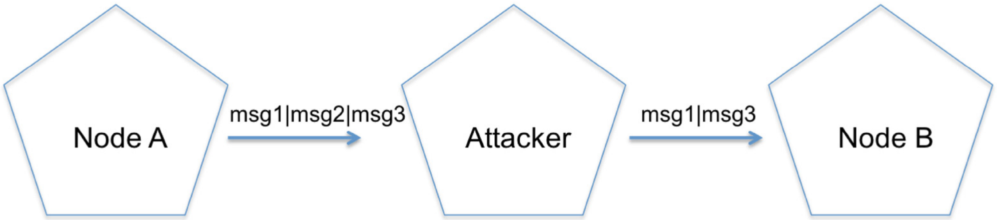


Figure 4: Selective Forwarding Attack

Wormhole attacks are when two malicious/compromised nodes advertise having a very short path between them. A pure wormhole attack is impossible to detect but does not affect the data/traffic. In the worst case, a pure wormhole would force the network to recalculate routes. Wormholes used with other attacks such as selective forwarding can disrupt network communications [Tsao13].

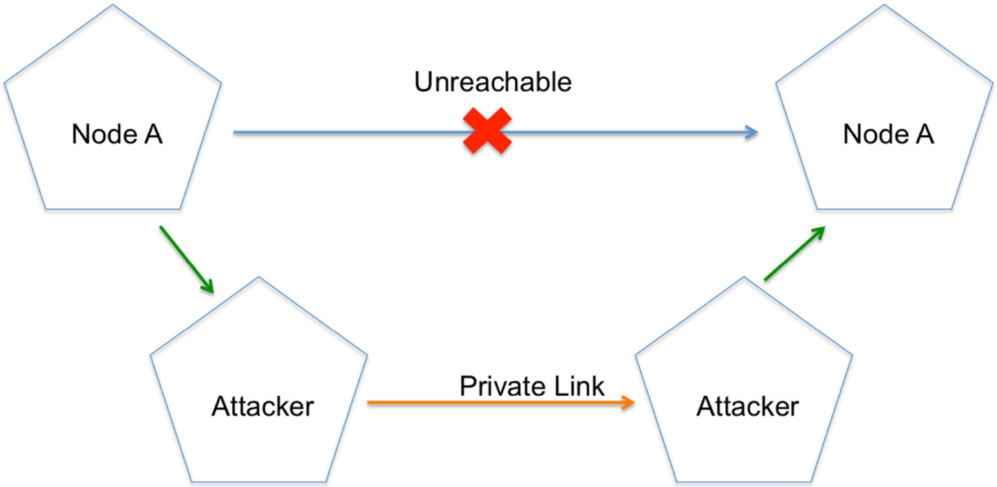


Figure 5: Wormhole Attack

Sinkhole attacks use a compromised node to advertise good links to attract traffic. This attack can only be done with an inside node [Garcia13]. If sinkholes are coupled with selective forwarding, a portion of the network may be disabled. These attacks are generally harder to detect. Sinkholes can be countered by adding a similar threshold for receiving traffic. Otherwise, this attack can also be countered by picking the next hop from a group of candidates.

Overload attacks are another type of denial-of-service attack where a malicious node fills the network with random traffic. It aims to deplete the energy resources of the network and take down the network by overburdening it. These attacks can be countered by adding limits on the traffic rate for each node or by isolating nodes, which are sending excessive amounts of traffic [Tsao13].

HELLO Flood and ACK spoofing attacks are different ways of achieving the same result by leading nodes to believe routes exist when they do not. The optimal way to counter this attack is through bidirectionality, where the controller consistently validates connectivity at the data link layer.

5. Privacy and Regulation

As more companies and manufacturers aim to sell the Internet of Things, the Federal Trade Commission (FTC) is looking for ways to ensure consumer protection and to regulate the industry. The IoT changes the traditional business landscape.

5.1 Privacy Concerns

A major difference between traditional Internet and the IoT is the amount of data being collected about the user. Data is collected universally in the IoT and this data can be used to build an invasive profile of the consumer. The FTC recognized three major privacy concerns: facilitation of the collection of large amounts of consumer data, using that data in ways unexpected by the consumer, and security of data [FTC13]. This ubiquitous data collection makes the Internet of Things a much more data driven economy. With massive quantities of continuous data, new discoveries can be made, but little to no regulation can by harmful to the consumers. Privacy issues are especially hard to discuss because, by nature, privacy is subjective [Covert14]. The FTC aims to promote three best practices:privacy by design, simplifed consumer choice, transparency. Companies have to make an effort to build consumer protection in from the beginning [FTC13].

5.2 Regulations and Policy

With such an asymmetry of power between businesses and their consumers, the FTC is looking for ways to protect users against abuse of their data. The IoT, a data-driven ecosystem, requires a trust between the business and consumer that exists even now. A user shares data with a business and in return receives a service. The FTC is seeking to push businesses and companies towards built-in security and designing security into new devices. For the IoT, the data is usually passively and ubiquitously collected. As a result, the FTC believes businesses will have to earn user trust and at a data level, which means involving the user. A similar problem exists in the energy industry. A Green Button was created in order to standardize energy usage information, allow the consumers to download the information, and enlighten the users how their data is being used [FTC13]. Empowering and educating the consumer would help facilitate the integration of the IoT into our everyday lives.

5.3 Violations and Criticisms

There have been many critics and skeptics regarding security and regulation in the Internet of Things. In 2013, the FTC sued a company called TRENDnet Inc. that produces wireless webcams. The FTC believed that TRENDnet did not provide enough security for end-users. In the end, over 700 webcams were compromised and even some geographical information was compromised [Dimov13]. Despite these actions, many skeptics believe the FTC will not be able to regulate privacy in the IoT. One reason is because of the large variety and quantity of manufacturers. Regulation for each manufacturer, which builds very specific devices, is inconceivable. Other critics and experts believe software patching and updating will not be feasible for many applications of the IoT [Schneier14]. At the same time, with such growth in the industry, the FTC is slow and ineffective as a deterrent [Clearfield13]. As the IoT develop towards medical fields and vehicular automation, security and privacy can be come physical threats to users.

6. Summary

The ultimate differences between the Internet of Things and the standard Internet is the difference in which the networks are deployed. IoT uses low-power lossy networks, which complicates security issues by adding an additional constrain, energy. Protocols such as ROLL aim to secure lower layers from the described attacks while conserving resources. The Internet of Things is set the change the world in the upcoming decade; however, security, privacy, and policy must keep up to protect the users of these networks.

References

[Tsao13] Tsao, T., Alexander, R. Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL), Dec. 15, 2013. http://tools.ietf.org/pdf/draft-ietf-roll-security-threats-06.pdf

[Garcia13] Garcia-Morchon, O., Kumar, S. Security Considerations in the IP-based Internet of Things , Sept. 11., 2013. http://tools.ietf.org/html/draft-garcia-core-security-06

[FTC13] Cerf, Vint, and Maureen Ohlhausen. "Internet of Things." Lecture. Federal Trade Commission: Internet of Things Workshop. Federal Trade Commission, Washington DC. 19 Nov. 2013. FTC.gov. http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf

[Covington13] Covington, M. J., and R. Carskadden. "Threat Implications of the Internet of Things." 5th International Conference on Cyber Conflict (2013): 1-12. IEEE.

[Schneier14] Schneier, Bruce. "The Internet of Things Is Wildly Insecure" And Often Unpatchable." Wired.com. Conde Nast Digital, 04 Jan. 2014. http://www.wired.com/opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[Gartner13] Rivera, Janessa, and Rob Van Der Meulen. Gartner's 2013 Hype Cycle for Emerging Technologies Maps Out Evolving Relationship Between Humans and Machines. Gartner, 19 Aug. 2013. http://www.gartner.com/newsroom/id/2575515

[Covert14] Covert, Ed, and Angela Orebaugh. "Ethical Challenges of the Internet of Things." SC Magazine 29 Jan. 2014. Web. http://www.scmagazine.com/ethical-challenges-of-the-internet-of-things/article/331460/1/

[Dimov13] Dimov, Daniel. "Privacy Implications of the Internet of Things." InfoSec Institute, 14 Nov. 2013. Web. http://resources.infosecinstitute.com/privacy-implications-internet-things/

[Clearfield13] Clearfield, Chris. "Why The FTC Can't Regulate The Internet Of Things." Forbes. Forbes Magazine, 18 Sept. 2013. Web. http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/

[Shipley13] Shipley, AJ. "Security in the Internet of Things." Wind River, Sept. 2013. Web. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[RFC5191] Forsberg, D., Ohba, Y., Ed., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008. http://tools.ietf.org/html/rfc5191

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008. http://tools.ietf.org/html/rfc5246

[RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, August 2008. http://tools.ietf.org/html/rfc5282

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012. http://tools.ietf.org/html/rfc6550

[RFC3268] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002. http://tools.ietf.org/html/rfc3268

[IEEE802.15.4k] IEEE Std., 802.15.4k-2013, ISBN 0-7381-8446-3, August 2013.

List of Terms

IoT - Internet of Things
FTC - Federal Trade Commission
LLN - Low-power lossy networks
PANA - Protocol for Carrying Authentication for Network Access
EAP - Extensible Authentication Protocol
IKEv2 - Internet Key Exchange version 2
HIP - Host Identity Protocol
TLS - Transport Layer Security
DTLS - Datagram Transport Layer Security
ROLL - Routing over low-power lossy networks

AES - Advanced Encrytion Standard
CCM - Counter with CBC-MAC
DoS - Denial-of-Service

Last Modified: April 30, 2014
This and other papers on current issues in Wireless and Mobile Networking are available online at
http://www.cse.wustl.edu/~jain/cse574-14/index.html
Back to Raj Jain's Home Page