

Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)

Sachin Babar*, Parikshit Mahalle, Antonietta Stango, Neeli Prasad,
and Ramjee Prasad

Center for TeleInfrastruktur, Aalborg University, Aalborg, Denmark
{sdb,pnm,as,np,prasad}@es.aau.dk
<http://www.gisfi.org/>

Abstract. IoT is an intelligent collaboration of tiny sensors and devices giving new challenges to security and privacy in end to end communication of things. Protection of data and privacy of things is one of the key challenges in the IoT. Lack of security measures will result in decreased adoption among users and therefore is one of the driving factors in the success of the IoT. This paper gives an overview, analysis and taxonomy of security and privacy challenges in IoT. Finally, Security Model for IoT has been proposed.

Keywords: Security, Privacy, Internet of Things, trust, authentication, authorization.

1 Introduction

The Internet has undergone severe changes since its first launch in the late 1960s as an outcome of the ARPANET with number of users about 20% of the world population. “7 trillion wireless devices serving 7 billion people in 2017”. This vision reflects the increasing trend of introducing micro devices and tools in future i.e. IoT. In such ambient environment not only user become ubiquitous but also devices and their context become transparent and ubiquitous. With the miniaturization of devices, increase of computational power, and reduction of energy consumption, this trend will continue towards IoT[1]. One of the most challenging topics in such an interconnected world of miniaturized systems and sensors are security and privacy aspects. Having every ‘thing’ connected to the global future IoT communicating with each other, new security and privacy problems arise, e. g., confidentiality, authenticity, and integrity of data sensed and exchanged by ‘things’.

This paper is structured as follows : Section 2 talks about the IoT objectives with detailed description of each. Section 3 focuses on the security requirements in terms of privacy, trust and authentication for IoT. Section 4 describes the possible threats to IoT. Section 5 analyzes related work for IoT security. Section 6 proposes a security model for IoT. Section 7 concludes the paper.

* Corresponding author.

2 IoT Objectives

The IoT scenarios, like individual wireless device interfacing with internet, constellation of wireless devices, pervasive system and sensor network, are associated with new network service requirements that motivate rethinking of several Internet architecture issues. Several mobile/wireless features may require mechanisms that cannot be implemented through the conventional IP framework for the Internet, or if they can, may suffer from performance degradation due to the additional overhead associated with network protocols that were originally designed for static infrastructure computing. We discuss a set of objectives related to the networking requirements of the representative IoT scenarios identified earlier. Fig. 1 shows the IoT Objectives followed by their description.

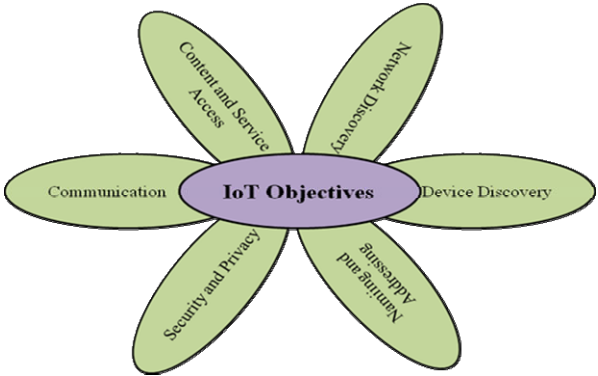


Fig. 1. IoT Objectives

2.1 Naming and Addressing

Today's Internet addressing scheme is rather rigid; it is well suited to a static, hierarchical topology structure. It provides a very efficient way to label (and find) each device interface in this hierarchy. To support mobility and routing the next generation Internet must provide ways to name and route to a much richer set of network elements than just attachment points. A clean architectural separation between name and routable address is a critical requirement [2].

2.2 Device Discovery and Network Discovery

The current Internet is text-dominated with relatively efficient search engines for discovering textual resources with manual configuration. An Internet dominated by unstructured information supplied from large numbers of sensor devices must support efficient mechanisms for discovering available sensor resources. The new architecture must support methods for the registering of a new sensor system in the broader network [3].

2.3 Content and Service Access

A new architecture should provide data cleansing mechanisms that prevent corrupted data from propagating through the sensor network. In particular, services that maintain

device calibration and monitor/detect adversarial manipulation of sensor devices should be integrated into sensor networks. This could be realized through obtaining context information, metadata, and statistical techniques to locally detect faulty inputs.

2.4 Communication

Wireless devices should be able to operate independently of the broader Internet. In particular, there may be times during which the connection of a wireless device or network to the Internet is not available. During these times, wireless devices should be able to operate stably in modes disconnected from the rest of the infrastructure, as well as be able to opportunistically establish "local" ad-hoc networks using their own native protocols. In particular, this means that issues such as authorization and updating the device state should be seamless, with minimal latency.

2.5 Security and Privacy

Wireless networks can be expected to be the platform of choice for launching a variety of attacks targeting the new Internet. At the most basic level, wireless devices will likely have evolving naming and addressing schemes and it will be necessary to ensure that the names and addresses that are used are verifiable and authenticated. One parameter uniquely associated with wireless networks is the notion of location. Location information provided by the network should be trustworthy [4]. Additionally the architecture should provision hooks for future extensions to accommodate legal regulations.

3 Security Requirements

3.1 Key Properties of IoT

There are a number of key properties of IoT that create several issues for security and raises additional requirements for security. These key properties are listed below:

Mobility. IoT devices are mobile and often generally connect to the Internet via a large set of providers.

Wireless. These devices typically connect to the rest of the Internet via a wide range of wireless links, including Bluetooth, 802.11, WiMAX, Zigbee and GSM/UMTS. With wireless communications, any nearby observer can intercept unique low-level identifiers that are sent in the clear, e.g., Bluetooth and 802.11 device addresses.

Embedded Use. Major IoT devices have a single use (e.g., blood pressure or heart monitors and household appliances). As a result, the detection of communication patterns unique to a specialized device allows users to be profiled[5].

Diversity. These devices span a range of computational abilities from full-fledged PCs to low-end RFID tags. Privacy designs must accommodate even the simplest of devices.

Scale. These devices are convenient, growing in number daily, and increasingly embedded network connectivity into everyday settings. This makes it difficult for users to monitor privacy concerns.

3.2 Challenges

Following are the challenges which need to be tackled in the world of pervasive devices.

- Management, scalability and heterogeneity of devices
- Networked knowledge and context
- Privacy, security and trust will have to be adapted to both devices and information

This will involve the development of highly efficient cryptographic algorithms and protocols that provide basic security properties such as confidentiality, integrity, and authenticity, as well as secure implementations for the various kinds of mostly resource constrained devices.

3.3 High Level Security Requirements

In business process, security requirements are described as follows :

Resilience to attacks. The system has to avoid single points of failure and should adjust itself to node failures.

Data authentication. As a principle, retrieved address and object information must be authenticated.

Access control. Information providers must be able to implement access control on the data provided.

Client privacy. Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

Fig. 2 summarizes the high level security requirements for IoT.

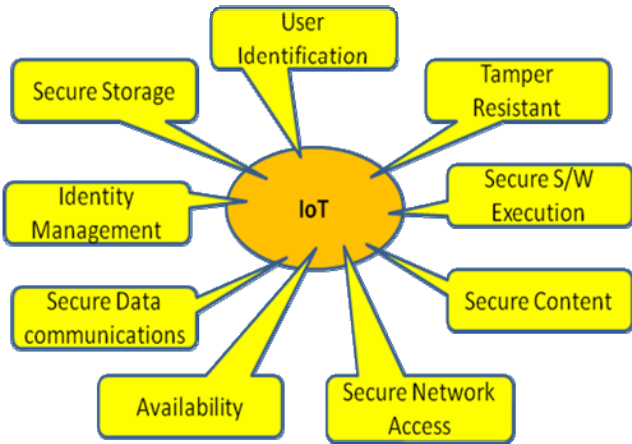


Fig. 2. High level Security Requirements for IoT

User identification. It refers to the process of validating users before allowing them to use the system.

Secure storage. This involves confidentiality and integrity of sensitive information stored in the system.

Identity Management. It is broad administrative area that deals with identifying individuals / things in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Secure data communication. It includes authenticating communicating peers, ensuring confidentiality and integrity of communicated data, preventing repudiation of a communication transaction, and protecting the identity of communicating entities.

Availability. Availability refers to ensuring that unauthorized persons or systems cannot deny access or use to authorize users.

Secure network access. This provides a network connection or service access only if the device is authorized.

Secure content. Content security or Digital Rights Management (DRM) protects the rights of the digital content used in the system.

Secure execution environment. It refers to a secure, managed-code, runtime environment designed to protect against deviant applications.

Tamper resistance. It refers to the desire to maintain these security requirements even when the device falls into the hands of malicious parties, and can be physically or logically probed.

4 Security and Threat Taxonomy for IoT

IoT is coupled with new security threats and alters overall information security risk profile. Although the implementation of technological solutions may respond to IoT threats and vulnerabilities, IoT security is primarily a management issue. Effective management of the threats associated with IoT requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. Following Fig. 3 presents threat taxonomy to understand and assess the various threats associated with the use of IoT [6].

Identification covers determination of unique device/user/session with authentication, authorization, accounting and provisioning.

Communication threats covers a Denial-of-Service attack (DoS) and it occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands.

Physical threat includes micro probing and reverse engineering causing serious security problem by directly tampering the hardware components. Some types of Physical attack requires expensive material because of which they are relatively hard to perform. Some examples are: De-packaging of chip, Layout reconstruction, Micro-probing.

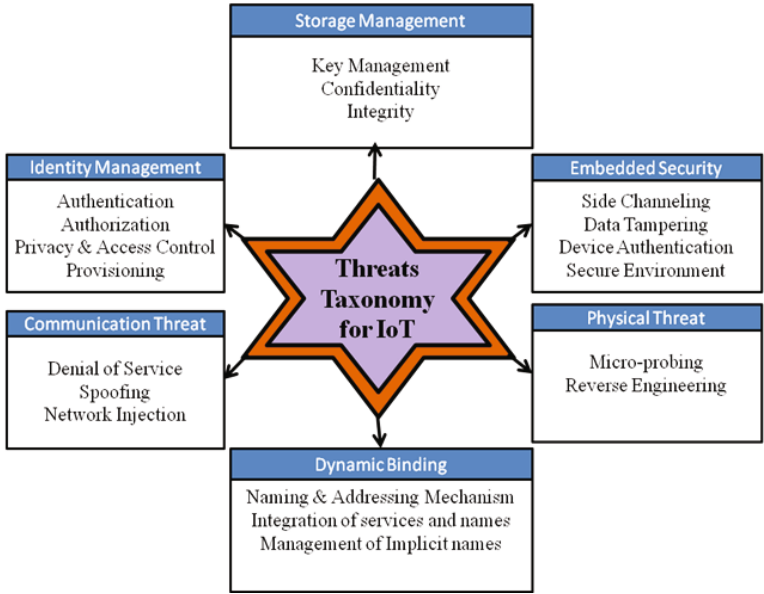


Fig. 3. Threats Taxonomy for IoT

Embedded Security threat model will span all the threats at physical and MAC layer. Security threats like device and data tampering, Side channel analysis, bus monitoring, etc will be the concerns at device level.

Storage management has crucial impact on the key management to achieve confidentiality and integrity. We must also be careful in choosing which cryptographic components to use as the building blocks since, for example, the cipher texts for some public key encryption schemes can reveal identifying information about the intended recipient .

5 Related Work

Security framework for IoT will mainly include architectures for providing and managing access control, authentication and authorization. It will provide methods for controlling the identification and authentication of users and for administering which authenticated users are granted access to protected resources. Some of the frameworks described can be used to provide several functions as shown in Table 1.

5.1 Identity Certificate Frameworks

These frameworks allow users without prior contact to authenticate to each other and digitally sign and encrypt messages. They are based on identity certificates, which are certificates that bind a public key to an identity. Examples of identity certificate frameworks include Public Key Infrastructures (PKIs), [8,14] and Pretty Good Privacy (PGP).

Table 1. State of Art Evaluation

Sr. No.	Framework	Identity Certificate Management	Single Sign-on	Federated Identity	User-centric	Device Security
1	PKI[7]	√				
2	PGP[8]	√				
3	Kerberos[9]		√			
4	Windows Live ID[10]		√		√	
5	OpenID[11]		√		√	
6	Liberty Alliance[12]		√	√	√	
7	WS-Federation[13]		√	√		

5.2 Single Sign-On

Single sign-on (SSO) allows users to be authenticated only once in a system. Users can then access all resources for which they have access permission without entering multiple passwords. Example SSO frameworks include:

Kerberos a distributed authentication service, which provides SSO within a single administrative domain.

Windows Live ID [10]: an Internet-based SSO framework used by Microsoft applications and web services such as MSN messenger.

OpenID [11]: an authentication framework that allows users to login to different web sites using a single digital identity, eliminating the need to have different usernames and passwords for each site.

Liberty Alliance [12]: a consortium that aims to establish open standards, guidelines and best practices for federated identity management.

WS-Federation [13]: a federated identity standard developed by Microsoft, IBM, VeriSign, BEA and RSA Security, which forms part of the Web Services Security framework.

5.3 Identity Federation

Federated Identity allows users of one security domain to securely access resources on another security domain, without the need for another user account. Users register with an authentication server in their own domain and other domains trust its assertions.

5.4 User-Centric Identity Management

User-centric identity management is a design principle that focuses on usability and cost-effectiveness from the user’s point of view. There are three main approaches to

user-centric identity management that are Managing multiple identities e.g. information cards [15], Giving users a single identity e.g. OpenID and lastly Giving users control over access to their resources.

5.5 Device Security

The Device Security Framework includes device-resident security software as well as security capabilities delivered across the network. The device-resident software is embedded into devices at the time of manufacture.

6 Proposed Security Model for IoT

Integrated and interrelated perspective on security, trust, privacy can potentially deliver an input to address protection issues in the IoT. Therefore we have chosen a cube structure as a modeling mechanism for security, trust and privacy in the IoT, referred to as IoT. A cube has three dimensions with the ability to clearly show the intersection thereof. Therefore a cube is an ideal modeling structure for depicting the convergence of security, trust and privacy for the IoT. In IoT access information, required to grant/reject access requests, is not only complex but also composite in nature. This is a direct result of the high level of interconnectedness between things, services and people. It is clear that the type and structure of information required to grant/reject such an access request is complex and should address the following IoT issues: security (authorization), trust(reputation), privacy(respondent). This is depicted in figure 4.

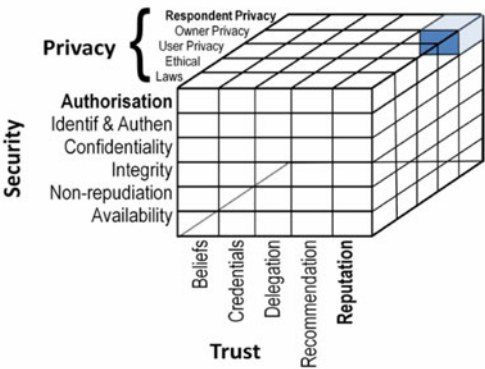


Fig. 4. Security Model for IoT

7 Conclusion

The incremental deployment of the technologies that will make up the IoT must not fail what the Internet has failed to do: provide adequate security and privacy mechanisms from the start. We must be sure that adequate security and privacy is available

before the technology gets deployed and becomes part of our daily live. Security requirement and threat taxonomy insist to go for Trusted Platform Module which offers facilities for the secure generation of cryptographic keys, and limitation of their use, in addition to a hardware pseudo-random number generator. It also includes capabilities such as remote attestation and sealed storage. "Remote attestation" creates a nearly unforgeable hash key summary of the hardware and software configuration. The extent of the summary of the software is decided by the program encrypting the data. This allows a third party to verify that the software has not been changed. "Binding" encrypts data using the TPM endorsement key, a unique RSA key burned into the chip during its production, or another trusted key descended from it.

In this paper we presented a categorization of topics and technologies in the IoT with analysis of sensitivity and state in research to different security and privacy properties. We see this (1) as a basis for coming up with an integrated systems approach for security and privacy in the Internet of Things, and (2) as stimulator for discussion on the categorization and sensitivity rating in the IoT. Furthermore, we presented key challenges like identity management, embedded security and authentication in the IoT.

References

1. Silverajan, B., Harju, J.: Developing network software and communications protocols towards the internet of things. In: Proceedings of the Fourth International ICST Conference on Communication System Software and MiddlewaRE, COMSWARE 2009, Dublin, Ireland, June 16-19, pp. 1-8. ACM, New York (2009)
2. Adjie-Winoto, W., Schwartz, E., Balakrishnan, H., Lilley, J.: The design and implementation of an intentional naming system. In: Proceedings of the Seventeenth ACM Symposium on Operating Systems Principles, SOSP 1999, Charleston, South Carolina, US, December 12-15, pp. 186-201. ACM, New York (1999)
3. Beerliova, Z., Eberhard, F., Erlebach, T., Hall, A., Hoffmann, M., Mihalák, M., Ram, L.S.: Network Discovery and Verification. *IEEE Journal on Selected Areas in Communications* 24(12), 2168-2181 (2006)
4. Hu, Y.-C., Wang, H.J.: Location Privacy in Wireless Networks. In: Proceedings of the ACM SIGCOMM Asia Workshop (2005)
5. Kocher, P., Lee, R., McGraw, G., Raghunathan, A.: Security as a new dimension in embedded system design. In: Proceedings of the 41st Annual Design Automation Conference, DAC 2004, San Diego, CA, USA, June 7-11, pp. 753-760. ACM, New York (2004)
6. Welch, D., Lathrop, S.: Wireless security threat taxonomy. In: Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, June 18-20, pp. 76-83 (2003)
7. Public-Key Infrastructure (X.509), <http://tools.ietf.org/wg/pkix/>
8. Kohnfelder, L.M.: Towards a Practical Public Key System, Thesis (1978), <http://dspace.mit.edu/bitstream/handle/1721.1/15993/07113748.pdf>
9. Neuman, B.C., Ts'o, T.: Kerberos: an authentication service for computer networks. *IEEE Communications Magazine* 32(9), 33-38 (1994)
10. Introduction to Windows Live ID, download, <http://msdn.microsoft.com/enus/library/bb288408.aspx/>

11. OpenID, http://openid.net/specs/openid-authentication-1_1.html
12. Introduction to the Liberty Alliance Identity Architecture (2003),
<http://xml.coverpages.org/LibertyAllianceArchitecture200303.pdf>
13. Goodner, M.: Understanding WS-Federation (2007),
<http://msdn.microsoft.com/en-us/library/bb498017.aspx>
14. Shim, S.S.Y., Bhalla, P.: Federated identity management. *IEEE Computer* 38(12), 120–122 (2005)
15. Chappell, D.: Introducing Windows CardSpace,
<http://msdn.microsoft.com/en-us/library/aa480189.aspx>