Security in Internet of Things

YUANJUN SONG

Master of Science Thesis
Stockholm, Sweden 2013

TRITA-ICT-EX-2013:196
Security in Internet of Things

Author:
Yuanjun Song
871129-0612
Yuanjuns@kth.se

Organization and Supervisor:
China Telecom
Ling Zhang

Academic Advisor/Examiner:
Fredrik Kilander/Louise Yngström

Starting Date: Dec 14, 2013
Ending Date: May 31, 2013
The Internet of Things (IoT) is emerging the Internet and other networks with wireless technologies to make physical objects interact online. The IoT has developed to become a promising technology and receives significant research attention in recent years because of the development of wireless communications and micro-electronics.

Like other immature technological inventions, although IoT will promise their users a better life in the near future, it is a security risk, especially today the privacy is increasingly concerned by people. The key technologies of IoT are not yet mature. Therefore the researches and applications of the IoT are in the early stage. In order to make the IoT pervade people’s everyday life, the security of the IoT must be strengthened.

In this thesis, first, the IoT is compared with the Internet. Though the IoT is based on the Internet, due to the characteristics of the IoT, those mature end-to-end security protocols and protective measures in the Internet can not directly provide the end-to-end data security through the perceptual layer, the transport layer the and application layer.

For the IoT security addressing issues (such as the Internet DNS attack), this thesis proposes the IoT addressing security model. The traditional access control and the identity authentication only works in the same layer. The IoT addressing security model designed in this thesis effectively solves the issues of vertically passing the authentication results in the addressing process without changing the protocols for two communication parties. Besides, this thesis provides the object access control and privacy protection from the object application layer addressing, DNS addressing and IP addressing phases.

Finally, combining the IoT object addressing security model with practical application scenario, this thesis designs the IoT object security access model. In this model, the access requester can access objects in different domains through a single sign-on. This model provides the protection for the end-to-end communication between the access requester and object.

**Keywords**

Internet of Things, IoT, security, addressing model, access model.
Contents

1. Introduction ..................................................................................................................1
   1.1 Background .............................................................................................................1
   1.2 Problem ..................................................................................................................3
   1.3 Goals ......................................................................................................................7
   1.4 Outline ....................................................................................................................7

2. Security Architecture of IoT ...................................................................................8
   2.1 Security Architecture Categories of IoT .................................................................8
      2.1.1 Off-line IoT architecture ................................................................................9
      2.1.2 On-line IoT architecture ..............................................................................10

3. IoT Addressing Security ......................................................................................12
   3.1 Security Issues of IoT Addressing ........................................................................12
   3.2 IoT Addressing Security Model ...........................................................................13
      3.2.1 Object Addressing Process ........................................................................13
      3.2.2 Object Name Service ....................................................................................14
      3.2.3 Object Addressing Basic Model ....................................................................14
      3.2.4 Object Addressing Improved Model .............................................................15
      3.2.5 Object Addressing Security Model ...............................................................17
      3.2.6 Addressing Model Security Analysis ..........................................................19

4. IoT Object Access Security ..................................................................................20
   4.1 Security Access Model .........................................................................................20
      4.1.1 Object Security Access Model ....................................................................21
      4.1.2 Access Model Security Analysis ................................................................26

5. Conclusions ............................................................................................................27

References ..................................................................................................................28
Figure

Figure 1-1 technology roadmap: the Internet of Things [5]................................................................. 2
Figure 1-2 Three Layers of IoT Architecture [6].................................................................................. 3
Figure 2-1 Off-line IoT architecture ..................................................................................................... 9
Figure 3-1 the IoT addressing process [15] ....................................................................................... 13
Figure 3-2 ONS layer architecture ....................................................................................................... 14
Figure 3-3 the IoT object addressing basic model .............................................................................. 14
Figure 3-4 the IoT object addressing improved model ....................................................................... 15
Figure 3-5 the IoT object addressing security model .......................................................................... 18
Figure 4-1 the application architecture in multiple domains ............................................................... 20
Figure 4-2 the object access ticket apply model .................................................................................. 21
Figure 4-3 Intra-domain access model ............................................................................................... 22
Figure 4-4 Intra-domain access model ............................................................................................... 22
Figure 4-5 Cross-domain access model .............................................................................................. 24
Figure 4-6 Cross-domain access model .............................................................................................. 25

Table

Table 2-1 the comparison between the ordinary devices and the smart devices................................. 8
Table 2-2 the name resource comparison between the direct connection and the platform ............ 11
1. Introduction

1.1 Background

With the continuous development of information and communication technology, the complex applications of computers, Internet, Wireless Sensor Network (WSN), radio frequency identification devices (RFID) and global positioning system (GPS) get into the life of the general public. In recent years, the market share of the smartphone has been increased rapidly. There is a huge technological change undergoing in the information communication. The form of information communication transforms from exchanging information between people to exchanging information between people and things, and eventually between things at any time, any place.

The “ITU Internet Report 2005: Internet of Things (IoT)” [1] was released by the International Telecommunication Union (ITU) in 2005. The concept of IoT was formally proposed. Then the IoT era begun. With the rapid development of a variety of networks and intelligent computing technology in recent years, the ITU issued "ubiquitous sensor network (USN)" research report in February 2008. It proposed that the sensor network was developing to the ubiquitous sensor network which is a network that consists of smart sensor nodes and can be deployed in the form of "any place, any time, any person, any object". [2] Now a variety of objects with embedded sensor, processor, wireless communication module or equipment connect to each other to constitute the IoT. Thus, the IoT has two characteristics: first, the IoT is an extension of a network based on the Internet. It integrates the Internet, mobile communication networks and sensor networks; second, the clients of IoT extend to any things so that they are able to exchange of information directly. [3]

Initially, the studies on the technology of reading information from things focused on the wireless sensor field, which read and collect related information from surrounding things in very close range. The sensors digitalize the physical states of things, such as temperature, location, etc. so that the data of the physical states can be conveniently collected and transmitted. In addition, the technologies of information collection, processing and analysis are mature enough to manage massive IoT information by the centralized information systems, such as remote cross-domain real-time inquiry, configuration and management. The IoT has become a promising technology and received significant research attention in recent years due to the development of wireless communications and micro-electronics. The WSN is the core part of the IoT. Many people believe that the importance of WSN is comparable with the Internet: The Internet enables a computer to access a variety of digital information, regardless of where it stores, while the WSN will be able to extend the ability to enable the real world remotely interact by cheap node sensor units. [3]

In the IoT, the "things" should have a certain degree ability of processing reacting to the changes in ambient. On one hand, in order to make a corresponding perception of the surrounding physical environment, the things detect the environment and digitalize the results to collect. On the other hand, the things can react with the variations in ambient through the interior information processing unit or through the external system by exchanging data and receiving the corresponding control signal. In most scenarios, the
things themselves have very limited processing capacity, and often fail to complete complex information processing. Thus, the data is usually analysed and processed by external systems.

In the early stage, the concept of the IoT is equivalent to the RFID technology plus the Internet. In 1990s, sales and logistics were considered the largest and most promising applications of IoT. The IoT technology was used to automatically identify the goods and share the information via the Internet. At present, most of the applications of the IoT are still just the extension of the data collection applications, not yet the intelligent, real dialogue between things and things. [4]

SRI Consulting Business Intelligence (SRIC-BI) analysed and pointed out that IoT would be developed into the integration of software and advanced sensor. Showed in Figure 1-1, this process can be divided into four phases: in the first phase (Supply-Chain Helpers), based on RFID technology, it accelerates sorting and checking items to improve logistics speed and reduce losses; in the second phase (Vertical-Market Applications), it establishes the industry applications to reduce operating costs, such as monitoring, security, healthcare, transportation and other vertical applications; in the third phase (Ubiquitous Positioning), it locates people and everyday objects indoor and outdoor; in the fourth phase (Physical World web), it remotely controls and senses distant objects by means of miniaturization, low power consumption.[5]

![Figure 1-1 technology roadmap: the Internet of Things](image)

The potential applications of IoT can be summarized as: military, aviation, counter-terrorism, explosion, disaster relief, environment, health care, household, commercial, logistics, warehousing, transportation, industrial production, identity, power and other fields. Security is a vital consideration in all information and communication systems in these fields.
The IoT is usually divided into three layers: perceptual layer, transport layer and application layer. [2][3][6] The details are showed in Figure 1-2.

![Figure 1-2 Three Layers of IoT Architecture](image)

RFID is an indispensable technology in the perceptual layer of the IoT structure. RFID in China has been large-scale applied, such as highway ETC toll system, bus cards, the second generation ID cards, college student ticket deals tags offered by the Ministry of Education and the Ministry of Railways. As can be seen, the main function of the RFID applications which well-known by the public is reading the electronic tag data, while the management control function is relatively less used. Internet Protocol version 6 (IPv6) is the next generation IP designed by Internet Engineering Task Force (IETF). IPv6 address capacity is about $2^{128}$, which is about $8 \times 10^{28}$ times the current address capacity of IPv4. In theory, it is enough to assign a unique IP address for "every grain of sand on the Earth". Thus the IP is also an important technology in transport layer of IoT.

### 1.2 Problem

Like other technological inventions, although IoT will promise their users a better life in the near future, it is a security risk. Especially today, the privacy is increasingly concerned by the public. In order to make the IoT pervade people's everyday life, the security of the IoT must be strengthened. The security of the IoT is crucial to the development of IoT industry. The IoT is an immature technology. The key issue that affects the development of IoT is lacking of mature and complete security model and standards. Compared to the traditional network, IoT integrates WSN, RFID systems, mobile vehicle network, 3G technology, WiMAX, personal area network, etc. As the IoT environment becomes more complex, the security issues are more complex than any
existing network systems. Although the IoT has good prospects and of great significance, the premise is whether the applications of IoT can be applied on a large scale. The challenges to this premise include at least the following three aspects: [7]

1) Cost: The devices of WSN should be available at relatively low prices to support their large-scale deployment. This requirement determines that these devices are resource-constrained. It means that these devices may have a small amount of memory, computational capability and limited power supply. The existing network security protocols do not consider about these restriction factors.

2) Security: Compared to traditional networks, the IoT merges more networks which perplex the security issues.

3) Privacy: The devices of WSN may not be able to defend all forms (physical and cyber) of attacks. The sensitive information or location privacy may be leaked.

Figure 1-3 Security problems of IoT’s all layers are facing [6]
Figure 1-3 shows the risks and threats faced by three layers of IoT. The main challenges to the Perceptual Layer are physical damage to the nodes, channel blocking, forgery attacks, fake attacks, copy attacks, replay attacks, information tampering and so on. While the Transport Layer are mostly challenged by DOS/DDOS attacks, counterfeiting/middleman attacks, heterogeneous network attacks, application risks of IPv6, conflicts of WLAN application, traditional network security threats and so on. As for the Application Layer, the information disclosure, illegal human intervention, unstable platform, and authentication are the main challenges. [6]

Since the IoT merged the traditional Internet, wireless communication networks, WSN and other network, the existing Internet security technologies can provide some security for the IoT, such as the deployment of the user authentication, access control and security audits in the application layer and VPN, firewall and other security policies in the network layer. However, the existing security architecture and security technology cannot cover all the security issues of all three layers of the IoT. Thus, the security architecture of IoT neither can simply copy the traditional Internet security architecture, nor completely redesign new security architectures. In order to distinguish which security issues that need to new solutions including deciding which security issues that can be solved by the existing technologies, some researches divide the IoT security issues into three categories. [8] Figure 1-4 shows the three categories of IoT security issues.

1) Internet’s own security issues

These security issues originally exist in the traditional Internet environment as well as in the IoT environment. They still can be solved by continuing using the traditional security architecture of the Internet.

For example: data eavesdropping, tampering, forgery, denial of service attacks, man-in-the-middle attacks and other common Internet attacks.

2) Internet security issues under the scene of IoT

These security issues are already solved by some security technologies in the Internet environment. However given to the special scene of IoT, they form some new security issues. These security issues cannot be simply solved by continuing using the security technology for the traditional Internet. The characteristics of IoT need to be taken into consideration. Thus, appropriately modifying the security architectures of the Internet or designing a new security architecture can solve these security issues.
For example: DNS does not authenticate the requester. In IoT environment it will cause leaking object privacy.

3) IoT’s own security issues

These security issues are caused by the new network structure, scene, terminal equipment and other factors of IoT. They cannot be solved with traditional Internet security architectures, therefore, new security architectures and security protocols need to be designed.

For example: authentication protocols, key agreement and privacy protection of WSN devices.

The key to strengthen the security of the IoT is to design new solutions to the security issues of category 2) and 3). From preliminary source information gathered by China Telecom, the security issues of category 2) tend to happen in the processes of the IoT object addressing and access. The security issues of category 3) occur mainly in the WSN part. The security architectures which may solve the IoT object addressing and access, and the WSN security (RFID mainly) are two major research aspects of the IoT security. [8]

At present the nodes of the WSN are multi-source and heterogeneous. The sensor nodes usually only have simple hardware and software functions, which fail to have complex security protection. The research of security issues of these simple devices is one major aspect of research of security issues of IoT. RFID security mechanisms can be divided into physical security mechanisms and cryptographic security mechanisms. The physical security mechanisms include: kill command mechanism, electrostatic shielding mechanism, active interference and blocking tags. [9] These mechanisms will increase the cost of hardware and are very difficult to be unified. The cryptographic security mechanisms include: Hash-Lock protocol proposed by Sarma [10], Random Hash-Lock protocol proposed by Weis [11], Hash-Chain agreement proposed by the NTT laboratories [12], the NTT laboratories Distributed RFID-challenge-response protocol proposed by Rhee [13], Elliptic Curve Digital Signature Algorithm (ECDSA) proposed by Scott Vanstone [14].

Compared to the WSN research, the studies of IoT security architectures are relatively few. Due to the multi-network integration features of IoT and the limited storage and computational capability of the terminal devices, it is difficult to implement the access control model of traditional Internet in the IoT. The traditional Internet security technology such as PKI and CA will increase the cost of in IoT. Geng comprehensively analyzed the security issues of IoT, and introduced some key technologies, such as user authentication, access control [3]. Mi proposed SOA-based security architecture of IoT [4]. Dong discusses an architecture about protecting the privacy information of IoT [7]. However, these researches only proposed the idea of the design, while the detail models and protocols were missing.

In the scenes of the IoT, whether the names of the object exist are trade secrets. However, the DNS, one of the infrastructures of the traditional Internet, cannot authenticate the requester in such a scene. In IoT environment, it is still risky to use only proceeding identity authentication and data encryption on the access layer. The process of addressing in IoT is based on the process in the Internet. Therefore, on one hand, the security issues of
The process of Internet addressing will be introduced to the IoT; on the other hand, the results of IoT objects addressing become the conditions of next step of addressing. This means that the Internet security addressing model cannot protect the confidentiality and integrity of the results of addressing in IoT. The relevant researches in the IoT addressing are the Electronic Product Code (EPC) and the Ubiquitous ID Center (uID Center). Both of them use the existing DNS infrastructure which cannot protect the privacy of the identities and only support single code system. [15]

The problem of this thesis can be summarized as:

The problem tackled by this thesis is to design a new IoT security access architecture to protect the object access security and solve the IoT addressing issues. The design should protect the object privacy and support multiple code system.

1.3 Goals

This thesis aims to design a security IoT application platform architecture. It consists mainly of the security addressing model and access control model.

First, this thesis will design a security addressing model of IoT to protect privacy information of object.

Second, this thesis will design a new IoT object access security model to protect the communication between the access requester and the object.

The criteria of the designs are as follow:

1) Resilience to attacks
2) Authentication
3) Access control
4) Privacy protection
5) Low cost

The goal is achieved when the above requirements are met in the designs. The outcome of this thesis will protect the confidentiality, integrity and privacy in the process of the IoT object addressing and access at a relative low cost.

1.4 Outline

The structure of this thesis is as follows. Chapter 2 starts by categorizing and analyzing the architecture of the IoT. Chapter 3 analyzes the IoT addressing process and designs a new IoT object addressing security model to protect the privacy information in the IoT addressing process. Chapter 4 provides a new IoT object access security model combined with the IoT object addressing security model proposed in Chapter 3. It analyzes the security of the new access model in the end. Chapter 5 draws the conclusion of the thesis and describes future work.
2. Security Architecture of IoT

2.1 Security Architecture Categories of IoT

At present, there are no unified standards of definition and classification of the things in the IoT. In this thesis the things will be divided into ordinary devices and smart devices. Table 2-1 shows the comparison between the ordinary devices and the smart devices.

The ordinary devices should be able to perceive the surroundings and have a certain degree of digital signal processing power and basic interaction capability such as reading and writing the data of the perception, but limited to specific data receiving devices.

The smart devices are based on ordinary devices, but have a certain programmable computing power, a certain degree of expansion of storage capacity and network access capability. It is possible that the smart devices communicate with others smart devices.

<table>
<thead>
<tr>
<th></th>
<th>Ordinary devices</th>
<th>Smart device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing capacity</td>
<td>Weak</td>
<td>Strong</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>Small</td>
<td>Support external storage</td>
</tr>
<tr>
<td>Network access capability</td>
<td>limited to specific devices</td>
<td>Wired or wireless</td>
</tr>
<tr>
<td>End to end communication</td>
<td>Nonsupport</td>
<td>Support</td>
</tr>
<tr>
<td>Devices expansibility</td>
<td>Nonsupport</td>
<td>Support</td>
</tr>
<tr>
<td>Authentication</td>
<td>Between ordinary devices and specific data receiving devices</td>
<td>Smart devices internal or third party</td>
</tr>
</tbody>
</table>

Table 2-1 the comparison between the ordinary devices and the smart devices

This thesis will divide the IoT security architecture into two types, the off-line architecture and the on-line architecture. The off-line architecture is used in the IoT application which is mainly composed of ordinary devices. The on-line architecture is applied to the IoT application which is mainly composed of smart devices. According to the characteristics of the two categories, this thesis will design different solutions for them.
2.1.1 Off-line IoT architecture

Figure 2-1 shows that in the off-line IoT architecture, the objects (perception devices) only communicate and exchange data with information receiving devices. The authentication and key agreement in offline architecture are divided into two parts: one is the authentication and key agreement between the objects and the receiving devices; the other is between the access requesters and the management information systems. The data perceived by object centralizes in the management information system by the information receiving devices. Access requesters only interact with management information systems to manage, analyze and apply the perception data. EPCglobal is a typical off-line architecture application.

In terms of the access requesters, there are no large differences in the behavioral patterns between the IoT and traditional Internet applications. So the traditional security technology can continue to be applied, such as password-based authentication, certificate-based authentication and other common authentication, role-based access control model as well.

As for the objects, the authentication and data communication security between them and the receiving device will, on the one hand, affect the accuracy of the data analysis in subsequent IoT applications; on the other hand, raising new requirements about protection of privacy.
2.1.2 On-line IoT architecture

Figure 2-2 shows that in the on-line IoT architecture, the objects can establish end-to-end communication links to access requesters via the Internet or IoT gateway. The on-line architecture can be divided into direct connection and platform two sub architectures.

In the direct connection IoT applications, access requesters and objects use the network to directly connect. The objects independently complete the access requester authentication, access control and other security protections.

In the platform IoT applications, access requesters and objects belong to different security domains: access requesters are in the public domain, and the objects in the application domain. The data communication between the two sides is proceeding through the application domain gateway. The access requesters and the objects do not establish direct network connections. The application domain gateway can complete the access requester authentication and access control in different layers.

Since the platform IoT architecture applications establish the end-to-end communication links between objects and access requesters, the implementation process requires a lot of available object name. Besides, in order to facilitate the research of object addressing security in later chapters, the object scale and object name resource of two types IoT architecture applications are compared.
<table>
<thead>
<tr>
<th>Object scale</th>
<th>Object name resource</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object name</strong></td>
<td><strong>Domain name</strong></td>
</tr>
<tr>
<td>Direct connection</td>
<td>One or several</td>
</tr>
<tr>
<td>Platform</td>
<td>Large scale</td>
</tr>
</tbody>
</table>

Table 2-2 shows the name resource comparison between the direct connection and the platform. These two types represent the intra-domain and cross-domain scenarios. The later chapters will discuss them respectively.
3. IoT Addressing Security

3.1 Security Issues of IoT Addressing

The IoT addressing is based on the Internet addressing. On one hand, the Internet addressing security issues will be introduced to the IoT addressing process; On the other hand, the results of the IoT object addressing will be the parameters in next step. The question whether the object names exist or not in the IoT may be the trade secrets which needs to be protected. In the process of IoT addressing, the access requester needs to be authenticated in every phase of addressing. To ensure that the authentication process is transparent to the access requesters in all layers, the authentication results transmit vertically in the process of layer-by-layer or cross-layer addressing. The DNS, as one of the important infrastructures of the IoT and the Internet, achieves the conversion between domain names and IP addresses. However, the DNS transmits data in clear text in its work process. The DNS protocol neither provides confidentiality and integrity protection, nor has the necessary requester authentication to control some domain resolutions. The IETF proposes DNSSEC protocol aiming at a series of security problems under DNS. However, it still does not have the requester authentication [15]. In addition to the DNS, the IP address in the IoT environment also has special requirements in privacy protection. At the same time, the confidentiality and integrity of addressing results must be protected to avoid the attacker eavesdropping, tampering and forging.

The typical DNS attacks are Denial of Service attack, Cache Poisoning attack, ID Guessing and Query Prediction attack, Untrusted Recursion attack and Denial of Existence of attack. When the access requesters request the Object Name Service (ONS), the DNS may be attacked by: [16]

Denial of service attacks and Denial of existence attack: The access requesters cannot get the real IP address of the ONS. Thus the access requesters cannot establish communication to get the query results.

Cache Poisoning attack, ID Guessing and Query Prediction attack and Untrusted Recursion attack: The access requesters get false IP address. The access requesters may fail to access the ONS, or be deceived to fake ONS.

Notably, even when the ONS returns the correct results of some object addressing (domain name or URL) to the access requester, the attacks to the DNS still will have impact. Such as forging the existence object and deceiving the access requesters to access it.

Although the DNSSEC effectively prevents the Cache poisoning attacks, ID Guessing and Query Prediction attack and Denial of Existence of attack and ensures that the domain name of the object is consistent with the IP, subject to the characteristics of the protocol, the DNSSEC cannot authenticate the access requesters.

In the IoT, the identification of “thing” is certain business property. A serial number segment in a coding system may represent a particular type of products in a company. So the essence of addressing according to object identification is a special case of inquiring about a number of attribute information. If there is no control measure being taken, then the
objects of a certain serial number segment will be polled. The statistics of the number of the returning results can estimate the product amount. However, these values may result in the disclosure of commercial secrets in practice.

When a requester directly queries the object name or serial number, if the ONS failed to identify and authenticate the requester, the “denial of existence” results will return to the access requester. In the Internet it is a DNS “denial of existence” attack, but it is an effective “access control” in the IoT.

Therefore, the IoT ONS needs to authenticate the query requester. At the same time, authorize and authenticate of the scope and results of the query items.

In the scene of the Internet, most authentications are completed within the systems. With the development of application systems, cross-domain, cross-application access has increased dramatically. In recent years, new authentication and identification protocol are also proposed. Similarly, the authorization, storage, authentication of identity information and access control in the IoT also have cross-domain and cross-application requirements.

3.2 IoT Addressing Security Model

3.2.1 Object Addressing Process

Every object in the IoT system has a unique code identification which can be derived from the different coding systems. Before the access requesters communicate with the objects, they need to address the object to locate the actual position in the network. The IoT addressing process is shown in Figure 3-1:

![Figure 3-1 the IoT addressing process](image)

In phase one, the access requester requests the Domain or Uniform Resource Locator (URL) in the Internet from the IoT ONS by the object identity.

In phase two, the access requester requests the IP address of the object from the DNS by the object domain name.

In phase three, the access requester establishes the communication connection by the object IP address. In the communication link, there may be physical gateway and other network equipment. So the IP address may transform.
3.2.2 Object Name Service

![Figure 3-2 ONS layer architecture][1]  

As shown in Figure 3-2, the ONS structure is similar to the DNS. Each object coding system has its ONS. The ONS is a tree structure, i.e. each object encoding system always contains certain layers encoding subsystems [15].

After the access requester sends a request to the ONS, the ONS selects the coding system which the object belongs to and sends the request to the corresponding ONS of the actual coding system. Eventually the address of the object is returned to the access requester. Due to the structure of ONS, the communication between all levels relies on the Internet facilities.

3.2.3 Object Addressing Basic Model

Figure 3-3 shows the object addressing basic model which is abstracted from the description of the IoT object addressing process in 3.2.1.

![Figure 3-3 the IoT object addressing basic model][2]
Step 1: the access requester sends a request to the ONS in public domain.

Step 2: the ONS in public domain finds the corresponding URL of the object name and returns the result.

Step 3: the access requester gets the object domain from the object URL.

Step 4: the access requester sends the object domain to the DNS to get the corresponding object IP address.

Step 5-8: the access requester establishes the end-to-end communication connection through the object IP address. The IP address may transform.

From the Internet application point of view, the Phase one of the IoT addressing basic model can be considered as the “URL addressing”; the Phase two can be considered as “DNS addressing”. For the protection of addressing results, the Phase one can be solved in application layer, but the Phase two cannot have an effective access control (for example, the attacker directly gets the object corresponding domain name from other source, bypass the Phase one) since the DNS is in the public domain. Meanwhile, the DNS protocol cannot authenticate the requester.

3.2.4 Object Addressing Improved Model

According to the above security issues, the object addressing model is improved by adding the ONS and DNS in the application domain to the object addressing basic model. In this improved model, showed in Figure 3-4, in order to support the different forms of authentication and access control in the three phase addressing, the ONS, DNS and objects all have an authentication and access control module defined in the abstract.

![Figure 3-4 the IoT object addressing improved model](image)
Step 1: the access requester sends a request to the ONS in public domain.

Step 2: the ONS in public domain sends the request to the corresponding ONS in application domain. The authentication and access control module authenticates the access requester. If the requester does not have the addressing authority, the request will be rejected directly.

Step 3: the ONS in application domain finds the corresponding URL of the object name and returns the result to the ONS in public domain.

Step 4: the ONS in public domain returns the corresponding URL of the object name.

Step 5: the access requester gets the object domain from the object URL.

Step 6: the DNS in public domain sends the request to the corresponding DNS in application domain. The authentication and access control module authenticates the authority of access requester. However, the identification information of access requester cannot be obtained directly because the DNS protocol does not contain the identification information of the access requester.

Step 7: the DNS in application domain returns the object IP address to the DNS in application domain.

Step 8: the DNS in public domain returns the object IP address.

Step 9-12: the access requester establishes the end-to-end communication connection through the object IP address. The IP address may transform.

In the phase one of the improved model, the access requester can be authenticated easily. However, this model still has some security issues:

- If the domain name of the object stays unchanged for a long time, the privacy of whether the object exists may disclosed.
- If the domain name of the object is randomized, the object domain name needs to be generated in the phase one. This will affect the normal use of the security protocol (e.g., SSL).
- If the IP address corresponding to the object is randomized, it will consume large amounts of IP address resources.
- Even the DNSSEC cannot directly authenticate the access requester.

The result of the phase one -- object domain name is provided by the ONS in the application domain. So it is possible to keep the traditional protocol and make a security design on the returned domain name to authenticate the requester in the phase two.

If the phase three uses IPsec transport mode for end-to-end communication and the object IP address is randomized, the object IP address configuration will be very complex; If the phase three uses IPsec tunnel mode, the communication between the access requestor and the object will use the VPN. It will face malicious access or attacks from the illegal visitors in the VPN. Therefore, the object privacy issues still exist.
3.2.5 Object Addressing Security Model

The object addressing security model assumes that there is no attack from the various components (name services, and state that any delivery service) in the addressing process.

- Object addressing request

  The request message of addressing in the model contains the access requester identification and object unique identification. The structure of the request should meet the following requirements:
  
  1. contain the identification of the access requestor.
  2. be able to authenticate the message source - to prove that the message comes from the legitimate access requester.
  3. contain the object identification. The object identification transmits in cipher text to prevent eavesdropping.
  4. can be detected by the receiver whether the request has been tampered.
  5. have a certain degree of randomness (fresh, one-off factor)

- Object addressing result

  The result of addressing in the model is not only the response to the requester, but also one of the parameter for the next step addressing. The structure of the result should meet the following requirements:
  
  1. contain the object identification. The object identification transmits in cipher text to prevent eavesdropping.
  2. be able to authenticate the message source - to prove that the message comes from the legitimate name service.
  3. can be detected by the receiver whether the result has been tampered.
  4. contain the shared key for the communication in the next addressing phase.

- Access requester authentication

  The access requester authentication is the first step of the IoT security addressing. In the security addressing model, it is assumed that the name service is trusted. Then the access requester authentication process accomplishes:
  
  1. authenticate the access requester by Name Service.
  2. generate the session key between the access requester and Name Service in application domain.
  3. transmit the addressing result encrypted with the session key.

  The entity-level authentication protocols have the symmetric key based authentication, Hash function based authentication, public key based authentication, trusted third party based authentication and password based authentication. Under normal circumstances, an authentication protocol is accompanied by the session key negotiation for the subsequent communication.
Figure 3-5 shows the IoT object addressing security model.

Step 1: the access requester sends a request to the ONS in public domain. The communication between the access requester and the ONS is encrypted with the shared session key.

Step 2: the ONS in public domain sends the request to the corresponding ONS in application domain. The communication between the ONS in public domain and the ONS in application domain is encrypted with the shared session key.

Step 3: the ONS in application domain authenticates the access requester and the object.

Step 4-5: the State Transfer Service (STS) stores parts of the addressing result.

Step 6: the ONS in application domain generates the addressing result with signature and encryption, returns the result to the ONS in public domain.

Step 7: the ONS in public domain returns the result to the access requester.

Step 8-14: the access requester uses the result of the phase n addressing to continue the phase n+1 addressing. The process of phase n+1 is similar to phase n.
3.2.6 Addressing Model Security Analysis

Since this model has assumed that there will be no internal attacks (modifying or forging the addressing conditions and results) from the name services in all levels in the addressing process, and the ONS and STS use the symmetric key to encrypt the message, the model may only be attacked from the outside of the model. For example, denial of service attacks, privacy guessing attacks and replay attacks.

- Denial of service attacks

Denial of service attack means that the attacker either sends the request to the service in a short period of time to cause program abnormalities by using the vulnerability of the service or directly sends large number of requests to the service to make the service busy dealing with the abnormal requests but refusing the normal requests.

In this model, the access control service is an effective means of protecting the ONS in applications domain against the denial of service attacks from the public domain. The methods of access control in each phase of addressing are different.

- Privacy guessing attacks

Privacy guessing attack means the attacker attempts to detect the existence of the object which may have privacy protection requirements by sending the forged object addressing requests to the name service.

In this model, the object name transmits in cipher text in the public domain. The attacker first needs to get the key and object identification to construct the object addressing requests. However, in the public domain, the shared key and object identification are only known by the communicating parties. So the attacker cannot directly forge object addressing requests.

- Addressing replay attacks

Addressing replay attacks means that the attacker eavesdrops the object addressing request sent by the access requester to the ONS, attempting to obtain the result of addressing by replaying the same data to the ONS.

In this model, firstly, the object name transmits in cipher text in the public domain, and secondly, the object name in cipher text contains a one-off factor. After the legitimate access requester sending the request to the ONS, the one-off factor has failed. So the same object request data will be refused by the access control. Therefore, the attacker cannot get the addressing results by the replay attacks.

In addition, the attacker may eavesdrop the ONS addressing results and send it to the ONS in next phase before the legitimate access requester sends the result to the ONS in next phase. Due to lacking the shared key between the access requester and ONS in the next phase, the attacker cannot forge new object addressing requester to get the addressing result in the next phase.
4. IoT Object Access Security

4.1 Security Access Model

With the increase in the number of the IoT applications, the IoT will become more complex. The different IoT applications should take the different security architectures to improve application security. In the IoT application, the "things" will gradually replace the “people”, who are the main users of applications in the Internet era, to become the main users in the IoT applications.

The IoT mainly composed of "things" (i.e. smart device) in the networks. The numerous smart devices and the access requesters are distributed in different application domains. Under normal circumstances, the storage and computing capability of these smart devices are limited. Thus they need to be managed through effective platforms.

Shown in Figure 4-1, both “people” and “things” have access requirements to the other “things” in the same application domain or in different application domains.

![Figure 4-1 the application architecture in multiple domains](image)

In the object addressing security model proposed in the chapter 3, the addressing results of the phase one are the object domain names. However, these domain names have randomness. On the other hand, the Internet application layer security protocol SSL/TLS applications need the support of the Public Key Infrastructure (PKI). The SSL/TLS protocol at least in three aspects authenticates the certificate security: verifies the consistency of the issued domain and the actual domain, then verifies the certificate and the authenticity by using the CA root certificate. Thus, randomly generating the object URL in the dynamic domain method will make the SSL/TLS protocol difficult to use.
4.1.1 Object Security Access Model

This thesis designs a new object security access model to meet the data access requirements in different trust domains and simplifies authentication in different domains. The protocol needs to protect the integrity, confidentiality and availability, and to be able to resist the man-in-the-middle attacks and replay attacks from outside the systems.

In this model, each application domain must have a unique Ticket Service (TS). Its main function is issuing the object access ticket for the access requester. The object access ticket contains ticket unique identification, access requester identification, access requester authentication type, ticket issuer identification (TS identification), the start time, the end time, the ticket main signature, the ticket subordinate signature and other attributes. Figure 4-2 shows the object access ticket apply model.

The main function of object access ticket is identifying the access requester. The identity of the requestor remains unchanged in a short period of time. Therefore, the period of validity of the ticket can be relatively long.

In this model, each application domain must have a unique object gateway (G) which generates the random factor every time the access requester accesses the object. The G can authenticate the object access ticket. For the cross-domain object access ticket, the G asks the TS in local domain to authenticate and update the object access ticket. The G also performs the functions of name service and IP gateway which was described in Chapter 3.

- Ticket apply model

![Figure 4-2 the object access ticket apply model](image)

Step 1: the access requester sends the requester identification and the secret to the TS. The secret is the basis of the identity authentication.

Step 2: the TS sends the requester identification and the secret to the Authentication Service (AS).

Step 3: the AS returns the authentication result to the TS.
Step 4: the TS according to the authentication type and result generates the object access ticket and signs in the main signature.

Step 5: the TS returns the object access ticket to the access requester.

- Intra-domain access model

Figure 4-3 Intra-domain access model

Figure 4-4 Intra-domain access model
Figure 4-3, and 4-4 show the Intra-domain access model.

Step 1: the access requester sends the requester identification and the secret to the TS.
Step 2: the TS returns the object access ticket to the access requester.
Step 3: the access requester according to the period of validity of the ticket, caches in the appropriate range of time.
Step 4: the access requester sends the object identification, the object access ticket and key agreement message to the G. The G verifies the signatures in the object access ticket and authenticates the access authority of the access requester. If the object access ticket has expired or has been canceled, or the requester does not have the authority to access the object, the G directly returns a rejection message.
Step 5: the G generates a random factor (R) for this access and sends the R and the key agreement message to the object.
Step 6-7: the object according the key agreement message and the R generates the key agreement message and returns to the G.
Step 8: the G returns the key agreement message, the R, the object access ticket and the URL of the object to the access requester.
Step 9: the access requester gets the session key from the key agreement message and uses the session key to encrypt the R and the object access ticket.
Step 10: the access requester sends the encrypted message to the object.
Step 11: the object decrypts the message to get the object access ticket.
Step 12: the object uses the public key of the TS to verify the signature in the object access ticket.
Step 13(optional): the object checks the state of the object access ticket from the TS.
Step 14(optional): the TS returns the state of the object access ticket to the object.
Step 15: the object returns the decision whether the access requester can access or not according to the verification results.
Figure 4-5 and 4-6 show the Cross-domain access model.

Step 1: the access requester sends the requester identification and the secret to the TS (A).

Step 2: the TS (A) returns the object access ticket (A) to the access requester.

Step 3: the access requester according to the period of validity of the object access ticket (A), caches in the appropriate range of time.

Step 4: the access requester sends the object identification, the object access ticket (A) and key agreement message to the G (A).

Step 5: the G (A) verifies the signatures in the object access ticket (A) and authenticates the cross access authority of the access requester. If the object access ticket (A) has expired or has been canceled, or the requester does not have the authority to access the object, the G (A) directly returns a rejection message.

Step 6: the G (A) sends the object identification, the object access ticket (A) and key agreement message to the G (B).

Step 7: the G (B) verifies the signatures in the object access ticket (A).

Step 8: the G (B) sends the object access ticket (A) to the TS (B).
Step 9: the TS (B) verifies the signatures in the object access ticket (A), signs its signature on the object access ticket (A) to generate the object access ticket (B) and returns the object access ticket (B) to the G (B). The G (B) gets the identification of the access requester from the object access ticket (B). If the object access ticket (B) has expired or has been canceled, or the requester does not have the authority to access the object, the G (B) directly returns a rejection message.

Step 10: the G (B) generates a random factor (R) for this access and sends the R and the key agreement message to the object.

Step 11-12: the object according the key agreement message and the R generates the key agreement message and returns to the G (B).

Step 13: the G (B) returns the key agreement message, the R, the object access ticket (B) and the URL of the object to the G (A).

Step 14: the G (A) verifies the signatures in the object access ticket (B) and updates the object access ticket (A) to the object access ticket (B) in the cache.

Step 15: the G (A) returns the key agreement message, the R, the object access ticket (B) and the URL of the object to the access requester.
Step 16: the access requester gets the session key from the key agreement message and uses the session key to encrypt the R and the object access ticket (B).

Step 17: the access requester sends the encrypted message to the object.

Step 18: the object decrypts the message to get the object access ticket (B).

Step 19: the object uses the public key of the TS (B) to verify the signature in the object access ticket (B).

Step 20(optional): the object checks the state of the object access ticket (B) from the TS (B).

Step 21(optional): the TS (B) returns the state of the object access ticket (B) to the object.

Step 22: the object returns the decision whether the access requester can access or not according to the verification results

4.1.2 Access Model Security Analysis

The object access ticket converts the information of access requester, the authentication results and the authentication types to the format of ticket. The integrity, confidentiality of the object access ticket needs to be protected because it is the only carrier of the identification of the access requester in the single sign on process.

In this model, the digital signature of the object access ticket is an effective means of integrity protection. The object access ticket transmits respectively in the following communication links:

- access requester and ticket services
- access requester and objects gateway
- object gateway and ticket service
- local object Gateway and remote objects gateway
- access requester and object

In practical application scenarios, the addresses and domain names of the ticket services and the object gateway are fixed, so the mature security measures (such as the SSL protocol) can be used to protect the security.

In this model, when the access requester initiates a session direct to the object, the object access ticket transmits in the cipher text. The attacker cannot easily gain the content of the object access ticket. If the attacker tampers the cipher text, the access requester will find out. If the attacker uses the eavesdropped cipher text for replay attacks, the object will deny the access from the attacker since the cipher text contains the random factor R. In addition, the object gateway returns the random object URL for every legitimate access requester. When the attacker uses the replay attacks, the object gateway will deny the requester. Even if the attacker gets the IP address of the object in the public domain, in the network layer, the security devices (such as firewalls) will block the attack.

In summary, the object access session gets the anti-replay attack protection in the application layer, URL, DNS and IP network layer.
5. Conclusions

The IoT is still in the early stage of development. The infrastructure, application architecture and security measures have not yet established a standard system for wide range usage.

In this thesis, first, the Internet and IoT are compared. Though the IoT is based on the Internet, due to the characteristics of the IoT, those mature end-to-end security protocols and protective measures (such as SSL/TLS and IPsec) in the Internet can not directly provide the end-to-end data security through the perceptual layer, the transport layer the and application layer.

For the IoT security addressing issues (such as the Internet DNS attack), this thesis proposes the IoT addressing security model. The traditional access control and the identity authentication only works in the same layer. The IoT addressing security model designed in this thesis effectively solves the issues of vertically passing the authentication results in the addressing process without changing the protocols for two communication parties. Besides, this thesis provides the object access control and privacy protection from the object application layer addressing, DNS addressing and IP addressing phases.

Finally, combining the IoT object addressing security model and practical application scenario, this thesis designs the IoT object security access model. In this model, the access requester can access objects in different domains through a single sign-on. This model provides the protection for the end-to-end communication between the access requester and object.

The research of IoT security in this thesis is only part of the security problems faced by the IoT. Meanwhile there is a certain degree of defects.

First, the IoT object addressing security model is based on that the Internet protocols and security measures work properly. The scenario that the security issues of the Internet and the IoT addressing security issues happens at the same time, need to be further analyzed and studied.

Second, this thesis has not studied the session key agreement protocol for the end-to-end communications in the object security access model. In the future, the key agreement protocol needs to be designed fully integrated into the mutual communication end-to-end authentication.

Third, the IoT object security access model proposed in this thesis is still subject to the security communication between the terminal equipment and the access gateway.

In a word, the end-to-end authentication, key negotiation and cross-domain access in the IoT still need in-depth study.
References


