SecIoT: A Security Framework for the Internet of Things

Xin Huang * (Corresponding author), Paul Craig,
Department of Computer Science and Software Engineering,
Xi’an Jiaotong-Liverpool University, Suzhou, China, 215123
Email: {Xin.Huang, P.Craig}@xjtlu.edu.cn
Tel: 86-(0)512-8816 1511

Hangyu Lin,
Department of Computer Science, University of Oxford
Email: linhangyu@gmail.com

Zheng Yan
State Key Lab of Integrated Services Networks, Xidian University, Xi’an, China
Department of Communications and Networking, Aalto University, Espoo, Finland
Email: zyan@xidian.edu.cn; zheng.yan@aalto.fi
Abstract. The 5th generation wireless system (5G) will support Internet of Things (IoT) by increasing the interconnectivity of electronic devices to support a variety of new and promising networked applications such as the home of the future, environmental monitoring networks and infrastructure management systems. The potential benefits of the IoT are as profound as they are diverse. However, the benefits of the IoT come with some significant challenges. Not the least of these is that the increased interconnectivity integral to an IoT network increases its vulnerability to malevolent attacks. There is still no proven methodology for the design of security frameworks with device authentication and access control. This paper attempts to address this problem through the development of a prototype security framework with robust and transparent security protection. This includes an investigation into the security requirements of three different characteristic IoT scenarios (concretely, body IoT, home IoT, and hotel IoT), a design of new authentication mechanisms, and an access control subsystem with fine-grained roles and risk indicators. Our prototype security framework gives us an insight into some of the major difficulties of IoT security as well as providing some feasible solutions.

Keywords: Internet of Things, 5G, security, authentication, access control, risk

1 Introduction
The Internet of Things (IoT) aims to improve our lives by increasing the interconnectivity of an increased variety of embedded computing devices using components of existing Internet infrastructure. This will allow for communications between sensors in home appliances, mobile
phones, cars, laptops, factory machineries, and many other devices that are already capable of network access through existing protocols such as 3G, Wi-Fi, Bluetooth and ZigBee. Practical applications of this new technology are numerous, ranging from environmental monitoring to infrastructure management and home automation. This is the idea of ubiquitous computing where computers appear everywhere and applications run seamlessly between devices to manage everything from efficient energy consumption in factories to our weekly shopping.

The establishment of the next generation mobile networks and wireless systems (5G) looks to make things easier for establishing the IoT across a unified all-IP network layer [5]. Here, 5G SIM cards or 5G communication stacks can be embedded into gateway nodes that are in charge of interoperations between different networks of "things" (or even embedded into every node). These "things" can be accessed using their IP addresses. This is more convenient because it conforms to a large network that is already established.

The problem with having more things interconnected and accessible in a 5G IoT network is that there are more data available with more sensors and more opportunities for malicious attacks where the network can be hijacked or sensitive personal data can be leaked due to inadequate security protection. Therefore, a security framework is needed to help users to control which of their devices can be accessed, who is accessing the devices, and the time at which access occurs, as well as sensing the risk of the above. However, little research has been undertaken into the design of security frameworks without degrading usability.

The work presented in this paper explores how security can be improved in IoT through the implementation of a new security framework, the SecIoT. Throughout the development of this new framework the needs and limitations of end users are given extensive attention. User requirements are investigated from the beginning through to the end of the project. These requirements are refined and revised through an incremental process of usability study and testing. The user-centric design philosophy makes the security framework suitable for IoT applications supported by 5G, which can be used for applications such as body area IoT, home IoT, and hotel IoT where user experience is particularly important.

The SecIoT framework includes secure authentication mechanisms, a flexible role-based access system, and a security risk indicator interface to help users understand and control system security risks. These are evaluated using three case studies looking at personal body networks, home networks and hotel networks. The results help to confirm our initial assumption that secure authentication, fine-grained access control and improved security interfaces are key issues in the further development of a secure and viable IoT application. Contributions of the work can be summarized as follows:
1) An investigation of key security requirements for three IoT applications where human interaction is particularly important. These are: body IoT, home IoT, and hotel IoT. Security requirements relate to device authentication, access control and risk notification.

2) An authentication mechanism for IoT security. Specifically this is a device authentication prototype that employs a multi-channel security protocol in order to associate sensor nodes to a central unit securely.

3) The design for a novel access control protocol with fine-grained flexible access control services based on the results of contribution (1).

4) A security risk indicator that helps users to understand and control security risks using some novel methods for risk visualization.

The paper is organized as follows. In Section 2, we briefly review some work related to IoT security applications. Section 3 studies the security requirements for IoT applications where human interaction is important. Section 4 proposes our SecIoT security framework which aims to specifically address these requirements. Section 5 presents the results of our investigation and sections 6 concludes by discussing how these results can be used by researchers and developers to build more usable and functional secure IoT applications.

2 Background and Related Work

The main advantages of 5G are its capacity [1] and unified all-IP network layer [5]. These allow a 5G network to create dynamic networking constructs consisting of interconnected objects [1-4]. This makes 5G ideal for the IoT, which promises to be one of its principle application areas. An example of an IoT application running on 5G is the remote patient monitoring system running on a future 5G infrastructure described by Oleshchuk and Fensli [6].

A lot of attention has been focused on potential applications of IoT technologies in the 5G era, security and privacy, which are major concerns for users, have received relatively little attention. While a general discussion regarding the security and privacy challenges of IoT can be found in papers by Marias et al. [24] and Ziegeldorf et al. [25], this paper focuses specifically on IoT applications where usability is crucial to satisfactory performance. This gives us an insight that better prepares us to propose general solutions to the problems of IoT security usability.

The security framework we propose can be divided into two parts: authentication protocol and access control. Compared to other comprehensive security frameworks, for example the frameworks in [26, 27], our framework pays particular attention to user requirements including security requirements for IoT applications and user opinions regarding access control models and risk indication methods.
The main advantage of our authentication protocol over other proposed technologies is that secure connections between IoT devices and the central unit can be established without pre-distributed cryptographic keys (This can help users easily change the expired or compromised security tokens). Techniques that rely on pre-distributed keys include Multi-channel secure protocols [10] which were proposed as authentication protocols for IoTs by Huang et.al [8, 9]. The trust management aspect of these techniques is discussed by Yan et. al [7]. Other such authentication protocols are IPsec, RFID tag management protocol, password-based authentication protocol, establishment protocol, and device authentication protocol [28-32].

Another important aspect of IoT security framework is access control [11-14, 33, 34]. In this paper, we combine the access control with a k-anonymity [13] scheme and improve the design using information about users’ opinions related to access control models.

3 IoT and Security Requirements
This section gives a brief overview of security requirements based on three typical IoT scenarios where user interaction is likely to be particularly important for secure functionality and general usability. Here we survey user opinions related to these three scenarios in order to characterize user requirements for the security functionality of IoT applications in general.

3.1 Internet of Things
The Internet of Things (IoT) is a worldwide network of physical objects using the Internet as a communication media. The ‘things’ in the IoT are objects accessible or controllable via the Internet. Many analysts predict that IoTs will create new opportunities in various application domains, and play an important role in future business, information and social processes.

Sensors are one important type of objects in IoTs. Sensors are usually connected as sensor networks for providing better measurement results, because the capability of one single sensor is usually limited. These sensors collaborate with each other in a distributed manner to provide information of its physical surroundings.

A central unit provides centralized services in IoTs. Its primary function is to store, process, and deliver data to users. In addition, users can control objects via this unit. Web servers can work as a central unit in many cases. Moreover, recent advances in cloud-computing have provided more possibilities for the centralized control in IoTs.

3.2 Scenarios
In order to develop our IoT security framework we have based our analysis on three IoT environments where user experience is particularly important. These are a body area IoT, a home IoT and a service industry hotel IoT.
**Body area IoT:** Nowadays, there are over three million pacemakers and 1.7 million Implantable Cardioverter Defibrillators (ICDs) inside people's chests. In 2006, they started becoming wireless. In 2013, a computer hacker called Barnaby Jack claimed that he can hack pacemakers to either shut them down or make them send a high voltage shot to the heart [22]. The US Food and Drug Administration also issued guidance to medical technology manufacturers warning against the security risks in body area devices' systems [23]. Therefore, currently body area devices really need protections. A session key between the device and its coordinator can dramatically improve the security of body area IoTs.

**Home IoT:** Smart homes are becoming very popular in recent years. This includes home automation, intelligent lighting, security services, and many other services. All services require many different types of devices or sensors installed in different places. Security of wireless communications between devices and the coordinator plays an important role in this situation.

**Hotel IoT:** Hotels provide a wireless access service. Thus, guests can access the Internet using this service. Guests' devices, e.g. mobile phones and on-body sensors, can also access the Internet using this service. If an attacker set up a hotspot with the same name as the hotspot provided by the hotel, and if a guest chooses to connect to the fake hotspot, their private information and even bank details (provided for purchasing wireless service) will be known to the attacker.

### 3.3 Security Requirements for the IoT

A number of specialists have highlighted concerns on security in the IoT. While these concerns may not influence early adoption, if real security issues are not resolved and IoT applications develop a reputation for being insecure this is likely to adversely affect long term adoption and prevent the technology from becoming established. It is therefore important to understand security risks to the IoT and user attitudes to security so as to make security and functionality compatible in real-world IoT applications. It is important to know when users can accept reduced levels of security, or are willing to put more effort into making their applications secure, in order to strike the right balance in the design of the interface. This is particularly important for IoT applications where key functionality, such as connecting nodes and adding users, requires user interaction and has the potential to make an application sensitive to attacks. A user-study involving questionnaires and scenarios is known as an effective method to gauge user attitudes for the development of emerging technologies, and should work well to investigate attitudes to security in an IoT.

Our study includes 30 adult participants who mainly from London and Oxford. About half of them were UK university students and staff, and the other half were from many other professions. They were balanced in gender and also separated into age groups.
Before the survey, we presented each user eleven statements related to security awareness (e.g. “I update PC/Mobile software regularly”) asking them to note if they agreed with the statement or not. The number of positive answers was totaled for each user and they were divided into groups accordingly. As the result, we grouped the survey participants into three groups based on their security concerns. Group A participants had prior experiences on security systems and showed serious concerns on security. Group B participants showed medium concerns on security. The participants in Group C showed low concerns on security.

Candidates were asked to fill out a questionnaire asking their opinion regarding different aspects of security related to the three different IoT environments, body area IoT, home IoT and hotel IoT, outlined in section 3.2. The survey related to three different dimensions of security, these were:

a) **Authenticity and confidentiality.** The system or information can only be accessed by the legal user.

b) **Integrity.** Related information is not tampered.

c) **Availability.** The service is available at expected time.

Figure 1 illustrates the opinions of our three groups according to the level of security concerns on different functions in the three IoT scenarios. We observed that access systems and payment systems are both ranked as being important for all three groups; however, a personal schedule system drew the most attention for group A participants. This was also the case for health information, personal location, hotel room service, hotel electronics, and hotel alarm.

There were four common categories of systems discussed in both home and hotel IoTs: access control systems, alarm systems, environment sensors systems, and electronic device control systems. Two additional systems (digital room service systems and hotel payment systems) were considered in the hotel IoT. Security for both access control systems and hotel payment systems were considered important for all three groups of candidates. Alarm systems gained a considerable degree of concern in both home and hotel IoTs. Environment sensor systems attract the least attention for all our groups.

There were five categories of information studied for body area IoTs: personal location, health information (e.g., blood pressure), information that includes personal photos or videos, real-time emotional information, and personal schedule information. Personal location, health information, personal photos/videos and personal schedule information were considered the most important information to protect.

In order to get more detailed information regarding the type of protection needed for each IoT scenario we asked our participants to qualify each system component according to the
requirements of service availability, authenticity and integrity. The participants where asked to agree or disagree with the following statements for each system component:

a) **Authenticity.** Only paired devices should be able to access the service.

b) **Message Integrity and Authenticity.** Only legal users should be able to modify the data in storage or during transmission.

c) **Service availability.** The service should always be available.

Results of this evaluation are shown in Figures 2-4. As we can see, users do feel that security is important. In particular, we find that people care more about authenticity, message integrity and message authenticity in the body area IoT. In the home IoT and the hotel IoT, authenticity is important for door/window access control systems and digital payment systems. Message Integrity and message authenticity are important for door/window access control systems, alarm systems in home IoT, room service, and digital payment systems. Moreover, service availability is important in alarm systems and digital payment systems. In summary, security is widely considered as an important aspect of IoT. Especially, authentication and access control, which are the foundation of authenticity, message integrity and message authenticity, are very important.

To supplement these results and provide a picture of how people consider security requirements for a wider range of IoT applications we investigated two further applications where user experience is somewhat less important. These were a logistics IoT and an Office IoT. In our logistics IoT sensor and GPS can be used for monitoring cargo transportations. Customers and managers can monitor cargo locations and transport conditions (this is important for perishable cargo such as fresh food or plants) and RFID can be used to provide traceability without human participation. Our office IoT was described as somewhat similar to a home IoT but with more less recreational and more professional applications.

In Figure 5, shows how our sample considered the security of different aspects of these IoT scenarios. For the logistics IoT, we found that security requirements regarding location and weight/temperature sensors warrant significantly more concern than those in a home or hotel. For an office environment alarm systems raised more concern than these in home or hotel. Indeed, many of the aspects of these systems raised similar levels of concern as different aspects of the more user experience critical systems.

In summary, we find that security protections are generally required in IoTs. In addition, for certain functions or system components, security requirements are different; however, we can claim that mechanisms for authenticity, message integrity and authenticity, and service availability are required in most cases.
Figure 1. Percentage of security concern of three participant groups. “high” refers to the group A; “medium” refers to the group B; and “low” refers to the group C. The x-axle refers to the percentage of participants who think that security protection is important.
Figure 2. Security requirements in the body area IoT. The x-axis refers to the percentage of participants who think that certain type of protection is important.

Figure 3. Security requirements in the home IoT. The x-axis refers to the percentage of participants who think that certain type of protection is important.
Figure 4. Security requirements in the hotel IoT. The x-axis refers to the percentage of participants who think that certain type of protection is important.

Figure 5. Security requirements in Logistics IoT and Office IoT. The x-axis refers to the percentage of participants who think that certain type of protection is important. Overall refers to general security protection.

4 SecIoT Framework
In this section, we introduce the SecIoT framework. This is specified from what can be considered as crucial aspects of security.

4.1 Authentication
The authentication component is mainly located in the central unit. Both data providers (e.g., sensors) and information consumers (e.g., user applications) connect to this central unit securely. As a consequence, there are two types of authentication procedures: user authentication and device authentication.

User Authentication
Objects and central unit should be confident on a user identity that is requesting a certain operation. It means that user authentication is necessary. In this authentication procedure, single-sign-on (SSO) mechanisms are applicable, since users need to authenticate only once to interact with various devices.

Device Authentication
Without authentication, it is not possible to assure that the data flow is produced by a certain device. Thus, device authentication is important. In traditional authentication procedure, public key infrastructure is a widely used framework. It allows entities without prior contact to authenticate each other. However, this authentication framework is complex and too cumbersome for many small devices, for example sensor nodes.

Recent years, multi-channel security protocols become another authentication option. These protocols bootstrap security using out-of-band channels, for example emails, SMS messages, phone calls, and even face-to-face conversations. A definition is summarized as below.

Definition 1 (Multi-channel security protocol). A multi-channel security protocol is a protocol that bootstraps security in networks based on security properties of out-of-band channels. These security properties make it difficult for an attacker to eavesdrop, spoof, or/and block messages over out-of-band channels.

Definition 2 (No-spoofing and no-blocking channel). Over a no-spoofing and no-blocking (NSB) channel, the attacker finds it difficult to block, modify, fake, replay, or delay messages [15].

Suppose there is a user; and the user has a mobile phone that is associated with a phone number or email address. It is easy to exchange public keys between the mobile phone and the IoT central service provider using public key infrastructure or other frameworks.

Assume again that there are some sensor nodes; some nodes are worn by the user, and some are fixed in the user's home. In 5G networks, all these nodes are allocated with an IP address. However, public infrastructure is complex and too cumbersome for sensor nodes. In this
circumstance, how can a sensor node and the central service provider securely exchange their IP addresses and public keys?

Multi-channel security protocols could be one solution. Firstly, notations are listed below.

- $S$: the identity of the sensor node
- $C$: the identity of the central service provider
- $IP_S$: the IP address of the sensor node
- $IP_C$: the IP address of the central service provider
- $PK_S$: the public key of the sensor node
- $PK_C$: the public key of the central service provider
- $N_S$: a nonce generated by the sensor node
- $N_C$: a nonce generated by the central service provider
- $\text{hash}()$: a hash function

The identity of the sensor node is $S$, the corresponding IP address is $IP_S$, and the public key is $PK_S$; the identity of the service provider is $C$, the corresponding IP address is $IP_C$, and the public key is $PK_C$. They can exchange keys using the following protocol.

Step 1. The provider sends the sensor node its identity $C$, its IP address $IP_C$, its public key $PK_C$, and a nonce $N_C$. This message is message 1:

$$\{C, IP_C, PK_C, N_C\}$$

Step 2. The sensor node sends the provider its identity $S$, its IP address $IP_S$, its public key $PK_S$, a new nonce $N_S$, and the received nonce in message 1 $N_C$. This message is message 2:

$$\{S, IP_S, PK_S, N_S, N_C\}$$

Step 3. The provider computes a hash of previous messages. The hash output is sent to the sensor node via a NSB out-of-band channel. This message is message 3:

$$\{\text{hash}(C, IP_C, PK_C, N_C, S, IP_S, PK_S, N_S)\}$$

Step 4. The sensor node also computes the hash value, and compares the two hash values. If they are the same, the node replies with Yes via a NSB out-of-band channel; otherwise, the user replies with No via a NSB out-of-band channel. This message is message 4:
Remark 1. We have verified the general version of the device authentication protocol using Casper/FDR, and no attacks have been found. Details can be found later.

Remark 2. One example NSB out-of-band channel can be established as follows. (1) From the provider to the mobile phone. As mentioned previously, it is easy to exchange public keys between the mobile phone and the central service provider. Then, the provider can send the hash output to the mobile phone securely with the help of these public keys. (2) From the mobile phone to the sensor node. It is easy to establish a secure Bluetooth link (or other secure links, e.g., visible light link [9, 16], audible sound link [17], and shaking based link [18]) between the mobile phone and the sensor node. The hash output can be transmitted from the mobile phone to the sensor node securely using these links.

Remark 3. Using this protocol, the out-of-band channels that are used to deliver the hash output are assumed as NSB channels. In other words, attackers cannot block, modify, fake, replay, or delay messages. This threat model has a basic requirement: nodes are trustworthy. In other words, there are no malicious programs in the sensor nodes, the mobile phone or the central service provider.

Remark 4. Requirements to users. (1) Users should update operating systems or even use anti-virus software in order to make sure that their nodes are trustworthy. (2) Users should not allow other people to use their nodes unless a) they are trustworthy, and b) this is necessary. (3) When users are running protocols, especially when they are transmitting messages among nodes, users should prevent other people from disturbing this procedure.

4.2 Secure Communications
A secure communications channel is, in most cases, a byproduct of a successful authentication. This process will make use of certain user credentials, such as public keys or public key certificates. As IoT inhabits the Internet ecosystem, it is important to provide support for existing security protocols. In fact, the security of IoT protocols, such as CoAP (Constrained Application Protocol), is largely dependent on the implementation of these security protocols [19].

Some protocols can be implemented without any major changes. However, other protocols need to be adapted due to the complexity of their design. Such protocols must achieve a tradeoff between simplicity and compatibility.

4.3 Authorization
Once identities are proved, it is necessary to check whether the user has the rights to access certain data. Access control system is the corresponding mechanism to check whether a
authenticated entity is authorized to perform an operation. This system is also a useful tool for privacy protection: it can help users to manage their own data.

Role-based access control (RBAC) is one popular access control mechanism. A role is a job title based on some semantics regarding the authority and responsibility conferred on the subject assigned to the role. Different roles are assigned to different groups of user.

However, it is necessary to consider factors such as context as part of the role model. For example, only authenticated users located in my vicinity during working hours can access today’s reports. In order to meet this requirement, granularity of roles can be adjusted: one general role is subdivided into fine-grained roles. Fine-grained roles might be different in various contexts even if they refer to the same type of entity, i.e. the same general role. Fine-grained role is defined below.

**Definition 3** (Fine-grained role).

Suppose $R$ is a role, $\{T, V\}$ is a context set, where $T$ is the type, and $V$ is the value. A fine-grained role $r$ is generated using the following mapping:

$$(R, \{T, V\}) \rightarrow r.$$

When a user is assigned with a fine-grained role, corresponding resource or data that the user can access is determined. In SecIoT, policies are used in such determination processes. The policies can be generally described as follows.

**Definition 4** (Permission policy).

Suppose user $U_b$ wants to access data $D_a$ of user $U_a$, and $U_b$ finally gets data $D_a'$. Permission policy is a collection of rules or mapping functions from $D_a$ to $D_a'$ based on the fine-grained role $r_b$ assigned to $U_b$:

$$(D_a, r_b) \rightarrow D_a'$$

**4.4 Risk Indicator**

A security indicator shows security risks of current configurations. It can help users to understand their security risks. The indicator is designed based on security risk analysis techniques [20, 21]. These techniques mainly involve the following steps.

- Asset identification. Assets in the system that should be protected are identified. In addition, methods of accessing assets are identified.
• Threat identification. A threat is something that can potentially do harm to the asset. These threats usually make use of system vulnerabilities.
• Risk evaluation. In this step, the outcome and impact of threats are identified. Outcome is the attack consequence: disclosure, modification, loss, destruction and interruption. Impact is the severity of the outcome: low, medium and high.

5 Results
This section describes our prototype IoT with authentication protocol analysis, access control and risk indicator interface.

5.1 Prototype IoT
Our prototype IoT consists of sensor networks, a data center, and a web site. After users login to their account, they can access data of their IoT devices via the website; one example is shown in Figure 6. It shows the location and the value of a queried sensor node.

• Sensor network. (1) Some sensors can be associated with patients. Sensor data such as pulse rate and motion data can be collected and transmitted to doctors' mobile phones. Using the data, doctors can make quick and better decisions. (2) Some sensors are fixed inside buildings. They can provide physical data such as temperature, humidity, light strength, and sound. They enable applications, for example home automation and monitoring.
• Data centre. The collected sensor data is sent to and stored in a data centre.
• Web site. It is the interface between SecIoT and users. Besides, there are some links of user profile, sensor profile and security policy.
5.2 Authentication Protocol Analysis

We have verified the authenticity of our device authentication protocol. The protocol is generalized to a few steps shown below.

1) Step1. A sends B message 1.
2) Step 2. B sends A message 2.
3) Step 3. A sends B via a NSB out-of-band channel: hash(message 1, message 2)
4) Step 4. B sends A via a NSB out-of-band channel: yes/no

The aim of this verification is to find out whether or not an attacker can maliciously change message 1 or message 2 (that contains the public key) to another message (another public key). We did this verification using Casper/FDR, and no attack was found.

Meanwhile, since we use public keys, confidentiality is not a problem as long as good cryptographic algorithms are used. Also, if there are denial-of-service attacks, we can directly use NSB out-of-band channels to transmit public keys. The general procedure is shown below.

1) Step1. A sends B message 1 that contains A’s public key via NSB out-of-band channel.
2) Step 2. B sends A message 2 that contains B’s public key via NSB out-of-band channel.

NSB out-of-band channels are not vulnerable to message blocking, thus the protocol can prevent denial-of-service attacks. Certainly, there is no absolute NSB channel; however, the attacker will
find that it is extremely difficult to block these channels comparing to block WiFi or Zigbee signals.

5.3 Access Control
With the fine-grained role, users can get more flexible access control systems. Objects can control the granularity of the data they produced (e.g. Hyde Park or London).

Suppose a user $U_b$ wants to know a user $U_a$’s location. $U_b$ ’s pre-defined role is $R = \text{doctor}$.

When $U_a$ ’s context is $\{\text{Event, accident}\}$, $U_b$ is assigned to fine-grained role $r_b = \text{doctor @ accident}$. With this role, $U_b$ can get the exact location of $U_a$.

However, when $U_a$ ’s context is $\{\text{Event, on duty}\}$, $U_b$ ’s fine-grained role becomes $r_b = \text{doctor @ no _ accident}$. With this role, $U_b$ can only know an ambiguous location.

Next, the access control system will compute the data $D'_a$ granted to $U_b$ based on $r_b$ and the permission policy. The policy is a set of rules shown below.

{ID:1, Role:"doctor", Context:"on duty", k:10}
{ID:2, Role:"doctor", Context:"emergency", k:1}

The policy specifies role, event (or Context), and a parameter $k$ [13]. This $k$ is a parameter generated using the original data $D_a$ (corresponding to data $D'_a$) and the fine-grained role $r_b$; and it is used to compute $D'_a$. Their relationships can be summarized as a series of mapping functions below.

$$(D_a, r_b) \rightarrow k \rightarrow D'_a$$

For example, the exact location is $D_a$. Next, the access control system generate a circle shown in Figure 5; the centre of the circle is $D_a$, and the radius is $k$ kilometers. Then, a random location $D'_a$ is selected in this circle.

In order to find out users’ opinion on the fine-grained role, we conducted a small user study with 12 participants. Nine of them work in IT related area. We provide two types of access control systems:

1) Role-based access control. If a user is a doctor, s/he can always access your exact location.
2) Fine-grained role based access control. A doctor can access your exact location in an emergency scenario. In other scenarios, the doctor can only get an ambiguous location.
The result is shown in Figure 7 (multiple choice questions). Seven of the twelve participants preferred the fine-grained role based access control. Two participants thought that the fine-grained role based access control is as good as the role based access control. Meanwhile, most participants thought that the fine-grained role based access control can be easily understood. Thus, we conclude that the fine-grained role based access control should be supported in IoT.

![Figure 7. User study results of access control models. Y-axle refers to the number of participants.](image)

### 5.4 Risk Indicator
Three types of risk representation methods are designed. They are shown in Figure 8.

- **Risk table.** Assets, their access methods, possible attack outcomes and corresponding impacts are represented using a table.
- **Risk tree map.** For each critical asset, threats and their risks are represented by the area of square trees with colours.
- **Risk tree.** The critical asset is the root. Its children are threats. Leaf nodes are risks.

An investigation was performed through a user study with 12 participants in order to find the best risk representation method. Participants were asked to mark their preferred methods of risk indication (multiple choices can be made). Figure 9 shows the results. We can see that risk tree map is the best way of representing risks. Especially, when mobile phones are used, displays are not big enough for a big table or tree.
Figure 8. Risk representation methods. The upper left is a risk table; the upper right is a risk map; and the lower one is a risk tree.
Figure 9. User study results of risk indicators. The y-axle refers to the number of participants.

6 Conclusion
The 5th generation of wireless systems (5G) aims to offer infinite networking capability, where IoT will be involved to provide device-to-device communications across a unified all-IP network layer. This merge will allow 5G to operate at any time, in any places and in any situation.

Despite the wealth of potential applications of IoT and the fact that many of the technologies to support IoT are already in use, the IoT is still not a reality in a practical sense. This can be largely attributed to concerns on security. The inherent physical nature of the IoT implies that cyber-attacks, where damage is normally confined to a virtual world, can now present an actual physical threat. This could be a threat to privacy (where personal information is harvested from electronic devices or video recording equipment), a nuisance (e.g. adjusting the levels on a thermostat) or even an actual threat to personal safety (in cases where devices are part of safety critical systems such as a car braking system or a home security network). Networking connections are also notoriously sensitive to security breaches in existing systems and the higher level of interconnectivity in the IoT is likely to make it especially vulnerable to attacks if the right precautions are not taken.

In this paper, we investigated three typical IoT applications, namely body area IoT, home IoT and hotel IoT through user studies. We found that IoT security is a serious problem concerned by users. Furthermore, we designed a security framework named SecIoT. It provides essential authentication, ensures secure communications, supports user authorization, and offers risk notification, thus satisfying the main concerns of users derived from our user studies. In
particular, we explored the user acceptance of the fine-grained access control and risk indication methods. The framework can serve as a foundation for supporting the security of IoT applications.

While the framework we have developed can fulfill the basic security requirements, it also helped to highlight some additional open issues such as availability enhancement and trust management, which will be our future work.

Acknowledgment
This work has been supported in part by the Oxford Martin School. It is also sponsored by the PhD grant (JY0300130104) of Chinese Educational Ministry, the initial grant of Chinese Educational Ministry for researchers from abroad (JY0600132901), National Natural Science Foundation of China (Grant No. 61472308), and the grant of Shaanxi Province for excellent researchers from abroad (680F1303) and Aalto University.

Reference


