Security/Privacy Models for "Internet of things":
What should be studied from RFID-schemes?

Daisuke Moriyama and Shin’ichiro Matsuo
NICT, Japan
Internet of Things (IoT)

CASAGRAS defined that:

A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent federated services and applications. These will be characterised by a high degree of autonomous data capture, transfer event network connectivity and interoperability.

Source: CASAGRAS Meeting
Internet of Things (IoT)

CASAGRAS’s inclusive model

Source: “The CASAGRAS Goal”
My talk

IoT Security

Common Security/privacy between RFID and IoT

Different Security/privacy between RFID and IoT

Solved problem

Unsolved problem

Target devices for IoT:
- RFIDs
- Sensors
- Smart Phones
- (future devices, etc.)
The existing effort in cryptography

Internet of Things consists of
- RFIDs
- Sensors
- Smart Phones
- (future devices, etc.)

Number of papers in IACR ePrint Archive:

“Internet of Things”, “IoT” – 0 hit

“RFID” – 52 hit

“Sensor” – 23 hit

“Mobile phone”, “Mobile device”, “Mobile (ad-hoc) network” – 12 hit
How to construct secure protocols for IoT

1. Abstract the requirement for IoT
2. Define proper security/privacy model
3. Propose a cryptographic protocol
4. Provide rigorous security proof

This flow has been used in any cryptographic schemes and protocols.
How to construct secure protocols for IoT

1. Abstract the requirement for IoT
2. Define proper security/privacy model
3. Propose a cryptographic protocol
4. Provide rigorous security proof

Object identification in IoT is mainly solved by RFID technology, and there are many results for RFID authentication protocol.

Let’s refer and compare them to construct the security model for IoT!
The existing RFID research in cryptography

Cryptographers concentrate on RFID authentication protocol

RFID authentication protocol provides:
- tag’s authentication and tag’s privacy (reader’s authentication as optional)

Several researcher consider additional properties

- **Distance-Bounding protocol**
  - “Accept”
  - “Reject”

- **Ownership transfer protocol**
  - Authentication right
Several unsolved problems

1. Suitable security model
   We analyzed the relationship among the security models

2. Identification vs. authentication

3. Real-Life Requirements for RFID
Problem 1: suitable security model

There are several security models for RFID authentication

- Juels-Weis (PerCom 2007, ACM TISSEC 2009)  
  *Indistinguishability based*  
  
- Vaudenay (ASIACRYPT 2007), Paise-Vaudenay (ACMCCS 2008)  
  *Simulation based*  
  
- Deng-Li-Yung-Zhao (ESORICS 2010)  
  *Zero-knowledge based*  
  
- Burmester-Li-Medeiros-Tsudik (ACM TISSEC 2009)  
  *Universal composability based*  
  
- Ha-Moon-Zhou-Ha (ESORICS 2008)  
  *Unpredictability based*  

...and many minor variants
Problem 1: suitable security model

Juels-Weis security model:

Correctness:
- Tags and Reader interact:
  - When the protocol is honestly executed, the reader accepts the tags.

Security:
- Tags and Reader interact:
  - Except the relay attack and corrupt tags, the reader does not accept the tags when an adversary interferes the message.
Problem 1: suitable security model

Juels-Weis security model:

Privacy:

The adversary cannot distinguish whether he interacts with tag $t_0$ or $t_1$. 

12
Problem 1: suitable security model

Juels-Weis security model:

\[
\begin{align*}
\text{Exp}^{\text{IND}-b}_A(k) \\
(pk, sk) &\overset{\text{R}}{\leftarrow} \text{Setup}(1^k) \\
(t_0, t_1, st_1) &\overset{\text{R}}{\leftarrow} \mathcal{A}_1^{\text{ReaderInit,Send,Corrupt,Result}}(pk, \mathcal{R}, \mathcal{T}) \\
b &\overset{\text{R}}{\leftarrow} \{0, 1\}, \mathcal{T}' := \mathcal{T} \setminus \{t_0, t_1\} \\
b' &\overset{\text{R}}{\leftarrow} \mathcal{A}_2^{\text{ReaderInit,Send,Corrupt,Result}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t_b), st_1) \\
\text{Output} \quad b' \\
\end{align*}
\]

(Reveal\(t_0\) and Reveal\(t_1\) are prohibited)

\[\mathcal{A}_2\text{ anonymously interacts with } t_b\]

\[
\text{Adv}^{\text{IND}}_A(k) := \left| \Pr \left[ \text{Exp}^{\text{IND}-0}_A(k) \rightarrow 1 \right] - \Pr \left[ \text{Exp}^{\text{IND}-1}_A(k) \rightarrow 1 \right] \right|
\]

This is a slight variant proposed by Deng-Li-Yung-Zhao (ESORICS 2010)

This definition is based on \[\text{IND-CCA security for PKE} / \text{anonymity for IBE}\] as a reference

If we allow \(\mathcal{A}_1\) to issue Reveal queries to \(t_0\) and \(t_1\), we need public key cryptography to satisfy the modified model
Problem 1: suitable security model

Indistinguishability-based formal privacy definition is useful to provide the security proof. However, only few (rigorous) relationship among the security models is proved.

Ma-Li-Deng-Li (ACMCCS 2009) proved that

\[
\text{Indistinguishability based privacy} \quad \leftrightarrow \quad \text{Unpredictability based privacy}
\]

We analyzed the other security models based on the several results for public key encryption. We recently found that

\[
\text{Indistinguishability based privacy} \quad \leftrightarrow \quad \text{Simulation based privacy} \quad \downarrow \quad \text{Zero-knowledge based privacy}
\]
Problem 2: identification vs. authentication

Many researcher describe “authentication” protocol for RF “Identification”

The reader outputs accept or reject (for Result query) < The reader outputs identity or (for Result query)

(The adversary can obtain information more than one bit if we actually treat it as identification)

Only authentication is necessary? Why?

I think the existing protocols are “Radio Frequency Authentication (RFAU)”!

It may cause a problem when the protocol is embedded in IoT
Problem 3: real-life requirements for RFID

- On-off control

"I don’t know the identity, but he is wearing a wig!" (because my reader received a response)

Cryptographic solution:

Reader authentication is needed before the tag responds a message, but digital signature is too expensive to compute.

Another solutions:

Breaking the RFID tag’s circuit is not good solution since the tag cannot be reused.

Physically protection (e.g. foil-wrapping) may be difficult in some cases.
Problem 3: real-life requirements for RFID

- Secrecy/integrity/availability of stored data

Several types of Tags can contain the Identity, secret key for authentication and usable data

Utilizing the data in RFID tag (in addition to Identity) is one of the attractive point (manufacturer, production date, expiration data)

Several data should be protected or verified, however cryptographers only study RFID authentication protocol now...

For the resource constraint, some kinds of merged scheme/protocol will be valuable

-- Example in public key crypto: Signcryption (faster than “Encrypt + Sign”)
Problem 3: real-life requirements for RFID

- Life-cycle of the tag

Some data on RFID tag (e.g. indication of origin) should be declared and not be modified

However, special commands for (partially) erasure is useful to reuse the tag

In addition to the transmission of the ownership (ownership transfer protocol), how to manage the tag’s data/identity/ownership respectively is important in the realistic setting
What are the additional requirements in IoT?

- Data integrity <-- it is necessary in sensor network
- Data secrecy <-- it is also necessary in sensor network
- Primary sender <-- who generates the data should be specified
- Key Management <-- how to keep/update/recover a secret is one of the main issue in all protocols

We should abstract the realistic requirement to the cryptographic-oriented notion as possible as we can. We can refer many types of security model in public key cryptography

- Anonymous IBE --- indistinguishability of data and identity
- Forward signature --- unforgeability, forward security
- Group signature --- unforgeability, anonymity, unlinkability, traceability
- Key exchange --- impersonation, unknown key share, key leakage...
What are the additional requirements in IoT?

In RFID authentication, researchers assume that the reader (and the background database) has enough computation resources.

However, it may be smart phone in IoT! This gap is not considered...

It is important to define the actual roll (tag, reader, sensor, etc.) of the “Things”.

It should also be discussed in the IoT environment.

“I will send you the weekly data I obtained. I am now computing fully homomorphic encryption. Please wait 1 year!”

Depending on the specific wide environment, we should organize the security requirement, choose the security model and propose an efficient protocol to spread the world of IoT!
Conclusion

Suitable security model to construct convenient protocols based on symmetric key cryptography

52+ papers

Common Security/privacy between RFID and IoT

52 papers

Authentication + privacy

Different Security/privacy between RFID and IoT

integrity + secrecy + ...

52 papers

Solved problem

0 paper

Unsolved problem

• Relationship among security models -- indistinguishability
• authentication ≠ identification
• Life-cycle
Thank you for your attention!