

A survey of secure middleware for the Internet of Things

Paul Fremantle and Philip Scott

Presented by: Becky Shanley

Introduction and Background

- Overwhelming growth in number of IoT devices
 - 2010 → ~12.5 billion IoT Devices
 - 2020 → ~50 billion IoT Devices
- These projected numbers raise multiple security concerns for the IoT

Security Concerns I

IoT Devices are becoming more central to people's lives

Security Concerns II

Many devices collect PII (Personally Identifiable Information)

Security Concerns III

IoT devices can affect the physical world

Security Concerns IV

Size & power limitations

Security Concerns V

Scale & number of devices create new challenges and
therefore require new solutions

Security Concerns, but an example

- “In 2016, more than 100,000 IoT devices were conjoined into a hostile botnet named Mirai that attacked the DNS servers of the east coast of the US” (Page 2, *A survey of secure middleware for the Internet of Things*)
- This number has been proven to be small compared to the number of devices available for attack (several million)

Contributions to Security Concerns

1. proposing a new security model for IoT (the matrix of security challenges + *Three Layer Privacy Model*)
2. reviewing (a lot of) relevant literature of security of middleware systems for IoT

Security Characteristic	A. Device / Hardware	B. Network	C. Cloud / Server-Side
1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
2. Integrity	A2. Spoofing; Lack of attestation	B2. Signatures with low capability devices Sybil attacks	C2. No common device Identity
3. Availability	A3. Physical attacks;	B3. Unreliable networks, DDoS, Radio jamming	C3. DDoS (as usual)
4. Authentication	A4. Lack of UI, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No common device identity, insecure flows
5. Access Control	A5. Physical access; Lack of local authentication	B5. Lightweight distributed protocols for Access Control	C5. Inappropriate use of traditional ACLs, Device Shadow
6. Non-Repudiation	A6. No secure local storage; No attestation forgery	B6. Lack of Signatures with low capability devices	C6. Lack of secure identity and signatures

Security Characteristic	A. Device / Hardware	B. Network	C. Cloud / Server-Side
1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
2. Integrity	A2. Spoofing; Lack of attestation	B2. Signatures with low capability devices Sybil attacks	C2. No common device Identity
3. Availability	A3. Physical attacks;	B3. Unreliable networks, DDoS, Radio jamming	C3. DDoS (as usual)
4. Authentication	A4. Lack of UI, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No common device identity, insecure flows
5. Access Control	A5. Physical access; Lack of local authentication	B5. Lightweight distributed protocols for Access Control	C5. Inappropriate use of traditional ACLs, Device Shadow
6. Non-Repudiation	A6. No secure local storage; No attestation, forgery	B6. Lack of Signatures with low capability devices	C6. Lack of secure identity and signatures

(New) Security Characteristics Definitions I

Authentication is the act of proving an assertion, such as the identity of a computer system user (Wikipedia, <https://en.wikipedia.org/wiki/Authentication>)

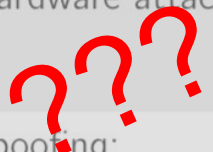
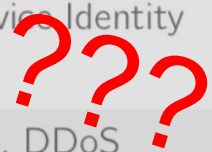
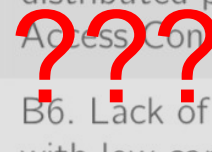
(New) Security Characteristics Definitions II

Access Control (Access Approval) is the system making a decision to grant or reject an access request from **an already authenticated subject**, based on what the subject is authorized to access (Wikipedia, https://en.wikipedia.org/wiki/Computer_access_control)

(New) Security Characteristics Definitions III

Non-Repudiation is the act of associating actions or changes with a unique individual

- ie, non-repudiation would be violated if key cards were shared or if lost and stolen cards were not immediately reported (Wikipedia, <https://en.wikipedia.org/wiki/Non-repudiation>)

Security Characteristic	A. Device / Hardware	B. Network	C. Cloud / Server-Side
1. Confidentiality	A1. Hardware attacks 	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
2. Integrity	A2. Spoofing; Lack of attestation	B2. Signatures with low capability devices Sybil attacks	C2. No common device Identity 
3. Availability	A3. Physical attacks;	B3. Unreliable	C3. DDoS
4. Authentication	A4. Lack of OT, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No Common device identity, insecure flows
5. Access Control	A5. Physical access; Lack of local authentication	B5. Lightweight distributed protocols for Access Control 	C5. Inappropriate use of traditional ACLs, Device Shadow
6. Non-Repudiation	A6. No secure local storage; No attestation forgery	B6. Lack of Signatures with low capability devices	C6. Lack of secure identity and signatures

Part I -- Matrix Evaluation

A1. Device Confidentiality

- If someone has physical access to the device, there are risks that are very difficult to be combatted
 - NAND Mirroring
 - Side-channel attacks
- Fingerprinting of sensors/data from sensors
 - there are small, random differences in the physical devices that appear during manufacturing that can be used to recognise individual devices across multiple interactions

1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
---------------------------	----------------------	--------------------------------------------	---------------------------------------------

B1. Network Confidentiality I

- Usually, encryption deals with this for non-IoT devices
- IoT devices have numerous challenges regarding encryption
 - RSA public-key encryption can take minutes to complete
 - ECC-based cryptography works very well on 8-bit controllers but is not used in many cases
- Encryption protocols (ie, Transport Layer Security) are complex to use with IoT devices
 - TLS can be configured to use ECC but is still suboptimal

1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
---------------------------	----------------------	--------------------------------------------	---------------------------------------------

B1. Network Confidentiality II

- IoT devices commonly communicate over the network via UDP (User Datagram Protocol) instead of TCP (Transport Control Protocol)
- Emergence of radio protocols present new security challenges for the IoT

1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
---------------------------	----------------------	--------------------------------------------	---------------------------------------------

C1. Cloud Confidentiality

- Social/Policy issues regarding ownership of data
 - Fitbit made data about users sexual activity publicly accessible online
- Government sponsored attacks identify further confidentiality issues in the cloud:
 1. deliberate backdoors are being added
 2. providers of cloud-hosting systems forced to hand over encryption keys
 3. the unknown extent to which metadata is being used by security services to build pictures of users

1. Confidentiality	A1. Hardware attacks	B1. Encryption with low capability devices	C1. Privacy Data leaks Fingerprinting
---------------------------	----------------------	--------------------------------------------	---------------------------------------------

A2. Integrity & Hardware I

- At risk of viruses, firmware attacks, hardware manipulation
 - → Attestation!
 -not that easy

2. Integrity

A2. Spoofing;
Lack of attestation

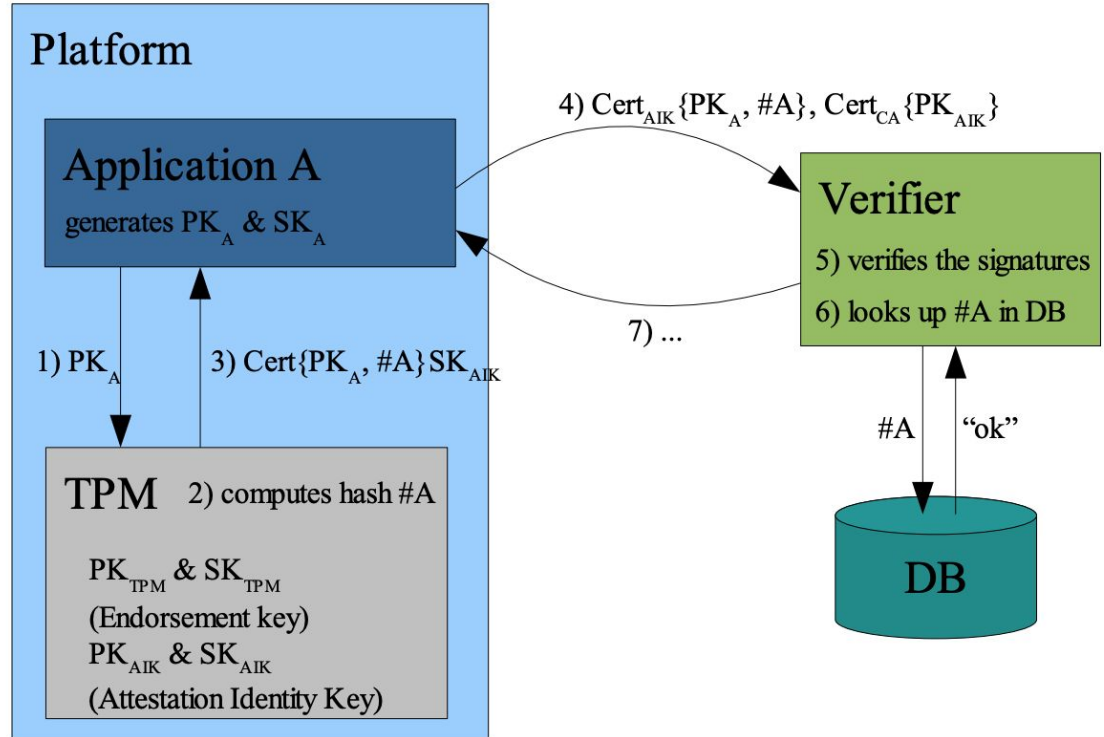
B2. Signatures with low
capability devices
Sybil attacks

C2. No common
device Identity

A2. Integrity & Hardware II

A basic remote attestation protocol looks something like this^[4]:

all this



B2. Integrity & Network

- Existing public-key encryption models provide integrity on networks!
but...
- Similar to B1, device & confidentiality → IoT devices are too low powered to provide adequate encryption

2. Integrity

A2. Spoofing;
Lack of attestation

B2. Signatures with low
capability devices
Sybil attacks

C2. No common
device Identity

C2. Integrity & Cloud

- Without device identity, there isn't really any cloud integrity

(device identity will be covered in more depth for A4/B4/C4)

2. Integrity

A2. Spoofing;
Lack of attestation

B2. Signatures with low
capability devices
Sybil attacks

C2. No common
device Identity

A3, B3, C3 Availability & Hardware, Network, Cloud

- **Hardware**
 - is unique in that there are things that can be done to physically limit availability, like draining power of a device or physically taking the device.
- **Network**
 - Mostly the same, save for the new exploration of the IoT using radio networks, which are susceptible to radio jamming
- **Cloud**
 - The only unique element of limiting availability is using the IoT device itself to perform a DDoS on the server (ie, Mirai Botnet)

3. Availability	A3. Physical attacks;	B3. Unreliable networks, DDoS, Radio jamming	C3. DDoS (as usual)
------------------------	-----------------------	----------------------------------------------	---------------------

A4. Device Authentication

- Initial registration of devices → many of the same types of devices share the same default passwords (ie, home routers)

4. Authentication	A4. Lack of UI, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No common device identity, insecure flows
--------------------------	-----------------------------------------------------------------------	-----------------------------------------------------	-----------------------------------------------------

B4. Network Authentication

- The device identifier needs to be stored in program memory/ROM/storage due to the nature of IoT devices (ie, rebooting without human interaction)

However..

1. If the program code has been changed after the device has validly authenticated, it can behave incorrectly
2. Spoofing!

4. Authentication	A4. Lack of UI, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No common device identity, insecure flows
--------------------------	-----------------------------------------------------------------------	-----------------------------------------------------	-----------------------------------------------------

C4. Cloud Authentication

- Establishing a secure conversation between the IoT device and other systems, challenging because → setting-up an encrypted and/or authenticated channel such as those using TLS

4. Authentication	A4. Lack of UI, Default Passwords, Hardware secret retrieval	B4. Default Passwords, lack of secure identities	C4. No common device identity, insecure flows
--------------------------	-----------------------------------------------------------------------	-----------------------------------------------------	-----------------------------------------------------

A5. Device Access Control

- Often physically distributed, thus increasing likelihood of attackers physically gaining access to the device
 - Already discussed in A1
- Access control requires devices to have a unique identity
 - Already discussed these challenges in A4

5. Access Control

A5. Physical access;
Lack of local
authentication

B5. Lightweight
distributed protocols for
Access Control

C5. Inappropriate use
of traditional ACLs,
Device Shadow

B5. Network Access Control

- Similar to many of the other network characteristics, we need a lighter weight protocol for network access control
 - Research is being done but this paper didn't identify any interesting approaches

5. Access Control	A5. Physical access; Lack of local authentication	B5. Lightweight distributed protocols for Access Control	C5. Inappropriate use of traditional ACLs, Device Shadow
--------------------------	---------------------------------------------------------	----------------------------------------------------------------	----------------------------------------------------------------

C5. Cloud Access Control

- Existing hierarchical models for access control are argued to not suit the scale of the IoT

1 of the proposed approaches to solving this→ user-directed security controls (a.k.a., consent)

- ensuring that users can control access to their own resources and to the data produced by the IoT that relates to those users
- UMA (User Managed Access) enhances OAuth spec to provide ^
- However, probably too complex to be widely adopted :(

5. Access Control	A5. Physical access; Lack of local authentication	B5. Lightweight distributed protocols for Access Control	C5. Inappropriate use of traditional ACLs, Device Shadow
--------------------------	------------------------------------------------------	----------------------------------------------------------	----------------------------------------------------------

A6, B6, C6. Non-Repudiation & Device, Network, Cloud

- Device
 - No attestation → no way to trust that the system hasn't been modified
- Network
 - Similar to other network concerns, cryptography is required to provide non-repudiation, and crypto == very challenging with few resources :(
- Cloud
 - Unchanged for IoT

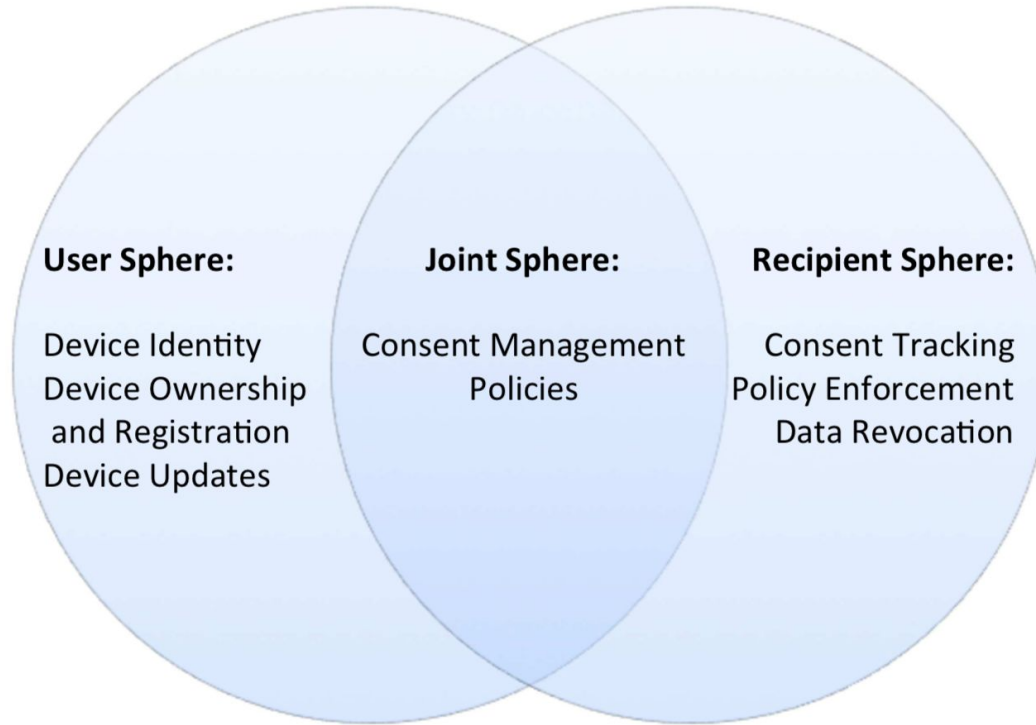
6. Non-Repudiation

A6. No secure local storage; No attestation forgery

B6. Lack of Signatures with low capability devices

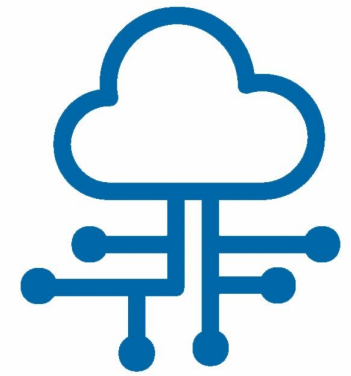
C6. Lack of secure identity and signatures

Three Layer Privacy Model



Summary of Security Review

- Matrix + three layer privacy model == a more secure IoT!
 - Using this combo, develops list of requirements to apply to the second half of the paper → middleware



Part II -- Secure Middleware for the Internet of Things



Secure Middleware for the Internet of Things

- What is middleware?
 - computer software that has an intermediary function between the various applications of a computer and its OS/the network (Page)
- This paper reviews two kinds of IoT middleware, non-secured and secured systems.
 - refers to the requirements detailed in the previous slides to determine secure/non-secure

Non-Secured Systems

- Out of a total of 54 middlewares examined, 35 middlewares had no published discussion or architecture for security.

Secure Systems Overview

	REQ1 -Integrity and Confidentiality	REQ2 -Access Control	REQ2.1 -Consent	REQ2.2 -Policy-based security	REQ3 - Authentication	REQ3.1 - Federated Identity	REQ3.2 -Secure Device Identity	REQ3.3 - Anonymous Identities	REQ4 -Attestation	REQ5 - Summarisation and Filtering	REQ6 -Context-based security/ Reputation	REQ7 -IoT-specific Protocol Support
&Cube	Y	Y			Y							Y
Device Cloud	Y	Y	Y		Y	Y						Y
DREMS	Y	Y			Y							Y
DropLock		Y	Y		Y	Y						Y
FIWARE	Y	Y	Y	Y	Y	Y						Y
Hydra/Linksmart	Y	Y			Y		Y					
Income	Y	Y		Y	Y						Y	
IoT-MP	Y				Y							
NERD	Y				Y							Y
NOS	Y	Y			Y						Y	Y
OpenIoT					Y	Y						
SensorAct		Y		Y								
SIRENA	Y				Y							
SMEPP	Y	Y			Y							
SOCRADES	Y	Y			Y							
UBIWARE				Y								
WEBINOS	Y	Y		Y	Y	Y	Y					
XMPP	Y	Y			Y	Y						
VIRTUS	Y	Y			Y	Y						

Summary of IoT Middleware Security

- A lot of IoT middleware doesn't even address security (35/54 of reviewed middlewares)
- Of the middlewares that do consider security, a lot of them use the SOAP/Web Services model, which doesn't scale properly to IoT
- There were some unique approaches that brought their own benefits
 - DREMS
 - SMEPP
 - Dioptase
 - FIWARE
 - Webinos

Overall Gaps

- No system supported attestation or anonymous identities
- User consent only identified in 3/54 systems
- 2/54 utilized context-based security/reputation
- 2/54 explicitly applied PBD (Privacy by Design)
- And, most importantly to this paper, no middleware met all of the defined requirements.

Conclusion

- This paper contributed to the field of security in IoT by designing a fleshed out security model that works with the unique security and privacy issues around the IoT
- It also studied existing IoT middleware and evaluated them against their security model

Questions from GitHub

- What bad things can be done with a non-connected device?
- Difference between Authentication and Access-Control
- Why is attestation so hard?
- Is more secure middleware the best way to secure IoT? Wouldn't focusing on the devices themselves or the cloud infrastructure have more of an impact on IoT security?