Special Session: The Future of IoT Security

S. Mohan, M. Asplund, G. Bloom, A. Sadeghi, A. Ibrahim, N. Salajageh, P. Griffioen, B. Sinopoli

Presented by: Álvaro Albero Gran

Introduction and Background

- IoT devices are growing at a huge pace (1 trillion by 2030) [1]
- Incidents are also growing
- The approaches to secure these devices need to evolve
- Security not only on the devices, also on the network carrying the data
- In summary, IoT security requires an effort in multiple lines

Outline

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Blockchain for IoT Security

- Buzz word, speculation, the solution for everything, is it valid for IoT?

Definition?

- Decentralized data structure
- P2P network
- Cryptographically secured
- Consensus algorithm
- Permanent ledger

Blockchain for IoT Security

Use Cases

- Logging device behavior for security monitoring
- Keep track of device status information

Then, why it is not getting used?

- Paper: Consensus algorithms (PoW, PoS, permissioned systems)
- Alvaro: Ecosystem is not matured enough

Outline

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Trustworthy Sensor Data

- The goal is to ensure sensor data integrity
- Design patterns of IoT are different than for general computing
- 3 existing approaches with their drawbacks and possible solutions

Cryptographic integrity

Algorithms incur in high resource cost

Lightweight cryptography

Byzantine agreement

Solutions designed for large-scale systems

Relaxing consensus

Data provenance

Cannot maintain a complete history

Compression

Outline

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Reliable Networks for IoT Systems

- IoT systems carry critical data
- Design constraints (end to end QoS)
- Previous work guaranteeing QoS is in isolated contained networks
- The IoT ecosystem can have heterogeneous open networks
- Even the internet

Software Defined Networks as a solution

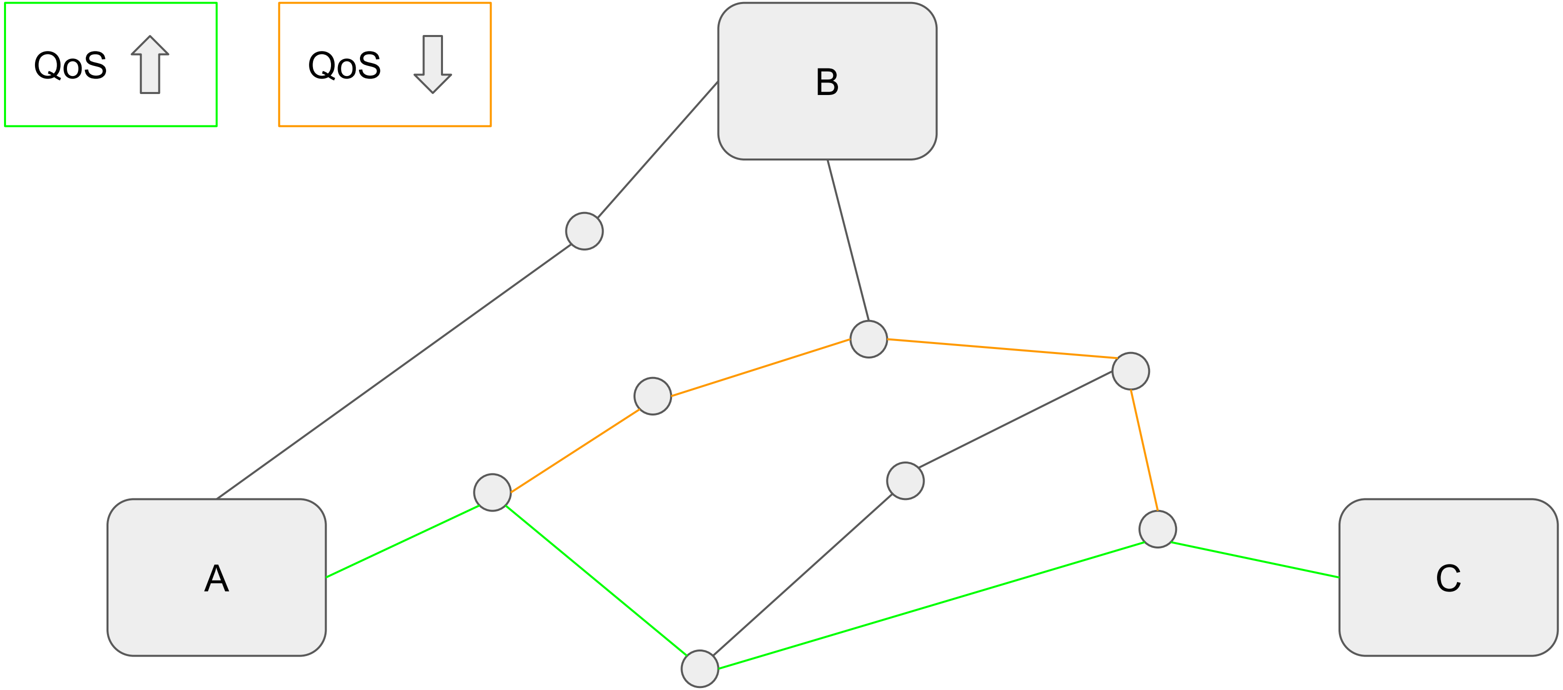
Reliable Networks for IoT Systems

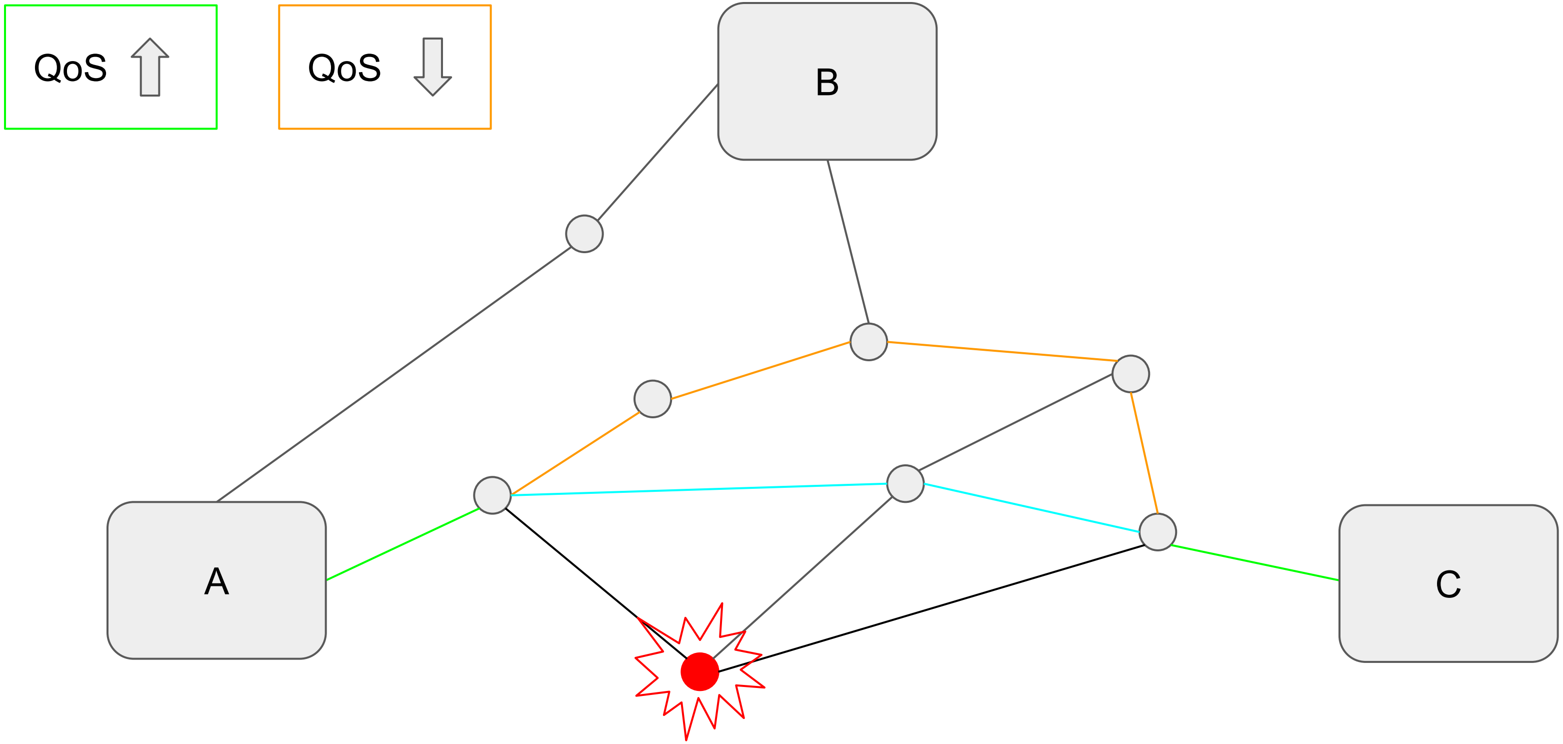
SDNs

- Give global visibility of the network
- Centralized controller (RYU, OpenDaylight)
- SDN switches simply implement the rules
- Can provide isolation and Resiliency

How?

- Send critical flows through higher capability links
- Adapt the traffic in the network when attacks/congestion


QoS ↑
QoS ↓
B
A
C


QoS ⇧
QoS ⇩
B
A
C

Outline

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Scalable Authentication of IoT Devices

- Authenticating users is a well studied field
- Three factor authentication pattern
- Not that easy to apply in embedded systems with low or none user interaction
- Physical threats are higher on IoT devices
- Relying on a central device may not be possible (moving sensors)

Scalable Authentication of IoT Devices

Properties IoT authentication systems should have:

- Scalability of the authentication method
- Decentralization
- Risk awareness and risk tolerance

Outline

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Remote Attestation for IoT Devices

“Remote attestation is a security service that allows a remote, potentially infected device (prover) to send a status report to a trusted party (verifier) to demonstrate it is in a known and trustworthy state”

- Create a Root of Trust
- What is different in IoT?

3 approaches:

- Lightweight security architecture
- Towards runtime attestation
- Swarm attestation

Remote Attestation for IoT Devices

Lightweight security architecture

- SMART
- Read Only Memory (ROM)
- Simple MPU to control access to ROM

Swarm attestation

- SEDA, uses SMART
- Distributes the load across the network
- Creates a verification spanning tree

Outline

1. Blockchains for IoT Security

2. Trustworthy Sensor Data

3. Reliable Networks for IoT Systems

4. Scalable Authentication for IoT devices

5. Remote Attestation for IoT Devices

6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Threat, Risk and Maturity Assessment Frameworks for the IoT

- IoT devices can be compromised at a huge scale
- Organizations need to assess threats and risks
- Current models are not adequate

Current assumptions

- Systems do not change significantly
- Require large amount of knowledge
- Do not consider relationships and couplings between devices

Threat, Risk and Maturity Assessment Frameworks for the IoT

Break attack in four parts:

- Attacker with a set of assets
- Perform an action
- Exploits vulnerabilities
- Compromising properties

Summary

1. Blockchains for IoT Security
2. Trustworthy Sensor Data
3. Reliable Networks for IoT Systems
4. Scalable Authentication for IoT devices
5. Remote Attestation for IoT Devices
6. Threat, Risk and Maturity Assessment Frameworks for the IoT

Critiques

- Good topic coverage
- Good comparison between general computing and IoT
- Some sections are very abstract and do not provide enough information
- Others are very complete
- I think you can tell that there were different authors involved