IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

TUM

Improving resilence of Industrial IoT

Renzo NAVAS

Table of contents

1 Introduction

2 Demo

3 Resilience

4 Moving Target Defense

5 IoT and Challenges

6 Thesis Perspectives

Introduction

Ph.D. Thesis: "Improving Resilience of the Industrial Internet of Things"

Thesis started 1st of December 2017 (3 months).

Before, I was working as research engineer on IoT: CoAP, LoRa, IETF IoT security protocols, Authenticated key establishment (on top of OAuth).

Context

- IoT and Industrie 4.0
- Gap between the security needs for industry and the state-of-the-art of IoT security.

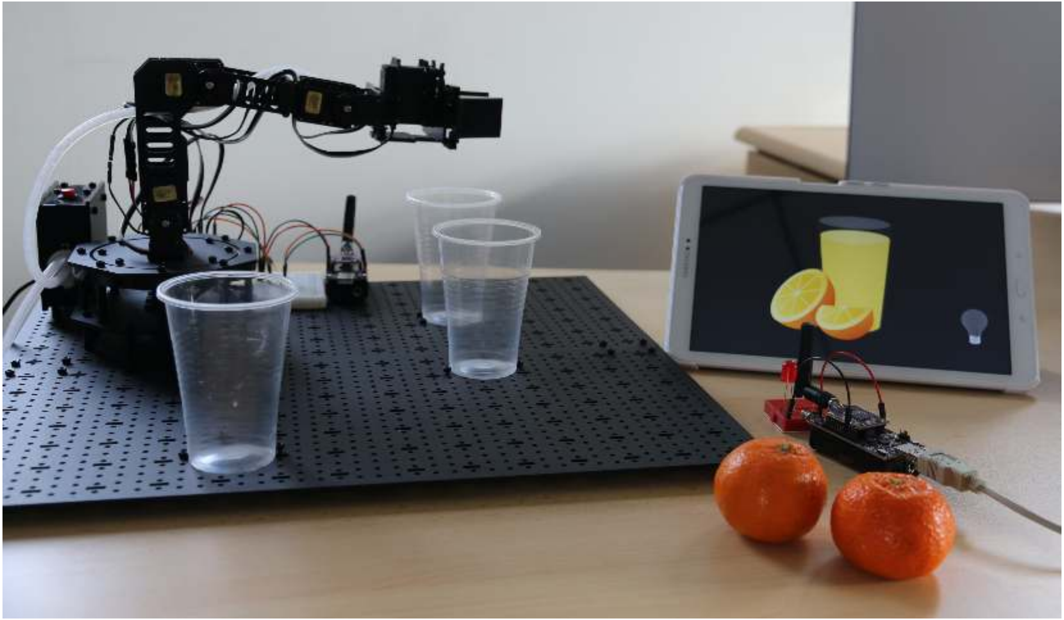
Objectives

Improve **resilience** of IoT systems in an industrial setting.
Moving Target Defense paradigm will be prioritized.

Challenges

- IoT constraints, MTD applicability.

IoT MitM attack Demo



IoT MitM attack Demo

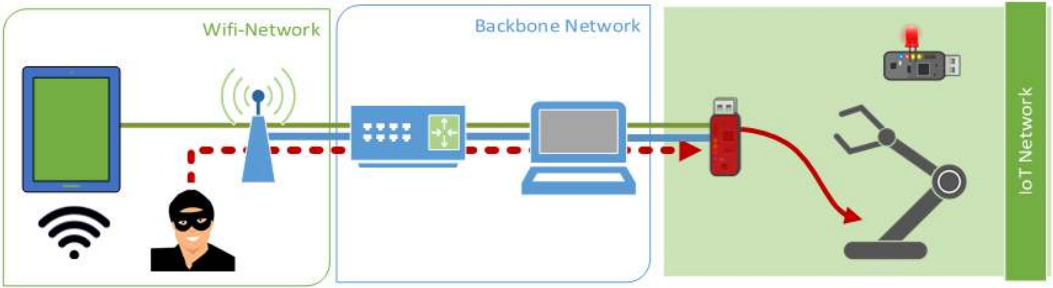
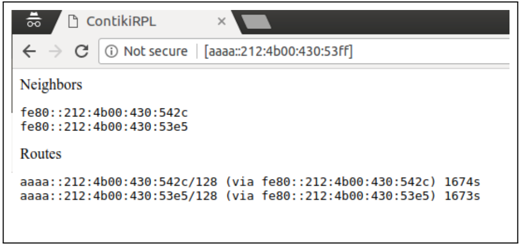


Figure: Scheme of the attack; in continuous red line the IPv6-CoAP message after being modified *in transit* by the insider malicious node

.

Click for Demo video

IoT MitM attack Demo



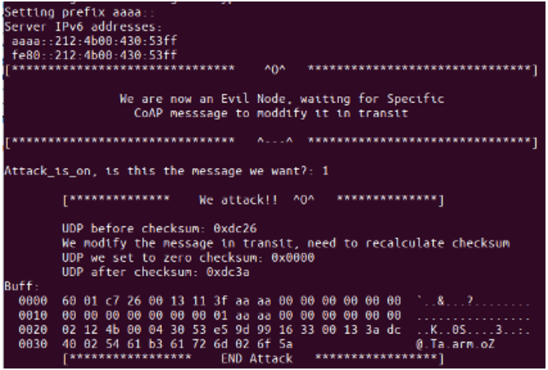
Neighbors

```
fe80::212:4b00:430:542c
fe80::212:4b00:430:53e5
```

Routes

```
aaaa::212:4b00:430:542c/128 (via fe80::212:4b00:430:542c) 1674s
aaaa::212:4b00:430:53e5/128 (via fe80::212:4b00:430:53e5) 1673s
```

Figure: RPL: a collaborative *mesh* network



```
Setting prefix aaaa::
Server IPv6 addresses:
 aaaa::212:4b00:430:53ff
 fe80::212:4b00:430:53ff
[*******************************    ^0^   *******************************]

                We are now an Evil Node, waiting for Specific
                  CoAP messsage to moddify it in transit

[*******************************   ^...^  *******************************]

Attack_is_on, is this the message we want?: 1

        [**************    We attack!!  ^0^   **************]

        UDP before checksum: 0xdc26
        We modify the message in transit, need to recalculate checksum
        UDP we set to zero checksum: 0x0000
        UDP after checksum: 0xdc3a
Buff:
  0000  60 01 c7 26 00 13 11 3f aa aa 00 00 00 00 00 00  `..&...?........
  0010  00 00 00 00 00 00 00 01 aa aa 00 00 00 00 00 00  ................
  0020  02 12 4b 00 04 30 53 e5 9d 99 16 33 00 13 3a dc  ..K..0S....3..:.
  0030  40 02 54 61 b3 61 72 6d 02 6f 5a                 @.Ta.arm.oZ
        [*****************    END Attack   *****************]
```

Figure: MitM Attack: Inside the compromised node

IoT state-of-the-art generic security vision

- CoAP, CBOR, COSE... are basic tools to define security services.
- Example of security services: application data confidentiality, authenticated key establishment, authorization policies ...
- All the security services are maintained end-to-end and agnostic to lower layers.

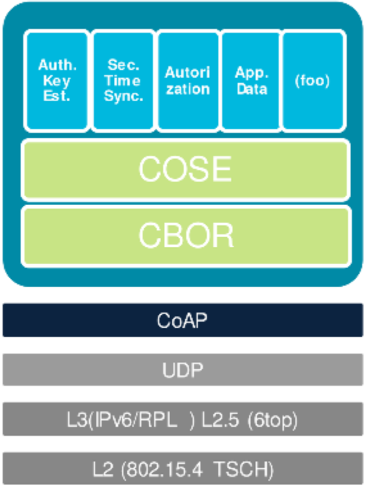


Figure: IoT network stack and sec. services

… and now

Resilience

"**Resilient** systems are capable of evading, withstanding, recovering and evolving from adversarial attacks and failures"[1]

- Despite the effort to protect systems, adversaries will get in, and will compromise and disrupt parts of it.
- For Industrial use cases resilience is a priority.
- For current IoT systems resilience is <u>not</u> a priority.

[1] M. Carvalho et al., Moving-target defenses for computer networks; IEEE Security and Privacy, 2014

Resilience

"**Resilient** systems are capable of evading, withstanding, recovering and evolving from adversarial attacks and failures"[1]

- Despite the effort to protect systems, adversaries will get in, and will compromise and disrupt parts of it.
- For Industrial use cases resilience is a priority.
- For current IoT systems resilience is not a priority.

[1] M. Carvalho et al., Moving-target defenses for computer networks; IEEE Security and Privacy, 2014

How to improve the resilience of a system?

Moving Target Defense (MTD)

Source: M. Carvalho et al., Moving-target defenses for computer networks; IEEE Security and Privacy, 2014

MTD: Introduction

- The static nature of computer systems makes them easy to operate and manage, but also easy targets of cyber attacks.
- An attacker can always have sufficient time to study a target system, which leads to an *information asymmetry* between attacking and protecting.

[2] NITRD. National Cyber Leap Year Summit 2009 Co-chairs' Report.

MTD: Introduction

- The static nature of computer systems makes them easy to operate and manage, but also easy targets of cyber attacks.
- An attacker can always have sufficient time to study a target system, which leads to an *information asymmetry* between attacking and protecting.

MTD: A change of paradigm

- Moving Target Defense (MTD)[2]is proposed as a promising defense paradigm to break the static nature of current computer systems
- MTD tries to introduce diverse uncertainties to make a computer system's running environment dynamic and unpredictable

[2] NITRD. National Cyber Leap Year Summit 2009 Co-chairs' Report.

MTD: Existing research

G. Cai et al. on "Moving target defense: state of the art and characteristics" [1]

Three main areas of MTD research:

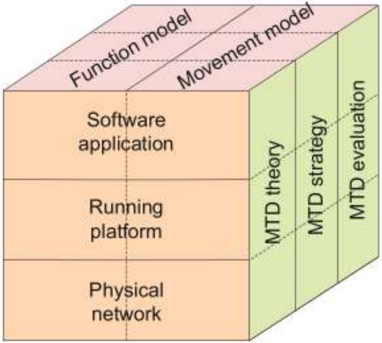
- **Theory**: answers to fundamental questions. e.g. what capabilities an MTD systems should have.
- **Strategy**: design moving mechanism for systems. The core of MTD to provide a defense mechanism.
- **Evaluation**: provides appropriate models and approaches to measure effect and cost of MTD.

MTD: Existing research

G. Cai et al. on "Moving target defense: state of the art and characteristics" [1]

Three main areas of MTD research:

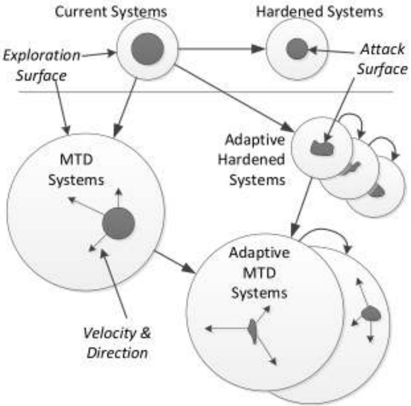
- **Theory**: answers to fundamental questions. e.g. what capabilities an MTD systems should have.
- **Strategy**: design moving mechanism for systems. The core of MTD to provide a defense mechanism.
- **Evaluation**: provides appropriate models and approaches to measure effect and cost of MTD.



G.Cai et al.[1] three-dimensional model for existing MTD research

MTD: Theory

- MTD Theory describes the common design principles as well as the capabilities and features that an MTD system should have.
- *Attack Surface* is the set of the system's properties that can be used for attack.
- *Attack surface shifting* means at least one parameter (or value) of the attack surface is replaced.
- MTD Theory also explores the attacker capabilities.
- Design principles: *what* to move, *how* to move, and *when* to move.



R. Zhuang et al. [2] MTD High Level Intruition

MTD: Strategies

MTD strategy is applied to the selected moving parameters of a system to make them move, continually, enhancing the resiliency and security of the protected target.

Existing MTD strategies are classified by G.Cai et al.[1] into three categories:

- Software transformations (Application)
- Dynamic platform techniques (Hardware and OS attributes. e.g. instruction set architecture, stack direction, OS, machine instance).
- Network address shuffling. e.g. Moving Target IPv6 defense (MT6D).

MTD: Strategies

Wang et al. [3] simplifies the strategies classification to only two: system-level, and network-level.

Some examples of network-level MTD strategies Wang et al. applies to SDN:

- changing network topology
- changing network attributes (node and network)
- network traffic manipulation
- network diversification
- network elements migration

MTD: Evaluation

MTD evaluation measures the effectiveness and efficiency of existing mechanisms. How?

- Metrics
- Approaches: Experiment-based, Theoretical analysis, Model-based analysis.

Picek et al. [4] summarizes the importance of this field on the title of the cited work:

If You Can't Measure It, You Can't Improve It

MTD for IoT systems?

MTD for IoT: State of the Art

New field (**good for this thesis!**), two lines of work exist

- *Micro-Moving Target IPv6 defense (μMT6D) for the IoT*
  - IPv6 shuffling.
  - Adapt MT6D to IoT. Implementation on IoT-OS Contiki 3.0, and simulations on Cooja using WisMote (CPU TI-MSP430; RF:TI-CC2520 2.4GHz).
  - 3 papers from Virginia Tech [5][6][7]
- *MTD for IoT Using Context Aware Code Partitioning and Code Diversification*
  - Secure server helps the IoT device: code only reside on the device when context dictates.
  - No implementation. Plans on testing on Drone controller (Pixhawk PX4).
  - One 2-page extended abstract at IEEE World Forum IoT 2016 [8].

MTD for IoT: Challenges

- Constrained nature of IoT, limits the MTD strategies practically feasible:
  - Constraint on the nodes: energy, cpu, flash, ram.
  - Constraint on the network: low-bandwidth, high packet-loss.
- Increased attack surface of IoT systems:
  - Radio communications (trivial eavesdropping, jamming).
  - Nodes are physically accessible (tampering, code extraction)
  - IoT topology may be fixed because of physical limitations (2.4 GHz).

MTD for IoT: working hypothesis

- Strong attacker assumptions: Insider attack will be studied.
- Work to achieve Software/Network-protocols (IMT expertise) tight interaction with hardware-cryptoprimitives (TUM expertise). The IoT node/MTD strategy can assume or define special HW properties.
- Simulation and evaluation of MTD strategies proposals is desired. Real IoT platform implementation.

Thesis Perspectives/Open questions

- MTD Strategies: Adapt current or define novel MTD strategies for IoT.
- Measurement: metrics, how to measure resilience of an IoT system?
- Explore other methods for IoT resilience improvement.
- Key enabling technologies:
  - Optimized security and communication protocols (IETF/IEEE sate of the art, and our new protocols).
  - Lightweight cryptography and Cryptoagility (easy to use new cryptoprimitives without changing the higher layer protocols)
- Implementation: define HW/SW platform (and use cases).

The End

Questions/Discussion?

Further Reading I

[1] G. Cai, B. Wang, W. Hu et al.
Moving target defense: state of the art and characteristics
Frontiers of Information Technology & Electronic Engineering, 2016.

[2] R. Zhuang, S. DeLoach, X. Ou
Towards a Theory of Moving Target Defense.
Proceedings of the First ACM Workshop on Moving Target Defense, 2014.

[3] Wang, L; Wu, D.
MTD-VirNet: A Moving Target Defense Architecture over Virtualized Networks.
Unpublished paper, 2017.

[4] S. Picek, E. Hemberg et al.
If You Can't Measure It, You Can't Improve It: Moving Target Defense Metrics
Proceedings of the 2017 Workshop on Moving Target Defense (MTD '17), 2017.

Further Reading II

[5] M. Sherburne; R. Marchany and J. Tront.
Implementing Moving Target IPv6 Defense to Secure 6LoWPAN in the Internet of Things and Smart Grid.
9th Annual Cyber and Information Security Research Conference CISR '14, 2014.

[6] K. Zeitz; M. Cantrell; R. Marchany and J. Tront.
Designing a Micro-Moving Target IPv6 Defense for the Internet of Things.
IoTDI, 2017.

[7] K. Zeitz; M. Cantrell; R. Marchany and J. Tront.
Changing the Game: A Micro Moving Target IPv6 Defense for the Internet of Things.
IEEE Wireless Communications Letters (Volume: PP, Issue: 99), 2018.

[8] K. Mahmood and D. Shila.
Moving Target Defense for Internet of Things Using Context Aware Code Partitioning and Code Diversification.
2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, 2016.