Lecture #9: IoT security in non-carpeted areas

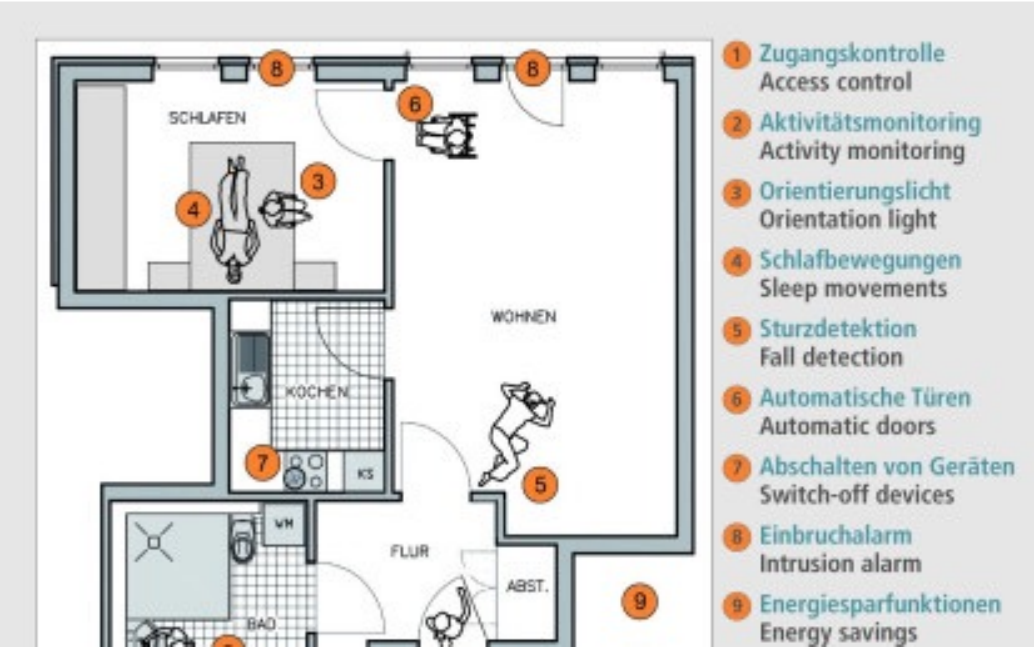
Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | June 9, 2021

Non-carpeted areas

UNIVERSITY OF TWENTE. SIDN LABS

The stuff one can do with carpets, though ;-)



https://archello.com/product/sensfloor

Today’s agenda

- Admin
- Introduction
- Paper #1: security in LoraWAN networks
- Paper #2: mapping Industrial Control Systems (ICSs)
- Feedback

Admin

Oral exams

Monday 28 June 2021

- Online through Canvas
- Signup through Canvas ‘Appointment’ (starting this afternoon)
- 45 minutes
- See: https://courses.sidnlabs.nl/ssi-2021/#oral-exam

Lab report progress

How far are you with the Lab report?

A. Developing methodology

B. Gathering network data from IoT devices

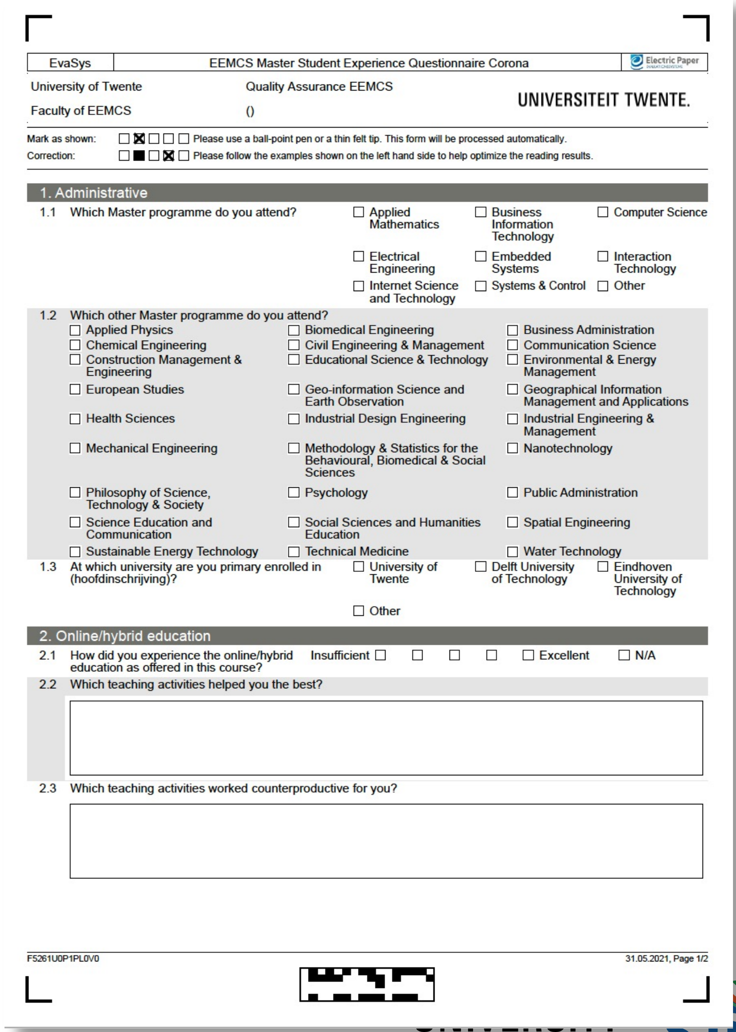
C. Analyzing network data from IoT devices

D. Writing report

Firm deadline: **Sunday June 20, 2020, 23:59 CEST**

Official feedback forms

- Survey by EEMCS Quality Assurance folks
- Will be sent out on June 10
- Closes on July 1
- Please fill it out, your feedback is **crucial** for us to further improve the course!
- Next year's students will thank you for it ;-)



EvaSys	EEMCS Master Student Experience Questionnaire Corona	Electric Paper

University of Twente — Quality Assurance EEMCS — UNIVERSITEIT TWENTE.

Faculty of EEMCS — ()

Mark as shown: ☐ ☒ ☐ ☐ ☐ Please use a ball-point pen or a thin felt tip. This form will be processed automatically.

Correction: ☐ ■ ☐ ☒ ☐ Please follow the examples shown on the left hand side to help optimize the reading results.

1. Administrative

1.1 Which Master programme do you attend?
☐ Applied Mathematics ☐ Business Information Technology ☐ Computer Science
☐ Electrical Engineering ☐ Embedded Systems ☐ Interaction Technology
☐ Internet Science and Technology ☐ Systems & Control ☐ Other

1.2 Which other Master programme do you attend?
☐ Applied Physics ☐ Biomedical Engineering ☐ Business Administration
☐ Chemical Engineering ☐ Civil Engineering & Management ☐ Communication Science
☐ Construction Management & Engineering ☐ Educational Science & Technology ☐ Environmental & Energy Management
☐ European Studies ☐ Geo-information Science and Earth Observation ☐ Geographical Information Management and Applications
☐ Health Sciences ☐ Industrial Design Engineering ☐ Industrial Engineering & Management
☐ Mechanical Engineering ☐ Methodology & Statistics for the Behavioural, Biomedical & Social Sciences ☐ Nanotechnology
☐ Philosophy of Science, Technology & Society ☐ Psychology ☐ Public Administration
☐ Science Education and Communication ☐ Social Sciences and Humanities Education ☐ Spatial Engineering
☐ Sustainable Energy Technology ☐ Technical Medicine ☐ Water Technology

1.3 At which university are you primary enrolled in (hoofdinschrijving)?
☐ University of Twente ☐ Delft University of Technology ☐ Eindhoven University of Technology
☐ Other

2. Online/hybrid education

2.1 How did you experience the online/hybrid education as offered in this course? Insufficient ☐ ☐ ☐ ☐ ☐ Excellent ☐ N/A

2.2 Which teaching activities helped you the best?

2.3 Which teaching activities worked counterproductive for you?

F5261U0P1PL0V0 — 31.05.2021, Page 1/2

Interactive lectures

- Overall objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the oral exam

- Interactive format
  - Teachers summarize two papers per lecture
  - Multiple-choice questions (not graded) and discussion
  - We ask at least one of you to share their thoughts on each paper (main lesson learned, etc.)
  - Enables you to learn from each other, so mandatory to participate

- **A 7th "re-sit" lecture in case you miss a lecture (optional for everybody else), same format**

UNIVERSITY OF TWENTE. SIDN LABS

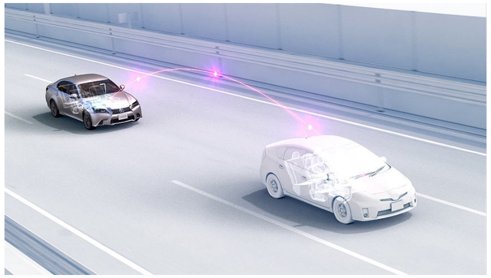
Where are we now?

No.	Date	Contents
1	Apr 21	Course introduction Guest lecture #1: how the core of the internet is organized, Marco Davids (SIDN Labs)
2	Apr 28	Guest lecture #2: the relationship between regulation & IoT security, Eelco Vriezekolk, Agentschap Telecom (Dutch telecoms regulator)
3	May 6*	Lecture: IoT Concepts and Applications
4	May 12	Lecture: IoT Botnet Measurements
5	May 18	Lecture: IoT Honeypots
6	May 25*	Guest lecture #3: The Life Of An IoT Device, Eliot Lear, Cisco Systems
7	May 26	Lecture: IoT Edge Security Systems
8	Jun 2	Lecture: IoT Device Behavior
9	Jun 9	Lecture: IoT security in Non-Carpeted Areas
10	Jun 16	Lecture: IoT Edge Security Systems (re-sit)

* Different lecture times/days. Default slot: Wednesdays 11:00 - 12:45

Introduction

Motivation for today: IoT is more than the home



UNIVERSITY OF TWENTE.

SIDN LABS

Discussion: other IoT/ICS applications?

What other IoT/ICS applications do you envision?

Today's papers

[Lora] X. Wang, E. Karampatzakis, C. Doerr, and F.A. Kuipers, "Security Vulnerabilities in LoRaWAN", Proc. of the 3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, Florida, USA, April 17-20, 2018

[ICS] Li, Q., Feng, X., Wang, H., & Sun, L. (2018). Understanding the Usage of Industrial Control System Devices on the Internet. IEEE Internet of Things Journal, 5(3), 2178–2189. doi:10.1109/jiot.2018.2826558

Today’s learning objective

- After the lecture, you will be able be able to discuss technologies for non-consumer IoT applications (“non-carpeted areas”), specifically
  - Security vulnerabilities of LoraWAN and their mitigations
  - Measurement techniques to detect ICS systems that are connected to the Internet but shouldn’t

- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Paper #1: “Security Vulnerabilities in LoRaWAN”, 3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, Florida, USA, April 17-20, 2018

UNIVERSITY OF TWENTE.

SIDN LABS

LoraWAN: low power, wide area, low bitrate comms

LoraWAN temperature sensor

Modbus-over-LoraWAN bridge

LoraWAN gateway

UNIVERSITY OF TWENTE.
SIDN LABS

Quiz: warming up

What classical definition of security does the paper use?

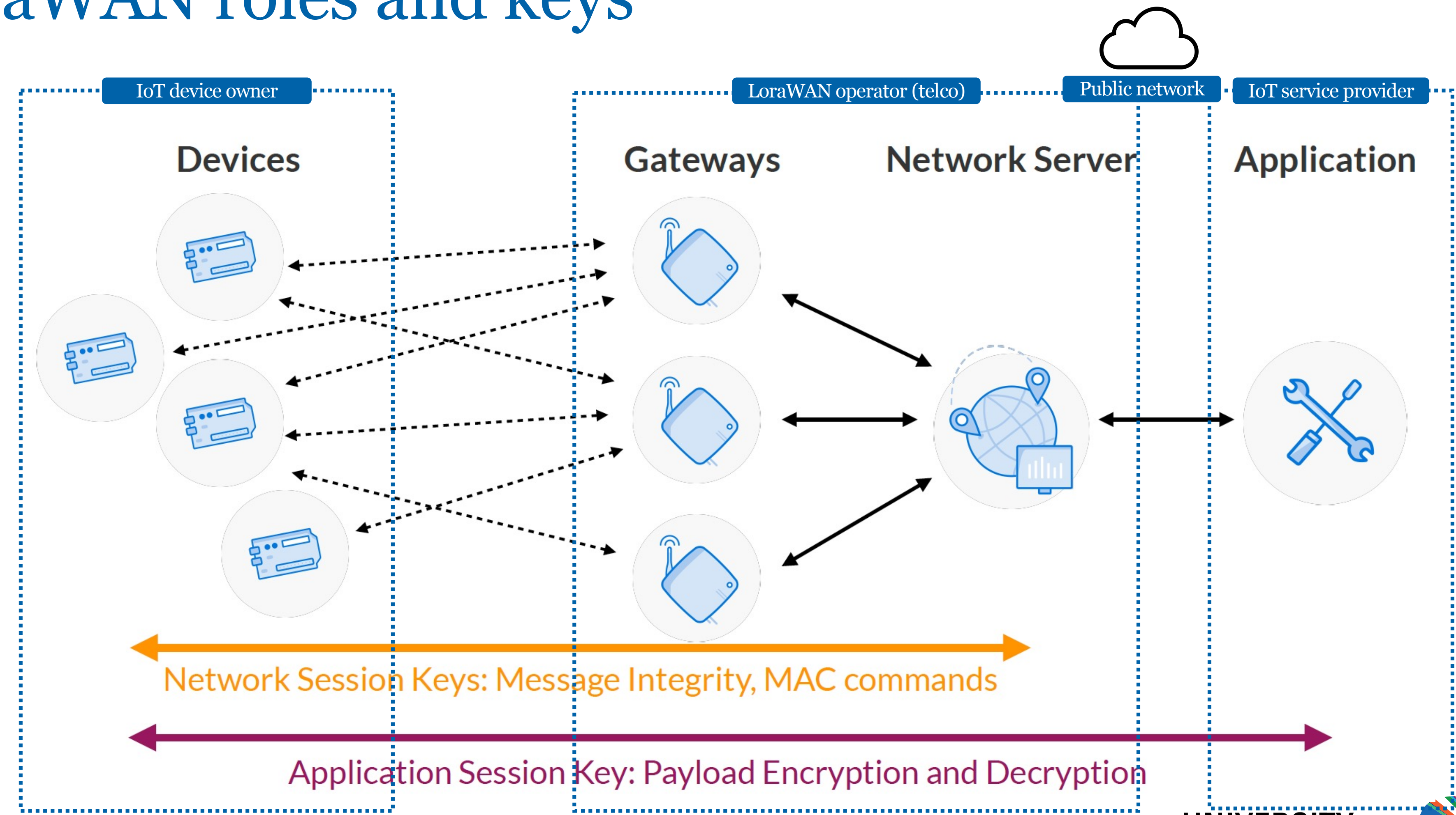
A. Communication, Information, and Authority

B. Confidentiality, Integrity, and Availability

C. Authentication, Authorization, and Accounting

D. Stability, Resilience, and Transparency

LoraWAN roles and keys



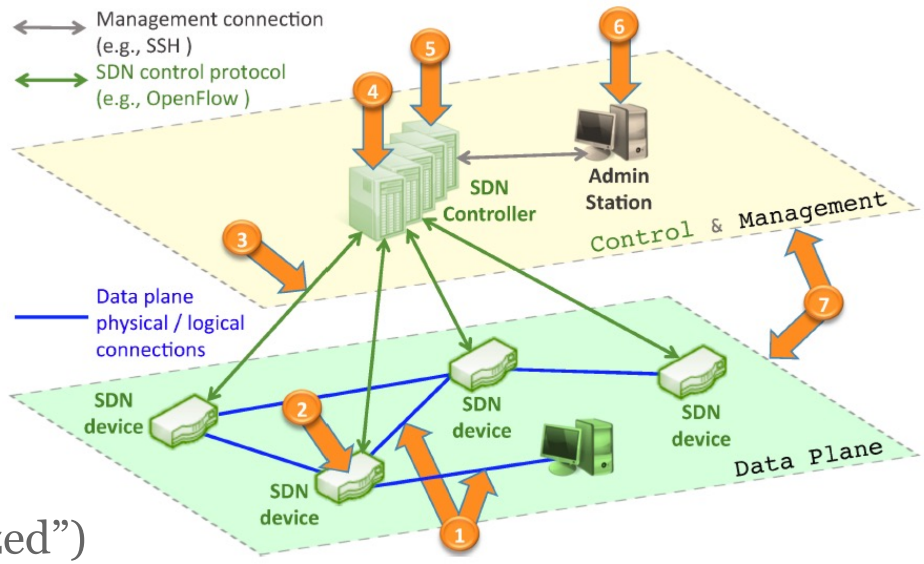
Picture: Johan Stokking, The Thing Industries

UNIVERSITY OF TWENTE. SIDN LABS

Key security functions

- Data plane (packet forwarding)
  - Encryption of LoraWAN payloads
  - Message integrity verification
  - Replay protection

- Management plane
  - Key derivation (symmetric)
  - Device enrollment protocol (OTA and "personalized")
  - Over the air firmware updates



Source: D. Kreutz, F. M. V. Ramos, P. Verissimo, HotSDN'13, August 16, 2013, Hong Kong, China.

UNIVERSITY OF TWENTE. SIDN LABS

Research based on older LoraWAN spec

- January 2015: 1.0
- February 2016: 1.0.1
- **July 2016: 1.0.2**
- October 2017: 1.1, adds Class B
- July 2018: 1.0.3
- October 2020: 1.0.4

Quiz: over-the-air activation

What's the root of trust in OTAA mode?

A. AppSKey

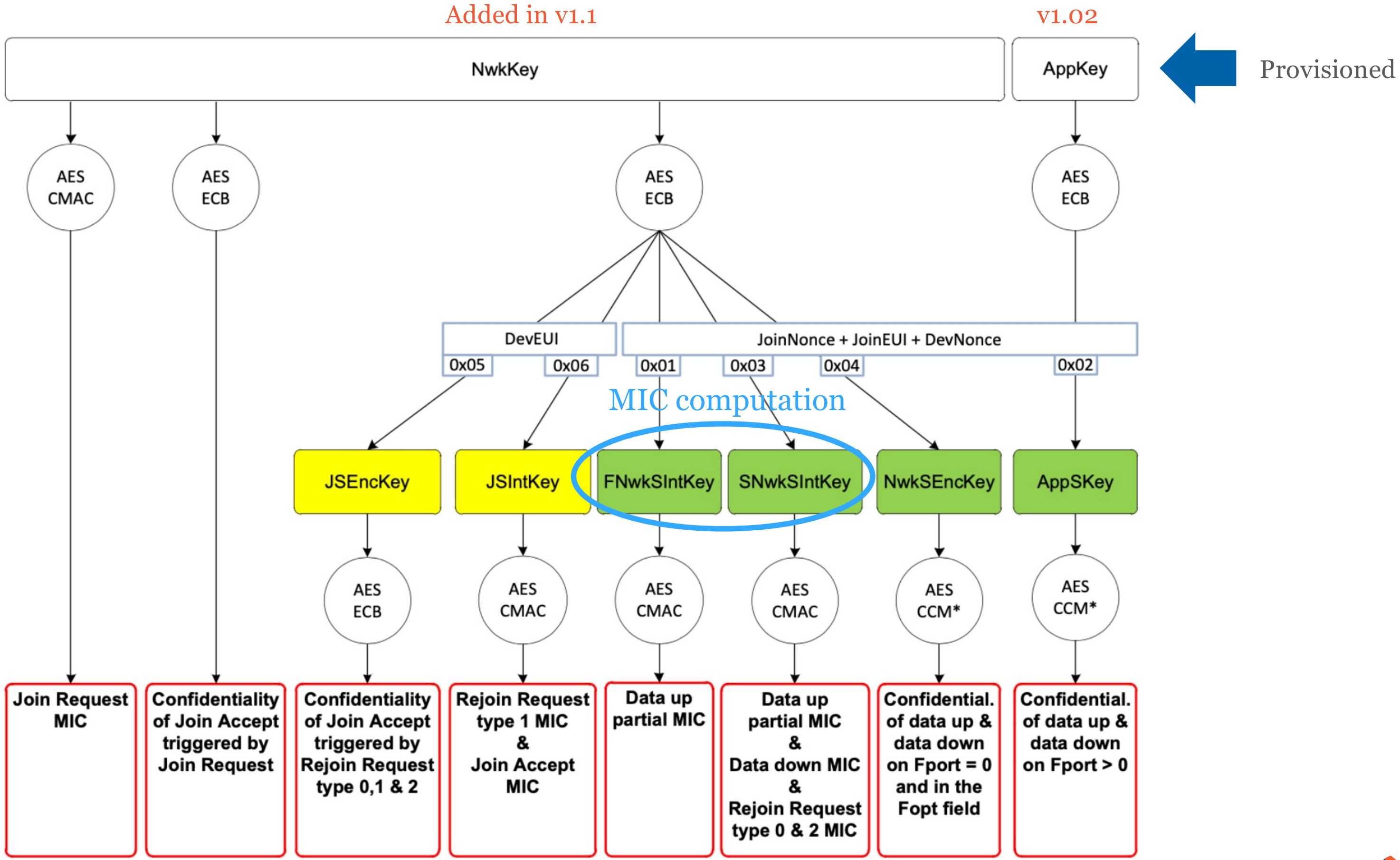
B. NwkSKey

C. AppKey

D. NwkKey

LoraWAN key derivation

v1.1: logical separation between network and application operator



Picture: Johan Stokking, The Thing Industries

Denial of Service through replay

Injected message

time	counter	port	dev id	
16:16:00	13	6	22	34 34 37 20 30 32 34 00
16:15:25	12	61	22	34 39 36 20 30 32 34 00
16:14:51	11	20	22	35 34 33 20 30 32 31 00
16:08:49	10	49	22	34 38 30 20 30 32 31 00
16:08:34	0	71	22	31 39 32 20 30 32 32 00
16:07:59	10	49	22	34 38 30 20 30 32 31 00
16:06:16	7	41	22	35 32 37 20 30 32 33 00
16:05:42	6	61	22	36 38 37 20 30 32 34 00
16:05:07	5	134	22	34 39 34 20 30 32 33 00
16:03:59	3	83	22	34 34 38 20 30 32 32 00

Fig. 7. Log file of the victim's server.

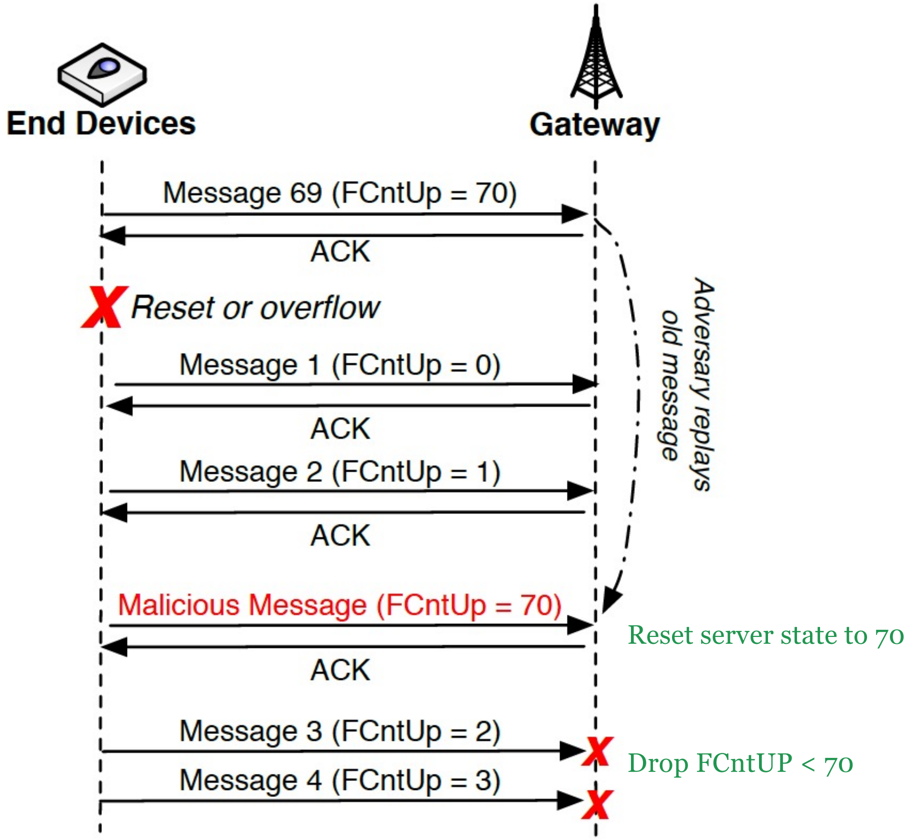


Fig. 4. An example of a replay attack for ABP.

UNIVERSITY OF TWENTE.

DACS LABS

Quiz: eavesdropping

What’s the root cause of the eavesdropping attack?

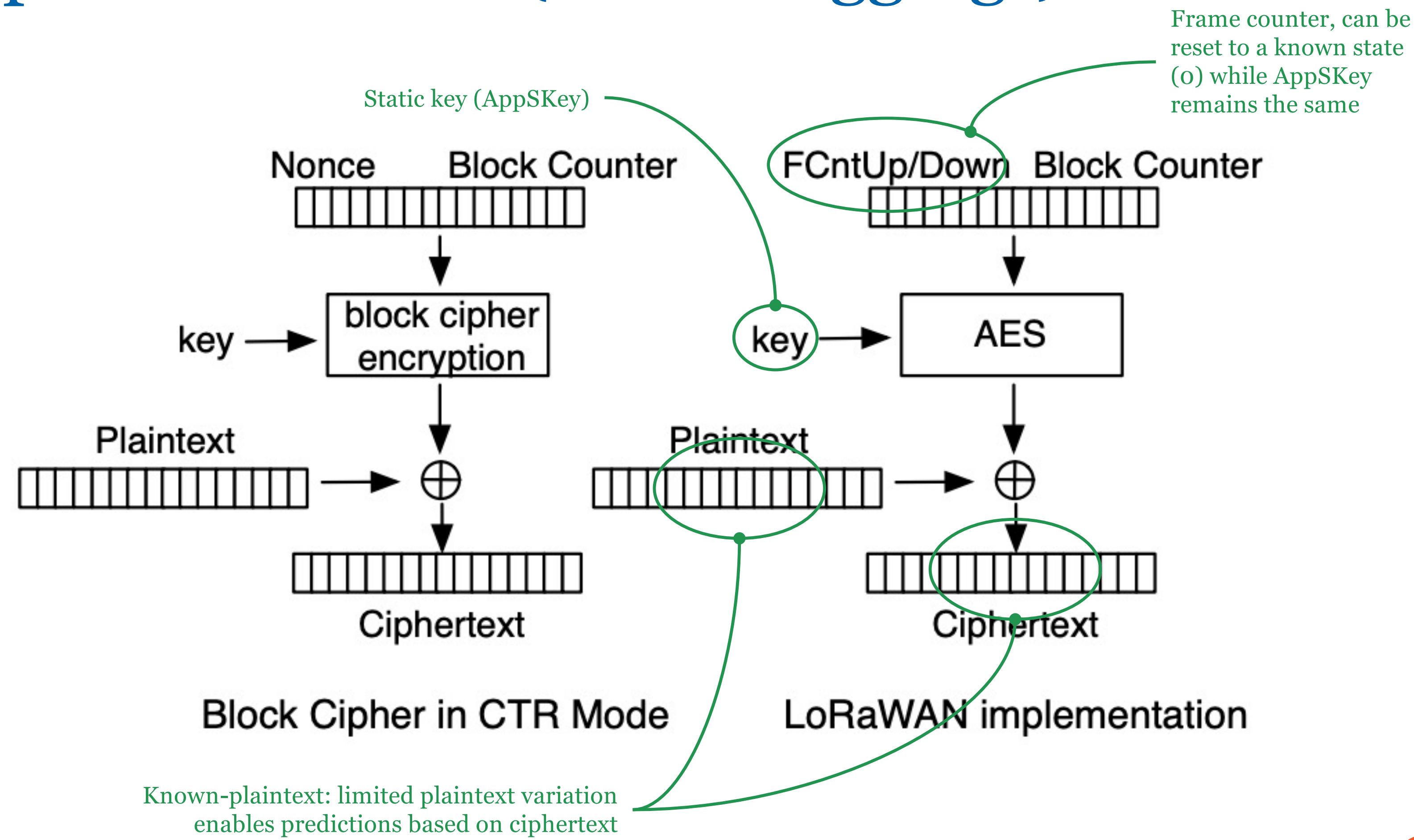
A. LoraWAN nodes use message counters as the encryption nonce

B. LoraWAN nodes use limited payload sizes

C. LoraWAN nodes use known formats for their messages

D. LoraWAN nodes use a block cipher in counter mode

Known-plaintext attack ("crib dragging")



https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
https://en.wikipedia.org/wiki/Known-plaintext_attack

Quiz: message integrity

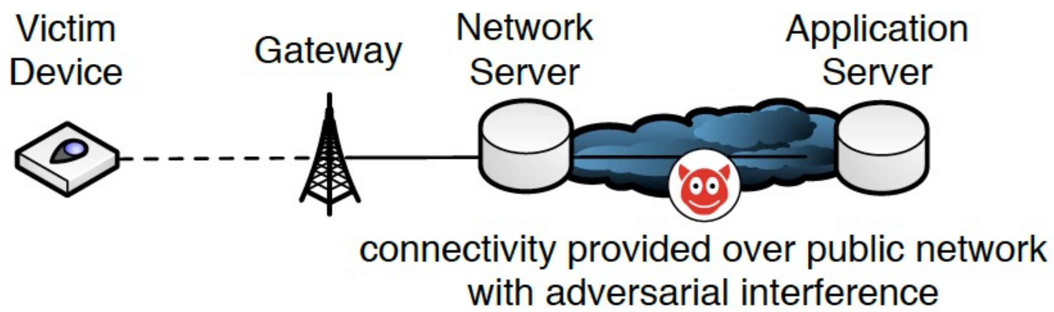
Why does LoraWAN not support end-to-end message integrity?

A. LoraWAN is a link-level technology

B. LoraWAN messages are encrypted

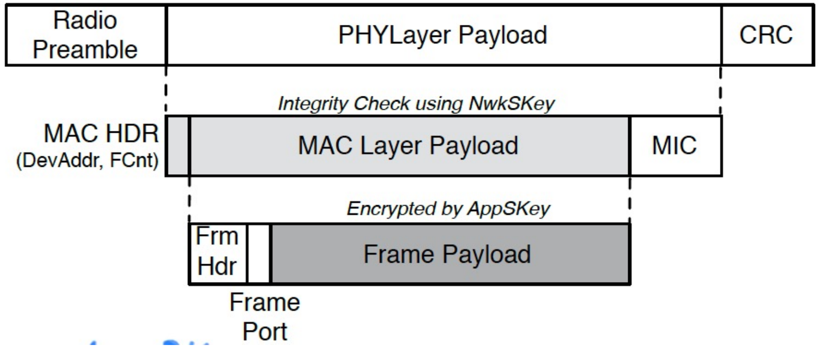
C. LoraWAN does not support application-level MICs

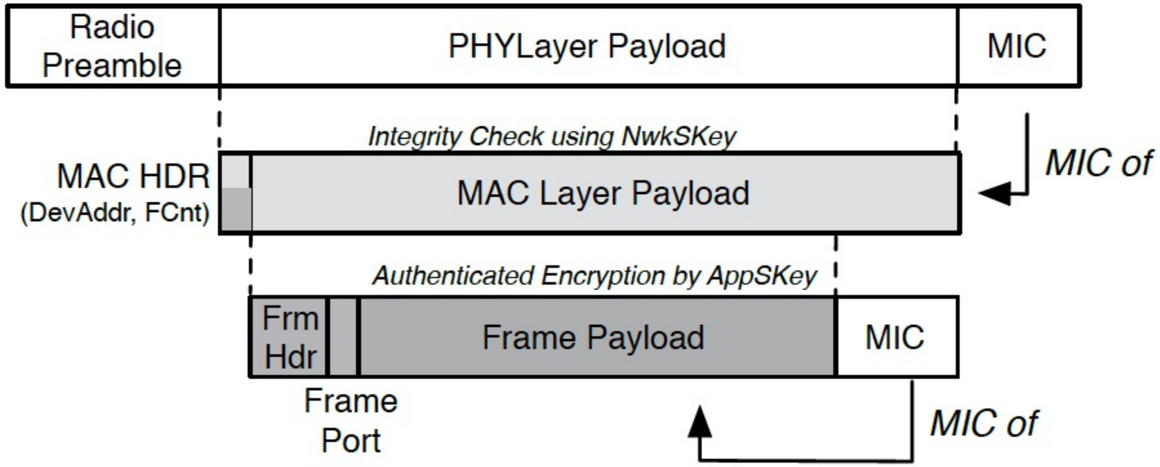
D. LoraWAN devices cannot be compromised



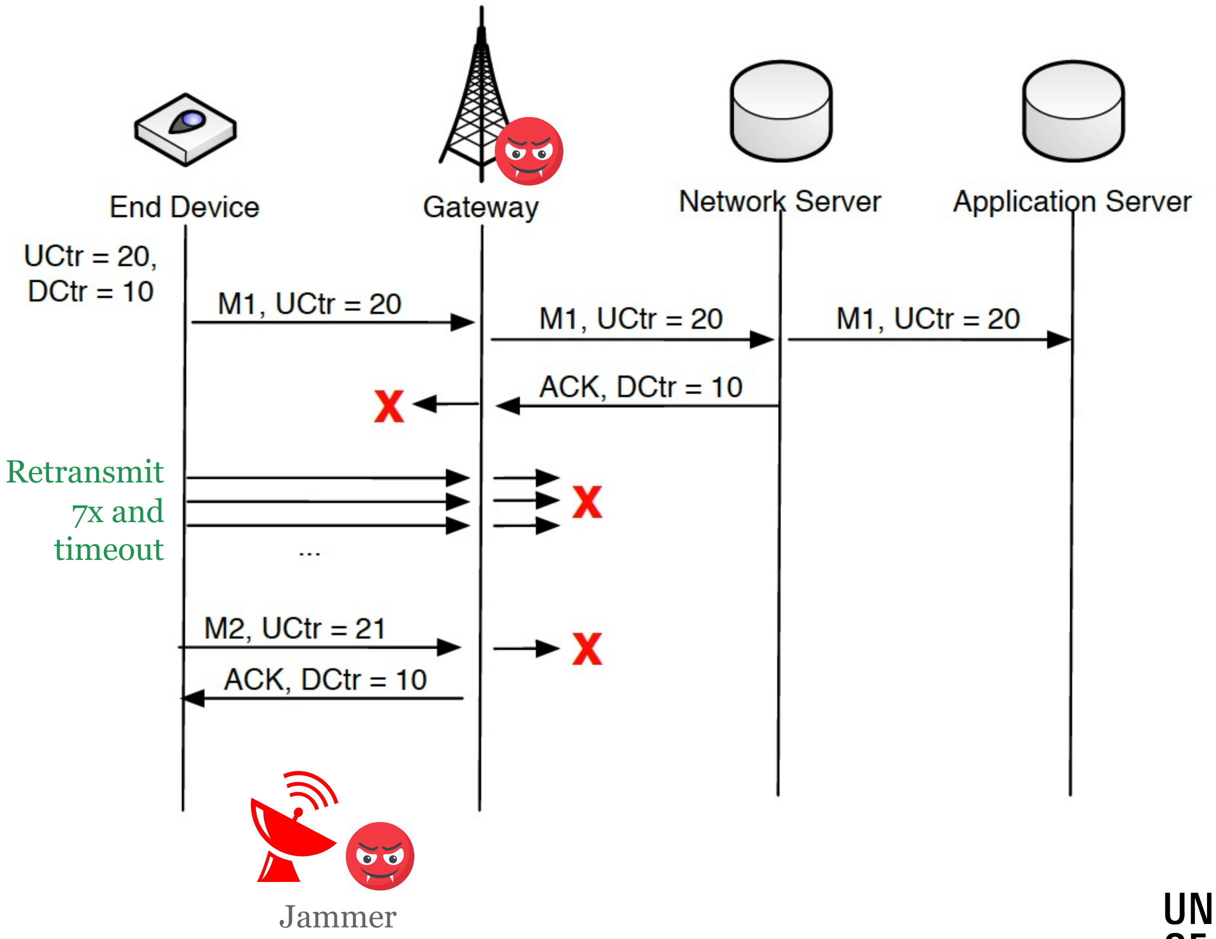
UNIVERSITY OF TWENTE. SIDN LABS

Proposed solution: 2 MICs





ACK spoofing: ack'ing other frames than original



UNIVERSITY OF TWENTE.

SIDN LABS

Quiz: ACK spoofing

The fundamental problem with the ACK spoofing attack is that ACKs do not indicate which specific uplink message they confirm. How do the authors propose to extend ACK messages to tackle this problem?

A. Include a nonce signed by the gateway's private key

B. Include the frame counter value of the uplink message

C. Include cryptographic checksum that covers the uplink packet

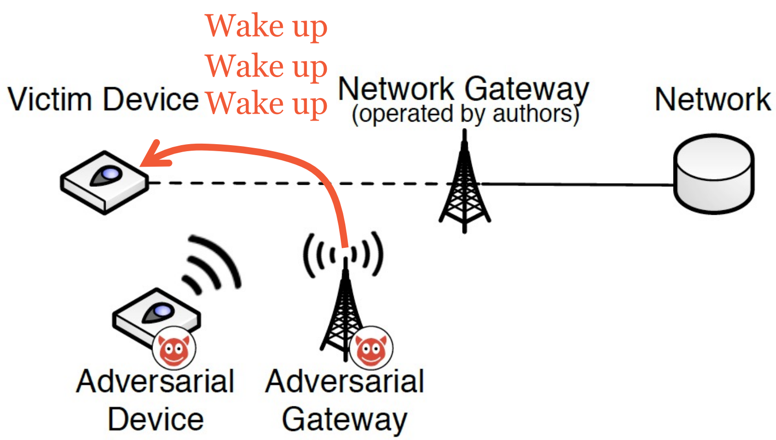
D. Accept the risk because adding more info to ACKs would be too expensive

Key takeaways

- Designing network security protocols is challenging

- Many different corner cases that folks will try to exploit

- My “favorite” attacks
  - Content guessing based on typical packet content (small messages, known data formats, etc.)
  - Remote battery draining



UNIVERSITY OF TWENTE. SIDN LABS

Discussion

- What would you do to better in the development process to make LoraWAN more secure?
  - IETF-like standardization?
  - Formal verification?
  - Open-source implementation?
  - …

Paper #2: “Understanding the Usage of Industrial Control System Devices on the Internet”, IEEE Internet of Things Journal

UNIVERSITY OF TWENTE. SIDN LABS

Key Concept: ICS exposure on the Internet

UNIVERSITY OF TWENTE.

Two major pitfalls in a large scale scan

- Honeypots

  addressed by using a Naive Bayes classifier

- Dynamic IP addresses

  other features used as a device identifier

Discussion Question #1

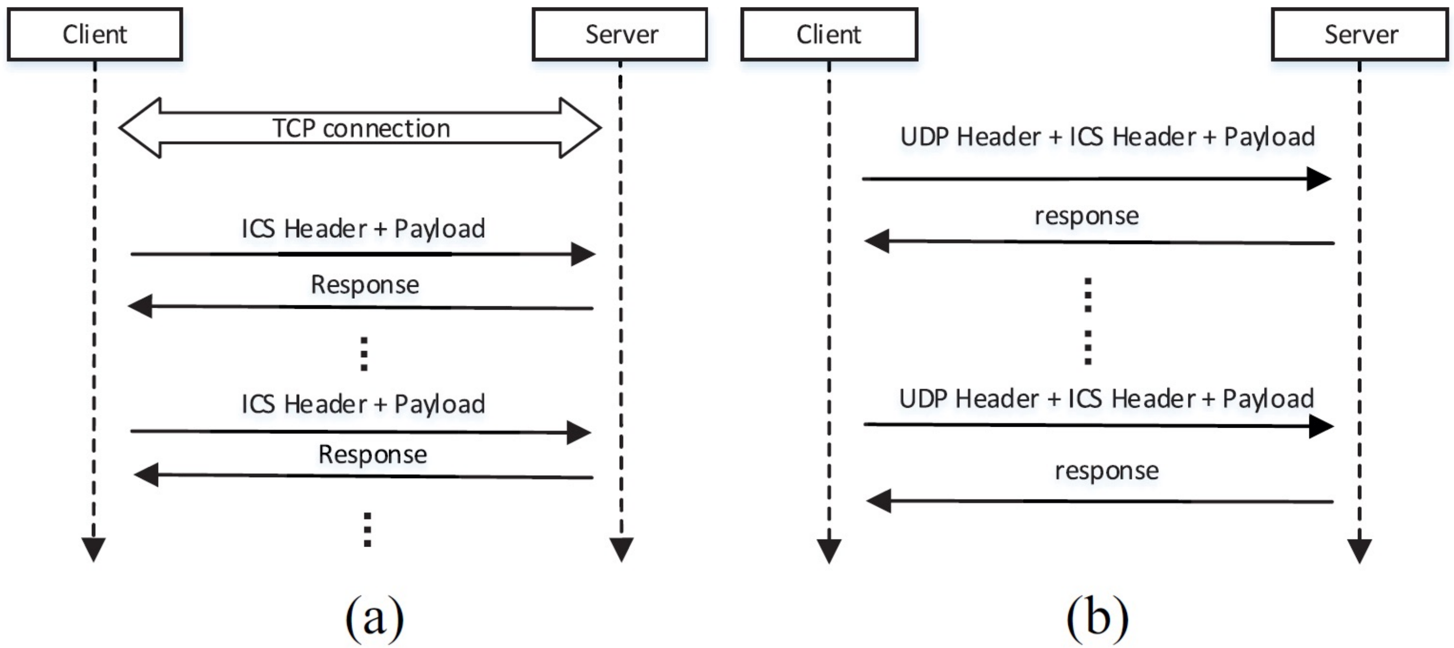
What other issues can you think of when running an Internet-wide scan?

Basics Considerations

- One stateless packet to detect live hosts in IPv4
- A learning model to reduce the number of honeypot detection queries
- Dynamic IPs addressed using extra identifiers

ICS Communication Interactions

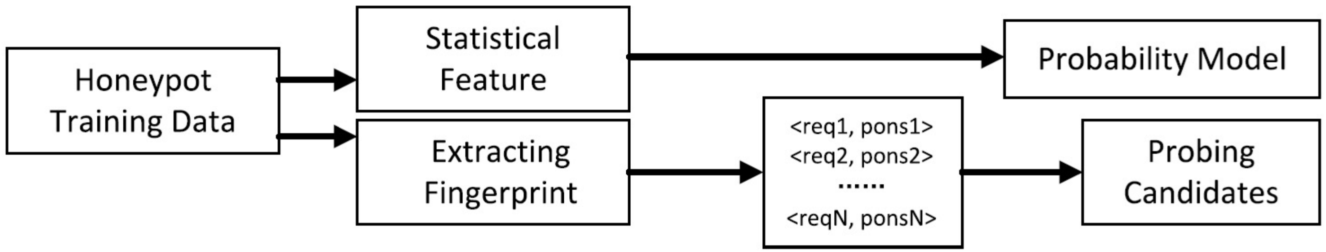
TCP vs UDP communication model



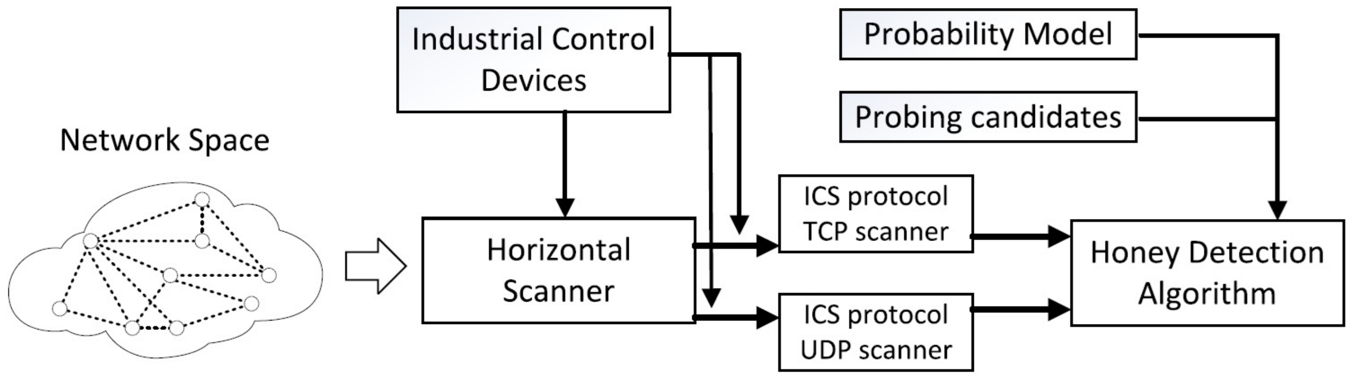
UNIVERSITY OF TWENTE. SIDN LABS

Device Discovery Architecture

- Offline training phase



- Online discovery phase



UNIVERSITY OF TWENTE.

Fingerprinting Honeypots (1/2)

- “Honeypot detection is straightforward because they are merely simulations of networking services and have their implementation details.”

- Naive Bayes classification:

$$p(y|X) \propto p(y)p(X|y)$$

$$p(X|y) = \prod_{x_i \in X} p(x_i|y)$$

$$p(x_i|y) = \frac{p(x_i \cap y)}{p(y)}$$

$$p(x_i \cap y) = \frac{N_{x_i \cap y}}{N_{total}}$$

- If $p(y|X)$ bigger than a threshold S_{th} then verify at the next stage.

Fingerprinting Honeypots (2/2)

Algorithm 1 Fingerprint Generation

Input: different kinds of ICS honeypot fingerprints, $F = \{f_1, \ldots, f_N\}$, every f_i has a accuracy R_i

Output: final fingerprint used to identify honeypots, F_{final}

for (each $f_i = \{(p_1, r_1), \ldots, (p_i, r_i), \ldots, (p_N, r_N)\}$ in F) **do**

$$T_i = \sum_{i=1}^{N} cost(p_i, r_i)$$

heuristic criterion: $H = \{h_1, h_2, \ldots, h_N\}$, $h_i = \frac{R_i}{T_i}$

Sort(H)

choose the lowest-cost top K C_i and its related f_i

generate final F_{final}

end for

Online Detection

Algorithm 2 Online Detection of ICS Devices

Input: The list of the detection range, *list*;
Output: The list of ICS devices, $list'$;

Using a random algorithm to resort the $list^r = list$;
for (each IP in $list^r$) **do**
    send one packet
    each packet with stateless
    add each live host into $list'$
end for
for (each IP in $list'$) **do**
    using ICS protocols verifies it
    add the quantified host into $list'$
end for
for (each IP in $list'$) **do**
    if ($p(y_i|X) > S_{th}$) **then**
        send packet with packets *FF* with Algorithm 1.
        if (get its responses & match the fingerprint) **then**
            add it into $list_{honeypots}$, remove it from $list'$
        end if
    end if
end for

UNIVERSITY OF TWENTE.
SIDN LABS

Quiz

Which feature wasn't used to identify a unique ICS device?

A: Country

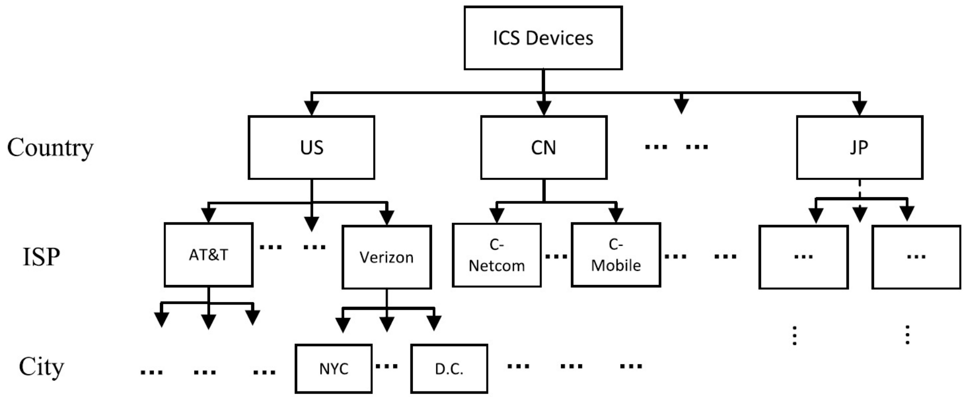
B: City

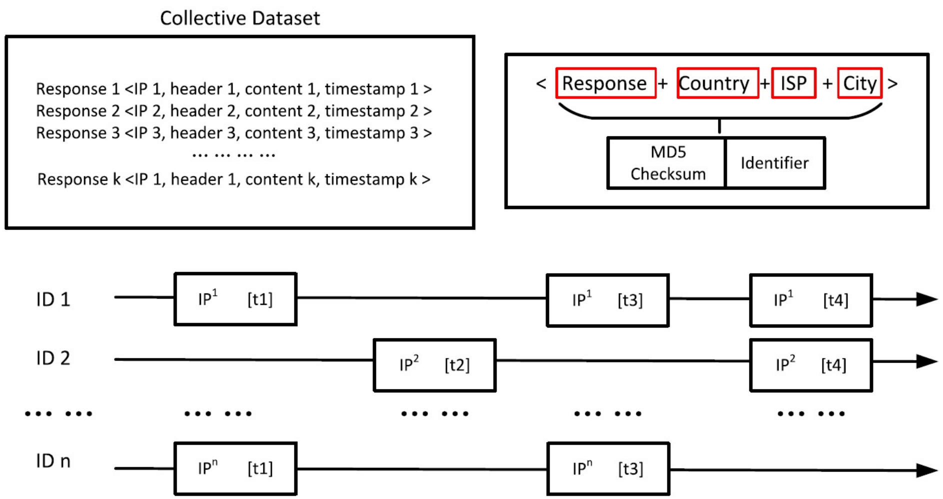
C: ASN

D: ISP

E: Response packet

Device Identifiers





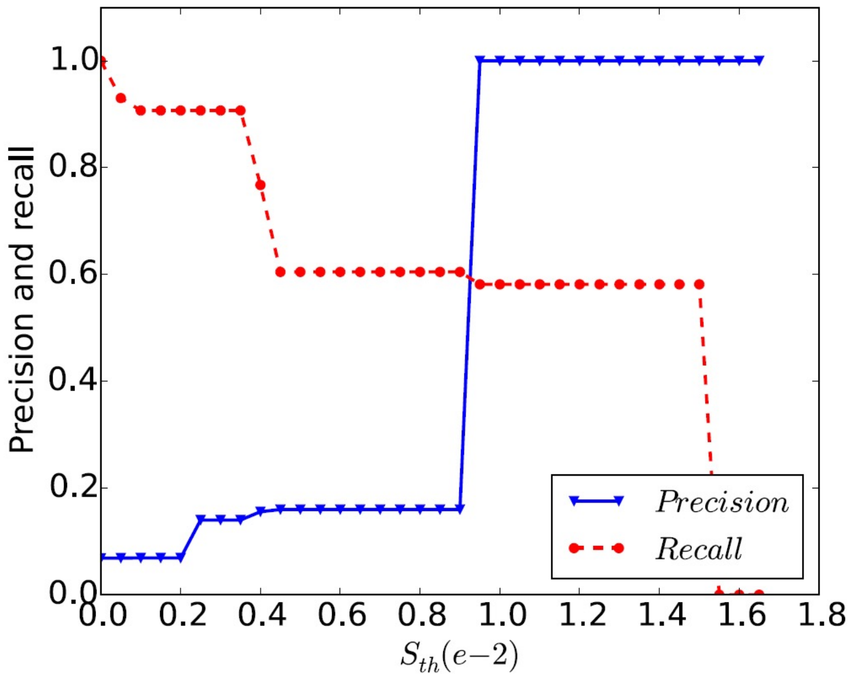
UNIVERSITY OF TWENTE. SIDN LABS

Evaluation

- Honeypot detection
- ICS device detection
- Dynamic IP and device identifier

Honeypot detection

- A random /16 (65536 IP addresses)
- Manually determine ICS vs honeypots
- In total 617 responsive hosts (575 real devices and 42 honeypots)
- Split into training and test datasets



- How reliable is this (manually labeling devices vs honeypots)?

UNIVERSITY OF TWENTE. SIDN LABS

Honeypot Fingerprinting

- Conpot (a typical ICS honeypot) is used for verification
- Four features (#open ports, HTTP config, Modbus, S7 signal code)

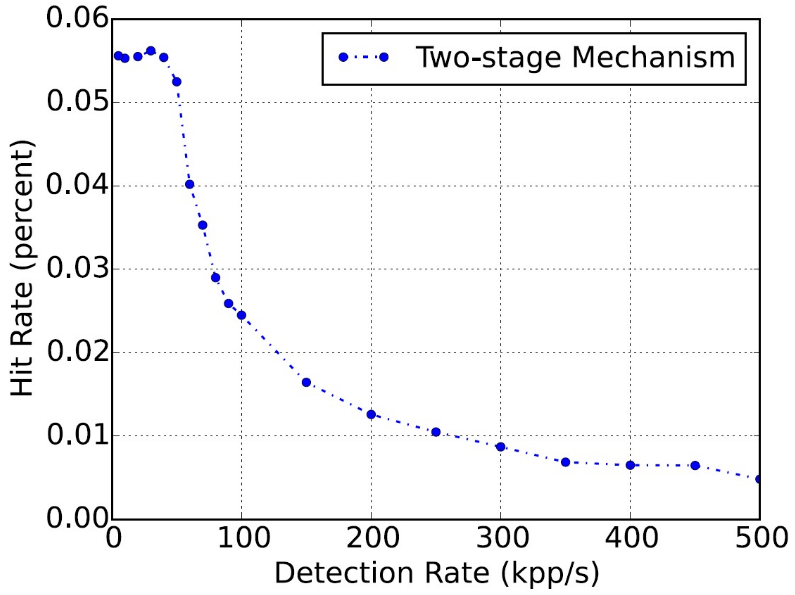
TABLE II
COST AND RELATIVE DEGREE OF FEATURES

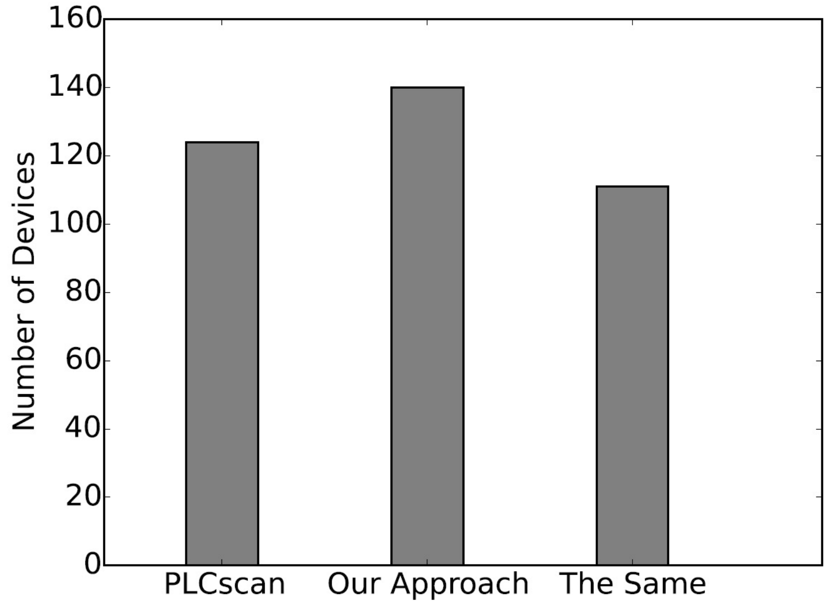
Features	Cost (packet)	Relative degree
Amount of open ports	6	26/297
HTTP configuration	4	9/297
Modbus signal code	5	15/297
S7 signal code	9	15/297

TABLE III
COMPARISON BETWEEN OUR GENERATED FINGERPRINTS AND TRADITIONAL FINGERPRINTS

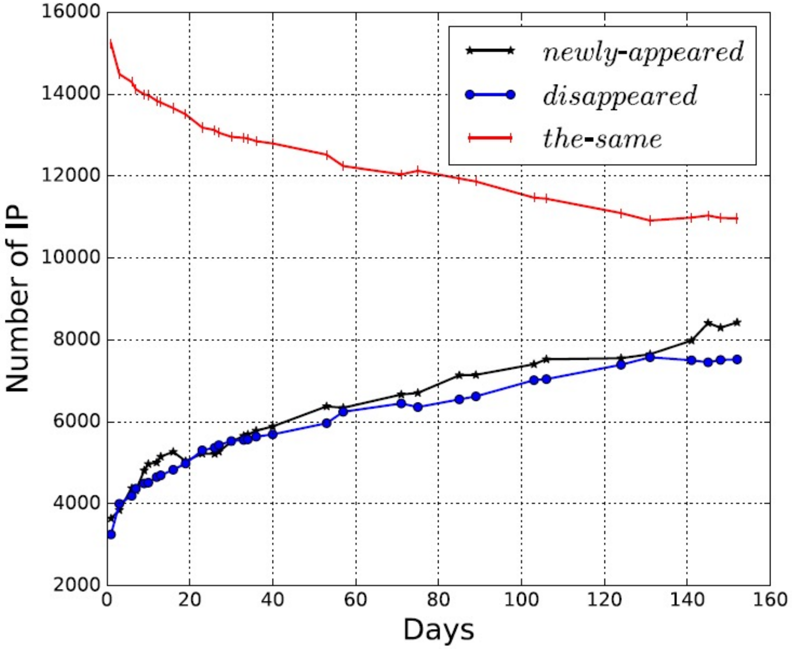
	Cost (every host)	Accuracy
Traditional fingerprint	20+ packets	100%
Our generated fingerprint	5 packets	95.2%

ICS Device Detection

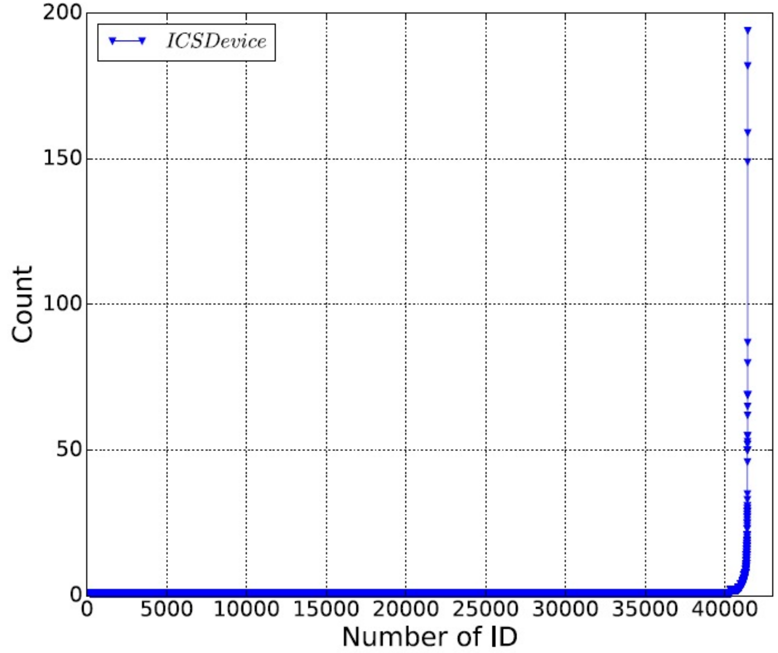




Dynamic IP and Device ID



Modbus
August 2015 - March 2016



S7, Modbus, Tridium Niagara Fox and BACnet
October 2015

UNIVERSITY OF TWENTE. SIDN LABS

ICS Lookup using Shodan

Shodan.io

/explore

/category

/industrial-control-systems

TOTAL RESULTS

39,251

TOP COUNTRIES

United States	8,054
China	2,584
France	2,468
Israel	1,983
Taiwan	1,909

More...

TOP ORGANIZATIONS

Amazon Technologies Inc.	2,359
Amazon.com, Inc.	2,353
Internet Rimon	1,526
Chunghwa Telecom Co.,Ltd.nNo.21-3, Sec. 1, Xinyi Rd., Taipei 10048, Taiwan, R.O.C.nTaipei Taiwan	1,509
Viettel Group	751

More...

UNIVERSITY OF TWENTE.

SIDN LABS

Discussion

- Would you propose a different identifier than one in the paper to overcome dynamic IPs?
- How realistic is the honeypot fingerprinting method?

Key takeaways

- Device discovery as the first step of security analysis is more sensitive in this context due to ICS device nature

- Honeypot detection might not be as straight forward as the authors of this paper claim

- Device identifiers (if properly chosen) are a promising metric to overcome dynamic IP addresses

Feedback

Today’s objective revisited

- After the lecture, you will be able be able to discuss technologies for non-consumer IoT applications (“non-carpeted areas”), specifically
  - Security vulnerabilities of LoraWAN and their mitigations
  - Measurement techniques to detect ICS systems that are connected to the Internet but shouldn’t

- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Lecture feedback

1. To what extent do you think you'll be able to discuss security vulnerabilities of LoraWAN and their mitigations? (A = 🟢, B = 🟠, C = 🔴)

2. To what extent do you think you'll be able to discuss measurement techniques to detect Internet-connected ICS systems (A = 🟢, B = 🟠, C = 🔴)

UNIVERSITY OF TWENTE. SIDN LABS

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion & feedback

Next lecture: **Wed Jun 16 (resit), 11:00-12:45**
Topic: IoT edge security systems II

UNIVERSITY OF TWENTE.

SIDN LABS