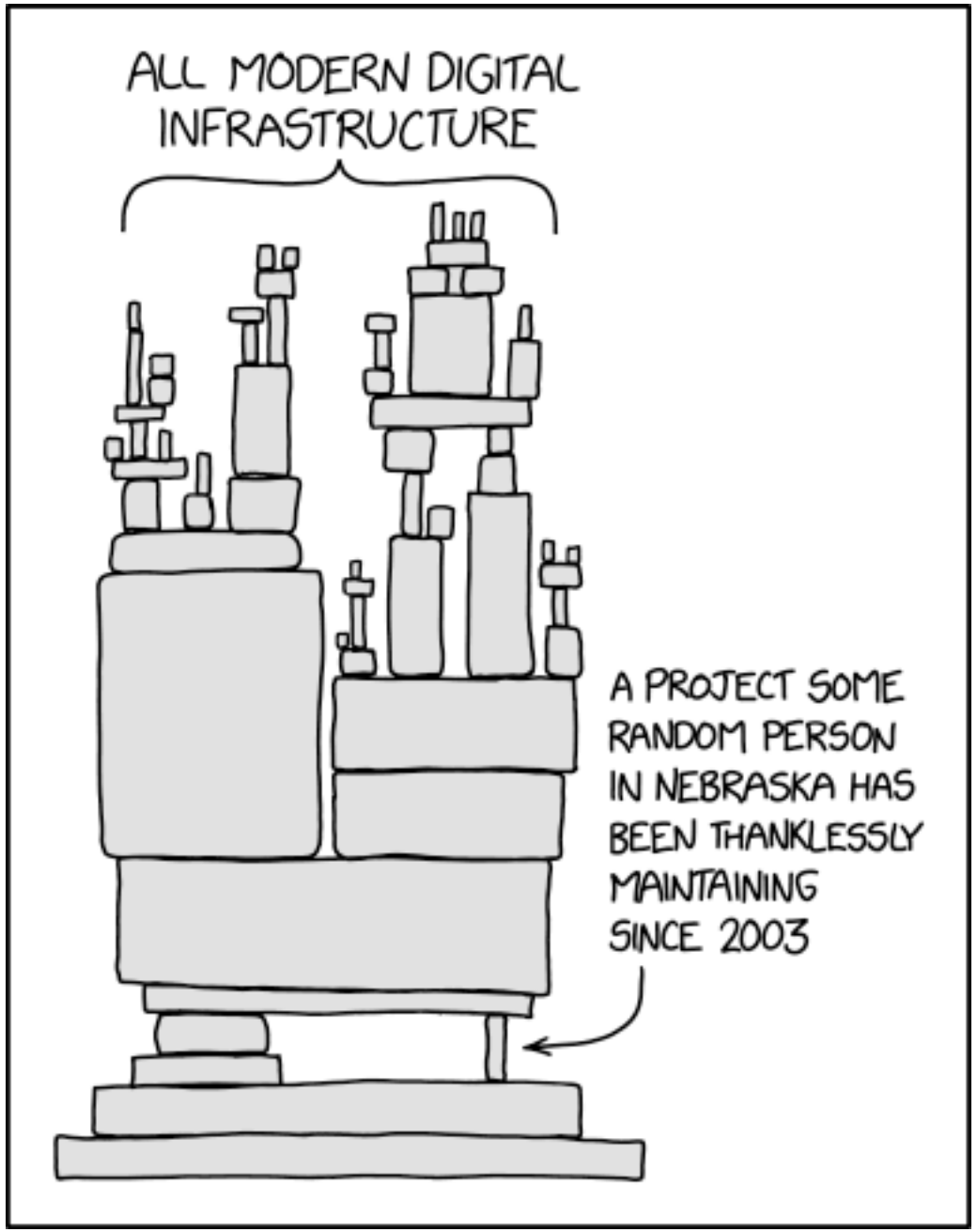
Lecture #6: IoT security vulnerabilities

Antonia Affinito, Etienne Khan, Pascal Huppert, Ting-Han Chen, and Cristian Hesselman

University of Twente | June 13, 2025

UNIVERSITY OF TWENTE.

SIDN LABS



UNIVERSITY OF TWENTE.

SDN LABS

Today's agenda

- Admin
- Introduction to today's lecture
- Paper #1: security in LoraWAN networks
- Paper #2: coordinated vulnerability disclosure for the IoT
- Feedback

Admin

Schedule

Lecture	Date	Contents
R1	Apr 25	Course Introduction
G1	Apr 30	How the core of the Internet works.
R2	May 9	Principles of IoT security
R3	May 16	Internet Core Protocols
R4	May 23	IoT Botnet Measurements
R5	May 27	IoT TLS and Q&A lab assignment
G2	Jun 6	IoT and post-quantum crypto
R6	Jun 13	IoT Security Vulnerabilities
R7	**Jun 18**	IoT Forensics

UNIVERSITY OF TWENTE.

SDN LABS

Important dates 

- All summaries due: **Fri Jun 20**

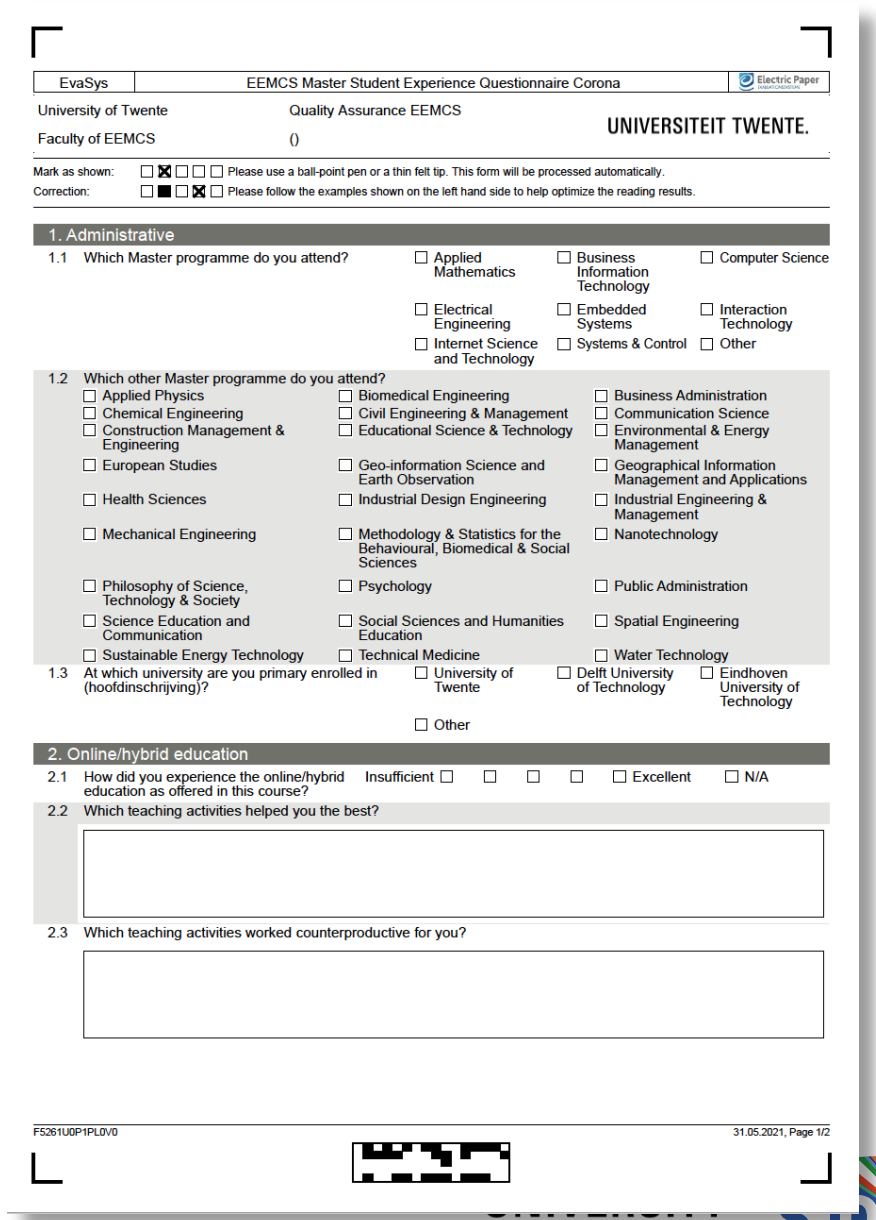
- Written exam: **Mon Jun 23**

- Slides (PDF), PCAP, MUD, README files due: **Wed Jun 25, 9AM CEST**

- Presentations:
  - **Fri June 27**, from 8:45 to 12:30 in NH 115 and NH 124
  - **Mon June 30**, from 8:45 to 12:30 in NH 115 and NH 124

Official feedback forms

- Survey by EEMCS Quality Assurance folks
- Will be sent out on in the next week or so
- Please fill it out, your feedback is **crucial** for us to further improve the course!
- Next year's students will thank you for it ;-)
- We'll let you know how we handled your feedback



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

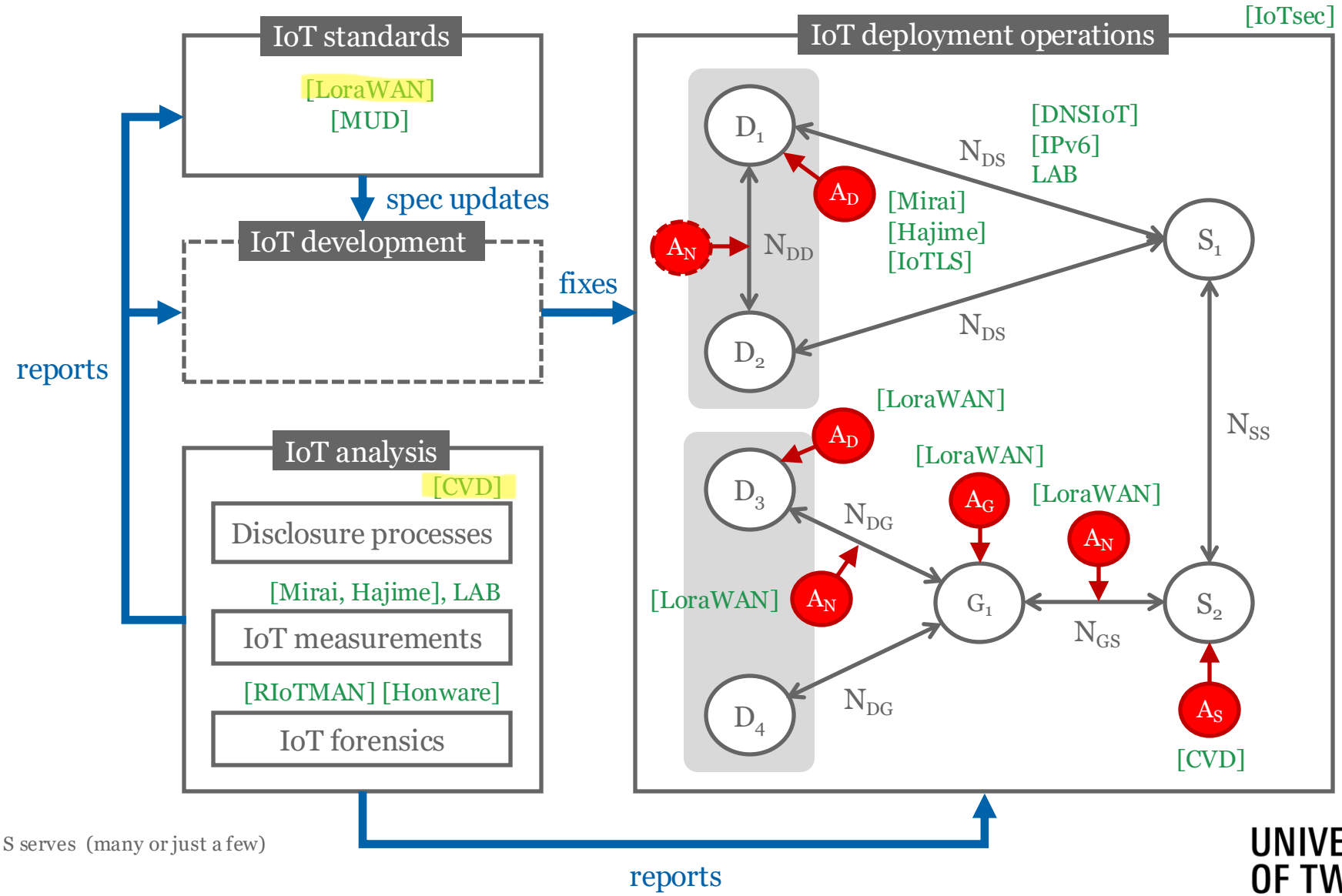
Introduction to today's lecture

How to fix security vulnerabilities?

- Types of IoT vulnerabilities
  - Design decisions
  - Software/firmware or config errors

- How to fix them?
  - Step 1: find vulnerabilities, such as through scanning, Shodan, testing
  - Step 2: fix them through patches or redesign/re-spec
  - Proactive or reactive

SSI covers different parts of the IoT ecosystem



A = attack
N = network
D = device
S = server
D(S) = devices that S serves (many or just a few)

UNIVERSITY OF TWENTE.

SDN LABS

So that's why we selected today's papers for you

Design decisions:

[LoraWAN] 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

Disclosure processes:

[CVD] T.-H. Chen, C. Tagliaro, M. Lindorfer, K. Borgolte, and J. Van Der Ham-De Vos, "Are You Sure You Want To Do Coordinated Vulnerability Disclosure?", 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 307–314, IEEE, April 2024

Today's learning objective

- After the lecture, you will be able to discuss IoT security design vulnerabilities and vulnerability disclosure processes

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

“Security Vulnerabilities in LoRaWAN”

3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, Florida, USA, April 17-20, 2018

Old but **gold** ⭐

UNIVERSITY OF TWENTE.

SDN LABS

Get your phones ready!

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
QXLMYR

Enable answers by SMS

UNIVERSITY OF TWENTE.

SIDN LABS

What struck you about the paper?

LoraWAN: low-power, wide-area network, low bitrate

UNIVERSITY OF TWENTE.

SDN LABS

Deutsche Bahn is using LoraWAN, too

https://www.thethingsindustries.com/stories/deutsche-bahn/
https://www.youtube.com/watch?v=7zXNnb2qr6s

UNIVERSITY OF TWENTE.

SDN LABS

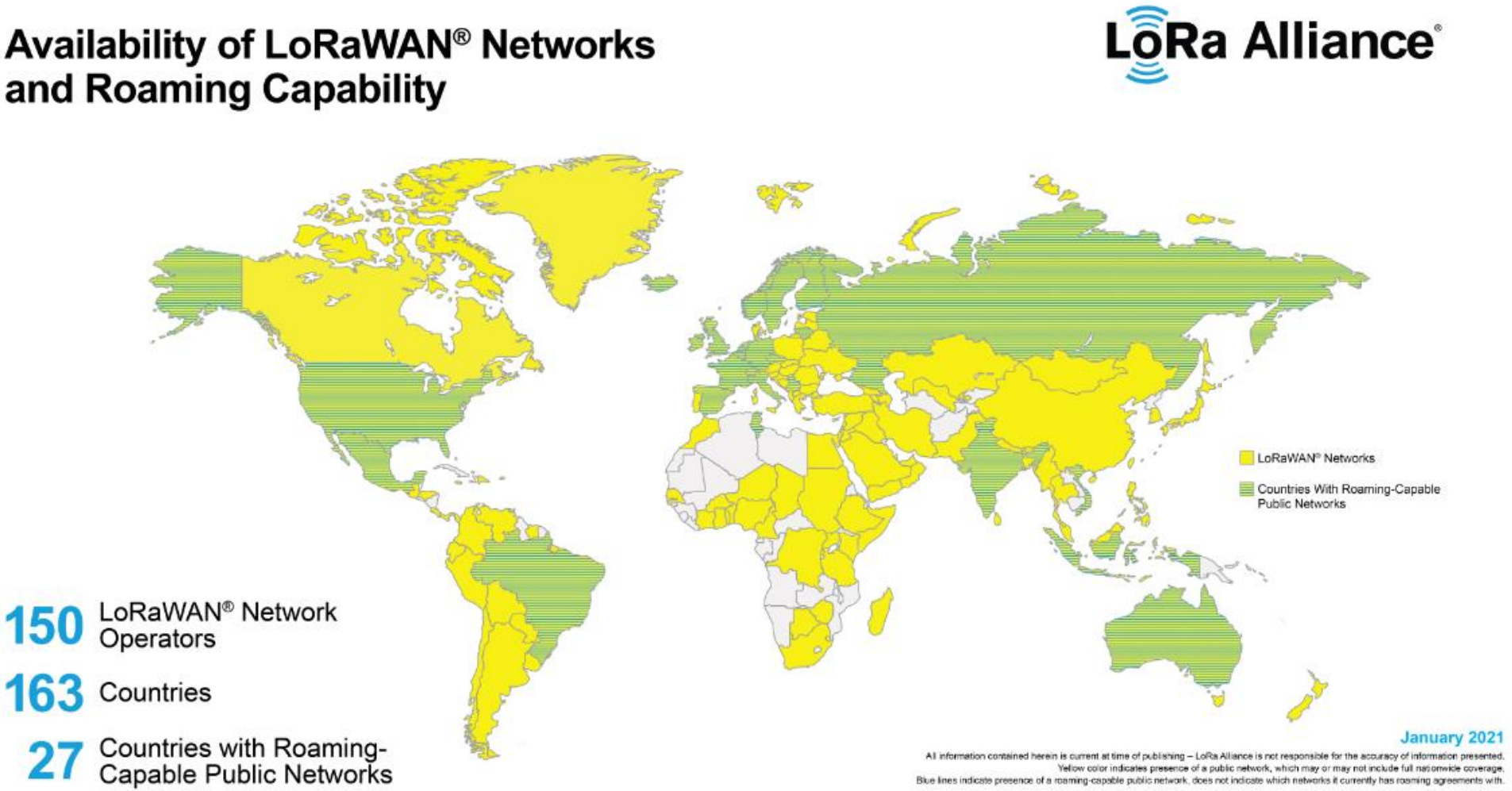
Long distance communications

公尺 = meter, record: 8km (832 km is the world record)
Source: https://www.intelligentagri.com.tw/en

UNIVERSITY OF TWENTE.

SDN LABS

Coverage worldwide



UNIVERSITY OF TWENTE.

SDN LABS

Coverage in the Netherlands (KPN)

Bekijk de dekking van het LoRa-netwerk

Met onze LoRa coverage checker

KPN werkt hard aan de verdichting van het LoRa-netwerk zodat je overal in Nederland eenzelfde dekking ervaart als bij onze andere mobiele netwerken. De LoRa-dekking, zoals in de coverage checker weergegeven, is gebaseerd op een theoretisch model. De LoRa-dekking kan onderhevig zijn aan veranderingen.

Postcode of plaats | Zoek

- Lora netwerk
  - LoRa Outdoor
  - LoRa Indoor

TY OF TWENTE.

SDN LABS

LoraWAN: key components

LoraWAN sensor (e.g., temperature)

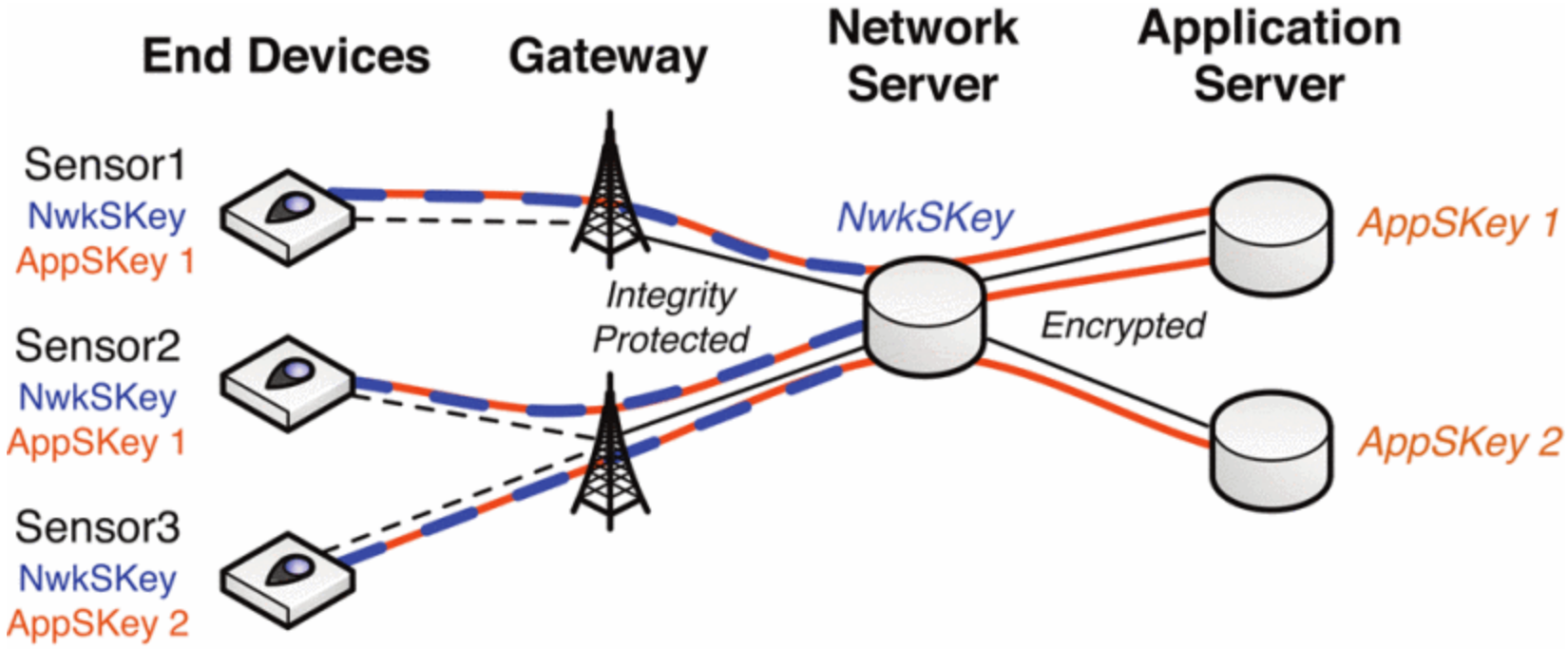
LoraWAN gateway

LoraWAN bridge (e.g., for ModBus)

UNIVERSITY OF TWENTE.

SDN LABS

LoraWAN roles and keys



Network Session Key

message integrity

Application Session Key

payload encryption & decryption

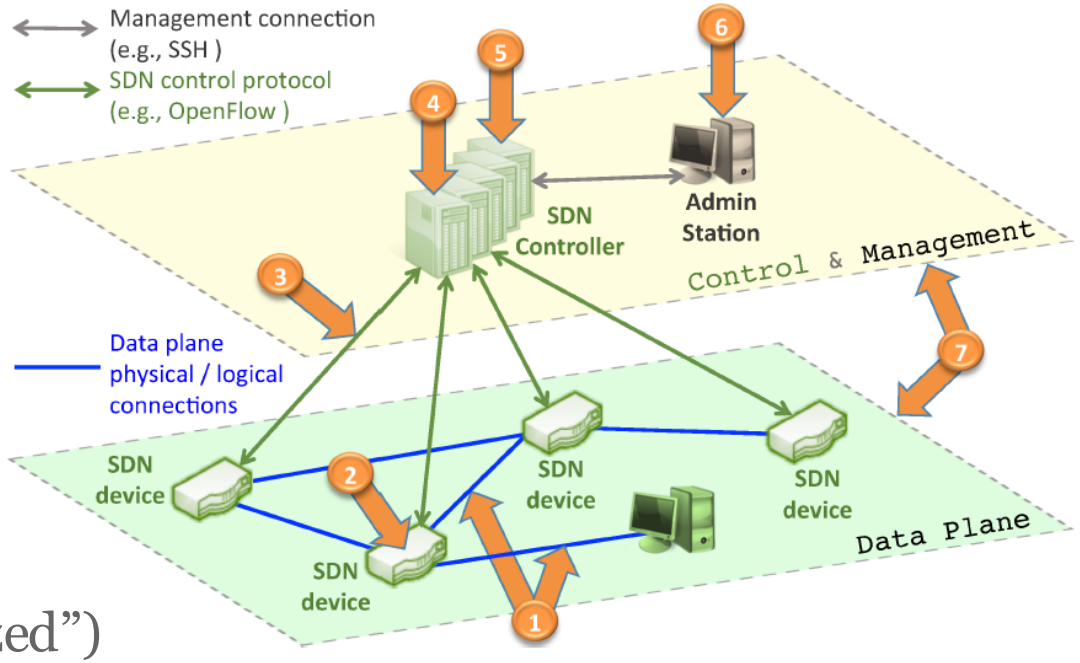
UNIVERSITY OF TWENTE.

SDN 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



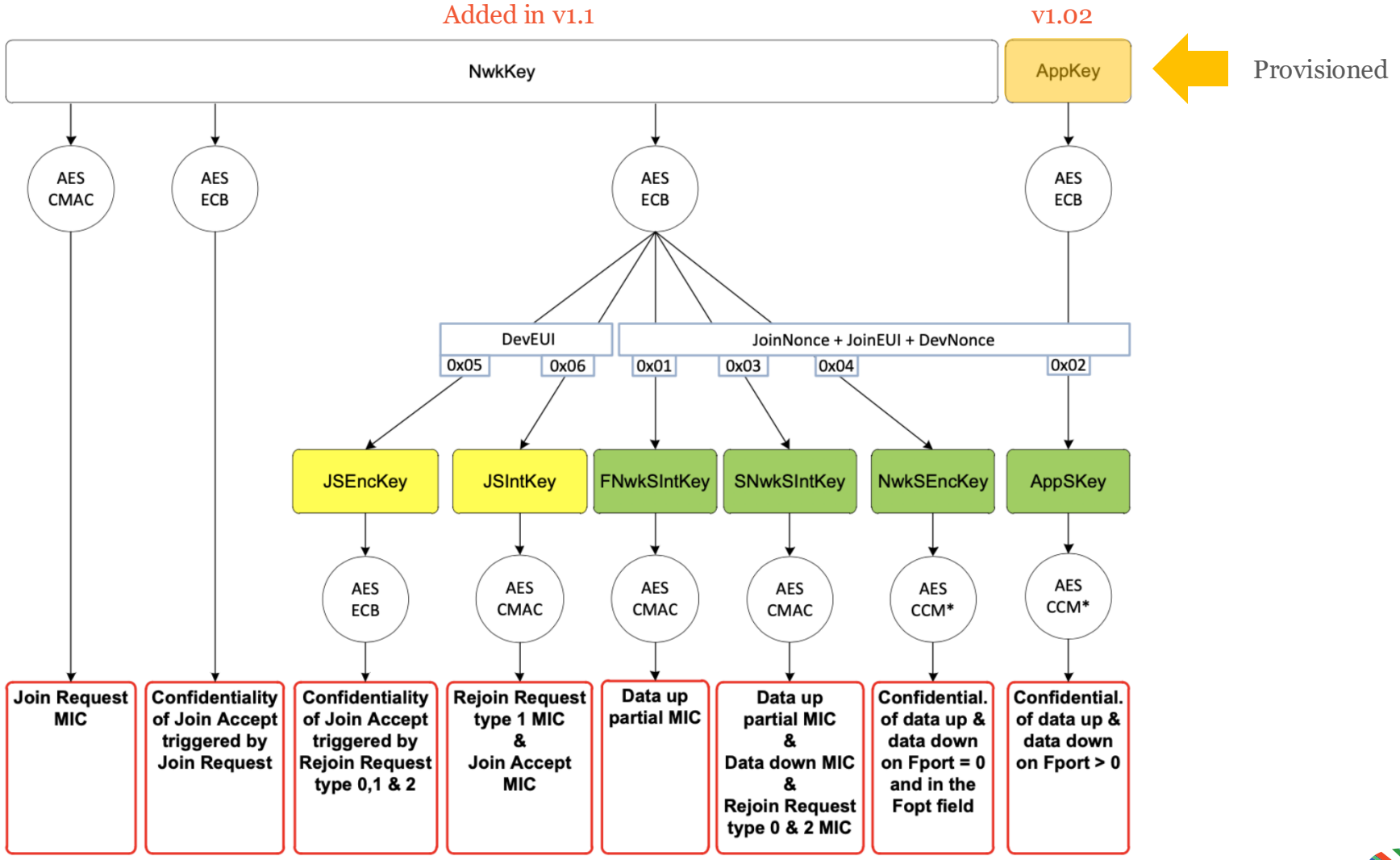
Source: D. Kreutz, F. M. V. Ramos, P. Verissimo, HotSDN’13, August 16, 2013, Hong Kong, China.

UNIVERSITY OF TWENTE.

SDN LABS

LoraWAN key derivation

v1.1: logical separation between network and application operator (Oct 2017)



Picture: Johan Stokking, The Thing Industries

Attack #1: denial of service through replay

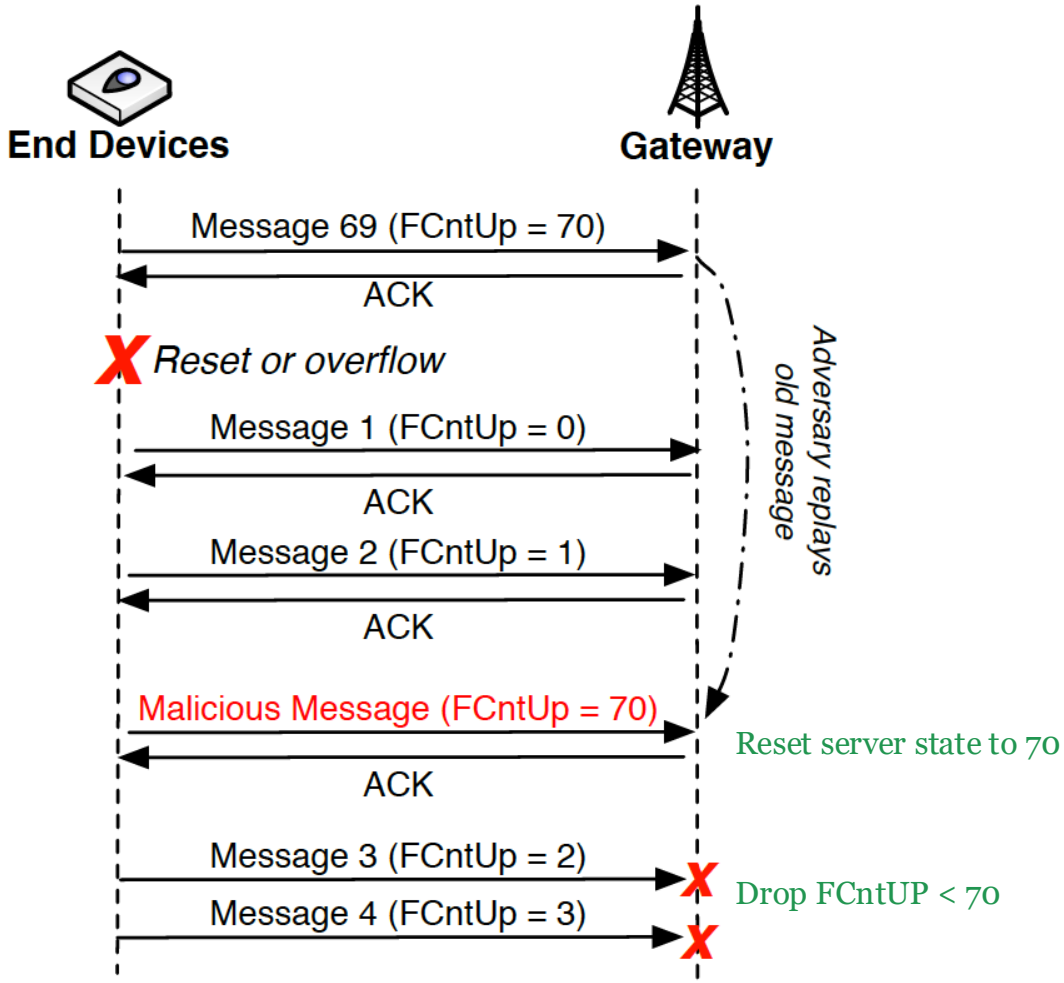


Fig. 4. An example of a replay attack for ABP.

Injected message

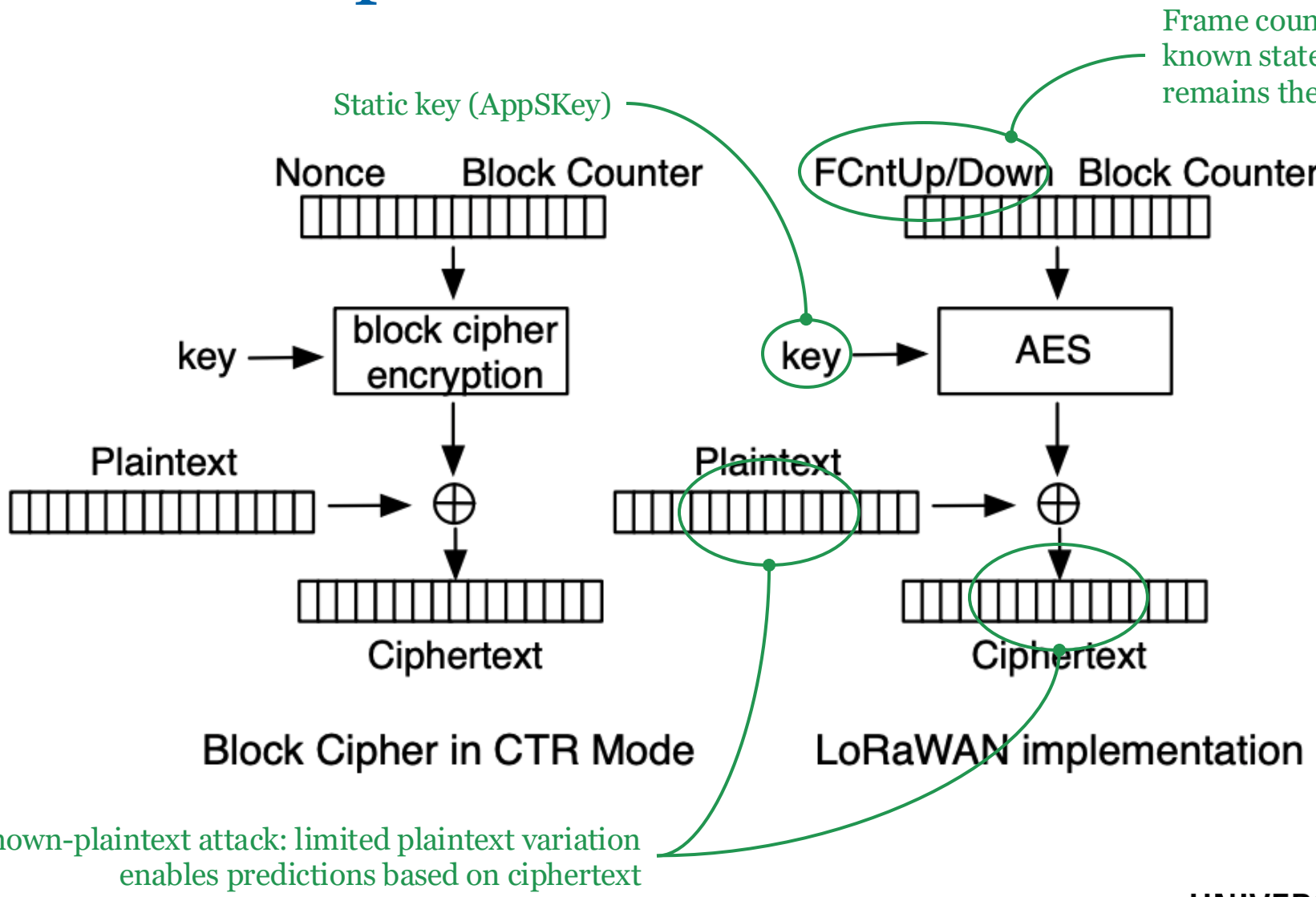
time	counter	port	dev id	
16:16:00	13	6	22	34 34 37 20 30 32 34 00
16:15:25	12	61	22	34 39 36 20 30 32 34 00
16:14:51	11	20	22	35 34 33 20 30 32 31 00
16:08:49	10	49	22	34 38 30 20 30 32 31 00
16:08:34	0	71	22	31 39 32 20 30 32 32 00
16:07:59	10	49	22	34 38 30 20 30 32 31 00
16:06:16	7	41	22	35 32 37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

UNIVERSITY OF TWENTE.

SDN LABS

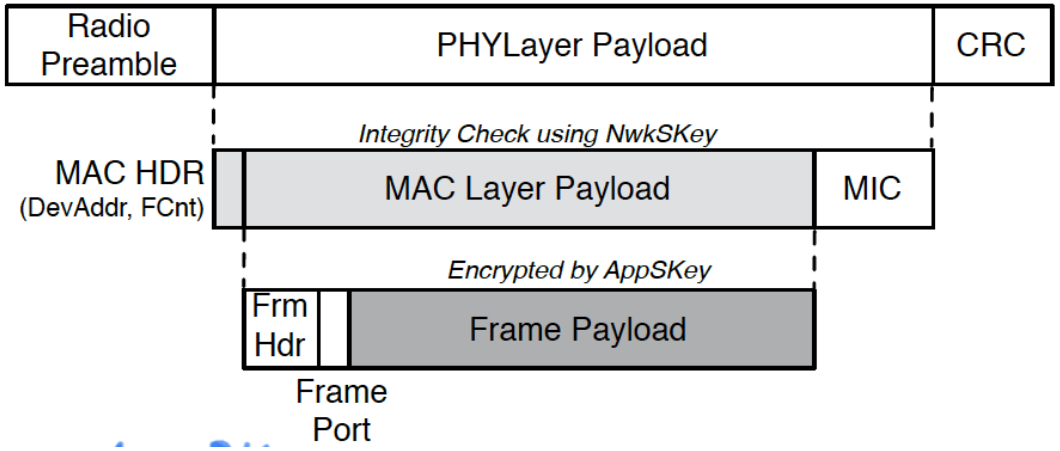
Attack #2: known-plaintext attack

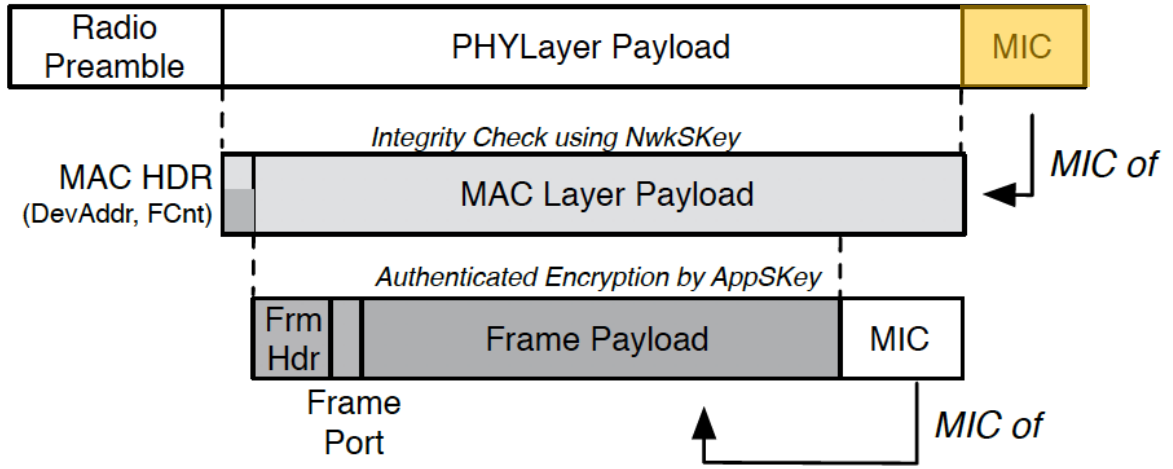


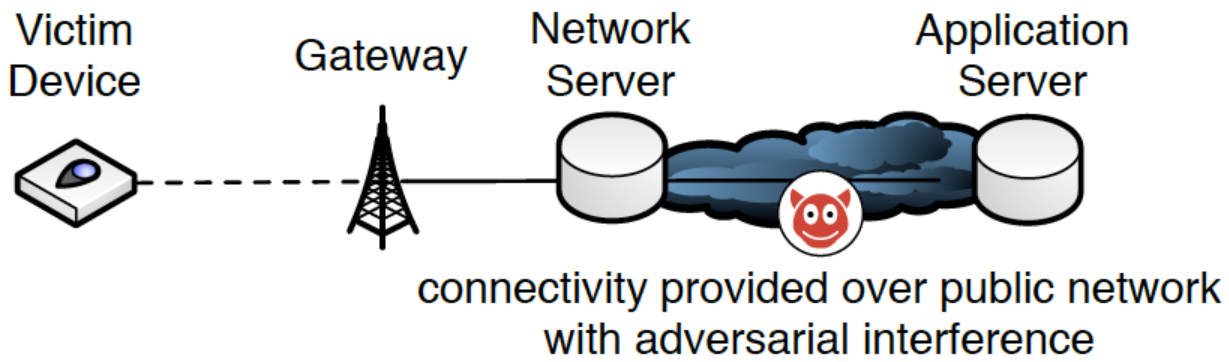
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
https://en.wikipedia.org/wiki/Known-plaintext_attack
https://en.wikipedia.org/wiki/Block_cipher

UNIVERSITY OF TWENTE.
SDN LABS

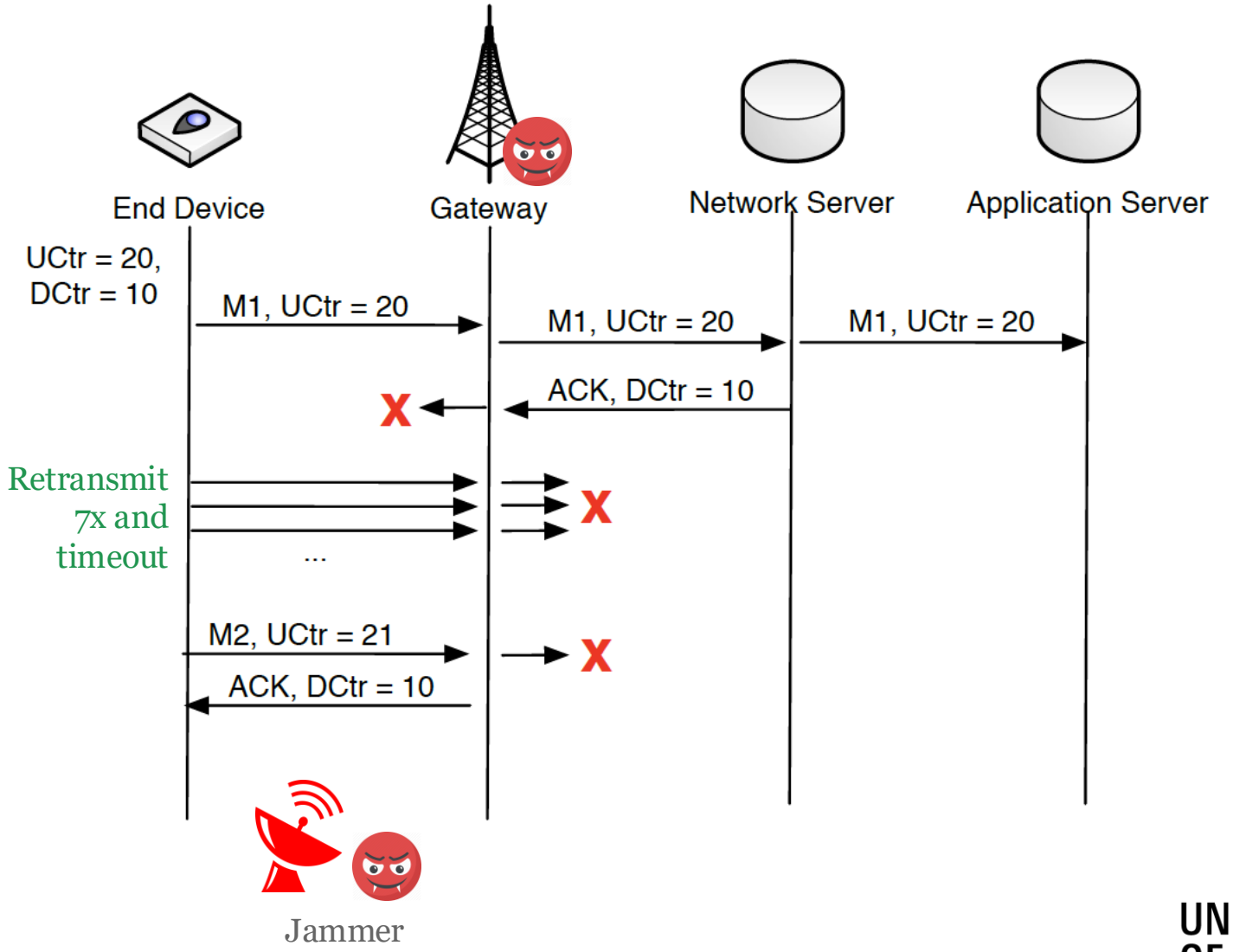
Proposed solution using 2 MICs







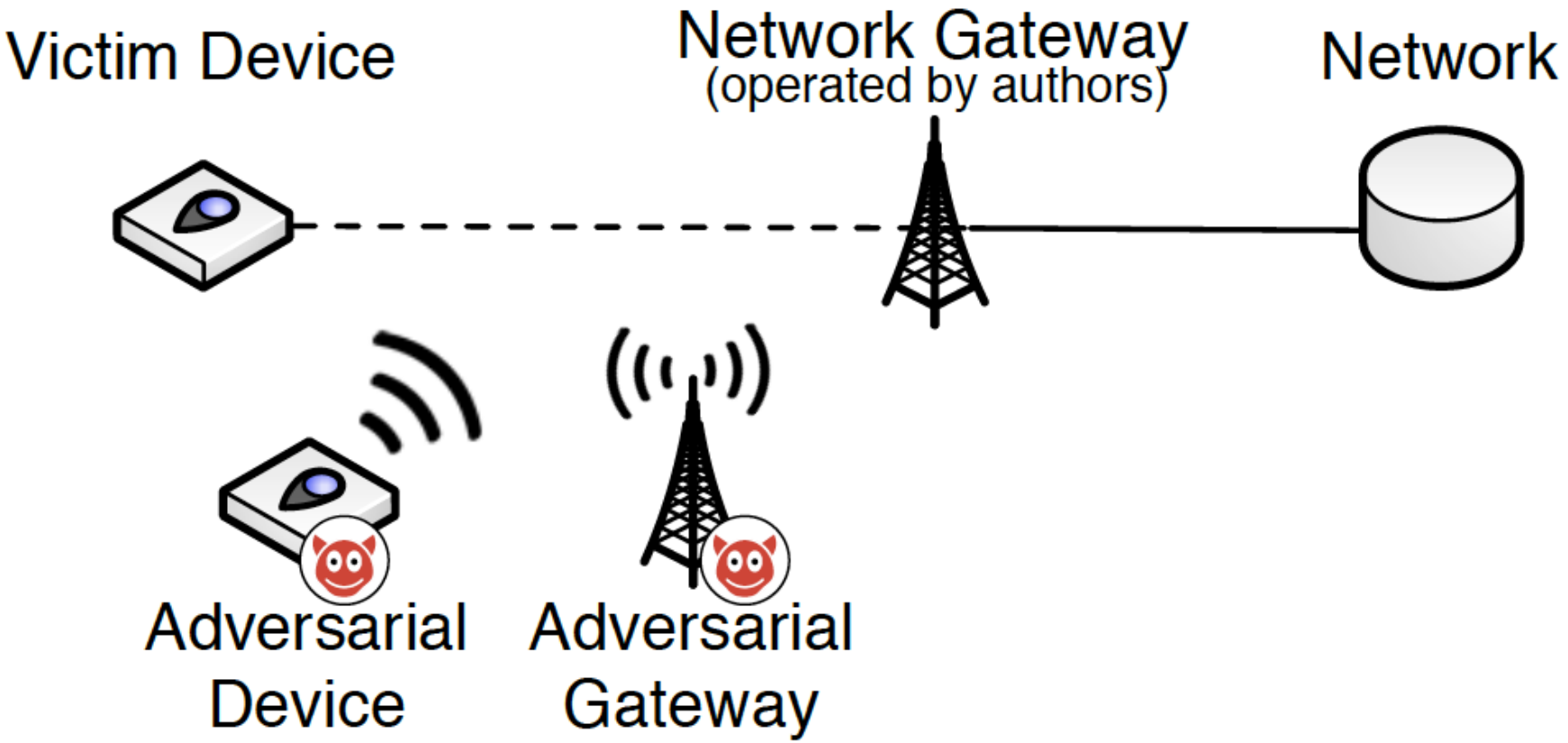
Attack #3: ACK spoofing



UNIVERSITY OF TWENTE.

SDN LABS

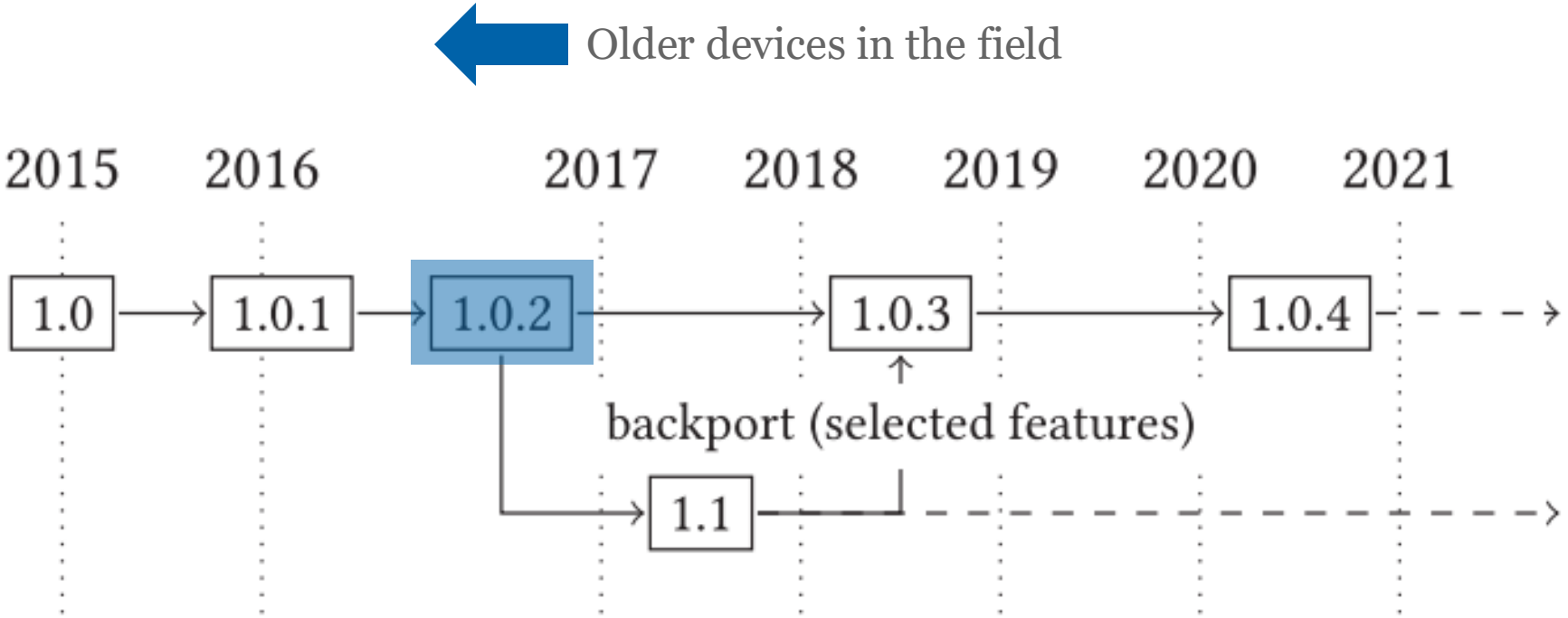
Attack #4: class B attacks (battery draining)



UNIVERSITY OF TWENTE.

SDN LABS

Let's look at the version history of LoraWAN



F. Hessel, L. Almon, and M. Hollick, "LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation", ACM Trans. Sens. Netw., vol. 18, no. 4, p. 70:1-70:55, Mar. 2023, doi: 10.1145/3561973.

UNIVERSITY OF TWENTE.

SDN LABS

Open standardization (vs. more closed like LoraWAN)

IETF®

UNIVERSITY OF TWENTE.

SDN LABS

Key takeaways

- Designing network protocols typically involves many tradeoffs and design decisions sometimes result in vulnerabilities

- Attacks can have a physical component, such as jamming, device resets, or being able to locate gateways

- Highlights the importance of an open protocol development process to maximize scrutiny, such as in the IETF

UNIVERSITY OF TWENTE.

SDN LABS

Coffee break

Are you sure you want to do **Coordinated Vulnerability Disclosure?**

University of Twente

Ting-Han Chen

Jeroen van der Ham-de Vos

Vienna University of Technology

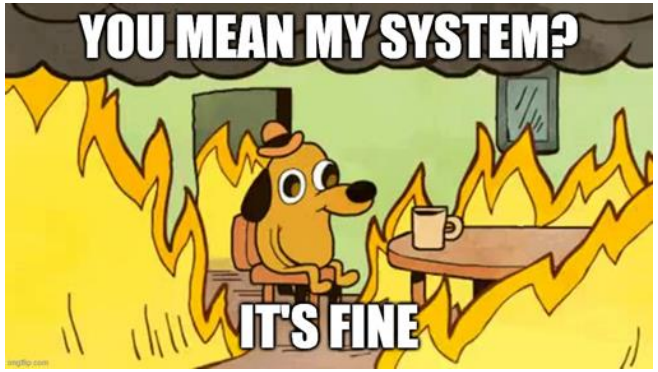
Carlotta Tagliaro

Martina Lindorfer

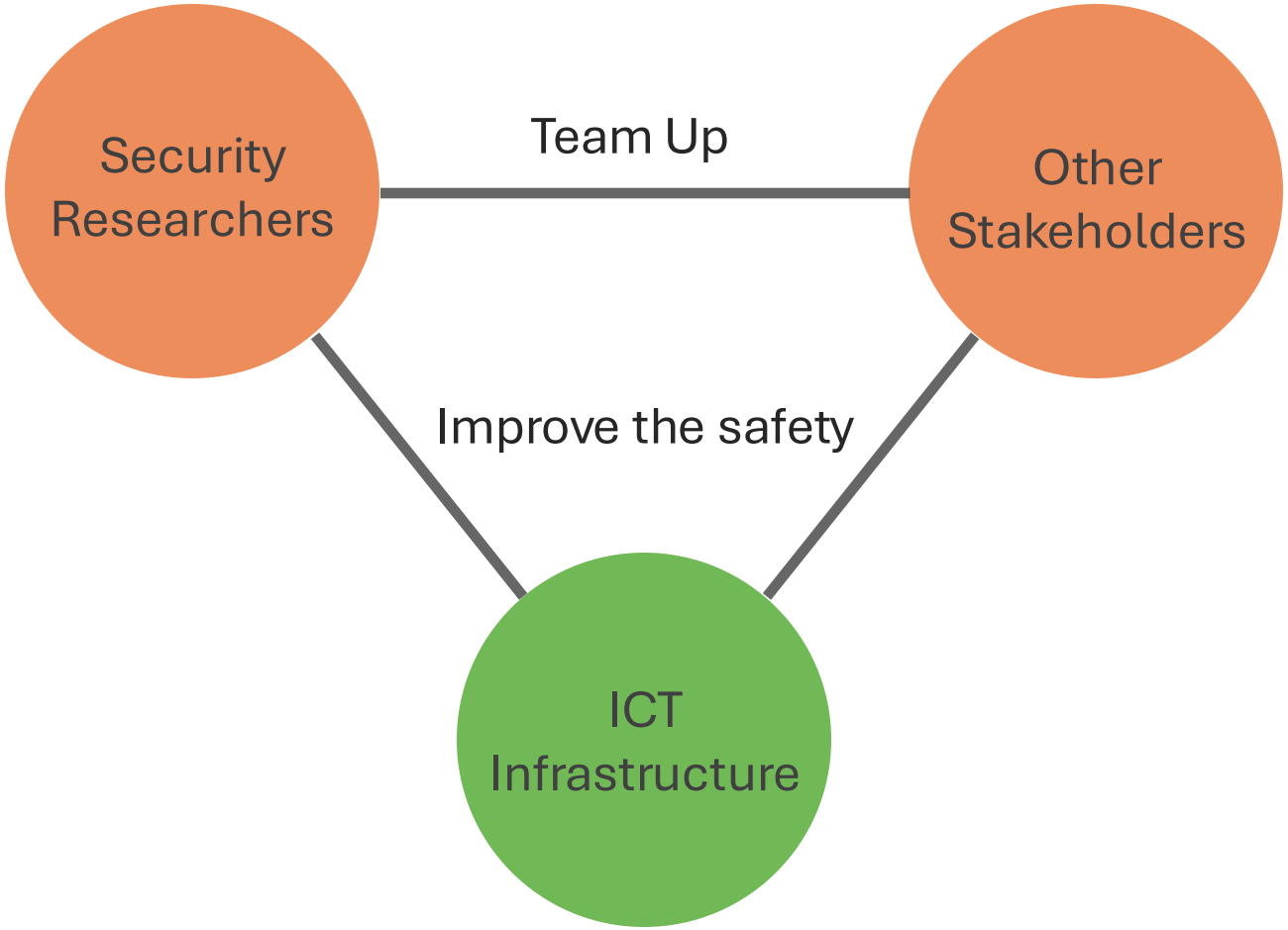
Ruhr University Bochum

Kevin Borgolte

Why did we do **Coordinated Vulnerability Disclosure?**



Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure

Information and Communication Technology Infrastructure

▼

Hardware, Software, Networks, Facilities, Equipment,… IoT

IoT Devices Characteristics

Information and Communication Technology Infrastructure

▼

IoT Products

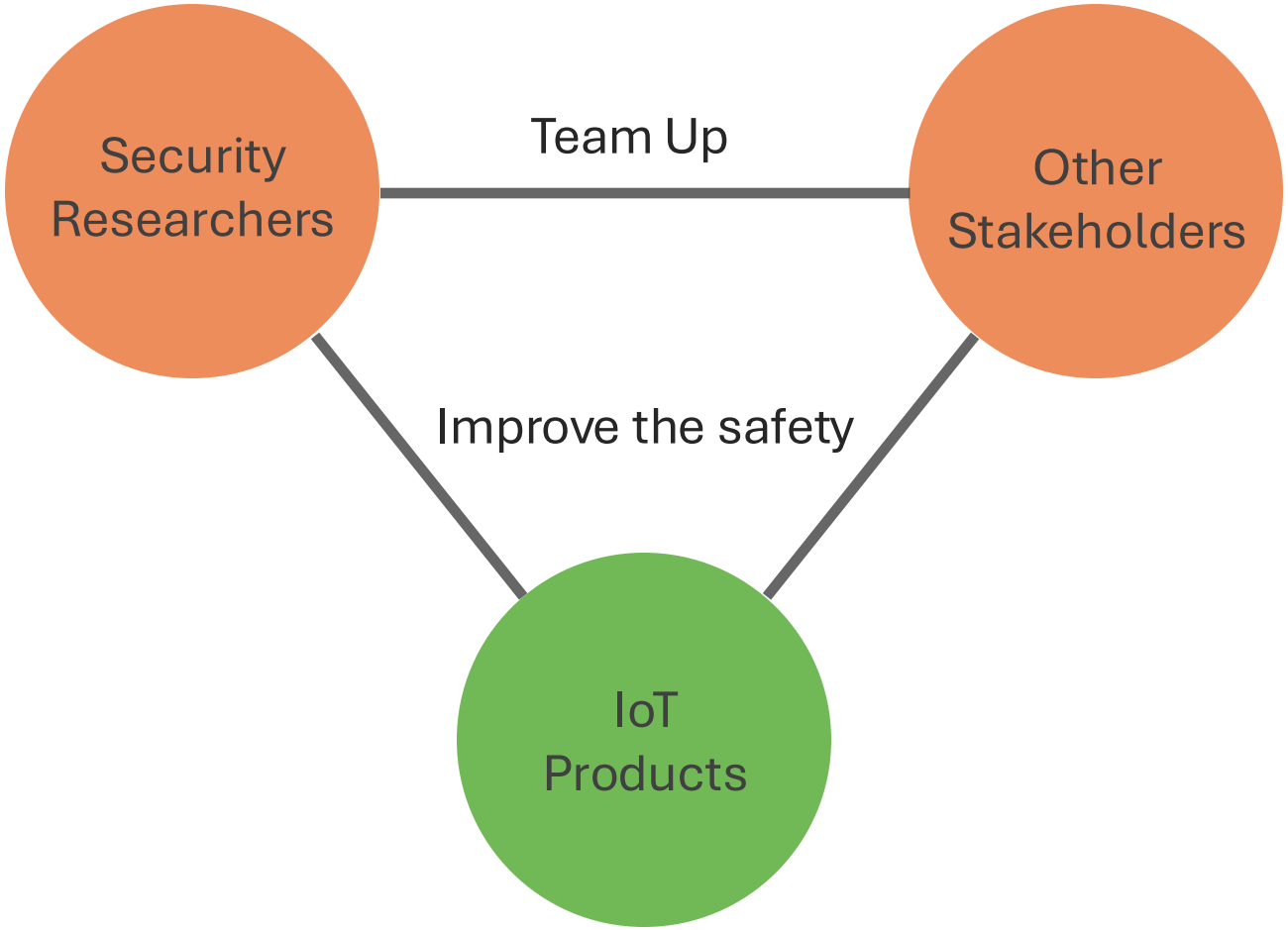
▼

• Type	Diverse OS, Firmware, APIs, and so on
• Scale	Few in smart home, Tons on the net
• Iteration	Every Season to a Decade
• Life	Barely works to super durable
• Cost	Cheap to expensive

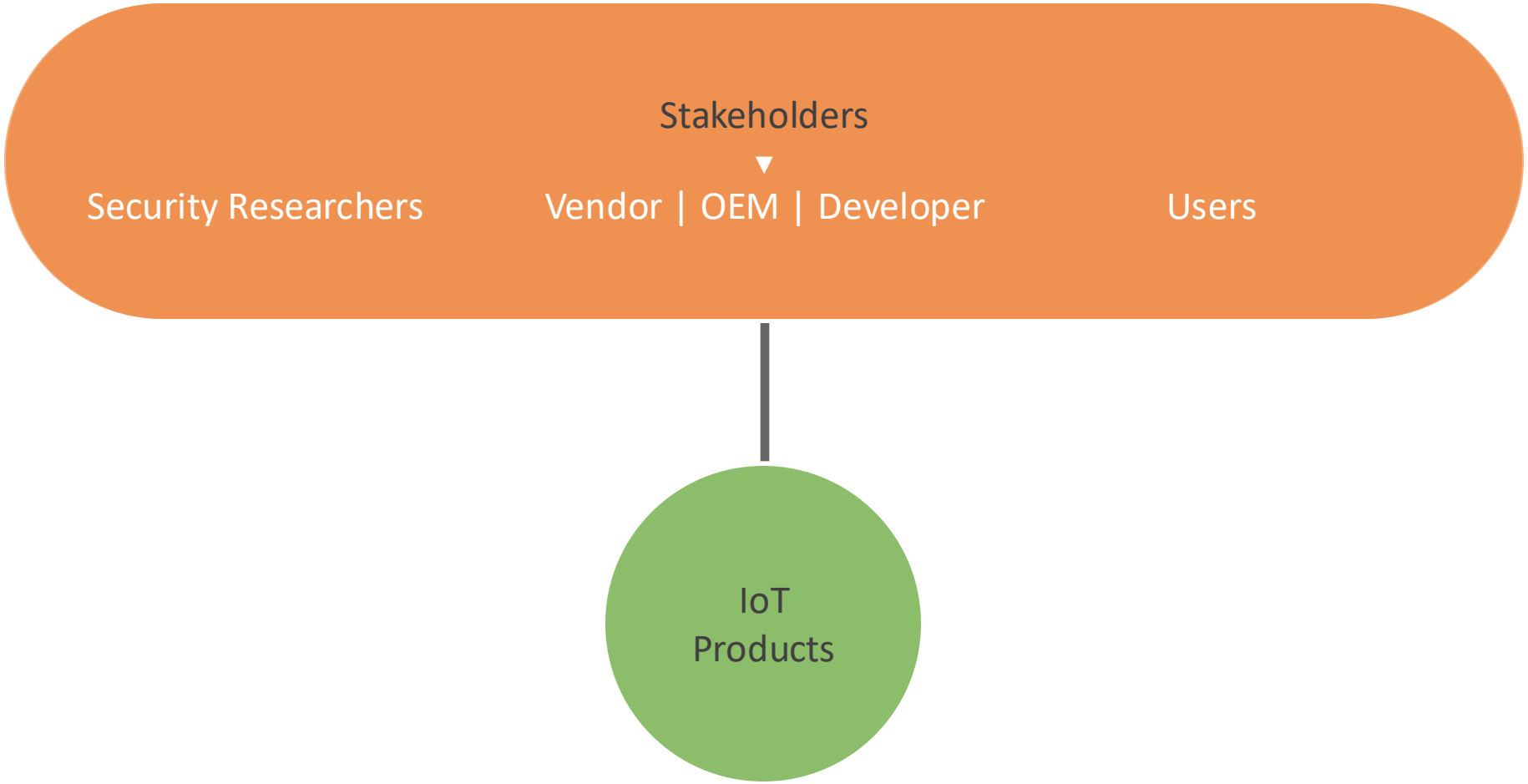
Lecture: Internet Core Protocols

[DNSIoT] C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen "The DNS in IoT: Opportunities, Risks, and Challenges", IEEE Internet Computing, 2020.

Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure

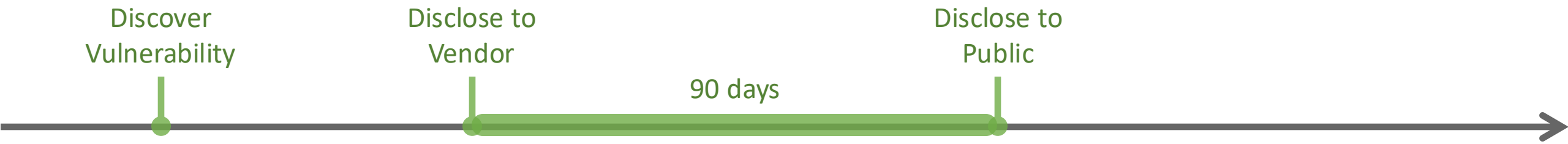
Stakeholders

Security Researchers	Vendor | OEM | Developer	Users
as fast as possible make it public	normally need more time marketing strategy	stable and secure No idea

CVD Timeline

Stakeholders

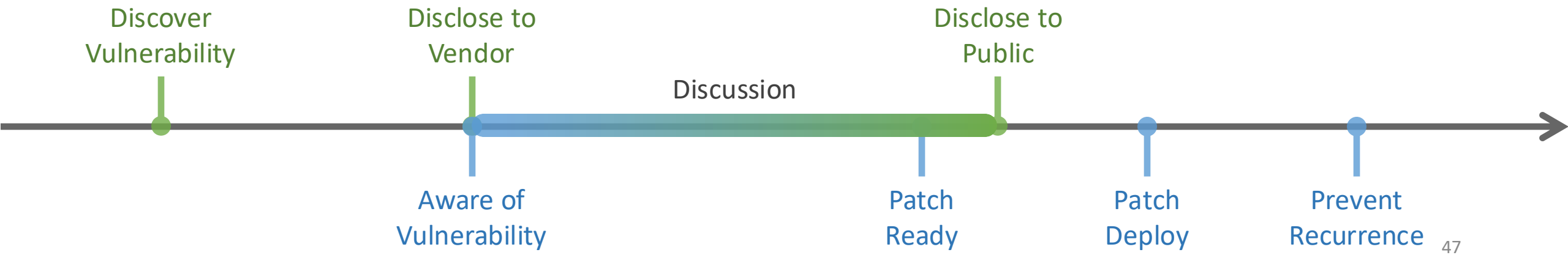
Security Researchers	Vendor | OEM | Developer	Users
as fast as possible make it public	normally need more time marketing strategy	stable and secure No idea



CVD Timeline

Stakeholders

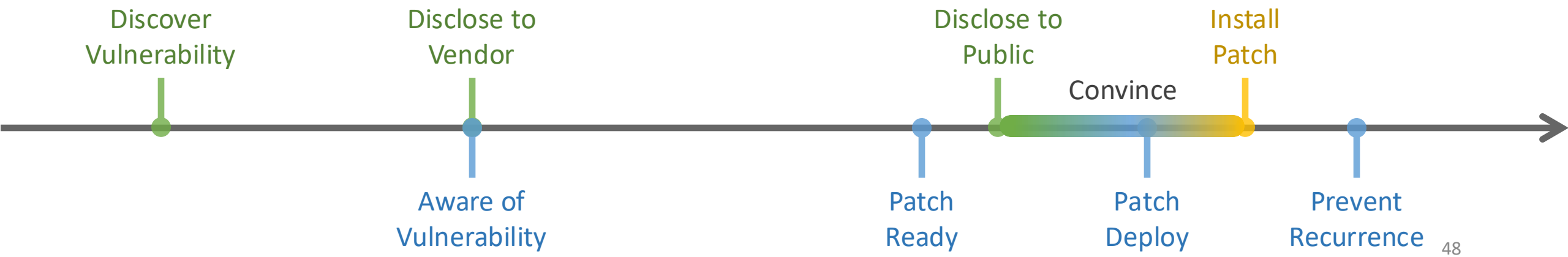
Security Researchers	Vendor | OEM | Developer	Users
as fast as possible make it public	normally need more time marketing strategy	stable and secure No idea



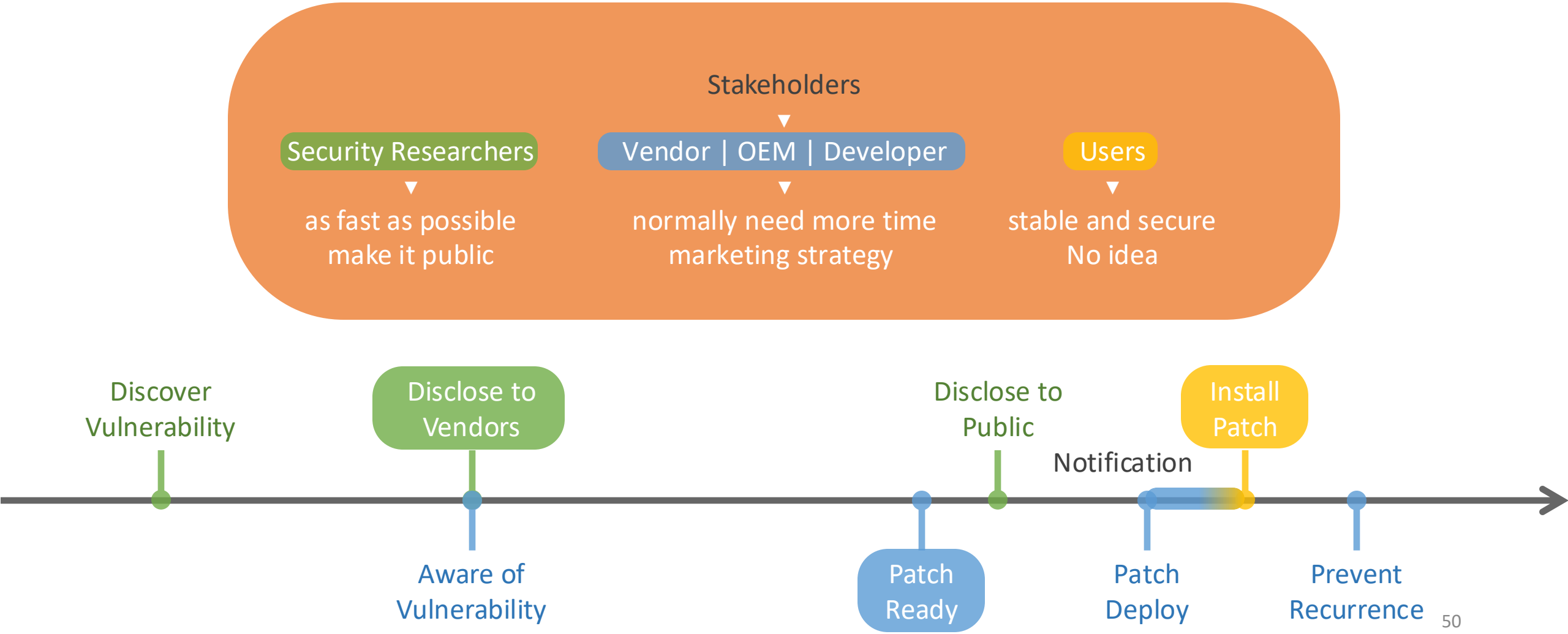
CVD Timeline

Stakeholders

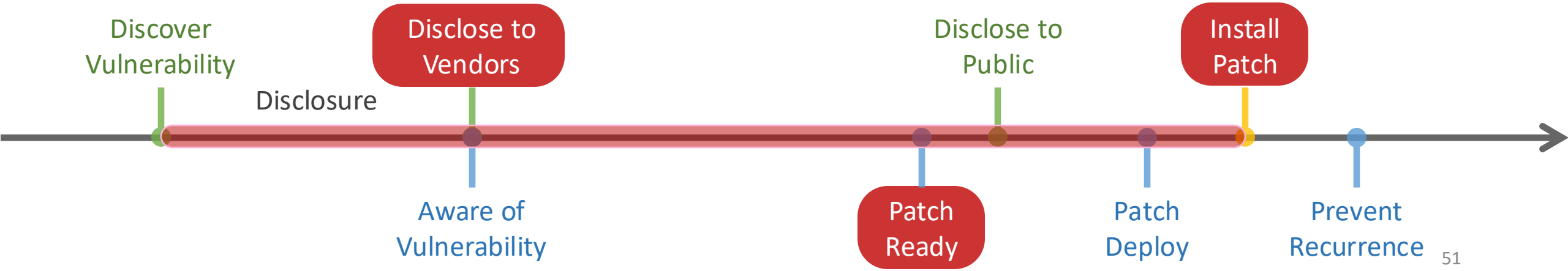
Security Researchers	Vendor | OEM | Developer	Users
as fast as possible make it public	normally need more time marketing strategy	stable and secure No idea



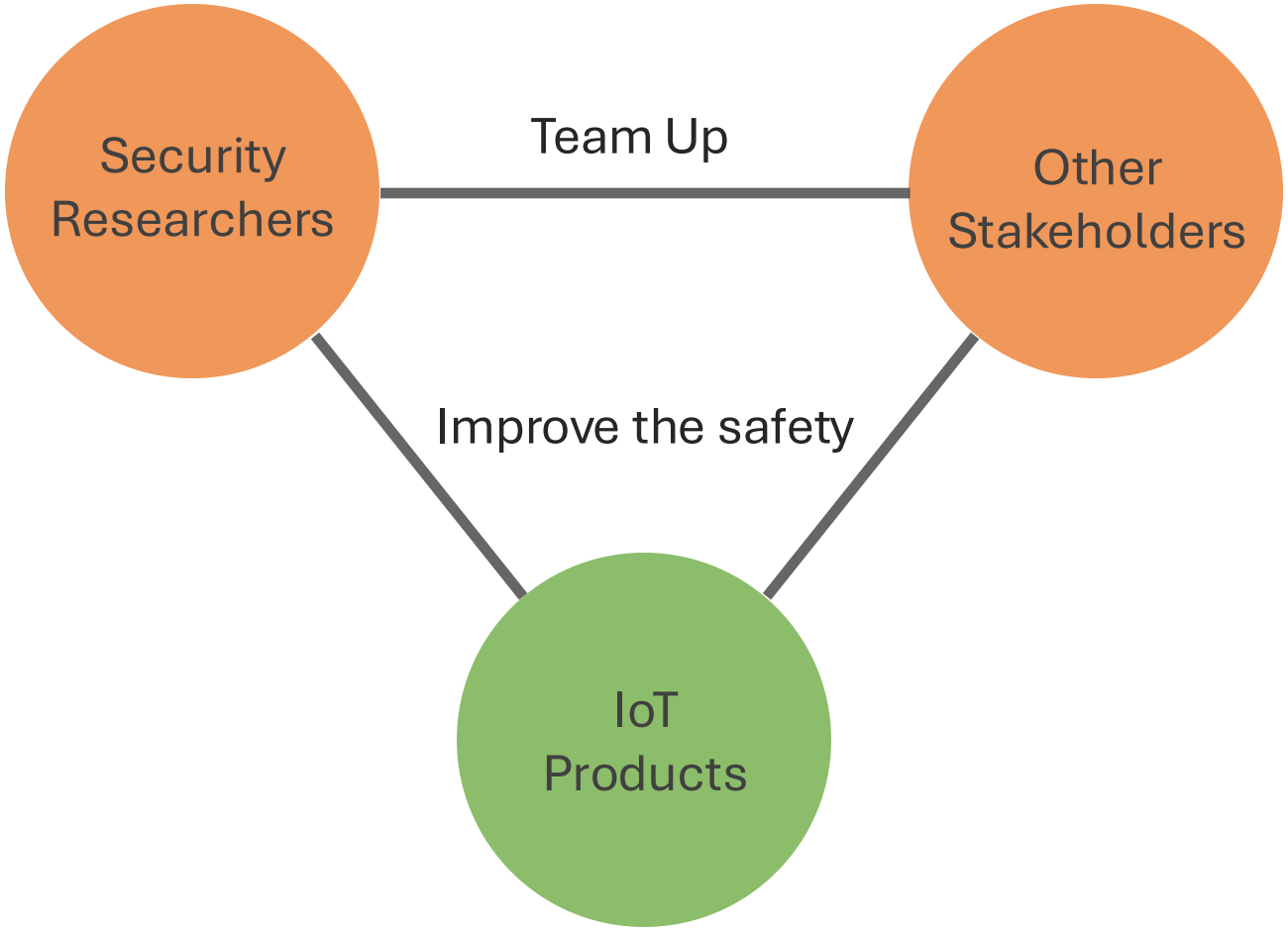
CVD Timeline with IoT



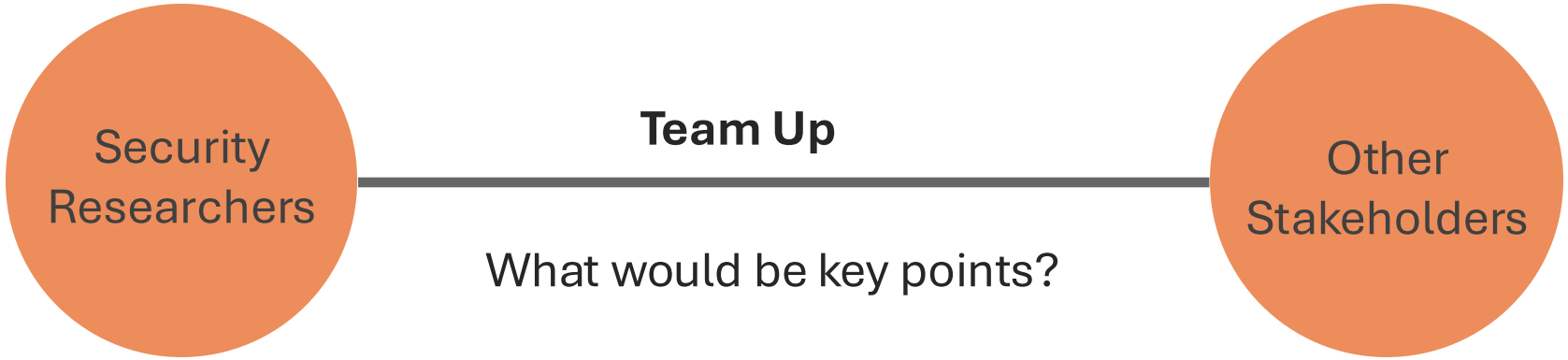
CVD Challenges with IoT at Scale



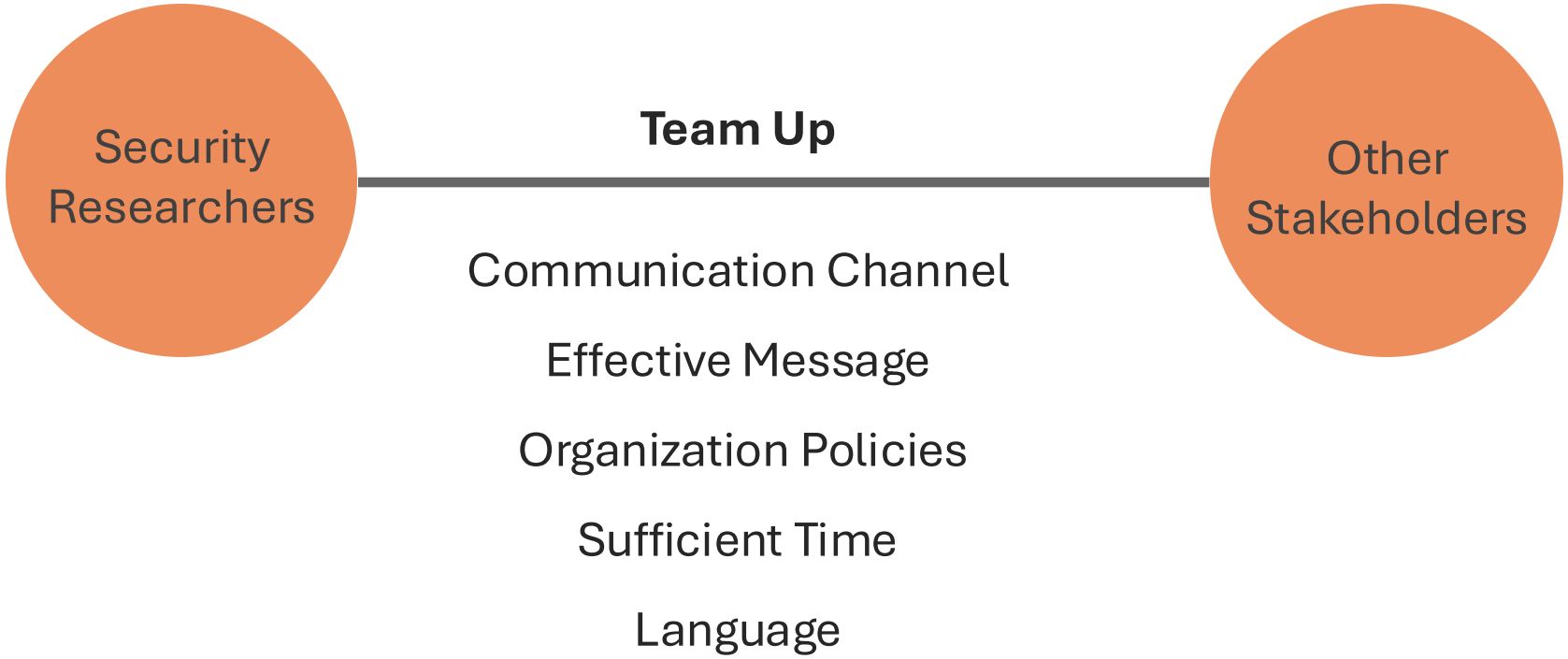
Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure



Coordinated Vulnerability Disclosure

Security Researchers

University

Network operators

Ethical hackers

Organizations

CSIRTs

Team Up

Communication Channel

Effective Message

Organization Policies

Sufficient Time

Language

Other Stakeholders

Universities

Domain Name owners

Cloud providers

Governments

Vendors/End-users

Coordinated Vulnerability Disclosure

Team Up

Communication Channel

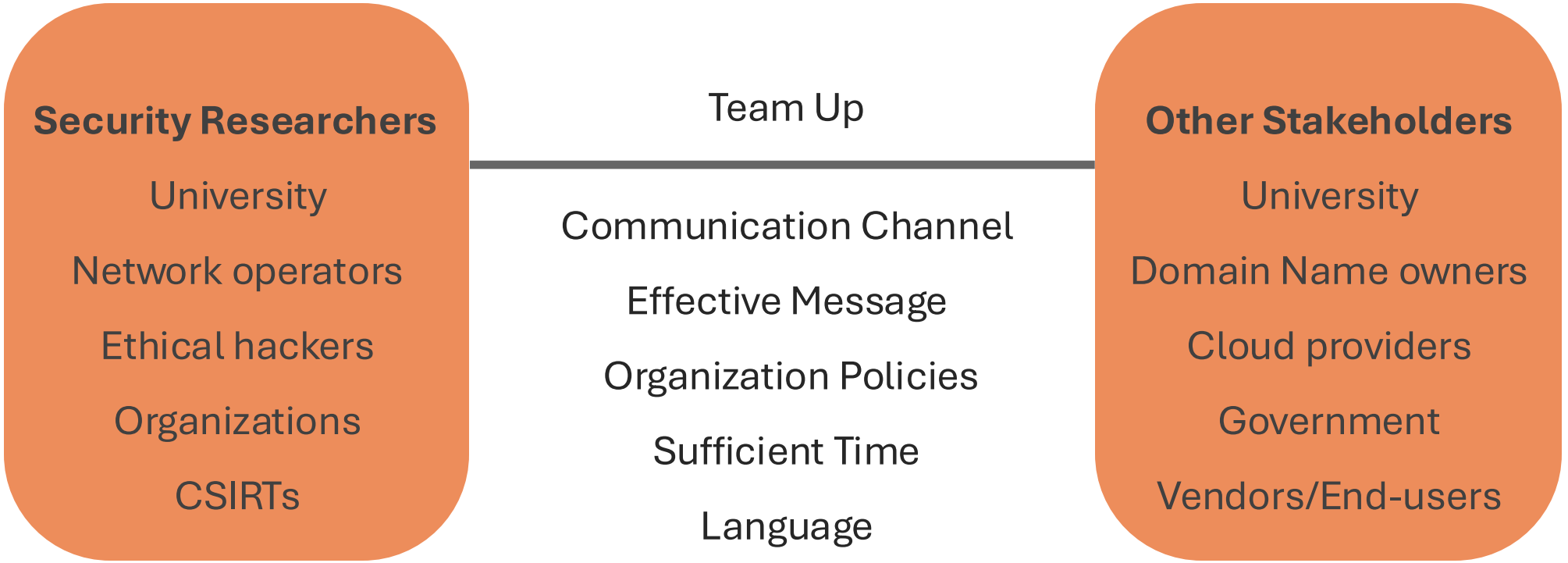
Effective Message

Organization Policies

Sufficient Time

Language

Challenges of CVD



We accepted the Challenges of CVD

This work focus on improving the existing guideline and giving suggestions to best practices

The Team

Network Scanning

Vienna University of Technology

Carlotta Tagliaro

Martina Lindorfer

Ruhr University Bochum

Kevin Borgolte

Man in the Middle

University of Twente

Andrea Continella

Vulnerability Notification

University of Twente

Ting-Han Chen

Jeroen van der Ham-de Vos

Network Scanning

We leveraged Shodan to identify backends that speak common IoT communication protocols

MQTT
Message Queuing Telemetry Transport

CoAP
Constrained Application Protocol

XMPP
Extensible Messaging and Presence Protocol

IoT Backends

IP addresses

Hostnames

Connection Codes

Geolocation information

Attack Classes

Information Leakage

Weak Authentication

Denial of Service

[25] C. Tagliaro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer.
"Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols." May 2024. arXiv: 2405.09662 [cs.CR].

Network Scanning on IoT Backends

In this paper, we focused on the vulnerability notification of backends running MQTT protocol

MQTT
Message Queuing Telemetry Transport

CoAP
Constrained Application Protocol

XMPP
Extensible Messaging and Presence Protocol

IoT Backends

IP addresses

Hostnames

Connection Codes

Geolocation information

Attack Classes

Information Leakage

Weak Authentication

Denial of Service

[25] C. Tagliaro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer.
“Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols.” May 2024. arXiv: 2405.09662 [cs.CR].
RAID '24: Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses, Pages 561 - 578

Network Scanning on IoT Backends

Below are the information we collected to perform the vulnerability notification to stakeholders

MQTT

Message Queuing Telemetry Transport

IoT Backends

IP addresses

Hostnames

Port

Timestamp

Attack Classes

Information Leakage

Weak Authentication

Denial of Service

Connected Clients

From 10 to 150

Vulnerabilities & Pitfalls

Unintended Exposed Access

No Authentication

CVE-2018-12550

CVE-2018-12551

CVE-2017-7655

CVE-2018-19417

CVE-2019-9749

[25] C. Tagliaro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer.
"Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols." May 2024. arXiv: 2405.09662 [cs.CR].


The epic CVD journey began

15820 IP addresses

Across the world

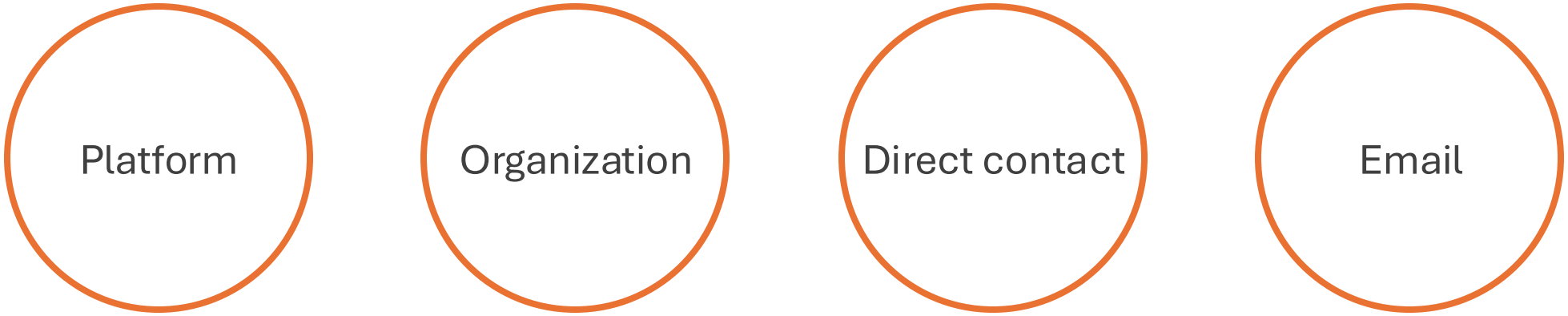
Multiple parties involved

Large-Scale Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved

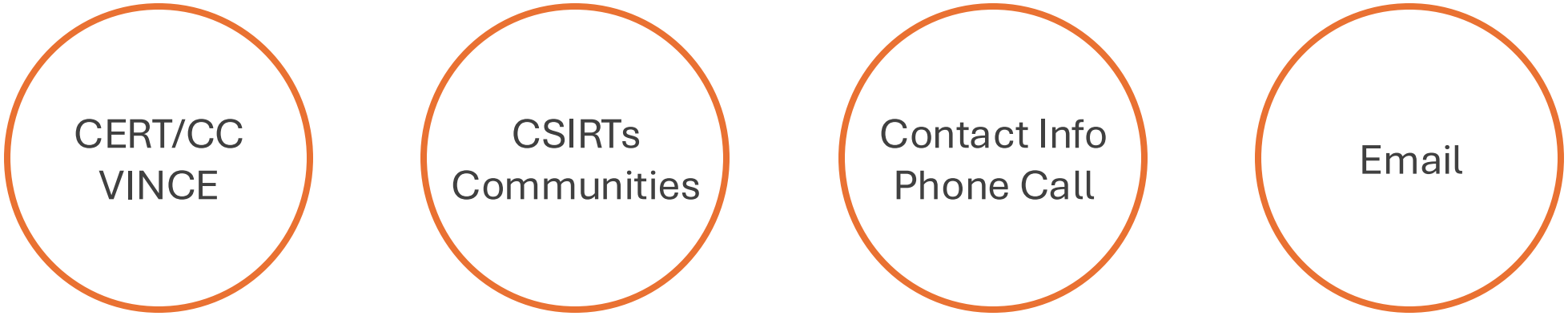
Large-Scale Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved



Large-Scale Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved



Which communication channel would you choose?

Large-Scale Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved

Large-Scale Email Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved

[9] S. Fernandez, O. Hureau, A. Duda, and M. Korczynski.
"WHOIS Right? An Analysis of WHOIS and RDAP Consistency." In: Proceedings of the 16th Passive and Active Measurement Conference (PAM). Springer, Mar. 2024. doi: 10.1007 / 978-3-031-56249-5_9.

Large-Scale Email Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved

[9] S. Fernandez, O. Hureau, A. Duda, and M. Korczynski.
"WHOIS Right? An Analysis of WHOIS and RDAP Consistency." In: Proceedings of the 16th Passive and Active Measurement Conference (PAM). Springer, Mar. 2024. doi: 10.1007 / 978-3-031-56249-5_9.

Large-Scale Email Vulnerability Notification

15820 IP addresses, Across the world, Multiple parties involved

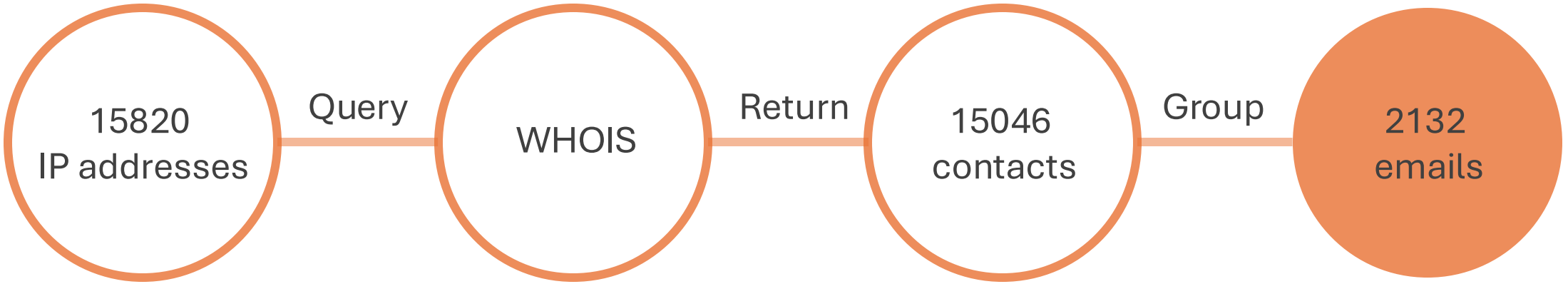
[9] S. Fernandez, O. Hureau, A. Duda, and M. Korczynski.
"WHOIS Right? An Analysis of WHOIS and RDAP Consistency." In: Proceedings of the 16th Passive and Active Measurement Conference (PAM). Springer, Mar. 2024. doi: 10.1007 / 978-3-031-56249-5_9.

Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved

Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved



Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved, 2132 emails

The messages should be brief, clear, and informative

[Our Identify]

[Statement]

[IP addresses, Timestamp, CVEs if found]

[IoT Protocol: MQTT, Port]

[Webpage for more details]

[Please inform the responsible parties]

[Our policies, University of Twente and Dutch National Cyber Security Center (NCSC)]

[Attachment CSV file]

[13] J. van der Ham, A. Continella, P. de Willigen, and D. Reidsma.
University of Twente Policy for Coordinated Vulnerability Disclosure in Research.
https://www.utwente.nl/en/service-portal/research-support/procedures-facilities/coordinated-vulnerability-disclosure-policy-for-research

Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved, 2132 emails

Having outgoing policy can help to build the trust between the stakeholders

[Our Identify]

[Statement]

[IP addresses, Timestamp, CVEs if found]

[IoT Protocol: MQTT, Port]

[Webpage for more details]

[Please inform the responsible parties]

[Our policies, University of Twente and Dutch National Cyber Security Center (NCSC)]

[Attachment CSV file]

[13] J. van der Ham, A. Continella, P. de Willigen, and D. Reidsma.
University of Twente Policy for Coordinated Vulnerability Disclosure in Research.
https://www.utwente.nl/en/service-portal/research-support/procedures-facilities/coordinated-vulnerability-disclosure-policy-for-research

Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved, 2132 emails

It may not be the best way to disclose every detail in the first message

[Our Identify]

[Statement]

[IP addresses, Timestamp, CVEs if found]

[IoT Protocol: MQTT, Port]

[Issue details]

[Security suggestions]

[Webpage for more details]

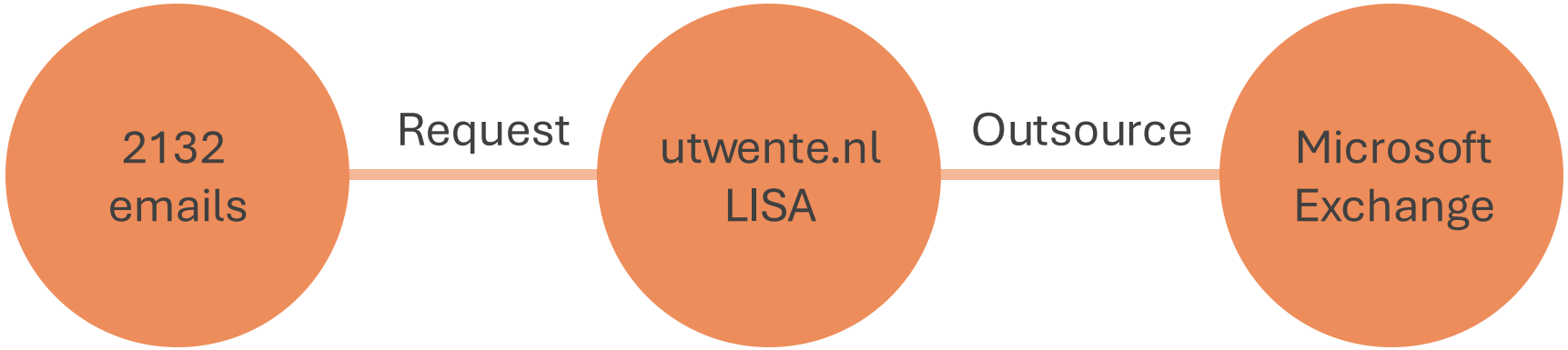
[Please inform the responsible parties]

[Our policies, University of Twente and Dutch National Cyber Security Center (NCSC)]

[Attachment CSV file]

Large-Scale Email Vulnerability Notification

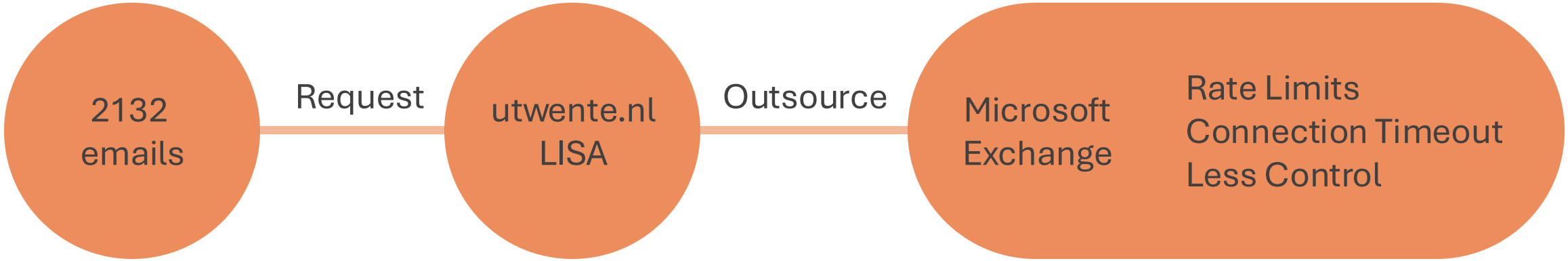
Across the world, Multiple parties involved



[14] M. van der Horst.
Global Vulnerability Vigilance: Timely Disaster Notification using Internet-Scale Coordinated Vulnerability Disclosure. July 11, 2023.

Large-Scale Email Vulnerability Notification

Across the world, Multiple parties involved



Exchange Online limits
https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits

2132 emails sent

iot-disclosure-2023@utwente.nl

2132 emails sent in batch

iot-disclosure-2023@utwente.nl

2132 emails sent in batch in 2 weeks

iot-disclosure-2023@utwente.nl

After the first batch of emails were sent…

iot-disclosure-2023@utwente.nl


A FEW SECONDS LATER...
Loading

The first responses came!

Guess what came to us first?

Emails Bouncing Back...

Quota exceeds, Recipients not found, Message Filter, Unavailable...

Emails Bouncing Back...

Quota exceeds, Recipients not found, Message Filter, Unavailable...

Restrict length of content messages, attachment type, and file size

Emails Bouncing Back... < 5%

This is delivery failure. Successful delivery can still go into spam

This is not the only type of message

Stakeholders also have different way to handle our message

Ticketing System Automatic Responses

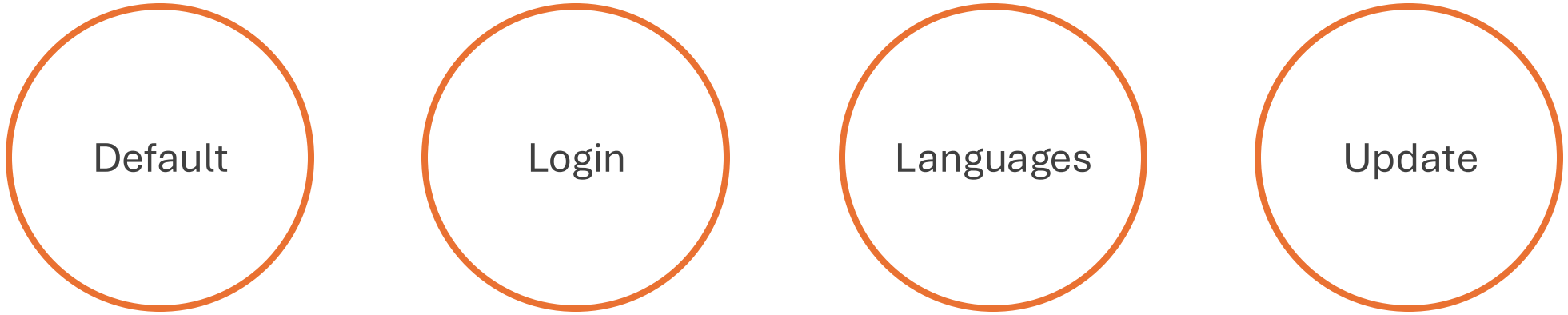
This is where the fun part comes

Ticketing System Automatic Responses 36.48%

Cloud Providers, Domain Name Owners, Universities, and so on

Ticketing System Automatic Responses

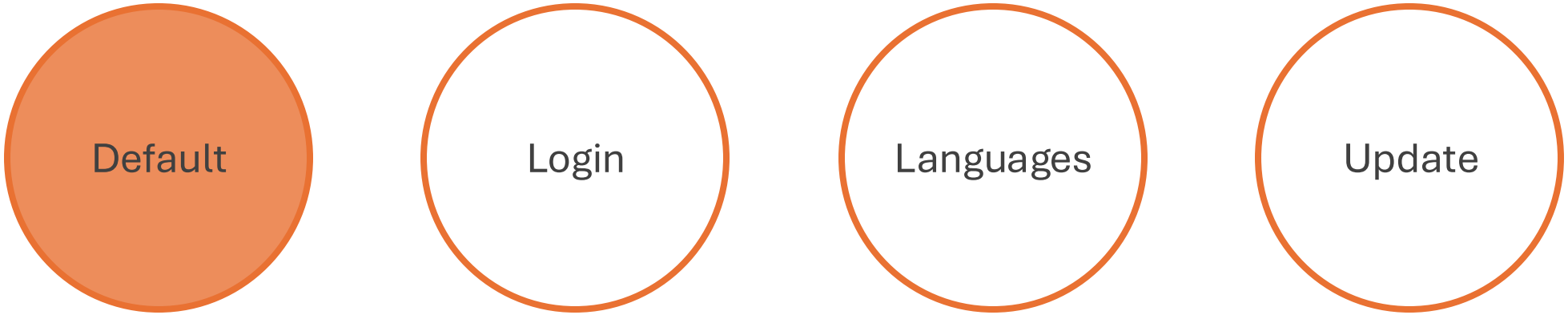
Cloud Providers, Domain Name Owners, Universities, and so on



Which automatic responses can be hard to handle?

Ticketing System Automatic Responses

Cloud Providers, Domain Name Owners, Universities, and so on



Count: 400

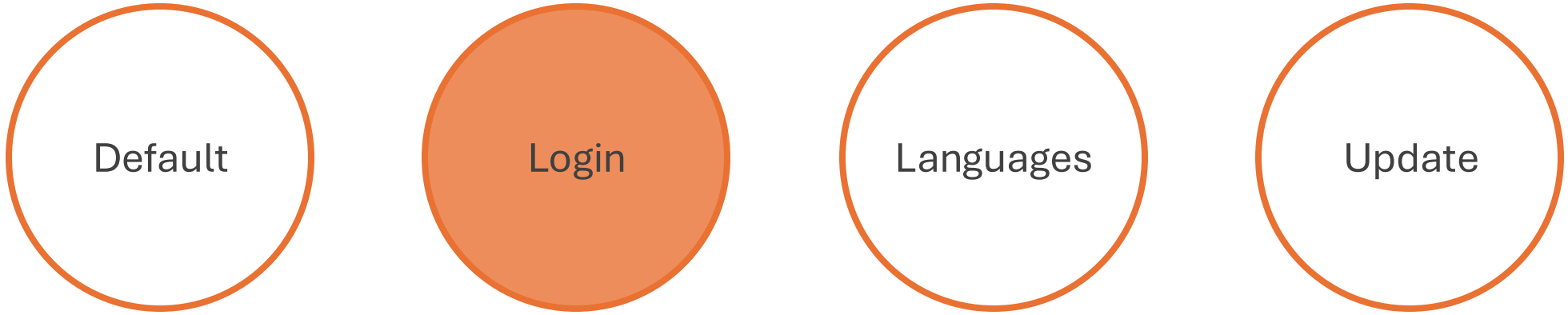
Thank you for your messages.

We will soon look into your requests.

We have informed the responsible parties.

Ticketing System Automatic Responses

Cloud Providers, Domain Name Owners, Universities, and so on



Count: 27

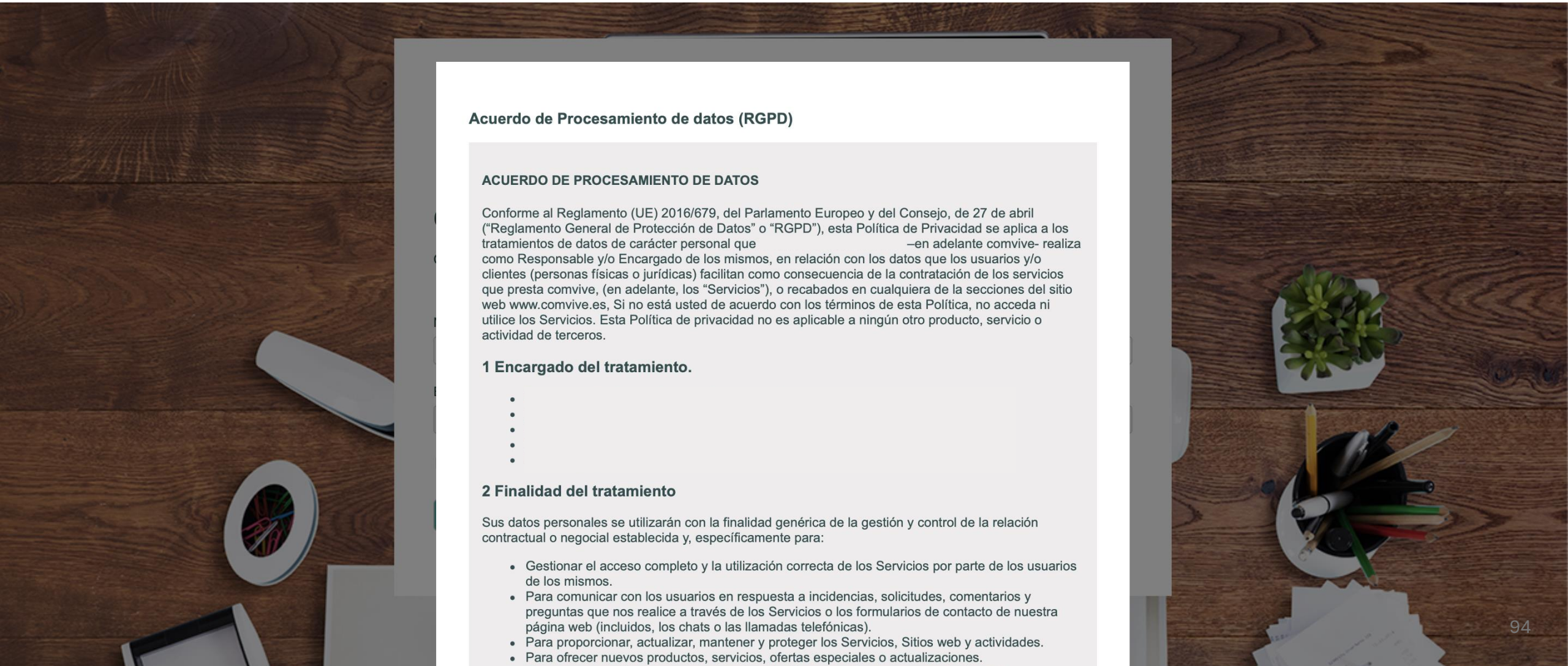
Please create an account and confirm the message

Please use the generated account and continue

Please agree with our policies then proceed

Ticketing System Automatic Responses

Cloud Providers, Domain Name Owners, Universities, and so on

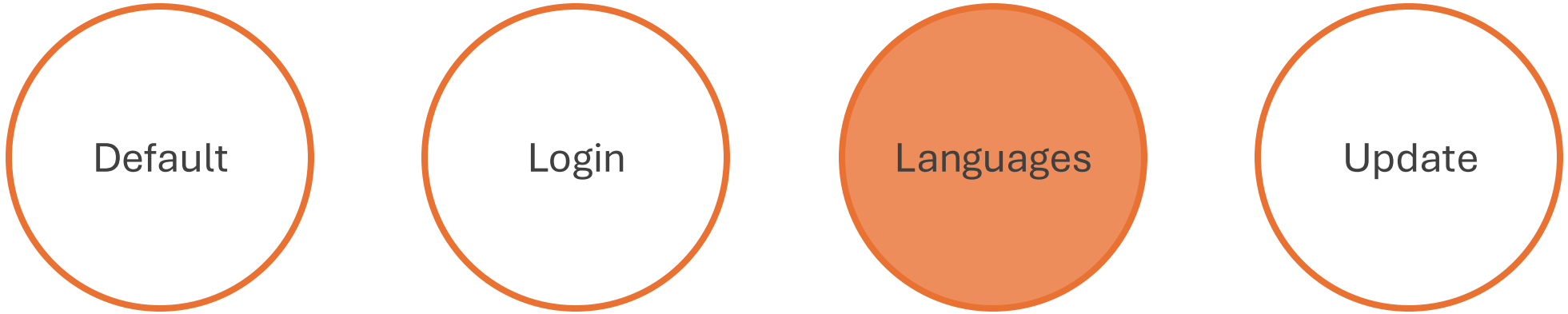


Ticketing System Automatic Responses

Cloud Providers, Domain Name Owners, Universities, and so on

Ticketing System Automatic Responses

Cloud Providers, Domain Name Owners, Universities, and so on



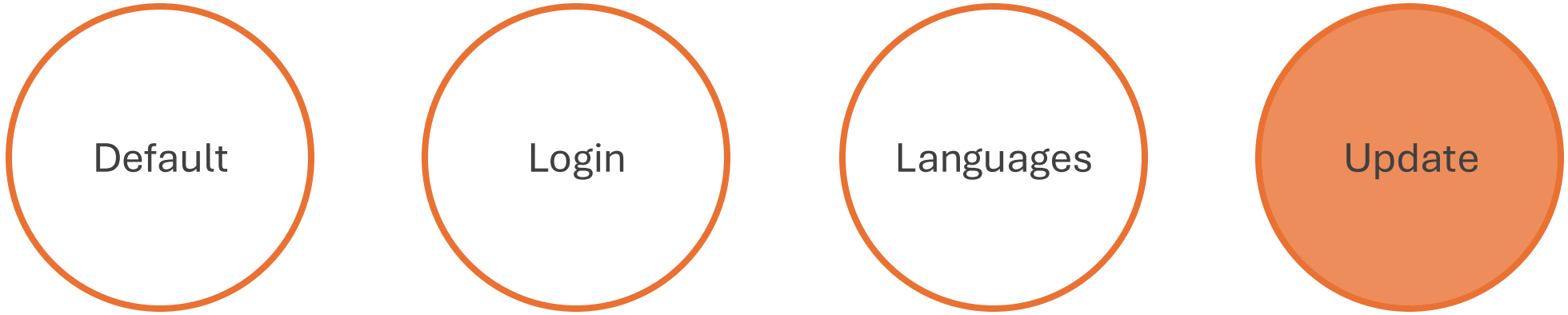
Count: 112

German, French, Spanish, Russian, Chinese, and more

The effort to understand properly can be high

Ticketing System Automatic Responses

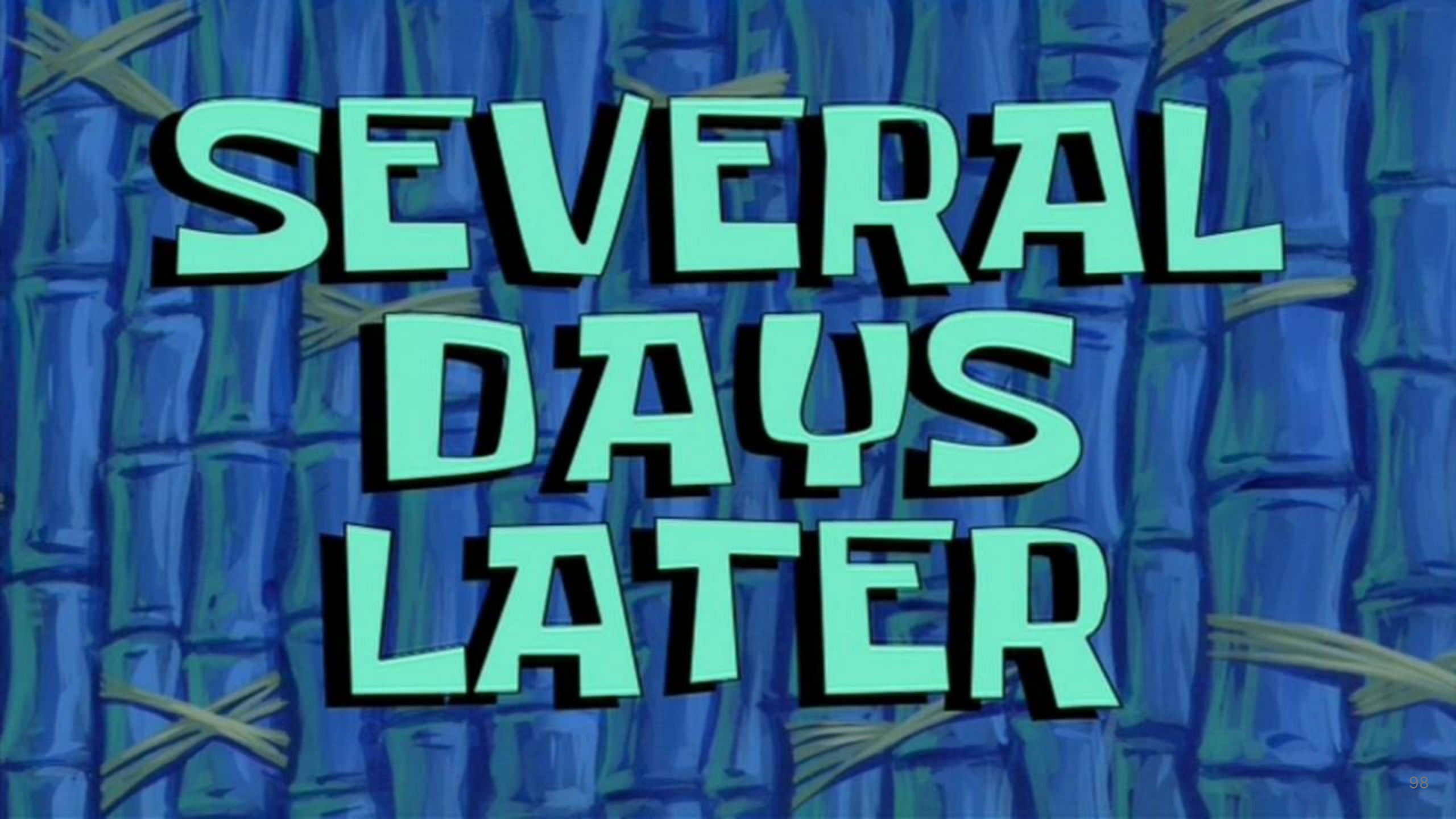
Cloud Providers, Domain Name Owners, Universities, and so on



Count: 7

Their communication with their customers

We can see the workflow and talk to the clients in 2 systems


SEVERAL
DAYS
LATER

Manual Responses

They care and they want to know more

32 Manual Responses - Question

- 4 No Further Response
- 28 Positive Responses

32 Manual Responses - Question

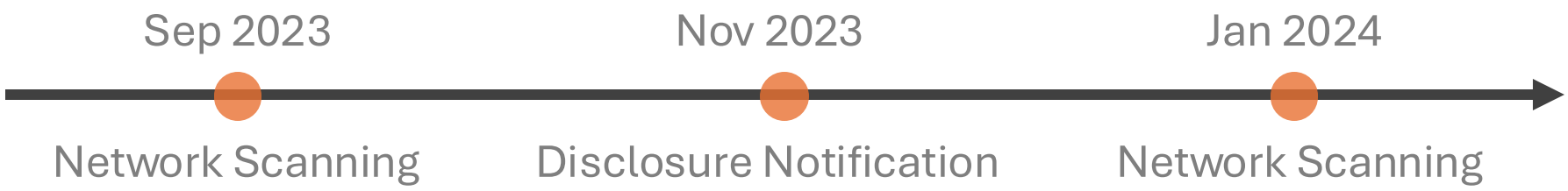
- 4 No Further Response
  - They did not respond nor fixed the issues
  - Our disclosure message doesn’t apply to their setup
- 28 Positive Responses

32 Manual Responses - Question

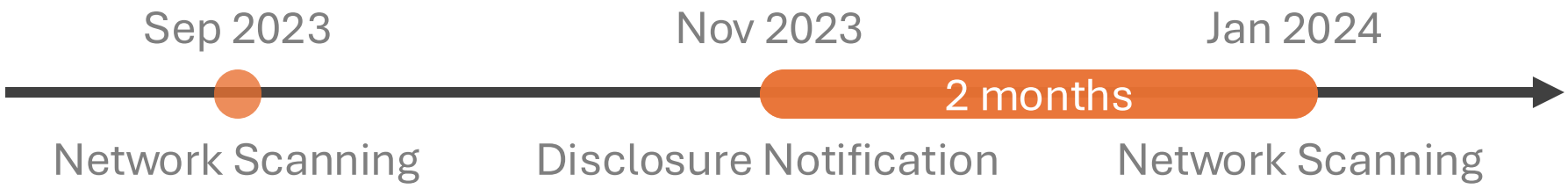
- 4 No Further Response
- 28 Positive Responses
  - They initiated active conversations with us
  - They needed more details to check on our systems
  - Few needed to handle the issues within 48/72 hrs
  - They solved the problem with our suggestions
  - Their clients didn’t respond and they took backends down
  - One asked for additional risk assessment

Did the stakeholders really fix the backends?

Network Scanning After the Disclosure



Network Scanning After the Disclosure



After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

Stakeholders addressed

all the vulnerabilities with CVEs

security issues as no authentication, unintended exposed access

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

Stakeholders addressed

all the vulnerabilities with CVEs

security issues as no authentication, unintended exposed access

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

Stakeholders did not address

all the vulnerabilities with CVEs

security issues as no authentication, unintended exposed access

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

Stakeholders did not address all the vulnerabilities with CVEs (The backends have no CVE) security issues as no authentication, unintended exposed access

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage
Mitigated All Issues	52	0.35 %
Mitigated CVEs only	282	1.90 %
No Change with CVEs	4780	32.22 %
No Change no CVES	6554	44.18 %
Unresponsive	3168	21.35 %

The backends were not responsive during the scanning due to IP address instability or going offline

After the Disclosure

15046 - 210 (Delivery Failure, all contacts failed) = 14836 IoT Backends / IP addresses

Type	Count	Percentage	
Mitigated All Issues	52	0.35 %	2.25%
Mitigated CVEs only	282	1.90 %	
No Change with CVEs	4780	32.22 %	
No Change no CVES	6554	44.18 %	
Unresponsive	3168	21.35 %	

Why didn’t the stakeholders fix the backends?

Reflections

Reflections based on **Challenges of CVD**

Reflections

Communication Channel

Effective Message

Organization Policies

Sufficient Time

Language

Reflections

Communication Channel - Email (WHOIS)

Pro	Effective for large-scale diverse contacts
Con	WHOIS email contact may not be always accurate (8 complaints)
Action	Need another reliable communication channel with stakeholders

Effective Message

Organization Policies

Sufficient Time

Language

Reflections

Communication Channel - Email (WHOIS)

Pro	Effective for large-scale diverse contacts
Con	WHOIS email contact not always accurate
Action	RDAP, Better Connection, Third Party

Effective Message

Organization Policies

Sufficient Time

Language

Reflections

Communication Channel - RDAP, Better Connection, Third Party

Effective Message

Pro	Draw attention with less details in case of wrong recipients
Con	Stakeholders prefer clear and informative initial message
Action	Depends on stakeholders and vulnerabilities

Organization Policies

Sufficient Time

Language

Reflections

Communication Channel - RDAP, Better Connection, Third Party

Effective Message - Depends on stakeholders and vulnerabilities

Organization Policies

Pro	We have clear outgoing policy from University of Twente
Con	Stakeholders with less interactive policy or no policy
Action	Be aware of the difference

Sufficient Time

Language

Reflections

Communication Channel - RDAP, Better Connection, Third Party

Effective Message - Depends on stakeholders and vulnerabilities

Organization Policies - Be aware of the difference

Sufficient Time

Pro	Approximately 90 days has become typical
Con	We have seen 48/72hrs mitigation time limits
Action	Stakeholders will have different mitigation time limits

Language

Reflections

Communication Channel - RDAP, Better Connection, Third Party

Effective Message - Depends on stakeholders and vulnerabilities

Organization Policies - Be aware of the difference

Sufficient Time - Apply different mitigation time limits

Language

Action Cooperation or local organizations like a CSIRT can be helpful

Key Takeaways

Communication Channel - RDAP, Better Connection, Third Party

Effective Message - Depends on stakeholders and vulnerabilities

Organization Policies - Be aware of the difference

Sufficient Time - Apply different mitigation time limits

Language - Contact local organizations

Future work ongoing!

For the next time you do **Coordinated Vulnerability Disclosure!**

University of Twente
Ting-Han Chen
Jeroen van der Ham-de Vos

Vienna University of Technology
Carlotta Tagliaro
Martina Lindorfer

Ruhr University Bochum
Kevin Borgolte


SHADOWSERVER

Wrap-up

Next lecture:

Wed June 18, 15:45-17:30

Topic: IoT forensics

Dr. Antonia Affinito | a.affinito@utwente.nl
Prof. Cristian Hesselman | c.e.w.hesselman@utwente.nl

UNIVERSITY OF TWENTE.

SIDN LABS