LTE Security Disabled
Misconfiguration in Commercial Networks

Merlin Chlosta, David Rupprecht, Thorsten Holz
RUHR UNIVERSITY BOCHUM

Christina Pöpper
NEW YORK UNIVERSITY ABU DHABI

May 16, 2019

Motivation – Complex Infrastructure

User

Base Stations

Core Network

Motivation – Complex Infrastructure

User

Base Stations

Core Network

Motivation – Complex Infrastructure

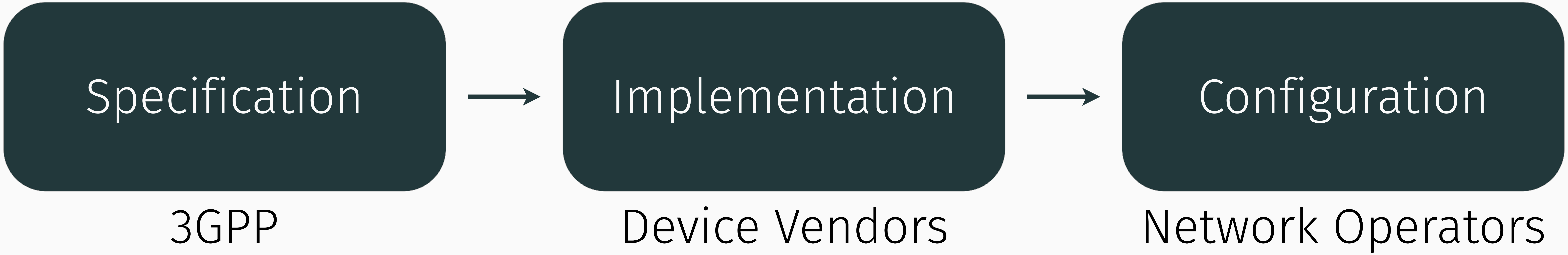
MOTOROLA
NOKIA
HUAWEI
NOKIA

User

Base Stations

Core Network

Research Question



Specification → Implementation → Configuration

3GPP

Device Vendors

Network Operators

- Recent work focuses on specification, implementation
- Configuration has potential to disable security measures

Security Capabilities

Security Capabilities

	Integrity	Encryption	
NULL	✗	?	
Snow3G	✓	✓	Mandatory
AES	✓	✓	
ZUC	?	?	Optional

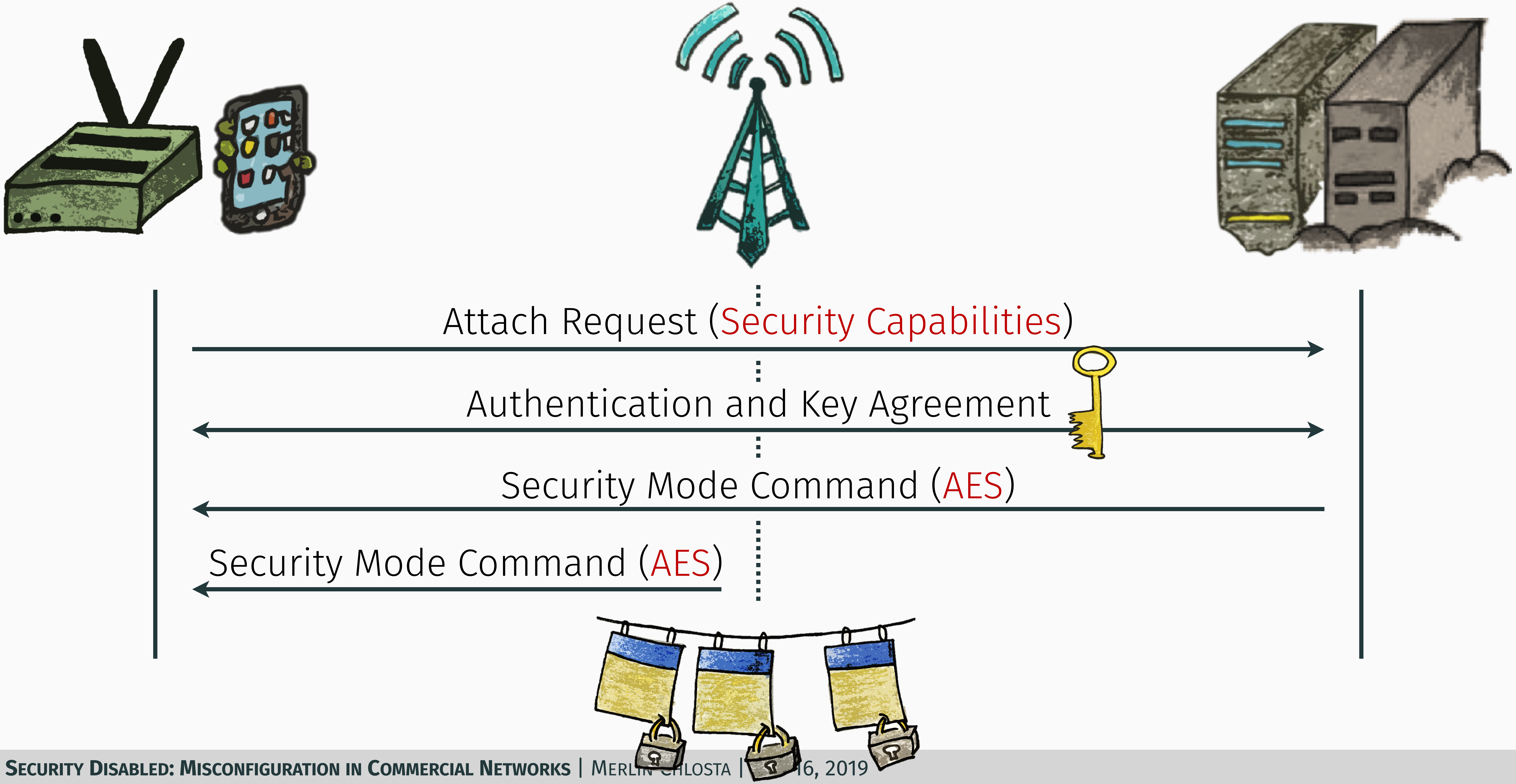
Security Capabilities

Emergency call without SIM

Legislative requirement

	Integrity	Encryption	
NULL	✗	?	
Snow3G	✓	✓	Mandatory
AES	✓	✓	
ZUC	?	?	Optional

Algorithm Negotiation



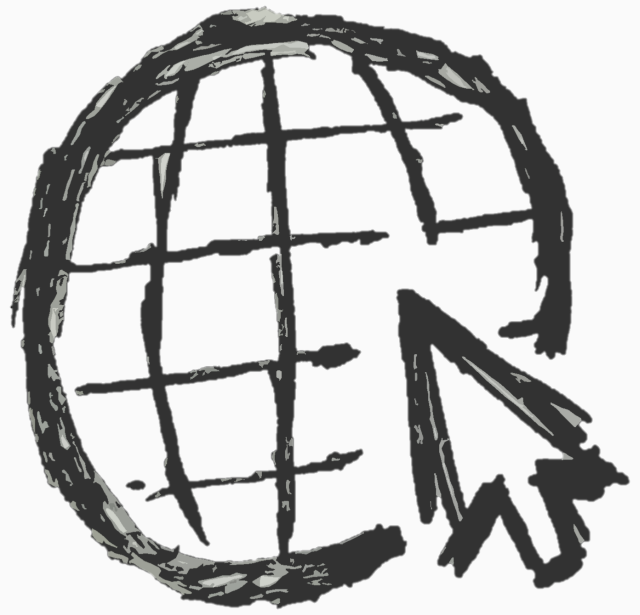
Attach Request (Security Capabilities)

Authentication and Key Agreement

Security Mode Command (AES)

Security Mode Command (AES)

Tools for Network Testing



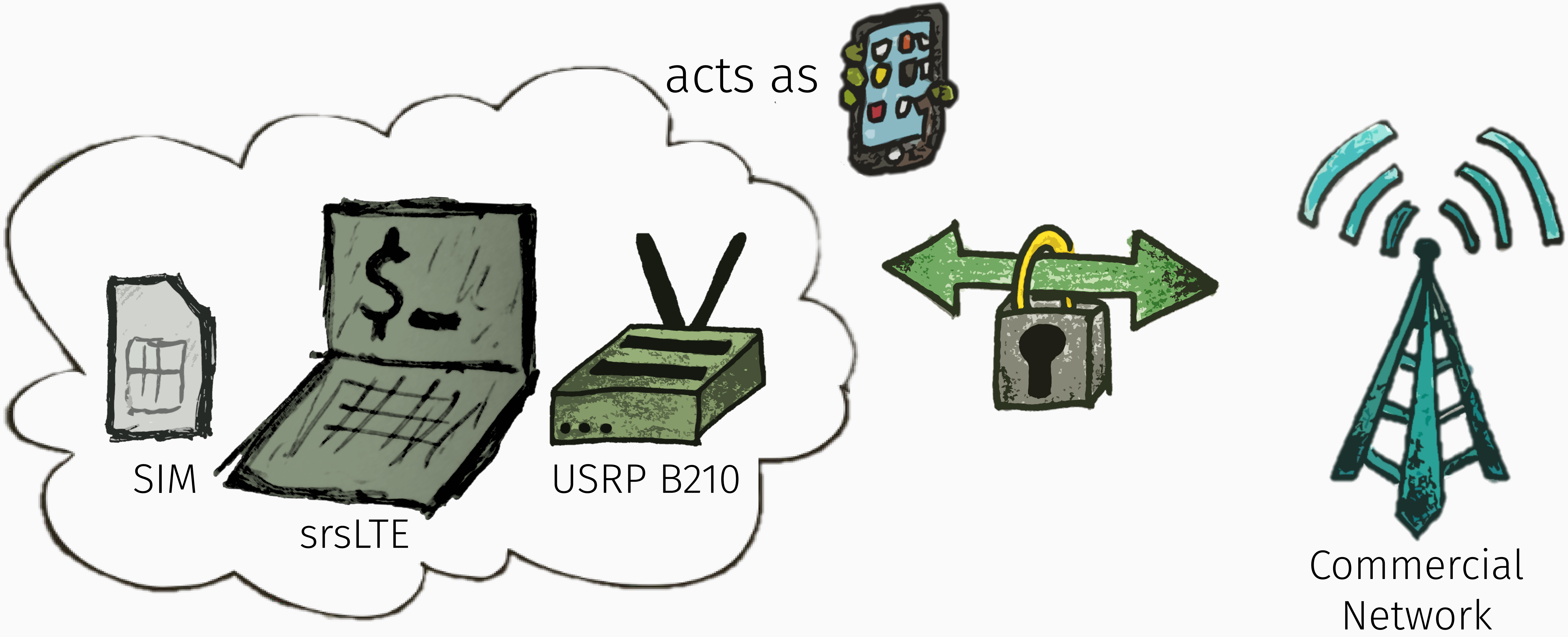
NMAP

Nessus®

?

Our paper: provide standard test — security algorithm support

Equipment – Software-Defined Radio



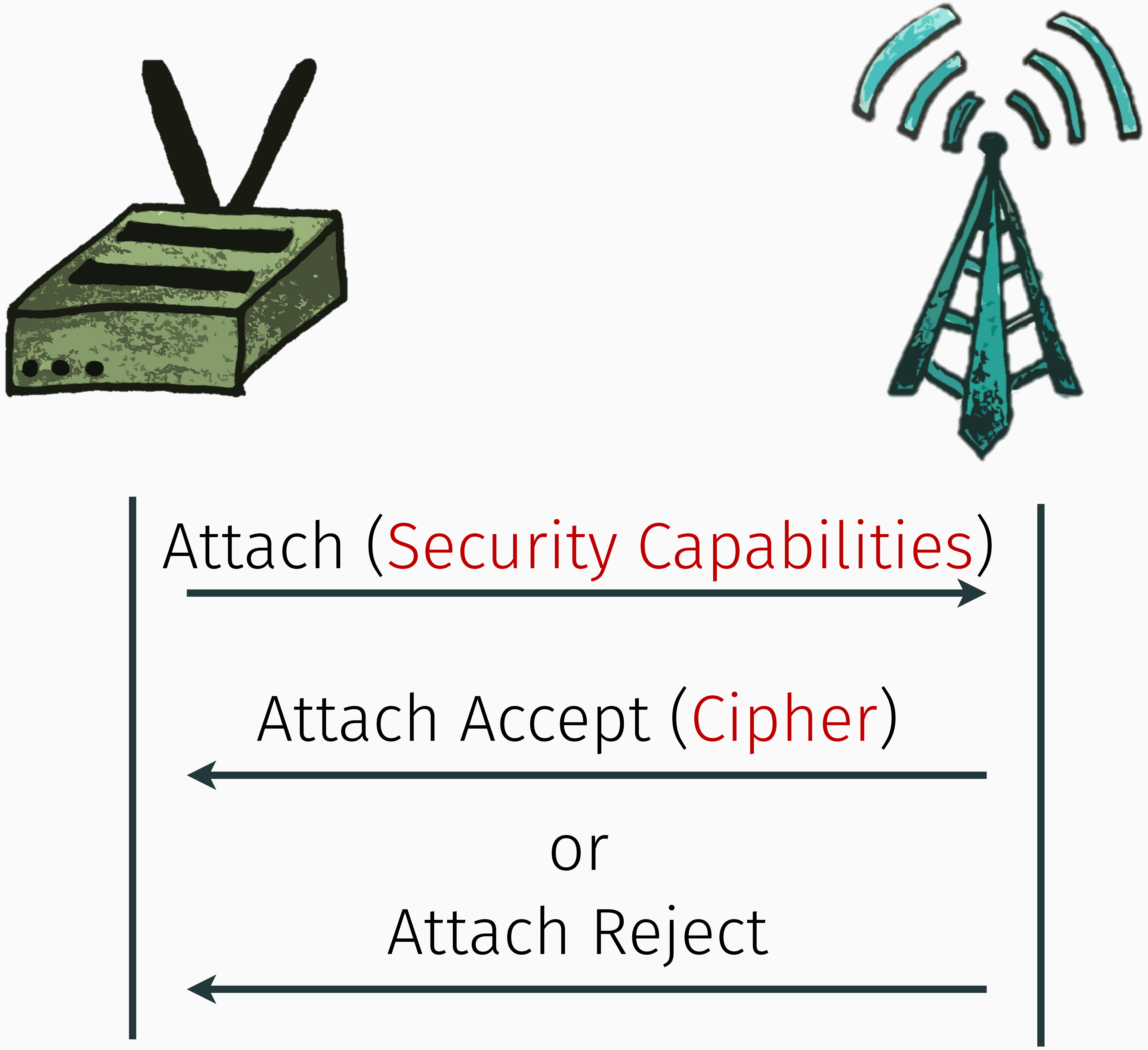
Contribution: SIM cards and encryption for srsLTE

Commercial network support, tested at operator's lab

Security Modes

What Do Real Networks Say?

Test Procedure



Attach (Security Capabilities)

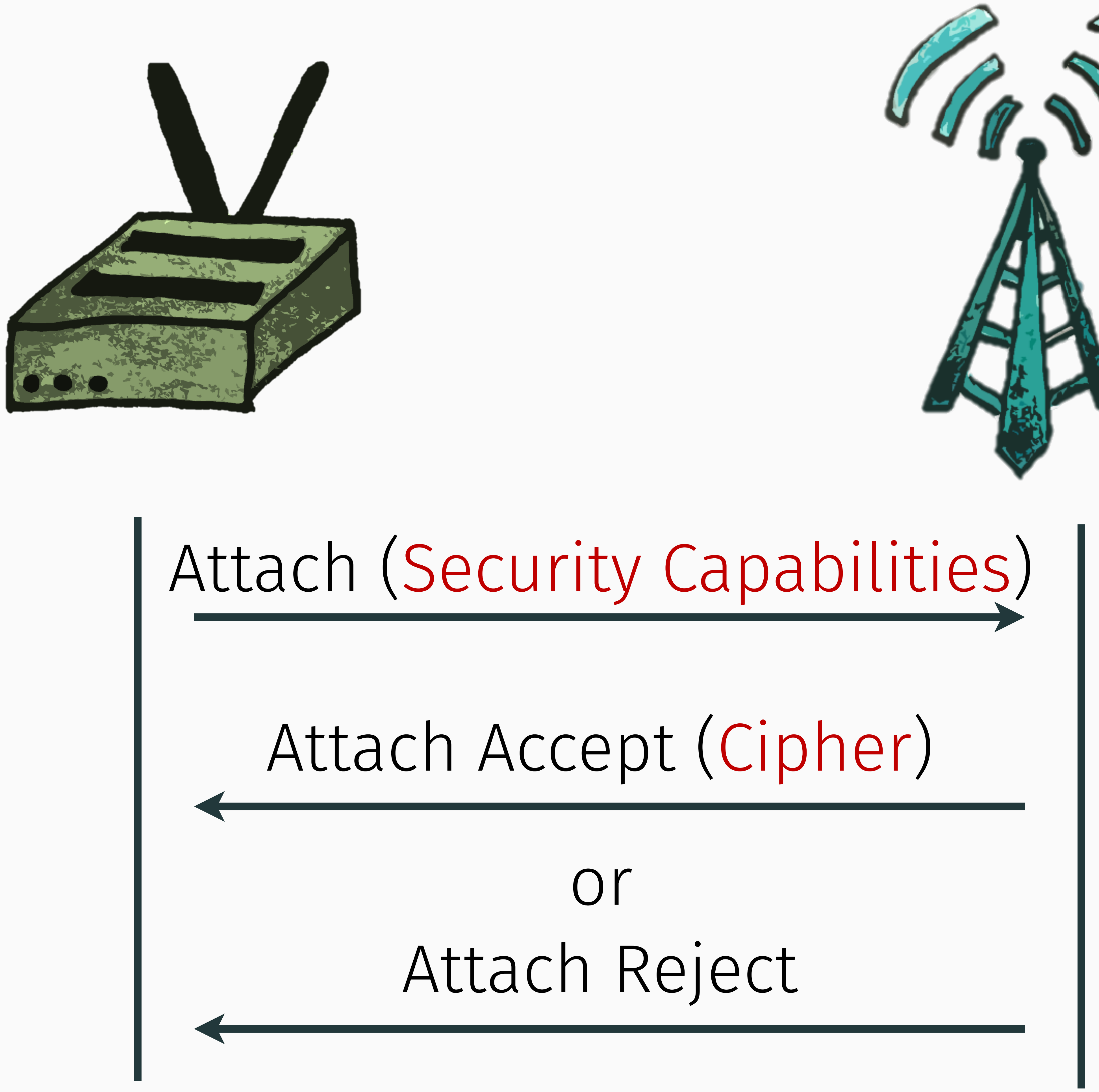
Attach Accept (Cipher)

or

Attach Reject

Security Capabilities — Example Test Case

Test Procedure



Attach (Security Capabilities)

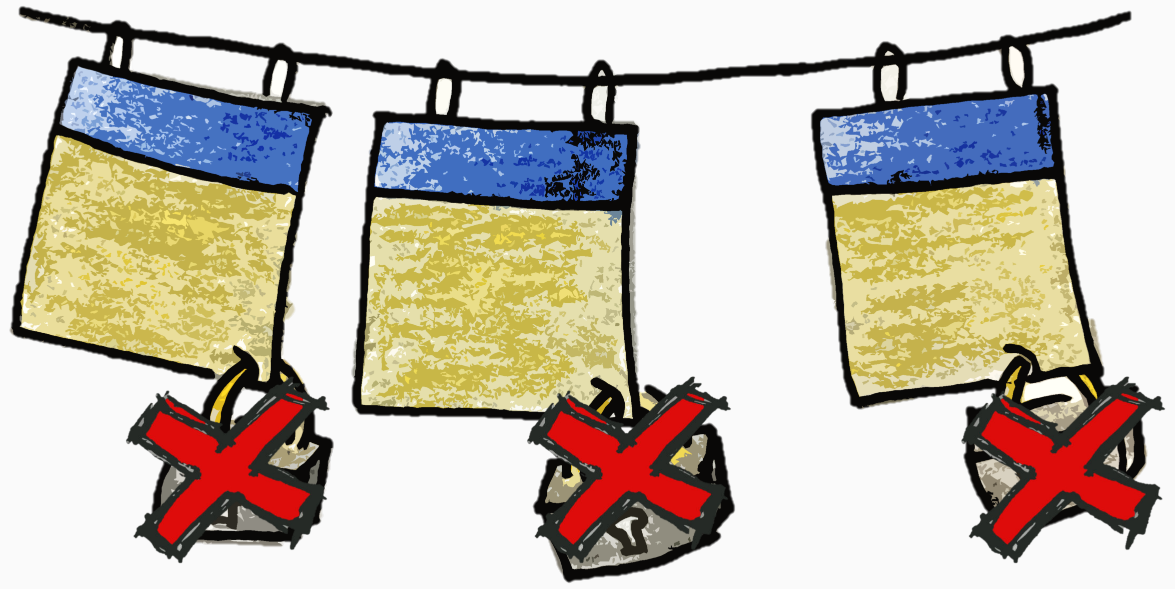
Attach Accept (Cipher)

or

Attach Reject

Security Capabilities — Example Test Case

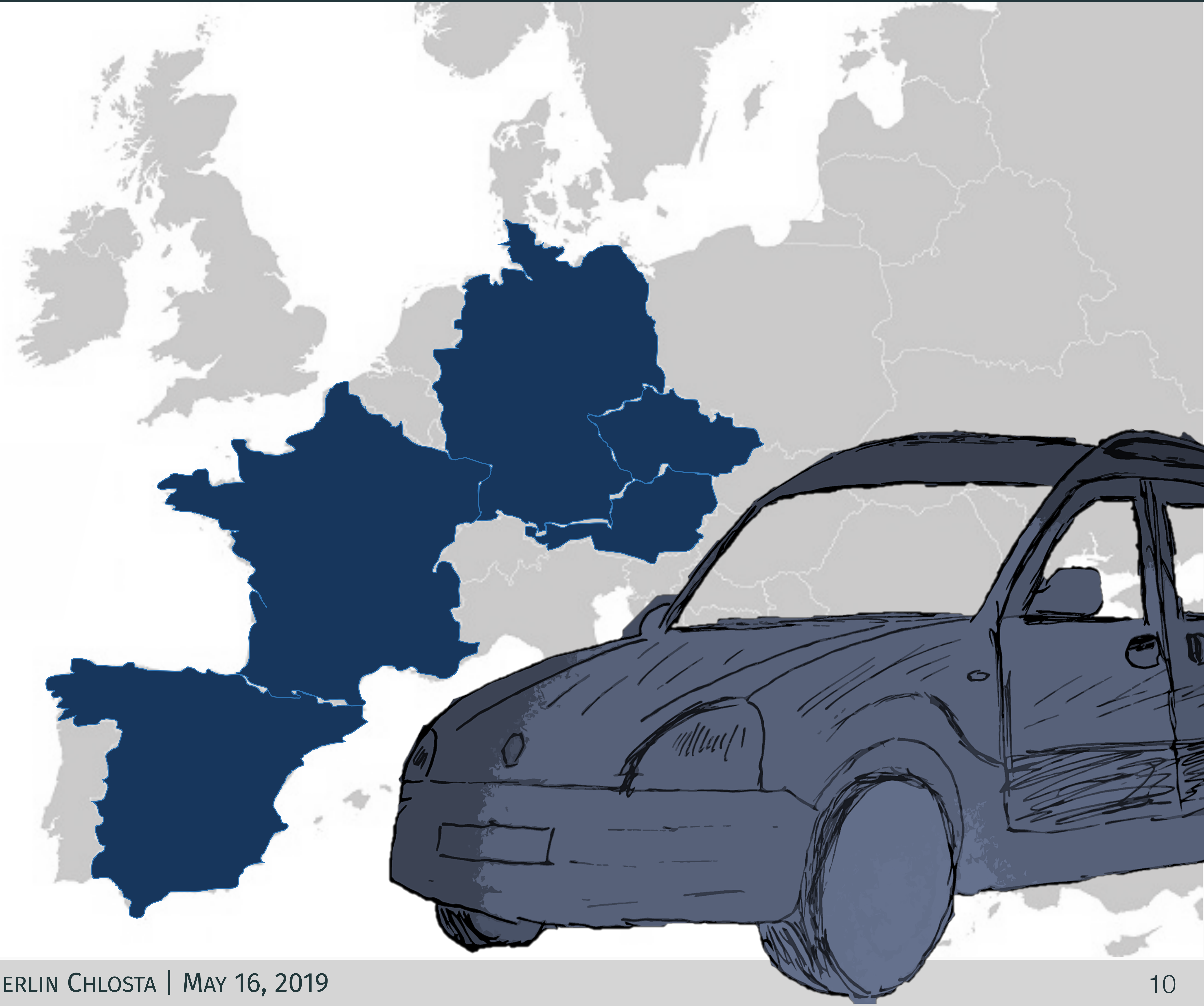
	Integrity	Encryption	
NULL	✓	✓	Plaintext
Snow3G	✗	✗	
AES	✗	✗	
ZUC	✗	✗	



Drive Tests

- 12 operators in 5 countries

- Reception in hotels, mobility
- Car-mounted setup



Results

What Could Go Wrong?

Full Results

	AT-1	AT-2	CZ-1	CZ-2	CZ-3	DE-1	DE-2	DE-3	ES-1	ES-2	ES-3	FR-1
Null-Encryption	!		!				!		!	!	!	
Null-Integrity	!		!				!			!		

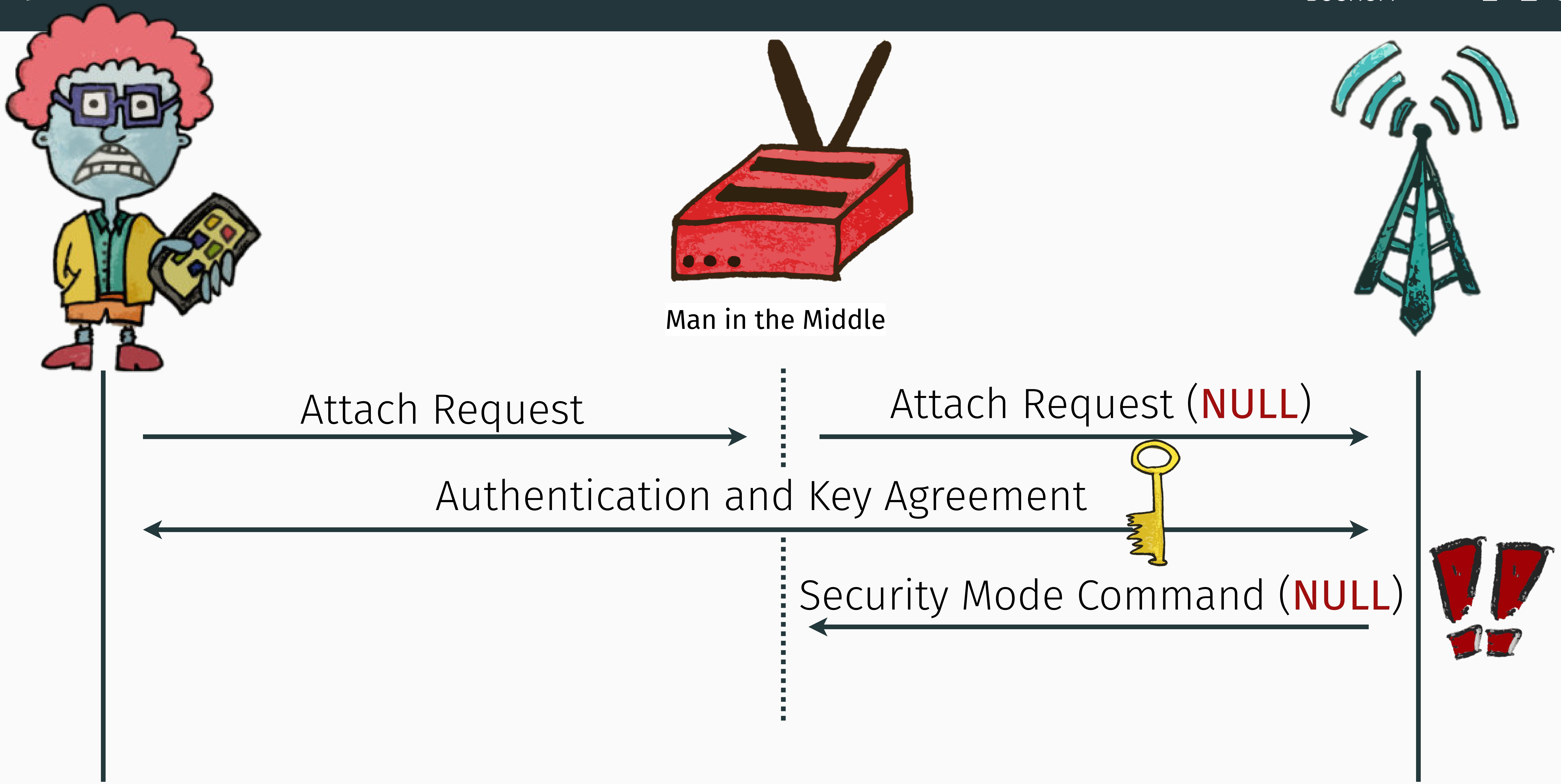
Null-Encryption & Null-Integrity

Key Findings – Null-Integrity & Null-Encryption

NULL ok? — Sure

- Completely undermines LTE security goals
  - Unauthenticated users, network and traffic
- Enables impersonation attack in 3 out of 12 networks
  - Free data, anonymous Internet access.

Impersonation Attack



Man in the Middle

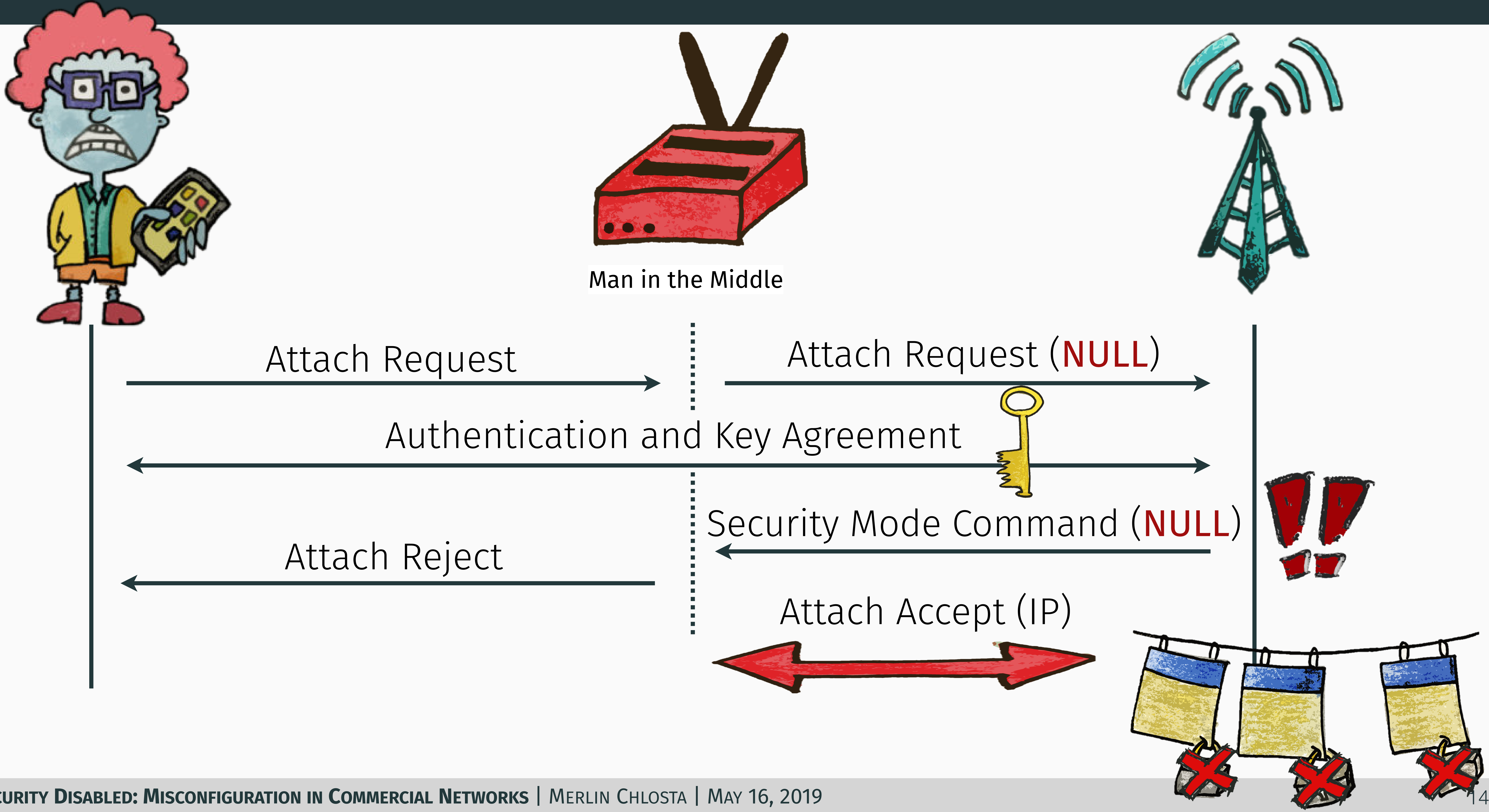
Attach Request

Attach Request (NULL)

Authentication and Key Agreement

Security Mode Command (NULL)

Impersonation Attack



Man in the Middle

Attach Request

Attach Request (NULL)

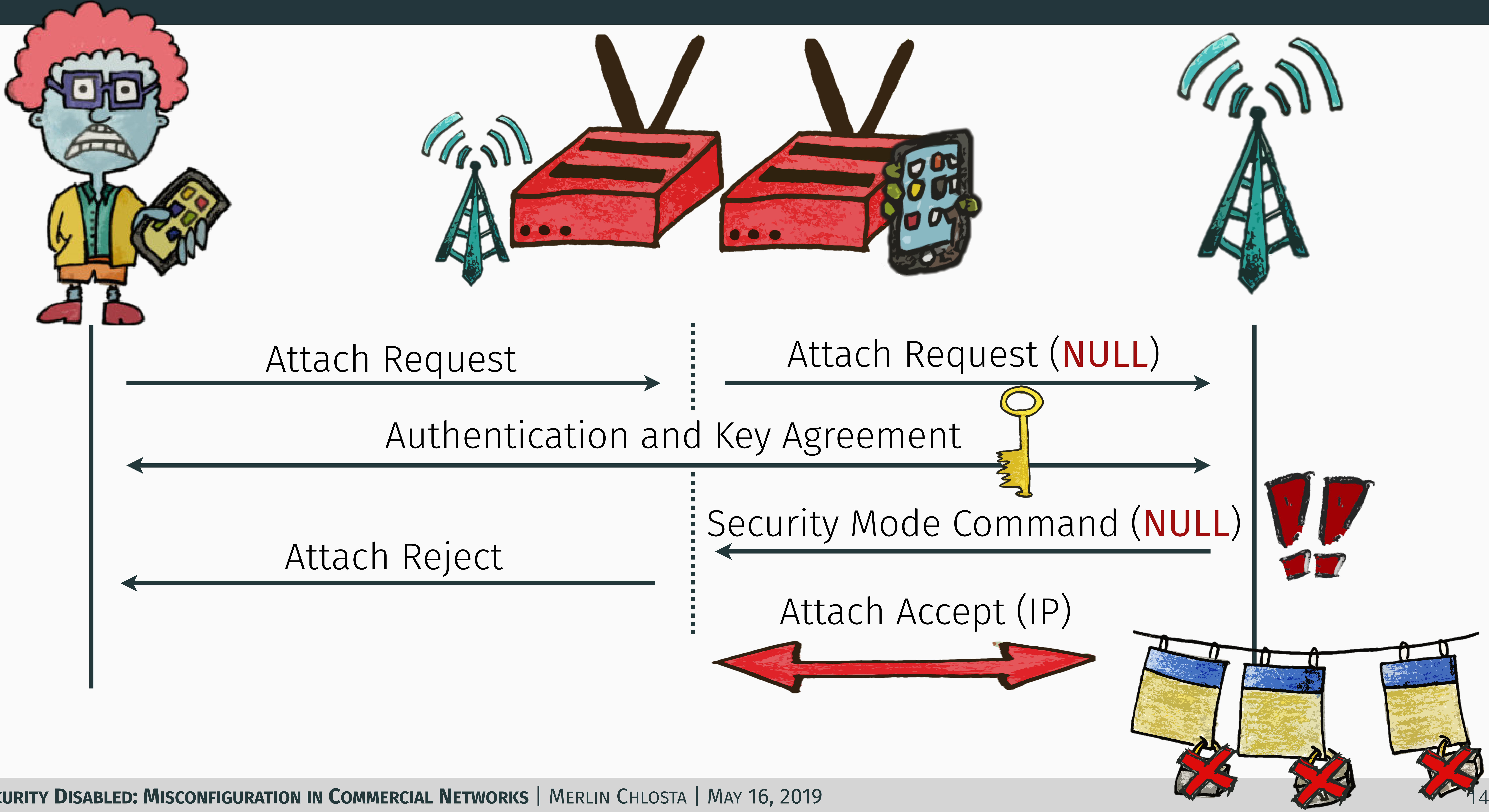
Authentication and Key Agreement

Security Mode Command (NULL)

Attach Reject

Attach Accept (IP)

Impersonation Attack



Attach Request

Attach Request (NULL)

Authentication and Key Agreement

Security Mode Command (NULL)

Attach Reject

Attach Accept (IP)

Worldwide Impact

Forward authentication via Internet

Full Results

	AT-1	AT-2	CZ-1	CZ-2	CZ-3	DE-1	DE-2	DE-3	ES-1	ES-2	ES-3	FR-1
Null-Encryption	❗		❗				❗		❗	❗	❗	
Null-Integrity	❗		❗				❗			❗		

Null-Encryption & Null-Integrity

Insecure Fallback

Key Findings – Insecure Fallback

NULL ok? — No. Go away.

ZUC ok? — No, but let’s talk NULL.

Key Findings – Insecure Fallback

RUHR UNIVERSITÄT BOCHUM RUB

Occurs in two cases

- Empty security capabilities (not even NULL signalled)
- Base station and core network disagree

NULL ok? — No. Go away.

ZUC ok? — No, but let's talk NULL. !!

Full Results

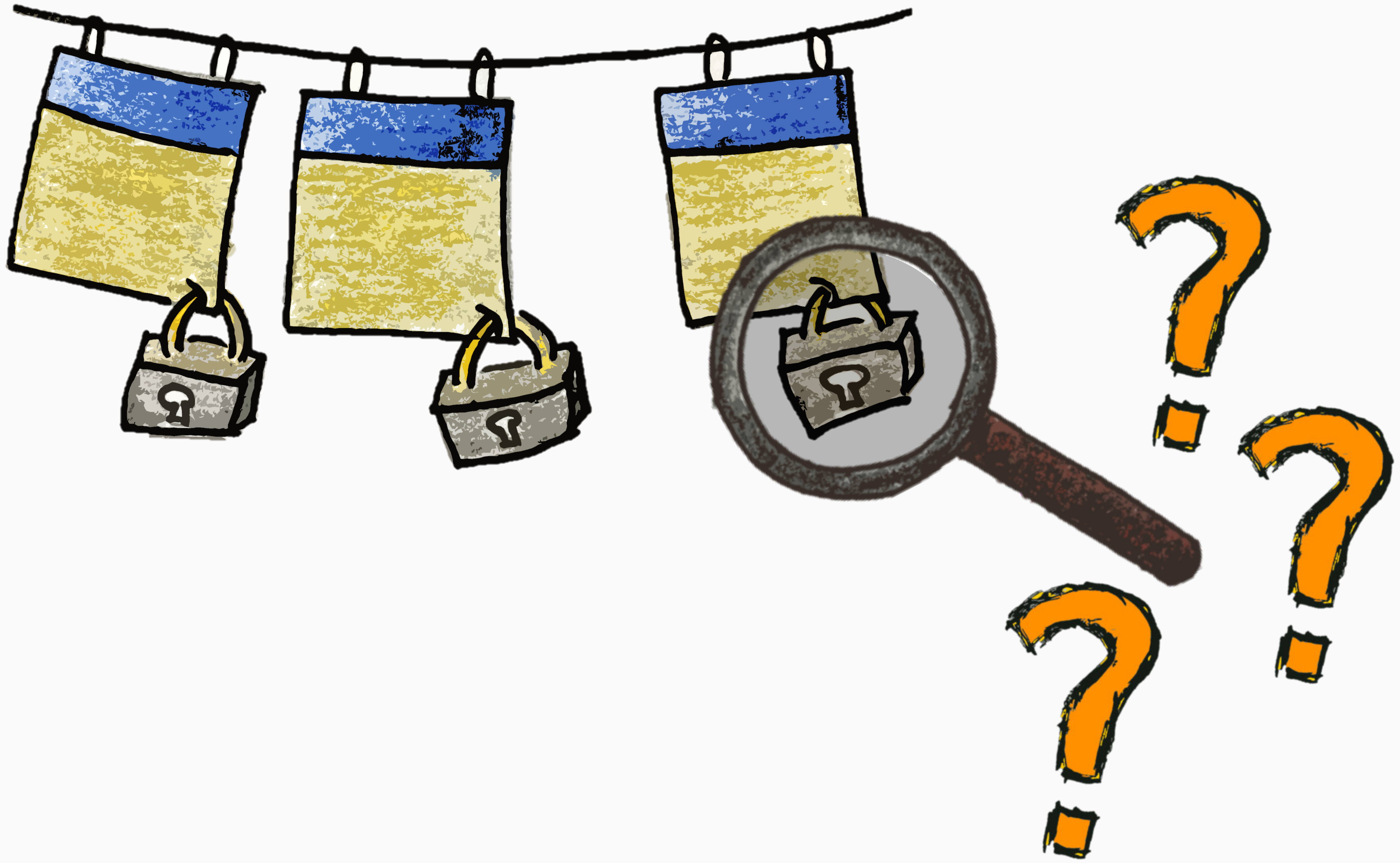
	AT-1	AT-2	CZ-1	CZ-2	CZ-3	DE-1	DE-2	DE-3	ES-1	ES-2	ES-3	FR-1
Null-Encryption	❗		❗				❗		❗	❗	❗	
Null-Integrity	❗		❗				❗			❗		

Null-Encryption & Null-Integrity

Insecure Fallback

Illegal Encoding

Key Findings – Illegal Encoding



- Base station signals *undefined* “EIA7” integrity
- In practice: EIA7 == EIA0 == Null-Integrity

Disclosure

- GSMA Coordinated Disclosure CVD-2018-13
  - Contact with vendors, operators, standardisation
- Changes integrated to 4G, 5G standards
- Immediate mitigation by affected operators

- Null-integrity & null-encryption is reality
  - Insecure Fallback
  - Encoding Issues
- Impersonation Attack in Commercial Networks

Download at
https://github.com/mrlnc/eia0