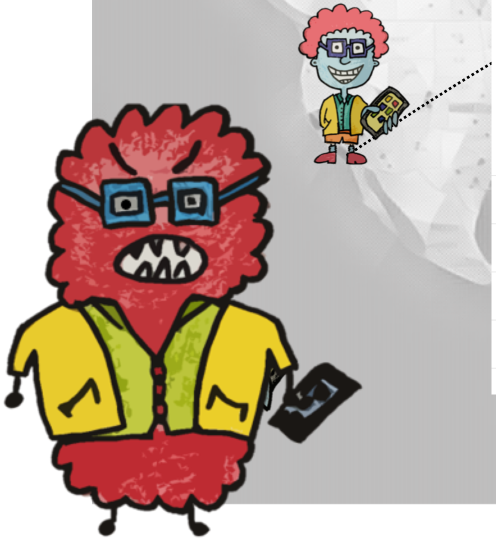
IMP4GT

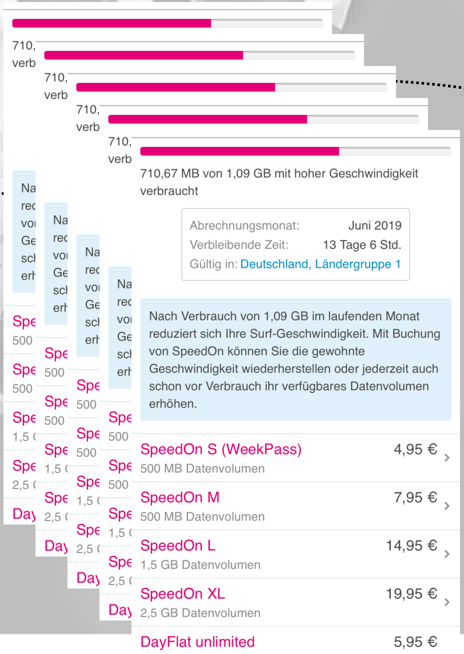
IMPersonation Attacks in 4G NeTworks

David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper

25.02.2020 NDSS Symposium, San Diego, USA

Motivation: Internet Passes



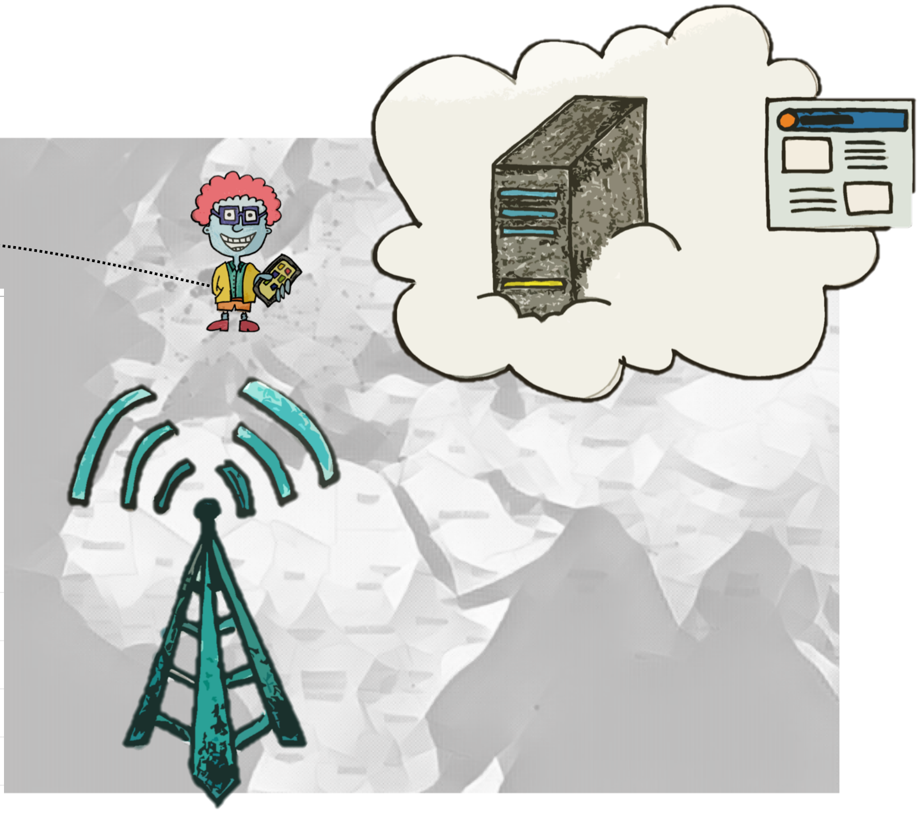


710,67 MB von 1,09 GB mit hoher Geschwindigkeit verbraucht

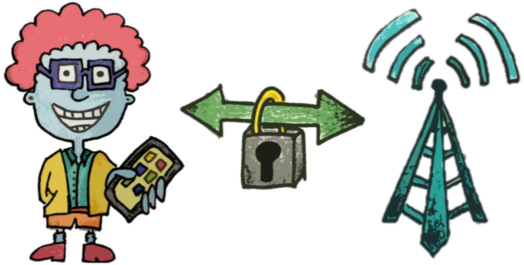
Abrechnungsmonat:	Juni 2019
Verbleibende Zeit:	13 Tage 6 Std.
Gültig in: Deutschland, Ländergruppe 1	

Nach Verbrauch von 1,09 GB im laufenden Monat reduziert sich Ihre Surf-Geschwindigkeit. Mit Buchung von SpeedOn können Sie die gewohnte Geschwindigkeit wiederherstellen oder jederzeit auch schon vor Verbrauch ihr verfügbares Datenvolumen erhöhen.

SpeedOn S (WeekPass) 500 MB Datenvolumen	4,95 € ›
SpeedOn M 500 MB Datenvolumen	7,95 € ›
SpeedOn L 1,5 GB Datenvolumen	14,95 € ›
SpeedOn XL 2,5 GB Datenvolumen	19,95 € ›
DayFlat unlimited	5,95 €



LTE Security Aims

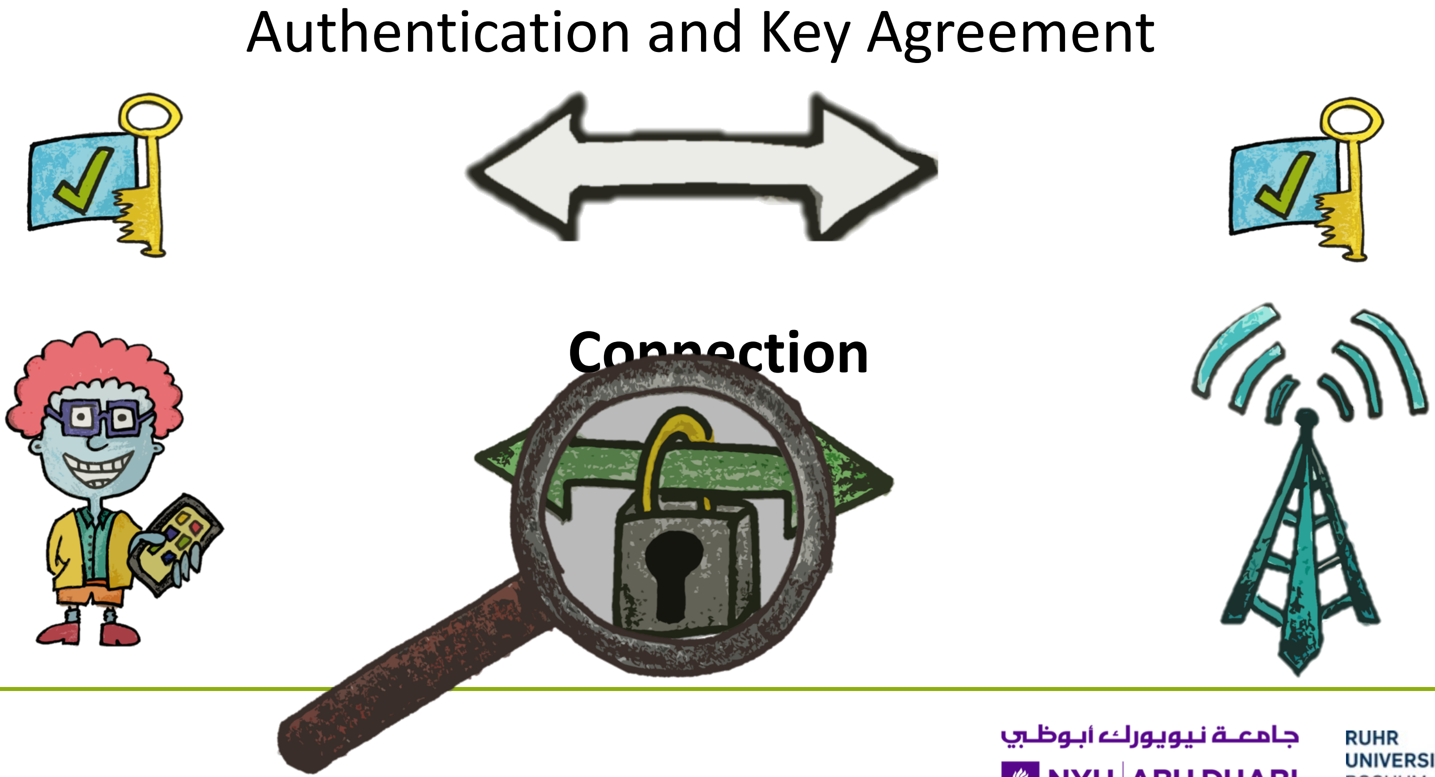


Mutual Authentication

Traffic Confidentiality

Identity & Location Confidentiality

Security Features



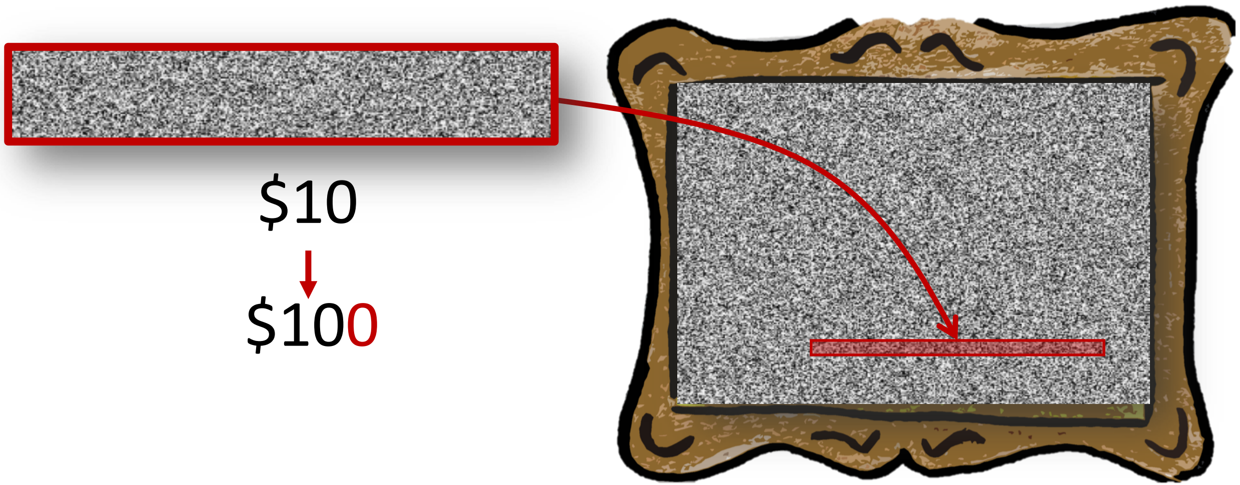
Authentication and Key Agreement

Connection

Missing Integrity Protection

🔒	Control Plane	User Plane
Encryption stream cipher	✓	✓
Integrity Protection	✓	✗

Malleable Encryption



$10

↓

$100

Stream Cipher

$$\begin{array}{cc} & 1\;0\;1\;0 \\ \oplus & 0\;1\;0\;1 \\ = & 1\;1\;1\;1 \end{array}$$

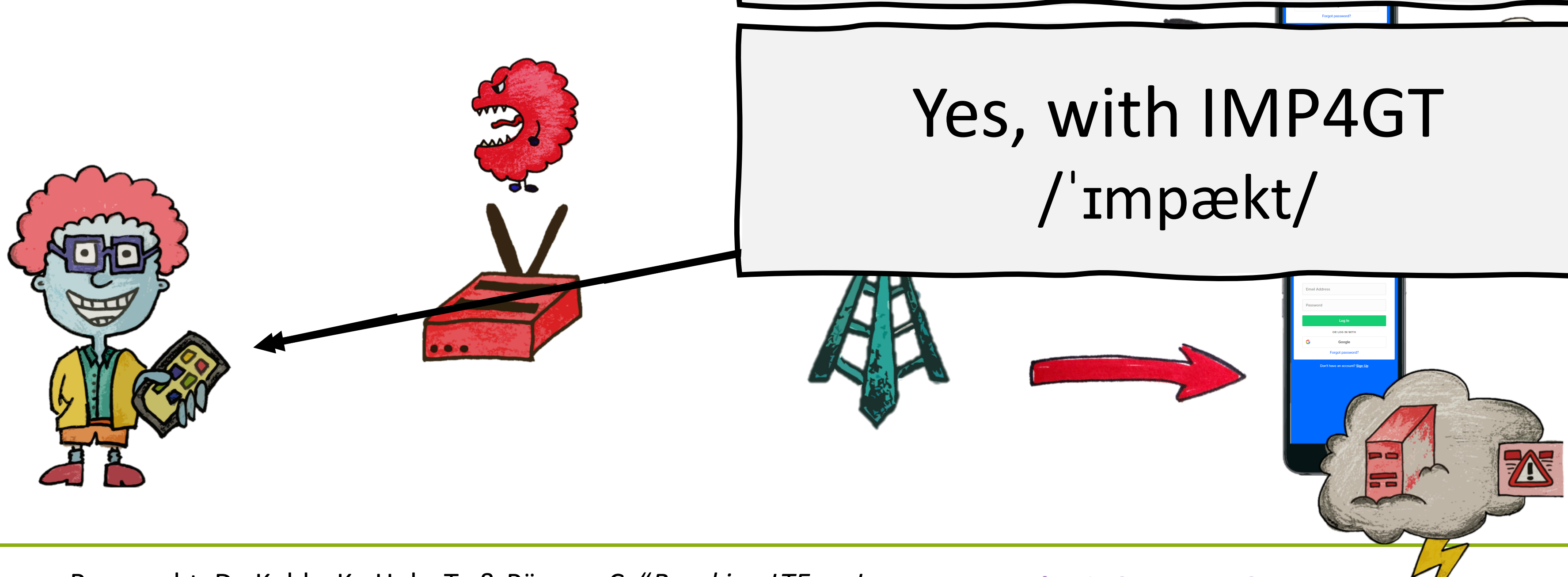
Encryption

Decryption

Already Known: Redirection

Can it be worse?

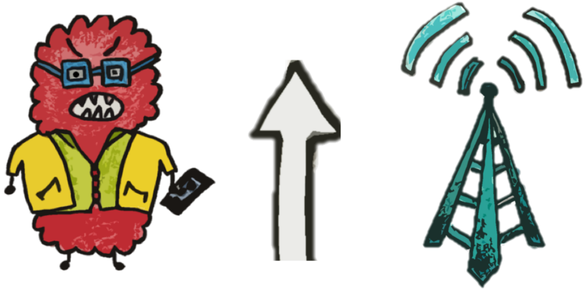
Yes, with IMP4GT
/ˈɪmpækt/

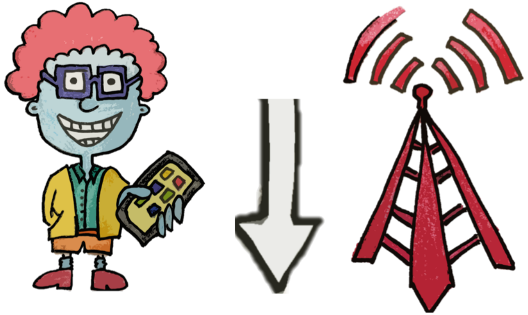


Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. “*Breaking LTE on Layer Two*”. In 2019 IEEE Symposium on Security and Privacy (SP)

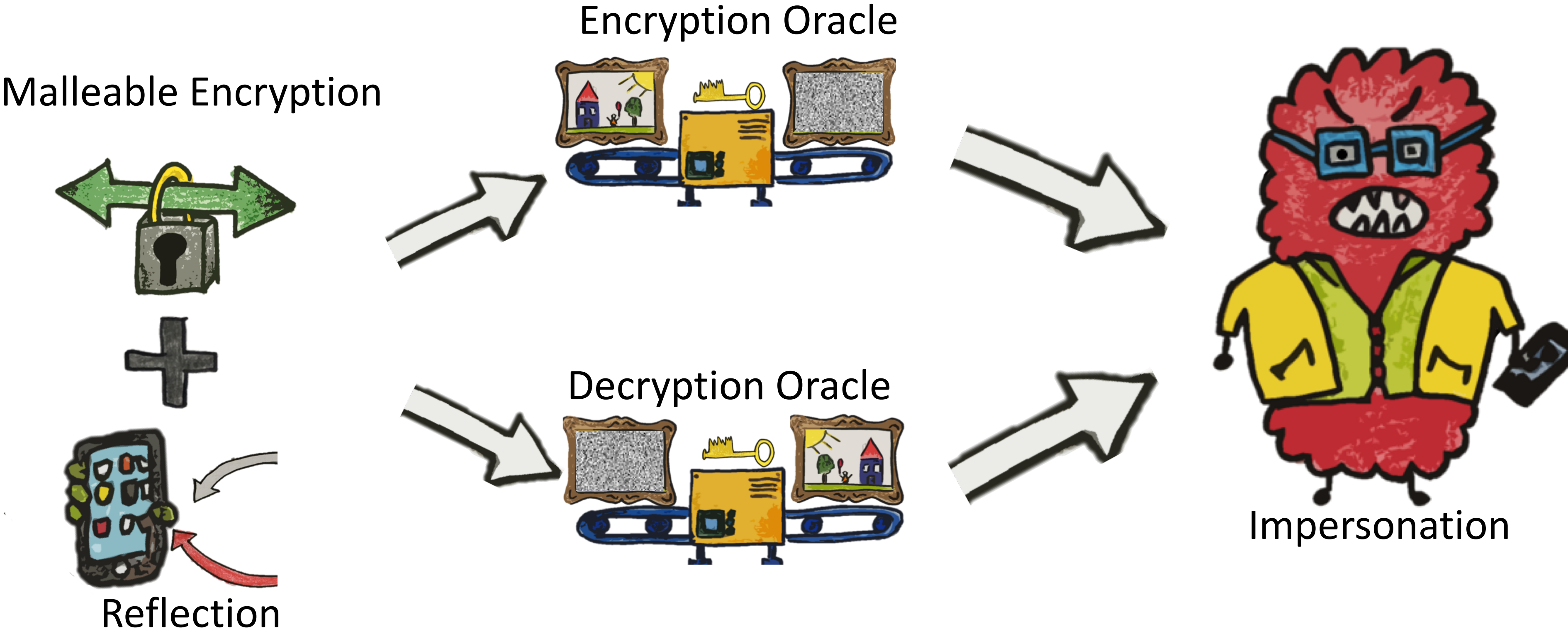
Impersonation in 4G Networks (IMP4GT)

Breaks mutual authentication
in **both directions.**





The Basic Principle



Malleable Encryption

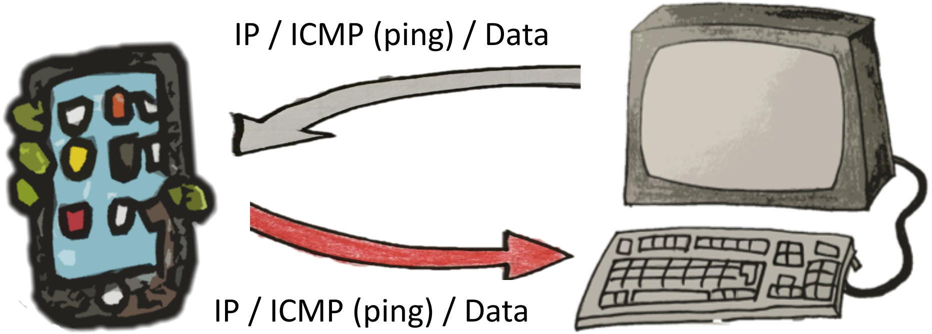
Reflection

Encryption Oracle

Decryption Oracle

Impersonation

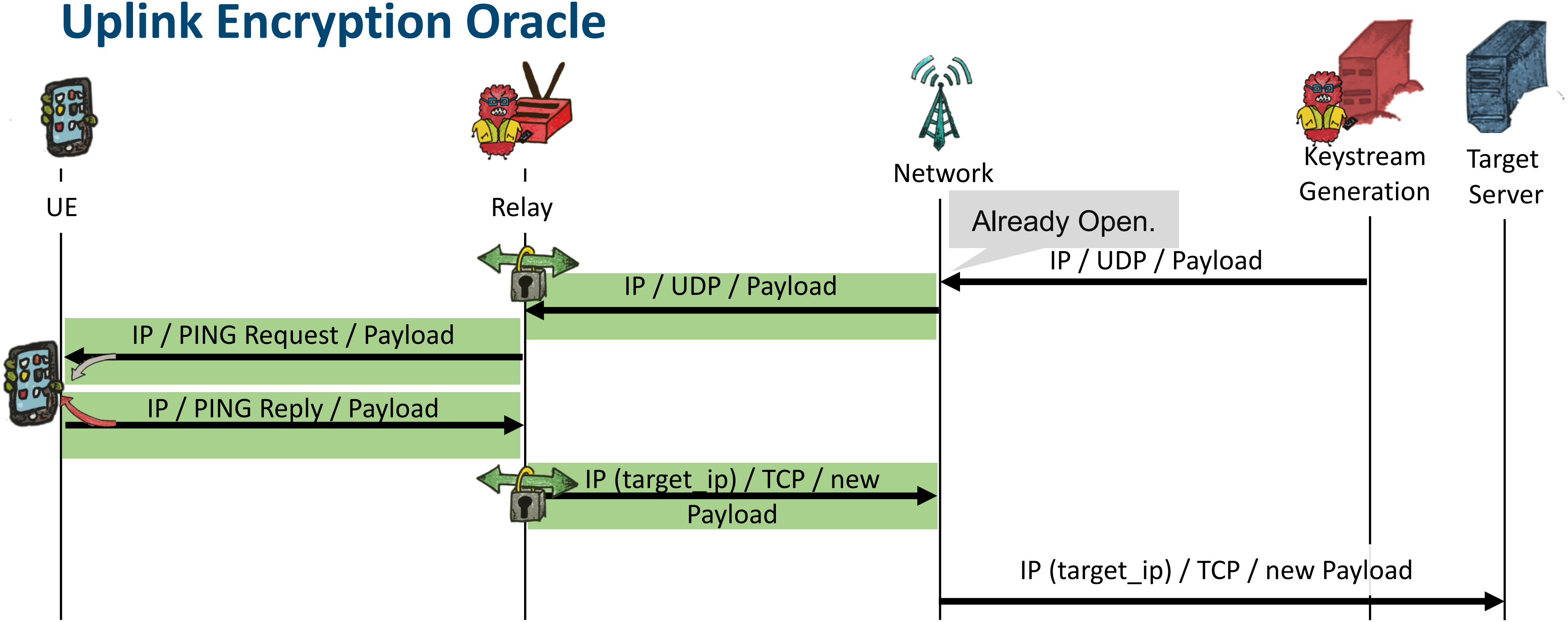
Reflection: ICMP Ping



IP / ICMP (ping) / Data

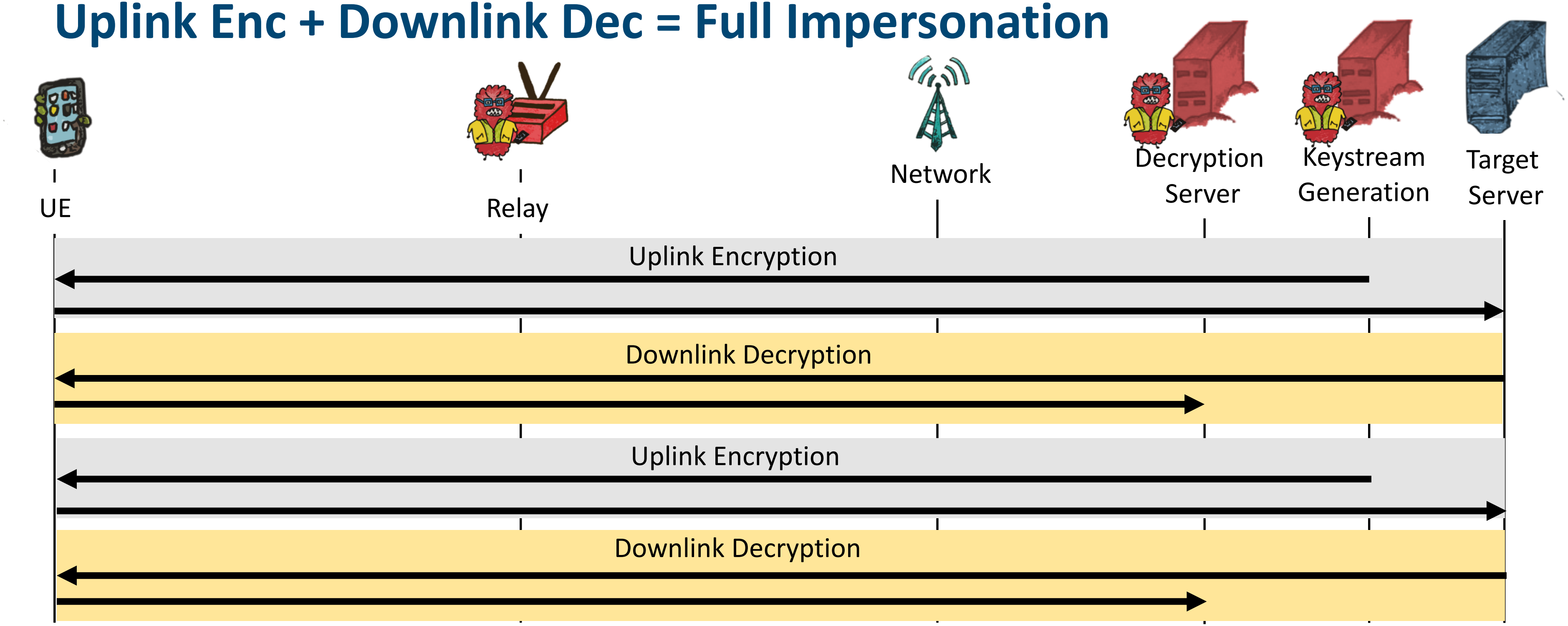
IP / ICMP (ping) / Data

Uplink Encryption Oracle


UE
Relay
Network
Keystream Generation
Target Server
Already Open.
IP / UDP / Payload
IP / UDP / Payload
IP / PING Request / Payload
IP / PING Reply / Payload
IP (target_ip) / TCP / new Payload
IP (target_ip) / TCP / new Payload

Encrypted on the Radio Layer

Uplink Enc + Downlink Dec = Full Impersonation



Experiments

- **Commercial** network and phone
- **Uplink** impersonation
  - Visit a website only accessible by a **victim:** pass.telekom.de
  - **Upload** a 10KB file to a server
- **Downlink** impersonation
  - **TCP** connection towards the phone
- **No** interaction of the user
  - **connectivitycheck.android.com**
  - Checks if you have an Internet connection

SRSLTE

Consequences

Providers

- Over Billing
- Authorization

Law Enforcement

- Lawful Interception
- Lawful Disclosure Process

User

- Privacy
- Firewall / NAT
- IoT

Conclusion: We need Integrity Protection!

David Rupprecht
Ruhr University Bochum
david.rupprecht@rub.de
https://imp4gt-attacks.net

- Fully specified and deployed
- Unlikely…

- Optional integrity protection
- Limited support in early implementations

We emphasize the need for mandatory integrity protection.