THALES

Moving to 4G PMR:
What are the cyber threats and how to mitigate them?

PSCE MUNICH – 4TH MAY 2017
JÉRÔME BROUET – PRODUCT LINE MANAGER

OPEN

Agenda

You (are) will be exposed !

It already happened!

Where are the risks?

Recommendations

OPEN

THALES

You (are) will be exposed!

TETRA

LTE

- **Specialized standard (millions users)**
- **(Circuit) Voice intensive**
- **Narrowband data**
- **Legacy terminal OS**
- **Private / closed systems**
- **Limited interfaces to other networks**
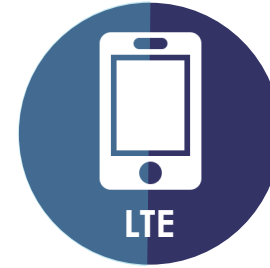
- **Open and global standard (billions users)**
- **All-IP services**
- **Application intensive**
- **Terminal OS = Android**
- **Private / Hybrid / Commercial deployments**
- **Interworking with other networks**

MANY OPERATIONAL BENEFITS, BUT INCREASED CYBER-RISKS

OPEN

THALES

3

It already happened!

Non-malicious

Malicious

Signaling flood

Catfishing

"State-sponsored hackers turn to Android malware to spy on Israeli soldiers", January 2017
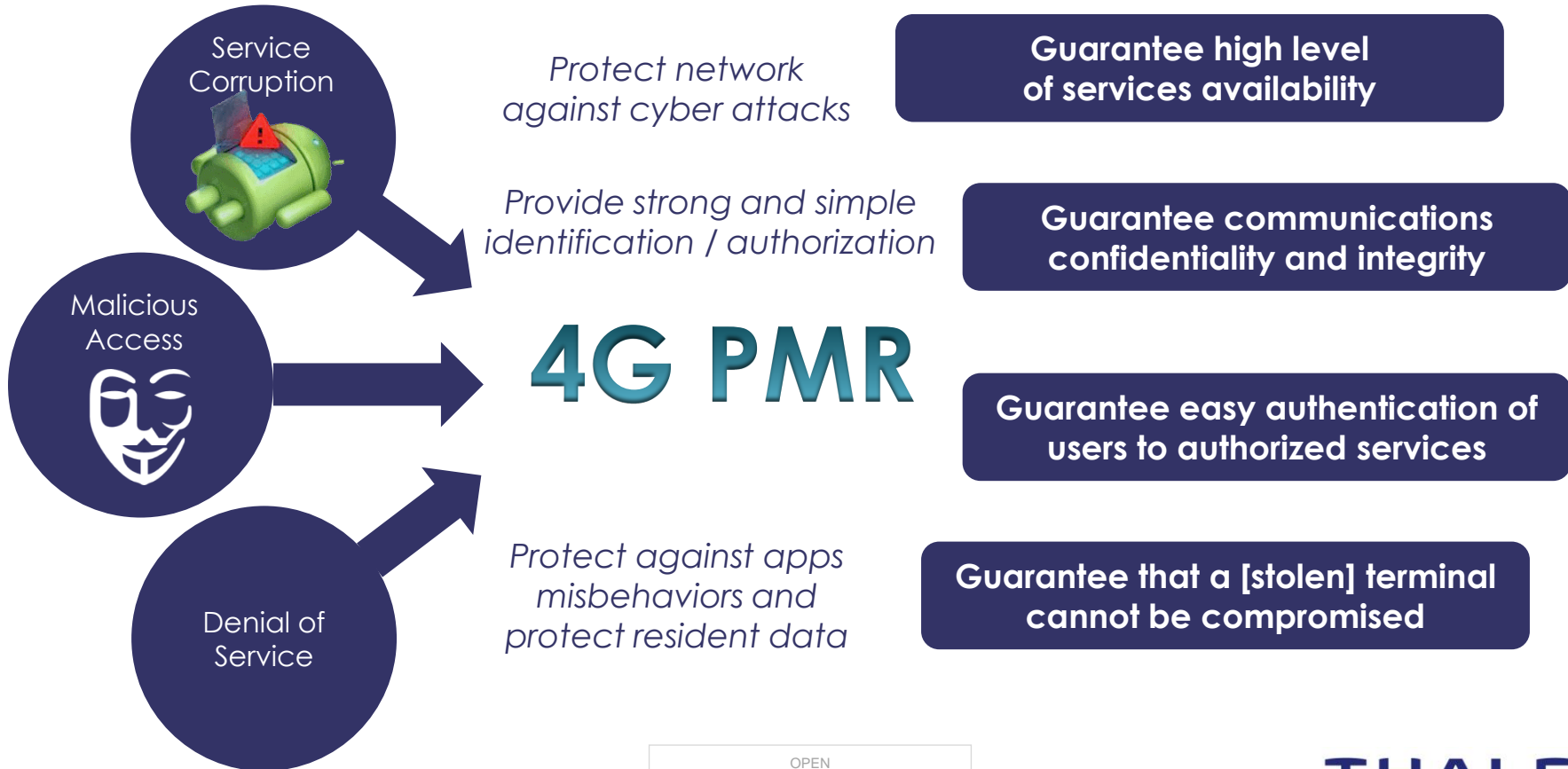
"NTT DoCoMo experienced a signaling flood caused by a VoIP application running on Android phones that disrupted network access leaving 2.5 million subscribers out of service for over four hours", January 2012

OPEN

4

THALES

Cyber threats for 4G PMR: a reality…

Service Corruption

Malicious Access

Denial of Service

Protect network against cyber attacks

Provide strong and simple identification / authorization

4G PMR

Protect against apps misbehaviors and protect resident data

Guarantee high level of services availability

Guarantee communications confidentiality and integrity

Guarantee easy authentication of users to authorized services

Guarantee that a [stolen] terminal cannot be compromised

OPEN

THALES

What are the risks?

Service disruption

Compromised secrets

Compromised data

Eavesdropping

Missions at risk

OPEN

THALES

Terminal

LTE Network

Applications

User / Application

Confidentiality / integrity

Other apps

MCC

DDoS, (Non)-malicious access

LTE Layer

Air interface encryption
[AES 128/SNOW 3G]

Mutual authentication
[EAP – AKA]

Internet

Partner's 3G/4G

eNodeB

LTE core

WAN

OPEN

Malware / Resident data

7

THALES

Securing the 4G PMR Network – High Level Approach

Terminal

LTE Network

Applications

User / Application

2 — E... [LTE ...e]

2 — Application ... Encryption [Mikey Sakke ..., AES 256]

3 — User/Applica... thentication

VPN GW — Other apps

MCC

SBC

User/App AuC

LTE layer

Air interface encryption [AES 128/SNOW 3G]

Mutual authentication [EAP – AKA]

Internet

Partner's 3G/4G

WAN

Security by design – Tiers FW + IPS Anti-DDoS

...rdened Terminal

eNodeB

LTE core

OPEN

THALES

8
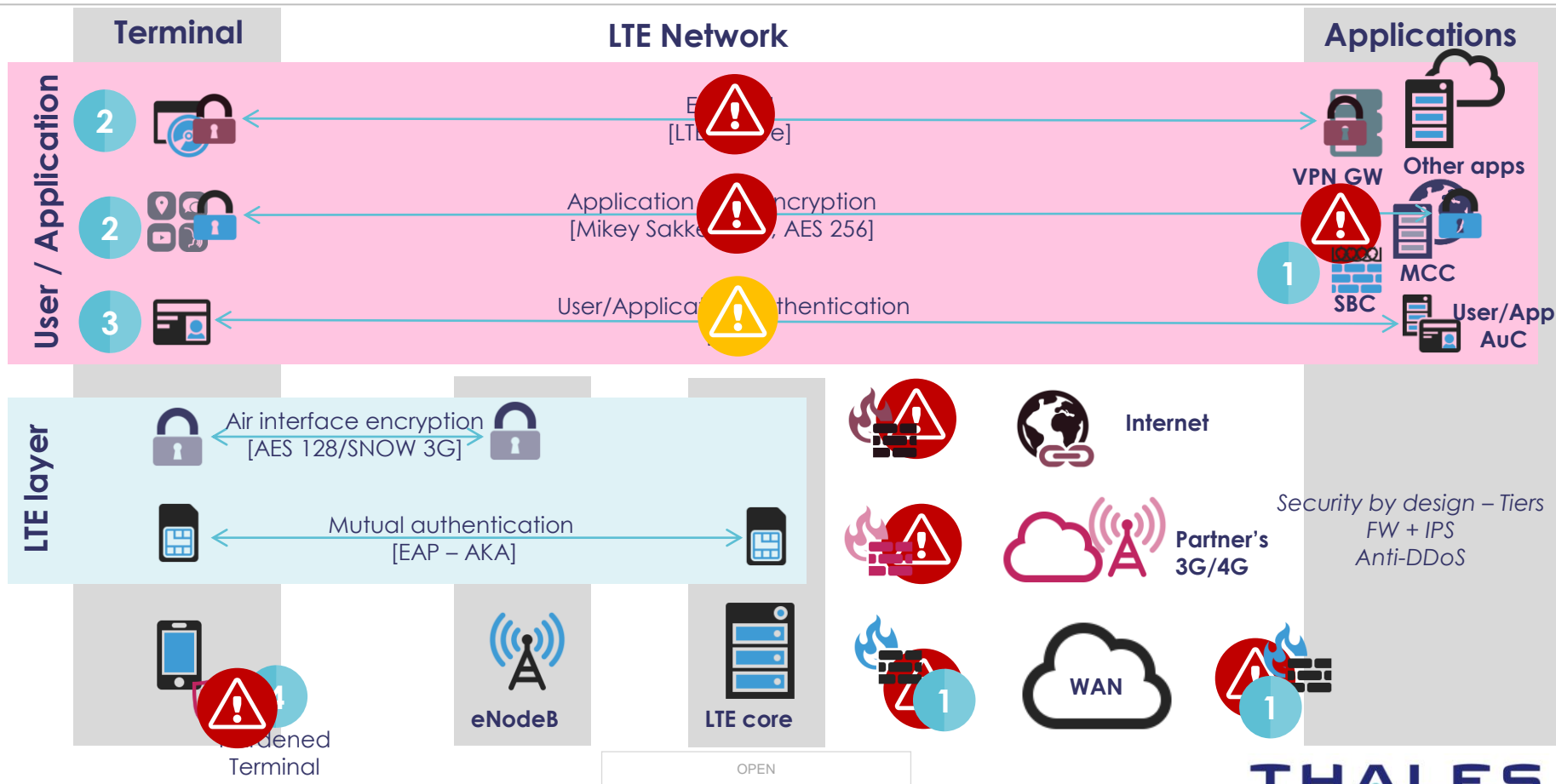
One single open door may let a system vulnerable…

- Denial-of-service
- Intrusions & Eavesdropping
- Man in the middle
- …

- Critical data loss or modification
- …

- Applications misbehaviors
- Compromised applications
- …

… and creates critical missions failure !

OPEN

THALES

4G PMR Security against permanent evolution of threats

Detect & Respond

- Detect and Analyse
- Investigate
- Manage Crisis

Anticipate

- Threat Intelligence
- Vulnerability Mngt
- Security Operations

SOC

Comply

- Sec. Policy Control
- Log Management
- Risk Management

24/7 up to date cyber-secured system

OPEN

THALES

Nexium Wireless Security – A security you can trust !

360° cyber-secured 4G PMR…

Your mission first
- Single Sign On
- QoS
- Any access, same security and same experience

Fits in your environment
- Modular
- Standard based
- Expert

360° security
- No doors left open
- Security by design
- Security services

… by the world leader in data protection

OPEN

THALES

Thank you!

OPEN

THALES