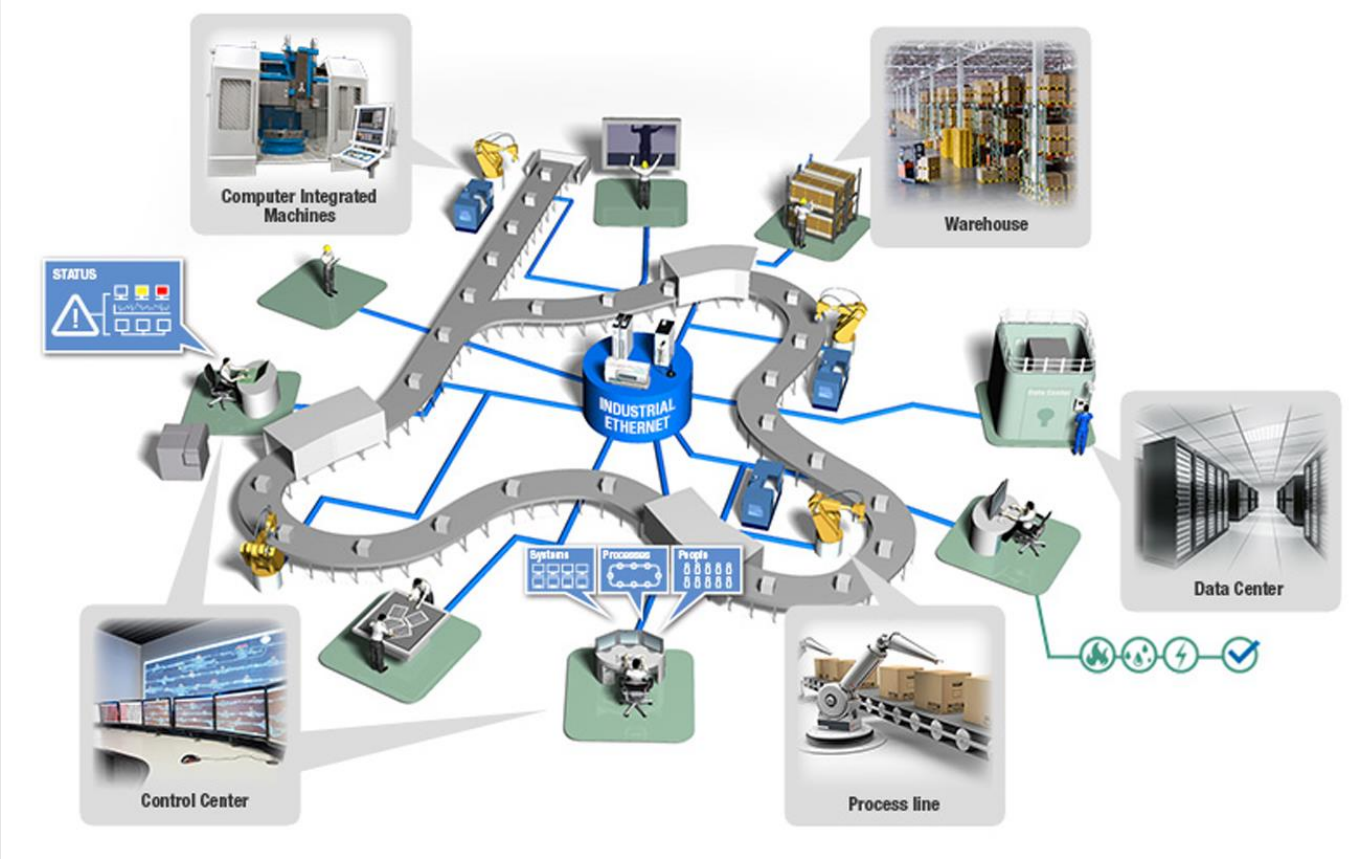
Cyber Threats to Critical Information Infrastructur

Haythem EL MIR, CISSP
CEO, keystone Group & CISRT.tn

CSIRT.TN


State Sponsored Attack
Multi-stage-Attack
Political Warfare
AI Botnets
Email Compromise
Social Engineering
Supply Chain Attack
APT Groups
ATM Fraud
IoT Malware
CIIP Attacks
Commercial Espionage
Crypto-jacking
ICO/Smart Contract Attack

Industrial Projection



This is how ICS/OT people see it

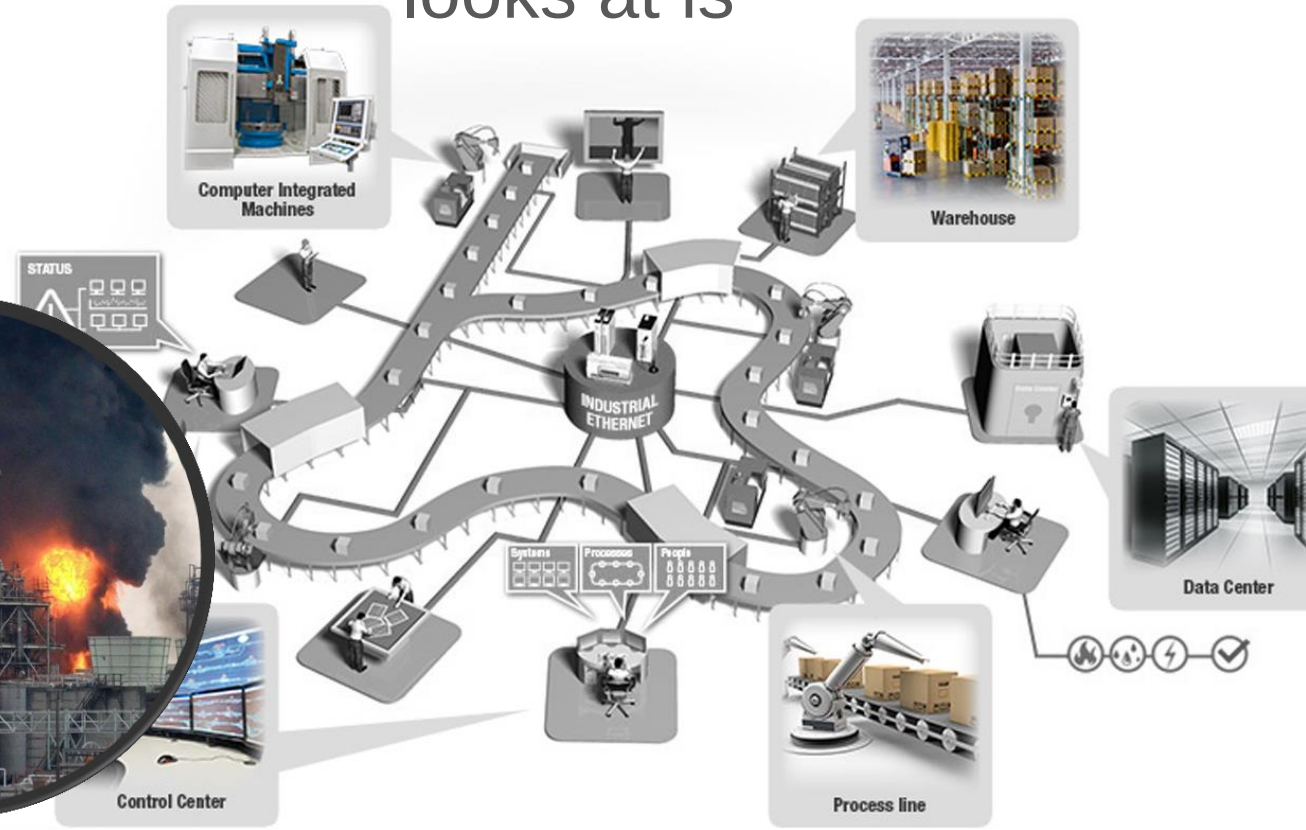
Hacker Projection

```
me@evil:~/hack/rail$ hydra -L logins.txt -P swords.txt ftp://10.0.172.238

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizat
ions, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 1970-01-01 18:11:30
[DATA] max 1024 tasks per 1 server, overall 1024 tasks, 1048576 login tries (l:1024/p:1024), ~0 t
ries per task
[DATA] attacking service ftp on port 21
```

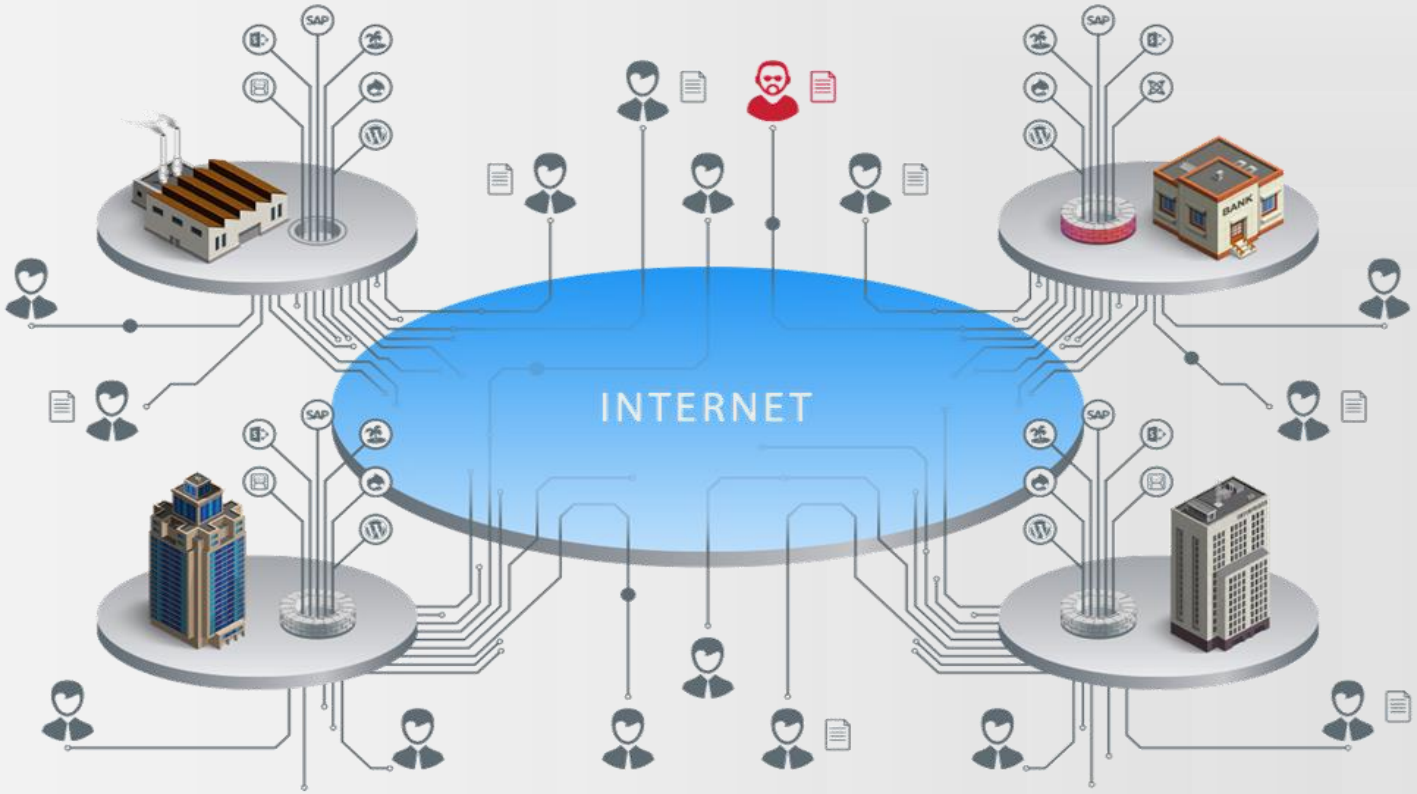
This is how Hacker looks at is



OT - real-life convergence

Critical infrastructure is a part of society.

And now, it is fully convergence



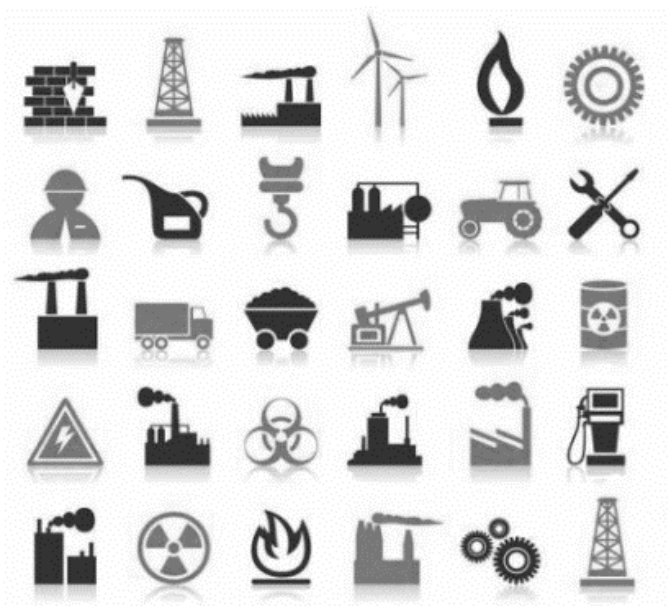
Modern OT:

- ICS/SCADA
- Telecom
- Transportation
- IoT

Business process is not limited by ICS/SCADA. Around you can see lot of accompanying technology which help to operate business process and brings new threats!

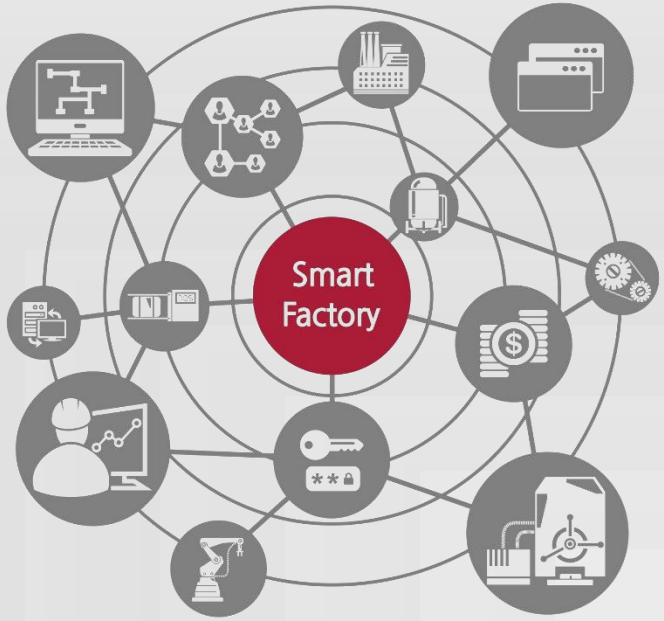
Taking the Challenge

BEFORE
Threat Model for separate ICS



→ **Challenging**

NOW
Threat Model for ALL industries!



→ **Is it possible?**

Security Threats landscape

Today’s reality on Critical Infrastructures & Enterprises

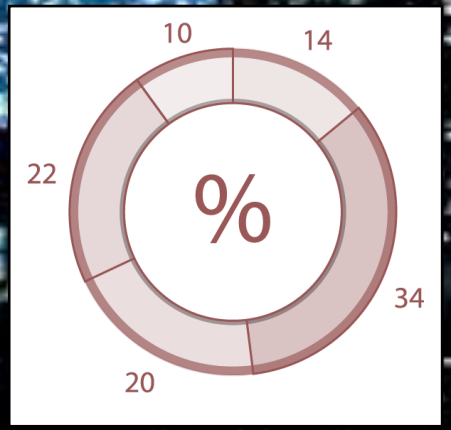
Industrial and Energy sector

INDUSTRIAL CONTROL SYSTEMS (ICS)

By January 2016 more than 150 000 of industrial systems were found to be accessible through the Internet. Among them, about 15 000 are **vulnerable** with a **high risk** level

Most of these components were accessible via **HTTP, Fox, Modbus, and BACnet**, and in most cases, a **dictionary password** was used for authentication.

Time to patch vulnerabilities



- 14% Fixed within 3 months
- 34% Remained unpatched more than 3 months
- 20% Reported to vendor, Patch to be released
- 22% Reported to vendor, Status unknown
- 10% Unpatched

STUXNET → 2010 → **DUQU** → 2011 → **Cutting Sword of Justice attacked Saudi Aramco** → 2012 → **Mexican Pemex suffered from targeted attack** → 2014 →

Key risks for ICS

Modes of attack

Cyber systems may be subject to unauthorized access through various means:

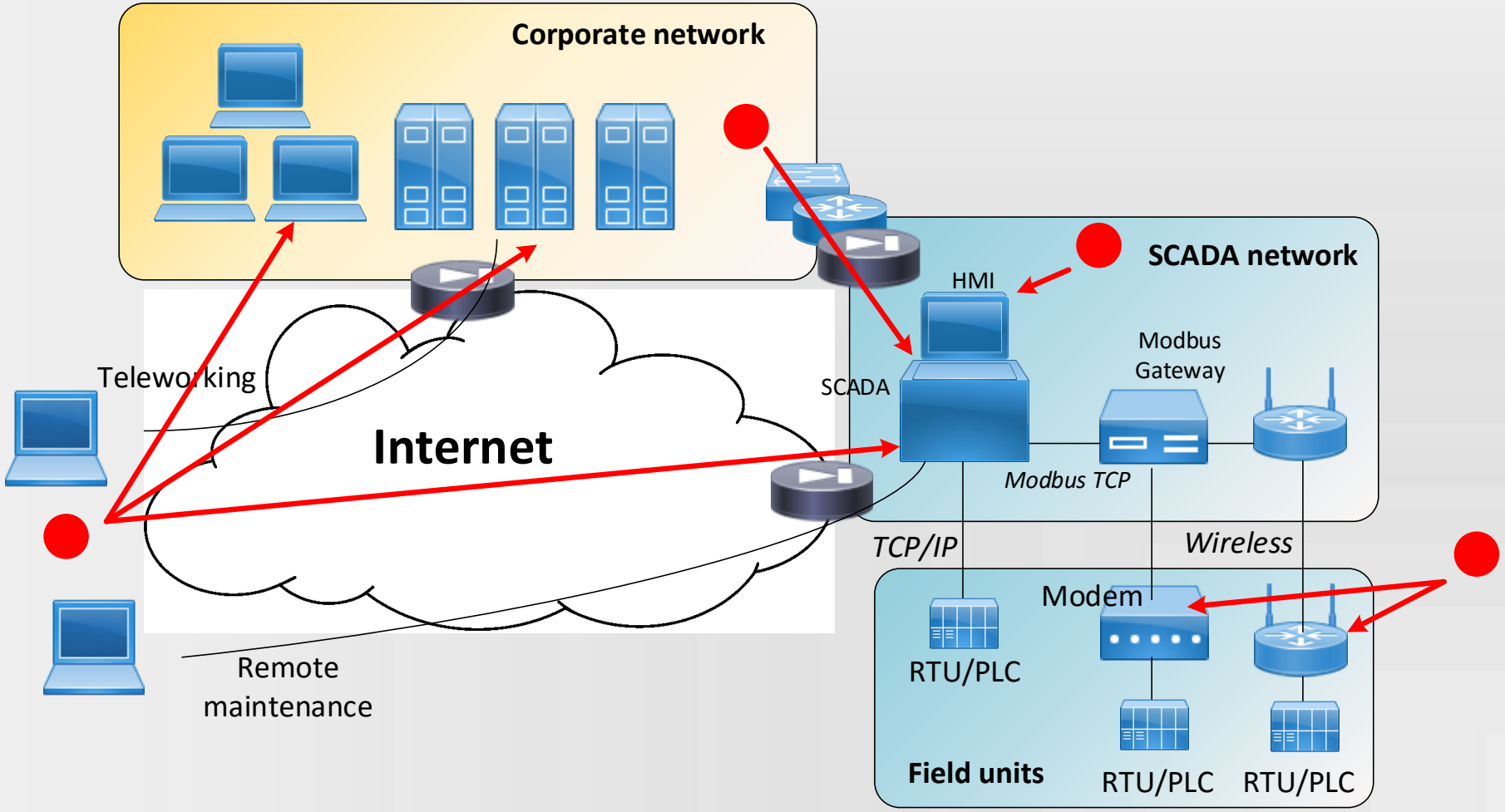
• remotely, via the Internet, or unsecured telecom networks.
• at close hand, through direct contact with infrastructure (e.g. through a USB port).
• locally, through unauthorized access to physical infrastructure, or insider threat (infiltration).

The Impacts and consequences

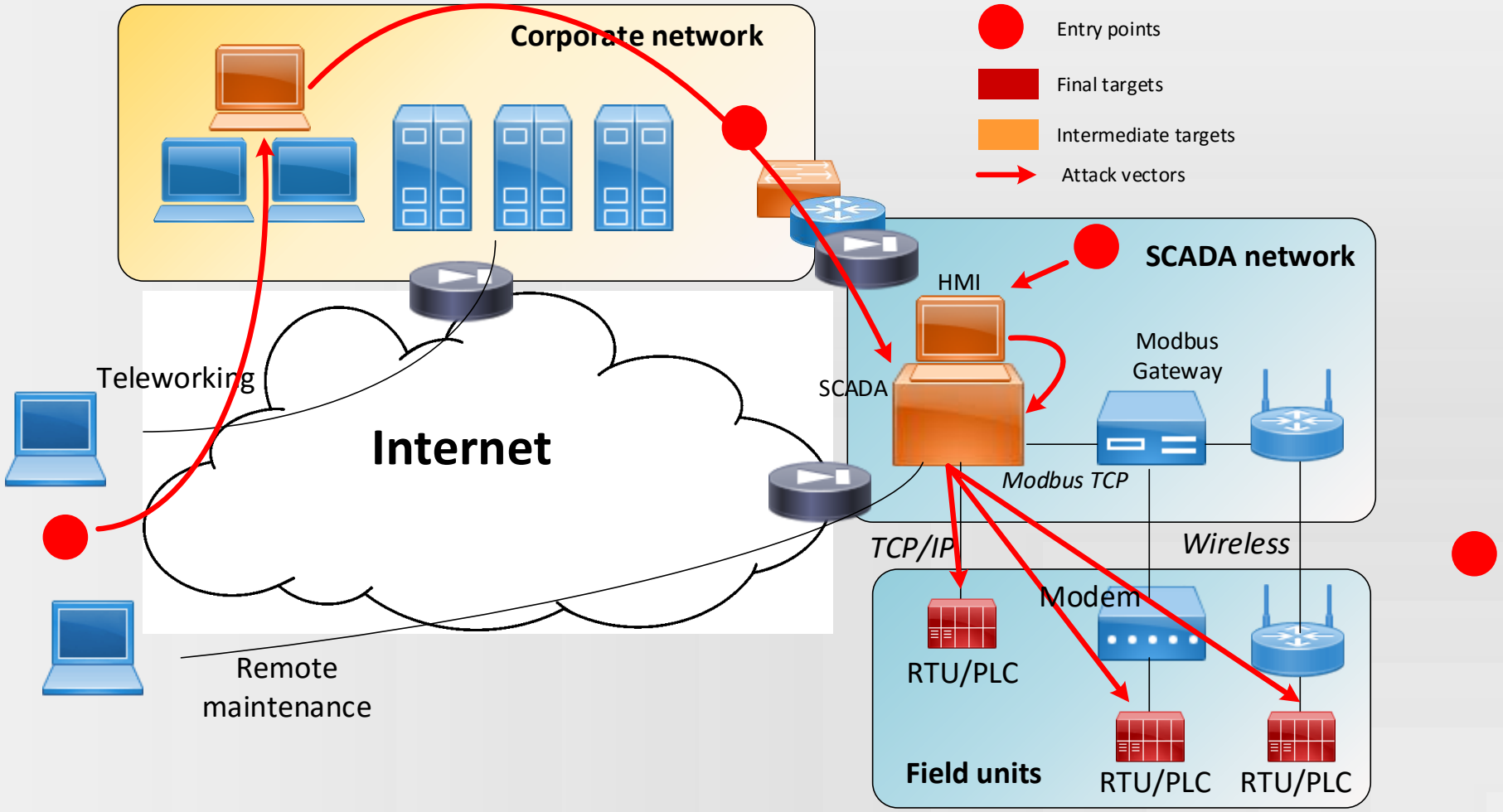
Successful cyber attacks could result in:

- Utilities interruption
- Plant sabotage / shutdown
- Production disruption
- Threats to safety
- Economic loss
- Reputational damage
- Loss of real-time monitoring and control
- Potential to cause death and injury

Network access

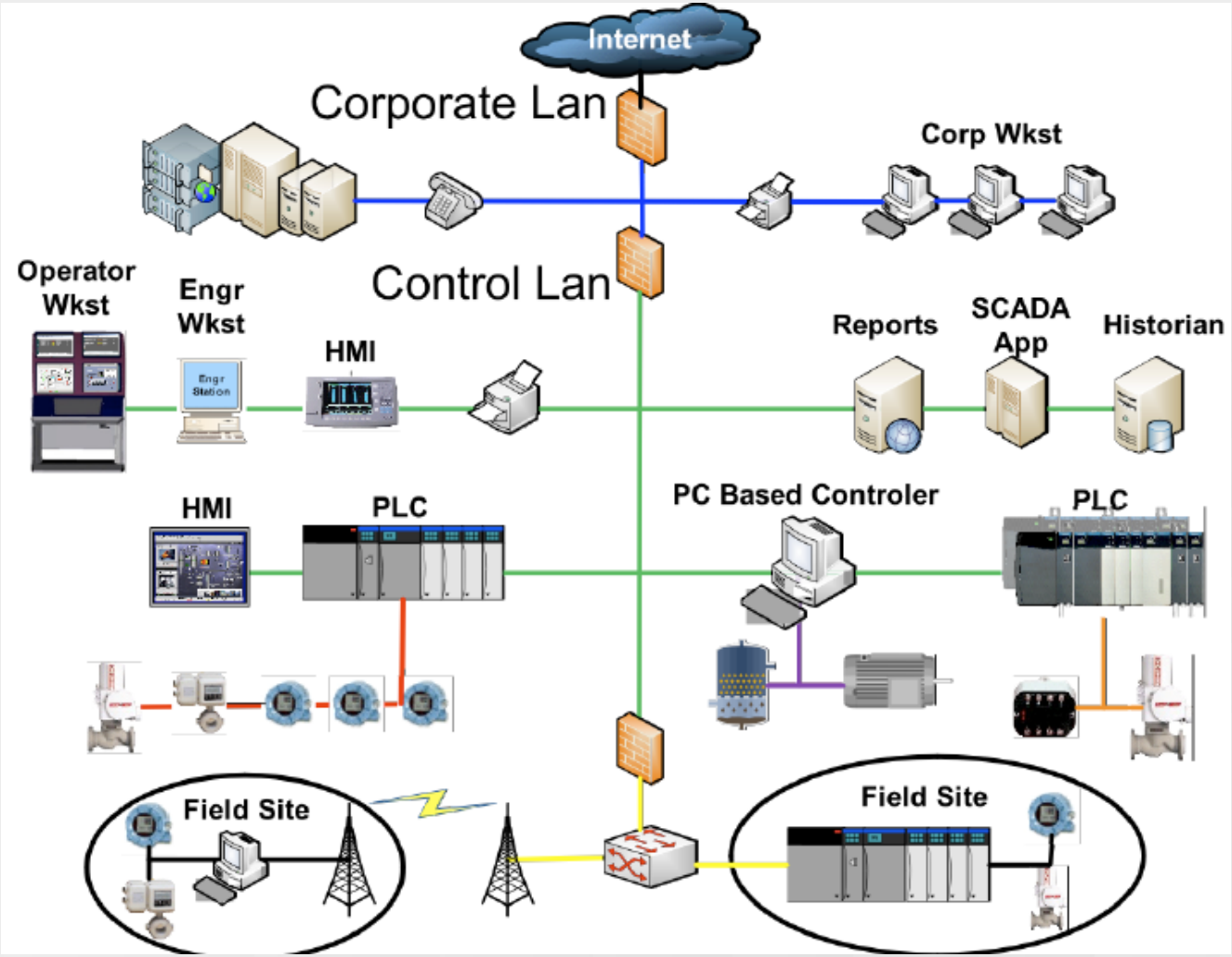


Attack vectors



Typical network

TCP/IP



Modbus, DNP3, OPC, S7, EtherCAT, FL-net, etc.

Exposed and vulnerable

- 100% of tested SCADA networks are exposed to Internet/Corporate network
  - Network equipment/firewalls misconfiguration
  - MES/OPC/ERP integration gateways
  - HMI external devices (Phones/Modems/USB Flash) abuse
  - VPN/Dialup remote access

- 90% of tested SCADA can be hacked with Metasploit
  - Standard platforms (Windows, Linux, QNX, BusyBox, Solaris…)
  - Standard protocols (RCP, CIFS/SMB, Telnet, HTTP…)
  - Standard bugs (patch management, passwords, firewalling, application vulnerabilities)

Train hacking

'Absolutely easy': Global train systems are vulnerable to hacking, warn security researchers

Published time: 31 Dec, 2015 04:12 Get short URL

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | CISO For

Trains Vulnerable to Hacker Attacks: Researchers

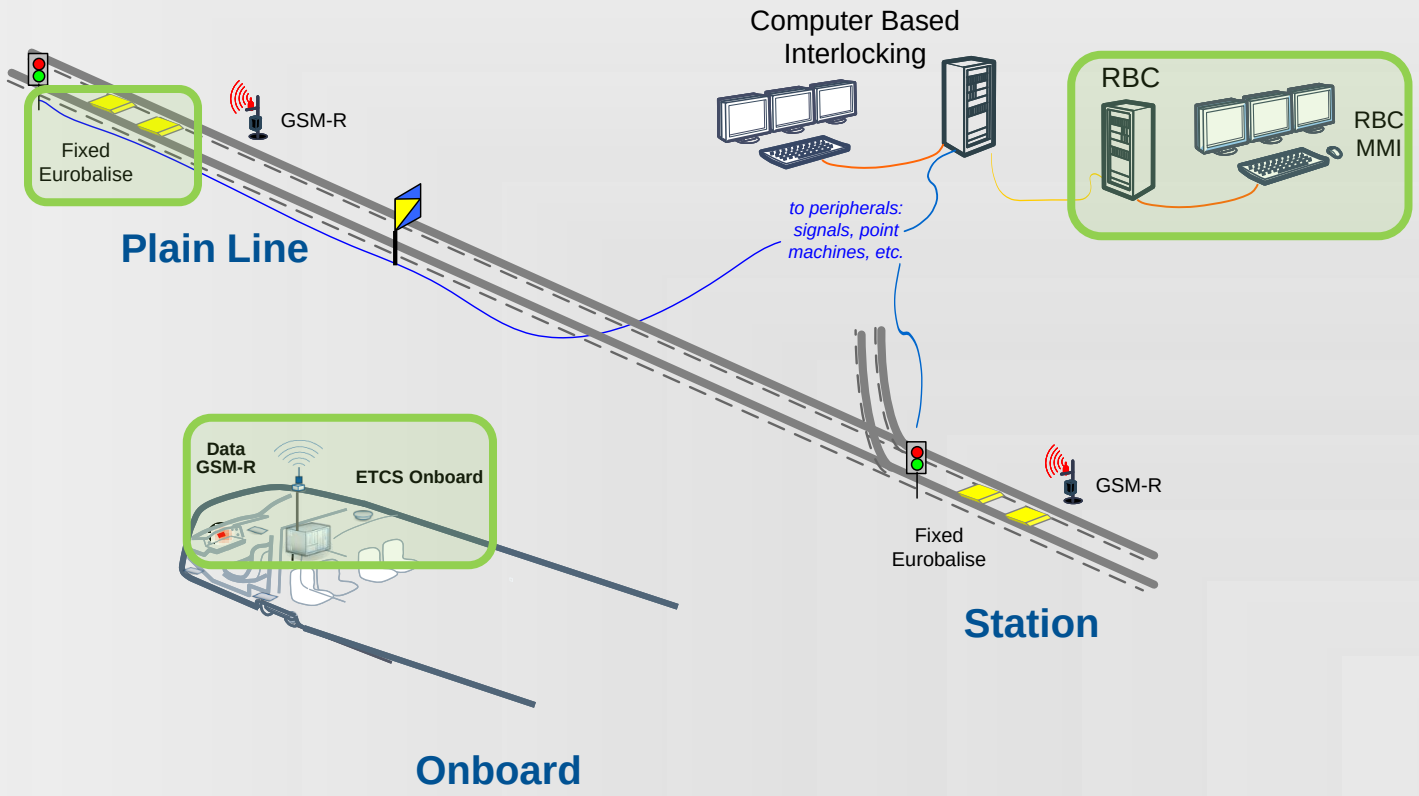
A team of researchers has analyzed modern railway systems and they've determined it would not be difficult for a motivated attacker to pull off a cyber "train robbery."

Sergey Gordeychik, Alexander Timorin and Gleb Gritsai of SCADA StrangeLove, a research group focusing on the security of ICS/SCADA systems, **disclosed their findings** on Sunday the 32nd Chaos Communication Congress (32C3) in Germany.

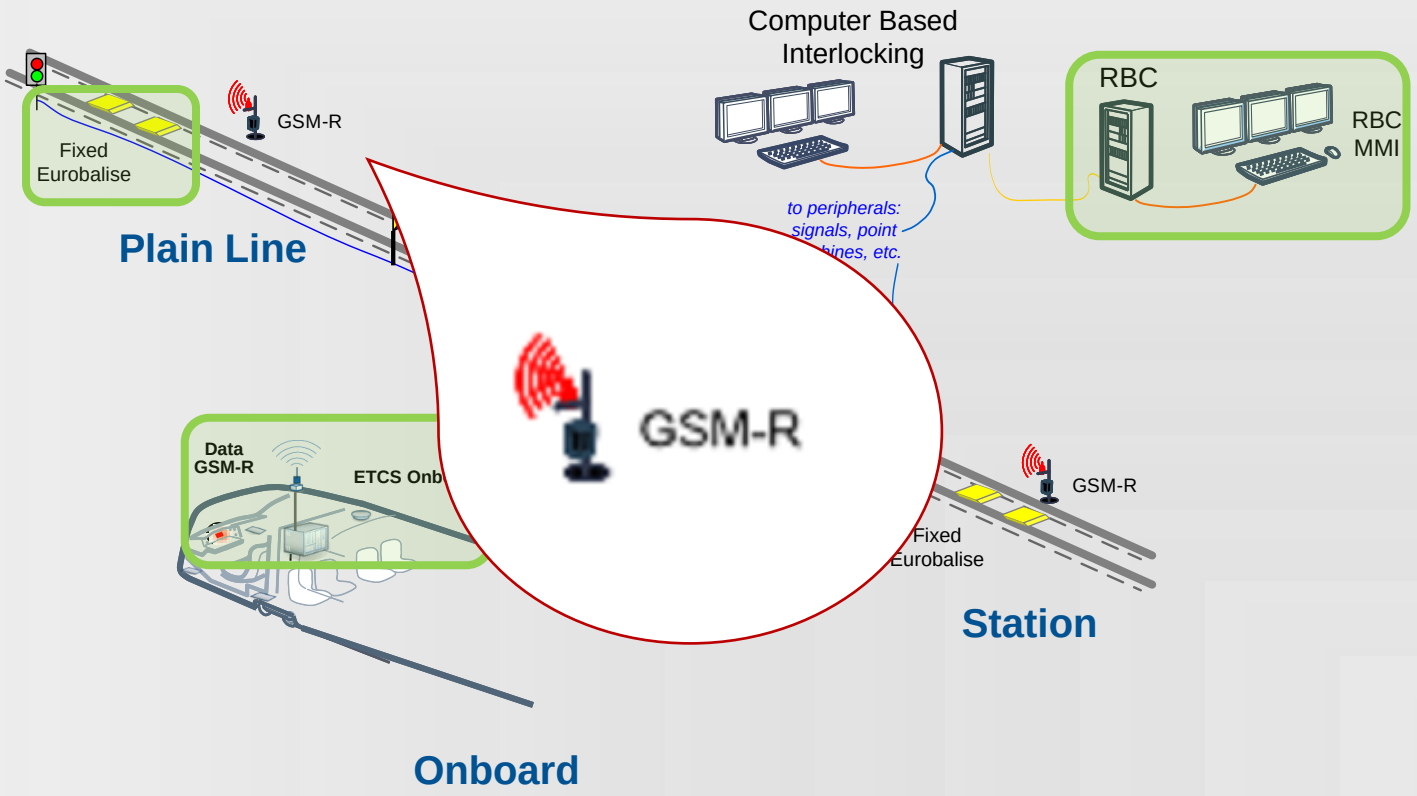
Hackers warn European trains are vulnerable to derailment and hijack attacks

By James Billington
January 4, 2016 15:51 GMT

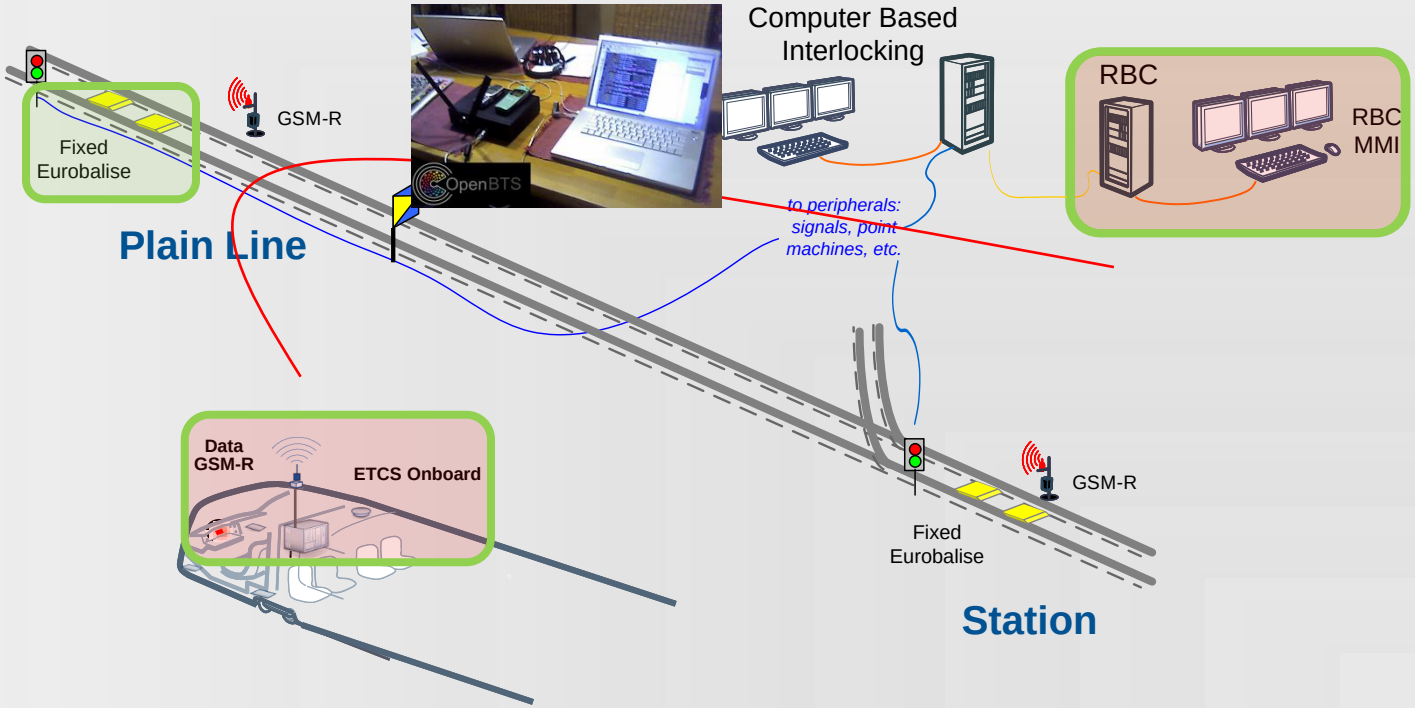
ETCS level2


Computer Based
Interlocking
RBC
RBC
MMI
GSM-R
Fixed
Eurobalise
Plain Line
to peripherals:
signals, point
machines, etc.
Data
GSM-R
ETCS Onboard
GSM-R
Fixed
Eurobalise
Station
Onboard

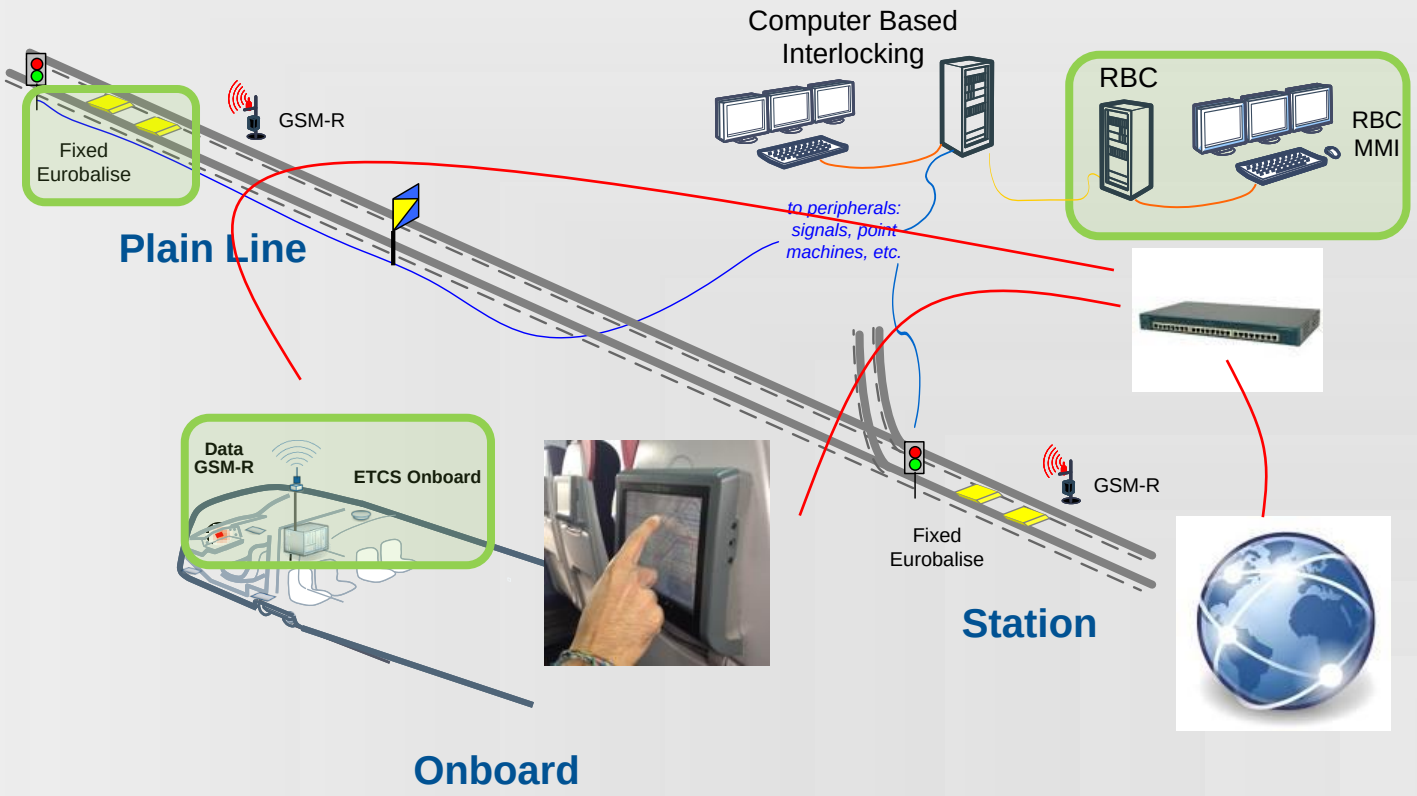
GSM-R: signaling and telemetry



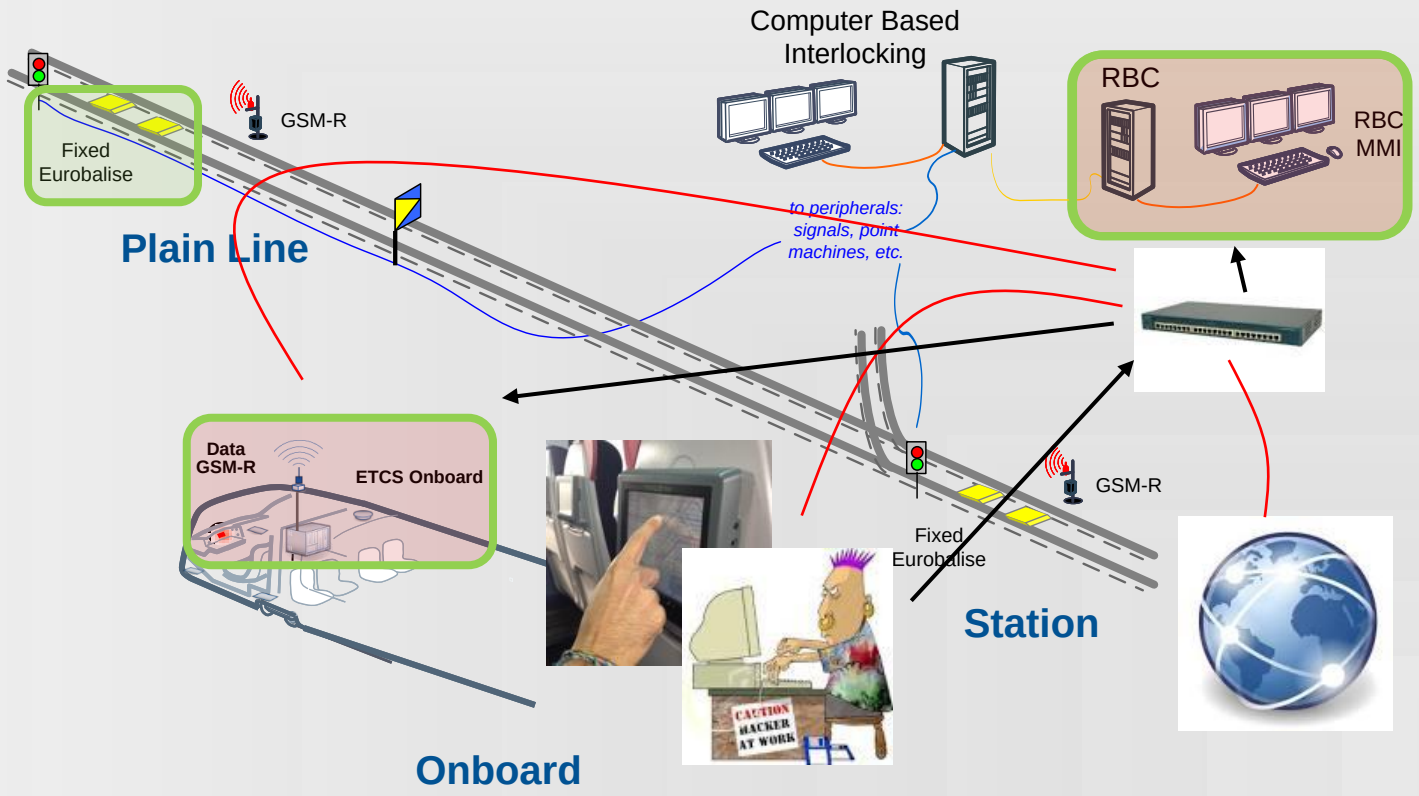
OpenBTS MitM/Jamming/Replay



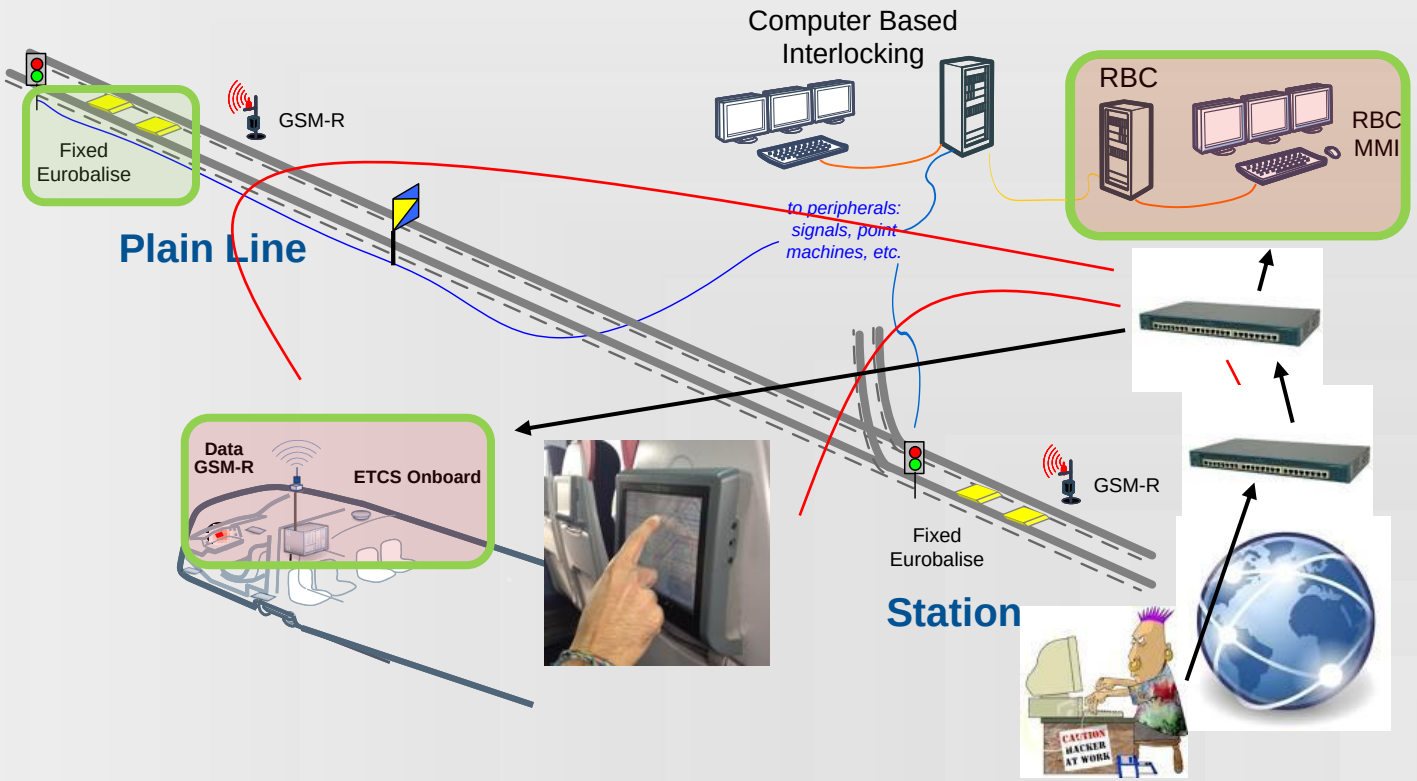
When you connect to the Internet – the Internet connects to you



Passenger attacking the infrastructure



Attacks from the Internet



More hacking on ICS to come

Electric utility hit by ransomware shuts down IT systems for a week

Lansing BWL @BWLComm — Follow

[1/4] Today we were the victim of ransomware that came in through a phishing virus and infected our corporate networks.

5:55 PM - 25 Apr 2016

The Register® — Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH | SCIE

Security

Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

24 Mar 2016 at 12:19, John Leyden — 1070

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told.

SECURITYWEEK — INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CIS

Home › SCADA / ICS

Michigan Power and Water Utility Hit by Ransomware Attack

By Kevin Townsend on May 03, 2016

Share 67 | G+1 4 | Tweet | Recommend 22 | RSS

Lansing Board of Water & Light Hit By Ransomware Att

The Board of Water and Light (BWL) in Lansing, Michigan, was struck by ransomwar Monday, April 25. Only the corporate network was affected, with no disruption to w energy supplies. The BWL has kept its customers updated through its Twitter feed, details (apparently on advice from the FBI) are yet known. Nevertheless, this would be the first disclosed example of a utility being successfully compromised by ranso

Telcos Critical Infrastructure Threats

International Business Times

Technology | Social Media

Hackers can impersonate victims and reply to WhatsApp and Telegram chats

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Rene Millman
May 13, 2016

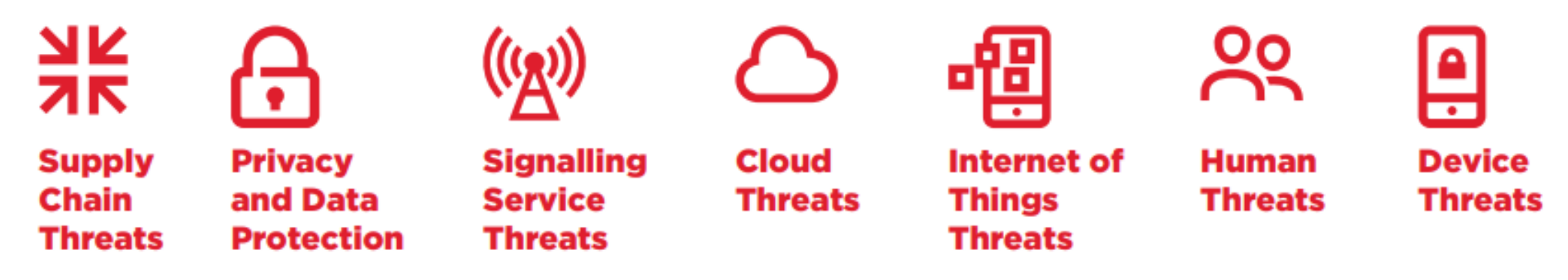
SS7 vulnerability defeats WhatsApp encryption, researchers claim

Hackers Can Steal Your Facebook Account With Just A Phone Number

theguardian

SS7 hack explained: what can you do about it?

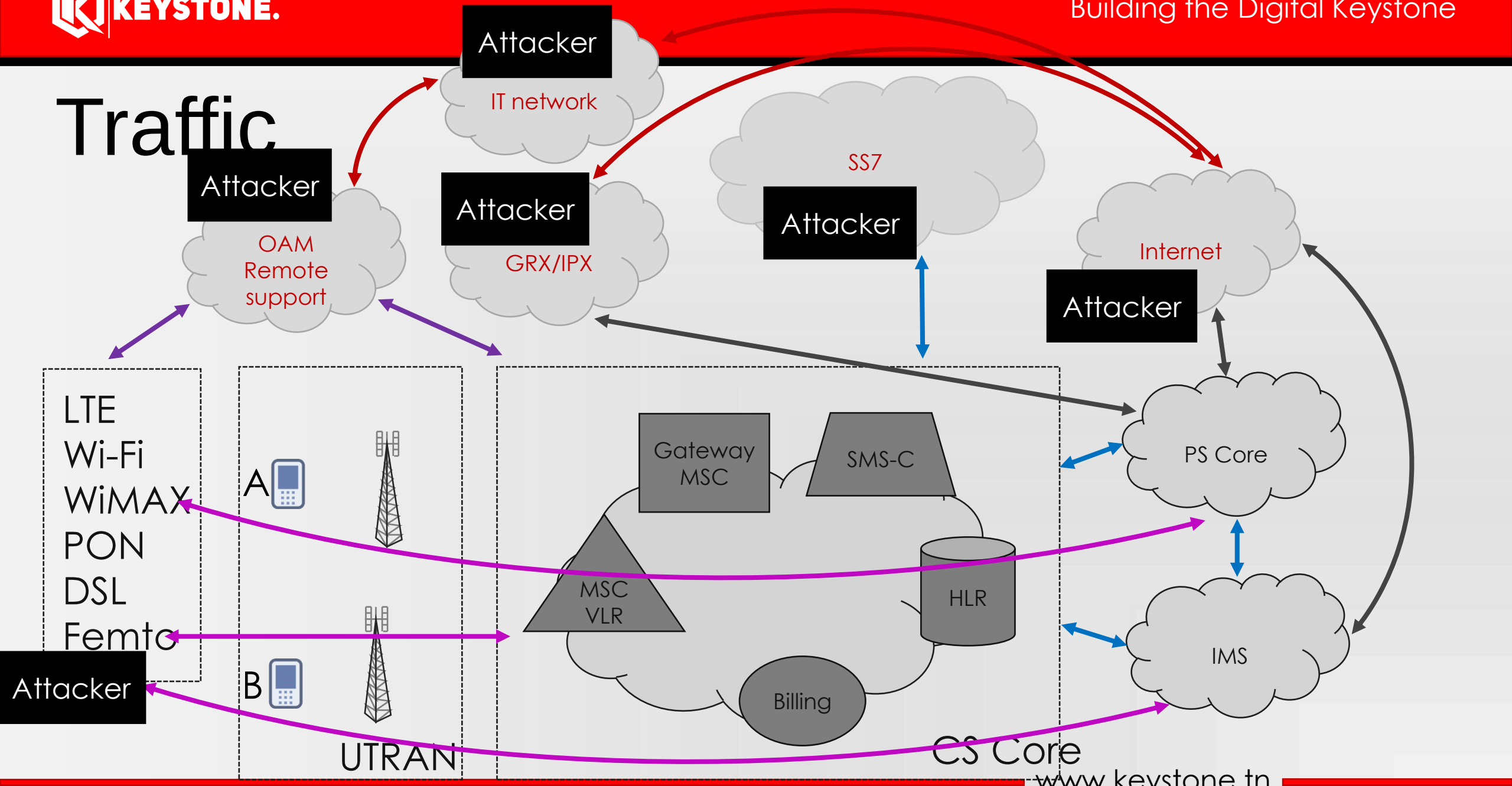
Main threats of 2018



Predicted threats of 2019 and beyond

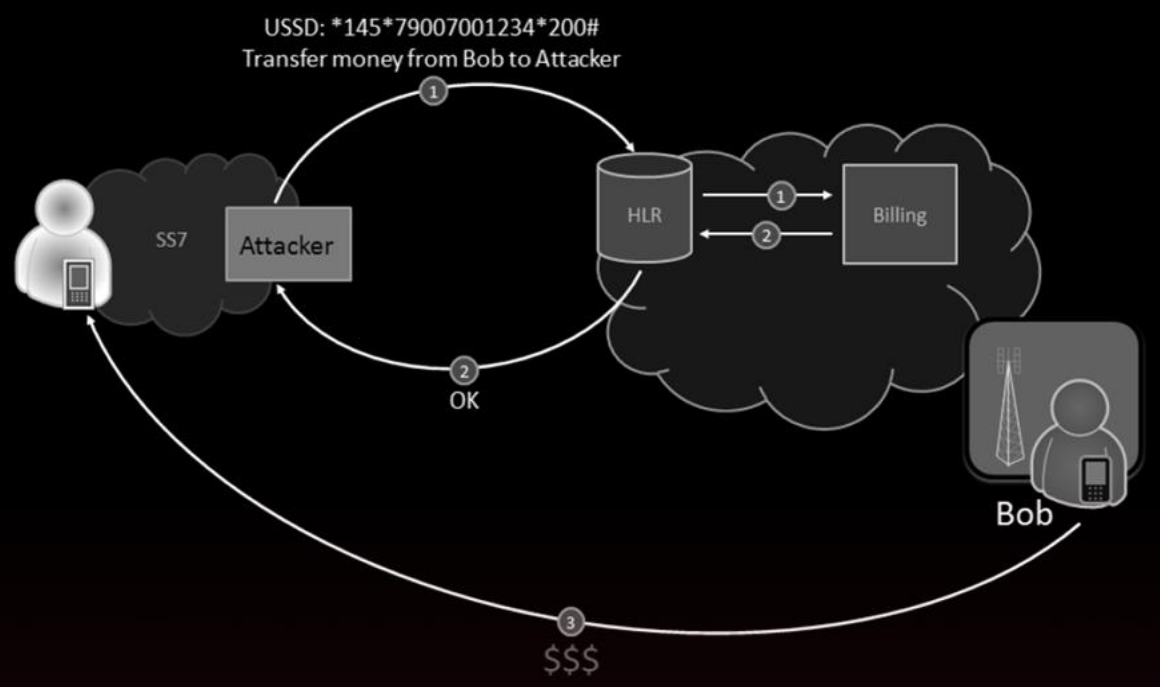
- AI used against the industry
- IoT attacks on the rise
- Uneducated overreliance on cloud
- 5G threats
- Quantum and the Public Key Infrastructure (PKI)

Traffic


Attacker
IT network
Attacker
OAM
Remote
support
Attacker
GRX/IPX
SS7
Attacker
Internet
Attacker
LTE
Wi-Fi
WiMAX
PON
DSL
Femto
Attacker
A
B
UTRAN
Gateway
MSC
SMS-C
MSC
VLR
HLR
Billing
CS Core
PS Core
IMS

MOBILE NETWORKS

Attacks on SS7



Attacker capacities:

Detect the subscriber location, violate accessibility, eavesdrop communications, intercept sms, withdraw balance account. Even TOP Telecom companies are not secure.

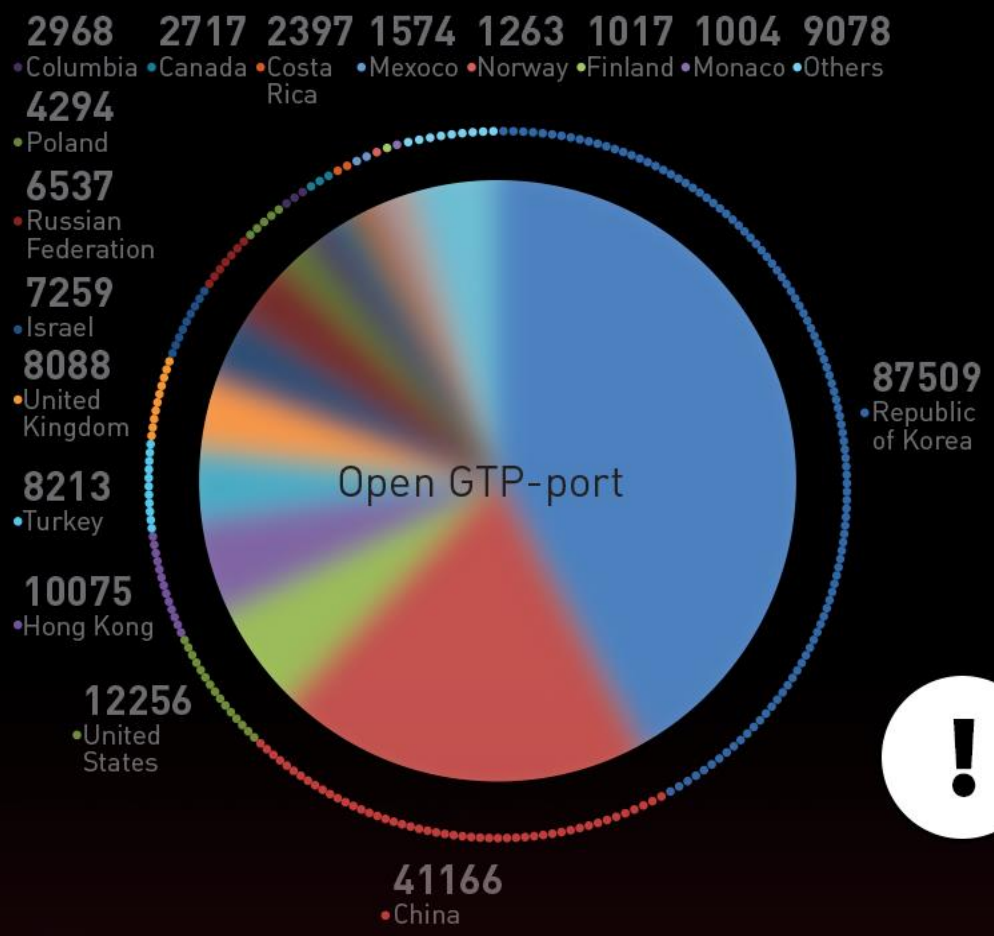
Attacker instruments:

Regular Linux PC with freeware installed or external service (SkyLock)

Incidents:

Politicians and military officers' communications interception.

MOBILE INTERNET



Hundreds of thousands devices, connected to 2G/3G networks, are accessible via Internet, because of the open GTP ports and other protocols of data transmission(FTP, Telnet, HTTP). Exploiting these vulnerabilities, malefactor can connect to the operator's node, and then via GRX attack the subscriber of any other operator.

Attacker capacities:
GPRS traffic interception, spoofing and fishing, access blocking to the Internet, location detection

At threat:
ATM machines, payment kiosks, remote control transport systems, remote monitoring systems, etc.

Financial Sector

FINANCIAL SERVICES

In 2014, 95% of all ATM machines are operated by Windows XP (vulnerabilities of which are not patched). Any malicious software and firmware can be installed.

High-risk vulnerabilities are discovered in 78% of remote banking service systems, including 70% of mobile banking applications for Android and 50% for iOS.

!

As a result, it is possible to steal confidential data (89% of systems), money from account (46% of systems), and cause denial of service (52% of systems).

Attack vectors

Unpatched vulnerabilities

Misconfiguration

Lack of encryption

End-of-life systems

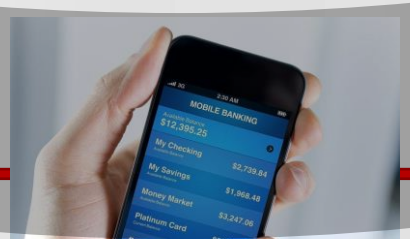
CBS

Lack of assessment

GRH

Weak filtering

Web Portal



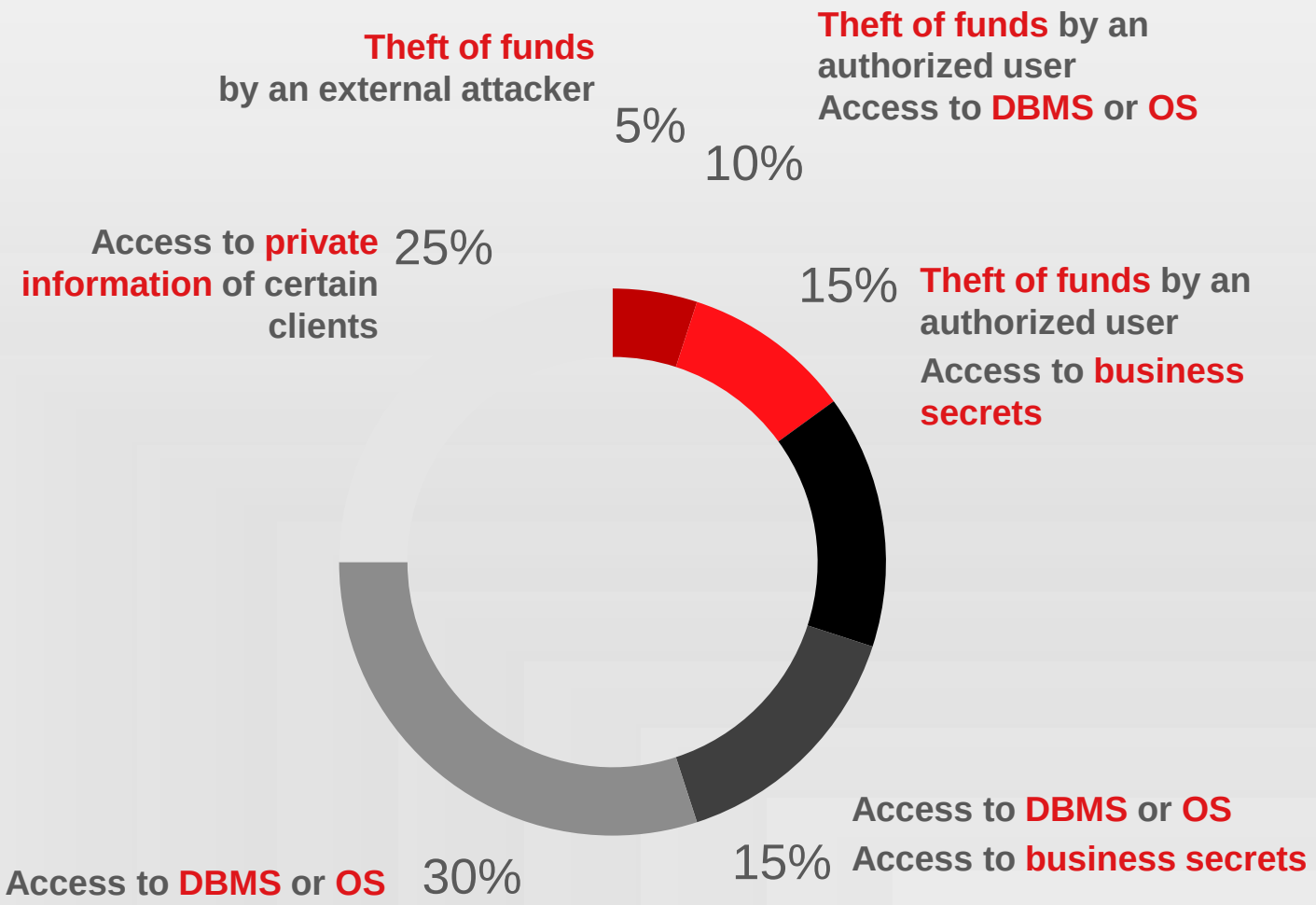
Weak authentication and access control

Employee errors

Lack of awareness

OLB: Critical Threats

- **Theft of funds**
- Access to **payment card data**
- Access to users' **personal data**
- OLB **denial of service**
- Compromise of **business secrets** and/or **client privacy**



OLB information security threats

SWIFT attack case (2016)

US$81 million

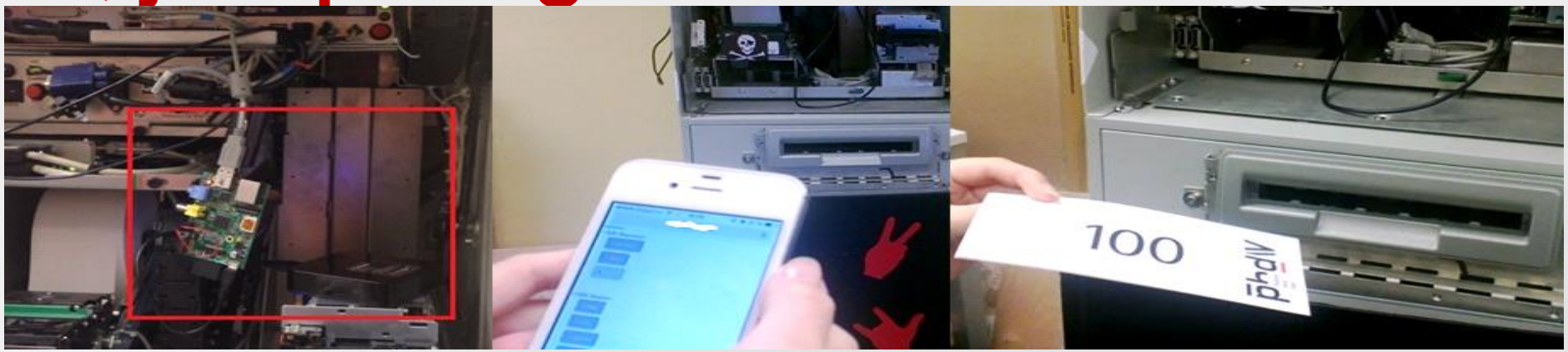
Lazarus group could have made off with $1 billion

APT: Carbanack case

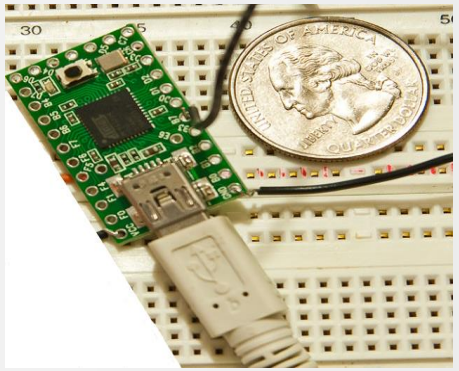
- Spear phishing → Old vulnerabilities exploitation,
- Remote command execution (screenshot capture while accessing sensitive web application, cookies theft, etc.)
- Install a RAT (Ammyy Admin) for lateral attacks to access the banking accounts processing systems,
- On the target, the attacker record the screen activities to get familiar with procedures and banking workflow via the stolen data.
- These information is used to steal money via SWIFT network.

A billion-dollar APT

Blackbox, jackpotting



“Black box attack”: unauthorized cash withdrawal is possible with a cheap and popular computer. The credit-card sized and fast programmable device can be easily hidden inside an ATM. Sometimes it can be plugged even outside an ATM.



USB-based microcontroller – the most HIDden jackpotting device

Other critical sectors

Gouvernement

Healthcare

Transport

Mass Media

Merci pour votre attention

KEYSTONE.
CSIRT.TN
+216 36 322 191
contact@keystone.tn
Appartement n° b25 bloc b, résidence étoile du nord centre urbain nord-Tunis 1003