Panel on ICWMC / VEHICULAR «Challenges on Security and Trust in Mobile Environments» ICWMC 2015, 11-16 October 2015, St. Julians, Malta

Panelists

- Pascal Urien, Télécom ParisTech, France
- Markus Ullmann, BSI, Germany
- Josef Noll, University Graduate Center (UNIK), Norway

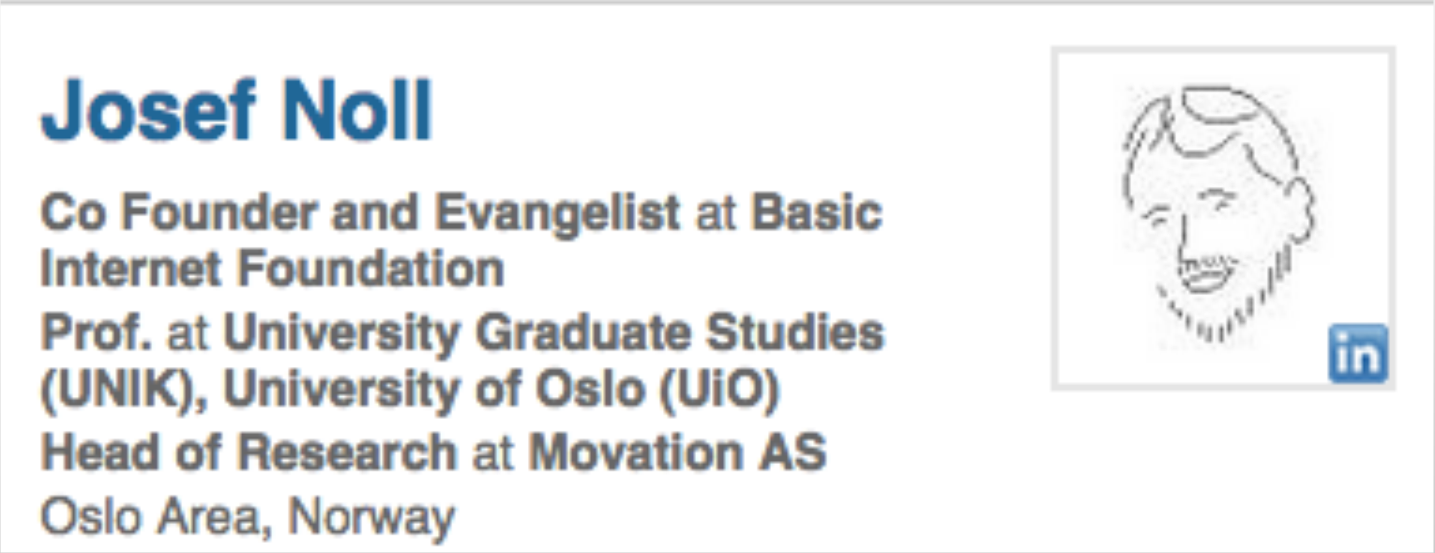
Main findings on Security and Trust

- Who is the trust entity?
  - government, «Google»
  - car manufacturer, e.g. Volvo «if you have an accident with your automated car, we pay».
  - trust is often traded for convenience: «it's convenient and easy, I'll trust»
- Believe is more important than Service Level Agreement (SLA)
  - «believe they are doing a reasonable job»
  - expectation & history driven
  - SLA is not an agreement: «accept or leave»
- Privacy
  - attack on security and privacy is a business
  - no (real) alternatives to the convenient services
- Expectations
  - governments/EU to take care of a minimum of privacy
  - identify responsibility
  - create awareness
  - awareness boosts alternatives

UNIK
UNIVERSITY GRADUATE CENTER

Panel on ICWMC / VEHICULAR «Challenges on Security and Trust in Mobile Environments» ICWMC 2015, 11-16 October 2015, St. Julians, Malta

Security and Trust measures for IoT infrastructures



Josef Noll

Co Founder and Evangelist at Basic Internet Foundation
Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)
Head of Research at Movation AS
Oslo Area, Norway

DNV report 2013, DNV GL report 2014

Technology Outlook 2020 / Transformative Technologies

- Technology applications in Maritime, Renewables & Electricity, Health Care, Oil & Gas and Food & Water industries
  - sensors will drive automated data management
  - from passive data to automated decisions
  - automated decision tools by 2020

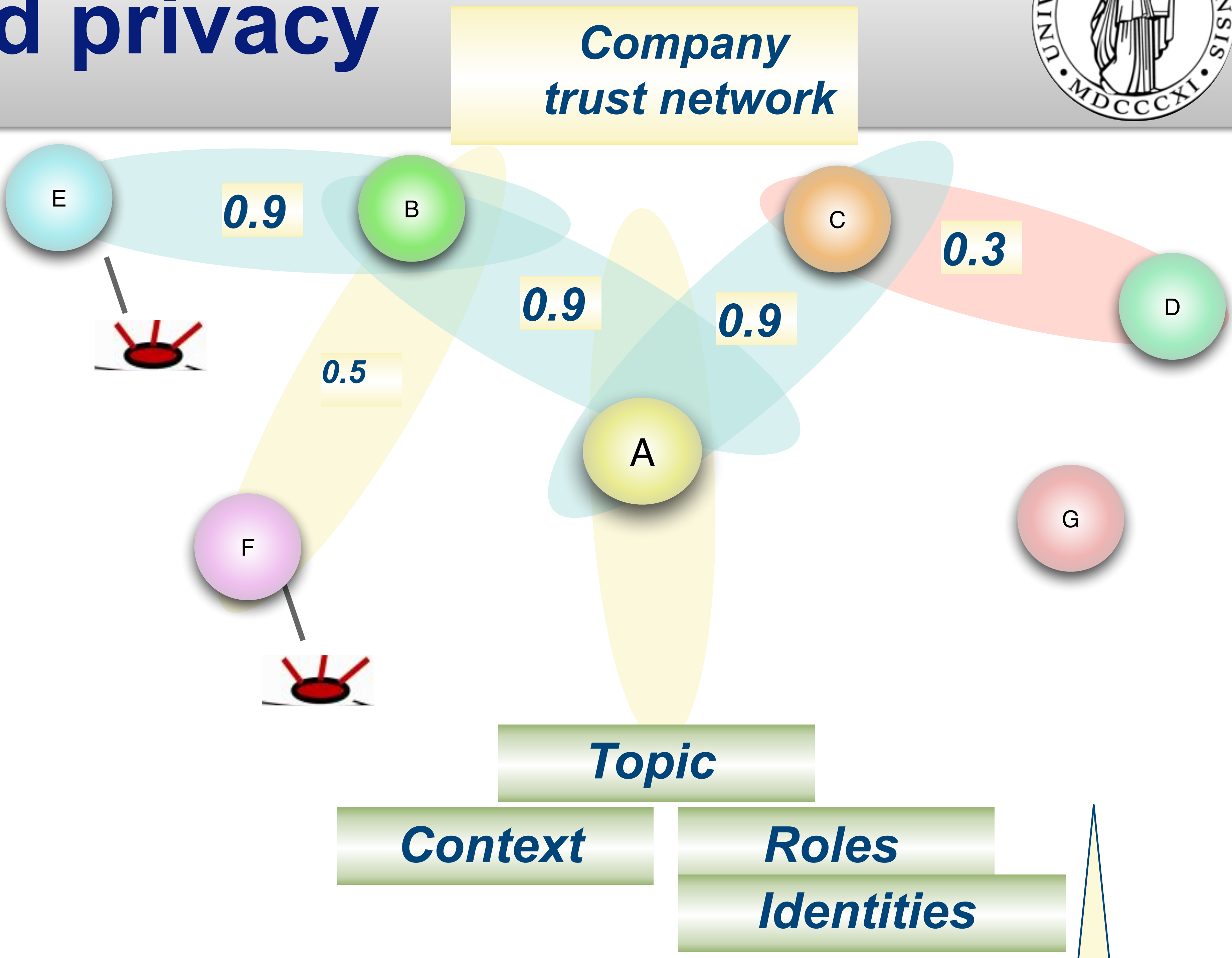
- Maritime: «policy driven»
- Health care: «trust» on sensor and mobile apps

"Only 59% of the public trust the energy industry," (Edelman Trust Barometer 2013)

"In any change management process, the challenge is communicating risk," (Peter Bjerager, DNV GL)

Trust-based privacy

- "With whom to collaborate?"
- Share data?
- Trust-based privacy
- Information and your social life

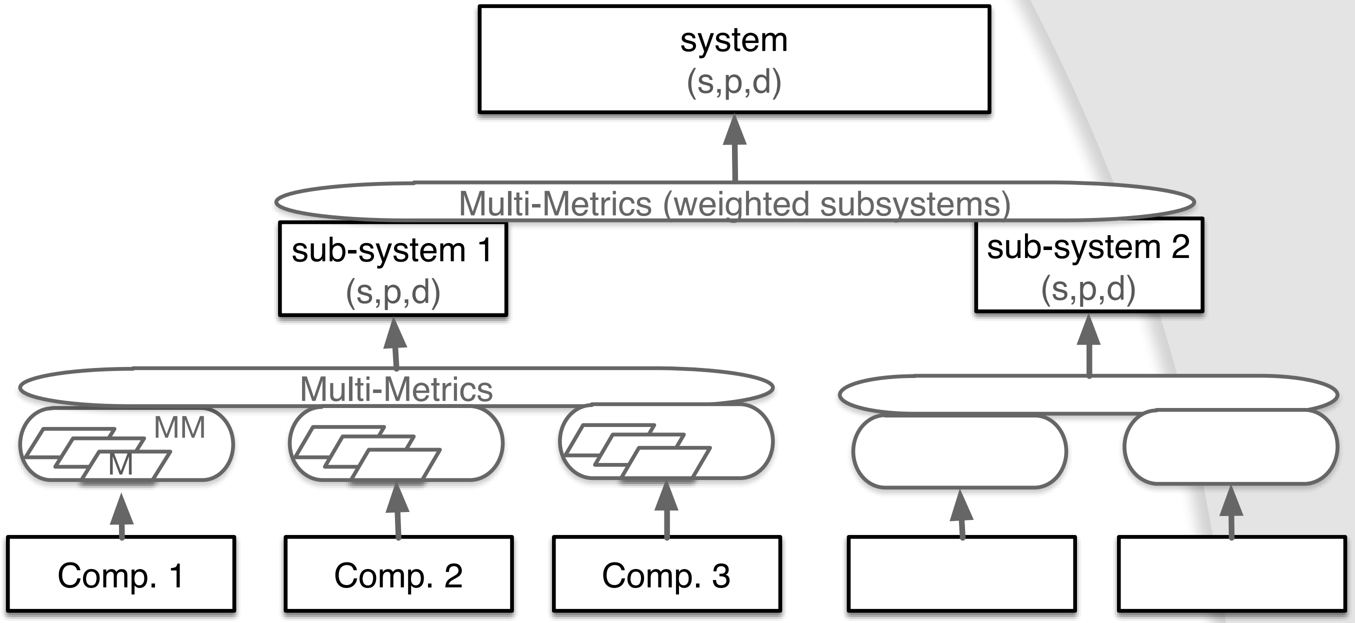


- *Measurable trust? Transient Trust?*
- *Value chains: from sensors to systems*

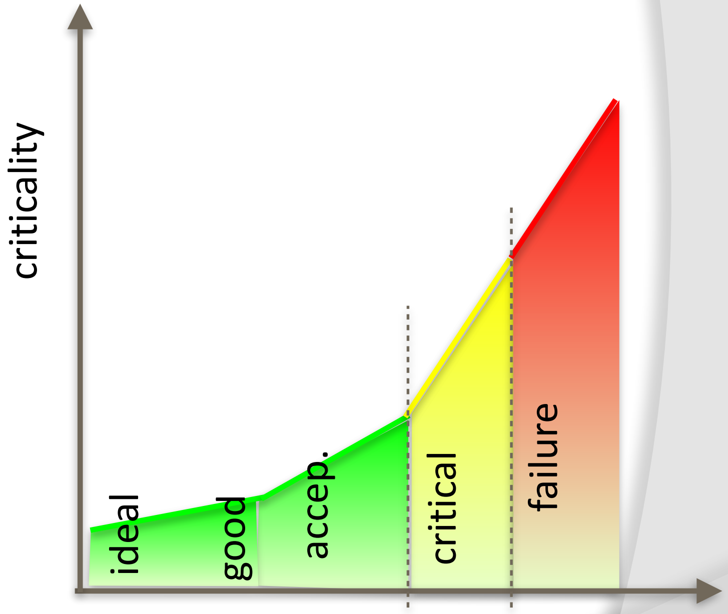
Thanks to Vladimir Oleshchuk for ideas and discussions

Measurable Security, Privacy and Dependability

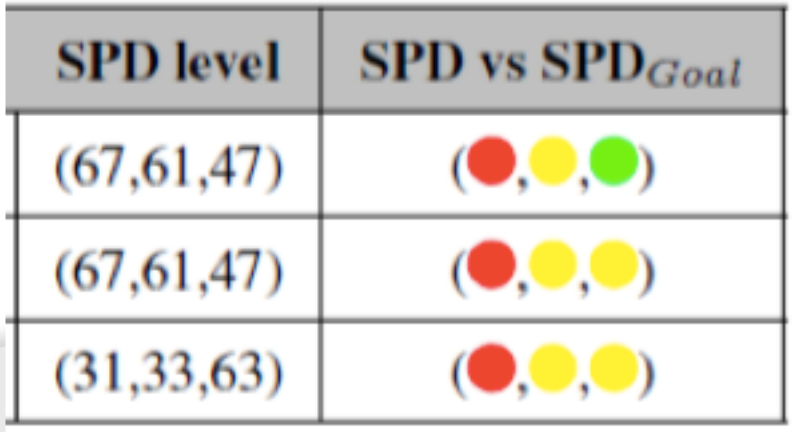
- System consists of sub-systems consists of components



- Component/Sub-system Criticality



- Multi Metrics approach
  - System security vs Application security demand



SPD level	SPD vs SPD$_{Goal}$
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)

Bonn-Rhine-Sieg University
of Applied Sciences

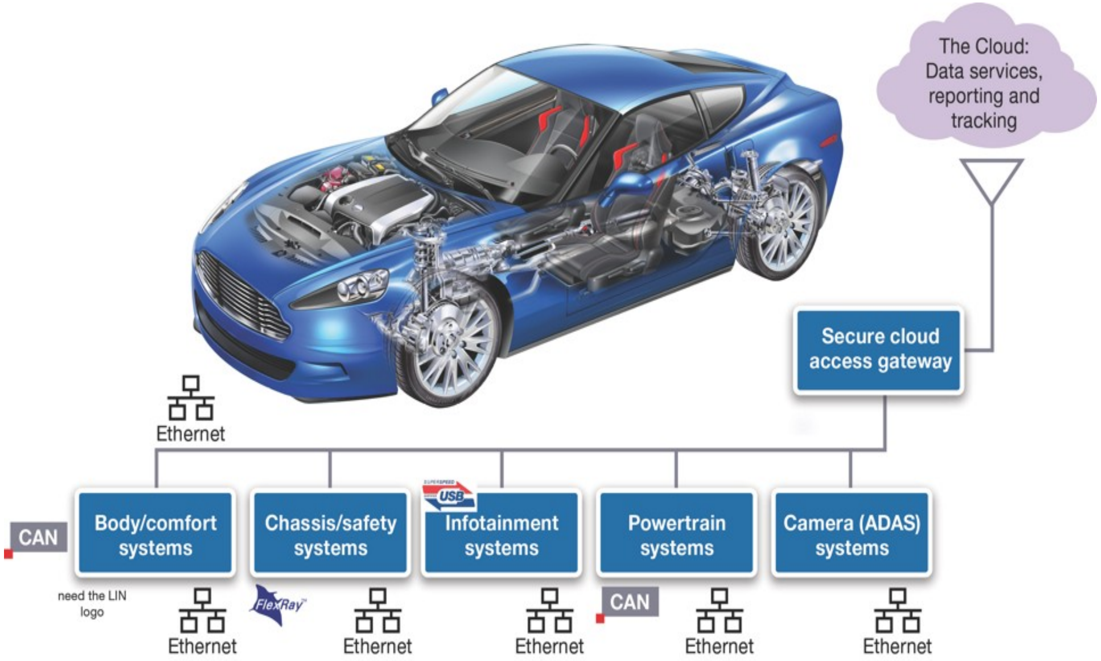
Challenges on Security and Trust in Mobile Environments

Markus Ullmann

Modern Vehicles

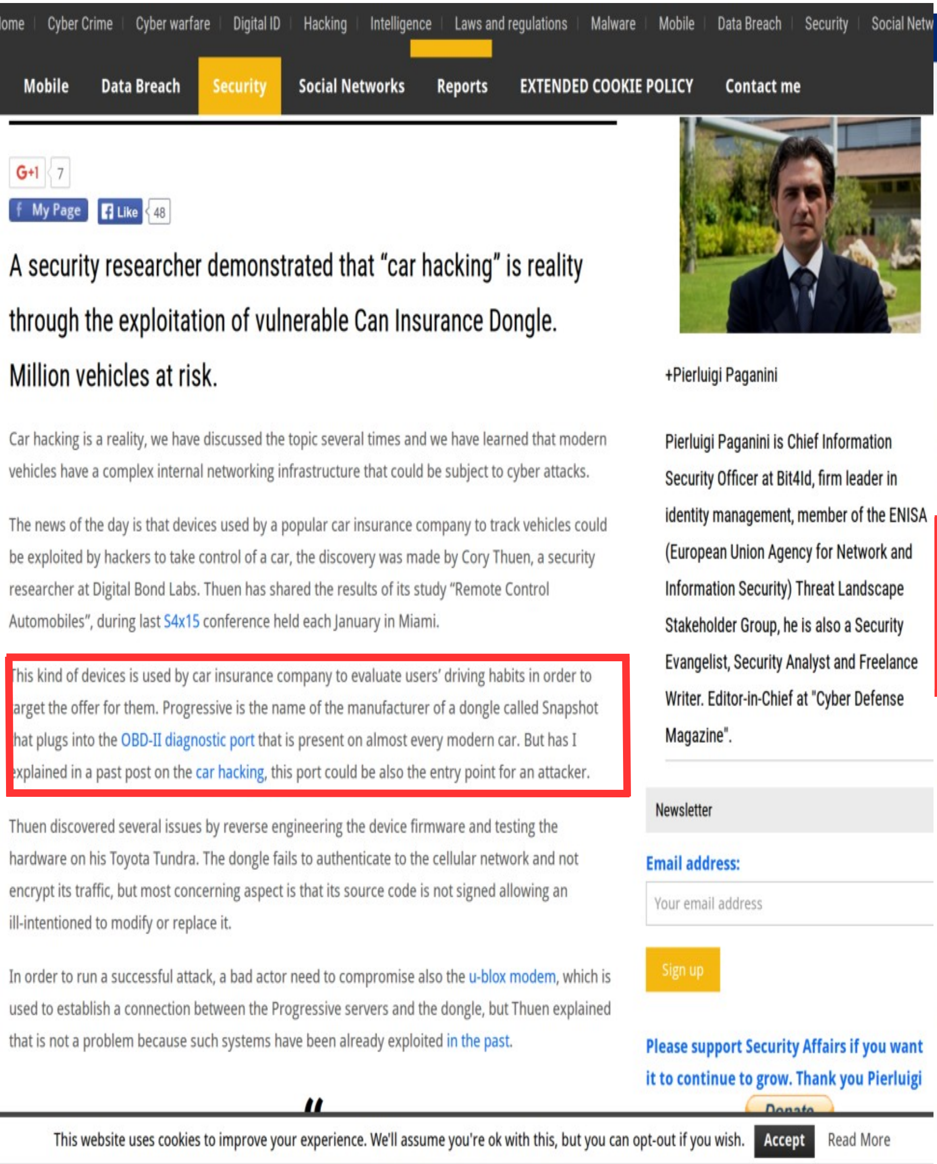
- Much more then
  - Chassis + Cabine
  - Wheels
  - Engine
  - Gearbox
  - ...

Modern Vehicle: + Network of Controllers



Future Direction: Automated Driving

Real Attacks on Vehicles (1 of 2)


ome | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | Laws and regulations | Malware | Mobile | Data Breach | Security | Social Netw
Mobile
Data Breach
Security
Social Networks
Reports
EXTENDED COOKIE POLICY
Contact me
G+1 7
My Page
Like 48

A security researcher demonstrated that "car hacking" is reality through the exploitation of vulnerable Can Insurance Dongle. Million vehicles at risk.

Car hacking is a reality, we have discussed the topic several times and we have learned that modern vehicles have a complex internal networking infrastructure that could be subject to cyber attacks.

The news of the day is that devices used by a popular car insurance company to track vehicles could be exploited by hackers to take control of a car, the discovery was made by Cory Thuen, a security researcher at Digital Bond Labs. Thuen has shared the results of its study "Remote Control Automobiles", during last S4x15 conference held each January in Miami.

his kind of devices is used by car insurance company to evaluate users' driving habits in order to arget the offer for them. Progressive is the name of the manufacturer of a dongle called Snapshot hat plugs into the OBD-II diagnostic port that is present on almost every modern car. But has I xplained in a past post on the car hacking, this port could be also the entry point for an attacker.

Thuen discovered several issues by reverse engineering the device firmware and testing the hardware on his Toyota Tundra. The dongle fails to authenticate to the cellular network and not encrypt its traffic, but most concerning aspect is that its source code is not signed allowing an ill-intentioned to modify or replace it.

In order to run a successful attack, a bad actor need to compromise also the u-blox modem, which is used to establish a connection between the Progressive servers and the dongle, but Thuen explained that is not a problem because such systems have been already exploited in the past.

+Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Newsletter

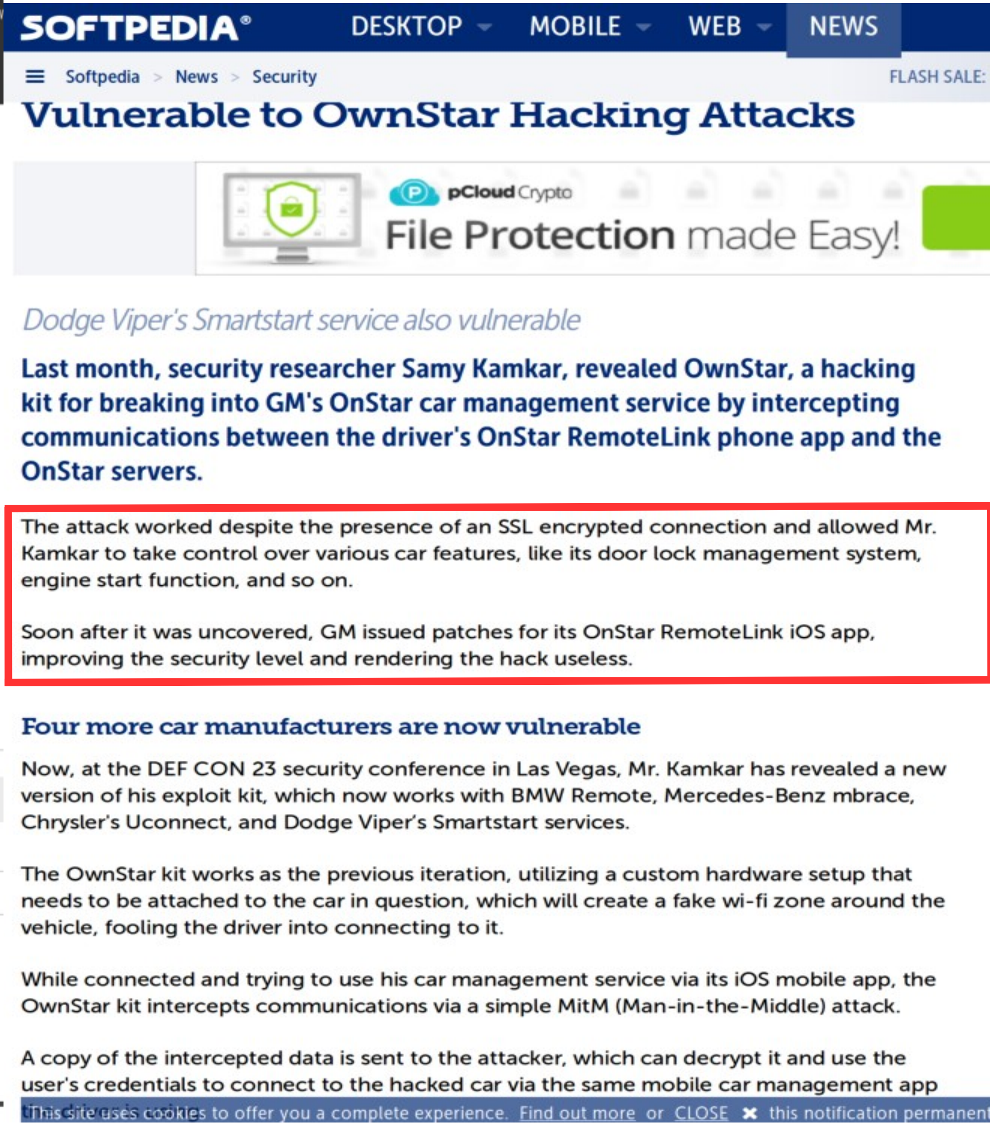
Email address:

Your email address

Sign up

Please support Security Affairs if you want it to continue to grow. Thank you Pierluigi

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. Accept Read More



Vulnerable to OwnStar Hacking Attacks

Dodge Viper's Smartstart service also vulnerable

Last month, security researcher Samy Kamkar, revealed OwnStar, a hacking kit for breaking into GM's OnStar car management service by intercepting communications between the driver's OnStar RemoteLink phone app and the OnStar servers.

The attack worked despite the presence of an SSL encrypted connection and allowed Mr. Kamkar to take control over various car features, like its door lock management system, engine start function, and so on.

Soon after it was uncovered, GM issued patches for its OnStar RemoteLink iOS app, improving the security level and rendering the hack useless.

Four more car manufacturers are now vulnerable

Now, at the DEF CON 23 security conference in Las Vegas, Mr. Kamkar has revealed a new version of his exploit kit, which now works with BMW Remote, Mercedes-Benz mbrace, Chrysler's Uconnect, and Dodge Viper's Smartstart services.

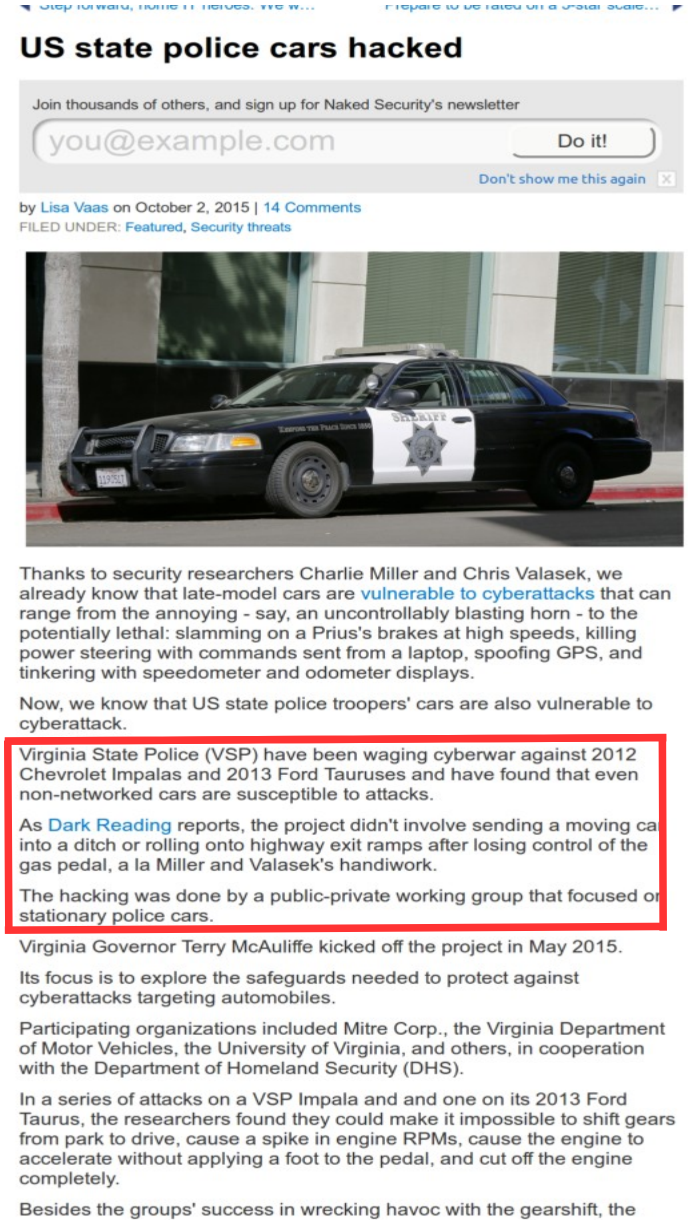
The OwnStar kit works as the previous iteration, utilizing a custom hardware setup that needs to be attached to the car in question, which will create a fake wi-fi zone around the vehicle, fooling the driver into connecting to it.

While connected and trying to use his car management service via its iOS mobile app, the OwnStar kit intercepts communications via a simple MitM (Man-in-the-Middle) attack.

A copy of the intercepted data is sent to the attacker, which can decrypt it and use the user's credentials to connect to the hacked car via the same mobile car management app

This site uses cookies to offer you a complete experience. Find out more or CLOSE ✖ this notification permanent

Real Attacks on Vehicles (2 of 2)



◄ Step forward, home IT heroes: We w... Prepare to be rated on a 5-star scale... ►

US state police cars hacked

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again

by Lisa Vaas on October 2, 2015 | 14 Comments
FILED UNDER: Featured, Security threats

Thanks to security researchers Charlie Miller and Chris Valasek, we already know that late-model cars are vulnerable to cyberattacks that can range from the annoying - say, an uncontrollably blasting horn - to the potentially lethal: slamming on a Prius's brakes at high speeds, killing power steering with commands sent from a laptop, spoofing GPS, and tinkering with speedometer and odometer displays.

Now, we know that US state police troopers' cars are also vulnerable to cyberattack.

Virginia State Police (VSP) have been waging cyberwar against 2012 Chevrolet Impalas and 2013 Ford Tauruses and have found that even non-networked cars are susceptible to attacks.

As Dark Reading reports, the project didn't involve sending a moving car into a ditch or rolling onto highway exit ramps after losing control of the gas pedal, a la Miller and Valasek's handiwork.

The hacking was done by a public-private working group that focused on stationary police cars.

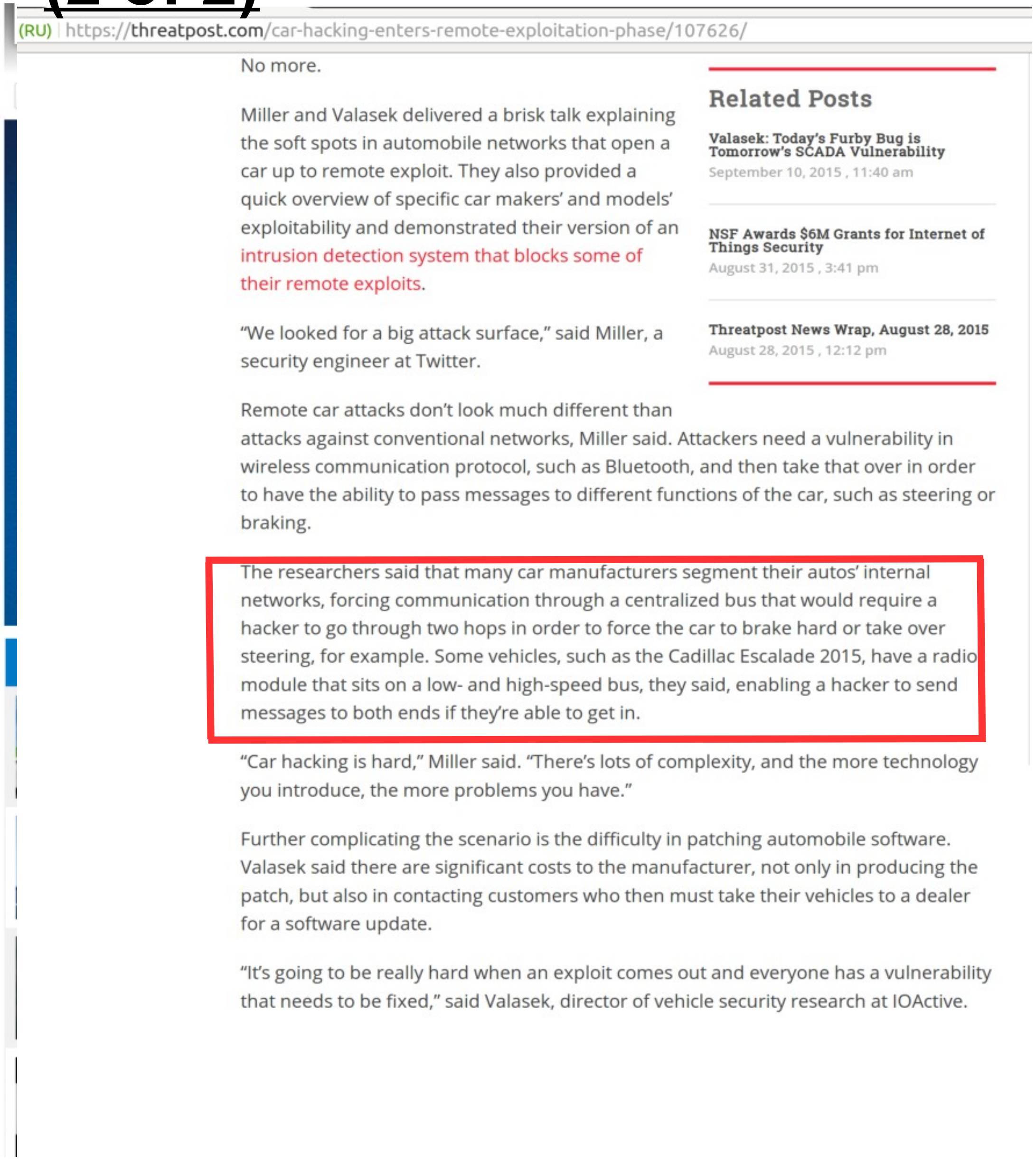
Virginia Governor Terry McAuliffe kicked off the project in May 2015.

Its focus is to explore the safeguards needed to protect against cyberattacks targeting automobiles.

Participating organizations included Mitre Corp., the Virginia Department of Motor Vehicles, the University of Virginia, and others, in cooperation with the Department of Homeland Security (DHS).

In a series of attacks on a VSP Impala and and one on its 2013 Ford Taurus, the researchers found they could make it impossible to shift gears from park to drive, cause a spike in engine RPMs, cause the engine to accelerate without applying a foot to the pedal, and cut off the engine completely.

Besides the groups' success in wrecking havoc with the gearshift, the



(RU) https://threatpost.com/car-hacking-enters-remote-exploitation-phase/107626/

No more.

Miller and Valasek delivered a brisk talk explaining the soft spots in automobile networks that open a car up to remote exploit. They also provided a quick overview of specific car makers' and models' exploitability and demonstrated their version of an intrusion detection system that blocks some of their remote exploits.

"We looked for a big attack surface," said Miller, a security engineer at Twitter.

Remote car attacks don't look much different than attacks against conventional networks, Miller said. Attackers need a vulnerability in wireless communication protocol, such as Bluetooth, and then take that over in order to have the ability to pass messages to different functions of the car, such as steering or braking.

The researchers said that many car manufacturers segment their autos' internal networks, forcing communication through a centralized bus that would require a hacker to go through two hops in order to force the car to brake hard or take over steering, for example. Some vehicles, such as the Cadillac Escalade 2015, have a radio module that sits on a low- and high-speed bus, they said, enabling a hacker to send messages to both ends if they're able to get in.

"Car hacking is hard," Miller said. "There's lots of complexity, and the more technology you introduce, the more problems you have."

Further complicating the scenario is the difficulty in patching automobile software. Valasek said there are significant costs to the manufacturer, not only in producing the patch, but also in contacting customers who then must take their vehicles to a dealer for a software update.

"It's going to be really hard when an exploit comes out and everyone has a vulnerability that needs to be fixed," said Valasek, director of vehicle security research at IOActive.

Related Posts

Valasek: Today's Furby Bug is Tomorrow's SCADA Vulnerability
September 10, 2015 , 11:40 am

NSF Awards $6M Grants for Internet of Things Security
August 31, 2015 , 3:41 pm

Threatpost News Wrap, August 28, 2015
August 28, 2015 , 12:12 pm

What is needed to enhance Protection of Vehicles against Cyber Attacks?

- Vehicle Manufacturer
  - Are Vehicular Networks - as they are (LIN-, CAN- Bus, …) prepared for integrating wireless technologies to support online services?
    => Are new network structures needed for vehicles ?
  - Security by design principle based on a dedicated security methodology ?
  - Pentesting of automotive networks and interfaces by third parties ?
  - Standardized security requirements ?
  - „Formal“ evaluation and certification of dedicated security components/separation techniques ?
  - …
- Vehicle Customer/Buyer
  - Protection against cyber attacks is part of buying decision ?

Panel on ICWMC / VEHICULAR
Topic: Challenges on Security and Trust in Mobile Environments

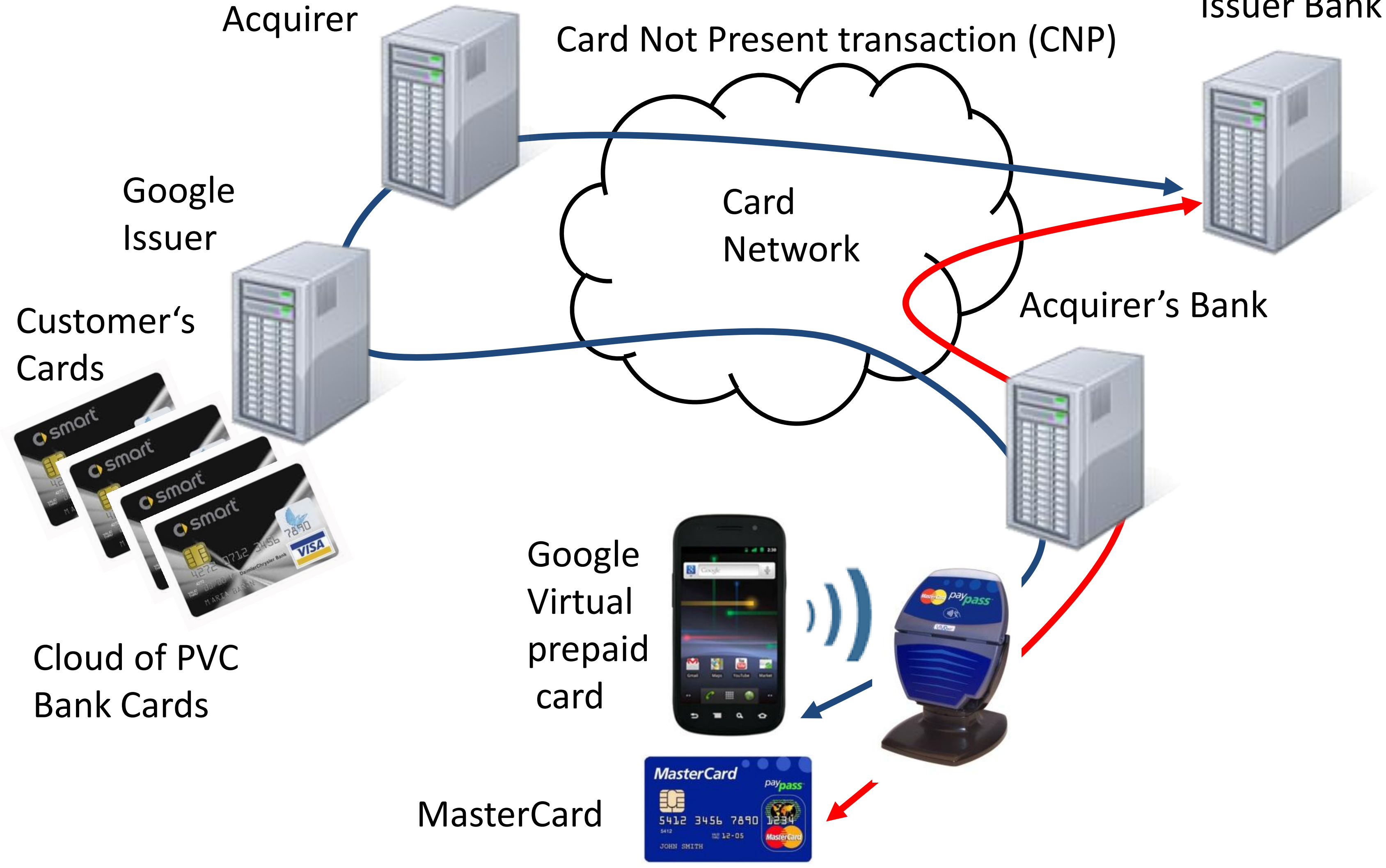
Secure and Trusted Mobile Payments
for Smart Cities

Pascal.Urien@Telecom-ParisTech.fr

About Mobile Payments

- Payments thanks to (connected) mobiles
- Huge market, $$$$$$$$$
- Different from legacy magnetic stripe or EMV (chip) payments
  - The mobile is your payment card
  - Connected device
  - With a screen
  - Able to establish user approval for transaction
- **Trust and Security are the main issues**

The Google Wallet 2 (2012)



Google Acquirer

Customer's Issuer Bank

Card Not Present transaction (CNP)

Card Network

Google Issuer

Customer's Cards

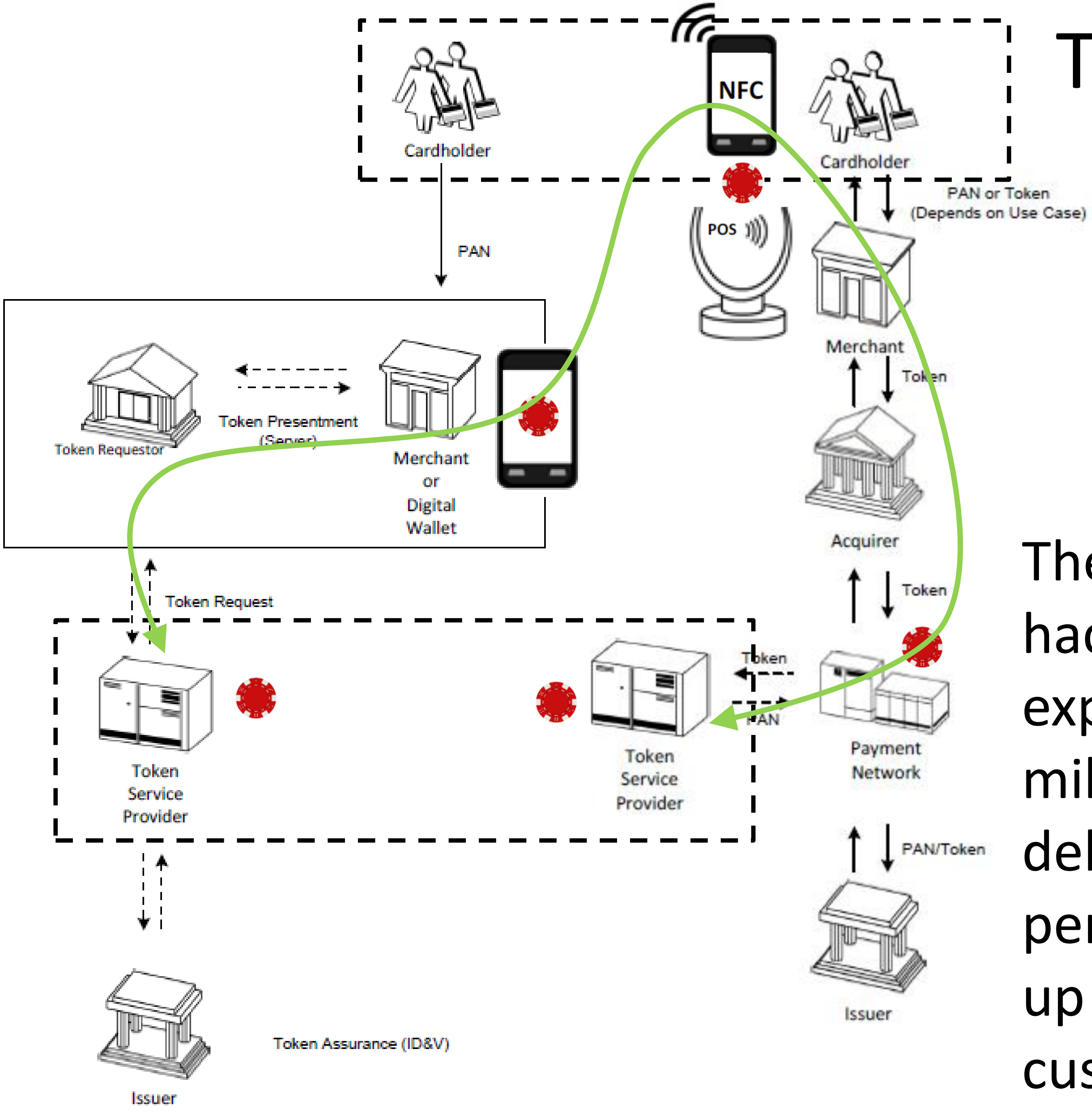
Acquirer's Bank

Cloud of PVC Bank Cards

Google Virtual prepaid card

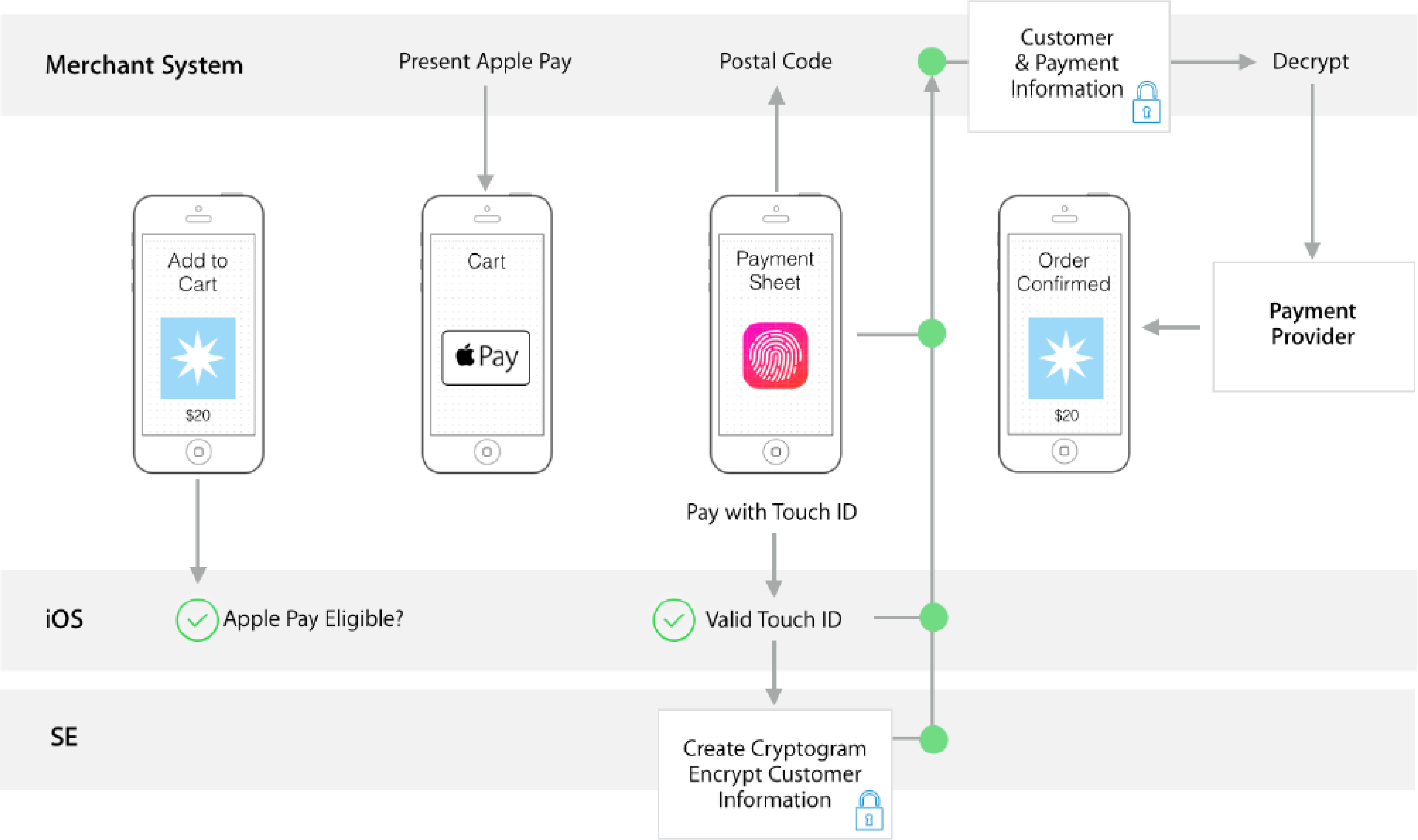
MasterCard

Tokenisation (2013)



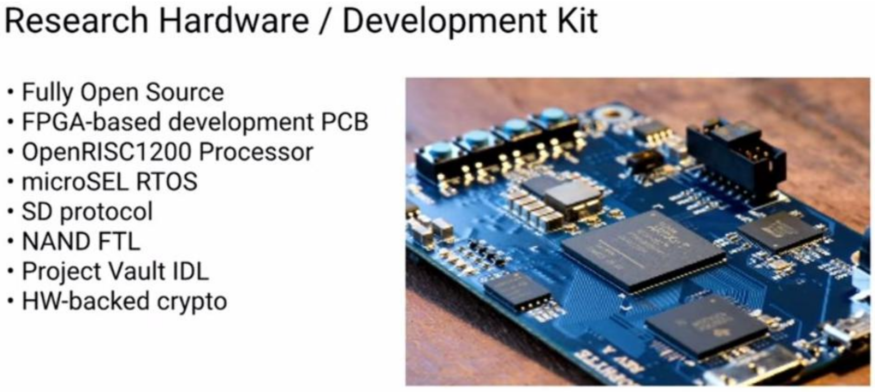
The Target stores hack fall 2013 exposed up to 40 million credit and debit cards and personal data for up to 70 million customers

ApplePay (2014): A Token Requestor



Getting Started with Apple Pay, Version 1.0, 2014

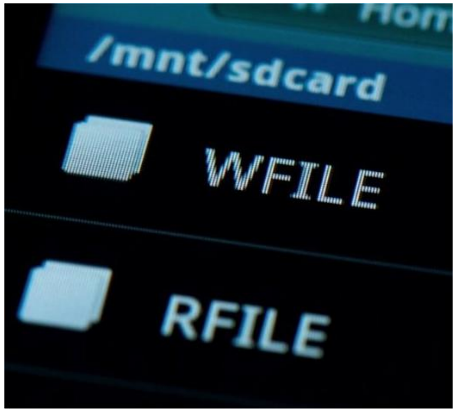
Google Vault (2015): a SD Card



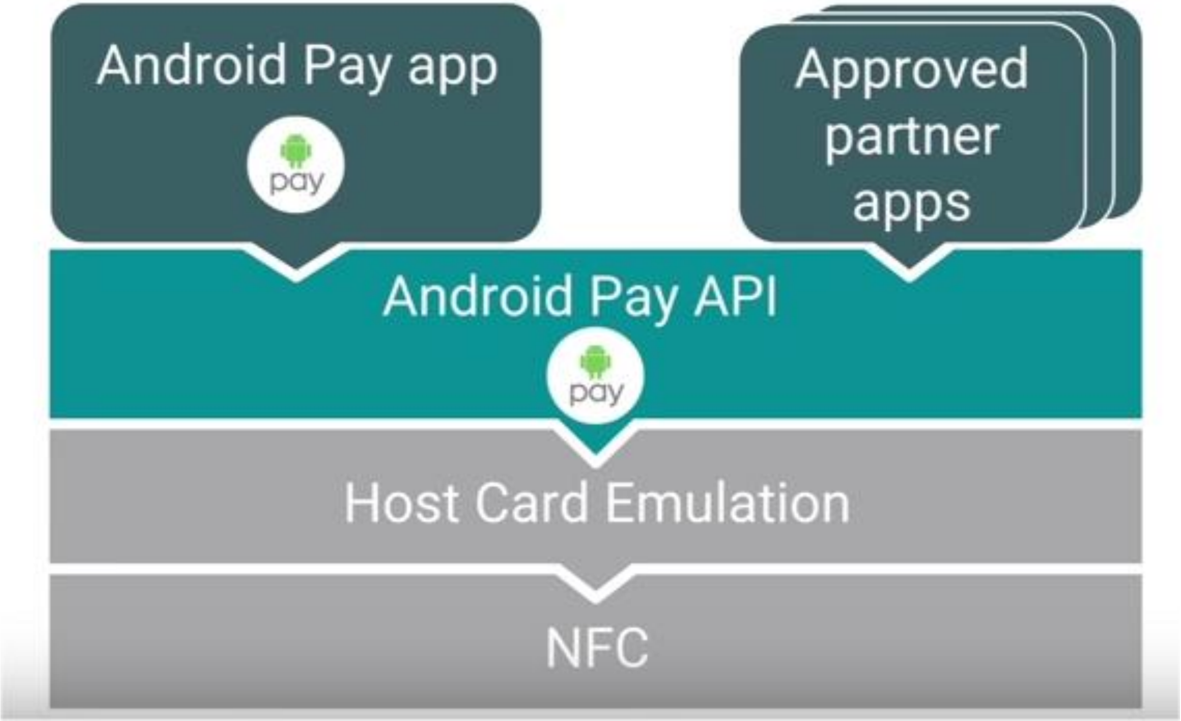
Research Hardware / Development Kit

- Fully Open Source
- FPGA-based development PCB
- OpenRISC1200 Processor
- microSEL RTOS
- SD protocol
- NAND FTL
- Project Vault IDL
- HW-backed crypto

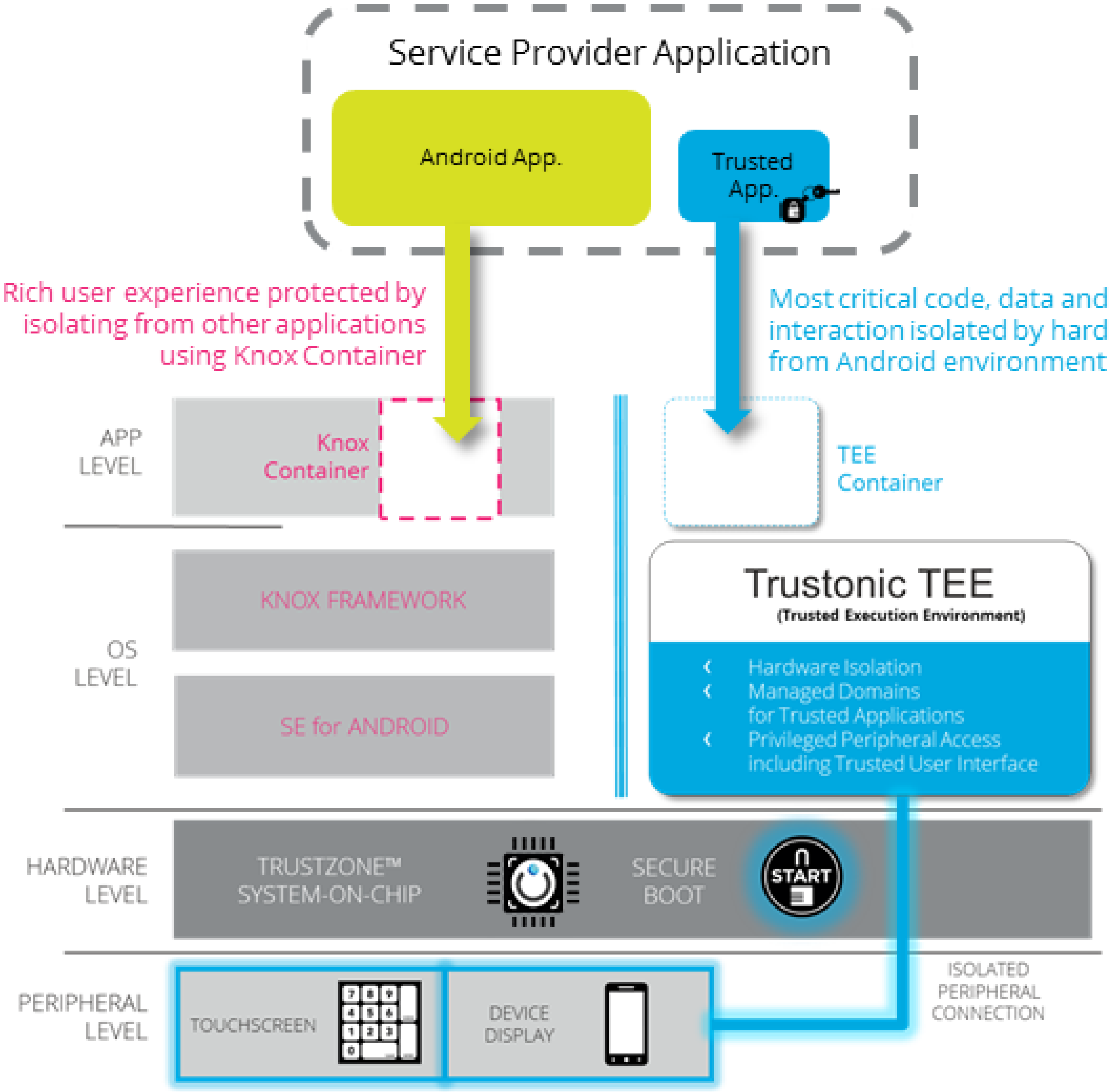
- SD card
- Only two files: WFILE and RDFILE
- Cryptographic procedures
- GB of storage
- MB of throughput
- NFC controller



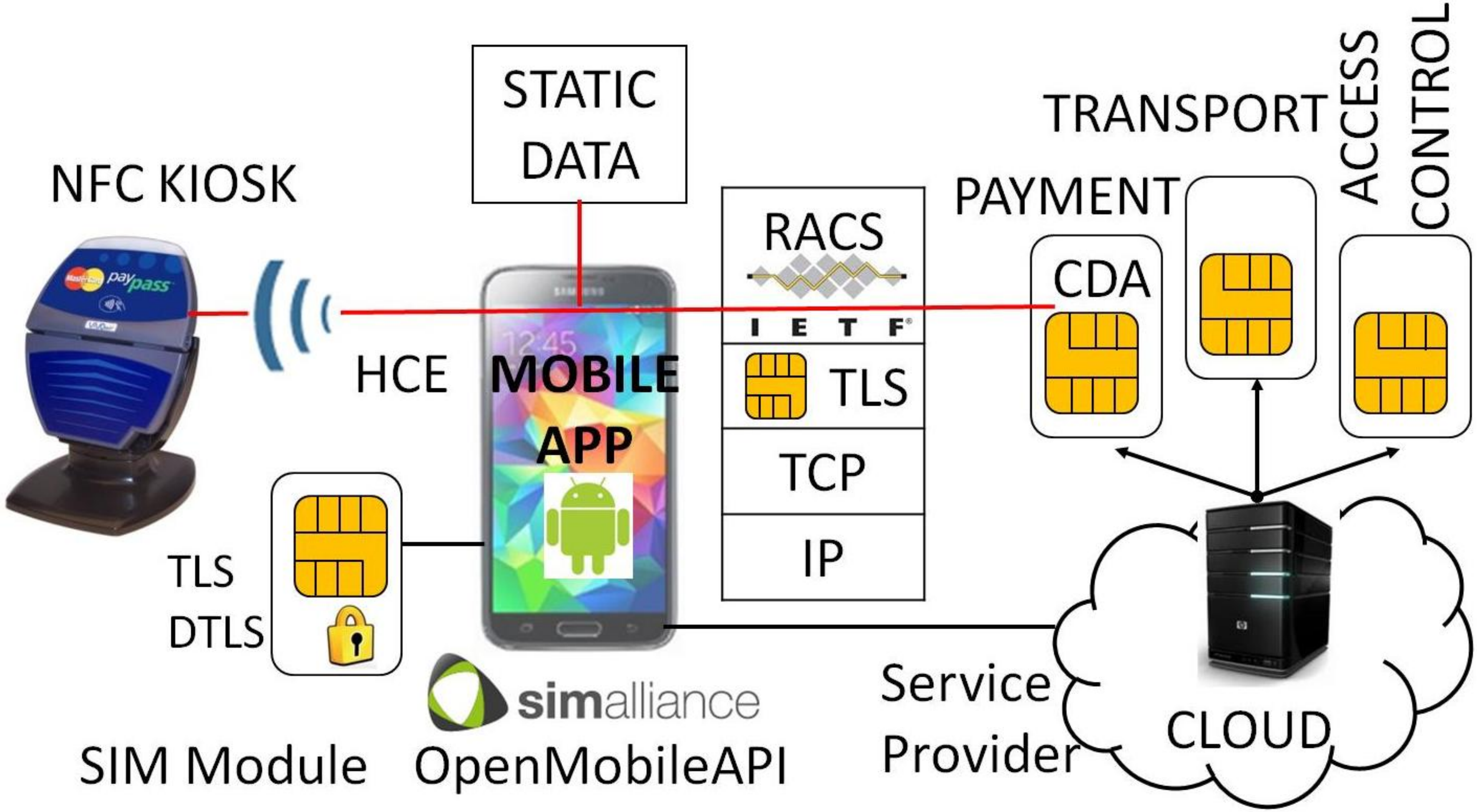
Android Pay (2015)



Samsung Pay (2015): Samsung KNOX


Service Provider Application
Android App.
Trusted App.
Rich user experience protected by isolating from other applications using Knox Container
Most critical code, data and user interaction isolated by hardware from Android environment
APP LEVEL
Knox Container
TEE Container
OS LEVEL
KNOX FRAMEWORK
SE for ANDROID
Trustonic TEE
(Trusted Execution Environment)
Hardware Isolation
Managed Domains for Trusted Applications
Privileged Peripheral Access including Trusted User Interface
HARDWARE LEVEL
TRUSTZONE™ SYSTEM-ON-CHIP
SECURE BOOT
START
PERIPHERAL LEVEL
TOUCHSCREEN
DEVICE DISPLAY
ISOLATED PERIPHERAL CONNECTION

Secure Elements In the Cloud (2015)


STATIC
DATA
NFC KIOSK
RACS
I E T F
TLS
TCP
IP
TRANSPORT
ACCESS
CONTROL
PAYMENT
CDA
HCE
MOBILE
APP
TLS
DTLS
simalliance
SIM Module
OpenMobileAPI
Service
Provider
CLOUD