Strong Security for Network Equipment

June 2020

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

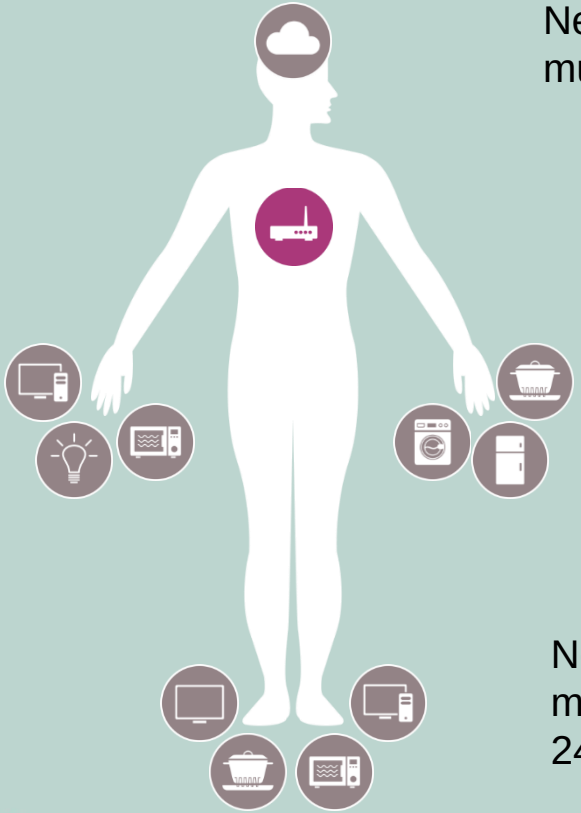
Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Network equipment: The nervous system of the connected world

Network Equipment connects the world

- Routers
- Switches
- Wireless Access Points
- Firewalls
- Gateways



Network Equipment must be

- Reliable
- Secured
- Efficient

While under constant attack

Network Equipment must **just work** 24 x 7 x 365

Impact of attacks on network equipment

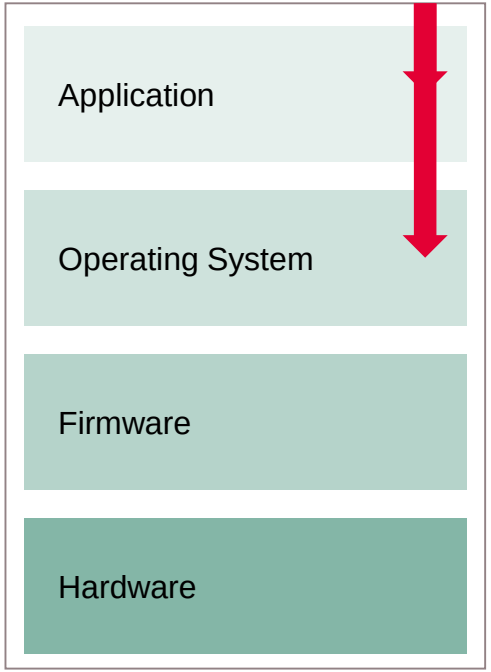
- Brand / Image
- Safety / Liability
- Equipment
- Uptime
- Revenue / Fines
- Impact on Dependents

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Software attacks

Typical Software Attack



Attack Steps

1. Find software vulnerabilities
2. Create exploits (malware)
3. Gain access
4. Escalate privilege

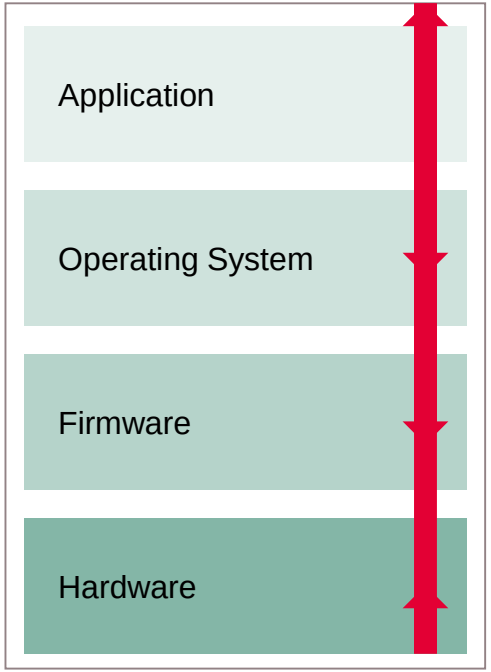
… or just buy a toolkit

Common Goals

- Temporarily Control Network Equipment
- Mount DDoS Attacks
- Build Botnet and Rent Out Bots
- Display Substitute Ads for Profit
- Infect Laptops and Install Ransomware

Firmware and hardware attacks

Typical Firmware or Hardware Attack



Attack Steps

1. Mount a software attack
2. Reflash firmware

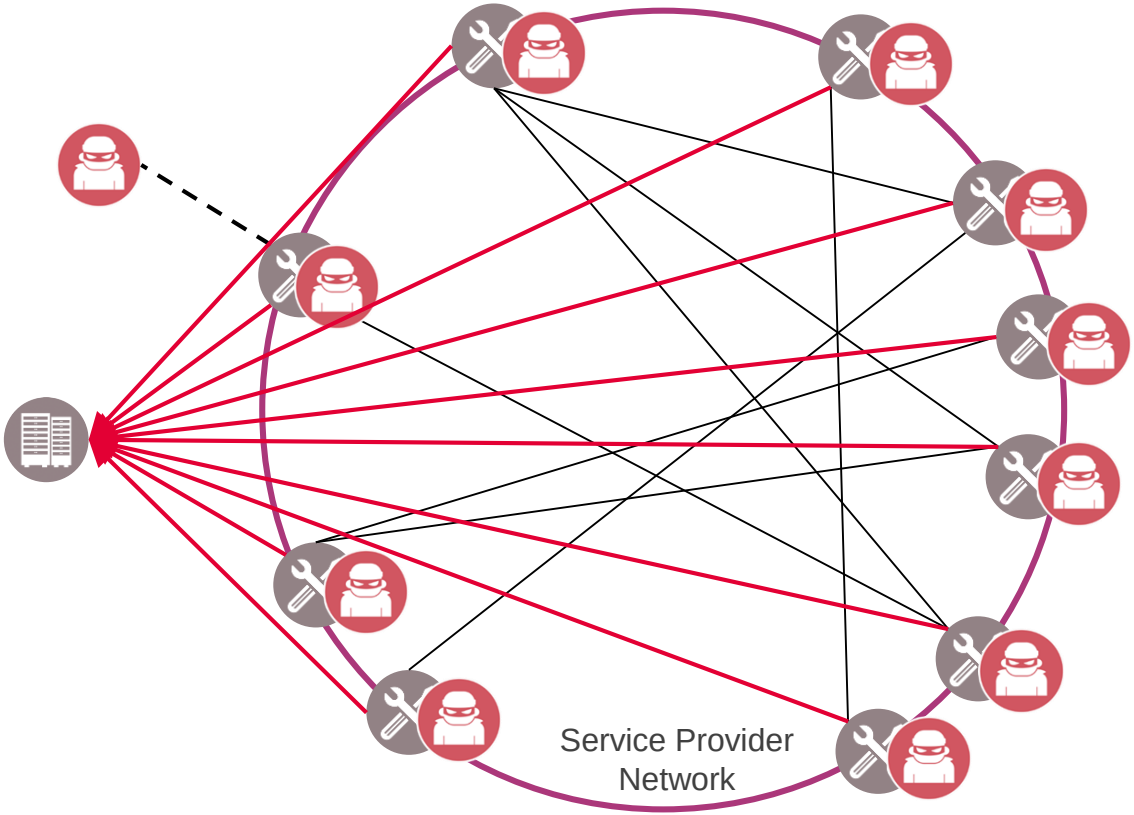
… or …

1. Mount a hardware attack
2. Subvert firmware and software

Common Goals

- Permanently Control Network Equipment
- Establish Permanent, Invisible Control
- Perform Attacks From Last Slide
- Disable (Brick) Network Equipment

Mirai attack flow description



Source: http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Top security concerns

- Protection against Fake Devices
- Protection against Eavesdropping
- Protection against Data Manipulation
- Protection against Infection

Anti-counterfeiting

Threat

- Counterfeit of devices or of parts and accessories
- Revenue & brand loss
- Malfunctioning of system leading to product & brand damage & inherent liabilities

Response

- One-way or mutual device authentication

Infineon Solution

OPTIGA™ Family to prove authenticity

Secured communication

Threat

- Malicious interaction with connected devices
- Eavesdropping
- Targeted or mass disruption
- IP loss due to eavesdropping equals lost business

Response

- Authenticate components and personnel and protect integrity of exchanged information
- Use tamper resistant secure elements with unique credentials
- Encrypt exchanged data

Infineon Solution

OPTIGA™ TPM empowered with the appropriate authentication, integrity, and/or encryption security functions

Secured software update

Need

- Enable remote configuration management
- Software versioning, licensing
- Avoid risks of corrupted software to be uploaded

Response

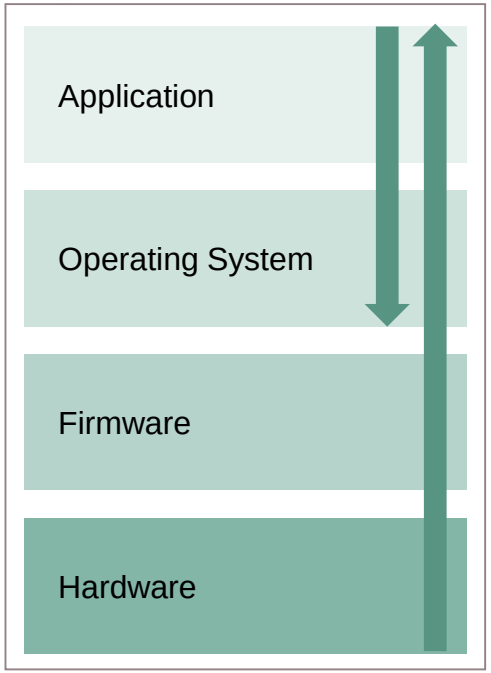
- Authentication and integrity check: signed and/or encrypted code
- Secured loading mechanisms
- User authentication

Infineon Solution

OPTIGA™ TPM for integrity check, device authentication, and encryption

Blocking software attacks

Blocking a Typical Software Attack



Defensive Steps

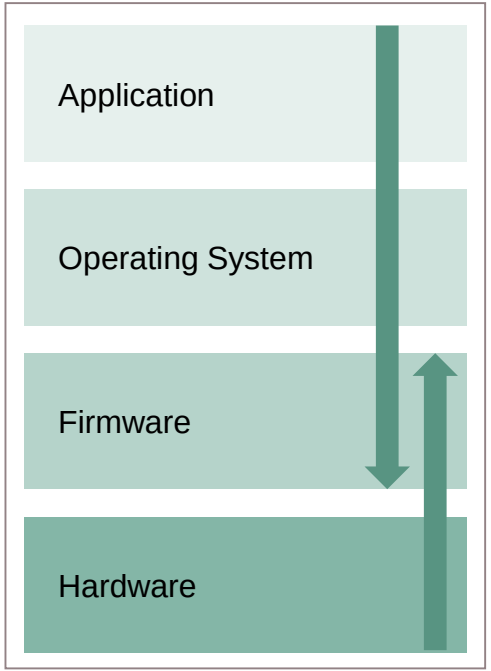
1. Find software vulnerabilities
2. Develop software updates to fix them
3. Securely install software updates
4. Use measured boot to verify proper updates

Role of Hardware Root of Trust

- Secure communications for update delivery
- Verify and optionally decrypt software update
- Verify proper installation of software updates
- Report to management server on installed software

Blocking firmware and hardware attacks

Blocking Firmware or Hardware Attacks



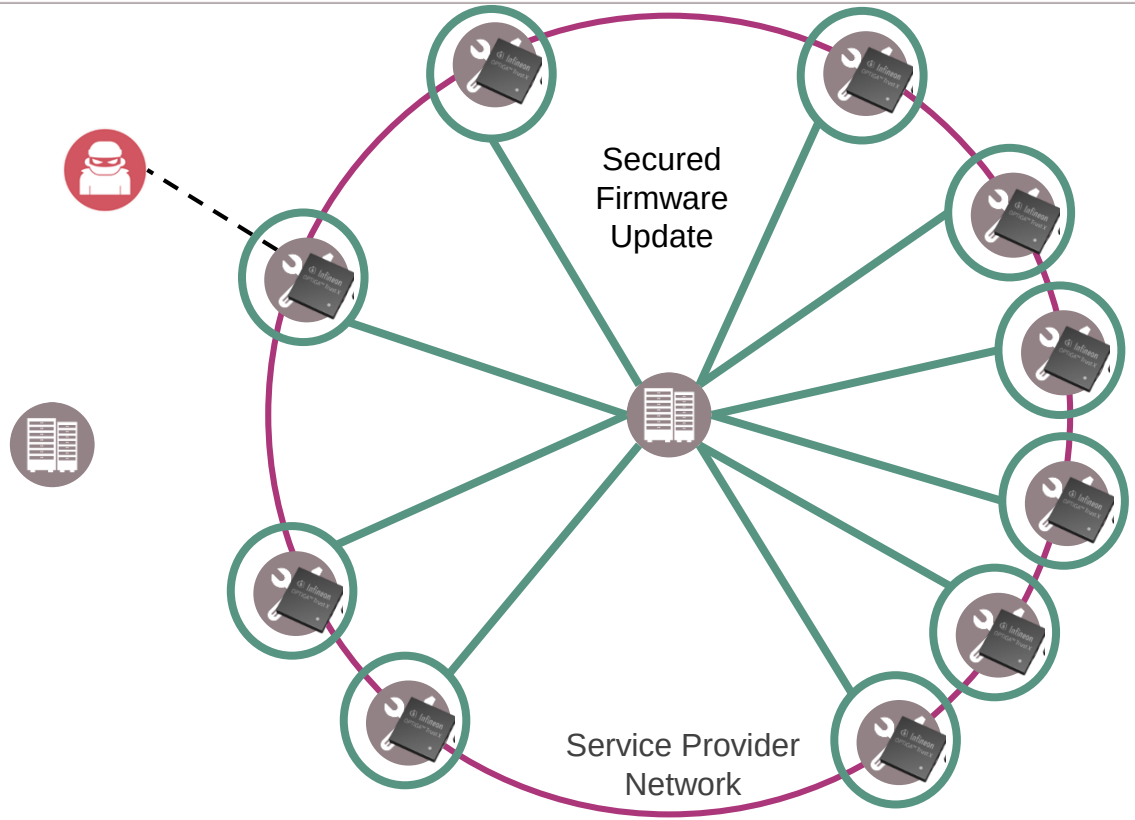
Defensive Steps

1. Find firmware vulnerabilities
2. Develop and install firmware updates to fix them
3. Prevent malicious reflashing of firmware
4. Prevent hardware tampering to subvert security

Role of Hardware Root of Trust

- Secure communications for update delivery
- Verify and optionally decrypt firmware update
- Prevent installation of unauthorized updates
- Report to management server on installed firmware
- Protect security functions against tampering

Blocking the Mirai attack



Source: http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

We understand your challenges, which we can address with our security solutions

Challenges we heard from ICT customers

"I need to protect my brand and manage risks"

"How can we address the growing sophistication of attacks?"

"Can security ease my customer experience and increase revenue?"

We can meet your own security needs and help you to meet your customers' needs

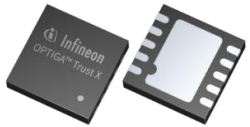
	Our understanding of your needs		How we address your needs
For you to meet your customers' needs	Easy deployment	✓	Simpler customer set up via injected device identity
	Reliable managed security	✓	Remote attestation enables remote security management
	Confidence in virtualization	✓	Hardware security extends to VMs via hypervisor support
Your own needs	Increased revenue	✓	Hardware security products support feature licensing
	Protection against sophisticated attacks	✓	Advanced defenses
	Protection of company brand and minimization of risks	✓	Hardware security minimizes vulnerabilities and maximizes sustainability

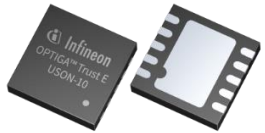
Why hardware security is needed for network equipment security

	Main CPU + Software	Main CPU + Software + Hardware
Crypto functionality	✓	✓
Strong isolation	-	✓
Security certified	-	✓
Tamper resistant	-	✓
Manufactured by security certified processes	-	✓
Resistant against IP Theft	-	✓

A strong network equipment business requires strong security

Trend/customer need	Feature/Service	Benefit
› Reassure customers on security and privacy › Provide reliable service › Enable feature sales › Reduce warranty repairs › Regulatory requirements › Easy for end use and integration	› The right security for IoT › Certification › Long lifetime › Tamper resistance › Recovery from host infection › Integrated solution › With keys and certificates loaded	› Increased sales › Increased after-market revenue › Decreased warranty costs › Protection of business model › Avoidance of regulatory impacts › Less costs (infrastructure, people)





Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

OPTIGA™ Family

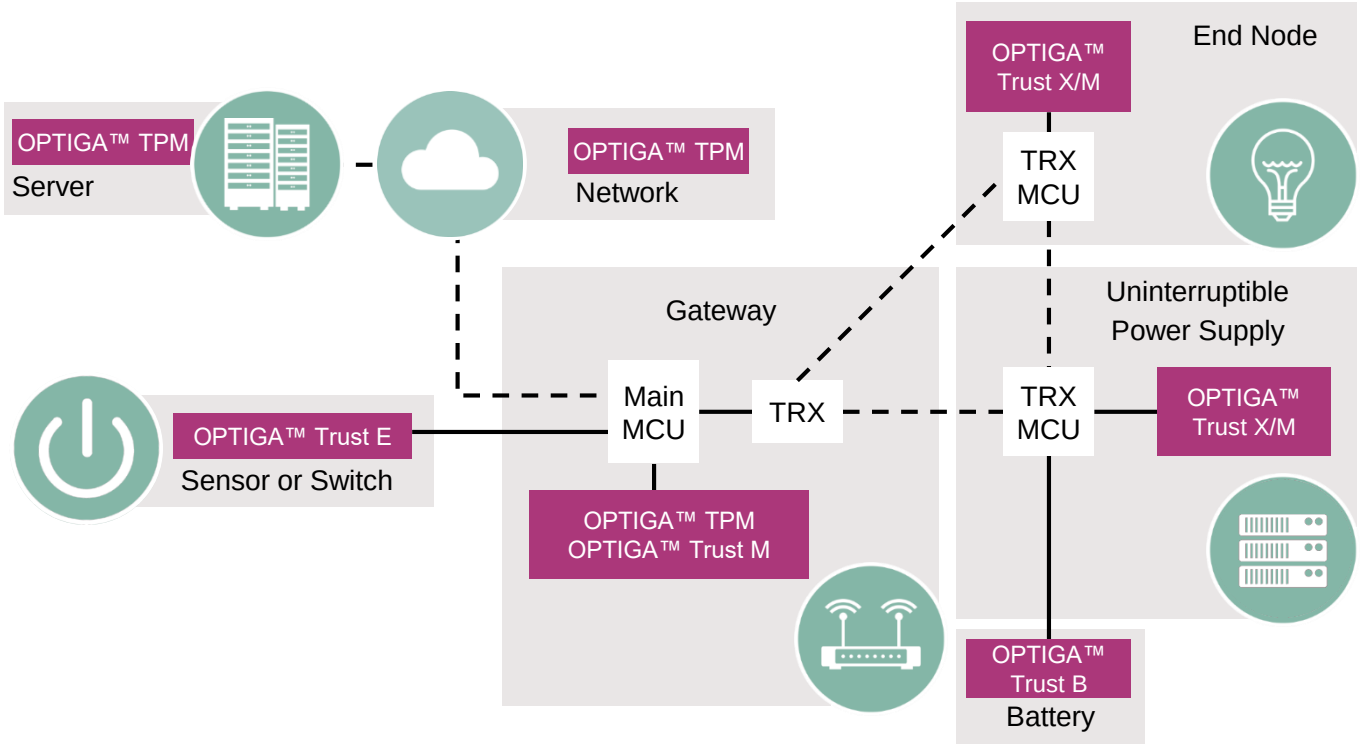
	OPTIGA™ Trust B	OPTIGA™ Trust E	OPTIGA™ Trust M	OPTIGA™ Trust X	OPTIGA™ TPM
					
Security Level	Basic	CC EAL 6+ *	CC EAL 6+ *	CC EAL 6+ *	CC EAL 4+ FIPS 140-2 L2
Functionality	Authentication	Authentication	Connected device security	Connected device security	Connected device security
NVM (Data)	64 Byte	3 kByte	10 kByte	10 kByte	6 kByte
Cryptography Private key stored in secure HW	ECC131	ECC256	ECC384 RSA2K	ECC384	ECC256 RSA2K
Type of Host System	MCU without OS / proprietary OS / RTOS				
			Embedded Linux		
					Windows / Linux
Interface	SWI	I2C	I2C	I2C	I2C, SPI, LPC
System integration	✓	✓	✓	✓	Platform vendor

✓ Done by IFX

* Based on certified HW

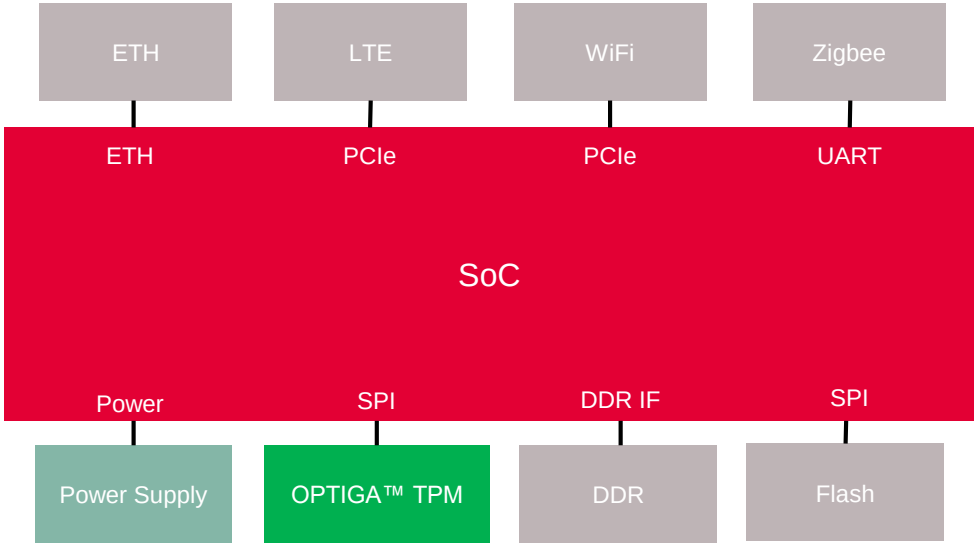
Security and Feature

Product recommendations for networks, servers, and connected Devices



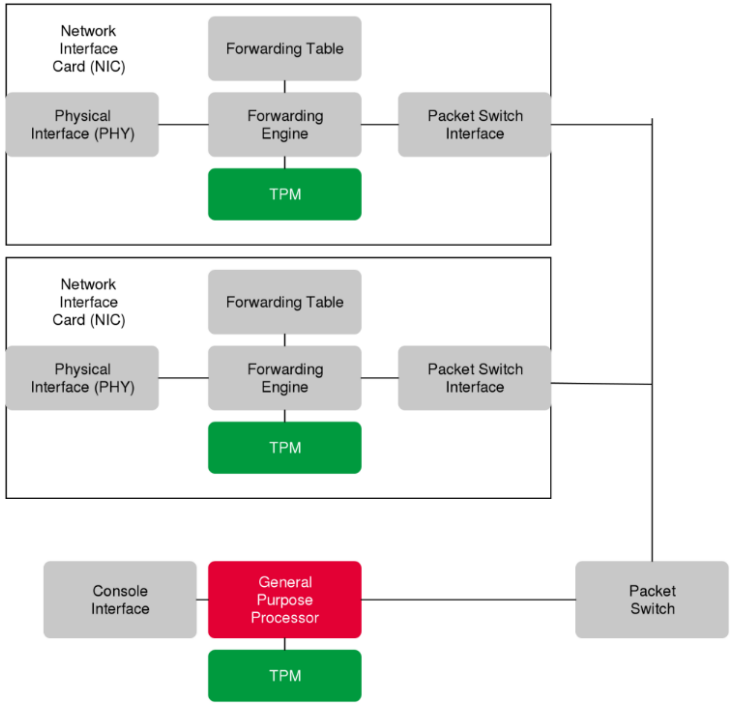
Note: TRX indicates communications function

Example: Home gateway



Power Microcontroller Security Other Products

Example: network router



Power Microcontroller Security Other Products

OPTIGA™ Trust B turnkey authentication

Strong Asymmetric Cryptographic Engine

- Elliptic Curve Cryptography (131 bit key)
- Unique 96 bit identifier (UID)
- Public key certified by ODC-163 based digital certificate
- Optional kill feature

Protected Memory

- 512 bits lockable NVM
- Integrated Lifecycle Counter
- -45 to +85°C now, -45 to +105°C available on request

Easy to Implement

- Full Turnkey Solution with Two Preloaded Key Pairs
- Host Code Provided
- Simple Single Wire Interface

Product Details

Set-up	Turnkey	Interface	SWI
Data Store	64 B	Interface Speed	500kbps
Cryptography	ECC-131	Package	TSNP-6
Available	Now	Size	1.5 x 1.1 mm

More Info:

www.infineon.com/optiga-trust

Contact your Infineon Sales Representative for more information

OPTIGA™ Trust E (SLS 32AIA)
Easy and cost effective security solution for high value goods

Premium Security
- Based on CC EAL 6+ (high) certified security controller
- ECC-256, SHA-256 implemented

Advanced Feature Set
- Secured data storage
- Cryptographic Functions for
  - Authentication
  - Certificate Exchange/ PKI support for customer domain
- -25 to +85°C and -40 to +85°C now, -40 to +105°C with E2

Easy to Implement
- Full Turnkey Solution
- Host Code Provided
- Evaluation kit

Set-up	Turnkey	Interface	I2C
Data Store	Up to 3kB	Interface Speed	400kbps
Cryptography	ECC-256, SHA-256	Package	USON-10
Available	E Now; E2 ES 5/17, QS 10/2017	Size	3 x 3 mm

More Info:

www.infineon.com/optiga-trust

Contact your Infineon Sales Representative for more information

OPTIGA™ Trust M
Secured cloud service provisioning – the easy way!

Easy to Integrate
- Full turnkey solution
- Customer specific certificate provided for zero-touch provisioning
- Host code with abstraction layer
- Evaluation kit

Premium Security
- Based on CC EAL 6+ (high) certified security controller
- X.509 certificate supported
- TRNG AIS-31 certified
- OPTIGA™ Shielded Connection
- CA certificate in-field update

Cryptographic ToolBox
- TLS/DTLS implementation
- Arbitrary security schemes

Extensive Set of Use Cases
- Mutual Authentication
- Secure Communication
- Data Store Protection
- Lifecycle Management
- Power Management
- Secure Update
- Platform Integrity Protection

Endurance
- Up to 1.6 M write cycles

Product Details

Temperature range	-40 to +105°C	Interface	I2C
Data Store	10kB	Interface Speed	1 Mbit/sec
Cryptography	ECC, RSA, AES, SHA	Package	USON-10
Available	Avaliable	Size	3 x 3 mm

OPTIGA™ Trust X (SLS32AIA)
Fully featured device security solution

Premium Security
- Based on CC EAL 6+ (high) certified security controller
- TLS/DTLS Support
- X.509 certificate supported
- TRNG AIS-31 certified
- USB Type C Authentication supported
- Cryptographic ToolBox for flexible customization

Extended Operating Temperatures
- -25 to +85°C
- -40 to +105°C

Extensive Set of Use Cases
- Mutual Authentication
- Secure Communication
- Data Store Protection
- Lifecycle Management
- Power Management
- Secured Update
- Platform Integrity Protection

Easy to Integrate
- Full turnkey solution
- Customer specific public key system provided
- Host Code Provided
- Evaluation kit

Product Details

Set-up	Turnkey	Interface	I2C
Data Store	10kB	Interface Speed	1 Mbit/sec
Cryptography	ECC, AES, SHA2	Package	USON-10
Available	January 2018	Size	3 x 3 mm

More Info:

www.infineon.com/optiga-trust-x

Contact your Infineon Sales Representative for more information

OPTIGA™ TPM (SLB 96xx)
TPM v1.2 and 2.0 certified platform protection

Trusted Platform Module: Secure your Software and Data

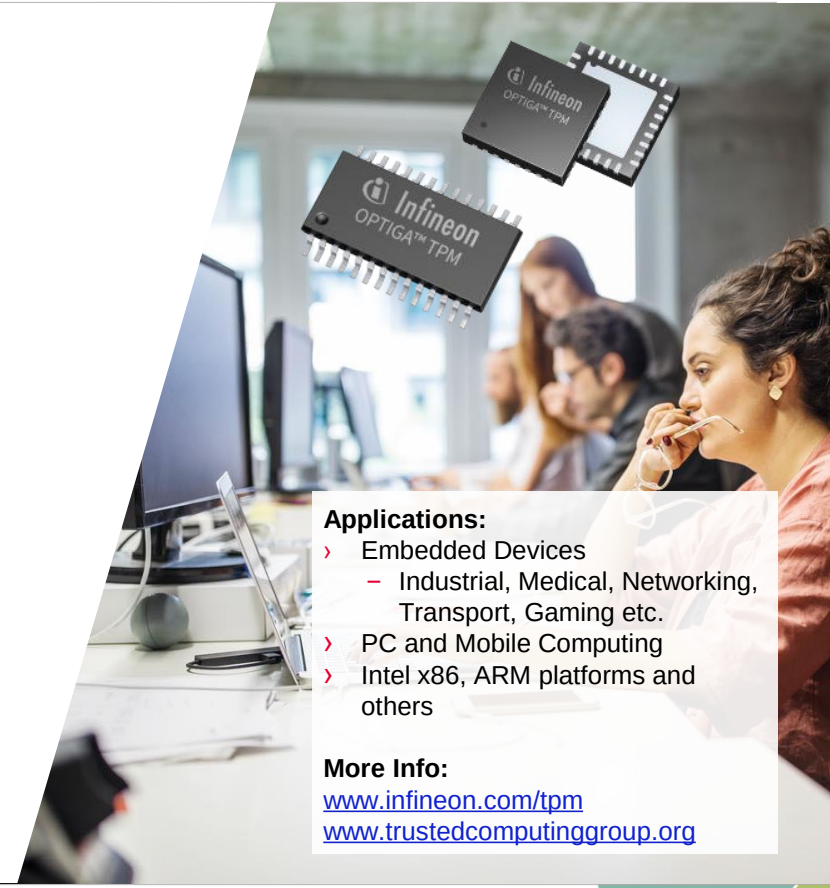
- Strong Authentication of Platform and Users
  - Unique embedded Endorsement Certificate
- Secured Storage and Management of Keys and Data
- Platform protection for embedded systems
  - Measured/Trusted Boot
- RNG, Tick-Counter, Dictionary Attack Lock-out
- Built-in algorithms including RSA, ECC, SHA-256

Certified & Standardized Security

- Official TPM product listed at Trusted Computing Group (TCG)
- Independently security evaluated and certified: According to the international standard Common Criteria

Infineon OPTIGA™ TPM products

Product	TPM	Domain
SLB9645	TPM 1.2	I2C: ARM/non-x86 architectures
SLB9670	TPM 1.2 / TPM 2.0	SPI: Intel/ARM architectures
SLB9660	TPM 1.2	LPC: Intel/x86 architectures
SLB9665	TPM 2.0	



Applications:

- Embedded Devices
  - Industrial, Medical, Networking, Transport, Gaming etc.
- PC and Mobile Computing
- Intel x86, ARM platforms and others

More Info:

www.infineon.com/tpm
www.trustedcomputinggroup.org

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Our solution comes with service and support

We support you by…

- Providing Design-In Application Notes for our Products
- Host side integration support
- Evaluation Kits

- Providing a secured Public Key Infrastructure
- Custom certificate loading in secured Production Environment

- Answering questions immediately
- Two Level Customer service

- Providing trainings for our security products
- Showing Demo Applications as a starting point for custom designs

Infineon Security Partner Network (ISPN)

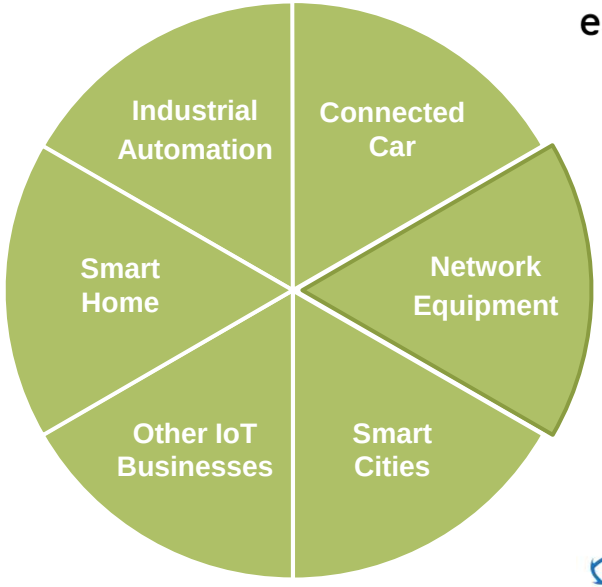
Mission

ISPN is a place for providers of connected devices and applications to find security solutions delivered by security players.

ISPN is the natural choice to get support and solutions for security challenges in an increasingly connected world.

www.infineon.com/ISPN

Partners for securing network equipment

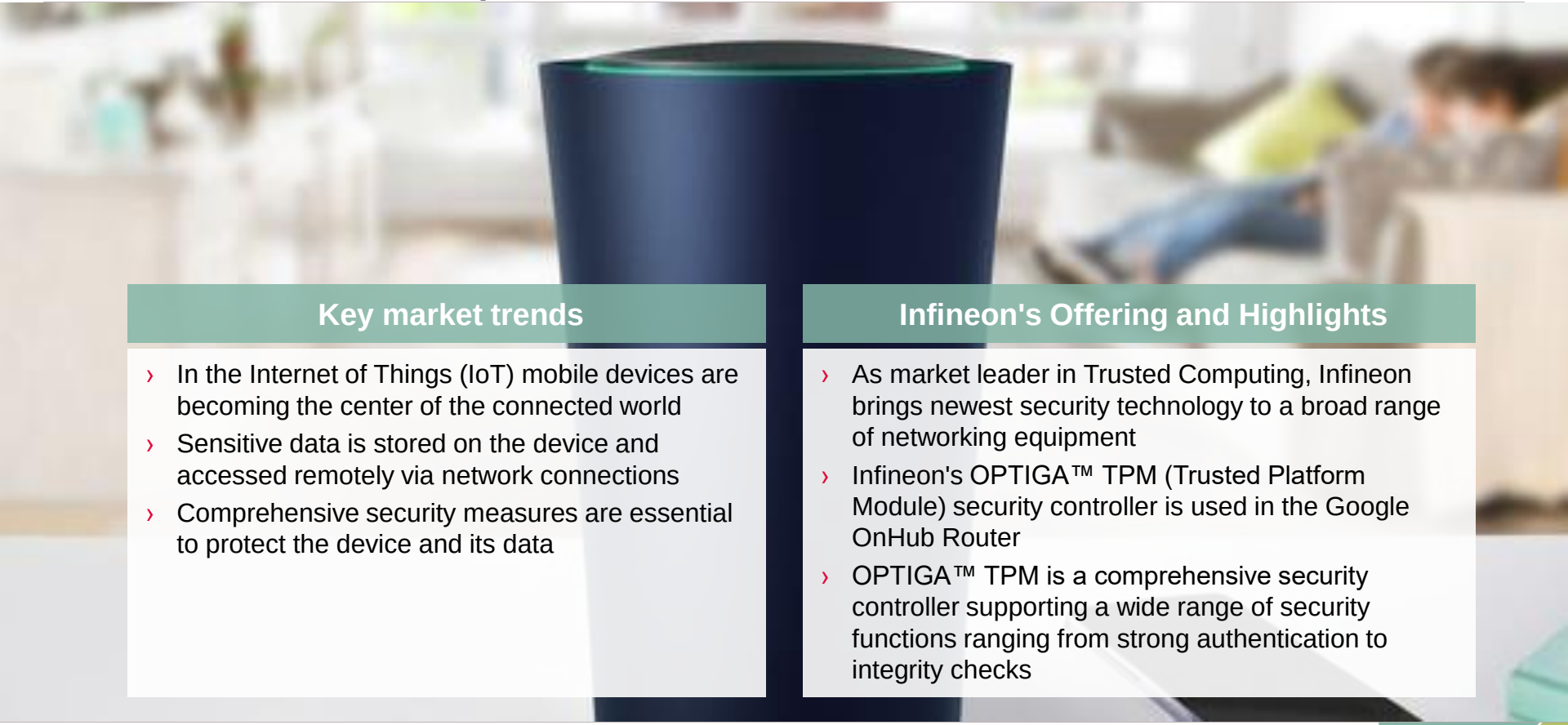


escrypt Embedded Security by ETAS	Security consulting
GlobalSign GMO INTERNET GROUP	Device Identity
MOCANA	Security software libraries
PrimeKey	Device Identity
SECTIGO	Device Identity Software Libraries
digicert	Device Identity

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Trusted Computing expertise for router & smart Home: OPTIGA™ TPM in Google OnHub



Key market trends

- In the Internet of Things (IoT) mobile devices are becoming the center of the connected world
- Sensitive data is stored on the device and accessed remotely via network connections
- Comprehensive security measures are essential to protect the device and its data

Infineon's Offering and Highlights

- As market leader in Trusted Computing, Infineon brings newest security technology to a broad range of networking equipment
- Infineon's OPTIGA™ TPM (Trusted Platform Module) security controller is used in the Google OnHub Router
- OPTIGA™ TPM is a comprehensive security controller supporting a wide range of security functions ranging from strong authentication to integrity checks

Agenda

1. Growing Threats to Network Equipment
2. Understanding Attacks
3. Effective Defenses
4. Business Considerations
5. Infineon Product Offerings
6. Beyond Products
7. Customer Case Study
8. Takeaways

Your personal key takeaways

Strong security is required for network equipment today

Infineon provides scalable, strong, easy to use security solutions

Infineon is the ideal partner for network equipment security

Part of your life. Part of tomorrow.

Infineon