life.augmented

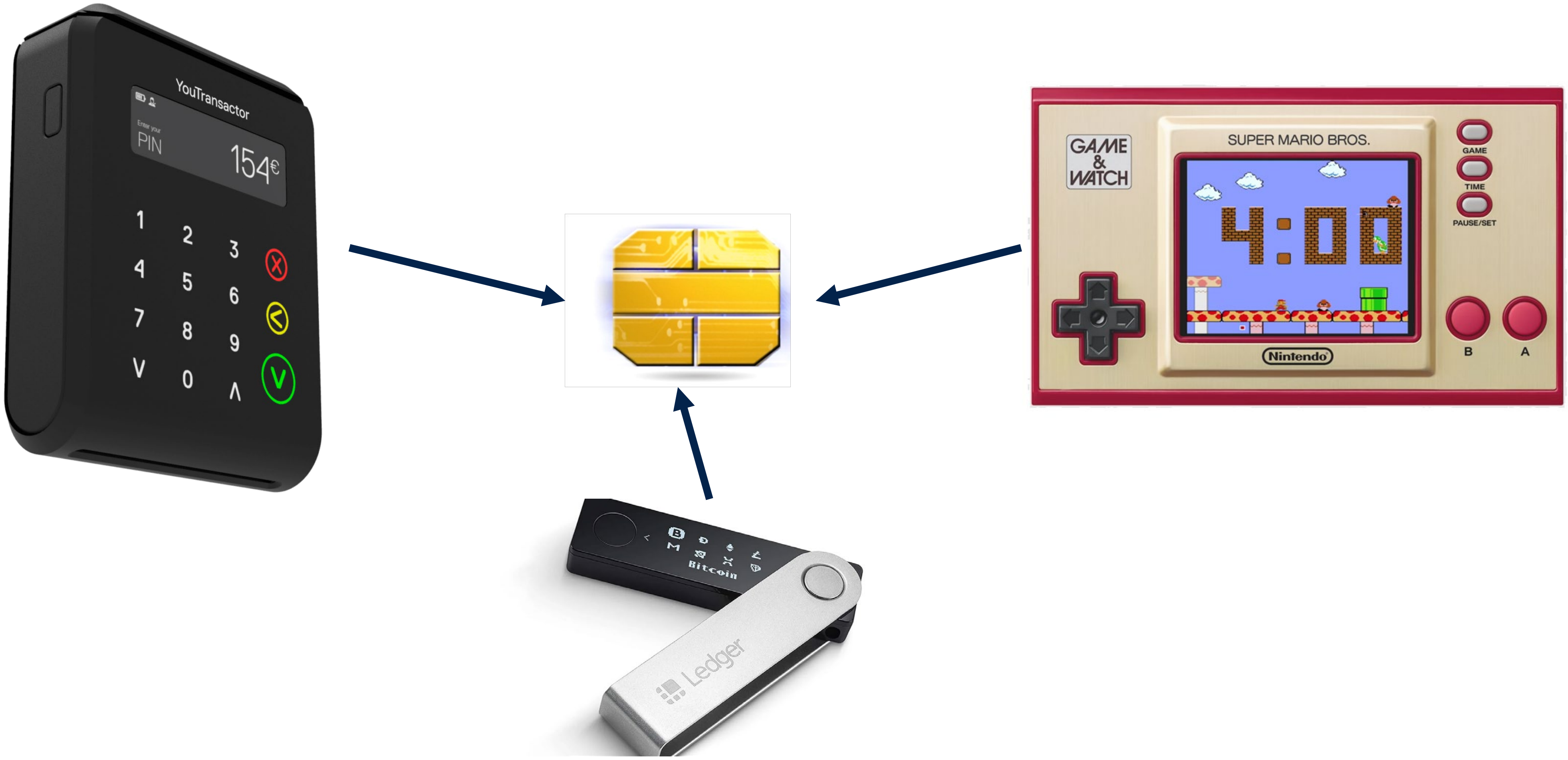
Trusted Chips, Threats and Protections

Olivier Van Nieuwenhuyze

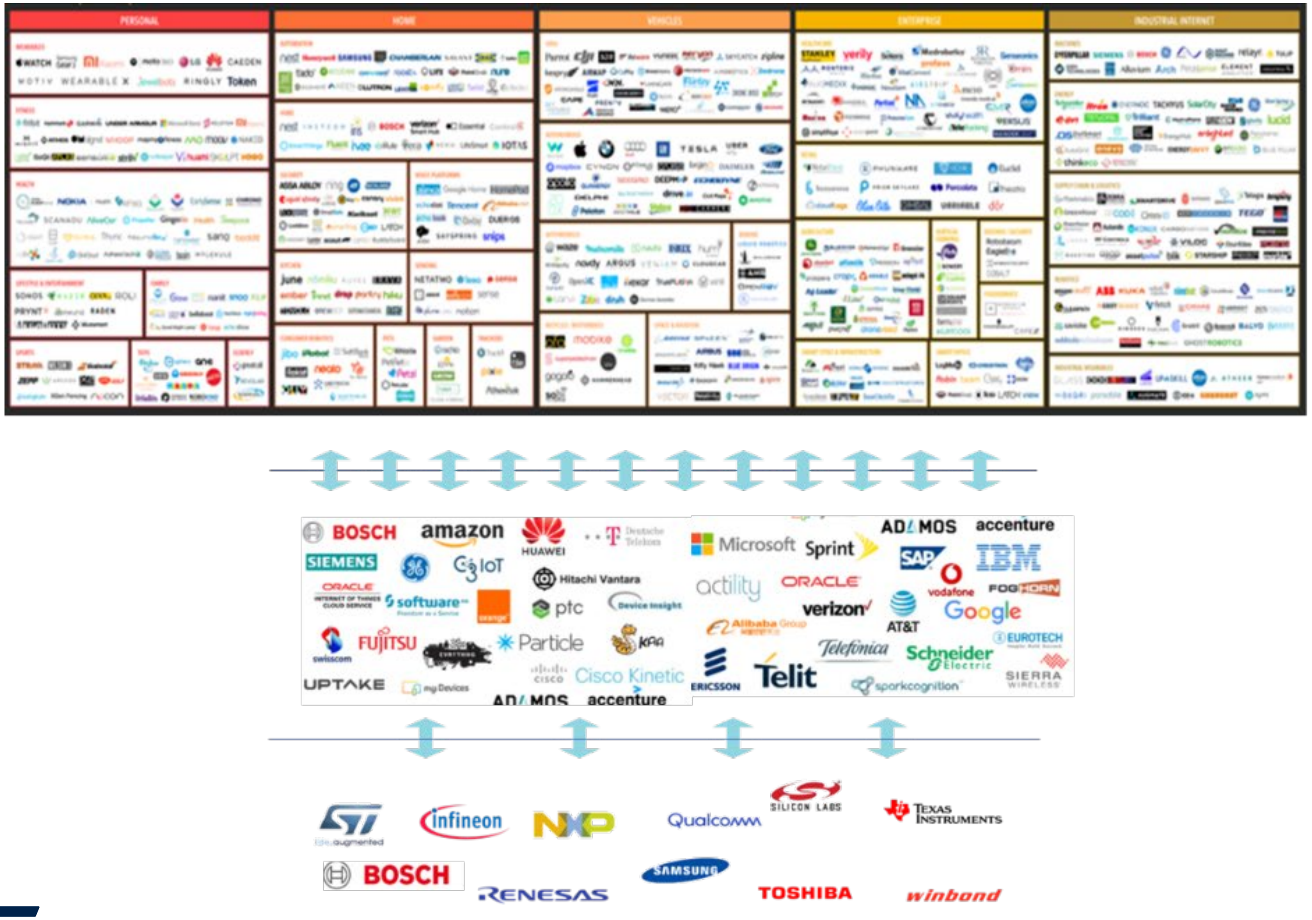
Security Standardization Senior manager

STMicroelectronics

What Is the Common Point ?



Why Semiconductor are Key for Protecting Europe Interest

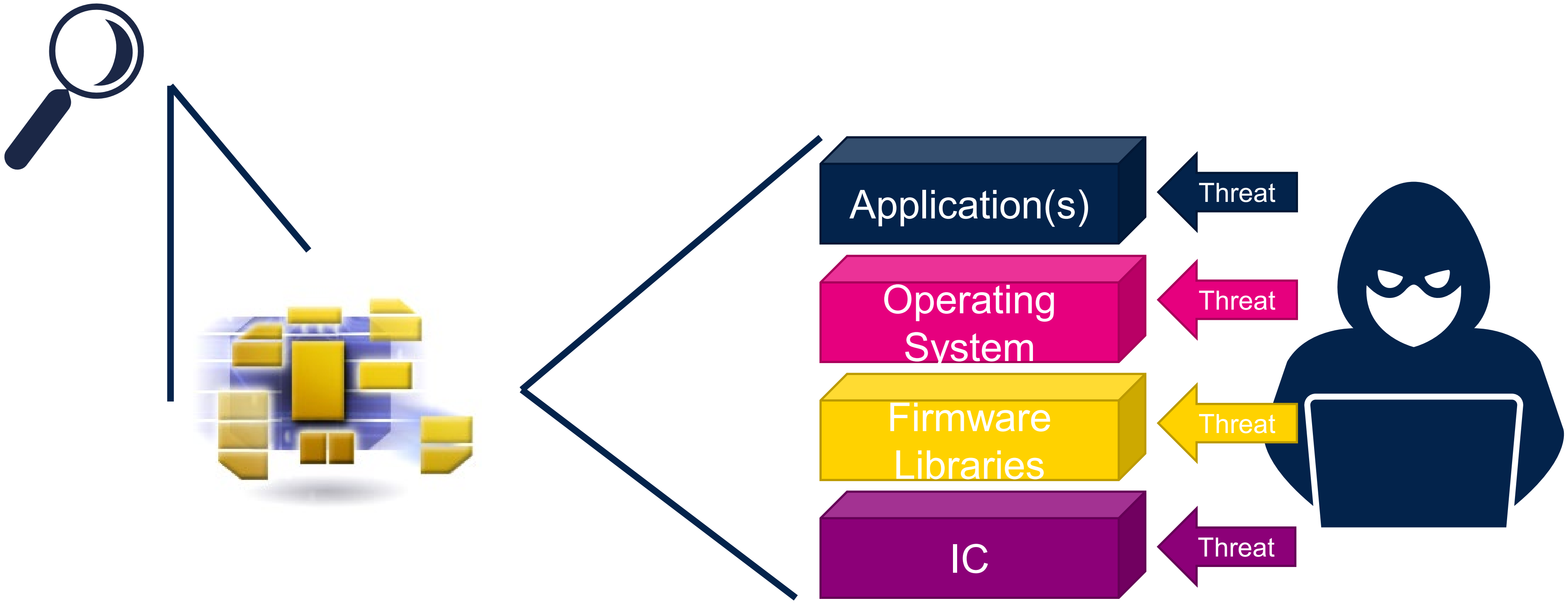


Devices: billions

Platforms: few hundreds

Chip vendors : few tenths

Chip Composition



Great Diversification of known attack techniques

- Denial of Services (DoS)
- Man in the Middle
- Phishing
- Break/stole password
- Malware …
- Ransomware
- Stole goods
- …

Two Categories of Attacks

- No physical access to the device
  - Attack default value
    - i.e.: Admin account with default password / default test key …
  - Install malware application
  - ...

- Physical access to the device
  - See next slide

Attacks and HW & SW Countermeasures

A complete set

More expensive, More time consuming

	Software attack	Board-level attack	Silicon-level attack
Major attacks	• Network protocols weakness (weak ciphers, short keys, mitm*) • Flaws in software design / implementation, buffer overflows • Debug interfaces, gaining admin rights	• Single/Differential Power Analysis (SPA/DPA), emission analysis, timing analysis • Fault injection: glitches, laser, light, UV, X-rays • Memory probing	• Device delayering, circuit reverse engineering, micro-probing • Fault injection: Focused Ion Beam • Advanced microscopy
Countermeasures *Hardware & Software*	• No external debug interface on products (Jtag) • Hardware secure crypto fast computing • Enhanced security of Secure Component with physical isolation of security toolbox (secure key storage, secure & trusted execution in secure element)	• Randomization • Secured crypto-engines • Design Flow • OS features (MPU) • Jittered Clocks • Data whitening • Environment Sensors • Integrity checkers • Code Signature • Internal Clock Integrity	• Physical Shield • Glue Logic Layout • Bus & Memory Scrambling • Bus & Memory Encryption • Anti-reverse • Advanced Lithography

Security Scalability

More information on the Infineon presentation

life.augmented

Patch Deployment

- Patch deployment is not simple
- Usually, no access to the final device
- The supply chain includes several actors (up to the end device)
- Patch needs to be included into a general device patch management/deployment
  - Complex if several components are present in the device

More information on the NXP presentation

Conclusion

- Chips are present in all digital products
  - Provide a horizontal view
- Notion of supply chain and several actors to build a product
- Security is not black or white
  - Additional dimension of the threats with physical access to the device
  - Security Scalability (Robustness + Assurance)
- Specific management vs General ICT product
- Standard(s) may improve the link between all different actors

Our technology starts with You

Find out more at www.st.com

life.augmented