Cybersecurity for Highly Automated Driving

A pragmatic approach

Sagar Behere
Head of EE Integration
Zoox Inc.

GOOD NEWS: CYBERSECURITY IS A SOLVED PROBLEM

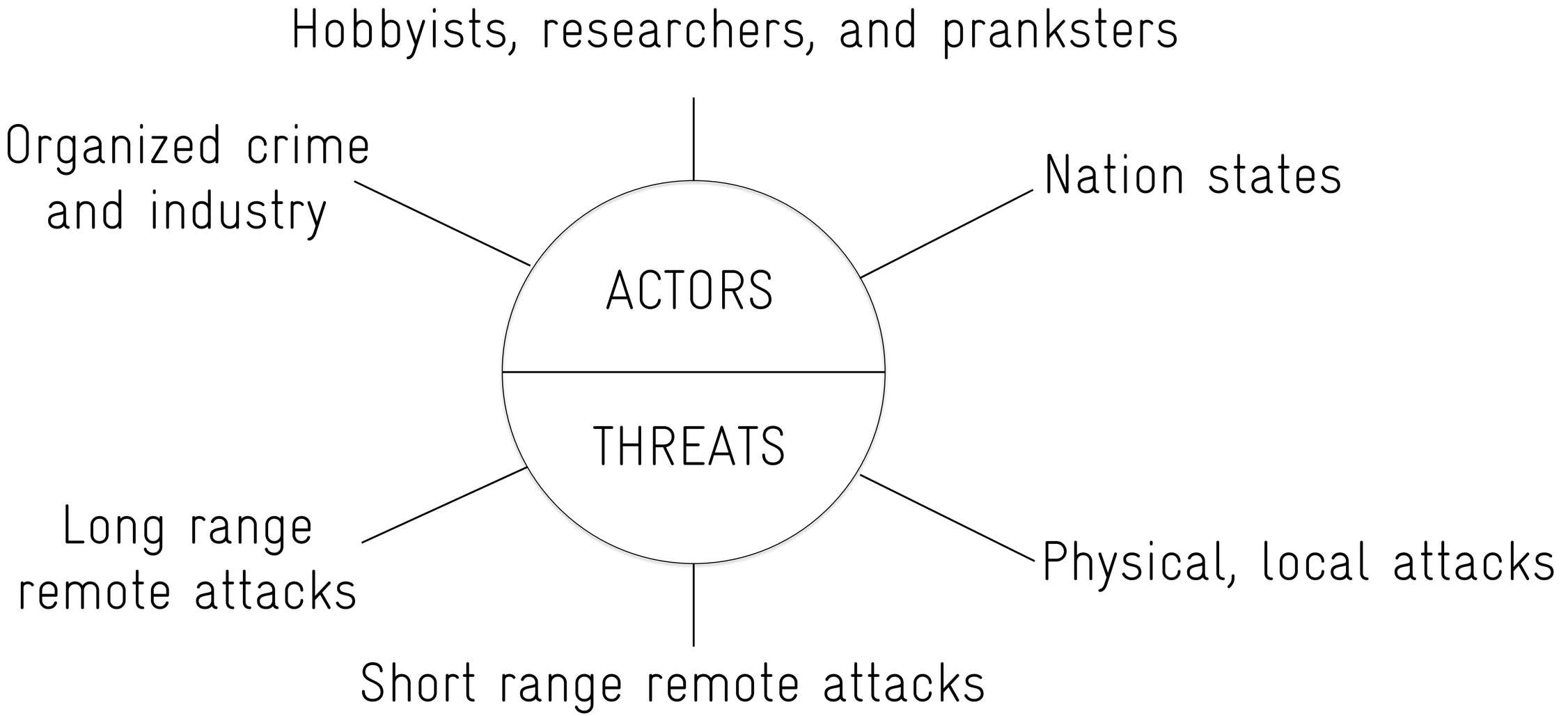
GOOD NEWS: CYBERSECURITY IS A SOLVED PROBLEM

BAD NEWS: IT DOES NOT SOLVE ITSELF

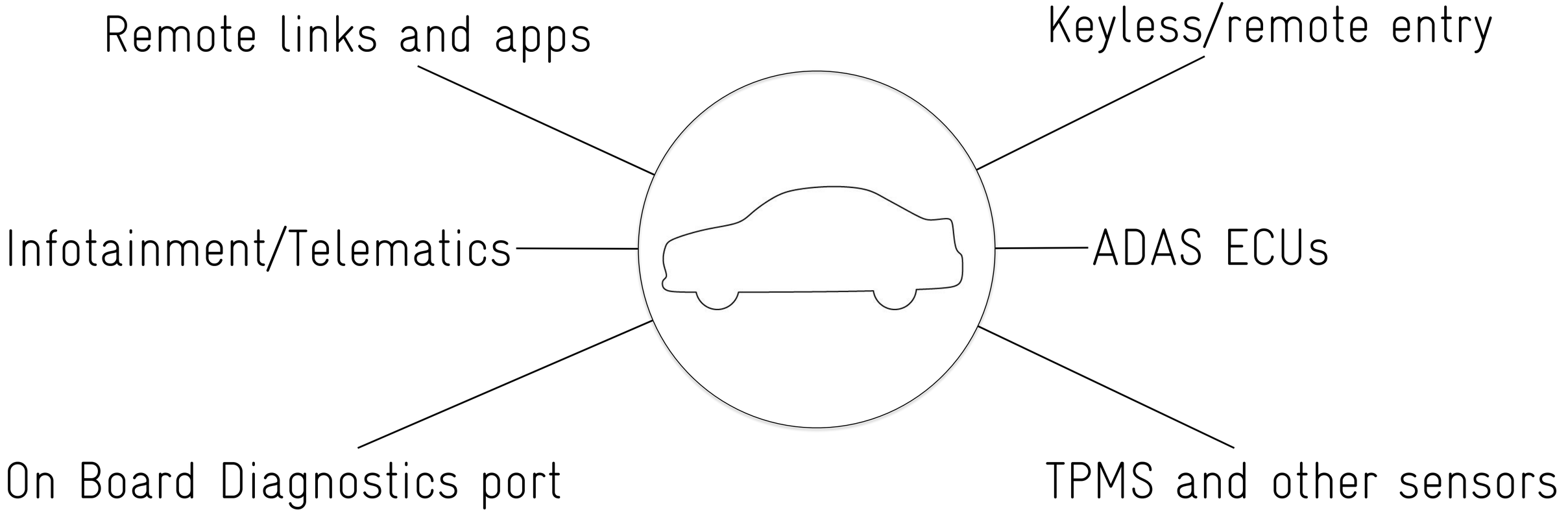
WHY CYBERSECURITY?

- Loss of safety
- Denial of service
- Theft
- IP protection
- Privacy and surveillance

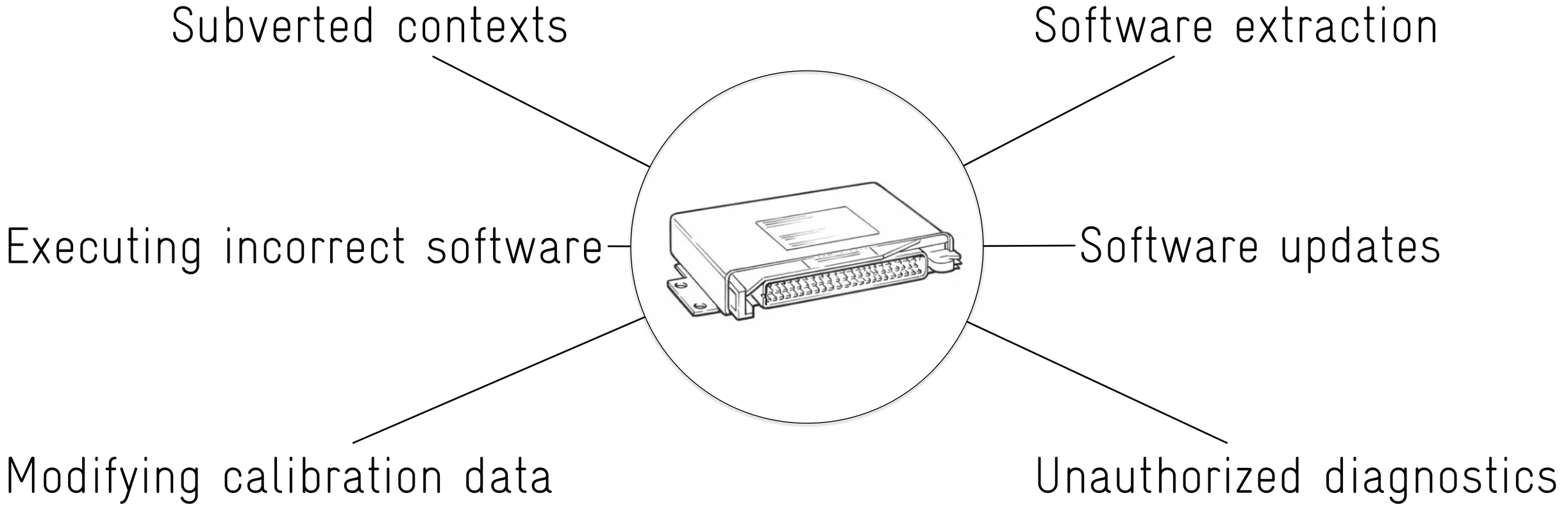
THREAT ACTORS AND THREATS



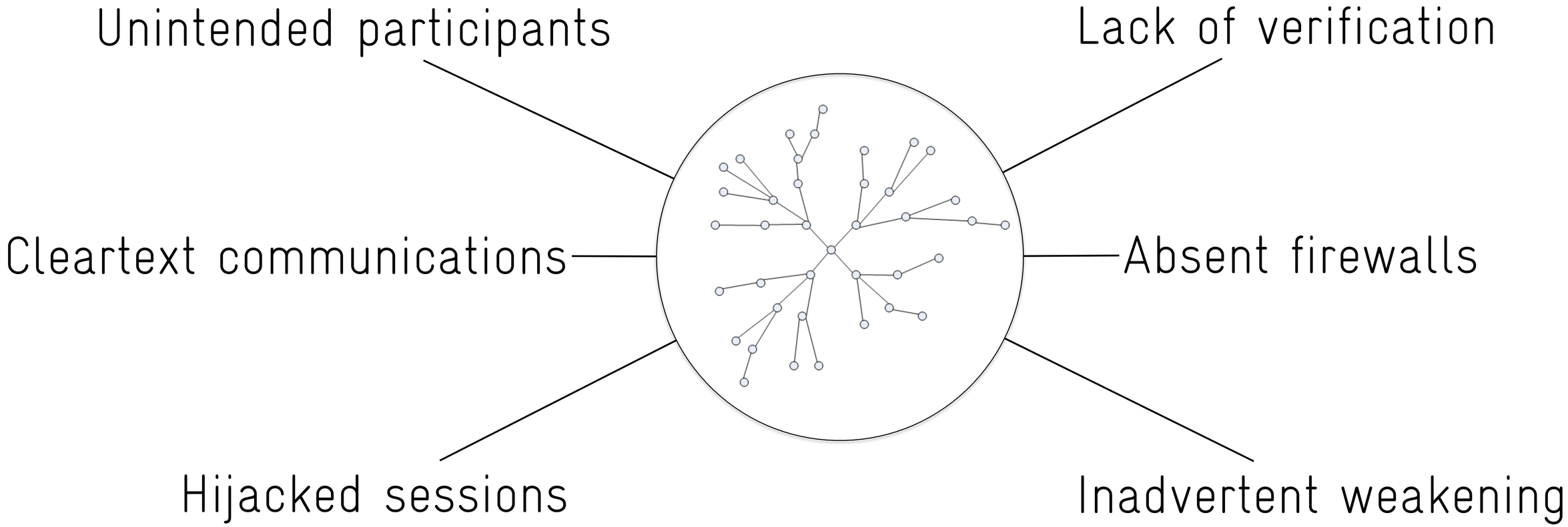
COMMON ATTACK SURFACES



HOW ECUS GET COMPROMISED



HOW NETWORKS GET COMPROMISED



A CRYPTOGRAPY PRIMER

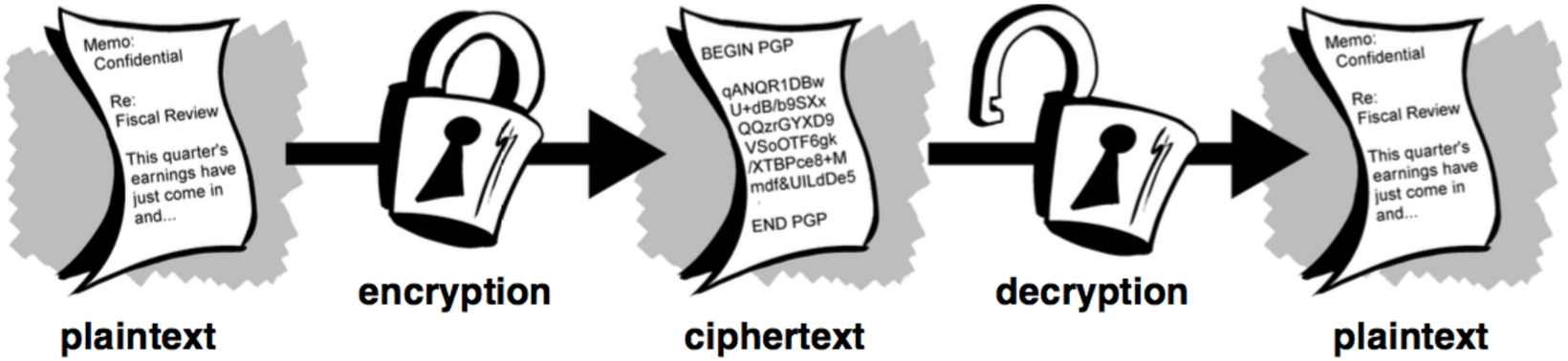


Image source: An Introduction to Cryptography. PGPi documentation.

SYMMETRIC KEY CRYPTOGRAPHY

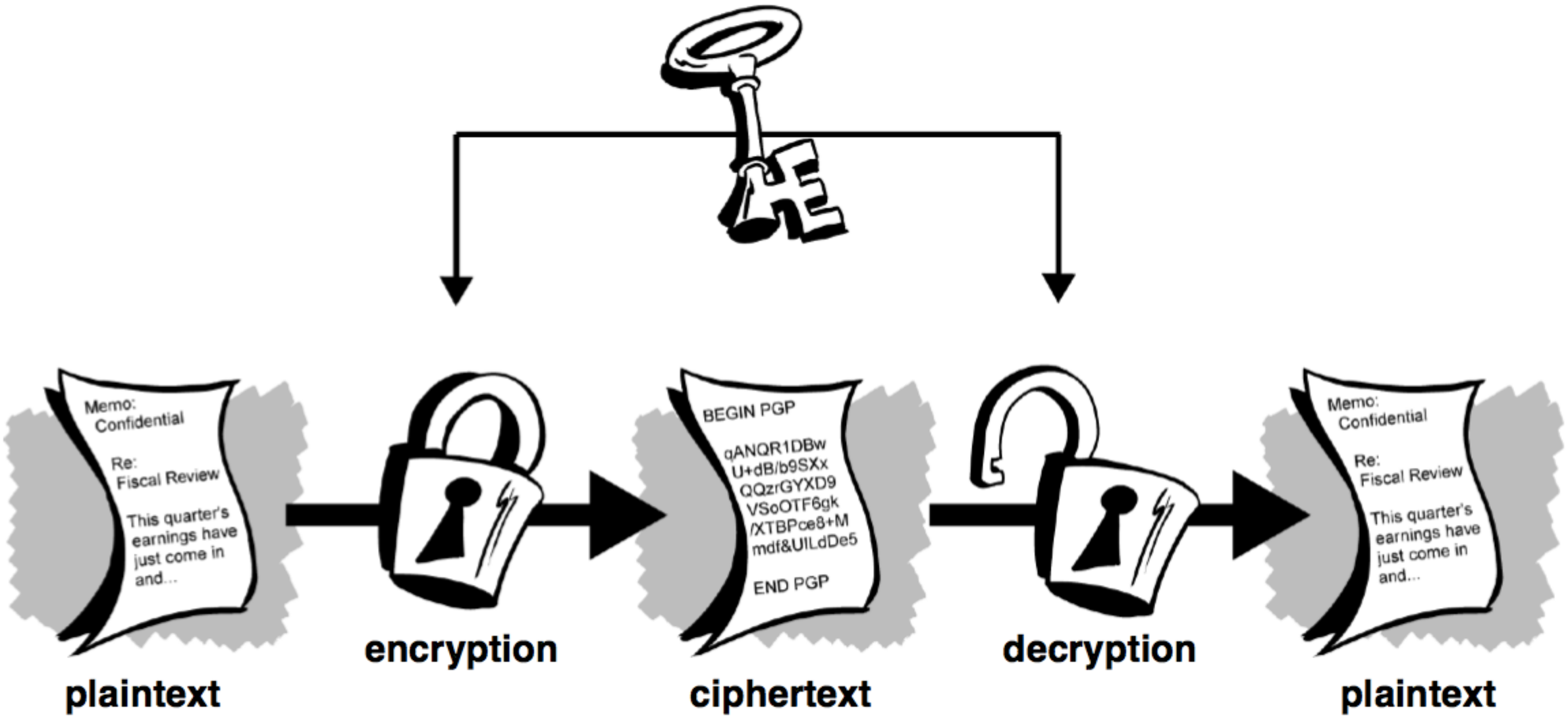


Image source: An Introduction to Cryptography. PGPi documentation.

ASYMMETRIC KEY CRYPTOGRAPHY

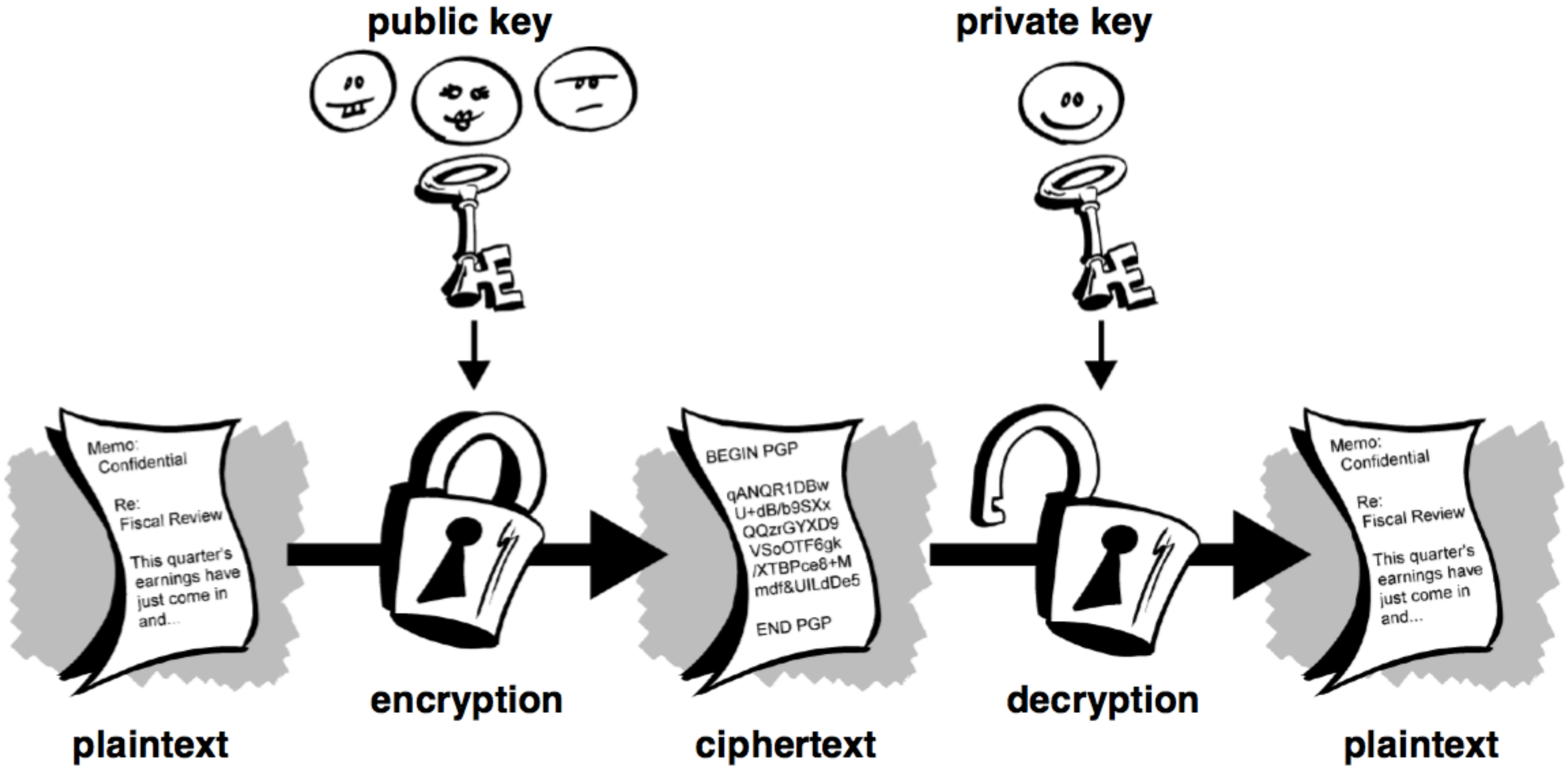


Image source: An Introduction to Cryptography. PGPi documentation.

DIGITAL SIGNATURES

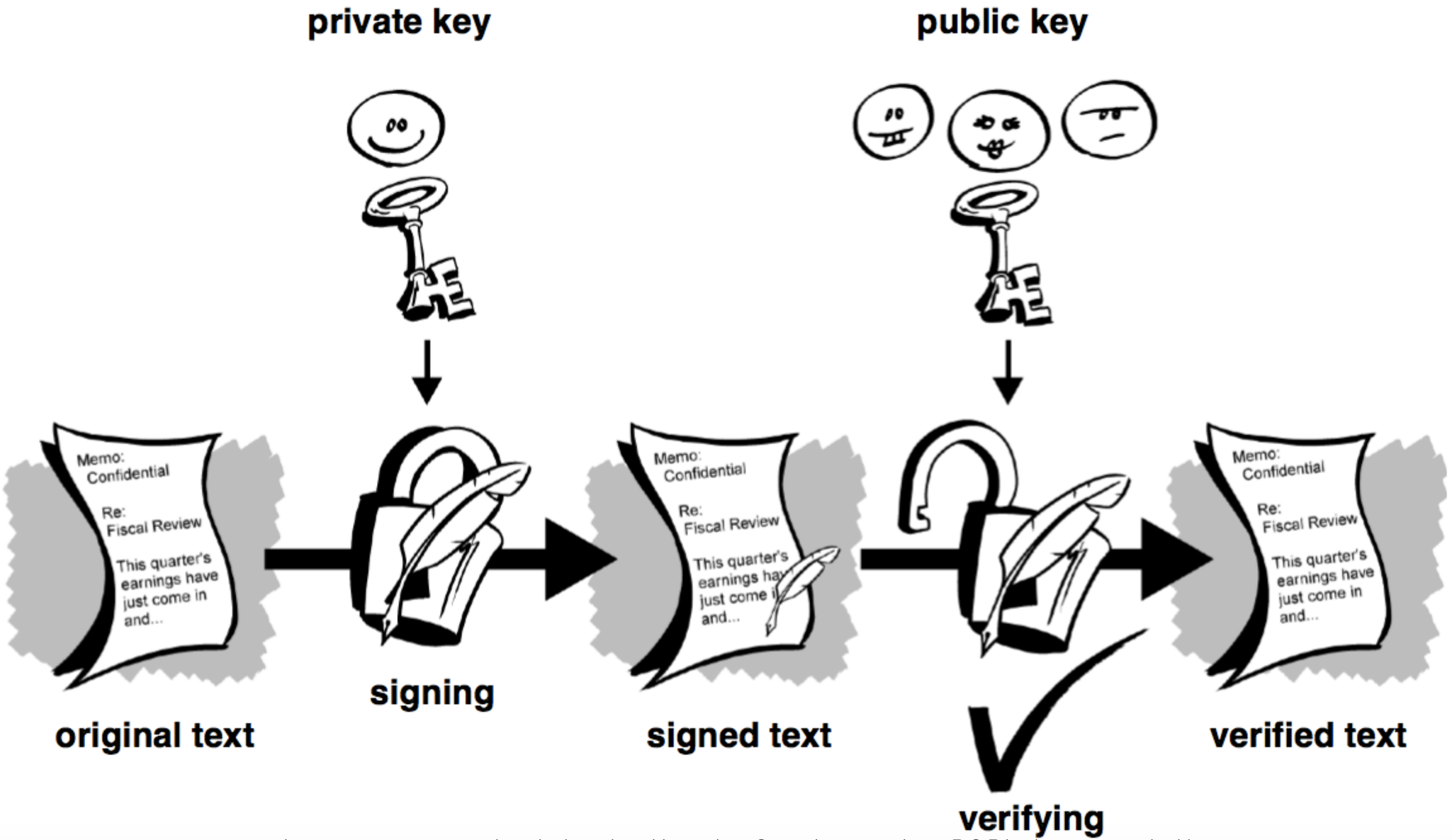


Image source: An Introduction to Cryptography. PGPi documentation.

HASH FUNCTIONS

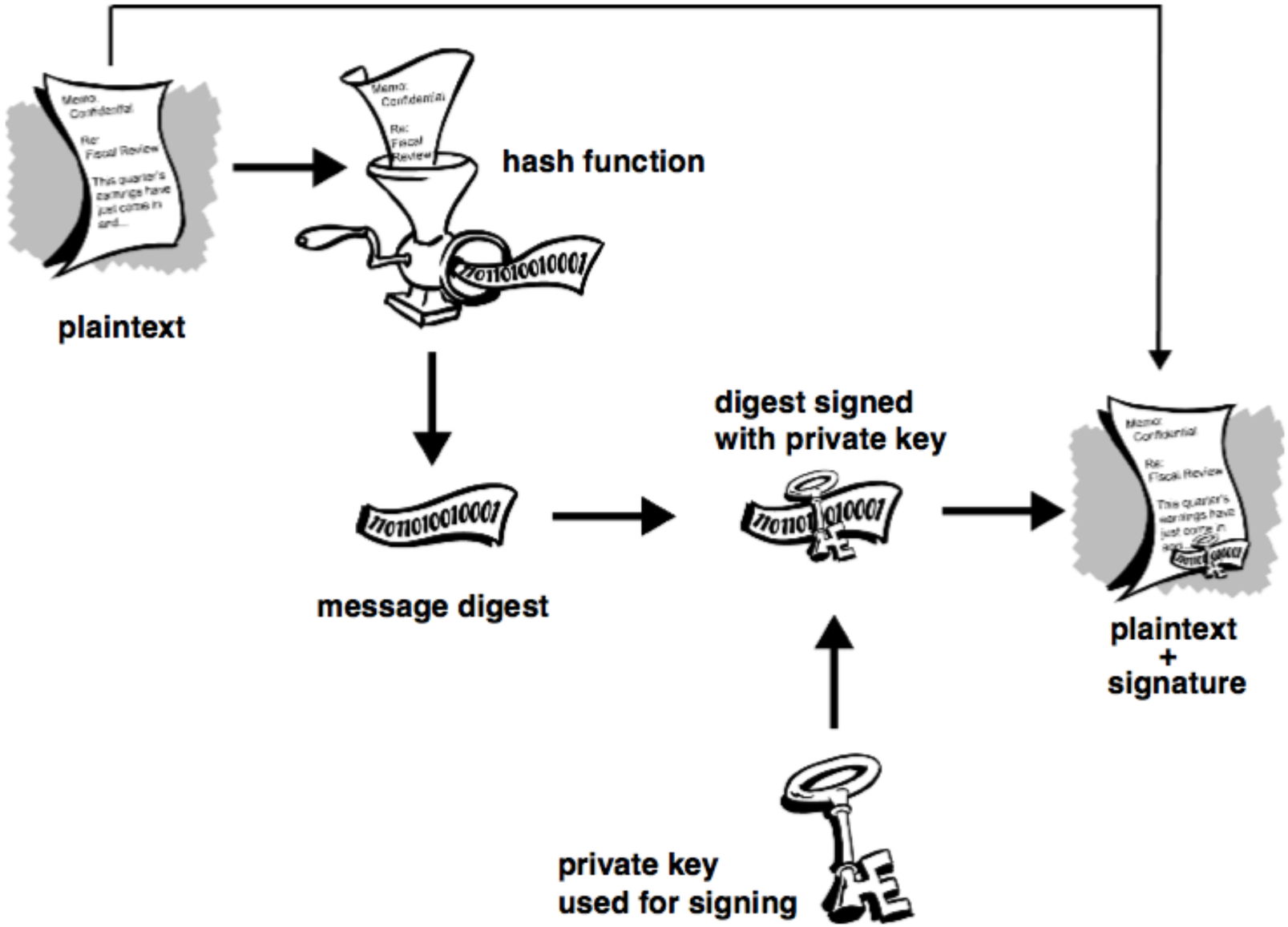
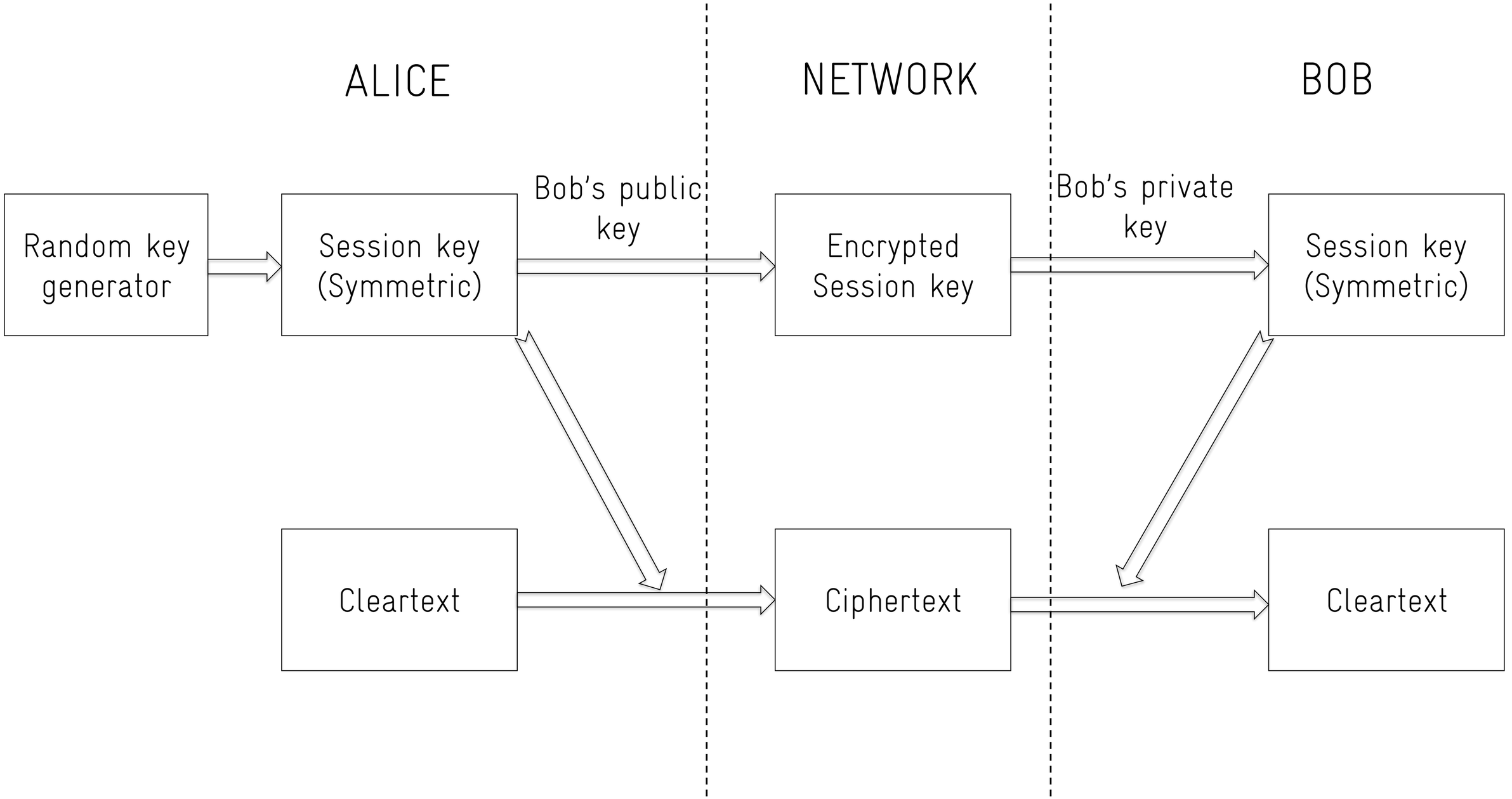
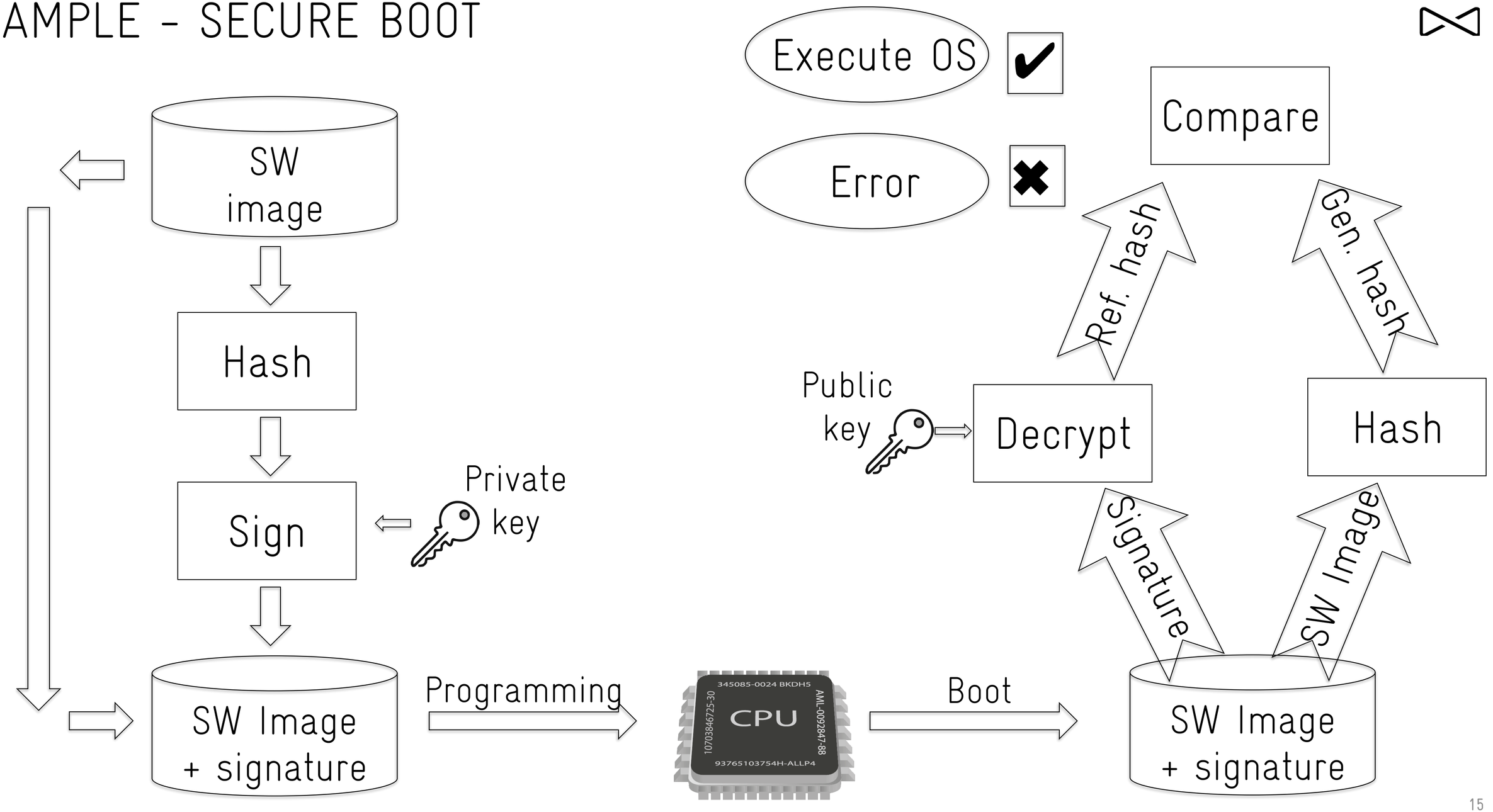


Image source: An Introduction to Cryptography. PGPi documentation.

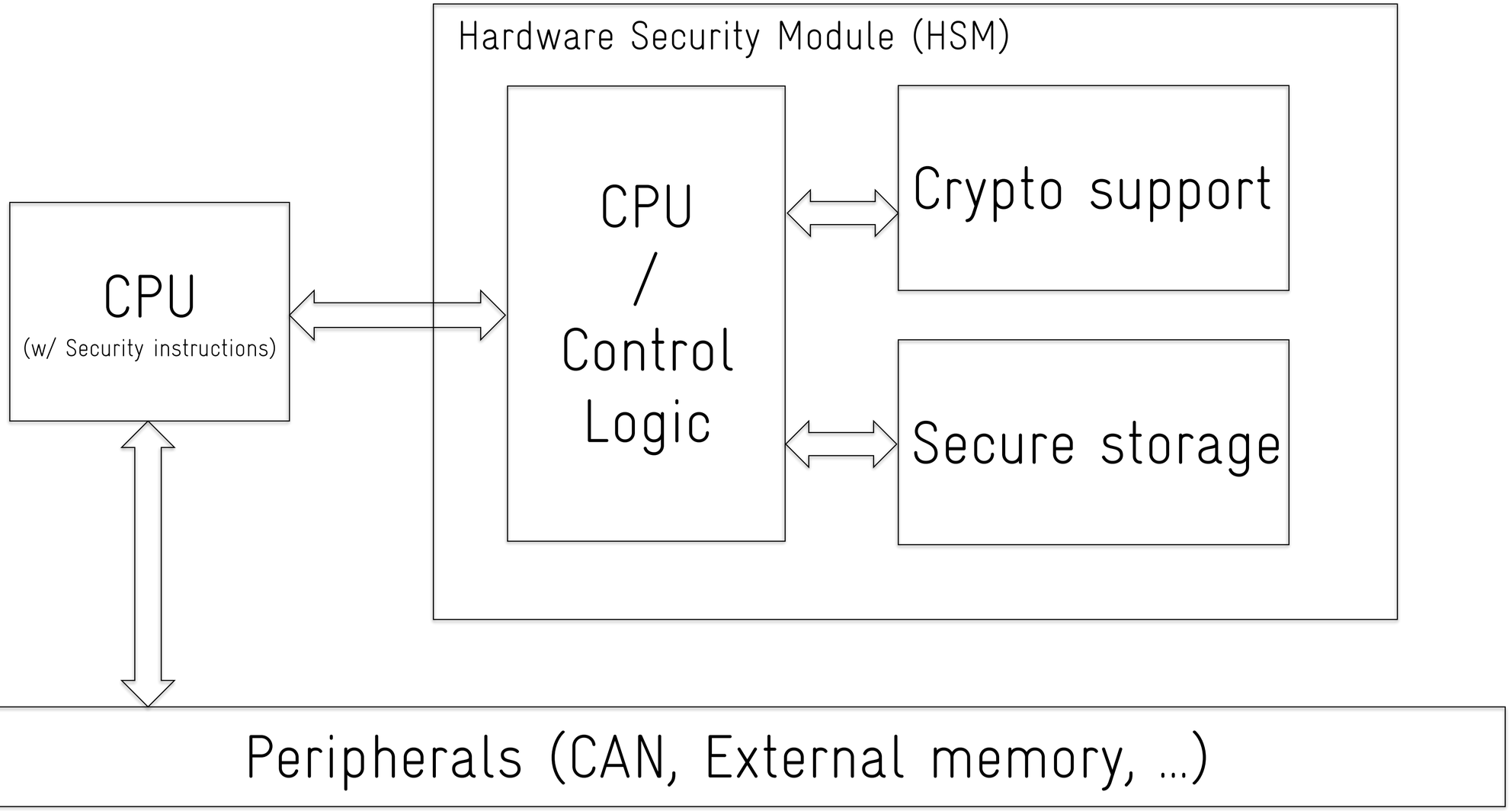
HYBRID CRYPTOSYSTEMS



EXAMPLE - SECURE BOOT



CRYPTOGRAPHY IN AUTOMOTIVE PRACTICE

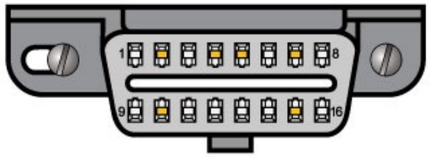


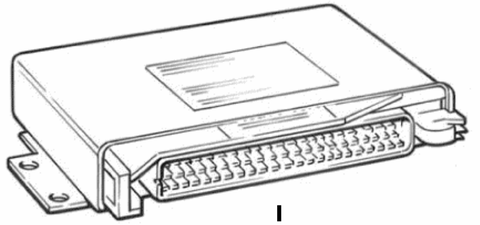
HARDWARE SECURITY MODULES

HSM / Feature	EVITA full	EVITA medium	EVITA light	HIS SHE	TCG TPM/MTM	Usual smartcard
Bootstrap integrity protection	Authentic and/or secure	Authentic and/or secure	Authentic and/or secure	Secure	Authentic	None
HW crypto algorithms (incl. key generation)	ECDSA,ECDH, AES/MAC, WHIRLPOOL/ HMAC	ECDSA,ECDH, AES/MAC, WHIRLPOOL/ HMAC	AES/MAC	AES/MAC	RSA, SHA-1/ HMAC	ECC, RSA, AES, 3DES, SHA-x & more possible (but seldom in parallel on chip)
HW crypto acceleration	ECC,AES, WHIRLPOOL (FPGA/ASIC)	AES (ASIC)	AES (ASIC)	AES (ASIC)	None	None
Internal CPU	Reprogrammable firmware & hardware (FPGA)	Reprogrammable firmware	None	None	Preset	Reprogrammable firmware
RNG	TRNG	TRNG	PRNG w/ external seed	PRNG w/ external seed	TRNG	TRNG

Source: Next Generation of Automotive Security: Secure Hardware and Secure Open Platforms. OVERSEE Project

SEED KEY PROTOCOL





SecurityAccess request

seed s

Compute key k

Compute key k'

key k

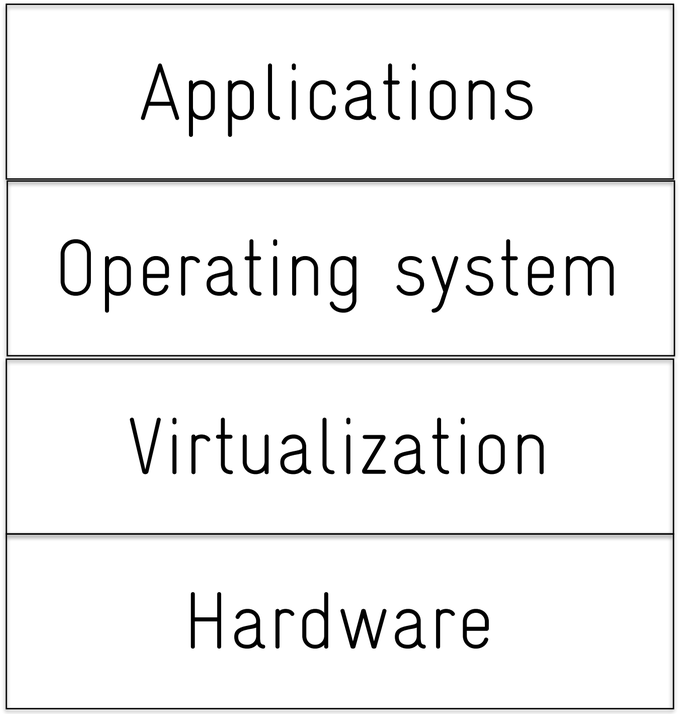
Verify k=k'

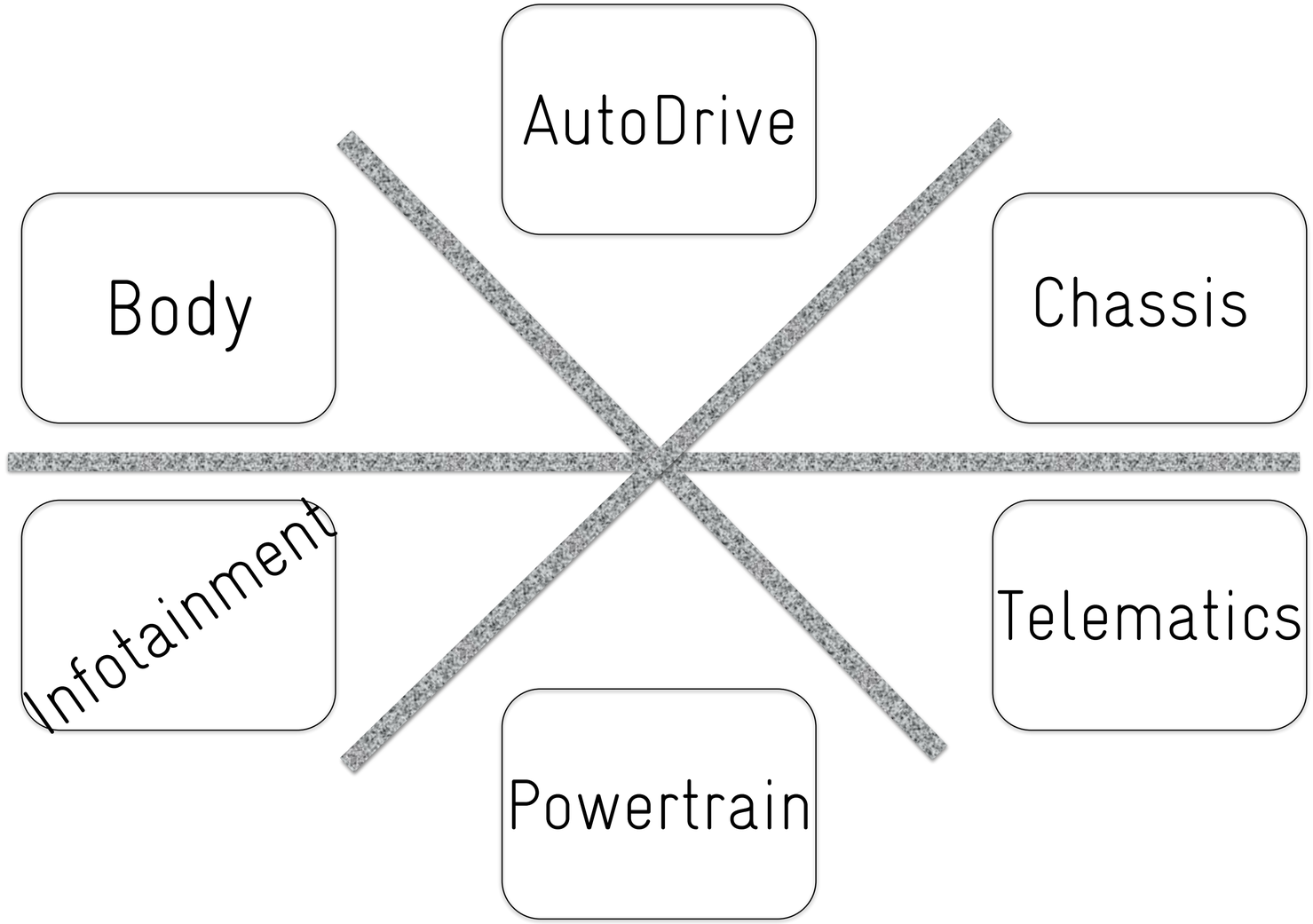
SecurityAccess response

Source: OBD = Open Barn Door? Security Vulnerabilities and Protections for Vehicular On-Board Diagnosis (OBD)


ENCRYPT
ALL THE THINGS
memegenerator.net

LAYERING AND PARTITIONING

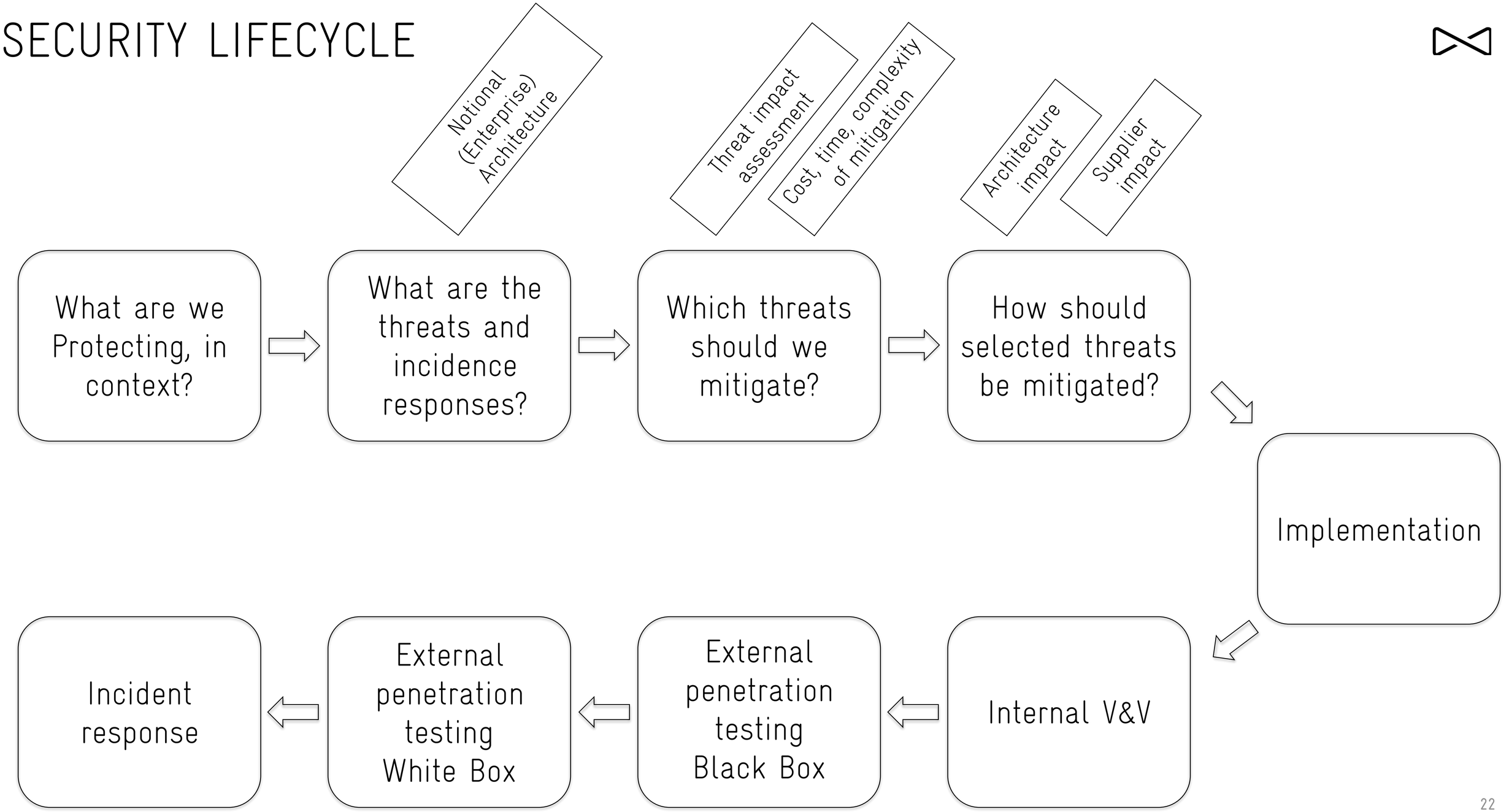




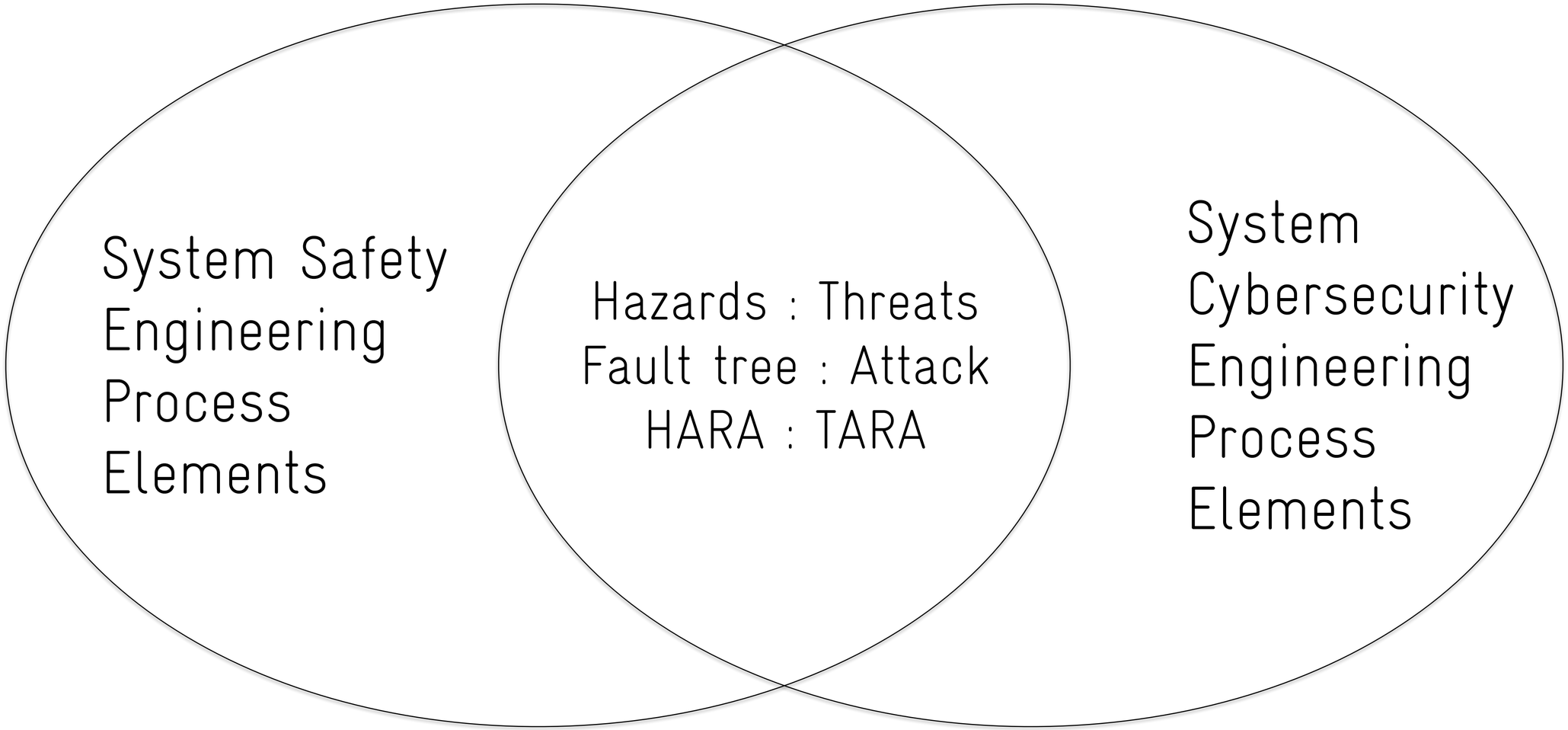
OPERATIONAL CYBERSECURITY MONITORING

- Intrusion Detection and Prevention System (IDPS)
- Independent network node(s) and SW modules in critical ECU(s)
- Monitors network traffic and ECU behavior in real-time
- Heuristics for determination of abnormal operation

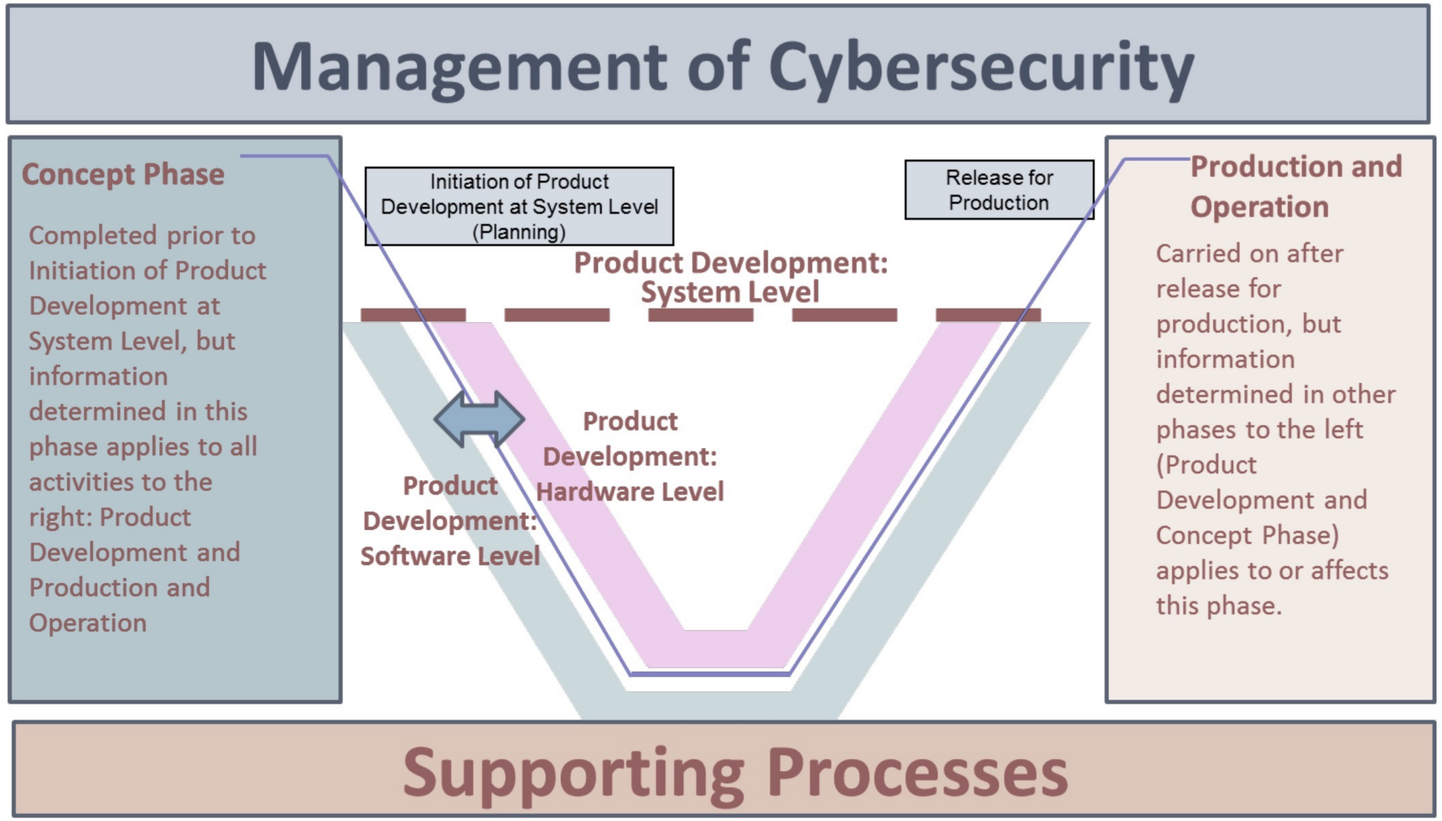
SECURITY LIFECYCLE

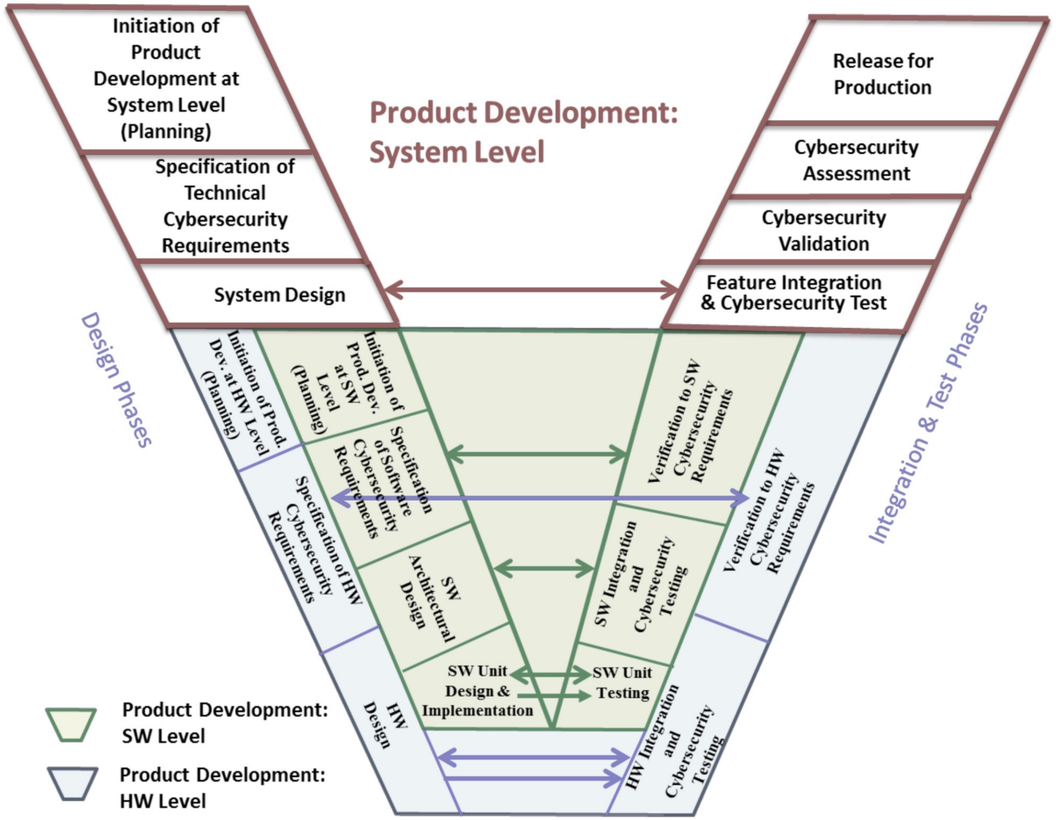


SAE J3061: SAFETY AND SECURITY

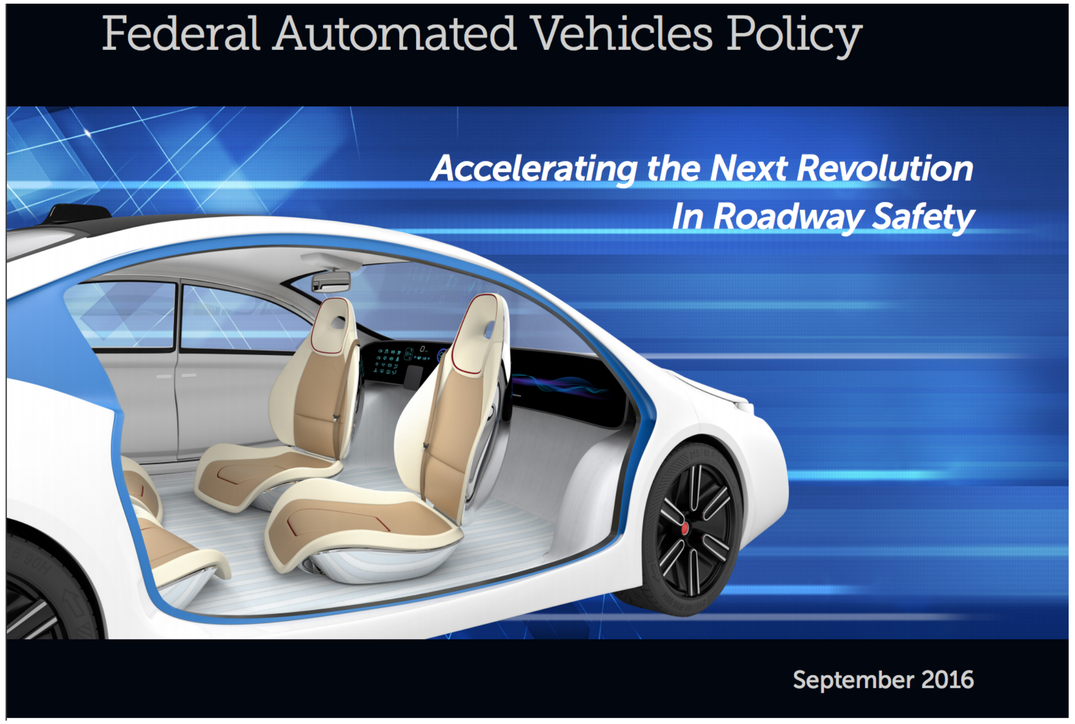


SAE J3061: PROCESS FRAMEWORK

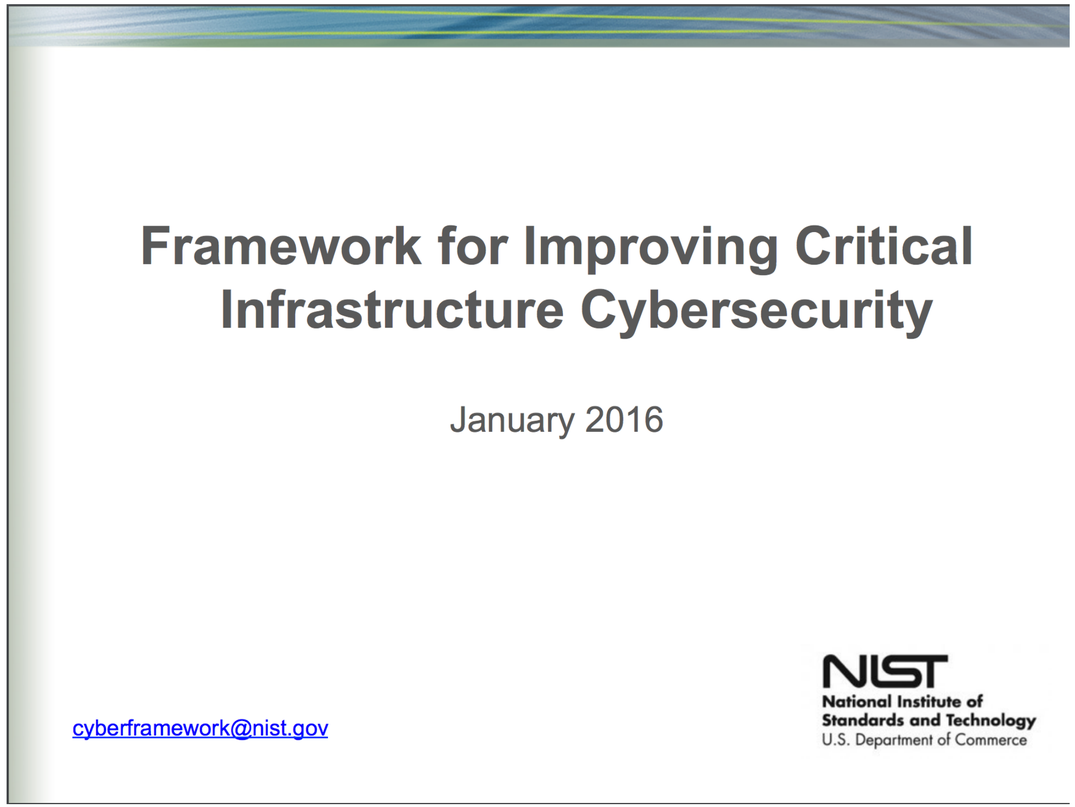


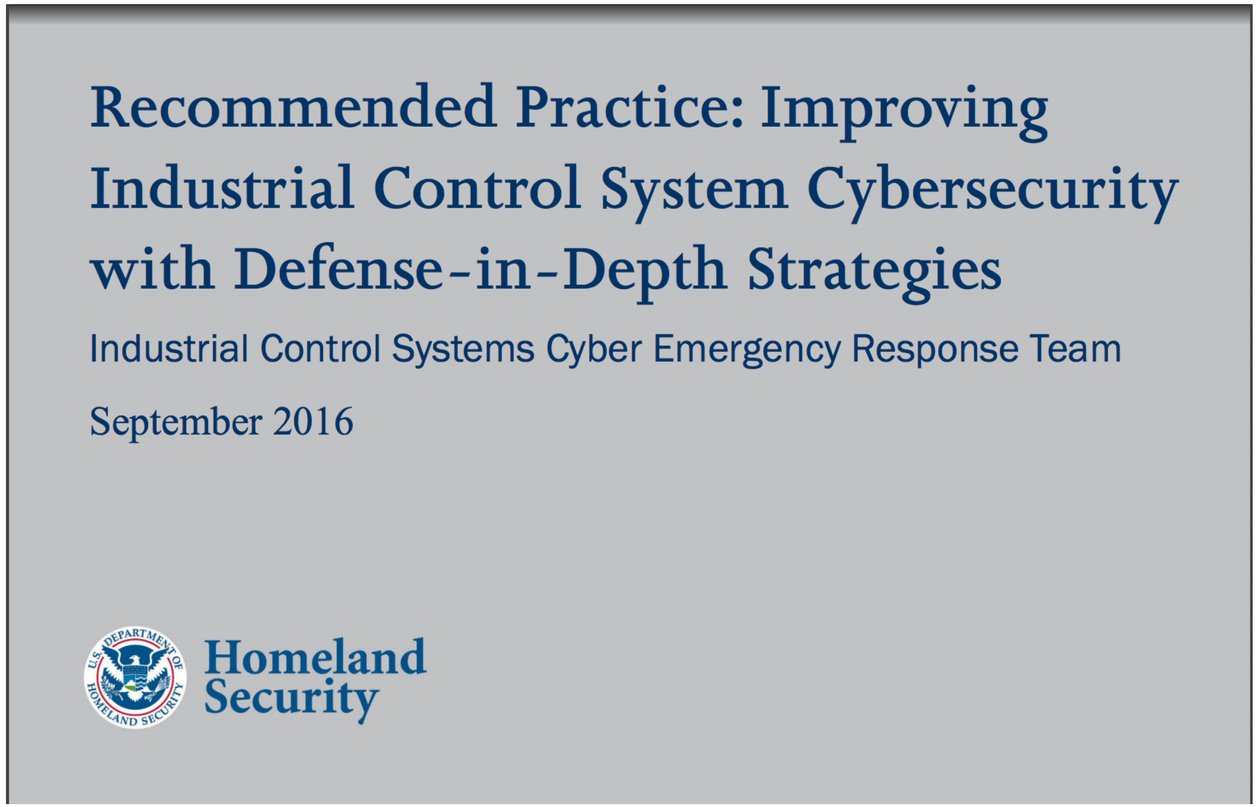


NHTSA GUIDANCE ON CYBERSECURITY



NIST AND DHS


Framework for Improving Critical Infrastructure Cybersecurity
January 2016
cyberframework@nist.gov
NIST
National Institute of Standards and Technology
U.S. Department of Commerce


Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
Industrial Control Systems Cyber Emergency Response Team
September 2016
Homeland Security

OTHER STANDARDS AND GUIDELINES

- ISO/IEC 9797-1: Security techniques – Message Authentication Codes
- ISO/IEC 11889: Trusted Platform Module
- ISO 12207: Systems and software engineering – Software lifecycle processes
- ISO 15408: Evaluation criteria for IT Security
- ISO 27001: Information security management system
- ISO 27002: Code of practice – Security
- ISO 27018: Code of practice – Handling PII / SPI (Privacy)
- ISO 27034: Application security techniques
- ISO 29101: Privacy architecture framework
- ISO 29119: Software testing standard
- IEC 62443: Industrial network and system security

INTERESTING HACKS

THE 80/20 OF AUTOMOTIVE CYBERSECURITY

- Communications with off-board systems MUST be cryptographically encrypted and signed
- ECUs should ONLY execute cryptographically signed and authenticated software
- “Larger” operating systems, like Linux, MUST be secured using techniques learned from Enterprise IT
- Gateways should provide strong partitioning and firewalls

OBVIOUS REMINDERS

- Security is a framework, not an add-on
- Security through obscurity DOES.NOT.WORK
- Do not “home brew” cryptography
- Do not half-bake security – If it is worth doing, it is worth overdoing

GOOD NEWS: CYBERSECURITY IS A SOLVED PROBLEM

BAD NEWS: IT DOES NOT SOLVE ITSELF

QUESTIONS?