Embedded Security Step-by-Step

Ron Keidar

Security Architect & Sr. FAE

Inside Secure

rkeidar@insidesecure.com

D&R IP-SOC DAYS Conference 2018

April 5th, 2018 – Santa Clara

D&R IP-SOC DAYS

inside secure
DRIVING TRUST

INSIDE Secure at a Glance

- Over **25 years of experience** and expertise in advanced security
- **600 patents** and patent applications
- Publicly Traded - **Euronext:INSD**
- Solutions protect more than **two billion products**
- Security is not an add-on, we are **100% security company!**

inside secure
DRIVING TRUST

INSIDE Secure at a Glance

Silicon IPs

Security IP Cores

- 600Gbps+ Cryptos
- Packet Engines
- Root-of-Trust Engine
- Public Key Engines
- FIPS 140-2
- Camouflage Tech
- Key Provisioning

SYPHERMEDIA INTERNATIONAL

Data & communication

Embedded Security Software

- TLS and DTLS
- IPsec, MACsec
- Secure Boot
- FIPS 140-2 Crypto Lib
- VPN, Data at Rest

Application protection

App Protection and Payment

- Mobile Payment
- eWallet
- Healthcare apps
- Car Key Apps
- Multi-factor authentication

mepin

Content protection

Content Protection

- DRMs Leadership:
  - ➢ OTT CE devices
  - ➢ Mobile embedded
  - ➢ Downloadable DRMs
- HDCP and DTCP stacks
- Studio-Approved

Supporting World Top Companies

Silicon IPs

Security IP Cores

Major Semiconductor Companies

BROADCOM.

QUALCOMM

intel

MStar semiconductor

TEXAS INSTRUMENTS

Data & communication

Embedded Security Software

Top IT Companies

SAMSUNG

htc

ASUS

hp

cisco

Application protection

App Protection and Payment

Banks and payment systems

CHASE

Santander

mastercard.

VISA

Content protection

Content Protection

Content distributors

HBO

Virgin media

at&t U-verse

orange

sky

amazon

Before We Go any further
Few Announcements:

1. Inside Secure introduce
   its Root-of-Trust Family
   Programmable Root-of-Trust core

RISC-V

2. Inside Secure Acquired SypherMedia
   Offering:
   - ➢ Largest 3rd Party Key Provisioning System
   - ➢ Silicon Camouflage

SMI
SYPHERMEDIA
INTERNATIONAL

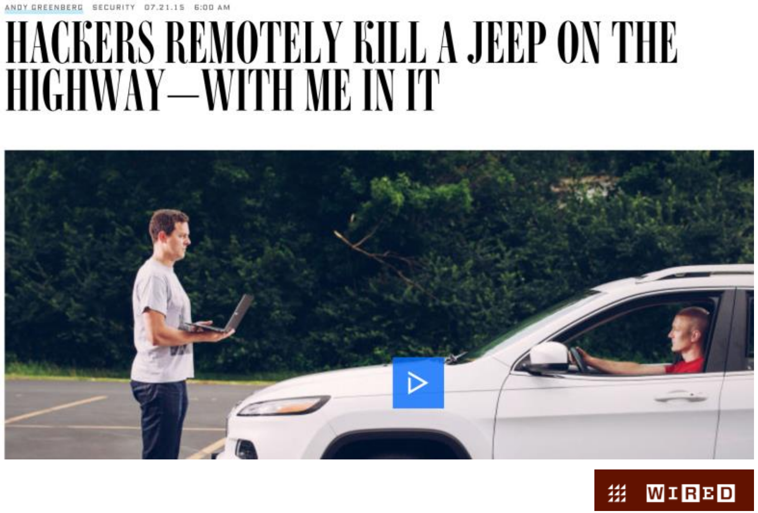
Solutions for Automotive Market

ECU solutions	Telematic Solutions	Infotainment Solutions	V2X Solutions	Mobile Application
Root-of-Trust Embedded HSM	E-Wallet & Payment	Root-of-Trust Secure Boot	V2V Public Key Engine	Application protection
Secure Boot Image encryption	FIPS Crypto Lib	HDCP SW and HW	IPsec, TLS/DTLS SW Toolkit	E-Wallet & Payment
MACsec IP Core	Root-of-Trust Secure Boot	Embedded DRM	Root-of-Trust Embedded HSM	VPN
	IPsec, TLS, DTLS, 3GPP VPNs		IPsec, TLS, DTLS, 3GPP IP Core	

Check it out on https://www.insidesecure.com/Markets/Automotive

Hacking Jeep – Case Study

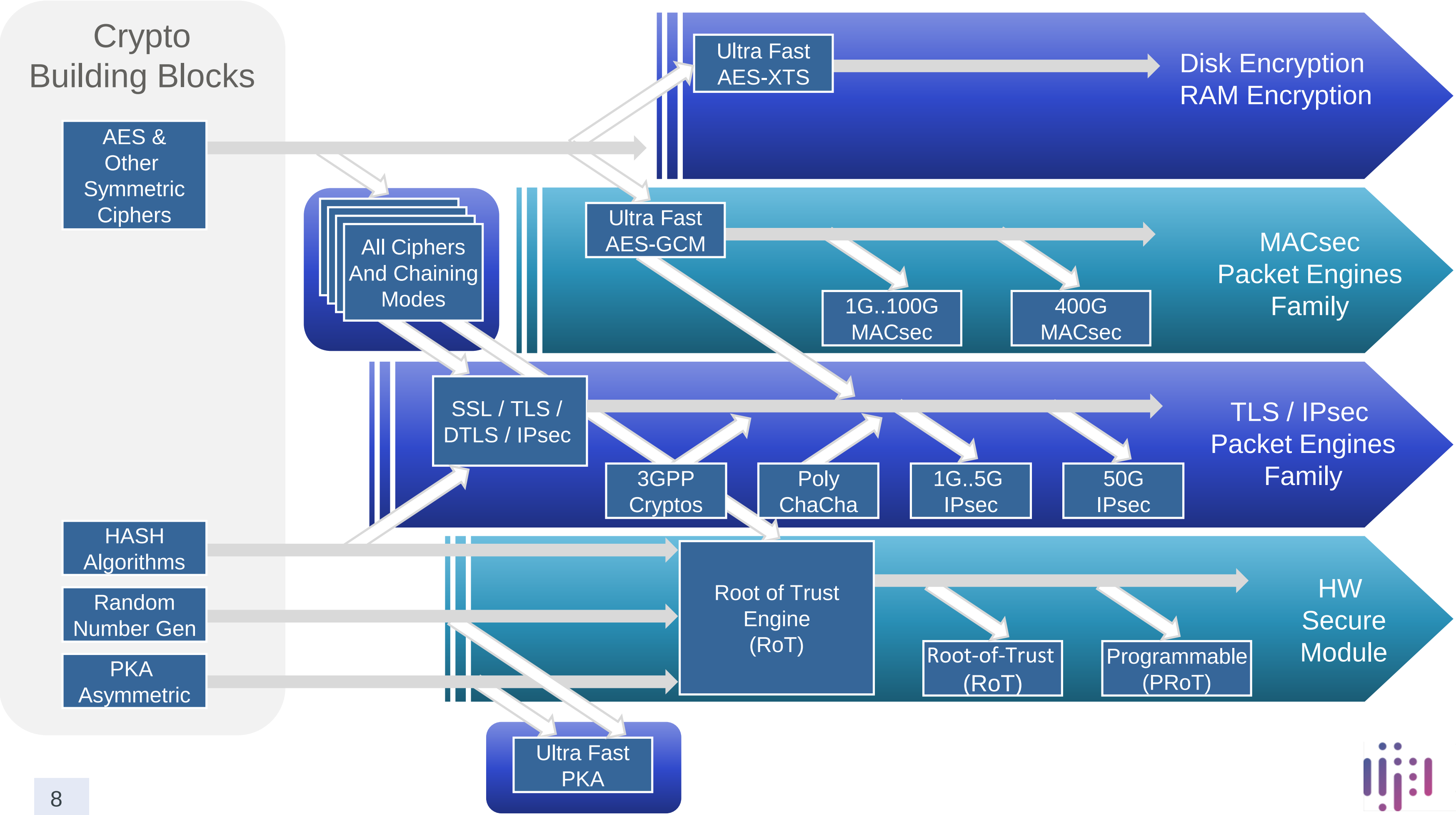
Problem	Think about it
Jeep Cherokee	Your IoT just the same
Open telnet port No authentication	Close ports or Enforce SSH auth
Bad random password	Use HW TRNG
FW Image analyzed	Use Image Encryption
FW Image modified	Use Secure Boot
CAN Bus allows full control to any sender	Use protocol with mutual-authentication
No OTA FW Upgrade	1.4M thumb drives sent to customers



ANDY GREENBERG SECURITY 07.21.15 6:00 AM

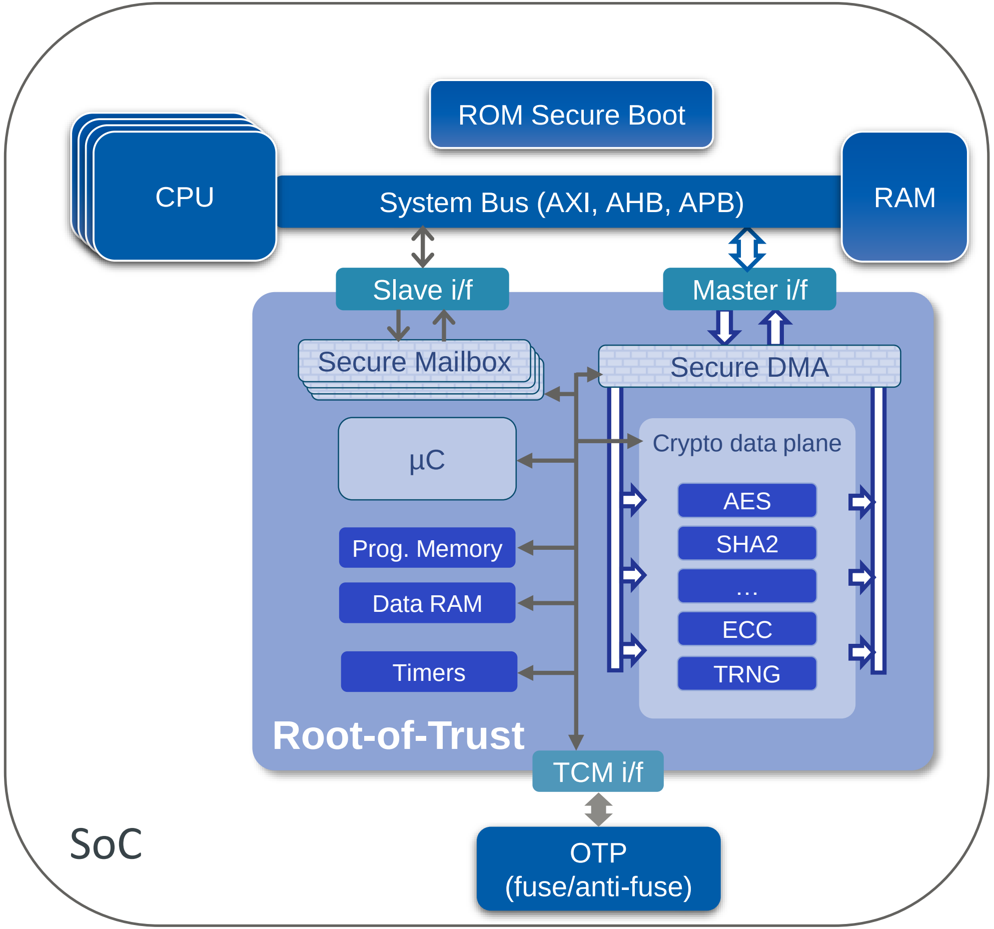
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Inside Secure IP Cores Portfolio (more than 500 configurations)



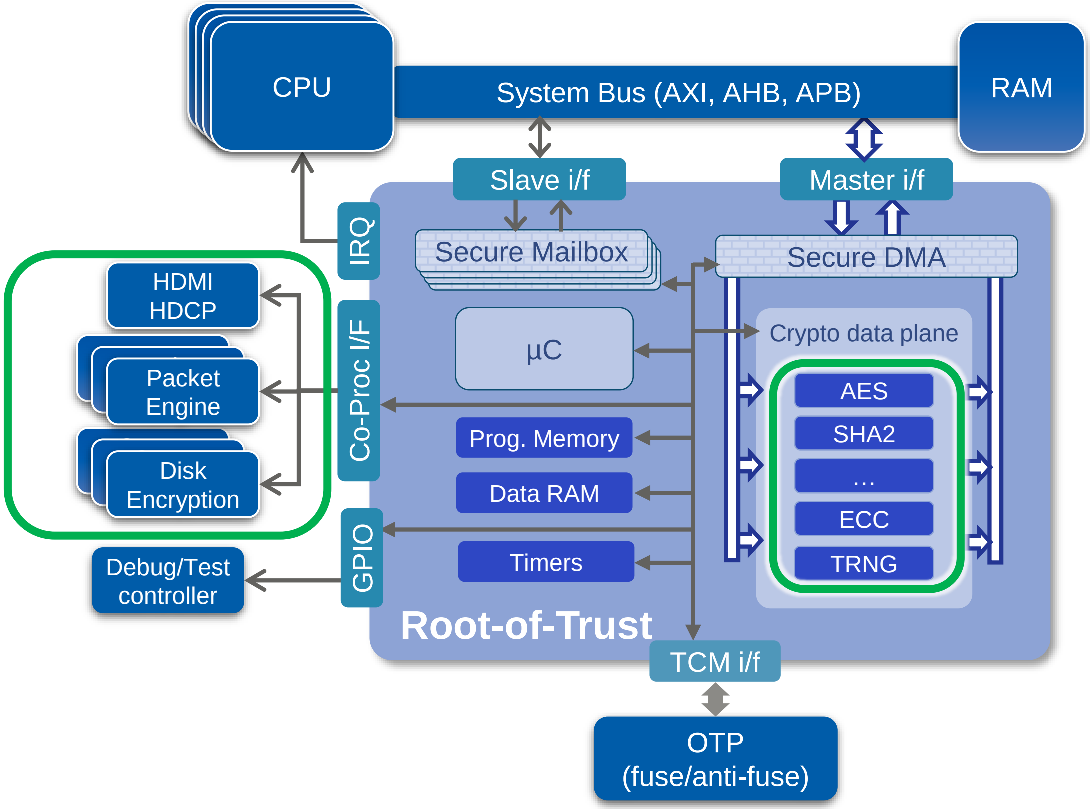
inside secure

Embedding Security Step by Step



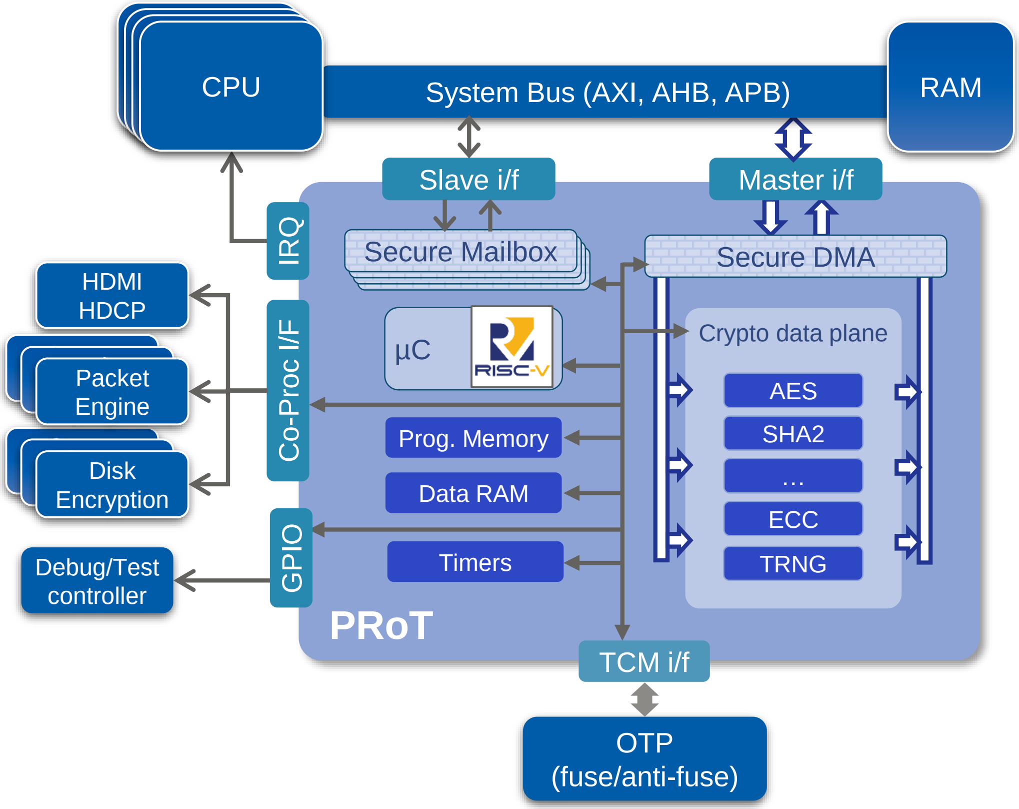
- Secure Boot
- SHA2 → Integrity
- ECC (Elliptic-Curve)→ Authentication
- OTP (One Time Programmable)
  - Immutable keys and state
- AES → Confidentiality
- Micro-Controller for flexibility
- Isolation of internal address space using Mailboxes
- TRNG and other CryptoEngines
- Integrate everything into IP Core

Root-of-Trust Swiss Army Knife



- FIPS-140-2 level 2 certified
- Secure Boot
- Side Channel Protection
- Anti Tampering
- HW Protection for keys
  - Even if Kernel/HV/TEE breached
  - Anti Cloning
- Scalable Crypto Accelerators
  - Internal and External
- Secure debug enablement
- Built-in Key Provisioning
- Life-cycle management

Programmable Root-of-Trust

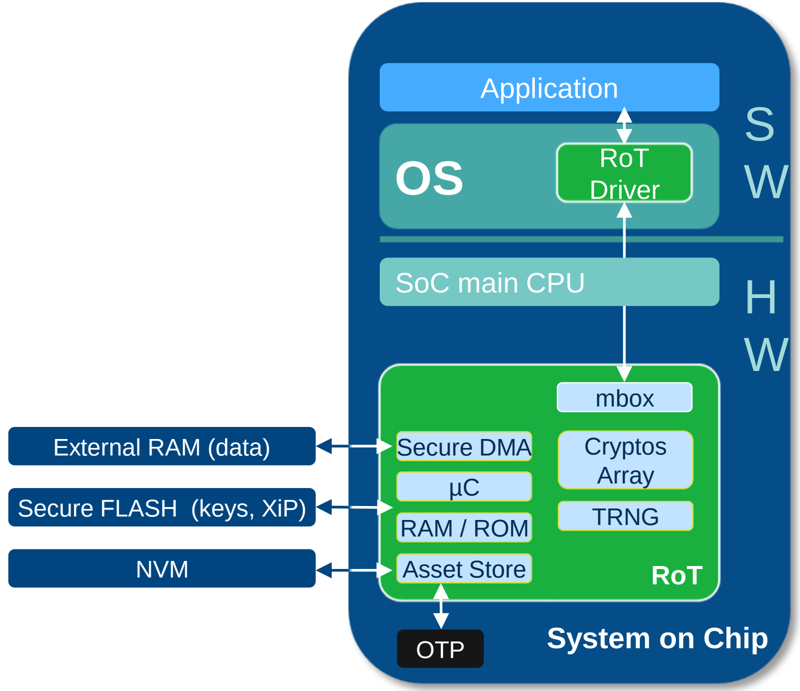


- Addition of Risc-V core to the secure perimeter
- Enables OEM to
  - Develop proprietary code
  - In-field SW upgrade
  - Manage Secure Boot
  - Terminate TLS inside the PRoT and support TLS Device Authentication
- Standard toolchain
- Potential enhancement with Secure flash for
  - Secure Element profile
  - Evita Full profile

RoT Scales Across your Portfolio

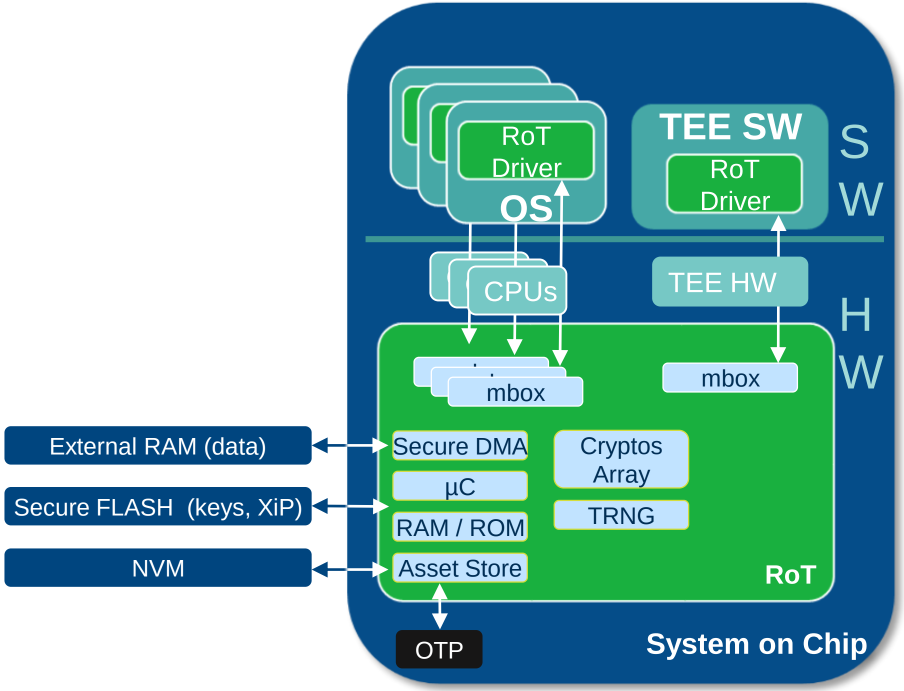
SoC without TEE

e.g. Micro controllers



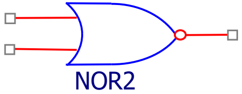
SoC with TEE and multiple CPUs

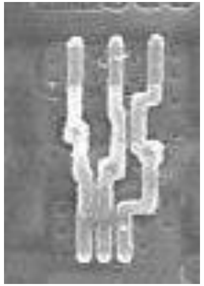
e.g. Mobile phones



Cell Camouflage

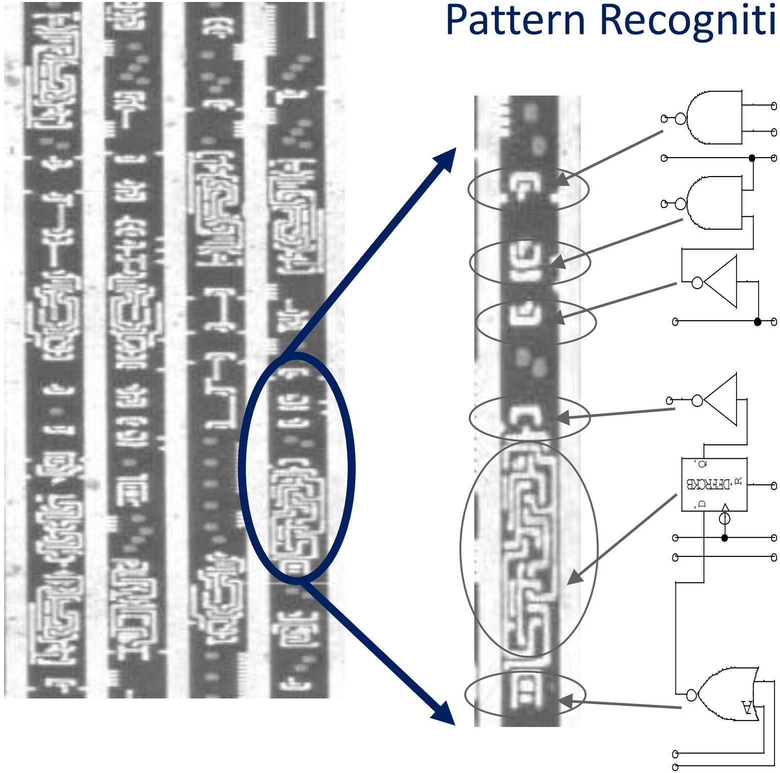
Conventional NOR2



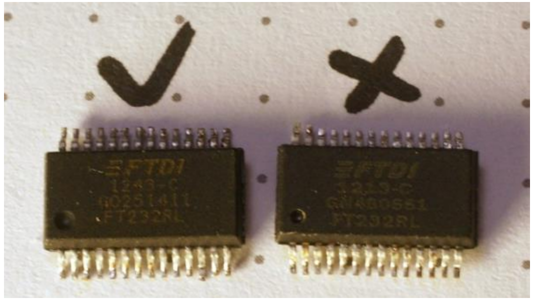


Conventional NAND3

Reverse Engineering using Pattern Recognition



Layout → Netlist



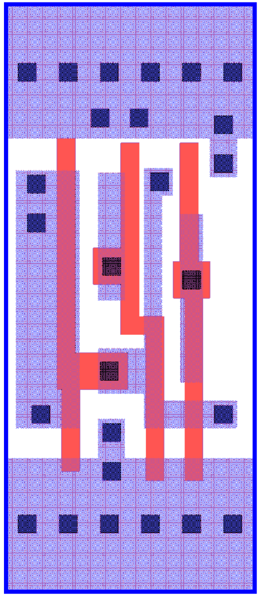
Identical Counterfeit,
at lower quality and price:

1. Consume market share
2. Damage Brand
3. Lower margin
4. Support and recalls

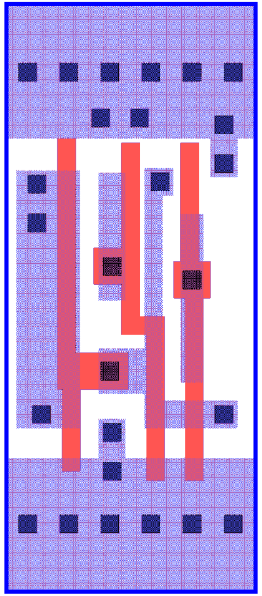
Foundry Standard Cells vs Camo Cells

Camo cells are designed to appear as foundry cells, but perform different logical functions

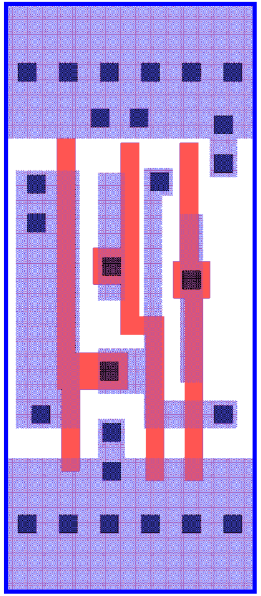
Foundry Standard AND2 Gate



Inside Secure Ver1 Camo Gate

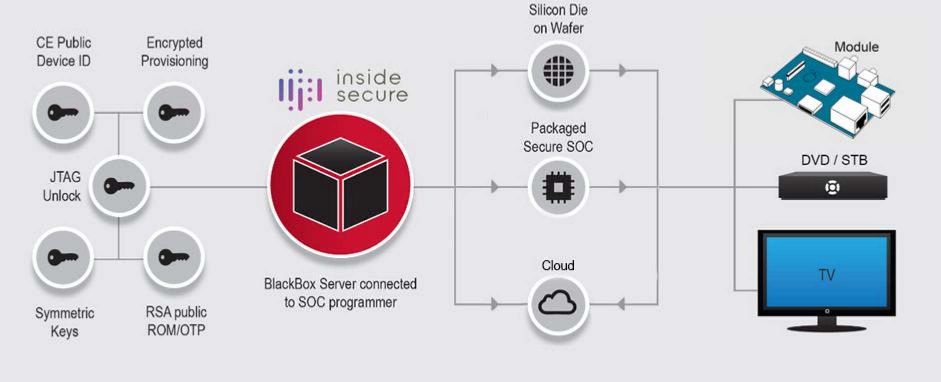


Inside Secure Ver2 Camo Gate



AND2 lookalike gates perform alternate functions

BlackBox Key Provisioning Overview

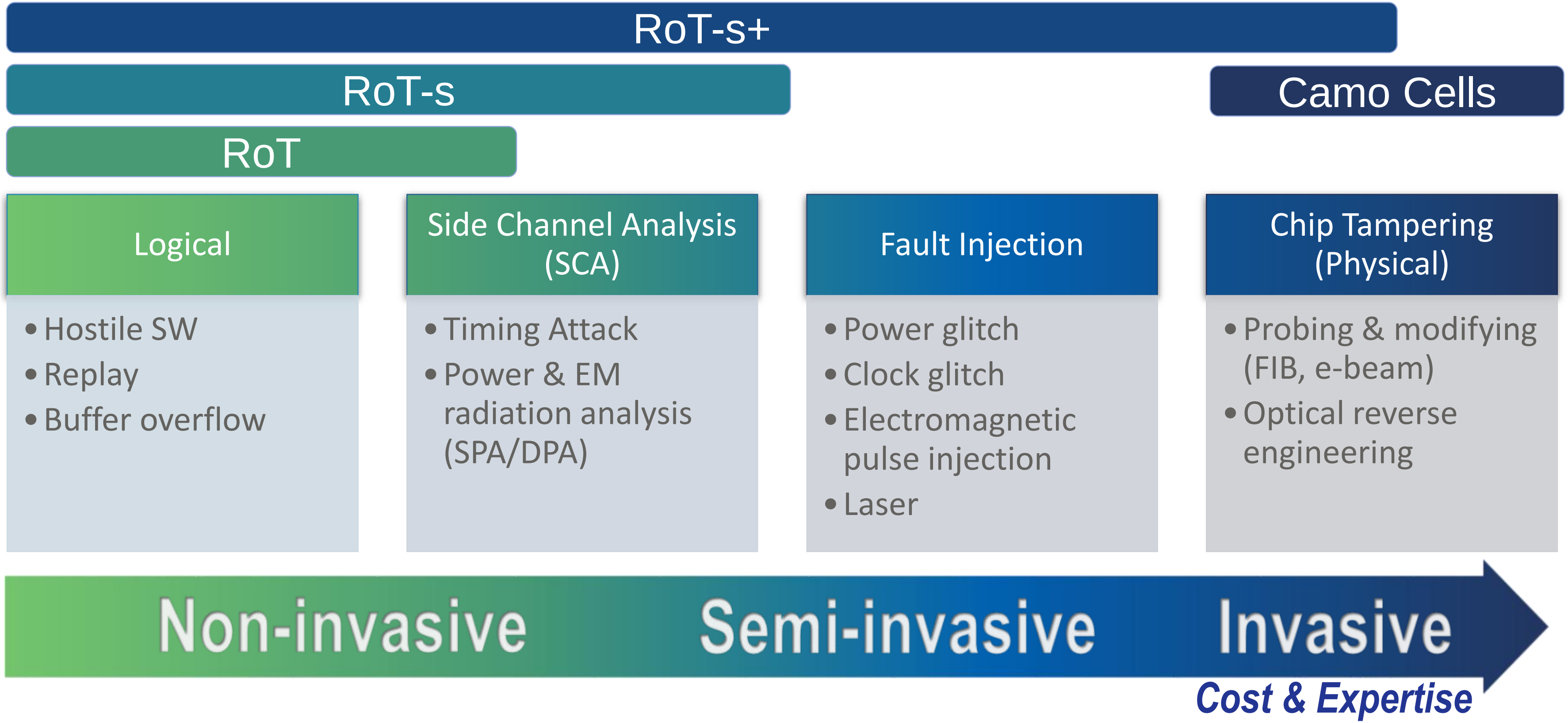


- Provisioning at Silicon stage, OEM stage and On-boarding stage
- Largest 3rd Party Key Provisioning with more that 60 OEMs
- And 13 leading SoC Vendors

ALi
BROADCOM.
HISILICON
intel
NationalChip
MAXLINEAR
MONTAGE Technology
MStar semiconductor
NOVATEK
socionext
SIGMA DESIGNS
ST
ViXS

ABS CBN
ADB
A DTH
amino
dishtv
CRYPTOGRAPHY RESEARCH a division of Rambus
CryptoGuard
BANG & OLUFSEN
EXSET
FORTIS
KATHREIN
LOEWE.
infomir im
INTERNATIONAL DATACASTING
RSCRYPTO
verimatrix Beyond Content Protection to Revenue Security
WOX
wyplay

Attack Landscape & RoT



RoT-s+

RoT-s

Camo Cells

RoT

Logical

- Hostile SW
- Replay
- Buffer overflow

Side Channel Analysis (SCA)

- Timing Attack
- Power & EM radiation analysis (SPA/DPA)

Fault Injection

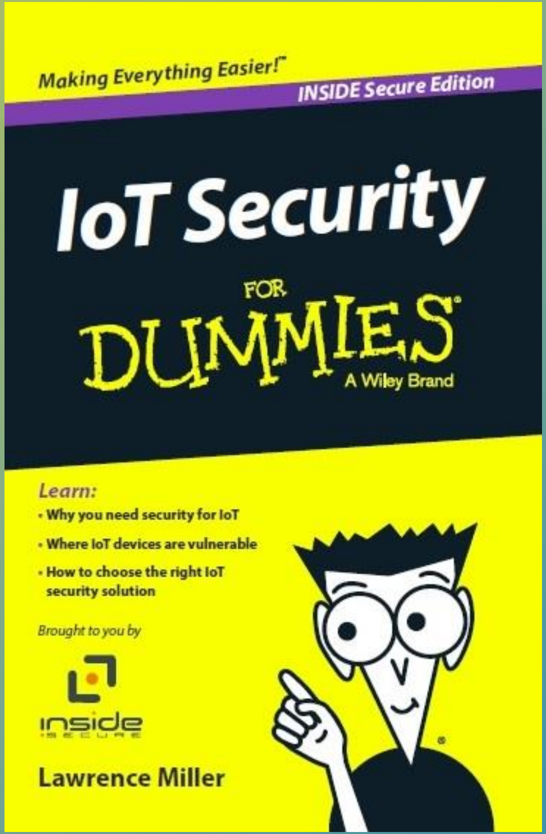
- Power glitch
- Clock glitch
- Electromagnetic pulse injection
- Laser

Chip Tampering (Physical)

- Probing & modifying (FIB, e-beam)
- Optical reverse engineering

Non-invasive Semi-invasive Invasive

Cost & Expertise



Making Everything Easier!™

INSIDE Secure Edition

IoT Security

FOR DUMMIES®

A Wiley Brand

Learn:

- Why you need security for IoT
- Where IoT devices are vulnerable
- How to choose the right IoT security solution

Brought to you by

inside SECURE

Lawrence Miller

Thank You!

Ron Keidar

rkeidar@insidesecure.com

Download your free copy of

IoT Security for Dummies

By INSIDE Secure Download