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
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 at a Glance

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

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

**App Protection and Payment**
- Mobile Payment
- eWallet
- Healthcare apps
- Car Key Apps
- Multi-factor authentication

**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, 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, Orange, Sky, Amazon

- **Content Protection**: Content distributors
  - HBO, Virgin Media, AT&T, Universe, Orange
Before We Go any further Few Announcements:

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

2. Inside Secure Acquired SypherMedia Offering:
   - Largest 3rd Party Key Provisioning System
   - Silicon Camouflage
Solutions for Automotive Market

ECU solutions
- Root-of-Trust Embedded HSM
- Secure Boot Image encryption
- MACsec IP Core

Telematic Solutions
- E-Wallet & Payment
- FIPS Crypto Lib
- Root-of-Trust Secure Boot
- IPsec, TLS, DTLS, 3GPP VPNs

Infotainment Solutions
- Root-of-Trust Secure Boot
- HDCP SW and HW
- Embedded DRM

V2X Solutions
- V2V Public Key Engine
- IPsec, TLS/DTLS SW Toolkit
- Root-of-Trust Embedded HSM
- IPsec, TLS, DTLS, 3GPP IP Core

Mobile Application
- Application protection
- E-Wallet & Payment
- VPN

Check it out on https://www.insidesecure.com/Markets/Automotive
## Hacking Jeep – Case Study

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

Hackers remotely kill a Jeep on the highway — with me in it.
Inside Secure IP Cores Portfolio (more than 500 configurations)

Crypto Building Blocks

- AES & Other Symmetric Ciphers
- Ultra Fast AES
  - XTS
  - GCM
- SSL / TLS / DTLS / IPsec
  - 3GPP Cryptos
  - Poly ChaCha
  - 1G..100G MACsec
  - 400G MACsec
  - 1G..5G IPsec
  - 50G IPsec
- Root of Trust Engine (RoT)
  - Root-of-Trust (RoT)
  - Programmable (PRoT)
- HW Secure Module
- Hash Algorithms
- Random Number Gen
- PKA Asymmetric

RAM Encryption
- Ultra Fast AES
- PKA
- MACsec Packet Engines Family
- 5G IPsec
- 100G MACsec

Disk Encryption
- Ultra Fast AES-XTS
- 400G MACsec
- 50G IPsec

Ultra Fast AES
- 3GPP Cryptos
- Poly ChaCha
- 1G..100G MACsec
- 400G MACsec
- 1G..5G IPsec
- 50G IPsec
- All Ciphers And Chaining Modes

Ultra Fast AES
- GCM
- All Chaining Modes
- All Ciphers And Chaining Modes

Root of Trust Engine (RoT)
- Root-of-Trust (RoT)
- Programmable (PRoT)
- HW Secure Module
- 50G IPsec
- 100G MACsec

All Ciphers And Chaining Modes
- Ultra Fast AES-GCM
- 1G..100G MACsec
- 400G MACsec
- 1G..5G IPsec
- 50G IPsec
- All Ciphers And Chaining Modes
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

**System on Chip**
- **Application**
- **OS**
  - **RoT Driver**
- **SoC main CPU**
- **mbox**
- Secure DMA
- Secure FLASH (keys, XiP)
- RAM / ROM
- Asset Store
- OTP

### SoC with TEE and multiple CPUs
- e.g. Mobile phones

**System on Chip**
- **TEE SW**
  - **RoT Driver**
- **CPUs**
- **mbox**
- Secure DMA
- Secure FLASH (keys, XiP)
- RAM / ROM
- TRNG
- NVM
- Asset Store
- OTP
Cell Camouflage
Reverse Engineering using Pattern Recognition

Conventional NOR2

Conventional NAND3

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 than 60 OEs
- And 13 leading SoC Vendors
Thank You!

Ron Keidar
rkeidar@insidesecure.com

Download your free copy of
IoT Security for Dummies
By INSIDE Secure