Security Solutions for IoT, Storage and Networking

Presented By:

Stephen Wu,

Senior Security IP and Software FAE

D&R IP SOC Day

September 14, 2017

inside secure

Disclaimer

This presentation and the information it contains are not intended to constitute, and should not be construed as an offer to sell or a solicitation to buy or subscribe to any INSIDE Secure securities, in any jurisdiction. Any public offering of INSIDE Secure securities would be made by means of a prospectus previously approved by the AMF that contains detailed information about INSIDE Secure. The disclosure, distribution and publication of this presentation may be restricted by law in certain jurisdictions and persons into whose possession any document or other information referred to herein comes should inform themselves about and comply with any such restrictions. INSIDE Secure takes no responsibility for any violation of any restrictions by any person.

This presentation contains certain forward-looking statements relating to the business of INSIDE Secure, which shall not be considered per se as historical facts, including the ability to manufacture, market, commercialize and achieve market acceptance for specific projects developed by INSIDE Secure, estimates for future performance and estimates regarding anticipated operating losses, future revenues, capital requirements, needs for additional financing. In addition, even if the actual results or development of INSIDE Secure are consistent with the forward-looking statements contained in this press release, those results or developments of INSIDE Secure may not be indicative of their in the future. In some cases, you can identify forward-looking statements by words such as "could," "should," "may," "expects," "anticipates," "believes," "intends," "estimates," "aims," "targets," or similar words. Although the management of INSIDE Secure believes that these forward-looking statements are reasonably made, they are based largely on the current expectations of INSIDE Secure as of the date of this communication and are subject to a number of known and unknown risks and uncertainties and other factors that may cause actual results, performance or achievements to be materially different from any future results, performance or achievement expressed or implied by these forward-looking statements. In particular, the expectations of INSIDE Secure could be affected by, among other things, uncertainties involved in unexpected regulatory actions or delays related notably to building and operating permits and renewable support policies, competition in general or any other risk and uncertainties developed or identified in any public documents filed by INSIDE Secure with the AMF, included those listed in chapter 4 “Risk factors” of the 2014 “document de reference” approved by the French financial market authority (the Autorité des marchés financiers – the “AMF”) on April 30, 2015 under number R.15-030. In light of these risks and uncertainties, there can be no assurance that the forward-looking statements made in this communication will in fact be realized. Notwithstanding the compliance with article 223-1 of the General Regulation of the AMF (the information disclosed must be “accurate, precise and fairly presented“), INSIDE Secure is providing the information in these materials as of this communication, and disclaims any intention or obligation to publicly update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise.

inside secure

Inside Secure at a Glance

shield

Comprehensive package of software protection tools

Greatly simplifies integration of security for mobile apps such as payment HCE, financial, banking, retail, healthcare, and IoT

Application protection

safe

Studios-approved, market leading solution

Allows secure distribution of premium content on all OTT devices

Supports all major DRM schemes, advanced playback functionalities, analytics

Content protection

vault

The largest silicon-proven security IP portfolio for SOC and ASIC designs

For high-speed networking, IoT, datacenters and content protection

Silicon IPs

guard

Secure communication toolkits & cryptographic modules certified with high interoperability and portability

Widely used in security gateways, cloud deployments, smartphones, printers and other IoT devices

Data & communication

inside secure

TRUSTED BY THE WORLD'S TOP COMPANIES

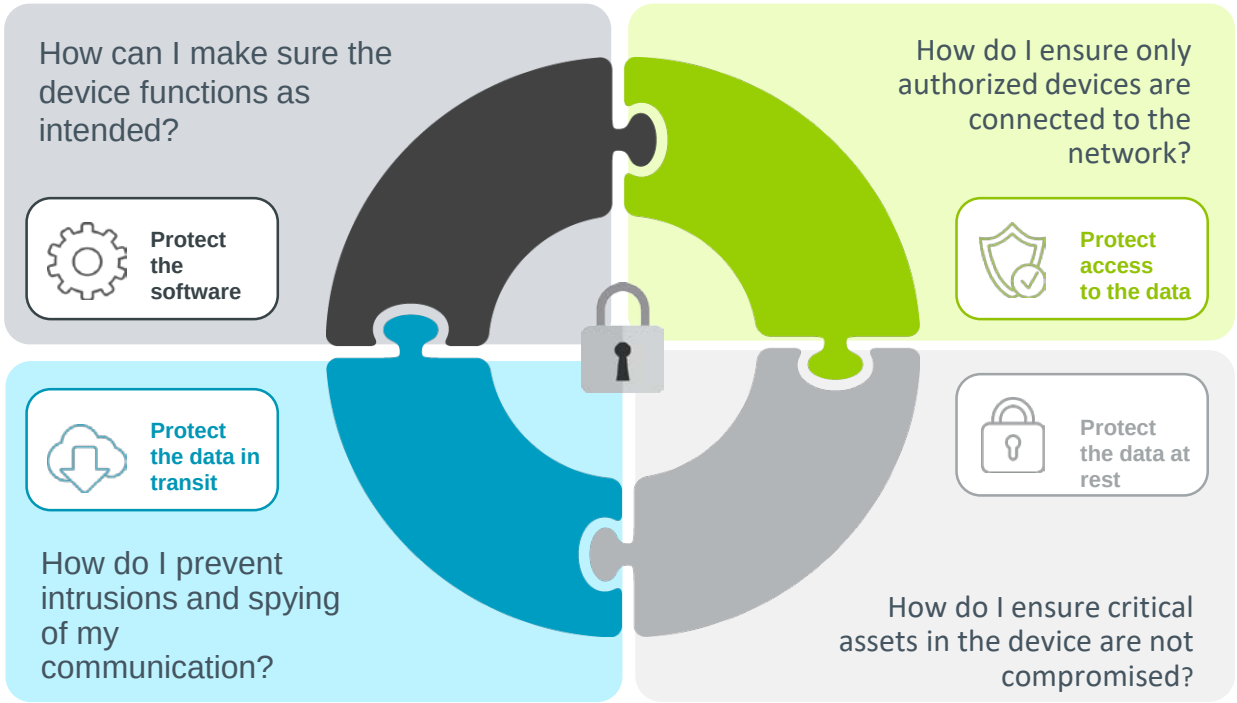
Banks and payment system	   
Content distributor	     
Top IT companies	  
Major semi conductor companies	    

We protect the solutions of the broadest range of customers: service providers, content distributors, security system integrators, device vendors, semiconductor manufacturers

inside secure

A complete “Secure Architecture”

INSIDE Secure VaultIP and Secure Boot SW



INSIDE Secure VaultIP & Device Authentication SW

INSIDE Secure Packet Engine IP or Guard SW

INSIDE Secure VaultIP & Secure Storage SW

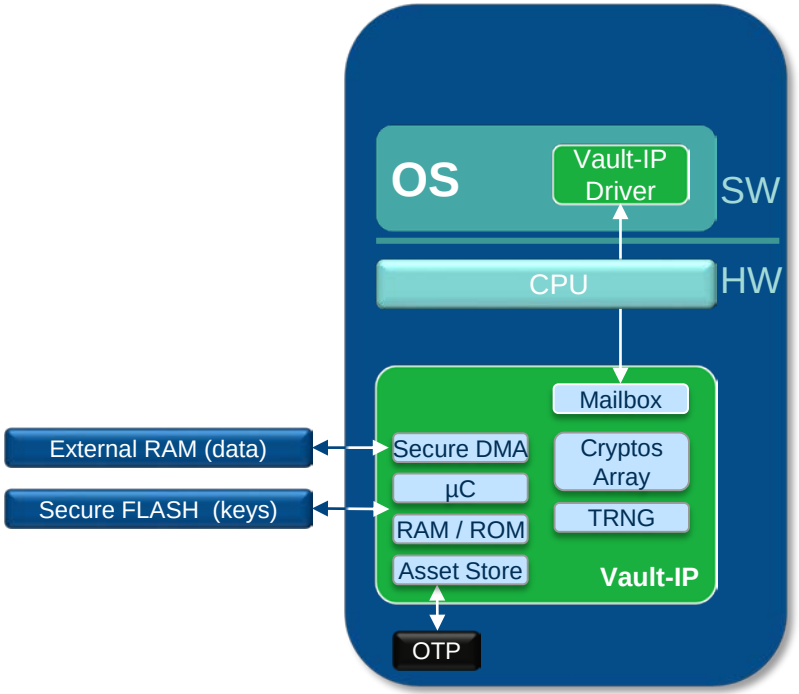
Security Requirements for Connected Systems

From Core to Cloud

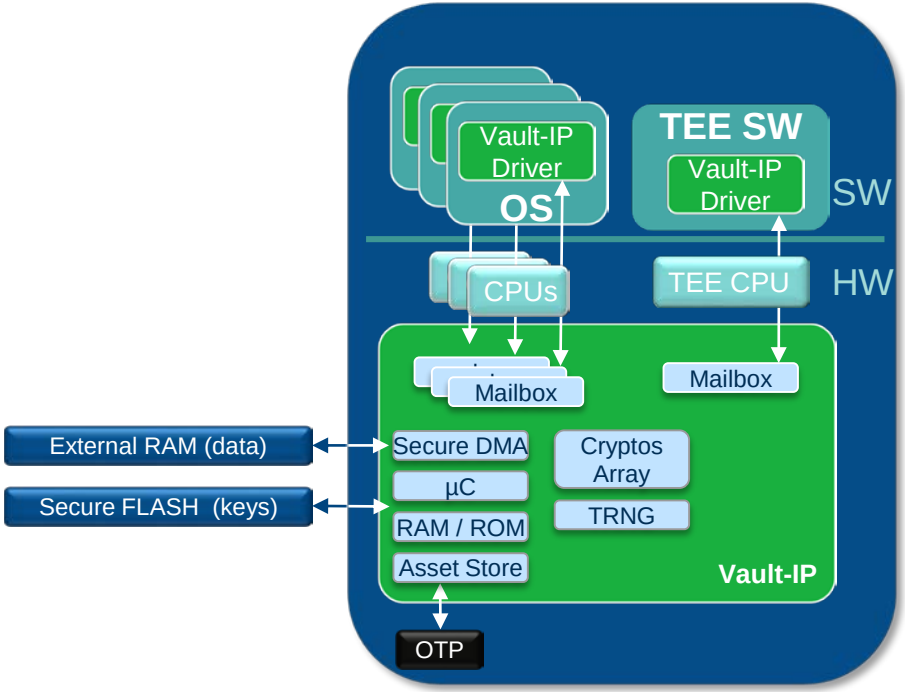
- Control plane secure tunnel establishment & key management:
  - Key refresh and tunnel setup rates matching 100Gbps and beyond
  - Efficient , area optimized Public Key Accelerators & True Random Number Generators needed
- Platform security
  - Secure Boot and Secure Debug
  - Trusted Execution Environment, Trust Anchor, Key Vault
- Mass adoption of standards based security protocols
  - SSL/TLS (Device/Server), IPsec (Client/Server), MACsec (Device)
  - Wireless – Zigbee, WPA, CAPWAP, LTE/3G Baseband,
  - Platform – Data Storage, Asset Protection
- Data plane performance continues to increase:
  - Not only client to cloud traffic increases but also inter cloud traffic, specifically server to data center and data center to data center bandwidth increase quickly.
  - L2: MACsec, many ports 400G Ethernet, 600Gbps FAT pipe & FlexE, multiport 100G, 1G, 10, 25G, 40G, 50G line speeds
  - L3: IPsec, 100Gbps and higher,
  - L4: SSL/TLS/DTLS, 40Gbps and higher

Security Anchor into your SoC

HSM without TEE

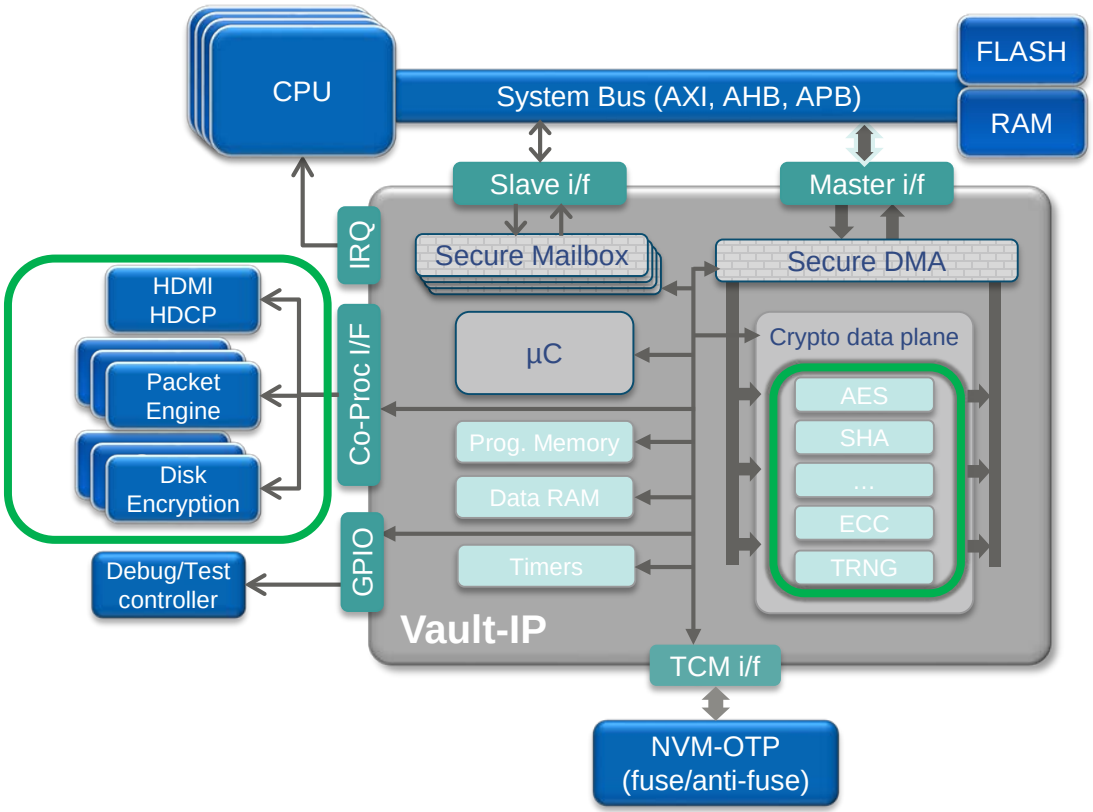


HSM with TEE and multiple CPUs



inside secure

Vault-IP Integration



- FIPS-140-2 level 2 certified
- Side Channel Protection
- Anti Tampering
- HW Protection for keys
  - Even if Kernel breached
  - Anti Cloning
- Scalable Crypto Accelerators
  - Internal and External
- TLS Device Authentication
- Secure debug enablement
- PKCS#11 API – Simplified
  - Easy to integrate
- Built-in provisioning
- Life-cycle management

inside secure

NETWORK SECURITY

www.insidesecure.com

inside secure

Security Challenges in the Network

Solution: Strong encryption, authentication, and platform integrity

2-Way Communication

Rogue or Personal Devices

Gateways / Router

2-Way Communication

Server

Data Management

Take control of the Device or Application

Insert Non-Authorized Devices

Take Control of the Routers/Servers

Man in The Middle: (Are we talking to the expected endpoint?)

- Spy the line
- Hijack network
- Broadcast private information

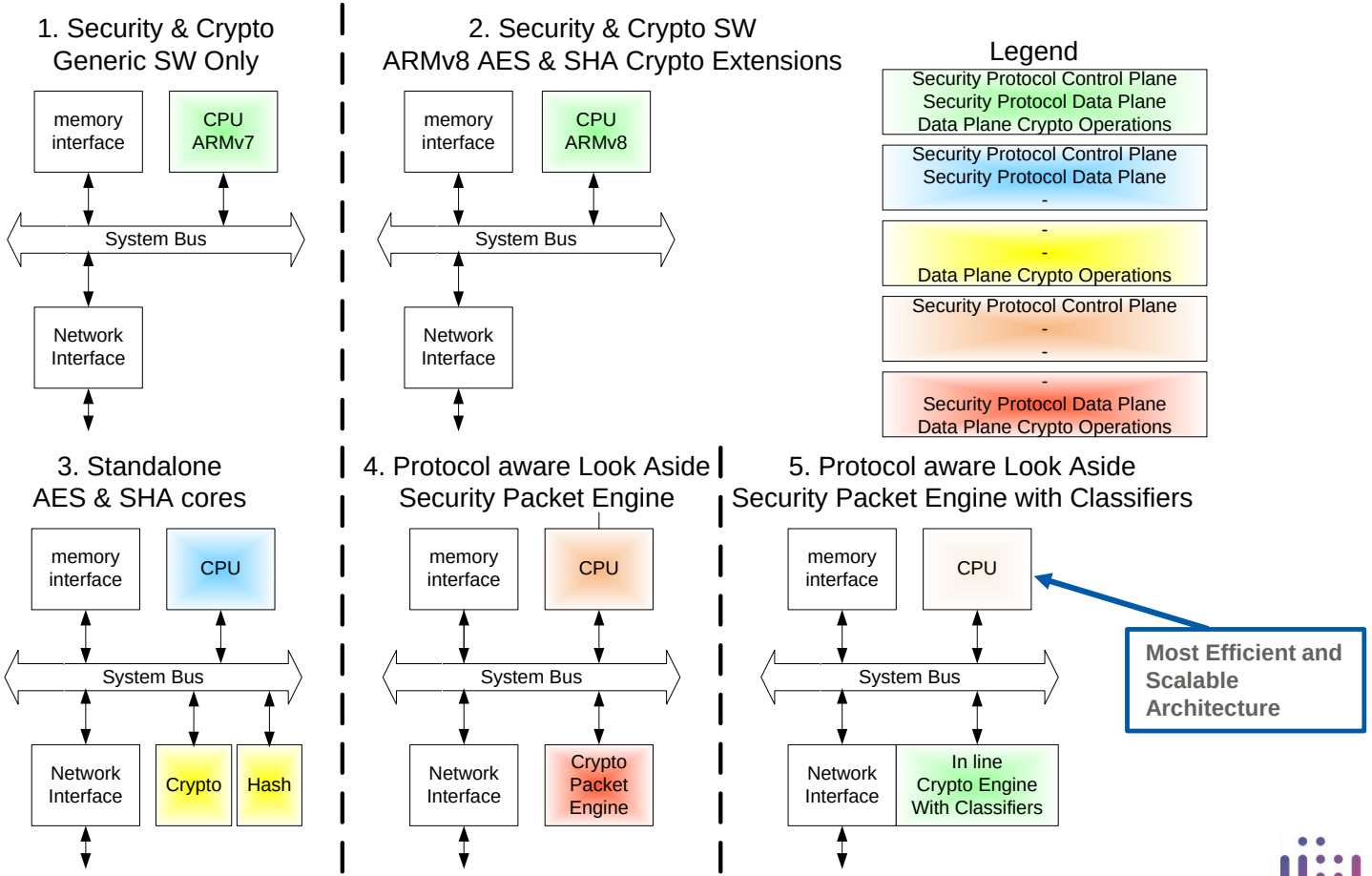
inside secure

System considerations when selecting a security architecture

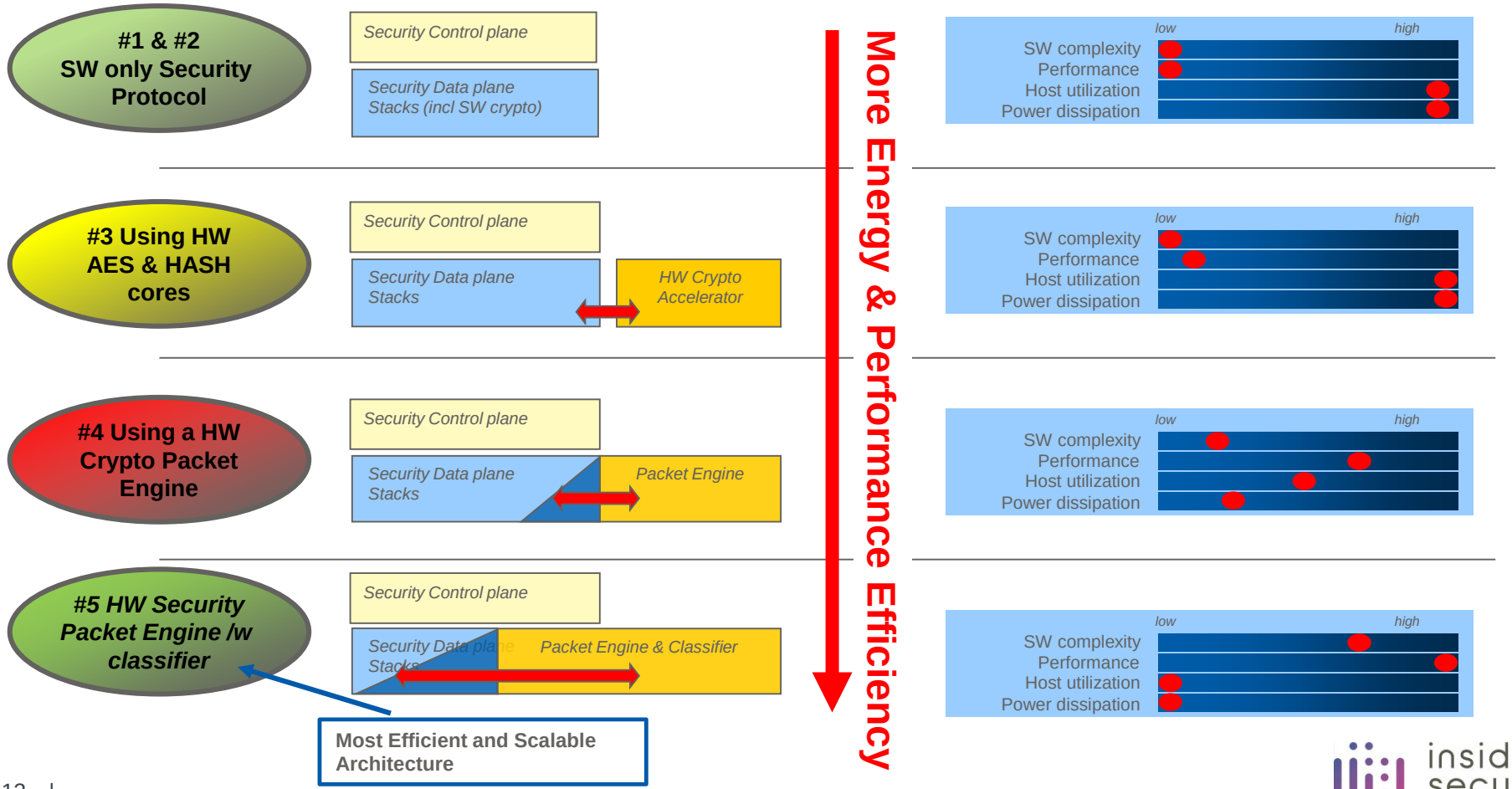
- Security Protocols:
  - Which security protocol will each application use?
    - Examples: IPsec (gateway/gateway), SSL/TLS (client/server), DTLS (client/server) for SSL VPNs, VoIP, and CAPWAP for Wireless AP Provisioning, MACsec (Ethernet)
- Performance:
  - What is the network bandwidth of the device? Do you require line rate security performance?
- CPU Utilization:
  - How compute intensive is the protocol implementation?
    - What is your power budget? (Battery, AC powered?)
    - How many CPU cycles are available for security?
      (Is this a forwarding device or is data initiated/terminated by apps on the local CPUs)
- Application Concurrency
  - Will multiple applications in the system all require security services?
  - Is there a requirement to isolate crypto keys & operations from other applications running in the system?
  - Is there a trusted execution environment present such as ARM TrustZone?

The solution to all these questions is a dedicated HW resource to accelerate all crypto functions

Architectural choices of implementing Security Protocols (IPSEC,SSL/TLS)

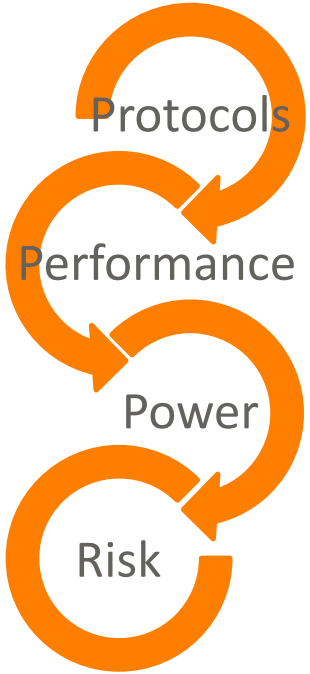


System tradeoffs for each architecture (IPSEC, SSL/TLS)



Why choose inside secure

- Security already pervasive and required
- High speed network systems continue to drive best profits
- Power efficiency lowers cost
- Manufacturers are liable when hacks succeed



SSL/TLS, DTLS, IPSec, MacSec, VPN's, HDCP, DTCP

Hardware acceleration enables the fastest systems

Hardware acceleration decreases power

Effective security keeps your company out of the news

INSIDE Secure has a complete suite of Silicon IP for all your design points, with the available protocol source code for a complete system implementation

inside secure




THANK YOU!

Stephen Wu
Senior Security Silicon IP and Software FAE

swu@insidesecure.com

inside secure