BKK19-315 Securing your next 96Boards design using Xilinx Zynq MPSoC

03.Apr.2019  Kevin Keryk
Avnet Public
Weak Security Impacts Everyone
Xilinx Security Solution Milestones

- Secure Boot App Note XAPP1175
- Measured Boot App Note XAPP1309
- Secure Boot @ XSWG
- Measured Boot @ XSWG
- Zynq-7000 Introduced
- Zynq US+ MPSoC Introduced
- Tamper Resistant Designs XAPP1323

IEC 62443-compliant Solution
Existing Standards:

- FIPS 140
- IEC 62443
- IIC IISF
- NIST SP 800-155

Value Added Resellers

OEMs
Cybersecurity Concept Design (CCD)

Solution Intent

- IIoT Security is complex but essential
- Reduce risk, cost, and time of customers, large and small, through pre-integrated solution
- Industrial-grade IEC62443 compliance requires HW+SW solution

Builds on Prior Work

- Picks up where XAPP1309 left off
- Extends Edge-Cloud
- All the Essentials

Optiga TPM2.0 – HW Root of Trust for Reporting and Storage

Zynq UltraScale+ MPSoC HW Root of Trust for Secure Boot
TPM 2.0 Pmod

AES-PMOD-TPM20-SLB9670-G
- Available from Avnet – 29.94USD

Features
- Infineon OPTIGA™ TPM SLB9670 2.0
- Enhanced SPI interface
- Small 1" x 0.6" plug-in Pmod (2x6 format)

For more information, visit our Ultra96 community website

http://avnet.me/tpm2.0
Security Mezzanine – Secure96

Presented by Joakim Bech during SFO17-111 Secure96 session

Features
• Infineon SLB9670
• Atmel ATSHA204A
• Atmel ATECC508A

For more information, visit 96Boards:

96boards.org/product/secure96/

youtu.be/nuoKQES0txU
Security Mezzanine – TRESOR

Available from Arrow – 81.56USD

Features
• SLB9670x TPM 2.0
• SLB9645x TPM 1.2
• SLS32AIA020A TRUST-E Authentication

For more information, visit 96Boards:

96boards.org/product/tresor/
Zynq UltraScale+ MPSoC Security Capabilities

- Secure and Measured Boot
- Secure Update/Reconfiguration
- Anti-Rollback Protection
- Secure Communications
- Secure Storage (Non-Volatile)
- Secure Debug
- Secure Execution Environment
- Configuration Limiter
- Unique ID
- Physical Security
- Tamper Responses

Today’s Focus

Basic components of Cybersecurity
Zynq UltraScale+ MPSoC - Block Diagram
Secure Boot Flow Overview

Source: Xilinx UG1085
Zynq MPSoC Security - More Resources

Zynq UltraScale+ MPSoC – OS and Libraries Documentation:

- XILFPGA – Secure loading of Programmable Logic Bitstreams
- XILSECURE – Secure loading of SW and Crypto Accelerators
- XILSKEY – Programming BBRAM and configuration eFuses

Zynq UltraScale+ MPSoC – Technical Reference Manual:

Zynq UltraScale+ MPSoC - Design Security Hub:
Acknowledgements

Thank you to the following people for the knowledge, wisdom, and encouragement to put this course together and pursue the ideal of a more secured world:

- Fred Kellerman – Avnet
- Jason Moore – Xilinx
- Bruce Schneier – Author of “Applied Cryptography”
Thank You