Leadership in Embedded Security

Breakout 4 -
Industrial/Supply-chain/Hardware

CCC
Computing Community Consortium
Catalyst

Identify 3 Key Challenges in the Application Area

- Semiconductor manufacturing is becoming increasingly concentrated in a small number of companies and countries.
    - The design IP must transit these companies to be manufactured.
    - The design may be modified during manufacture.
    - Manufacturers may choose to prioritize customers.

- Industrial / SCADA applications often have very long lifetimes and are beholden to legacy interfaces (e.g. ModBus)
    - As with IoT and automotive, concern about “abandonware”

- Emphasis on performance creates vulnerabilities and side channels (e.g. Meltdown)

- Vague threat model -- no clear information about weakest link in supply chain (CAD/design/foundry)

Identify 3 Key Trends in the Application Area

- Increased Cost and Complexity of ASIC *design*
  - > $500M for a new commercial smartphone SoC development
  - Reliance on third-party Intellectual Property (IP)

- Increased cost and complexity of ASIC *manufacturing*
  - $5-15B to build a modern fabrication facility,
    - plus recurring costs to run at a sufficient rate to get good yield

- For all but the largest players, increased reliance on commercial FPGAs / SoCs to reduce productization costs
  - firmware is readily patchable
  - hardware is mass-produced, takes efficient advantage of latest process nodes

Identify 3 Potential Novel Solutions in the Application Area

- Split design → leveraging a slower, trusted part to mediate technology executed in a state of the art, less trusted part.
  - “Split ASIC” fabrication
  - Multi-chiplet / 3D-integrated modules with hardware integration
  - Multi-chip modules with firmware / software integration

- Design escrow → ensure that an OEM’s design documents, source code, etc. are not lost if the OEM goes away or neglects its products. (Who will hold the IP? What regulations will require it? What product lifetime is required? What triggers release?)

- Decentralized trust network to maintain provenance information

Extra Slide

- This is a slide
- It is extra