TRUST THROUGH FUNCTIONAL DISAGGREGATION

Ken Plaks, DARPA/MTO Program Manager

NDIA Trusted Microelectronics Workshop

August 17, 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need. SPADE will help to prevent and respond to threats such as the malicious insertion of hardware trojans and reliability failures.
How do we ensure that the warfighter has access to state-of-the-art electronics?
Advanced packaging

- Manage complexity
- Improve yield
- Allow specialization

Global TSV Chip Wafer Forecast

CAGR ~ 56%
Key technical enabler ... interconnects

Source: MIT Lincoln Labs
ASIC trust solution

**Workhorse die**
- 14nm, ~250M gates
- UNTRUSTED

**Security die**
- 90+nm, ~500K gates
- PROTECT and PRESERVE
- TRUSTED

**Assembly and packaging**
- PROTECT and PRESERVE
- TRUSTED

---

**Unpowered**
- Nothing sensitive
- Sensitive Information lives on security die

**Boot**
- Information exposed
- Verify integrity, release information

**Runtime**
- Perform sensitive logic
- Perform mission
- Monitor operations

---

**Graph:**
Node Productivity and Trusted Availability
- Number of Trusted Fab
- Data: GD vs Commercial ASIC
- Source: TTR3
- "Average" ASIC complexity

---

DISTRIBUTION A. Approved for public release: distribution unlimited.
Malicious logic: passive techniques

• Goal: make it harder to insert hardware trojan/malicious logic
  • MITIGATE risk through obfuscation
  • Interconnect density allows much more thorough obfuscation

Source: MIT Lincoln Labs

• Plus: full suite of commercial obfuscation techniques...

State-Space Obfuscation

Logic Encryption

Camouflaging
Malicious logic: active techniques

- Assume: attacker has successfully compromised untrusted portion
- Goal: **MITIGATE** impact and contain contamination

**Key research questions:**
- How do you detect?
- How do you mitigate impact?
- Is it scalable? Performance impact?

- Security die moderates all signals:
  - Enables active monitoring
    - IO
    - Control
    - State (privilege, etc)
  - Out of band with mission circuits
  - Prevent spread of contagion by quarantine

**Artist's concept**

**Workhorse die**
Assume successfully compromised

**Monitor all traffic on/off chip**
MITIGATE by quarantine

**Security die:** Out of band,
TRUSTED manufacture
and less available to cyber compromise

DISTRIBUTION A. Approved for public release: distribution unlimited.
SPADE trust demo for ASICS

- Phase 1 DARPA SPADE demo
  - Trust-on-Trust: Surrogate 45/90 nm workhorse
  - Proof of concept, functional demo, security demo
  - Delivers data for phase 2 decision
- Phase 2 SPADE prototype
  - 14nm workhorse
  - Full obfuscation

Achieve the spirit and intent of trust while meeting warfighter need

DISTRIBUTION A. Approved for public release: distribution unlimited.
Conclusion

- DoD is good at protecting critical data,
  - has trouble with large designs
- Industry is good at massive integration,
  - has trouble protecting critical data
- Technology allows a marriage
  - Massive interconnect density
  - Vertical stacking
- Success will allow DoD to
  - **PROTECT** classified data /algorithms
  - **PRESERVE** warfighter advantage
  - **MITIGATE** Hardware Trojan risk
  - **FASTER** design cycles than the status quo

<table>
<thead>
<tr>
<th></th>
<th>Scale</th>
<th>Security</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>UnTrust</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Bring the state-of-the-art back to military electronics