# STARSS Workshop Survey & Summary of Results

In advance of a workshop on Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) on June 22, 2014, a survey of those invited to participate asked about threats and what research could help to address those.

Sixty responses were received from 39 industry, 13 academia, and 8 government respondents. Below are the survey and a summary of the results.

**SURVEY**

*1. Current Threats*

Which of the following threats to security or assurance (or other(s) that you specify) are the 1st, 2nd, and 3rd in terms of concern (= likelihood + impact) TODAY.

A. Theft of IP or proprietary data (e.g. design IP or personal/user data)
B. Inadvertent incorporation of IP that includes a security vulnerability (intentional or unintentional) that creates vulnerability
C. Security breach/attack linked to a vulnerability in a hardware component
D. Counterfeiting of legacy (no longer available from the original manufacturer) products
E. Counterfeiting of currently manufactured products, including cloning and overproduction
F. Malicious tampering or hardware Trojan, i.e. inserted functionality
G. Vulnerabilities associated with emerging technologies and applications (e.g. Internet of Things)
H. Other

*2. Future Threats*

Given trends toward more embedded functionality and connectivity, what are likely to be the greatest hardware assurance challenges in 10-20 years?

A. Theft of IP or proprietary data (e.g. design IP or personal/user data)
B. Inadvertent incorporation of IP that includes a security vulnerability (intentional or unintentional) that creates vulnerability
C. Security breach/attack linked to a vulnerability in a hardware component
D. Counterfeiting of legacy (no longer available from the original manufacturer) products
E. Counterfeiting of currently manufactured products, including cloning and overproduction
F. Malicious tampering or hardware Trojan, i.e. inserted functionality
G. Vulnerabilities associated with emerging technologies and applications (e.g. Internet of Things)
H. Other

*3. Threat agents/attackers*

Rank the following threat agents in order of concern to you/your organization today.

A. Hacker
B. Politically/socially motivated adversary (including individual activists and large, possibly state-funded activities/organizations)

C. Economically motivated adversary (including counterfeiters, those looking to steal valuable data, ranging from individual/small groups to large, well-organized activities, etc.)
D. Competitor (e.g. corporate espionage)
E. Insider (disgruntled employee or ex-employee with knowledge/access)
F. Other

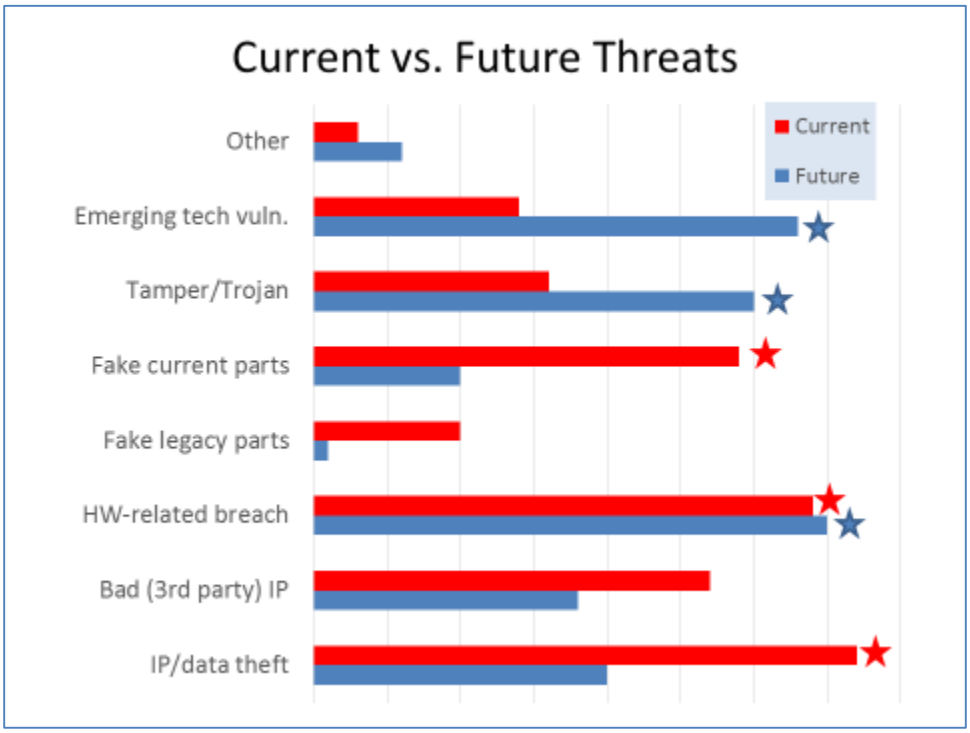
*4. Research Priorities*

What are the top research challenges that you feel can and should be addressed by university research in the next 3-5 years?

A. Advances in designing systems that do only what is intended
B. Advances in verifying that designs do only what is intended (including formal methods)
C. Fixed-function security features, e.g., PUFs, cryptographic offloading/acceleration, key management, etc.
D. Metrics for assessing security and trustworthiness
E. Strategies for assessing threats *without direct access to IP*
F. Run-time operational monitoring of integrity and related mitigation
G. Hardware Roots of Trust, i.e., minimal hardware element in a system that is responsible for a specific security priority without dependencies on other elements
H. Establishing Assurance, e.g., by way of the design process, testing, analysis, or formal methods
I. Security composition, i.e., the ability to reason about security properties of a system, which in turn is composed of components with properties that may or may not be well understood
J. Security of distributed networks / Internet of Things
K. Hardware/software co-design and design trade-offs
L. Provenance (of designs, components, etc.) for supply chain assurance
M. Other

**RESULTS**

## Q1 and Q2. Current and Future Threats (Top 3 are marked by stars.)

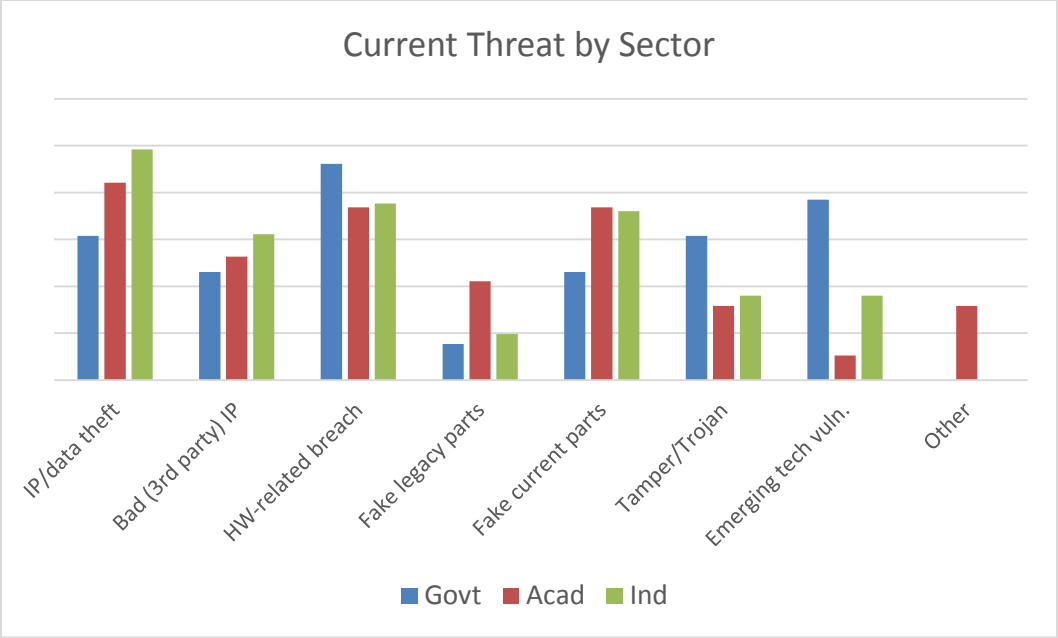


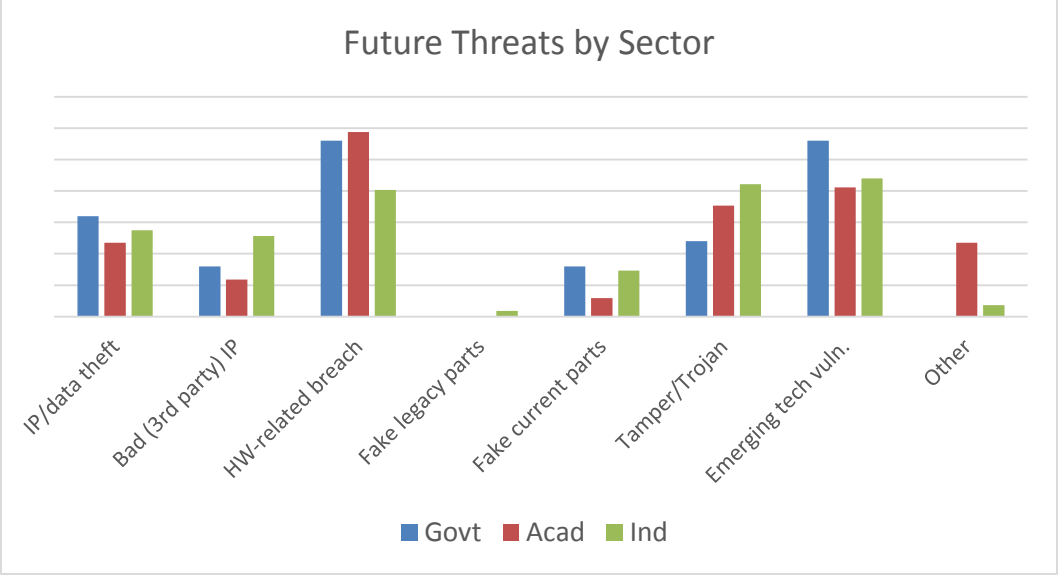

Other Current Threats

- Tampering and reverse engineering
- Lack of engineering processes for limiting/mitigating known vulnerabilities
- Monetary loss due to hacking

Other Future Threats

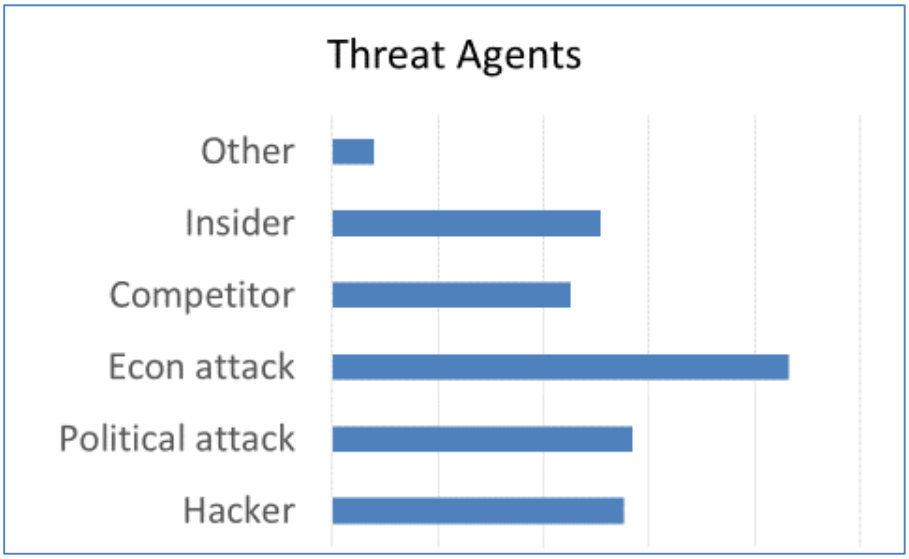
- Exploitation of flawed (buggy) systems
- Weaknesses in field-updates of SW and firmware
- Hardware features that enable software and data attack
- The primary challenge in 10 – 20 years will likely be something we are not aware of today.
- "All of the above" are future threats. I would add the concern of deliberate mal functionality, as 3rd party IP is increasingly used as a “fast implementation” solution. In a revision update, it can be hard to detect superset substitution in HDL, especially if the interface remains unchanged and the verification tests are the same to maintain coverage and validation.



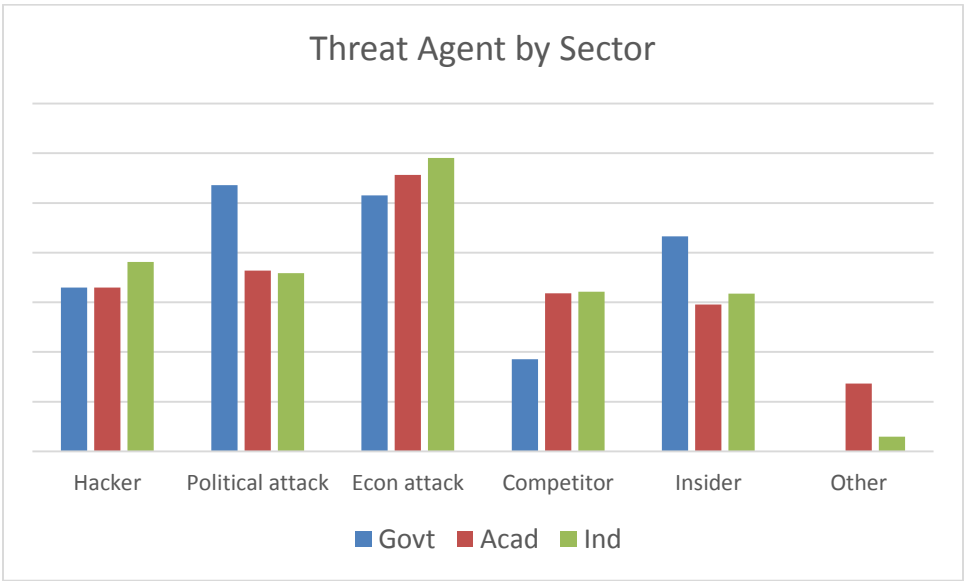

Responses are normalized within each sector.

**Q3. Threat Agents**



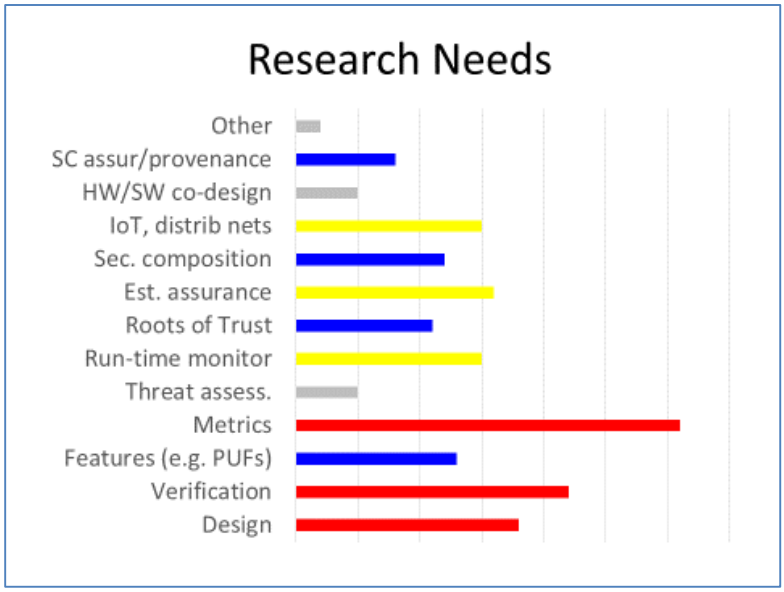

Other Threat Agents

- Professional people that search for weaknesses
- Motivated students that undermine university business (and grading) systems.
- National governments; insiders acting on behalf of national governments.
- Peer nation states
- Customers end products being attacked by hackers
- “Economically motivated” agents may also be "socially motivated" (jealous ex, etc).



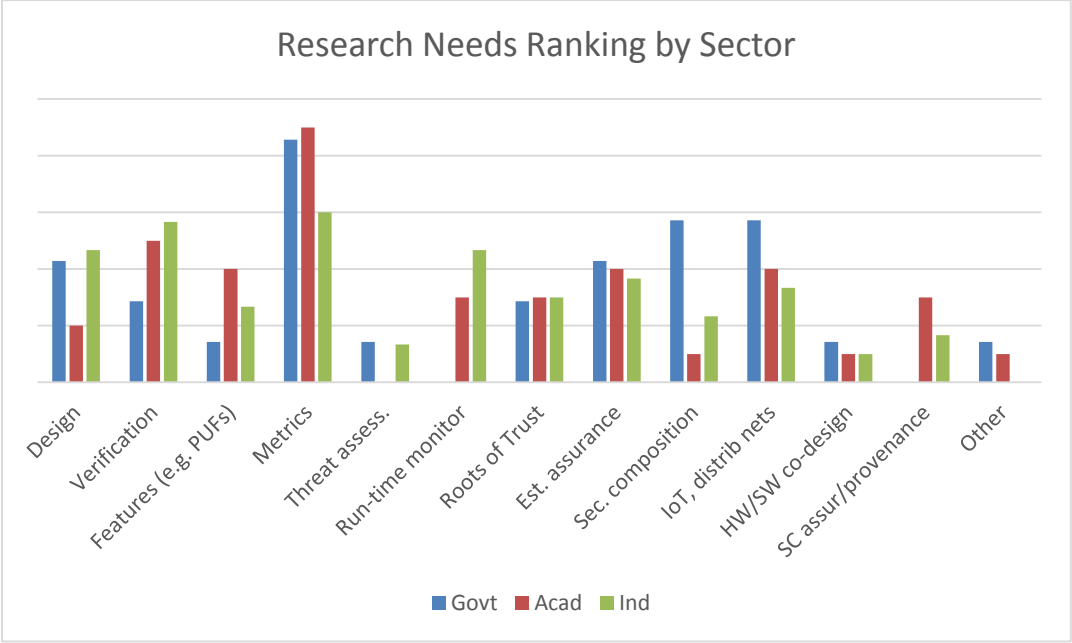

Responses are normalized within each sector.

**Q4. Research Needs (Color used to group topics according to the number of votes received.)**




Other Research Needs

- Design for resilience against security attacks (similar to fault tolerance against operational defects)
- Role of humans in building and operating capabilities with important assurance criteria




Responses are normalized within each sector.

**SUMMARY OF RESULTS**

Overall, the top current threats are:

- Theft of IP or data
- Security breach linked to a vulnerability in hardware
- Counterfeiting of currently manufactured products, including cloning and overproduction
- Inadvertent incorporation of IP (developed internally or from a third party) that includes a security vulnerability

However, respondents felt that in 10-20 years IP/data theft, counterfeits, and vulnerabilities due to "bad IP" will be of relatively less concern. The risk of breaches associated with hardware is predicted to remain high and threats due to tampering and from emerging technologies are forecasted to increase significantly relative to others.

The top concern varied by sector. In the near term, the top concern for government is hardware-associated security breaches/attacks, whereas industry and academia ranked IP and data theft highest. Counterfeiting of legacy parts was rated substantially higher by academics than by industry or government respondents. In the longer term, government respondents ranked hardware-related breaches and vulnerabilities associated with emerging technology as highest, whereas industry respondents viewed several threats as important, including tampering (which industry rated considerably higher than others, especially government). Academics rated hardware-related breaches as the highest long-term threat.

In response to the question about threat agents, overall, economically motivated attacks are seen as the greatest threat with all others being rated similarly. However, when viewed according to sector, government respondents are most concerned about politically motivated attacks whereas academic and industry respondents, along with many government respondents, see economically motivated attacks as the greatest concern.

Regarding areas in which targeted fundamental research could help improve hardware security and assurance, the overall highest priority was given to metrics, followed by security verification and design. When viewed by sector, however, metrics was rated considerably higher by academia and government than by industry. Areas that industry rated higher than other sectors include verification, design for security, and run-time monitoring. Government respondents rated secure composition much higher than others and Internet of Things somewhat higher. Academics felt that, in addition to metrics, security features (e.g. PUF's) and supply chain assurance were relatively more important research topics compared to government and industry respondents. Hardware/software co-design and threat assessment received relatively few votes among respondents from all sectors.

The survey is a useful snapshot of the opinions of a sample of respondents with varying backgrounds and expertise. The results are useful input to SRC's research program in this area and may also be of interest to government agencies that support hardware security research, as well as to academic researchers motivated by industry and government concerns and needs.

*For more information contact Celia Merzbacher at celia.merzbacher@src.org.*