NSF Webinar on NSF Solicitation 14-528

NSF-SRC: Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS)

Keith Marzullo, Jeremy Epstein, Nina Amla, Angelos Keromytis, Ralph Wachter, Paul Werbos
Directorate for Computer and Information Science and Engineering
Directorate for Engineering
National Science Foundation

Celia Merzbacher
Semiconductor Research Corporation

15 January 2014

Outline

- Joint NSF-SRC partnership
- Hardware Security Challenges
- Design for Assurance
- Topics of Interest
- Program Details
- Frequently Asked Questions
- Program Director Contacts

Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) Program

- Jointly funded partnership between National Science Foundation (NSF) and Semiconductor Research Corporation (SRC)
- Supporting fundamental research to make semiconductors and systems more trustworthy and secure
- Partnership with SRC provides researchers greater insight and access to industry needs/capabilities/resources; facilitates transition to practice; and provides students opportunities to engage with industry.

About SRC: Maximizing Value of Industry-Driven University Research

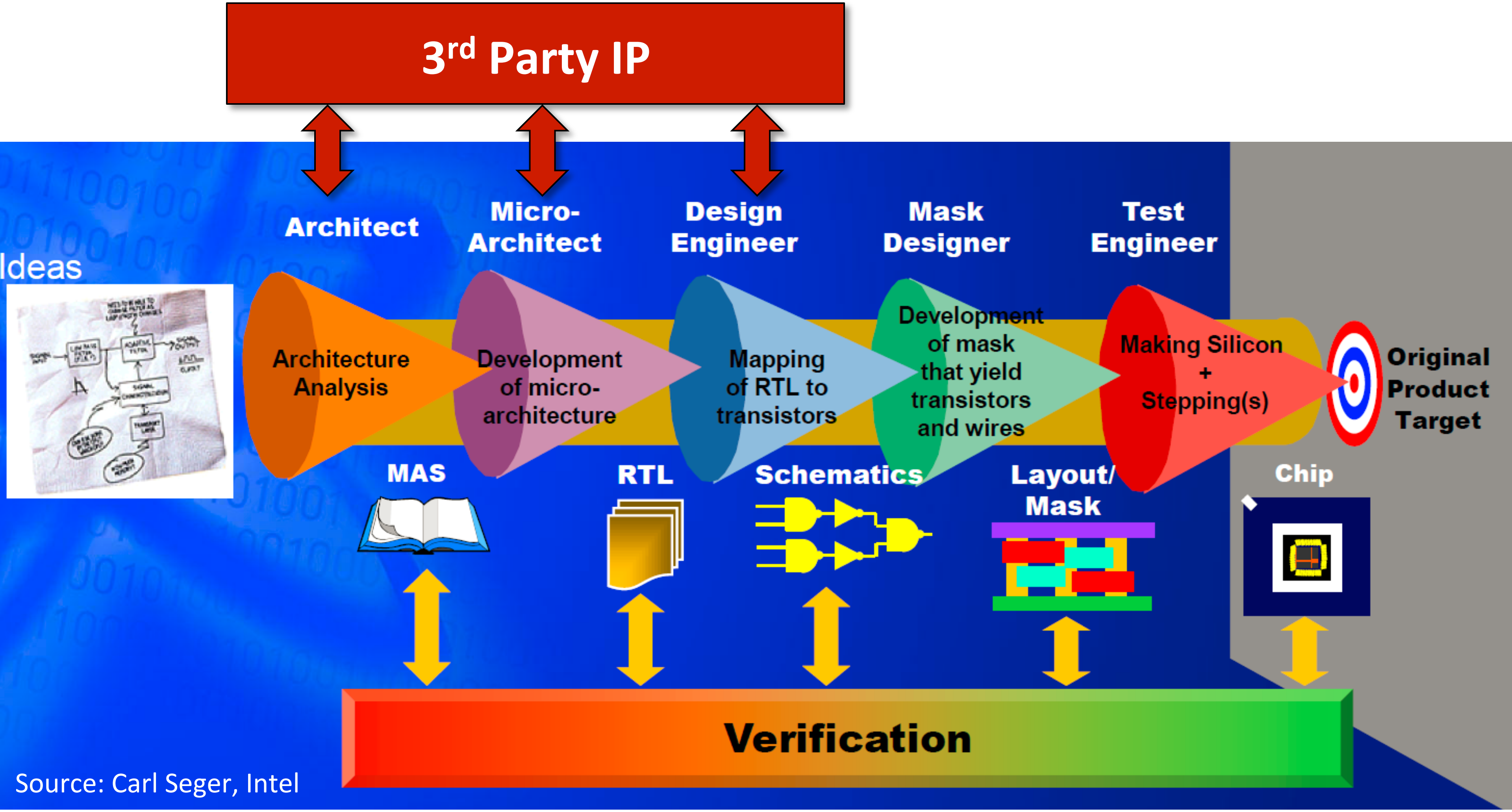
- SRC industry consortia provide university researchers:
  - Guidance on industry needs
  - Funding, often in partnership with government
  - Input and feedback during research
  - Industry contacts
  - Pathways to practical application and technology transfer
- Since 1982, SRC has invested nearly $2B of industry funding in support of more than 10,000 students and 2,000 faculty at over 200 universities
- New SRC focus on Trustworthy and Secure Semiconductors and Systems (T3S) initially supported by AMD, Freescale, Intel and Mentor Graphics

Semiconductor Trends Impacting Security & Trustworthiness

- More pervasive—contributing the proper and safe functioning of every electronic or "smart" device or system
- Increasingly networked—making unintended access possible
- More complex—billions of transistors comprising a multifunctional "system on a chip"
- Intellectual property from multiple 3rd party sources
- Design and manufacture involves a long and global supply chain —many processes are done by businesses outside the U.S.

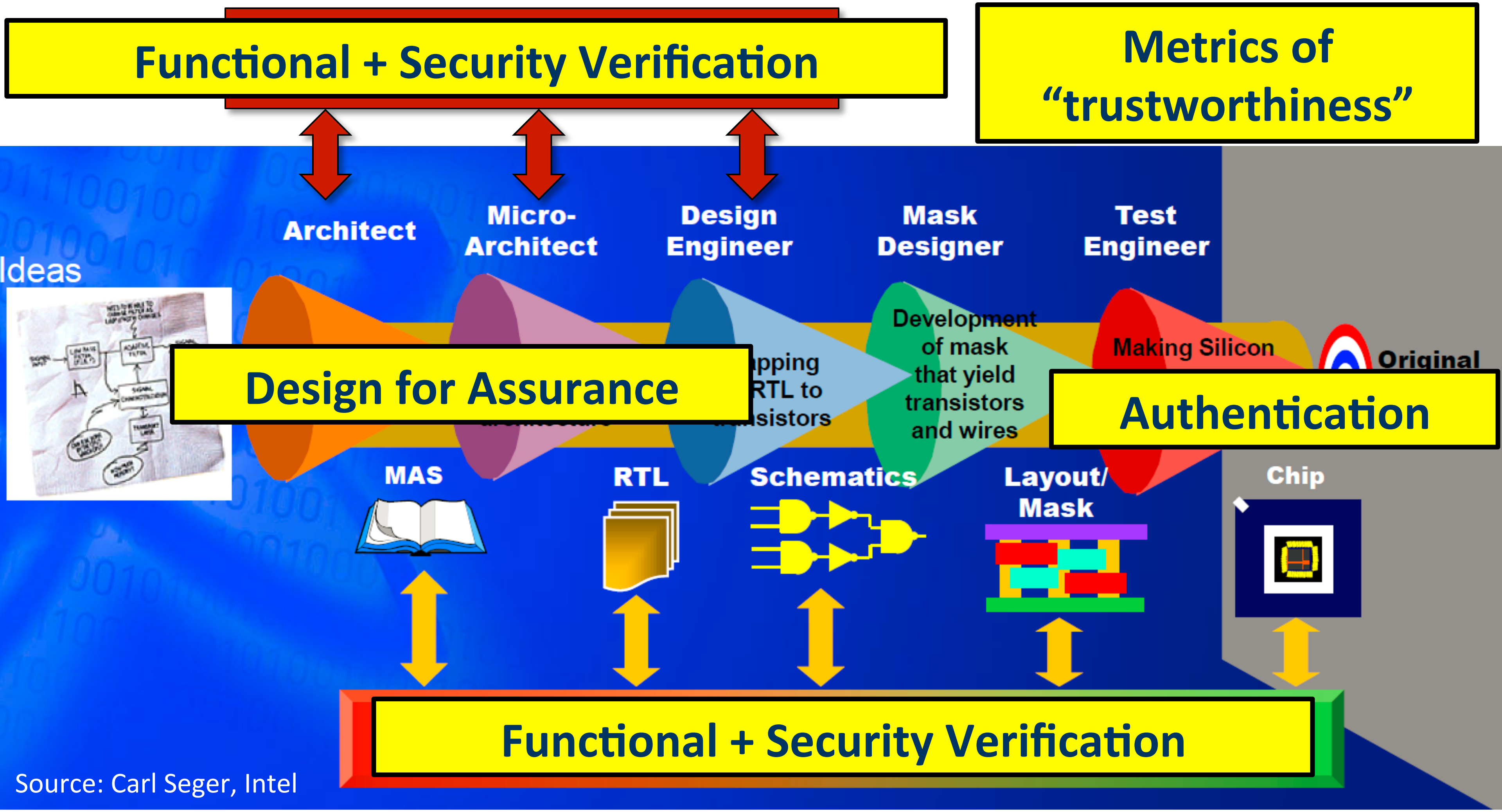
★ ***Trends lead to: increased vulnerabilities, greater impact if a chip fails, and more attractive targets for attack***

Semiconductor Design & Manufacture



Source: Carl Seger, Intel

Priority Research for STARSS



Functional + Security Verification

Metrics of “trustworthiness”

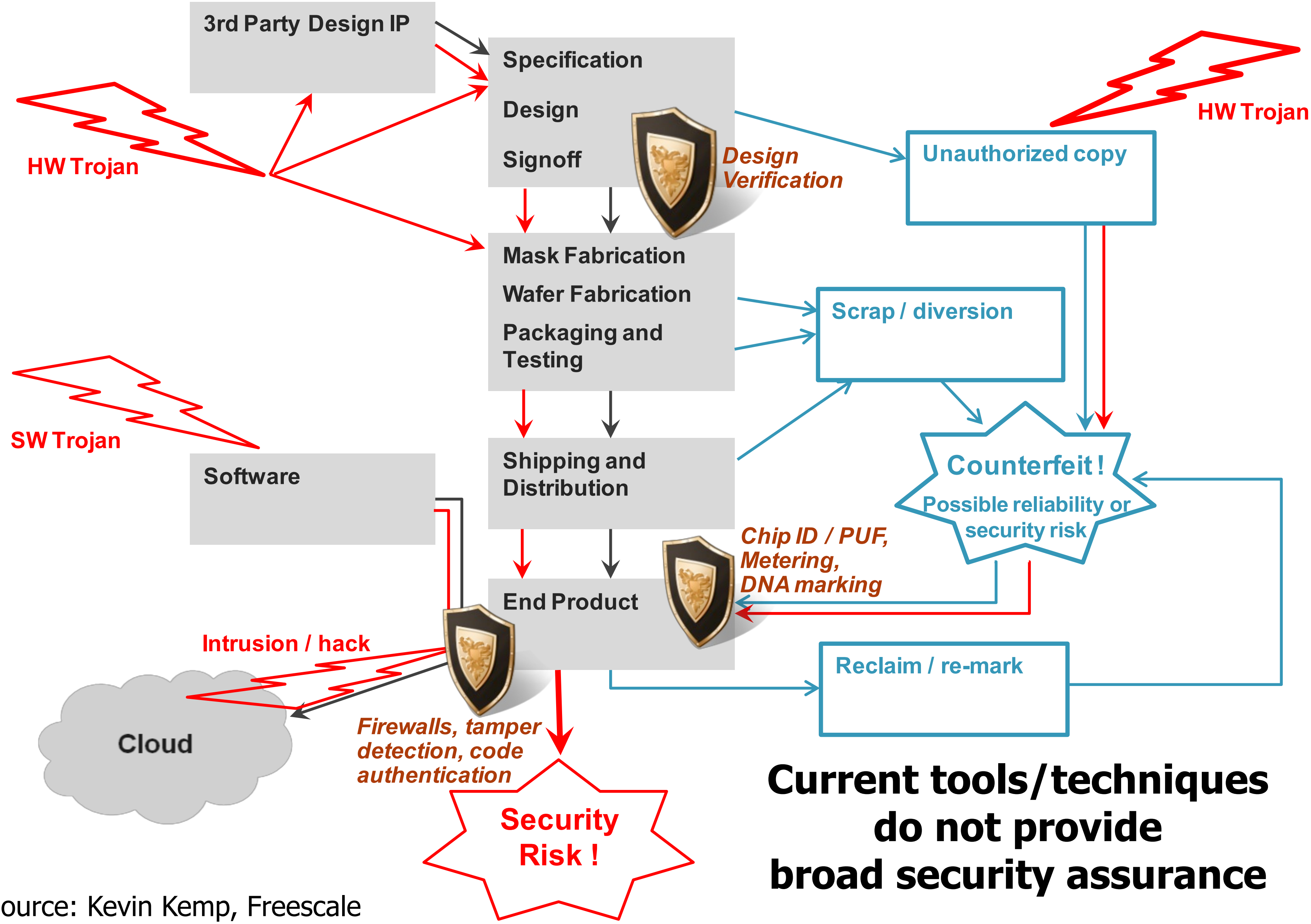
Design for Assurance

Authentication

Functional + Security Verification

Source: Carl Seger, Intel

Semiconductor Design & Manufacture Flow: Potential Points of Vulnerability to Attack/Theft



3rd Party Design IP

Specification

Design

Signoff

Design Verification

HW Trojan

HW Trojan

Unauthorized copy

Mask Fabrication

Wafer Fabrication

Packaging and Testing

Scrap / diversion

SW Trojan

Software

Shipping and Distribution

Counterfeit !

Possible reliability or security risk

Chip ID / PUF, Metering, DNA marking

End Product

Intrusion / hack

Cloud

Reclaim / re-mark

Firewalls, tamper detection, code authentication

Security Risk !

Current tools/techniques do not provide broad security assurance

Source: Kevin Kemp, Freescale

Threats and Challenges

- Unwanted functionality in specification, design or implementation
- Unauthorized access to sensitive data or control functions
- Tampering with electronic circuit while in operation via side channel
- Hardware Trojans and other tampering during design or manufacturing
- Lack of control at interfaces, leaking sensitive data, vulnerable to attack
- Poor resistance to tampering at functional, logical, electrical level
- Dependence on outsourced components that are not verifiable
- Inadequate hardware authentication
- Uncertain provenance of circuitry

How can one be assured that a chip does what it was designed to do

…and *nothing* else?

STARSS Goals & Objectives

- **Goal:** Develop strategies and tools to design & manufacture chips and systems that are secure, trustworthy, assured, and resistant to attack or counterfeiting.
- **Objectives**
  – Decrease likelihood of unintended behavior or access
  – Increase resistance to tampering and counterfeiting
  – Improve ability to provide authentication throughout the supply chain and in the field

Topics of Interest

- Architecture and Design
- Properties, Principles and Metrics
- Current and Future Threat Assessment
- Security Verification and Analysis
- Tools and Frameworks
- Authentication and Attestation

Topics of Interest

Architecture and Design

- Architectural and design approaches that minimize vulnerabilities
- Models and frameworks for specification and reasoning about hardware-specific security properties
- Methods for protecting against security-related vulnerabilities resulting from side effects
- New design or specification languages

Topics of Interest

Properties, Principles & Metrics

- High-level hardware security design principles and generalizing semiconductor-specific properties
  - e.g., confidentiality, integrity and availability of security-sensitive assets and access mechanisms
- Develop knowledge base of concrete examples, scenarios, and other empirical evidence
- Metrics that provide a measure of the security of a particular design

Topics of Interest

Current and Future Threat Assessment

- Dynamic information base to identify, classify, analyze and share information about security threats in hardware
  - unintended vulnerabilities and malicious design or fabrication
- Taxonomies and representations of hardware-related security threats

Topics of Interest
Security Verification & Analysis

Tools, techniques and methodologies for

- Verifying hardware-specific security properties
- Enforcing security design principles
- Regression and other forms of testing
- Formal methods for hardware security verification
- Ensuring coverage and equivalency across different phases, *e.g., design, implementation, integration and manufacturing*

Topics of Interest
Tools and Frameworks

- A semiconductor security development model
  - To help designers utilize Design for Assurance strategies and tools
  - Similar to existing software security engineering models.
  - Aimed at academic and industrial education and training
  - To provide for assessment of organizational (security) maturity and product assurance over time
- Facilitated by providing researchers access to current industry processes

Topics of Interest

Authentication & Attestation

- Support for insertion of artifacts or design elements that can be verified during design and implementation, and manufacturing
- Support for dynamic verification in the field and non-destructive authentication for supply chain assurance
- Semiconductor provenance model and related design artifacts, *e.g., hardware fingerprinting and third party design element model checking*
- Generation, protection and establishment of trust models for hardware-implemented keys

Submission Details

- Proposals (< $500,000 for 3 years)
- Submit proposal to NSF, deadline: 26 March 2014
- Begin Proposal Title with "**SaTC:STARSS**:"
- Limit of 1 proposal per PI to STARSS
  - **Note**: this limit is distinct from the PI limit in the SaTC solicitation
- No classified proposals will be accepted

Must upload *statement of consent* that indicates NSF may share with SRC the proposal, the reviews generated for the proposal, and any related information

Proposal Review Process

- Administered by NSF, in accordance with NSF standards and procedures
- NSF and SRC program directors coordinate on review panels and award recommendations

Projects selected for joint funding by NSF and SRC will be funded through *separate* NSF and SRC funding instruments

Award Details

- All awards involving SRC funds will be made under a contract that:
  - Provides for *non-exclusive*, *royalty free rights* to *all* SRC members for *any* intellectual property generated as a result of the SRC-funded research.
  - Discloses any background or blocking IP
- NSF and SRC will manage their respective award according to their own procedures and guidelines

Post Award Management

- Awardees must submit annual reports to the appropriate funder(s)
- One or more project representatives must attend the first NSF/SaTC PI meeting in Fall of 2014
- In years in which no SaTC PI meeting is held, SRC will hold a review of all STARSS projects

Frequently Asked Questions

Frequently Asked Questions

Proposal Submission Related

Q: Can I submit the same proposal to SaTC and STARSS?

A: No, you must choose one program.

Q: Does a submission to STARSS count towards the 2 proposal limit for SaTC?

A: No, you can submit 2 proposals to SaTC and 1 to STARSS.

Q: I just submitted the perfect STARSS proposal to SaTC, what should I do?

A: You can withdraw the proposal and submit to STARSS.

Q: Can a STARSS proposal include a Transition to Practice Option?

A: No, those are for SaTC only.

Frequently Asked Questions
Scope Related

Q: How do I decide whether to submit to SaTC or STARSS?

A: If you are interested in the benefits that go along with SRC funding then please submit to STARSS. Talk to a SaTC or SRC program director if you are unsure.

Q: Does the new STARSS program mean that SaTC will be reducing funding for hardware security?

A: No. Hardware security is still a priority for SATC.

Q: Are only hardware proposals in scope for STARSS?

A: Yes. STARSS is hardware-oriented, but interfaces with software, including microcode, firmware, and software tools that are used to design circuits and systems.

Frequently Asked Questions
Award Related

Q: How many awards will be made?

A: We expect to make 6 STARSS awards, subject to the availability of funds.

Q: Is there a difference contractually between an NSF award and SRC award?

A: The NSF funding agreement is a "grant"; the SRC funding agreement is a "contract". Deliverables vary.

Frequently Asked Questions
Award Related

Q: If co-funded, is the same proposal used for both NSF and SRC?

A: Yes. There is a single technical description or Statement of Work for each project, but two funding agreements. Awardees will be provided guidance on how to split the budget.

Q: Will SRC fund participants at non-US institutions (which are not funded by NSF)?

A: No. All funded participants must follow standard NSF eligibility requirements.

Frequently Asked Questions

Financial Related

Q: Is this new money (in addition to SaTC)?

A: NSF is funding STARSS out of SaTC funds. We're pleased to combine NSF funds with SRC funds.

Q: Is STARSS a multi-year program?

A: Yes. NSF and SRC anticipate continuing investment in this area for multiple years, subject to the availability of funds.

Frequently Asked Questions

Intellectual Property Related

Q: Are there any restrictions on intellectual property as a result of SRC involvment?

A: Under the standard SRC contract, the University retains ownership and SRC receives a non-exclusive royalty free license for its members to any IP developed.

Q: Can we get access to SRC member company technology?

A: Potentially. This would be handled on a case by case basis between a member company and university.

Frequently Asked Questions

Additional PI Requirements

Q: Do I have to attend the NSF biennial SaTC PI Meetings and SRC reviews?

A: Yes. But there will be only one review per year; SRC reviews will be held in years in which there is no SaTC PI meeting.

Q: Do I have to submit reports to both SRC and NSF on a STARSS award?

A: Yes, assuming both SRC and NSF jointly fund the award. The contents of the two are similar.

Frequently Asked Questions

Post Award Related

Q: Will SRC be actively involved as collaborators and working on spin-off projects, or provide in-kind support?

A: SRC provides for interaction and engagement between technical experts at member companies and funded researchers, which can result in a variety of other collaborations.

Q: Will SRC act as an industrial advisory team or as part of a larger advisory team?

A: SRC coordinates industry input and feedback through a number of mechanisms, including webinars, annual reviews, and through an industry Liaison Program that connects individuals from member companies with university research projects.

For further questions

If you have additional questions after the webinar concludes, please send them via email to

Nina Amla, NSF CISE/CCF, (703) 292-8910, namla@nsf.gov
Celia Merzbacher, SRC, (919) 941-9413, celia.merzbacher@src.org
Ralph Wachter, NSF CISE/CNS, (703) 292-8950, rwachter@nsf.gov
Paul Werbos, NSF ENG/ECCS, (703) 292-8339, pwerbos@nsf.gov

with the subject line starting with "SaTC:STARSS:"

The presentation will be available following the WEBINAR at
https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504996

The solicitation is available at

http://www.nsf.gov/pubs/2014/nsf14528/nsf14528.htm

Questions ?

The telephone line is now open

Takeaways

- STARSS is an exciting new opportunity for NSF funded researchers to work closely with industry. STARSS researchers will help to provide assurance that hardware will be secure and trustworthy into the future.
- Proposals due 26 Mar 2014 to NSF
- Contact an NSF and/or SRC program officer with questions!