Designed-In Security

Workshop Summary

Brad Martin, NSA

Bill Scherlis, CMU

Ron Perez, AMD

Celia Merzbacher, SRC

HCSS Conference, Annapolis

7 May 2014

Background

- NITRD report http://cybersecurity.nitrd.gov/
  - *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program* (2011)

  - **Designed-In Security** identified as a research theme to foster research that:

    Builds the capability to design, develop, and evolve high assurance, software-intensive systems predictably and reliably while effectively managing risk, cost, schedule, quality, and complexity…

Designed-In Security

Using assurance-focused engineering practices, languages, and tools, software developers will be able to **develop a system while simultaneously generating the assurance artifacts** necessary to attest to the level of confidence in the system's capabilities to withstand attack.

Research is required to develop:

- Models and techniques to support **on-the-fly evidence creation** during a systems engineering process
- Mathematically sound techniques to support **combination** of models and **composition** of results from separate components
- Analysis techniques (based on model checking, abstract interpretation, semantics-based testing, and/or verification) to enable **traceable linking among diverse models and code**
- **Language** design, **processing**, and **tooling** techniques that are oriented to achieving high assurance for systems with high levels of capability, modularity, and flexibility
- **Team and supply chain practices** to facilitate composition of assurance in the supply chain
- **Tooling** to support information management, configuration management, and developer/team interaction to support rapid and automatic management of the **chains of evidence linking software code, models, analysis results, etc**
- **Psychology and human factors** for how to build software specification, implementation, verification, analysis, and testing tools that are easy to use and provide positive feedback to users
- **Economics to improve motivation** for use of tools through measurement of improved reliability and security

http://cybersecurity.nitrd.gov/page/designed-in-security

FY15 NITRD
Supplement to the President's Budget

Designed-in Security theme: Develop capabilities to design and evolve high-assurance, software-intensive systems predictably and reliably while effectively managing risk, cost, schedule, quality, and complexity. Create tools and environments that enable the simultaneous development of cyber-secure systems and the associated assurance evidence necessary to prove the system's resistance to vulnerabilities, flaws, and attacks.

Highlight Requests:

- Survivable Systems Engineering – OSD
- Trusted Computing – AFRL, NSA, and OSD
- Software Development Environment for Secure System Software and Applications – ONR
- Roots of Trust – AFRL, NIST, and NSA
- Secure and Trustworthy Cyberspace (SaTC) Program – NSF
- Software Assurance Toolkit (SWAT) – ARL
- Static Tool Analysis Modernization Project (STAMP) – DHS
- Software Assurance Metrics And Tool Evaluation (SAMATE) – DHS and NIST
- Automated Program Analysis for Cybersecurity (APAC) – DARPA
- High-Assurance Cyber Military Systems (HACMS) – DARPA
- Cybersecurity for Energy Delivery Systems (CEDS) Program – DOE/OE
- Programming Computation on Encrypted Data (PROCEED) – AFRL and DARPA

Workshop Background

- Workshop
  - ***Designed-In Security: Current Practices and Research Needs*** (July 1-2, 2013 at SEI Arlington)
- Focused on the **IT hardware and software sectors**, and positioned to respond to the following questions:
  - What procedures are in use in your industry now for designing in security?
  - What processes do you use to identify and validate the best practices in use or that are contemplated for use in your organization?
  - What approaches for designed-in security, beyond those currently in use, would you advocate are ready for industry adoption?
  - What is the evidence to support the approaches use?
  - What hard research problems are in most urgent need of solutions?
- Workshop report available on HCSS Conference Site

Workshop Committee

Martin, Brad	Software	Committee Chair	NSA
Landwehr, Carl	Bus Case	Research Consultant	
Maughan, Douglas		Director, Cyber Security Division	DHS S&T
Newhouse, Bill	Hardware	National Initiative for Cybersecurity Education (NICE) Program Lead, Cybersecurity R&D Coordination	NIST
Scherlis, Bill	Software	Professor & Director, Institute for Software Research (SCS/ISR), School of Computer Science	CMU/SEI
Vagoun, Tomas	Software	Cybersecurity R&D Coordinator	NCO/NITRD
Vishik, Claire	Bus Case	Security & Privacy Technology & Policy Manager	Intel

Software WG

Martin, Brad	Software	Committee Chair	NSA
Scherlis, Bill	Software	Professor & Director, Institute for Software Research (SCS/ISR), School of Computer Science	CMU/SEI
Vagoun, Tomas	Software	Cybersecurity R&D Coordinator	NCO/NITRD
Elder, Matthew	Software	Sr. Manager, Development, Symantec Research Labs	Symantec
Halderman, Alex J.	Software	Assistant Professor, Electrical Engineering and Computer Science	University of Michigan
Kirby, James	Software	SW Engineering Researcher	Navy Research Laboratory
Lardieri, Patrick	Software	Senior Program Manager, Advanced Concepts Laboratory	Lockheed Martin
Lipner, Steve	Software	Partner Director of Program Management, Trustworthy Computing	Microsoft
Rajan, Anand	Software	Manager, Security Research Lab	Intel
Seacord, Robert	Software	Secure Coding Team Lead	SEI
Tinnel, Laura	Software	Senior Research Engineer	SRI International
Weyuker, Elaine	Software	Visiting Scholar, Center for Discrete Mathematics and Theoretical Computer Science & AT&T Labs	Rutgers University
Zurko, Mary Ellen	Software	Security Researcher	Cisco

Hardware WG

Newhouse, Bill	Hardware	National Initiative for Cybersecurity Education (NICE) Program Lead, Cybersecurity R&D Coordination	NIST
Aitken, Rob	Hardware	R&D Fellow	ARM
Anderson, Jim	Hardware	TRUST Technologies Lead, Defense Applications and System Architecture Engineering	Xilinx
Fogerson, Tim	Hardware	Security Engineering Manager	Intel
Jaeger, Trent	Hardware	Professor, Computer Science and Engineering	Pennsylvania State University
Keromytis, Angelos	Hardware	Associate Professor, Computer Science Department	Columbia University
Mijolovic, Simon	Hardware	Solutions Architect	VMware
Ozkaya, Ipek	Hardware	Senior Member of Technical Staff, Architecture Practices	SEI
Perez, Ron	Hardware	Senior Fellow, Senior Director, Security Architecture Organization	AMD
Rao, Josyula	Hardware	Director of Security Research	IBM Research
Reiter, Mike	Hardware	Professor, Department of Computer Science	University of North Carolina

Business Case WG

Landwehr, Carl	Bus Case	Research Consultant	
Vishik, Claire	Bus Case	Security & Privacy Technology & Policy Manager	Intel
Dill, Stephen	Bus Case	LM Fellow, Center for Cyber Security Innovation	Lockheed Martin
Green, Cordell	Bus Case	Director and Chief Scientist	Kestrel Institute
Launchbury, John	Bus Case	Chief Scientist	Galois
Lucero, Scott D.	Bus Case	Deputy Director, Strategic Initiatives	ODASD (Systems Engineering)
McGraw, Gary	Bus Case	CTO	Cigital
Merzbacher, Celia	Bus Case	Vice President, Innovative Partnerships	SRC
Nabil, Adam	Bus Case	Professor, Computer & Information Systems	Rutgers University
Ostrand, Tom	Bus Case	Visiting Scholar, Center for Discrete Mathematics and Theoretical Computer Science & AT&T Labs	Rutgers University
Schmidt, Douglas	Bus Case	Professor, Computer Science	Vanderbilt University
Totah, John	Bus Case	Technical Director in the Office of the CTO	Oracle
van Doorn, Leendert	Bus Case	Corporate Fellow, Corporate VP	AMD

Software Aspects of DIS 1 of 2

- **Software challenges**
  - Growth in criticality – higher assurance, more direct product evaluation
  - Evaluation / C&A – (1) Evolution, (2) variability, (3) components/composition
  - New/changing software ecologies, rapid technological growth, no plateau
- **Software DIS concept**
  - Evidence production throughout lifecycle, incremental and integrated
  - Technical interventions in sync with realities of devt process and tooling
- **Practice**
  - SDL and BSIMM – process + artifact focus, normative best practice
    - Integration into practice and culture – training, tools, etc.
  - Business cases – based on judgment and some measurement
  - Requirements – difficulties with risk-evaluation methodology
  - Technology transitions – modeling and analysis, language, tools, data
    - Software development is now a data-intensive activity ("MSR")
  - Architecture – an essential feature of success and a proprietary dark art
    - Essential roles of APIs, libraries, frameworks, and components
    - Shift from "platform" to "payload" (*ADM Greenert*)

Software Aspects of DIS 2 of 2

- **Research – status**
  - Areas of potential rapid progress – modeling, analysis, tools, language
  - Evidence production ideas are emerging (math) and timely (tools, analytics)
- **Research – opportunities**
  - Technical dimensions – modeling, analysis, tools, language
  - Process integration – SDL, managed code, etc.
  - Human aspects (developer, operator, user) and empiricism
    - Better abstractions, better metaphors, better tools
    - Developers: API design, tooling
    - Improved applicability of empirical methods to evaluate
- **Research – persistent hard problems**
  - Architecture modeling and analysis
  - Components, frameworks, and composition
  - Requirements for security – formulation and validation
- **Technology transition – positive signals**
  - Adoption, data/feedback (glimmerings), incrementality

Hardware Aspects of DIS

- **Hardware Security** – best practices / state-of-the-art
  - Quality: disciplined approach – e.g., process & documentation, design for test/verification/manufacturability, formal methods use, etc.
  - History of successful transition to practice and close academic ties
  - Security: islands of excellence focused on "security" products or specific capabilities/features, market segments – e.g., compliance
  - Requirements proliferating – e.g., "*high assurance,*" side-channel, etc.
- **Opportunities for Research**
  - "*Design for Security*": leverage strengths in quality, verification, formal methods – e.g., HW equivalents for SDL & BSIMM
  - Architecture & design: understanding and expressing/specifying security properties – e.g., privilege separation & least privilege
  - Systems approach: hardware/software security co-design, cycle-time & "*verticalization,*" TCB reduction, HW reference monitors, attestation & authentication, provenance, policy enforcement, etc.

Hardware Aspects of DIS

New Govt-Industry Program to Address Hardware-Oriented Security

- NSF SaTC program supports research broadly
- SRC Trustworthy and Secure Semiconductors & Systems (T3S) established
  - To develop strategies and tools to affordably enable design & manufacture chips and systems that are secure, trustworthy, assured, and resilient and resistant to attack or counterfeiting.
  - Membership open to any interested company; initial participants: AMD, Freescale, Intel, and Mentor Graphics
- T3S & NSF co-funding Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) program
  - Up to $500K over 3 years
  - Review and selection in progress; research planned to start before end of fiscal year.

Business Case Aspects of DIS

- Why make the investment in something that adds cost & time to development? ROI & risk factors include:
  - Loss of IP/sales (theft or counterfeits)
  - Damage to brand
  - Customer demand/requirement vs. unstated expectation
- Lack of measures of "security" is a barrier to investment
- Government requirements could drive broader demand
- Security research relevant to business decision making:
  - Techniques for reducing time/cost of designed-in security
  - Economic impact of inadequate security in various systems
  - Security in new environments, e.g. BYOD and social networks
  - Risk and resilience analysis

Future Steps & Discussion

- Contact information
  - Brad Martin: wbmarti@nsa.gov
  - William Scherlis: scherlis@cmu.edu
  - Ron Perez: ron.perez@amd.com
  - Celia Merzbacher: merzbacher@src.org