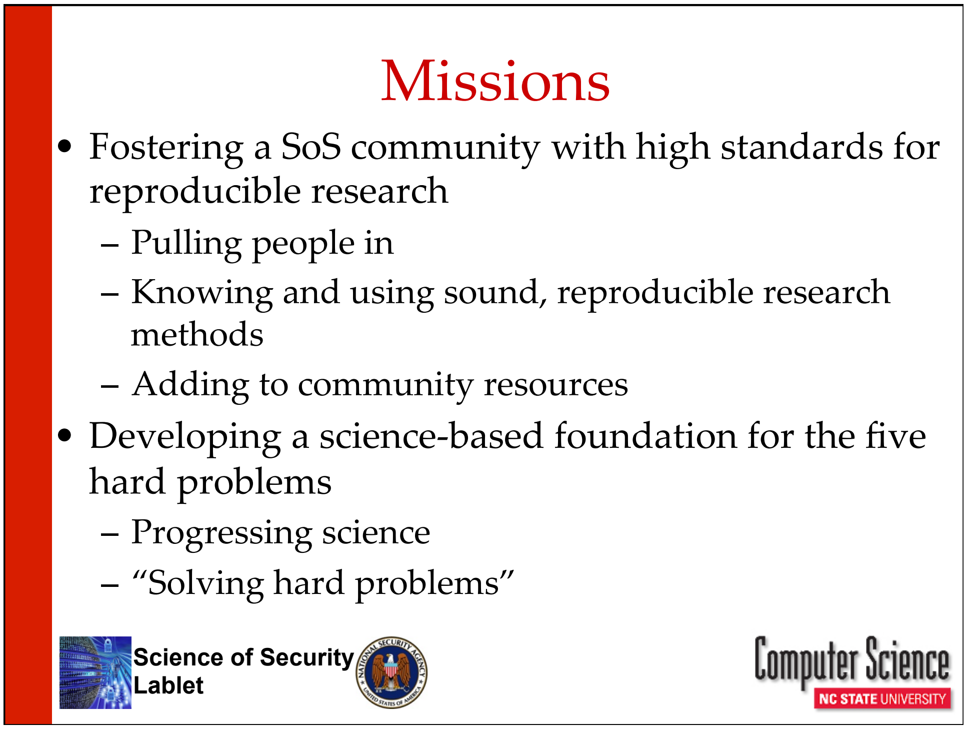
NCSU Update

Laurie Williams
Munindar Singh

Who are we now?

- 16 supported NCSU faculty; 18 supported NCSU students
- Multi-disciplinary: 4 NCSU colleges
  - Engineering (Comp Science, ECE, **Civil**); **Psychology; Education**; Statistics
- 6 collaborating university partners
  - Purdue, UNC-CH, UNC-C, Alabama, **RIT, University of Virginia**
- **Established "team captains" for each hard problem**

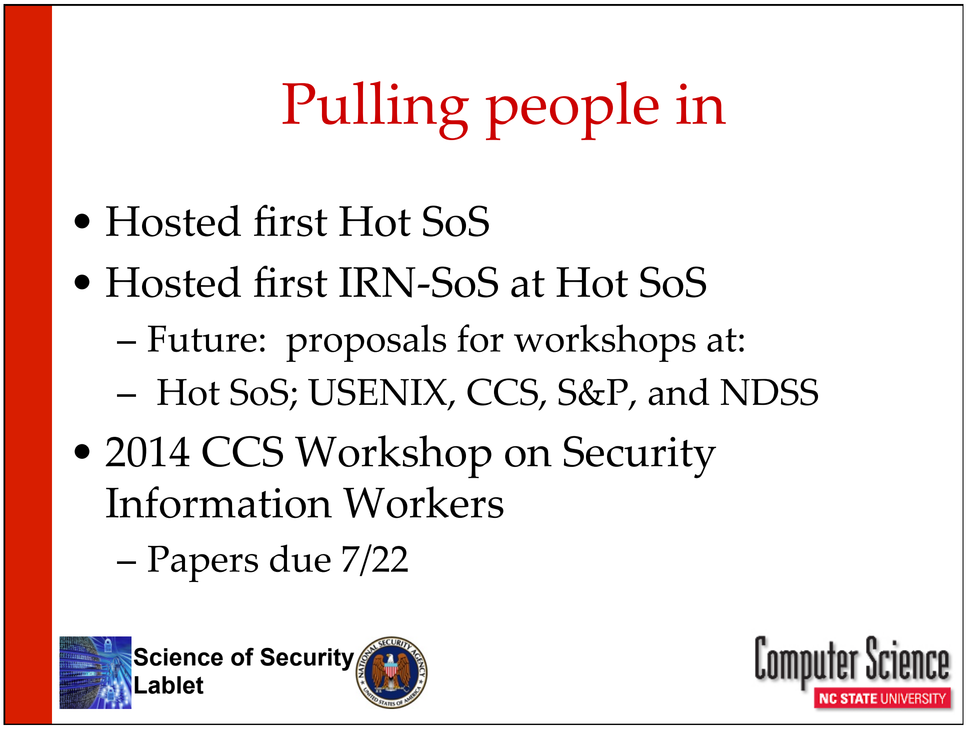


Missions

- Fostering a SoS community with high standards for reproducible research
  - Pulling people in
  - Knowing and using sound, reproducible research methods
  - Adding to community resources
- Developing a science-based foundation for the five hard problems
  - Progressing science
  - "Solving hard problems"

Science of Security Lablet

Computer Science NC STATE UNIVERSITY

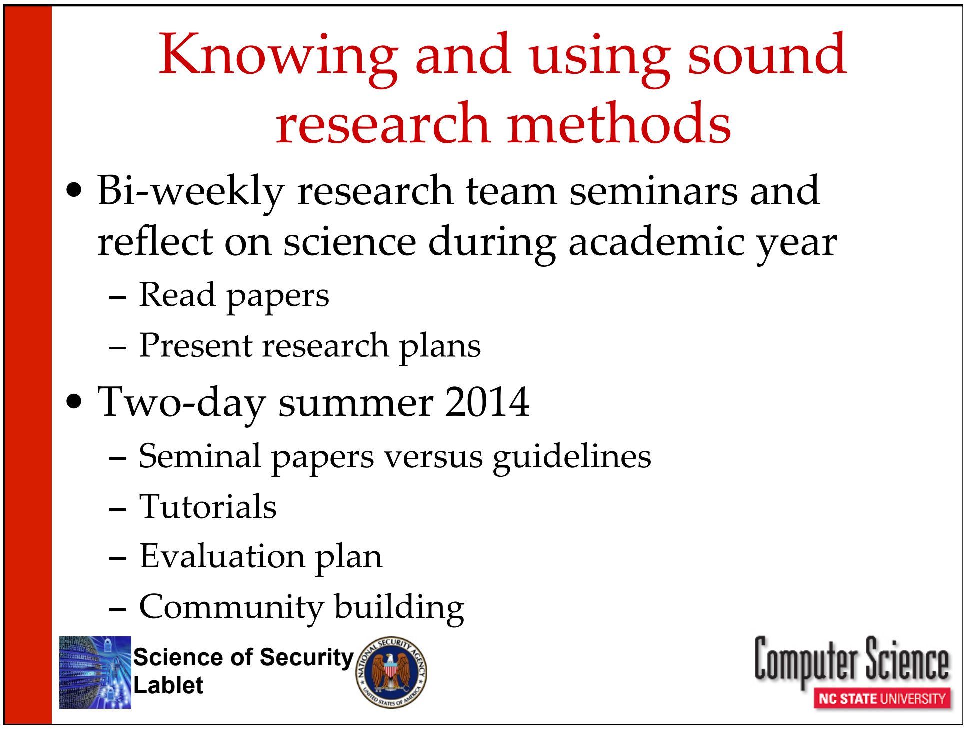


Pulling people in

- Hosted first Hot SoS
- Hosted first IRN-SoS at Hot SoS
  - Future: proposals for workshops at:
  - Hot SoS; USENIX, CCS, S&P, and NDSS
- 2014 CCS Workshop on Security Information Workers
  - Papers due 7/22

Science of Security Lablet

Computer Science NC STATE UNIVERSITY

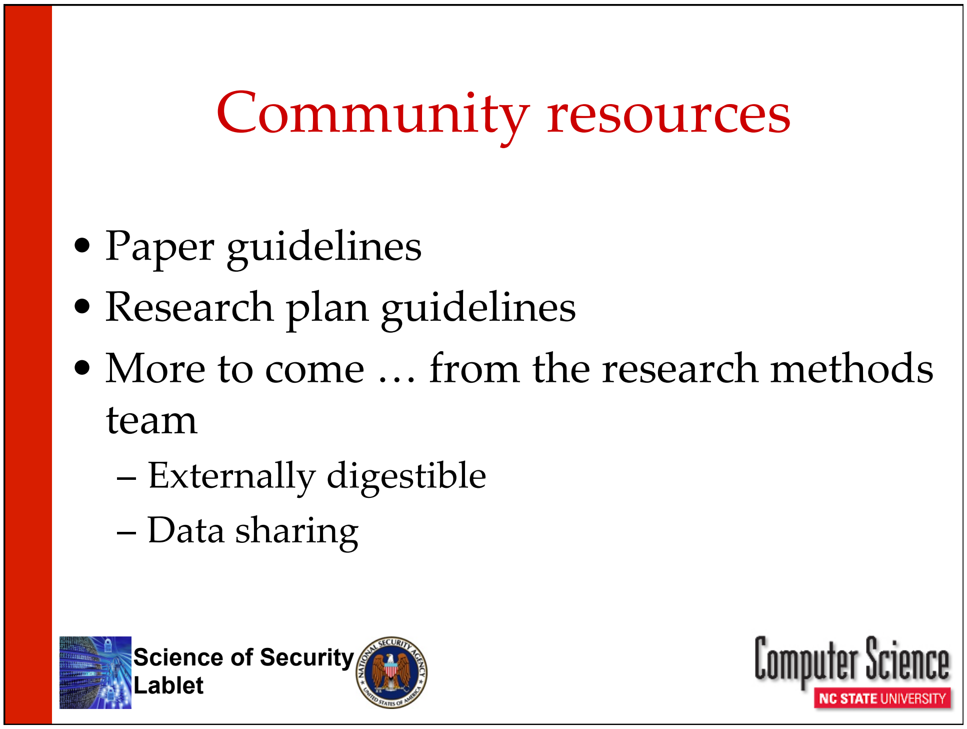


Knowing and using sound research methods

- Bi-weekly research team seminars and reflect on science during academic year
  - Read papers
  - Present research plans
- Two-day summer 2014
  - Seminal papers versus guidelines
  - Tutorials
  - Evaluation plan
  - Community building

Science of Security Lablet

Computer Science NC STATE UNIVERSITY

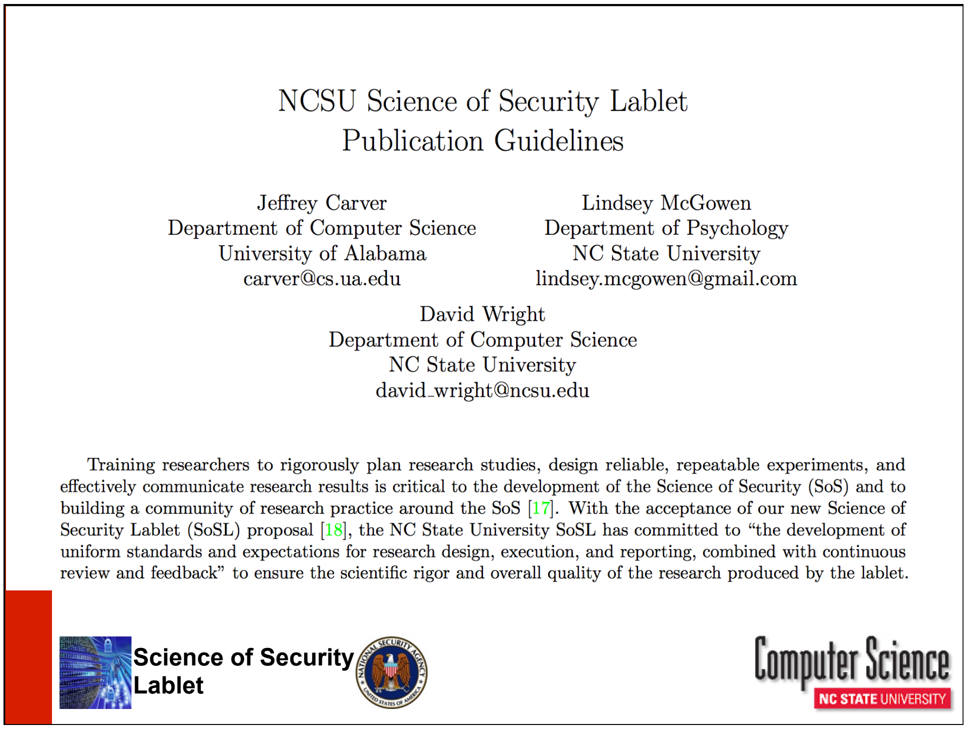


Community resources

- Paper guidelines
- Research plan guidelines
- More to come … from the research methods team
  - Externally digestible
  - Data sharing

Science of Security Lablet

Computer Science NC STATE UNIVERSITY



NCSU Science of Security Lablet Publication Guidelines

Jeffrey Carver
Department of Computer Science
University of Alabama
carver@cs.ua.edu

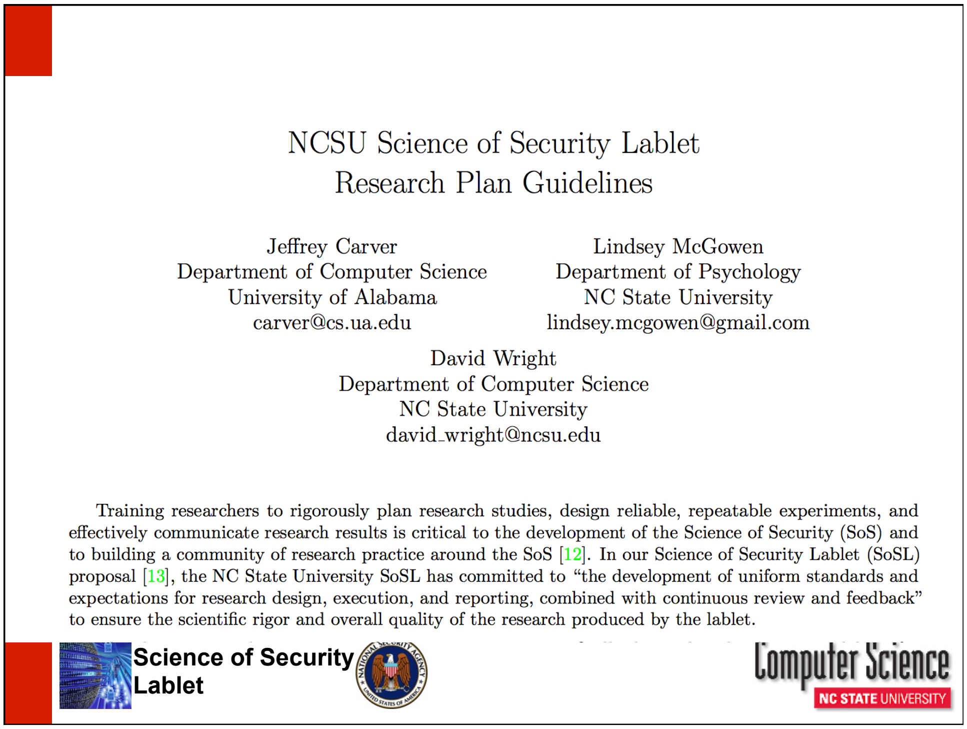
Lindsey McGowen
Department of Psychology
NC State University
lindsey.mcgowen@gmail.com

David Wright
Department of Computer Science
NC State University
david_wright@ncsu.edu

Training researchers to rigorously plan research studies, design reliable, repeatable experiments, and effectively communicate research results is critical to the development of the Science of Security (SoS) and to building a community of research practice around the SoS [17]. With the acceptance of our new Science of Security Lablet (SoSL) proposal [18], the NC State University SoSL has committed to "the development of uniform standards and expectations for research design, execution, and reporting, combined with continuous review and feedback" to ensure the scientific rigor and overall quality of the research produced by the lablet.

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY



NCSU Science of Security Lablet Research Plan Guidelines

Jeffrey Carver
Department of Computer Science
University of Alabama
carver@cs.ua.edu

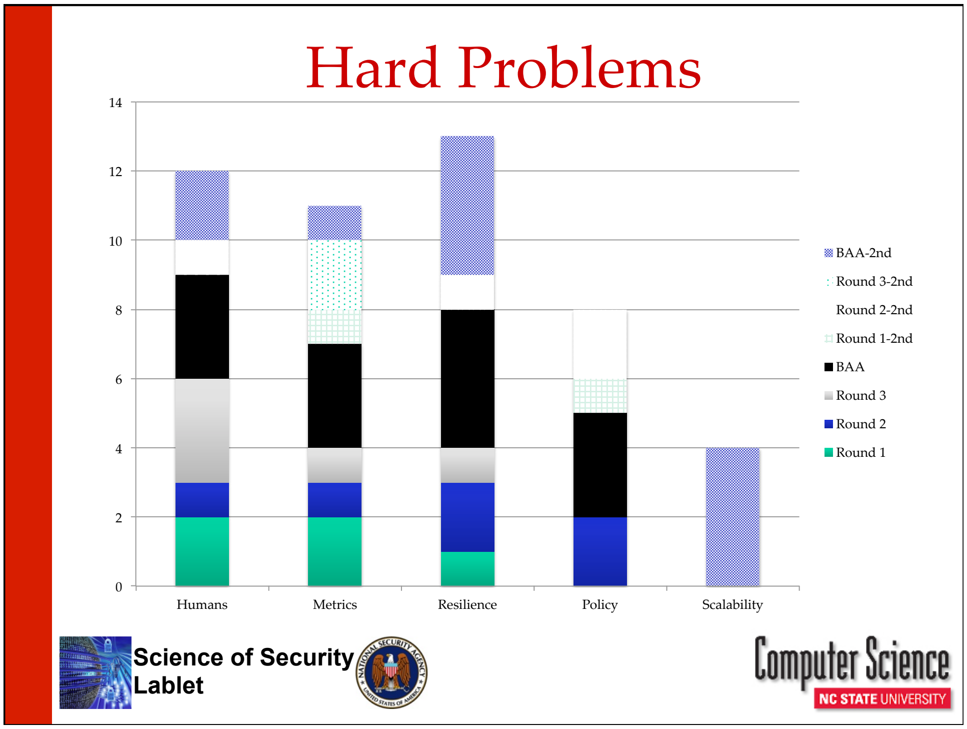
Lindsey McGowen
Department of Psychology
NC State University
lindsey.mcgowen@gmail.com

David Wright
Department of Computer Science
NC State University
david_wright@ncsu.edu

Training researchers to rigorously plan research studies, design reliable, repeatable experiments, and effectively communicate research results is critical to the development of the Science of Security (SoS) and to building a community of research practice around the SoS [12]. In our Science of Security Lablet (SoSL) proposal [13], the NC State University SoSL has committed to "the development of uniform standards and expectations for research design, execution, and reporting, combined with continuous review and feedback" to ensure the scientific rigor and overall quality of the research produced by the lablet.

Science of Security Lablet

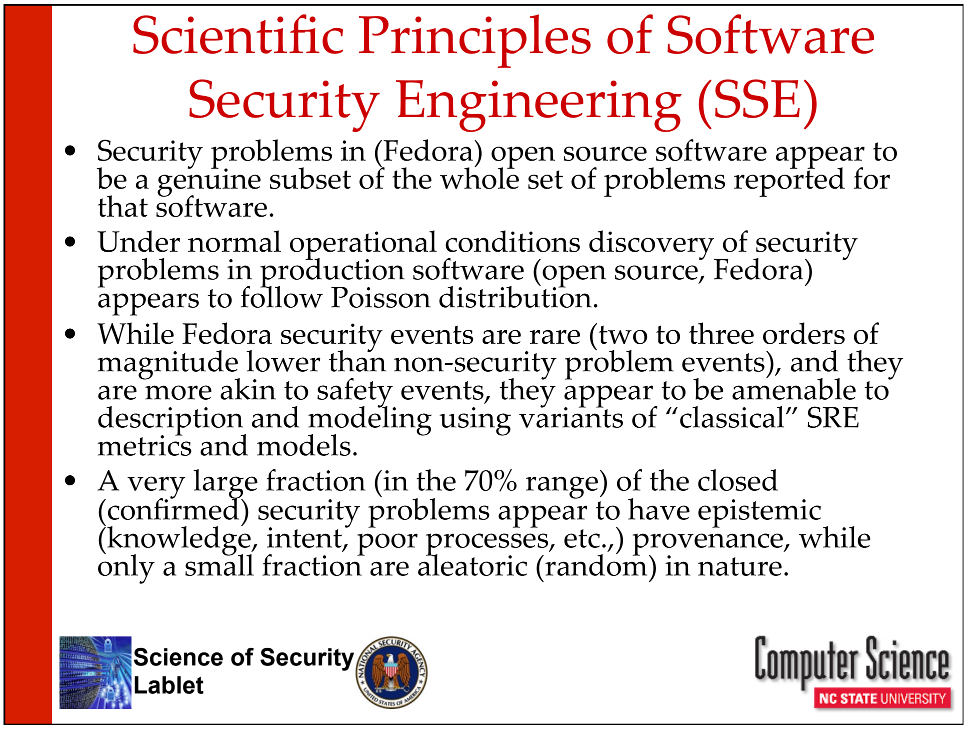
Computer Science
NC STATE UNIVERSITY



Hard Problems

Science of Security Lablet

Computer Science NC STATE UNIVERSITY



Scientific Principles of Software Security Engineering (SSE)

- Security problems in (Fedora) open source software appear to be a genuine subset of the whole set of problems reported for that software.
- Under normal operational conditions discovery of security problems in production software (open source, Fedora) appears to follow Poisson distribution.
- While Fedora security events are rare (two to three orders of magnitude lower than non-security problem events), and they are more akin to safety events, they appear to be amenable to description and modeling using variants of “classical” SRE metrics and models.
- A very large fraction (in the 70% range) of the closed (confirmed) security problems appear to have epistemic (knowledge, intent, poor processes, etc.,) provenance, while only a small fraction are aleatoric (random) in nature.

Science of Security Lablet

Computer Science NC STATE UNIVERSITY

SSE Continued …

- While that means that it is easier to construct reliable attack profiles (bad news),
- But … it is also true that improved software engineering practices and testing automation may be able to eliminate a large fraction of the security problems in this type of software (good news).
- Work will be done to rigorously confirm validity (assumptions, statistical conditions, predictive power, …) that would allow us to use classical or modified classical software reliability models and metrics (including risk metrics) in the security context
- Multiple contexts will be studied to examine generalizability.

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY

An Adoption Theory of Secure Development Tools

Recent Work:

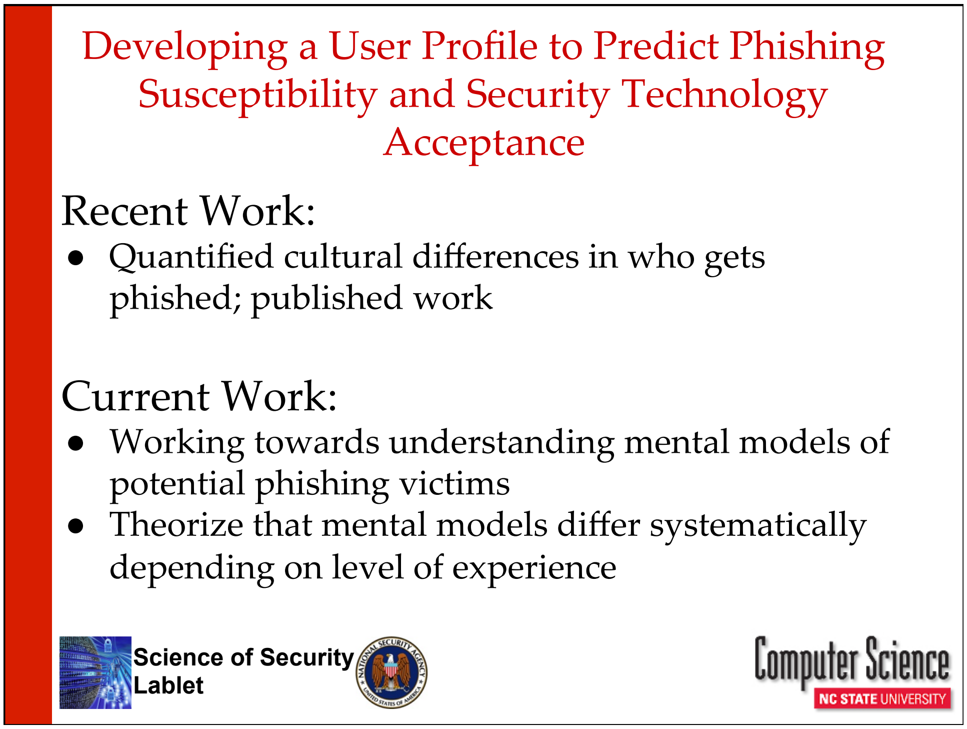
- Quantified theory through several hundred surveys deployed software developers

Current Work:

- Working towards measuring improvement in adoption by applying theory
- Building persuasive intervention in the form of automatically-generated tool recommendations to open source developers

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY



Developing a User Profile to Predict Phishing Susceptibility and Security Technology Acceptance

Recent Work:

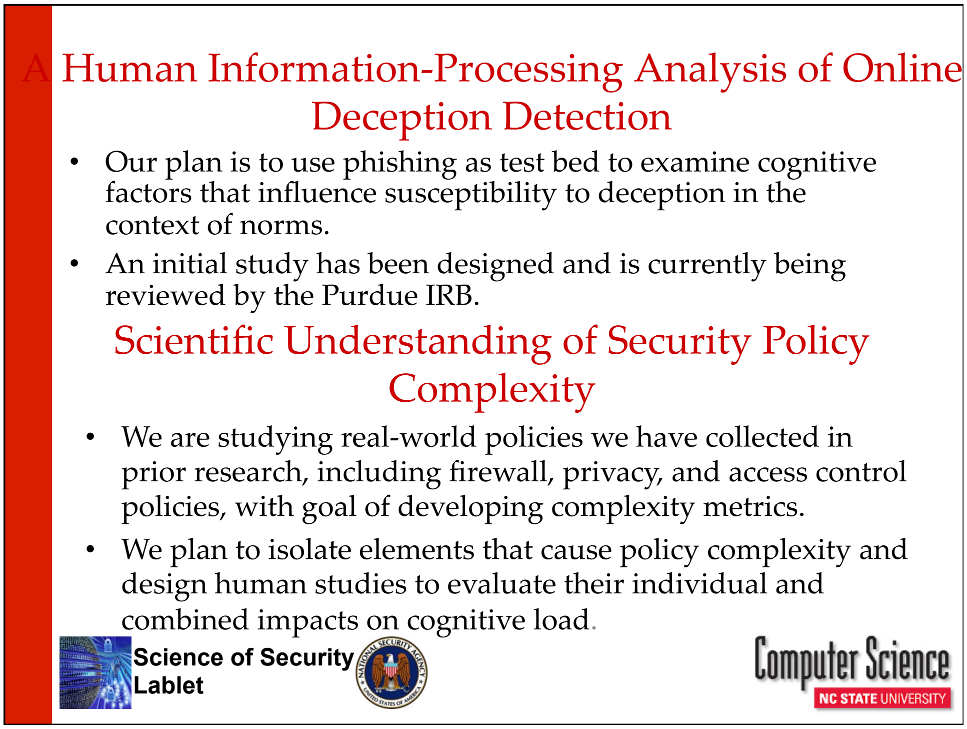
- Quantified cultural differences in who gets phished; published work

Current Work:

- Working towards understanding mental models of potential phishing victims
- Theorize that mental models differ systematically depending on level of experience

Science of Security Lablet

Computer Science NC STATE UNIVERSITY



A Human Information-Processing Analysis of Online Deception Detection

- Our plan is to use phishing as test bed to examine cognitive factors that influence susceptibility to deception in the context of norms.
- An initial study has been designed and is currently being reviewed by the Purdue IRB.

Scientific Understanding of Security Policy Complexity

- We are studying real-world policies we have collected in prior research, including firewall, privacy, and access control policies, with goal of developing complexity metrics.
- We plan to isolate elements that cause policy complexity and design human studies to evaluate their individual and combined impacts on cognitive load.

Science of Security Lablet

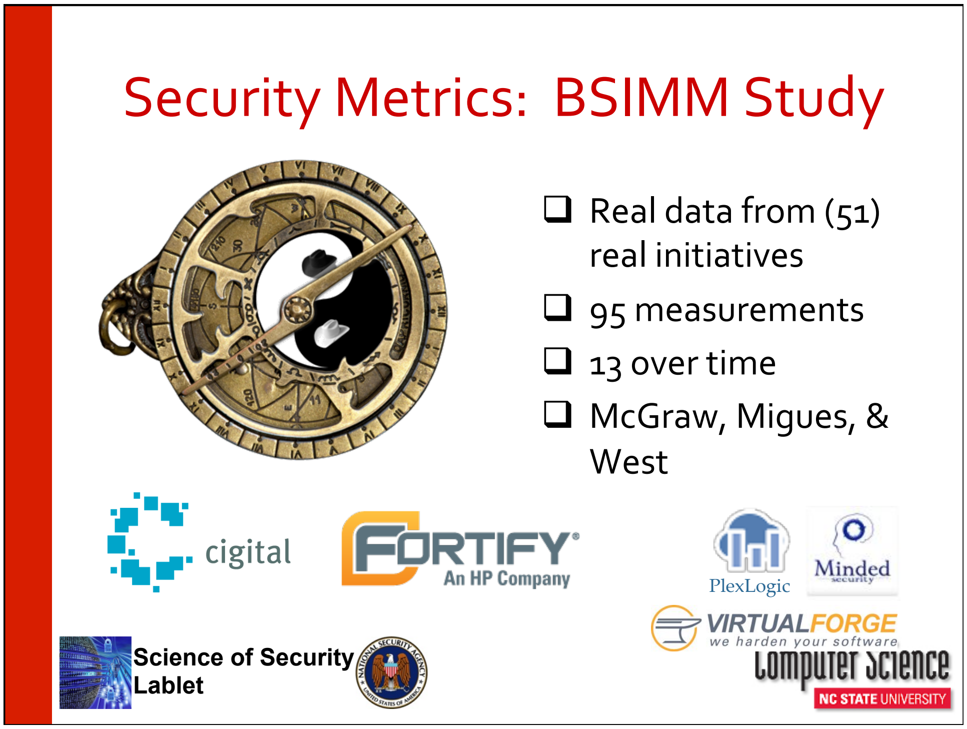
Computer Science NC STATE UNIVERSITY

Towards a Scientific Basis for User Centric Security Design

- We have completed several experiments showing the value of a summary risk index in app selection decisions.
- The results have shown that presenting the information in the form of amount of safety is more effective.
- A paper on this topic is to be presented at the annual meeting of the Human Factors and Ergonomics Society, and manuscripts are submitted to the *Journal of Cognitive Engineering and Decision Making* and *Human Factors*.
- We have conducted studies with security experts and novices to identify the dimensions of risk that they perceive as important, with the goal of developing a multidimensional risk index for app permissions.

Understanding Effects of Norms and Policies on the Robustness, Liveness, and Resilience of Systems

- Develop multi-agent system to simulate interactions of users, administrators, and policy-makers.
  - Example: PCs in a computer lab
    - Actors: Users, administrators
    - Technical artifacts: PCs, antivirus updates, password health, file system
    - Actors express norms
      - comply with antivirus and password policies
    - Security of lab may degrade or improve dynamically
- Explore definitions of security and policy properties to analyze the multi-agent simulations.



Security Metrics: BSIMM Study

- ❑ Real data from (51) real initiatives
- ❑ 95 measurements
- ❑ 13 over time
- ❑ McGraw, Migues, & West

cigital

FORTIFY An HP Company

PlexLogic

Minded security

VIRTUALFORGE we harden your software

Science of Security Lablet

Computer Science NC STATE UNIVERSITY

51 Firms in the BSIMM Community

Adobe

Google

SAP

VISA

rackspace

AON

F-Secure

SallieMae

WELLS FARGO

box

Fidelity INVESTMENTS

scrippsnetworks interactive

zynga

Intel

Bank of America

JPMORGAN CHASE & CO.

SWIFT

STANDARD LIFE

Intuit

Capital One

The image cannot be displayed. Your computer may not have enough

QUALCOMM

THOMSON REUTERS

Nokia Siemens Networks

salesforce.com

FannieMae

DTCC The Depository Trust & Clearing Corporation

Symantec.

vmware

Microsoft

Sony Mobile

EMC² where information lives

of

NOKIA Connecting People

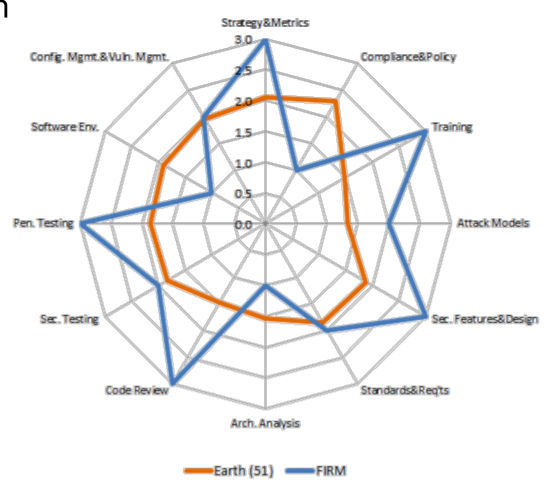
TELECOM ITALIA

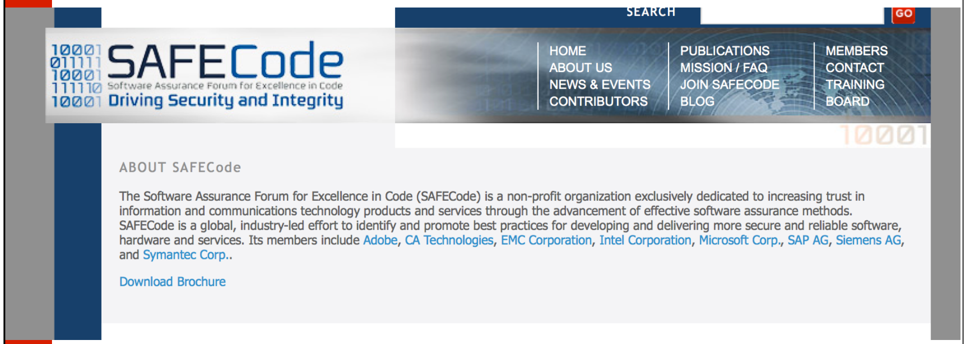
Plus 17 firms that remain anonymous

Computer Science NC STATE UNIVERSITY

BSIMM as a Measuring Stick

- ❑ Compare a firm with peers using the high water mark view
- ❑ Compare business units
- ❑ Chart an SSI over time

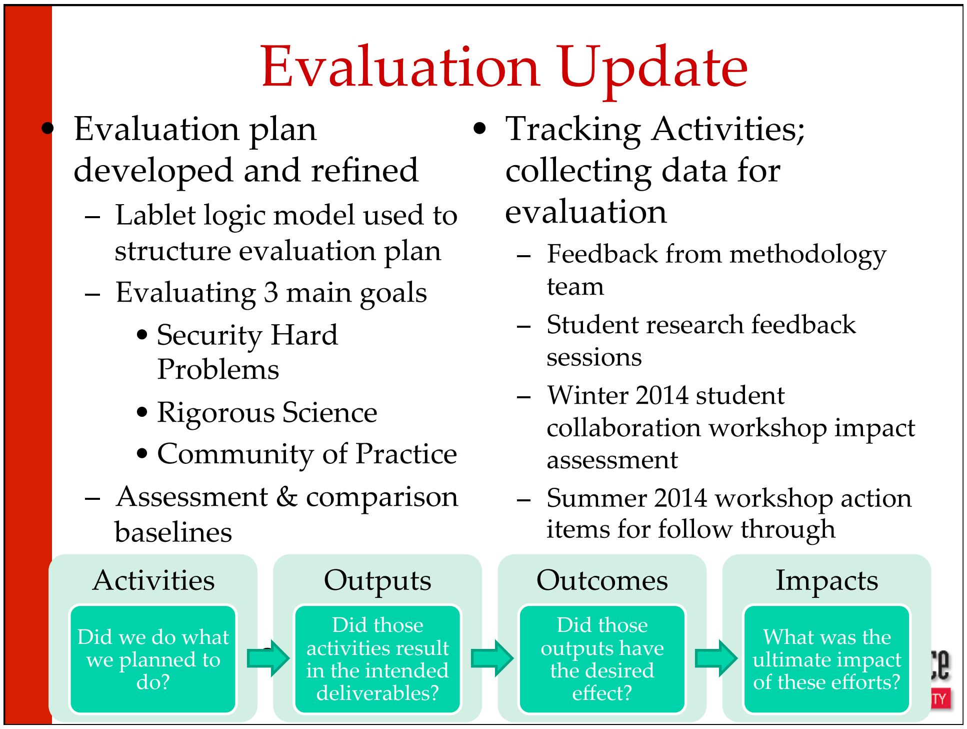




ABOUT SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe, CA Technologies, EMC Corporation, Intel Corporation, Microsoft Corp., SAP AG, Siemens AG, and Symantec Corp..

Download Brochure



Evaluation Update

- Evaluation plan developed and refined
  - Lablet logic model used to structure evaluation plan
  - Evaluating 3 main goals
    - Security Hard Problems
    - Rigorous Science
    - Community of Practice
  - Assessment & comparison baselines
- Tracking Activities; collecting data for evaluation
  - Feedback from methodology team
  - Student research feedback sessions
  - Winter 2014 student collaboration workshop impact assessment
  - Summer 2014 workshop action items for follow through

Activities

Did we do what we planned to do?

Outputs

Did those activities result in the intended deliverables?

Outcomes

Did those outputs have the desired effect?

Impacts

What was the ultimate impact of these efforts?