NCSU Update

Laurie Williams
Munindar Singh

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY

Resiliency Hard Problem - 1

- **Vulnerability and Resilience Prediction Models**
  - Use of data-flow based soft detectors based on provenance information tracking to recognize data-flow attacks.
  - Use of back-to-back comparison attack detectors.
  - Conducted a survey of Platform-as-a-Service (PaaS) vulnerability categories and the corresponding countermeasures
    - Our future focus: input validation, remote access validation and data integrity issue

Resiliency Hard Problem - 2

- **Redundancy for Network Intrusion Prevention Systems (NIPS)**
  - Goal: Scalable enforcement of network security policies that is resilient to traffic changes and traffic rerouting in response to failures
  - Identifying patterns that are common to a variety of diverse software-defined network (SDN) optimization problems and then by leveraging these patterns to expand our existing programming APIs to support development of SDN optimization applications.
  - Recent focus on optimization applications that involve more inherent uncertainty

Resiliency Hard Problem - 3

- **Resilience Requirements, Design, and Testing**
  - Formalized reusable framework for specifying, reasoning about, verifying, and certifying a broad range of system properties, including security resiliency.
    - Framework is parameterized by a range of "little languages" for specifying detailed properties, including security resiliency.
    - Developing property-specific formal language for resiliency specification.
  - Assessment of security problems in open source software. Non-operational testing can help accelerate and focus security problem discovery rate and it can be successfully modeled.

Resiliency Hard Problem - 4

- **Smart Isolation in Large-Scale Production Computing Infrastructures**
  - Creation and validation of a classification system of existing security isolation techniques, through which we will identify underlying design principles and tradeoffs that will lead to the design of next generation smart isolation techniques to support resilient architectures.
  - Survey paper
    - existing security isolation techniques fall short in terms of adaptability and measurability.
    - information flow control (IFC) can provide a form of smart isolation

Policy Hard Problem - 1

- **Formal Specification and Analysis of Security-Critical Norms and Policies**
  - Norms: standards of correct collaborative behavior
  - Policies: ways of achieving different collaborative behaviors
  - Created a formal model for conditional norms that includes a model of branching time and relates norms to primitives used for declarative information stores.
  - This model provides a basis for deciding when a norm is satisfied or violated.
  - This model prepares us to study norm conflicts and express situational preferences.

Policy Hard Problem - 2

- **Scientific Understanding of Policy Complexity**
  - Human-subject study on comprehension of firewall policies presented in different forms.
  - Our proposed modular language for expressing firewall policies yields enhanced comprehension over traditional representations.

Humans Hard Problem - 1

- **Warning of Phishing Attacks: Supporting Human Information Processing, Identifying Phishing Deception Indicators, and Reducing Vulnerability**
  - Experts construct significantly richer mental models (with greater links between concepts) than novices.
  - This finding will be applied to phishing vulnerability and the effectiveness of phishing training.

Humans Hard Problem - 2

- **A Human Information-Processing Analysis of Online Deception Detection**
  - Improved the phishing warning interface
    - Explicit mention of "Phishing" in the main page of the warning; a "Stop" sign highlighted the recommended "stopping" action; ranking examples of popular websites were provided as a reference; etc.
  - Three-week field phishing study using an e-commerce scenario.
    - Those who got warning did not enter in account info

Humans Hard Problem - 3

- **Leveraging the Effects of Cognitive Function on Input Device Analytics to Improve Security**
  - Goal is creating "Human Subtlety Proofs" (HSPs) to enable accurate differentiation between intended and unintended usage of a system during a controlled task interaction.
    - Eye tracking
    - Typing

Metrics Hard Problem - 1

- **Attack Surface and Defense-in-Depth Metrics**
  - We studied Designed Defenses, helping us understand how developers interact with parts of the system designed to aid with defensive coding.
  - A Designed Defense is a function whose explicit purpose is defensive coding, such as a utility function that wrap around memory management functions like malloc() to mitigate memory corruption.
  - We have used crash dumps as an approximation of the attack surface of a system
    - Prioritization
    - Prediction

Metrics Hard Problem - 2

- **Systematization of Knowledge from Intrusion Detection Models**
  - We progressed further on our collaborative systematic literature review of intrusion detection metrics.
  - Utilizing a taxonomy of: threshold-based approach, learning-based approach, detection-theory based approach, and compression-based approach.

Team Science: Past Year

- 20 publications … 9 under review
  - 55 authors
  - 13 institutions

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY

Building our Science Muscles

- Bi-weekly seminars
  - 18 supported students presented in Fall 2014/ Spring 2015
    - Research plans
    - Conference presentations
    - Paper submissions
- Summer 2015 workshop
  - Template evaluation and customization
  - Paper evaluation
  - Tutorials

Science of Security Lablet

Computer Science
NC STATE UNIVERSITY

Community Development

- IRN-SoS session at Hot SoS 2015
  - *What Should be Included in a Methodologically Science of Security Paper?*
- RTP Community Meeting
  - October 2014
  - October 29, 2015

Science of Privacy

- June 23-24, 2015
- Host of NSA-sponsored planning meeting
- Among discussions of privacy …
  - … shared hard problem strategy
  - … shared our focus on research methods