NCSU Science of Security Lablet

Highlights at the Quarterly Meeting

Munindar P. Singh
singh@ncsu.edu

Department of Computer Science
North Carolina State University

November 2016

Leveraging the Effects of Cognitive Function on Input Device Analytics to Improve Security

Hard Problem: Humans

- PIs: David L. Roberts, Robert St. Amant
- Researchers: Alok Goel, Ignacio X. Dominguez, Jayant Dhawan
- Synopsis
  - Understanding basic principles of human behavior through observations of input device usage to enable characterizing risk and identifying malicious (or accidental) misuses
  - Develop a novel class of security proofs that we call "Human Subtlety Proofs" that are both unobtrusive and interactive
- Recent finding or other outcome
  - Develop a tool for visualizing cognitive phenomena during user interface interaction as a way to acquire evidence of effect on device usage, yielding key metrics for changes in cognition that reflect changes in task-completion strategies that may reflect risky behavior
- NSA research keywords: Anomaly detection

A Human Information-Processing Analysis of Online Deception Detection

Hard Problem: Humans

- PIs: Robert Proctor, Ninghui Li
- Researchers: Jing Che, Weining Yang, Aiping Xiong, Wanling Zou
- Synopsis
  - Developing a cognitive model of user decision making processes as a basis for predicting individual users' judgments and decisions regarding online deception, specifically, phishing attacks
- Recent finding or other outcome
  - An empirical evaluation shows that a decision-aid tool developed according to our approach that incorporates training yields greater persistence of learning; specifically, users who were trained through our tool were better able to resist phishing attacks than the current Chrome phishing warning even a week after training
  - A study of human trust in automation found that higher automation reliability increased overall quality of user decisions and their self-reported trust; improved descriptions yielding greater trust
- NSA research keywords: Phishing

Warning of Phishing Attacks

Hard Problem: Humans

- PIs: Christopher Mayhorn, Emerson Murphy-Hill
- Researchers: Allaire Welk, Olga Zielinska
- Synopsis
  - Understand how mental models vary between novice users, experts (such as IT professionals), and hackers to help build software that reduces user vulnerability to phishing
  - Map out the mental models that underlie security decision making to inform behavioral models of users, security experts, and adversaries
- Recent findings or other outcomes
  - Attacker studies (887 hand-curated phishing emails from 2010–2015)
    - Attacks employ classic persuasion techniques (e.g., Cialdini's commitment-consistency and scarcity)
  - User studies (155 users)
    - Almost everyone is susceptible: over 90% make errors
    - Cognition, e.g., attention and working memory, predicts lower susceptibility (small effect)
    - Socioemotional factors—reservation (being able to keep emotions under control), distrust, financial loss—lead to reduced susceptibility
- NSA research keywords: Phishing

Scientific Understanding of Policy Complexity

Hard Problem: Policy (primary); Humans

- PIs: Ninghui Li, Robert Proctor, Emerson Murphy-Hill
- Researchers: Jing Chen, Haining Chen, Huangyi Ge, Matt Witte
- Synopsis
  - Develop two measures for a policy's (1) *inherent complexity* and (2) *representational complexity*, which depends upon a particular way of encoding the policy
- Recent finding or other outcome
  - An approach, realized in a tool, extracts SEAndroid policy to support such analysis of policy misconfigurations in SEAndroid due to unexpected composition of valid policies, e.g.,
    - *write* allows writing to a file opened by another program
    - *open, read* allows reading but not writing a file
    - Combination allows changing or deleting the file
- NSA research keywords: Secure programming

Formal Specification and Analysis of Security-Critical Norms and Policies

Hard Problem: Policy (primary); Scalability and Composability

- PIs: Rada Y. Chirkova, Jon Doyle, Munindar P. Singh
- Researchers: Nirav Ajmeri, Jiaming Jiang, Ozgur Kafali
- Collaborators: Amit Chopra
- Synopsis
  - Understand how to specify and analyze norms (standards of correct collaborative behavior) and policies (ways of achieving behaviors) to determine properties such as mutual consistency
  - Facilitate the composition of collaborative systems by combining sets of norms and policies, and verifying whether they satisfy desired properties
- Recent finding or other outcome
  - Reasoning at runtime about conflicts between commitments, authorizations, and prohibitions to help achieve secure collaboration
  - Developed a mapping from norm schemas to relational (SQL) queries to compute the lifecycle states of norm instances from the underlying relational information stores
- NSA research keywords: Access control

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

Hard Problem: Policy (primary); Resilient Architectures

- PIs: Emily Berglund, Jon Doyle, Munindar Singh
- Researchers: Shams Al Amin, Nirav Ajmeri
- Collaborators: Mehdi Mashayekhi
- Synopsis
  - Understand computational norms as standards of correctness for collaborative behavior, with respect to which policies of the participants can be evaluated individually or in groups
  - Study robustness and resilience of systems modeled in terms of norms to understand resilience in social architectures
- Recent finding or other outcome
  - Simulated norm-based regulation in sociotechnical systems (with constrained autonomy); our approach shows that norms emerge that reduce the overhead of sharing and promote fairness
  - (In progress) a conceptual model of a software development organization for studying the effects of norms pertaining to training and adoption of security-enhancing software development tools
- NSA research keywords: Simulation, workforce training

Privacy Incidents Database

Hard Problem: Policy

- PIs: Jessica Staddon
- Researchers: Esha Sharma
- Collaborators: Pradeep Murukannaiah
- Synopsis
  - Scientific study of privacy is hindered by a lack of curated datasets of privacy incidents
  - Security incidents often don't involve privacy and privacy loss can occur without a security incident
  - Developing a privacy incidents database
    - Conceptual model
    - Manual labor
    - Automated analysis of public media (e.g., newspapers)
- Recent finding or other outcome
  - This project is building the repository to enable the identification of patterns in incident root causes, entities, location, and so on, that will inform product and policy development and privacy training
- NSA research keywords: Privacy

Attack Surface and Defense-in-Depth Metrics

Hard Problem: Metrics (primary); Scalability and Composability; Resilient Architectures

- PIs: Andy Meneely, Laurie Williams, Munindar P. Singh
- Researchers: Nuthan Munaiah, Jason King, Chris Theisen, Ozgur Kafali
- Synopsis
  - Develop and analyze metrics that quantify the "shape" of a system's attack surface
  - Uses call graph data beyond the attack surface to determine the risk of a given entry point
  - Analyze a large system in terms of their inputs and outputs, providing information on its architecture
- Recent finding or other outcome
  - Substantial improvements in predicting vulnerabilities at the method level by using random walks on call graphs over baseline model based on source code
  - Investigation of the 1,577 healthcare breaches reported by the HHS revealed that 44% of them are misuses
  - Lack of coverage of such breaches by HIPAA policies
- NSA research keywords: Insider threat, secure programming

Systematization of Knowledge from Intrusion Detection Models

Hard Problem: Metrics (primary); Resilient Architectures; Scalability and Composability

- PIs: Huaiyu Dai, Andy Meneely
- Researchers: Xiaofan He, Yufan Huang, Richeng Jin, Nuthan Munaiah, Kevin Campusano Gonzalez
- Synopsis
  - Establish common criteria for evaluating and systematizing knowledge contributed by research on intrusion detection models
- Recent finding or other outcome
  - Our results show systemic inconsistency over time of critical evaluation metrics, demonstrating a lot of concerns we have had about the validity of most IDS studies
- NSA research keywords: Anomaly detection

Vulnerability and Resilience Prediction Models

Hard Problem: Metrics (primary); Resilient Architectures; Scalability and Composability

- PIs: Mladen Vouk, Laurie Williams
- Researchers: Donghoon Kim, Akond Rahman
- Synopsis
  - Recognition of attacks through metrics and models of software vulnerabilities
  - Models to predict resilience to attacks in the field
- Recent finding or other outcome
  - Existing experience in engineering high-assurance software with rare defects can be adapted to avoid, eliminate, and tolerate security vulnerabilities
  - Security problem avoidance, elimination, and fault tolerance are improved through enhanced safety-related knowledge in guiding security-sensitive software development, testing, acquisition, use, and maintenance
- NSA research keywords: Secure programming

Smart Isolation in Large-Scale Production Computing Infrastructures

Hard Problem: Resilient Architectures

- PIs: Xiaohui (Helen) Gu, William Enck
- Researchers: Rui Shu, Adwait Nadkarni, Luke Deshotels
- Synopsis
  - Creation and validation of a classification system of existing security isolation techniques
  - Identification of design principles and tradeoffs that will lead to the design of next generation smart isolation techniques to support resilient architectures
- Recent finding or other outcome
  - Analysis of 350,000 images on Docker Hub from nearly 100,000 repositories
  - About 100 vulnerabilities per image on average
  - 90% images have a high-severity vulnerability
  - Vulnerabilities commonly propagate from parent to children images
- NSA research keywords: Sandboxes

Redundancy for Network Intrusion Prevention Systems (NIPS)

Hard Problem: Resilient Architectures

- PIs: Mike Reiter
- Researchers: Victor Heorhiadi, Jun Jiang
- Collaborators:
- Synopsis
  - Developing an architecture for the scalable enforcement of network security policies that is resilient to traffic changes and traffic rerouting in response to failures
- Recent finding or other outcome
  - A programming framework that supports the expression of high-level policy requirements
  - Automated configuration of networking components to satisfy those requirements in ways that optimize desired performance goals
- NSA research keywords: Policies, firewalls

Resilience Requirements, Design, and Testing

Hard Problem: Resilient Architectures (primary); Metrics

- PIs: Kevin Sullivan, Mladen Vouk, Ehab Al-Shaer
- Researchers: Ghaith Husari, Mohamed Alsaleh, Anoosha Vangaveeti, Chong Tang
- Synopsis
  - Develop metrics as a basis for characterizing the attack-resiliency of software system to enable testing and implementation, and to promote strategies that effectively deal with vulnerabilities
  - Development of metrics and models for static and dynamic assessment of resilience of software
- Recent finding or other outcome
  - Defined two resiliency metrics: (1) *isolation* to quantify the counter-measure resistance on any path based on the network access controls including firewalls, IPSec, IDS, and proxies; and (2) *diversity* to quantify the gains from disjointness of attack surface due to OS and application diversity; integrated these metrics to determine the optimal isolation-diversity combination for multistage attacks
- NSA research keywords: Mitigation

Automated Synthesis of Resilient Architectures

Hard Problem: Resilient Architectures

- PIs: Ehab Al-Shaer
- Researchers: Mohamed Alsaleh, Ghaith Husari
- Synopsis
  - Develop a formal automated reasoning framework for designing resilient architectures with provable bounds for cyber and cyber-physical systems
  - Investigate metric-driven automated synthesis of security counter-measures to resist and mitigate attacks
- Recent finding or other outcome
  - Developed a formal model for synthesizing network resiliency configurations that takes the network topology, resiliency requirements, and business constraints as inputs, and creates cost-effective resiliency configurations satisfying target resiliency metrics and policy constraints
- NSA research keywords: Mitigation

Research Methods, Community Development and Support

This is a metalevel contribution

- PIs: Jeff Carver, Ehab Al-Shaer, Lindsey McGowen, Laurie Williams
- Researchers: Morgan Burcham, Mahran Al-Zyoud, Ozgur Kafali
- Collaborators: Rahul Pandita
- Synopsis
  - Develop an understanding of the scientific progress within the lablet and the effect of lablet research on the field at large
  - Develop, curate, and encourage the application of scientifically defensible research methods in cybersecurity
- Recent finding or other outcome
  - Developed interview guides and surveys to assess the impact of lablet participation on stakeholders and to gain improved understanding of potential benefits of our systematic approach to the science of security
  - Created a rubric for characterizing elements of scientific work as reflected in published cybersecurity research; used it to classify papers from leading conferences with the goal of producing guidelines that help bring out scientific contributions in cybersecurity research

Community Engagement

- Annual Summer Research Workshop
  - Industry panel on security with participation from finance, control equipment, healthcare, networking, IT (cybersecurity)
- Ongoing interactions with industry, academia, and government
- Ongoing interactions with NSA
  - Locally with Laboratory for Analytic Sciences
  - Brad Martin's visit
- REU student researchers (including female and minority) collaborating closely with postdocs and graduate students
- Annual Industry Day (last held on 20 October 2016)
  - Pecha Kucha (20 slides at 20 seconds each) student presentations
  - Invited industry presentations
- NSA research keywords: Workforce training

NSA Research Keywords (Combined and Simplified)

Interested researchers

Policy	Access control, Firewalls, PKI, Secure configuration	Berglund, Chirkova, Doyle, Li, Murphy-Hill, Reiter, Singh, Staddon, Williams
Resilience	Anomaly detection, Mitigation, Real-time monitoring, Sandboxes, Patching	Al-Shaer, Dai, Enck, Gu, Meneely, Reiter, Vouk
Metrics	Secure programming, Testing, Analyzing adversary code	Carver, Dai, Meneely, Vouk, Williams
Insider threats		Enck, Singh, Staddon, Williams
Humans	Phishing, Privacy, Workforce training	Doyle, Li, Mayhorn, Murphy-Hill, Proctor, Roberts, Singh, St. Amant, Staddon
Applications	IoT, Mobility	Enck, Reiter, Singh,
Simulation		Berglund, Doyle, Singh