The Importance of Being Earnest(ly Secure)

Jeremy Epstein
National Science Foundation
September 17 2015
Russian spy gang hijacks satellite links to steal data
SaTC Evolution

- Trusted Computing FY 02-03
  - Secure the IT components

- Cyber Trust FY 04-08
  - Make more predictable
  - Address policy and usability
  - Educate the workforce

- Trustworthy Computing FY 09-11
  - Develop a Science of Security
  - Support empirical investigations
  - Include social aspects of security

- Secure & Trustworthy Cyberspace FY 12 ++
  - Focus on interdisciplinary research
  - Emphasize social aspects
  - Join with SRC, Intel
  - Fund Transition-to-Practice

SaTC is the largest computer science research program at NSF, and the largest unclassified cybersecurity research program in the world.
SaTC Overview

• $75-80M/year in research funding, ~700 active projects
• Comprehensive & Multifaceted: Soup to Nuts
  • grass-roots proposals of research from the community (as usual for NSF) guided by a framework of national needs and priorities
• Broad scope of research encompassing technical, social, and educational perspectives to improving cybersecurity
• Encourage inter-disciplinary and cross-disciplinary research
• Advance education in K-12, undergrad, grad, professional, and general society
• Technology transition to NSF research, industry, government
Current SaTC Funding Areas

- Access control
- Anti-malware
- Anticensorship
- Authentication
- Biometrics
- Cellphone network security
- Citizen science
- Cloud security
- Cognitive psychology
- Competitions
- Cryptography, applied
- Cryptography, theory
- Crypto currency
- Cybereconomics
- Cyberwar
- Data analytics
- Deception
- Digital currencies
- Education
- Embedded systems
- Forensics
- Formal methods
- Governance
- Hardware security
- Healthcare security
- Insider threat
- Intrusion detection
- Mobile security
- Network security
- Operating systems
- Personalization
- Power grid security
- Privacy
- Provenance
- Security usability
- Situational awareness
- Social networks
- Sociology of security
- Software security
- Vehicle security
- Verifiable computation
- Voting systems security
- Web security
Security in Cyber Physical Systems

Interdisciplinary/multidisciplinary approaches to security
Security in Cyber Physical Systems
Looks Like Uber Got Hacked

By Alison Griswold

We've wondered a couple times if they compromised your pacemaker to some students at the idea: You die!
Smart refrigerator hack exposes Gmail login credentials
Sample Problem

- Vehicles are internet connected
- Vendors are slow to recognize the risk
- Solutions will be years in development, and longer before ubiquity
- Need to learn what that adversary is doing
What keeps me up at night?

• How do we design systems today, especially for IoT/CPS, that will be secure against the threats 10-20 years from now?
• How do we deal with the billions of IoT/CPS systems already out there, built without any consideration for security or updates?
NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy (CPS-Security)

Press Release 15-096
A partnership to secure and protect the emerging Internet of Things

National Science Foundation and Intel Corporation team to improve the security and privacy of computing systems that interact with the physical world using a new cooperative research model

The projects announced today as part of the NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy are:

- Insup Lee, University of Pennsylvania: Security and Privacy-Aware Cyber-Physical Systems
- Philip Levis, Stanford University: CPS-Security: End-to-End Security for the Internet of Things

Researchers will adapt smart alarm research to detect and react to attacks on medical devices.
Inter-Disciplinary Topics
STPI Portfolio Characterization by ACM Categories, 2008-2012

• Topics part of the ACM classification system for academic papers within the Security and Privacy subset
• Provides a set of academically oriented topics that undergoes periodic revision at the ACM
• Only two awards (< 1%) could not be placed into a category.

Could Not Be Categorized
Intrusion/Anomaly Detection & Malware Mitigation
Network Security
Security Services
Formal Methods and Theory of Security
Human and Societal Aspects of Security and Privacy
Database and Storage Security
Security in Hardware
Cryptography
Software and Applications Security
Systems Security
NSPW Agenda

- "If you were attacked, you'd be sorry": Counterfactuals as security arguments
- Examining the Contribution of Critical Visualisation to Information
- Maybe Poor Johnny Really Cannot Encrypt - The Case for a Complexity Theory for Usable Security
- Exploiting the Physical Environment for Securing the Internet of Things
- WebSheets: Web Applications for Non-Programmers
- Towards Managed Role Explosion
- Choose Your Own Authentication
- The Myth of the Average User: Improving Privacy and Security Systems through Individualization
- Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors
- Peace vs. Privacy: Leveraging Conflicting Jurisdictions for Email Security
- Milware: Identification and Implications of State Authored Malicious Software
- Bridging the Trust Gap: Integrating Models of Behavior and Perception
Challenges of Multidisciplinary Work

• Getting researchers to know each other!
• Finding research topics that advance both fields
• Logistical issues – e.g., publication, student funding norms
New CISE/SBE Collaborations

- Goal: Start collaboration between computer scientists and social scientists who have not previously worked together
- Two phase process:
  - Submit white paper
  - If accepted, submit EAGER proposal (8 pages, up to $300K, average $225K)
- 10 funded in FY13; 16 funded in FY14; 13 funded in FY15
<table>
<thead>
<tr>
<th>FY13 Award</th>
<th>PI Name</th>
<th>Institution</th>
<th>Project Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1343141</td>
<td>Zhu, Ye</td>
<td>Cleveland State U</td>
<td>EAGER: The Game Changer: A New Model for Password Security</td>
</tr>
<tr>
<td>1343258</td>
<td>Beyah, Raheem A.</td>
<td>Georgia Tech Research Corp</td>
<td>EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime</td>
</tr>
<tr>
<td>1343237</td>
<td>Wingfield, Adia Harvey</td>
<td>Georgia State U</td>
<td>EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime</td>
</tr>
<tr>
<td>1343430</td>
<td>Aliari Zonouz, Saman</td>
<td>U of Miami</td>
<td>EAGER: Cybercrime Susceptibility in the Sociotechnical System: Exploration of Integrated Micro- and Macro-Level Sociotechnical Models of Cybersecurity</td>
</tr>
<tr>
<td>1343433</td>
<td>Egelman, Serge M.</td>
<td>International Computer Science Institute</td>
<td>EAGER: Designing Individualized Privacy and Security Systems</td>
</tr>
<tr>
<td>1343451</td>
<td>Peer, Eyal</td>
<td>CMU</td>
<td>EAGER: Designing Individualized Privacy and Security Systems</td>
</tr>
<tr>
<td>1343453</td>
<td>Chellappan, Sriram</td>
<td>Missouri U S&amp;T</td>
<td>EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals</td>
</tr>
<tr>
<td>1343245</td>
<td>Bossler, Adam</td>
<td>Georgia Southern U</td>
<td>EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals</td>
</tr>
<tr>
<td>1343766</td>
<td>Khan, Mohammad</td>
<td>U of Connecticut</td>
<td>EAGER: The Role of Emotion in Risk Communication and Warning: Application to Risks of Failures to Update Software</td>
</tr>
<tr>
<td>1347113</td>
<td>Ho, Shuyuan M.</td>
<td>Florida State U</td>
<td>EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication</td>
</tr>
<tr>
<td>1347120</td>
<td>Hancock, Jeffrey T.</td>
<td>Cornell U</td>
<td>EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication</td>
</tr>
<tr>
<td>1347151</td>
<td>Garg, Vaibhav</td>
<td>Drexel U</td>
<td>EAGER: Cybercrime Science</td>
</tr>
<tr>
<td>1347186</td>
<td>Hong, Jason</td>
<td>CMU</td>
<td>EAGER: Social Cybersecurity: Applying Social Psychology to Improve Cybersecurity</td>
</tr>
<tr>
<td>Award Number</td>
<td>Name</td>
<td>Affiliation</td>
<td>Project Title</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1359542</td>
<td>Yue, Chuan</td>
<td>U of Colorado Colorado Springs</td>
<td>EAGER: Investigating Elderly Computer Users' Susceptibility to Phishing</td>
</tr>
<tr>
<td>1359632</td>
<td>Telang, Rahul</td>
<td>CMU</td>
<td>EAGER: Consumer Response to Security Incidences and Data Breach Notification: An Empirical Analysis</td>
</tr>
<tr>
<td>1444633</td>
<td>Maimon, David</td>
<td>U of Maryland College Park</td>
<td>EAGER: Physical, Social and Situational Factors as Deterrents of Public WiFi Users Online Behaviors</td>
</tr>
<tr>
<td>1444823</td>
<td>Yeh, K.-C. Martin</td>
<td>University Park</td>
<td>EAGER: Collaborative: Using Cognitive Techniques To Detect and Prevent Security Flaws</td>
</tr>
<tr>
<td>1444840</td>
<td>O'Brien, James F.</td>
<td>UC Berkeley</td>
<td>EAGER: Collaborative: Understanding How Manipulated Images Influence People</td>
</tr>
<tr>
<td>1444840</td>
<td>Shen, Cuihua</td>
<td>UC Davis</td>
<td>EAGER: Collaborative: Understanding How Manipulated Images Influence People</td>
</tr>
<tr>
<td>1444863</td>
<td>Moore, Tyler</td>
<td>Southern Methodist U</td>
<td>EAGER: Exploring Trade-offs in Cyber Offense and Defense Through the Lenses of Computer and Political Science</td>
</tr>
<tr>
<td>1444871</td>
<td>Forrest, Stephanie</td>
<td>U of New Mexico</td>
<td>EAGER: Collaborative: Policies for Enhancing U.S. Leadership in Cyberspace</td>
</tr>
<tr>
<td>1445079</td>
<td>Aranovich, Raul</td>
<td>UC Davis</td>
<td>EAGER: Effective Detection of Vulnerabilities and Linguistic Stratification in Open Source Software</td>
</tr>
<tr>
<td>1450193</td>
<td>Howard, Philip N.</td>
<td>U of Washington</td>
<td>EAGER: Computational Propaganda and The Production/Detection of Bots</td>
</tr>
<tr>
<td>1450500</td>
<td>Sundar, S. Shyam</td>
<td>Penn State U University Park</td>
<td>EAGER: Why do we Reveal or Withhold Private Information? Exploring Heuristics and Designing Interface Cues for Secure and Trustworthy Computing</td>
</tr>
<tr>
<td>1450600</td>
<td>Kelley, Patrick</td>
<td>U of New Mexico</td>
<td>EAGER: Privacy’s Sociocultural Divide across American Youth</td>
</tr>
<tr>
<td>1450619</td>
<td>Carbunar, Bogdan</td>
<td>Florida International U</td>
<td>EAGER: Digital Interventions for Reducing Social Networking Risks in Adolescents</td>
</tr>
<tr>
<td>1450624</td>
<td>Oliveira, Daniela A.</td>
<td>U of Florida</td>
<td>EAGER: Age-Targeted Automated Cueing Against Cyber Social Engineering Attacks</td>
</tr>
<tr>
<td>1450625</td>
<td>Shilton, Katherine</td>
<td>U of Maryland College Park</td>
<td>EAGER: Privacy in Citizen Science: An Emerging Concern for Research and Practice</td>
</tr>
<tr>
<td>Award Number</td>
<td>Investigator(s)</td>
<td>Institution(s)</td>
<td>Project Title</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1536871</td>
<td>Fabbri, Daniel</td>
<td>Vanderbilt U Medical Center</td>
<td>EAGER: Managing Information Risk and Breach Discovery</td>
</tr>
<tr>
<td>1537324</td>
<td>Nissenbaum, Helen</td>
<td>New York U</td>
<td>EAGER: Collaborative: A Research Agenda to Explore Privacy in Small Data Applications</td>
</tr>
<tr>
<td>1536897</td>
<td>Estrin, Deborah</td>
<td>Cornell U</td>
<td>EAGER: Collaborative: A Research Agenda to Explore Privacy in Small Data Applications</td>
</tr>
<tr>
<td>1537143</td>
<td>Acquisti, Alessandro</td>
<td>CMU</td>
<td>EAGER: Collaborative: Design, Perception, and Action - Engineering Information Give-Away</td>
</tr>
<tr>
<td>1537538</td>
<td>Cheng, Maggie X.</td>
<td>Missouri U of S&amp;T</td>
<td>EAGER: Factoring User Behavior in Network Security Analysis</td>
</tr>
<tr>
<td>1537768</td>
<td>Hill, Raquel L.</td>
<td>Indiana U</td>
<td>EAGER: Leveling the Digital Playing Field for the Job Seeker</td>
</tr>
<tr>
<td>1537924</td>
<td>Hu, Hongxin</td>
<td>Clemson U</td>
<td>EAGER: Defending Against Visual Cyberbullying Attacks in Emerging Mobile Social Networks</td>
</tr>
<tr>
<td>1538418</td>
<td>Liu, Bao</td>
<td>U of Texas San Antonio</td>
<td>EAGER: Collaborative: IC Supply Chain Security and Quality Control in Business and Social Context</td>
</tr>
<tr>
<td>1537591</td>
<td>Zhao, Yao</td>
<td>Rutgers U Newark</td>
<td>EAGER: Collaborative: IC Supply Chain Security and Quality Control in Business and Social Context</td>
</tr>
<tr>
<td>1544373</td>
<td>Kobsa, Alfred</td>
<td>UC Irvine</td>
<td>EAGER: Unattended/Automated Studies of Effects of Auditory Distractions on Users Performing Security-Critical Tasks</td>
</tr>
<tr>
<td>1544455</td>
<td>Li, Zhenhui</td>
<td>Penn State U</td>
<td>EAGER: Toward Transparency in Public Policy via Privacy-Enhanced Social Flow Analysis with Applications to Ecological Networks and Crime</td>
</tr>
<tr>
<td>1544493</td>
<td>Dahbura, Anton</td>
<td>Johns Hopkins U</td>
<td>EAGER: Collaborative: Computational Cognitive Modeling of User Security and Incentive Behaviors</td>
</tr>
<tr>
<td>1544385</td>
<td>Xiong, Kaiqi</td>
<td>Rochester Institute of Tech</td>
<td>EAGER: Collaborative: Computational Cognitive Modeling of User Security and Incentive Behaviors</td>
</tr>
<tr>
<td>1544535</td>
<td>Truxillo, Donald M.</td>
<td>Portland State U</td>
<td>EAGER: Exploring Job Applicant Privacy Concerns</td>
</tr>
</tbody>
</table>
FY13 & FY14 Word Cloud

- Cybersecurity
- Dynamics Temporal
- Risk
- Cybercrime
- Science
- Designing
- Communication
- Security
- Software
- Sociotechnical
- Susceptibility
- Social
- Computer
- Cognitive
- Vulnérabilities
- Secure Behaviors Citizen Attribution Cueing Using Psychology Attention Spatial Lenses
- Physical CyberSecurity Social-Class Computational Computing Social-Engineering Incidences Linguistic Divide Propaganda Software
- Detection Bots Political Influence Offense Prevention Response Flaws Leadership
- Computer
- Prevention
- Psychological
- Trustworthiness Production/Detection
- Language-Action
- Computer
- Trustworthy Cyberspace Networking
- CyberCriminals Alertness
- Cyber Effectiveness
- Communicating Deterrents Integrating Cyber-threats Deterrence
- Computer
- System Effective
- Manipulated Interventions Predictive
- Elderly Emotion
- Privacy
- Trustworthy
- Notification
- Human-centric Factors
- Knowledge Cyber Factors
- Communication
- Cues Update Defense Breach
- Predictive

NSF Secure and Trustworthy Cyberspace

SaTC Secure and Trustworthy Cyberspace
Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime (1343258/Beyah)

• Goal: Explore the ways that social class impacts groups’ susceptibilities to cybercrime tactics (in particular, phishing attacks) that highlight opportunities for economic advancement.

• Previous studies have focused on how factors such as age, gender, occupation, and level of STEM background affect one’s susceptibility to Internet crime (i.e., phishing attacks), however little work has focused on how social class factors into Internet crime susceptibility.

• Extensive sociological research suggests that social class is an important factor that influences individuals’ willingness to consider certain strategies as a route to economic improvement.
Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime (1343258/Beyah)

- Malicious infrastructure developed using Metasploit and Python Scripts.
- Various methods employed to defeat SPAM filters.
- The use of deception was employed: Participants with various income levels were recruited and were paid to evaluate benign websites while unknowingly phished.
- 47/60 participants have been phished.
- Response levels varied from no response, opened email, clicked link, to submitted form.
Designing Individualized Privacy and Security Systems (1343433/Egelman)

• Current usable privacy/security solutions only yield local maxima when they only consider human behavior in the aggregate; no individual perfectly matches the “average user.”

• This project aims to optimize privacy & security mitigations by tailoring them to the individual.

• An app was developed to collect:
  – privacy settings
  – frequency of posts
  – likes
  – network size
  – profile data
RESULTS

Designing Individualized Privacy and Security Systems (1343433/Egelman)

• Results showed that individual differences (e.g., personality traits) correlate with privacy preferences and behaviors
  – privacy concerns scale (PCS)
  – internet users’ information privacy concerns (IUIPC)
  – Westin
  – disclosure of sensitive activities/information

• Created a new condensed privacy preferences scale that is correlated with existing psychometrics

• Currently developing a scale to examine security behaviors and how they correlate with existing psychometrics

• Submission target: SIGCHI Conference on Human Factors in Computing Systems (CHI)
Prompt and regular software updates are important to system and network security and performance. Despite this, users often delay updates and ignore messages.

Using the C-HIP model, we investigate where, if at all, the failure in persuasion occurs when trying to convince a user to perform a behavior.

1. **Attention Switch and Maintenance** - Is the message noticeable?
2. **Comprehension** - Is the message understandable?
3. **Attitudes/Beliefs** - Does the message agree with the existing opinions of the receiver?
4. **Motivation** - Does the message provide necessary motivation for the receiver to act?

The Role of Emotion in Risk Communication and Warning: Application to Risks of Failures to Update Software (1343766/Khan)

- Winter 2013 survey gathered 155 responses
  - Average age of respondent = 22 years old
  - 60% female, 40% male
- Rate “How noticeable is the message?”, “How important is the message?”, “How annoying is the message?” and “How confusing is the message?”
- Annoyance and confusion may both be factors in common hesitation among users to apply updates.
- High level of hesitation indicates failed persuasion.
- Further study is needed to identify specific strengths and drawbacks of existing update message designs and to address them.
- **Poster:** Michael Fagan, Mohammad Maifi Hasan Khan, Ross Buck. A Preliminary Study of Users’ Experiences and Beliefs about Software Update Messages. The 10th Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA, USA, 2014. Acceptance rate: 70%
Consumer Response to Security Incidences and Data Breach Notification (1359632/Telang)

- Rahul Telang (applied economics), Artur Dubrawski (machine learning & data mining), CMU
- Access a large dataset regarding customer transactions and details on whether a customer encountered adverse security incidence or fraud, received a breach notification, and etc.
- Identify degree of user behavior changes due to an adverse security event or breach notification.
- Get executive interviews and end user interviews/surveys to study the firm's security policies and users' attitudes.
- Highlight the cost and benefits of existing policies & provide guidelines on more effective regulations
Exploring Spear-Phishing: a Socio-Technical Experimental Framework (1359601/Nov)

- Oded Nov (behavioral research), Nasir Memon (computer security), Polytechnic Institute of NYU
- Examine the effects of the Big Five personality traits on users’ response to spearphishing attacks and their ability to detect deception
- Send simulated spearphishing messages to people on their actual email accts at 4 organizations (2 universities and 2 companies)
- Develop novel types of cyber defenses that are tailored to users’ idiosyncratic characteristics
- Make cyber defenses more efficient and reduce the costs of attacks
Investigating Elderly Computer Users’ Susceptibility to Phishing (1359542/Yue)

• Chuan Yue (computer security), Brandon E Gavett (Psychology), U. Colorado at Colorado Springs

• Hypotheses
  – older users differ from younger ones in terms of their susceptibility to both types of phishing, and that this susceptibility can be explained by differences in cognitive abilities, specifically executive functioning and decision-making skills.

• Tasks
  – test hypotheses by: (1) building a comprehensive testbed that measures traditional and Web SSO phishing susceptibility in a realistic environment, and (2) performing a comprehensive user study.

• Progress
  – A comprehensive phishing susceptibility testbed has been built and will be shared with other researchers. The recruitment of participants is in progress.
Using Cognitive Techniques to Detect and Prevent Security Flaws (1444827/Cappos)

- **Developer blind spots** often lead to security breaches from malicious groups.
- Multi-discipline collaboration
  - Cognitive psychology
  - Software engineering
  - Software security
- Identify security bugs that are rooted from blind spots
  - Bug slicing (short code segment to understand security bugs and mental models)
  - Cognitive analysis and validation
  - Security flaws detection and prevention
# A Few More...

<table>
<thead>
<tr>
<th>ID</th>
<th>PI</th>
<th>Title</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1549508</td>
<td>Mario Caire, UTEP</td>
<td>EAGER: Understanding Cybersecurity Needs and Gaps at the Local Level</td>
<td>How are small &amp; medium businesses affected by cybersecurity?</td>
</tr>
<tr>
<td>1314925</td>
<td>Simon Ou, Kansas State Univ</td>
<td>Medium: Bringing Anthropology into Cybersecurity</td>
<td>What can we learn by putting anthropologists into security operations centers?</td>
</tr>
<tr>
<td>1513875</td>
<td>Kelly Caine, Clemson</td>
<td>Medium: Usable, Secure, and Trustworthy Communication for Journalists and Sources</td>
<td>What technologies can help journalists and sources be safe online?</td>
</tr>
<tr>
<td>1514192</td>
<td>Alessandro Acquisti, CMU</td>
<td>Medium: Understanding and Exploiting Visceral Roots of Privacy and Security Concerns</td>
<td>Are attitudes towards security influenced by the physical environment, and can that be used to improve security?</td>
</tr>
</tbody>
</table>
Going Forward

• Workshop on new collaborations, Jan 2015 (Lance Hoffman & Laura Brandimarte)
• US-Netherlands workshop on international collaborations in privacy
• Possible continuation of New Collaborations

• Interdisciplinary collaborations, especially the human aspects, are increasingly central to cybersecurity
And since you asked...
## Sizes and Schedule (NSF 15-575)

<table>
<thead>
<tr>
<th>Category</th>
<th>Amount &amp; duration</th>
<th>FY16 Submission dates</th>
<th># FY15 funded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Up to $500k, 3 years</td>
<td>Nov 04 2015 – Nov 18 2015</td>
<td>72 proposals/58 projects</td>
</tr>
<tr>
<td>Medium</td>
<td>Up to $1.2M, 4 years</td>
<td>Sep 10 2015 – Sep 16 2015</td>
<td>38 proposals/23 projects</td>
</tr>
<tr>
<td>Large</td>
<td>Up to $3M, 5 years</td>
<td>Sep 18 2015 – Sep 24 2015</td>
<td>10 proposals/3 projects</td>
</tr>
<tr>
<td>Education</td>
<td>Up to $300K, 2 years</td>
<td>Dec 03 2015 – Dec 16 2015</td>
<td>9 proposals/9 projects</td>
</tr>
</tbody>
</table>
Funding for Junior Faculty

• CRII proposals
  – Solicitation 15-569
  – For faculty in their first two years of an academic/research position (no more than 5 years post-PhD)
  – Up to $175K, 2 years
  – Due date: Sep 30 2015
<table>
<thead>
<tr>
<th>Program Director</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nina Amla</td>
<td>Formal methods, hardware, crypto (CISE)</td>
</tr>
<tr>
<td>Chris Clifton</td>
<td>Privacy, databases, data mining (CISE)</td>
</tr>
<tr>
<td>Jeremy Epstein</td>
<td>Systems, voting security (CISE)</td>
</tr>
<tr>
<td>Sol Greenspan</td>
<td>Software engineering (CISE)</td>
</tr>
<tr>
<td>Dongwon Lee</td>
<td>Education, CyberCorps ® SFS, data science, social computing (EHR)</td>
</tr>
<tr>
<td>Wenjing Lou</td>
<td>Wireless, networking (CISE)</td>
</tr>
<tr>
<td>Anita Nikolich</td>
<td>Transition to practice, data centers, SW Defined Networks (CISE)</td>
</tr>
<tr>
<td>Victor Piotrowski</td>
<td>Education, CyberCorps ® SFS, cyber operations (EHR)</td>
</tr>
<tr>
<td>Andrew Pollington</td>
<td>Mathematics, number theory, theoretical crypto (MPS/DMS)</td>
</tr>
<tr>
<td>Deborah Shands</td>
<td>Systems, cloud, scalable security administration (CISE)</td>
</tr>
<tr>
<td>Ralph Wachter</td>
<td>Cyber physical systems (CISE)</td>
</tr>
<tr>
<td>Chengshan Xiao</td>
<td>Physical layer comms, signal processing (ENG)</td>
</tr>
<tr>
<td>Heng Xu</td>
<td>Privacy, social and behavioral sciences, usability (SBE)</td>
</tr>
</tbody>
</table>
Last but not least...
SaTC mailing list

• Send “subscribe SaTC-announce” to listserv@listserv.nsf.gov
• About 10 messages/year
Thank you!