The Importance of Being Earnest(ly Secure)

Jeremy Epstein
National Science Foundation
September 17 2015

Securi

ZDNet

BUYER'S GUIDE APPLE IP

Hackers insuran

Insurance prov week

By John Fontana fo

Ashley Ma trouble ac

Rampant password re

by **Dan Goodin** - Sep 10, 2015

KIM ZETTER SECURITY 09.09.15 8:30 AM

RUSSIAN SPY GANG HIJACKS SATELLITE LINKS TO STEAL DATA

NEWSLETTERS

d last

NSF

SaTC
Secure and Trustworthy Cyberspace

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

SaTC
Secure and Trustworthy Cyberspace

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

SaTC
Secure and Trustworthy Cyberspace

Security in Cyber Physical Systems

Interdisciplinary/multidisciplinary approaches to security

SaTC
Secure and Trustworthy Cyberspace

Security in Cyber Physical Systems

Hackers K
Human By
Pacemake

September 7, 2015 // 11:45

Image: CAE Healthcare

We've wondered a coup
compromise your pacen
to some students at the
idea: You die!

Ruski
popul

WinCC
Collider.

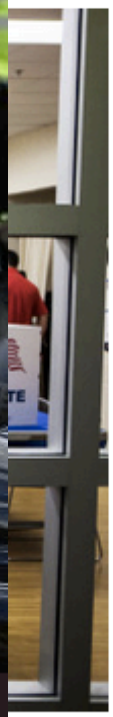
MONEYBOX | A BLOG ABOUT BUSINESS AND ECONOMICS. | FEB. 27 2015 6:15 PM

Looks Like Uber Got Hacked

By *Alison Griswold*

50

Really?



OPEN SOURCE COMMUNITY

By Colin Neagle | Follow

About
The Open Source subnet's hub.

Smart refrigerator hack exposes Gmail login credentials

@riding_red

internet and call for service in the case of malfunction, or devices that can monitor your energy usage and send you Twitter updates.

RELATED


Welcome to the smart home ... of horror!


Security holes in the 3 most popular smart home hubs and Honeywell Tuxedo Touch


Your router: Gateway for hackers

on IDG **Answers**
If I buy a Chromebook and can't get to grips with OS can I convert to windows?

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?

SaTC
Secure and Trustworthy Cyberspace

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

Researchers will adapt smart alarm research to detect and react to attacks on medical devices.

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

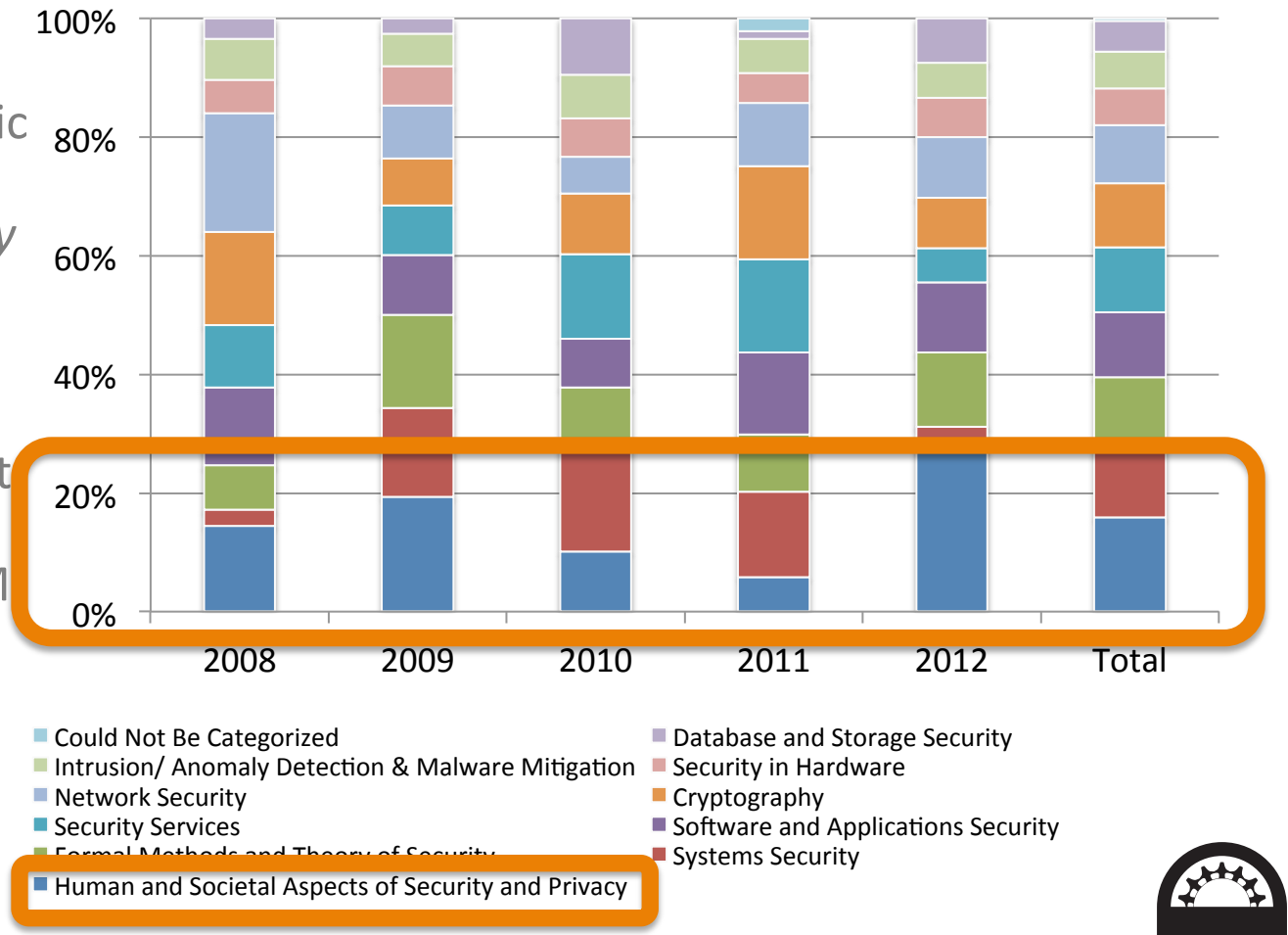
- Insup Lee, University of Pennsylvania: Security and Privacy-Aware Cyber-Physical Systems
- Philip Levis, Stanford University: CPS-Security: End-to-End Security for the Internet of Things

SaTC
Secure and Trustworthy Cyberspace

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.



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

Code:
Technical
People
Other

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

SaTC
Secure and Trustworthy Cyberspace

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

SaTC
Secure and Trustworthy Cyberspace

FY13 Awards

1343141	Zhu, Ye	Cleveland State U	EAGER: The Game Changer: A New Model for Password Security
1343258	Beyah, Raheem A.	Georgia Tech Res Corp	EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime
1343237	Wingfield, Adia Harvey	Georgia State U	EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime
1343430	Aliari Zonouz, Saman	U of Miami	EAGER: Cybercrime Susceptibility in the Sociotechnical System: Exploration of Integrated Micro- and Macro-Level Sociotechnical Models of Cybersecurity
1343433	Egelman, Serge M.	International Computer Science Institute	EAGER: Designing Individualized Privacy and Security Systems
1343451	Peer, Eyal	CMU	EAGER: Designing Individualized Privacy and Security Systems
1343453	Chellappan, Sriram	Missouri U S&T	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343482	Holt, Thomas J.	Michigan State U	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343245	Bossler, Adam	Georgia Southern U	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343766	Khan, Mohammad	U of Connecticut	EAGER: The Role of Emotion in Risk Communication and Warning: Application to Risks of Failures to Update Software
1347075	Milward, H. Brinton	U of Arizona	EAGER: Human-centric Predictive Analytics of Cyber-threats: a Temporal Dynamics Approach
1347113	Ho, Shuyuan M.	Florida State U	EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication
1347120	Hancock, Jeffrey T.	Cornell U	EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication
1347151	Garg, Vaibhav	Drexel U	EAGER: Cybercrime Science
1347186	Hong, Jason	CMU	EAGER: Social Cybersecurity: Applying Social Psychology to Improve Cybersecurity

FY14 Awards

1358723	Richard, Golden G.	U of New Orleans	EAGER: Integrating Cognitive and Computer Science to Improve Cyber Security: Selective Attention and Personality Traits for the Detection and Prevention of Risk
1359542	Yue, Chuan	U of Colorado Colorado Springs	EAGER: Investigating Elderly Computer Users' Susceptibility to Phishing
1359601	Nov, Oded	Polytechnic U of New York	EAGER: Exploring spear-phishing: a socio-technical experimental framework
1359632	Telang, Rahul	CMU	EAGER: Consumer Response to Security Incidences and Data Breach Notification: An Empirical Analysis
1444633	Maimon, David	U of Maryland College Park	EAGER: Physical, Social and Situational Factors as Determents of Public WiFi Users Online Behaviors
1444827	Cappos, Justin	New York U	EAGER: Collaborative: Using Cognitive Techniques To Detect and Prevent Security Flaws
1444823	Yeh, K.-C. Martin	Penn State U University Park	EAGER: Collaborative: Using Cognitive Techniques To Detect and Prevent Security Flaws
1444840	O'Brien, James F.	UC Berkeley	EAGER: Collaborative: Understanding How Manipulated Images Influence People
1444861	Shen, Cuihua	UC Davis	EAGER: Collaborative: Understanding How Manipulated Images Influence People
1444863	Moore, Tyler	Southern Methodist U	EAGER: Exploring Trade-offs in Cyber Offense and Defense Through the Lenses of Computer and Political Science
1444871	Forrest, Stephanie	U of New Mexico	EAGER: Collaborative: Policies for Enhancing U.S. Leadership in Cyberspace
1444500	Axelrod, Robert	U of Michigan Ann Arbor	EAGER: Collaborative: Policies for Enhancing U.S. Leadership in Cyberspace
1445079	Aranovich, Raul	UC Davis	EAGER: Effective Detection of Vulnerabilities and Linguistic Stratification in Open Source Software
1450193	Howard, Philip N.	U of Washington	EAGER: Computational Propaganda and The Production/Detection of Bots
1450500	Sundar, S. Shyam	Penn State U University Park	EAGER: Why do we Reveal or Withhold Private Information? Exploring Heuristics and Designing Interface Cues for Secure and Trustworthy Computing
1450600	Kelley, Patrick	U of New Mexico	EAGER: Privacy's Sociocultural Divide across American Youth
1450619	Carbunar, Bogdan	Florida International U	EAGER: Digital Interventions for Reducing Social Networking Risks in Adolescents
1450624	Oliveira, Daniela A.	U of Florida	EAGER: Age-Targeted Automated Cueing Against Cyber Social Engineering Attacks
1450625	Shilton, Katherine	U of Maryland College Park	EAGER: Privacy in Citizen Science: An Emerging Concern for Research and Practice

FY15 Awards

1536871	Fabbri, Daniel	Vanderbilt U Medical Center	EAGER: Managing Information Risk and Breach Discovery
1537324	Nissenbaum, Helen	New York U	EAGER: Collaborative: A Research Agenda to Explore Privacy in Small Data Applications
1536897	Estrin, Deborah	Cornell U	EAGER: Collaborative: A Research Agenda to Explore Privacy in Small Data Applications
1537483	Krupka, Erin Lea	U of Michigan Ann Arbor	EAGER: Collaborative: Design, Perception, and Action - Engineering Information Give-Away
1537143	Acquisti, Alessandro	CMU	EAGER: Collaborative: Design, Perception, and Action - Engineering Information Give-Away
1537528	Lee, Gwendolyn K.	U of Florida	EAGER: Lottery and Paradox: A Risk-based Framework on Privacy
1537538	Cheng, Maggie X.	Missouri U of S&T	EAGER: Factoring User Behavior in Network Security Analysis
1537768	Hill, Raquel L.	Indiana U	EAGER: Leveling the Digital Playing Field for the Job Seeker
1537924	Hu, Hongxin	Clemson U	EAGER: Defending Against Visual Cyberbullying Attacks in Emerging Mobile Social Networks
1538418	Liu, Bao	U of Texas San Antonio	EAGER: Collaborative: IC Supply Chain Security and Quality Control in Business and Social Context
1537591	Zhao, Yao	Rutgers U Newark	EAGER: Collaborative: IC Supply Chain Security and Quality Control in Business and Social Context
1544090	Farahmand, Fariborz	Georgia Tech Res Corp	EAGER: A Mathematical Model of Privacy Decisions: A Behavioral Economic Perspective
1544373	Kobsa, Alfred	UC Irvine	EAGER: Unattended/Automated Studies of Effects of Auditory Distractions on Users Performing Security-Critical Tasks
1544455	Li, Zhenhui	Penn State U	EAGER: Toward Transparency in Public Policy via Privacy-Enhanced Social Flow Analysis with Applications to Ecological Networks and Crime
1544493	Dahbura, Anton	Johns Hopkins U	EAGER: Collaborative: Computational Cognitive Modeling of User Security and Incentive Behaviors
1544385	Xiong, Kaiqi	Rochester Institute of Tech	EAGER: Collaborative: Computational Cognitive Modeling of User Security and Incentive Behaviors
1544535	Truxillo, Donald M.	Portland State U	EAGER: Exploring Job Applicant Privacy Concerns

FY13 & FY14 Word Cloud

SaTC
Secure and Trustworthy Cyberspace

TOPIC

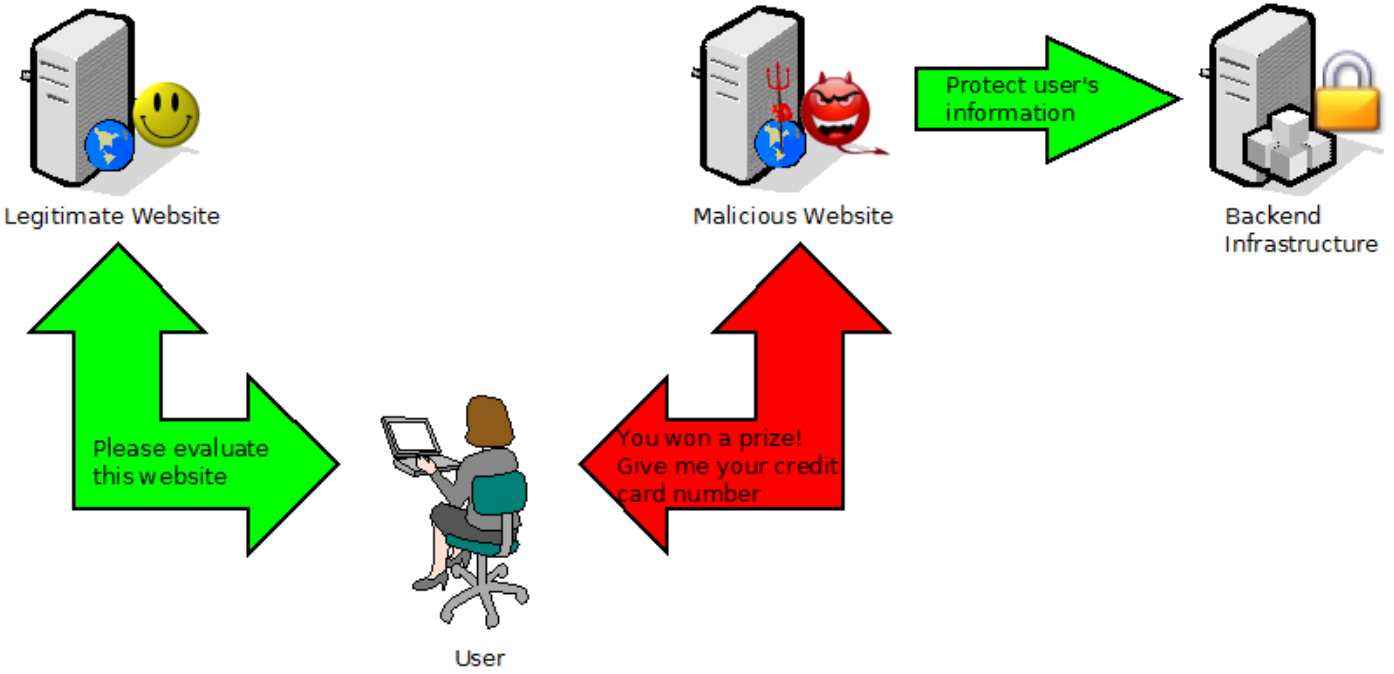
Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime (1343258/Beyah)

- 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.

SaTC
Secure and Trustworthy Cyberspace

RESULTS

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



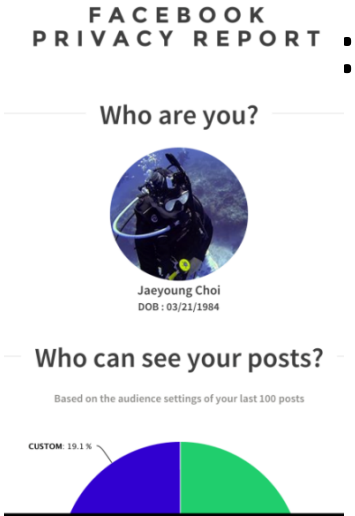
- Malicious infrastructure developed using Metasploit and Python Scripts.
- Various methods employed to defeat SPAM filters.
- The use of deception was employed: Participants with various income levels were recruited and were paid to evaluate benign websites while unknowingly phished.
- 47/60 participants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

SaTC
Secure and Trustworthy Cyberspace

TOPIC

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



SaTC
Secure and Trustworthy Cyberspace

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)*

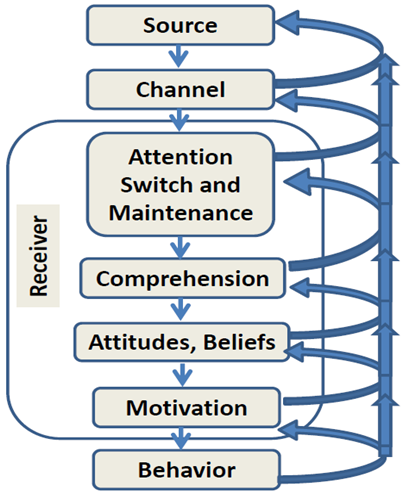
SaTC
Secure and Trustworthy Cyberspace

TOPIC

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

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.



Communication-Human Information Processing (C-HIP) Model (reproduced from [1])

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?

[1] M. S. Wogalter, D. DeJoy, and K. R. Laughery. *Warnings and risk communication*. CRC Press, 1999.

SaTC Secure and Trustworthy Cyberspace

RESULTS

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%
- ***Journal Paper Under Review:*** A Study of Users' Experiences and Beliefs about Software Update Messages. Michael Fagan, Mohammad Maifi Hasan Khan, Ross Buck. Submitted to International Journal of Human-Computer Studies. Elsevier.

SaTC
Secure and Trustworthy Cyberspace

TOPIC

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

SaTC
Secure and Trustworthy Cyberspace

TOPIC

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

SaTC
Secure and Trustworthy Cyberspace

TOPIC

Investigating Elderly Computer Users' Susceptibility to Phishing (1359542/Yue)

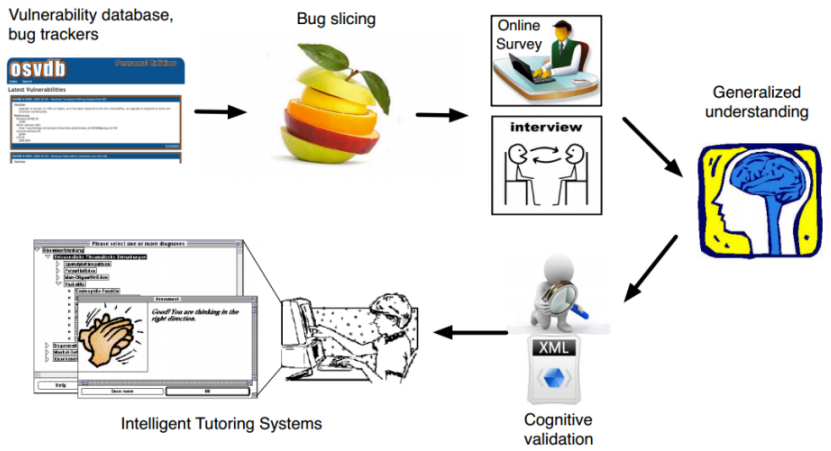
- Chuan Yue (computer security), Brandon E Gavett (Psychology), U. Colorado at Colorado Springs
- **Hypotheses**
  - older users differ from younger ones in terms of their susceptibility to both types of phishing, and that this susceptibility can be explained by differences in cognitive abilities, specifically 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.

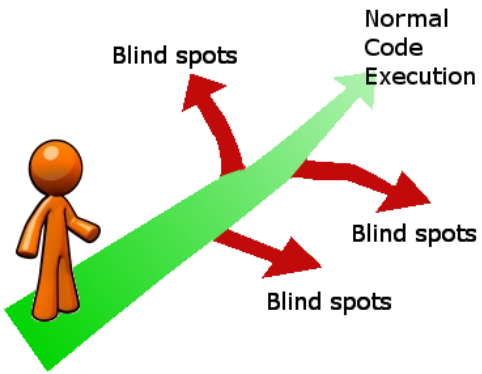
NSF

SaTC
Secure and Trustworthy Cyberspace

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





SaTC
Secure and Trustworthy Cyberspace

A Few More…

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

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*

SaTC
Secure and Trustworthy Cyberspace

And since you asked…

Sizes and Schedule (NSF 15-575)

	Amount & duration	FY16 Submission dates	# FY15 funded
Small	Up to $500k, 3 years	Nov 04 2015 – Nov 18 2015	72proposals/ 58 projects
Medium	Up to $1.2M, 4 years	Sep 10 2015 – Sep 16 2015	38 proposals/ 23 projects
Large	Up to $3M, 5 years	Sep 18 2015 – Sep 24 2015	10 proposals/ 3 projects
Education	Up to $300K, 2 years	Dec 03 2015 – Dec 16 2015	9 proposals/ 9 projects

SaTC
Secure and Trustworthy Cyberspace

Funding for Junior Faculty

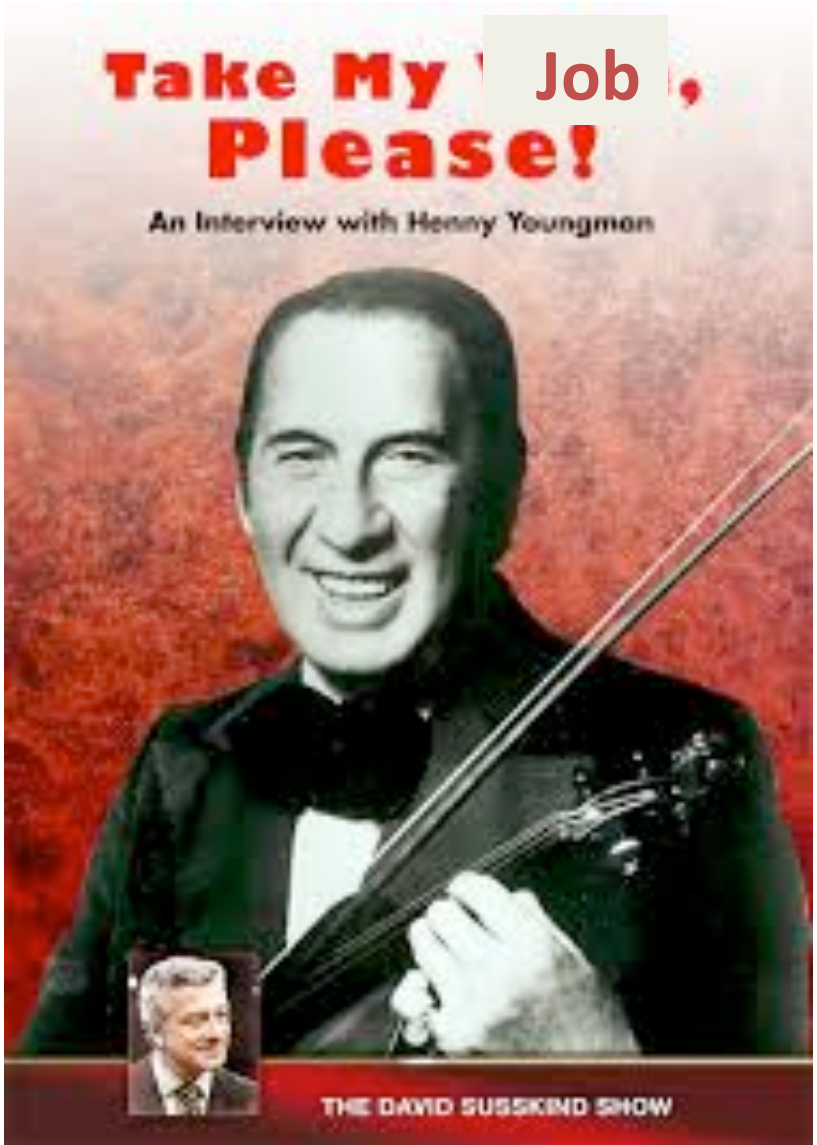
- CRII proposals
  - Solicitation 15-569
  - For faculty in their first two years of an academic/ research position (no more than 5 years post-PhD)
  - Up to $175K, 2 years
  - Due date: Sep 30 2015

SaTC
Secure and Trustworthy Cyberspace

SaTC Program Director topic areas

Program Director	Topic
Nina Amla	Formal methods, hardware, crypto (CISE)
Chris Clifton	Privacy, databases, data mining (CISE)
Jeremy Epstein	Systems, voting security (CISE)
Sol Greenspan	Software engineering (CISE)
Dongwon Lee	Education, CyberCorps ® SFS, data science, social computing (EHR)
Wenjing Lou	Wireless, networking (CISE)
Anita Nikolich	Transition to practice, data centers, SW Defined Networks (CISE)
Victor Piotrowski	Education, CyberCorps ® SFS, cyber operations (EHR)
Andrew Pollington	Mathematics, number theory, theoretical crypto (MPS/DMS)
Deborah Shands	Systems, cloud, scalable security administration (CISE)
Ralph Wachter	Cyber physical systems (CISE)
Chengshan Xiao	Physical layer comms, signal processing (ENG)
Heng Xu	Privacy, social and behavioral sciences, usability (SBE)

Last but not least…



SaTC
Secure and Trustworthy Cyberspace

SaTC mailing list

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

SaTC
Secure and Trustworthy Cyberspace