Team Profile

• **Indiana University**
  – Principal Investigator: Jean Camp
  – Doctoral Researchers: Zheng Dong, Greg Norcie, Vaibhav Garg
  – Research Programmer: Constantine Murenin

• **USC Information Sciences Institute**
  – Principal Investigators: John Wroclawski and Jim Blythe
  – Doctoral intern: Shirin Nilizadeh
Customer Need

• Non-expert human decisions play a role in many cases of security failures.

• Improving communication, decision-making, and tool usability will have a large impact on security.

• People need security that fits: personalized, customized, and appropriate for the context.
  – Contexts: banking, work, high risk
  – Mental models: violent crime, mischievous vandals, bad neighborhoods, organized crime.
Approach

• HATS models the user and context to tailor communication
  – Tracks risk context to help identify problems and guide communication
  – Decision-theoretic reasoning about when and what to communicate
  – Tailors risk communication with mental models
  – Coordinates response through automation
Architecture of Approach

Risk Context Analysis

- Network Context
- Web Context
- User Context

- Observed urls
- Observed settings, network activity

- Browser settings
- Dialog specification

- Browser Interface

Intelligent Interaction

- Security reconfig
- Dialog generation

- Probabilistic reasoning

- Metaphors

Ontology/MLN

Year 1 design
Approach: Web Context

- Built learned models of web certificates, applied in real time for web context
  - Complements red/green lists approach
  - Sorting into banks, 6 large banks, phishing, rogue, other
  - Can classify and identify uncertainty in classification
  - URL history reputation system
Approach: Probabilistic Fusion

- Overall risk picture combines uncertain data from network, web and user contexts
- Use decision theory to decide when and how best to act and how to involve the user
- Markov logic network: uses human-readable rules, but compiles to a fast, optimal Bayesian network
Approach: Mental Models

- Your Actions are Risky
- Your Property is At Risk
- Mischievous Vandals Here
- Physical Threat - High Risk!
Benefits

• Involve the user in decision making when appropriate and with understandable information
  – Risk illustration, action, risk escalated or resolved

• High security defaults, simple to override, personalized to individual and context.

• Machine learning approach allows updating responses to emerging threats

• Off-the-shelf tools can be coordinated through the mental model
Competition

• Products
  – Everbank password reuse prevention
  – Custom security configuration and audit

• Research
  – Other usable security research groups

• Open source
  – Certificate pinning
  – No script
Current Status

- Key components of HATS prototype developed
  - Built learned models of web certificates, applied in real time for web context
  - Mental models identified, warnings designed
  - Implemented ontology and probabilistic reasoner for context fusion and interaction
Next Steps

- User testing will quantify benefits and data will fine-tune mental models approach

- Build out risk context: e.g. update user context from responses and integrate resources from related projects

- Web certificate next steps

- Porting to easily deployable real-time tool
Technology Transfer Activities

• Off the record all-day meeting at Indiana University
  – Potential users/tech transfer targets represented
    • Microsoft, Mozilla, Apple, Goldman Sachs
  – others represented
    • Tor, ISOC, CAIDA

• Industrial outreach
  – Microsoft Research – ongoing certificate analysis discussions, project intern, speaking invitation
  – Google via integration with Mozilla
  – Tor: https everywhere, certificate sharing

• Placed doctoral students in industry
  – PARC
  – Microsoft
  – Big Switch
Contact Information

http://UsableSecurity.net

• Jean Camp: UI PI
  Lindley Hall
  Office 230D
  Indiana University
  Bloomington, IN 47405
  – ljcamp@gmail.com

• Jim Blythe: USC ISI
  4676 Admiralty Way
  Suite 1001
  Marina del Rey, CA 90292
  – blythe@isi.edu