Science of Human Circumvention of Security

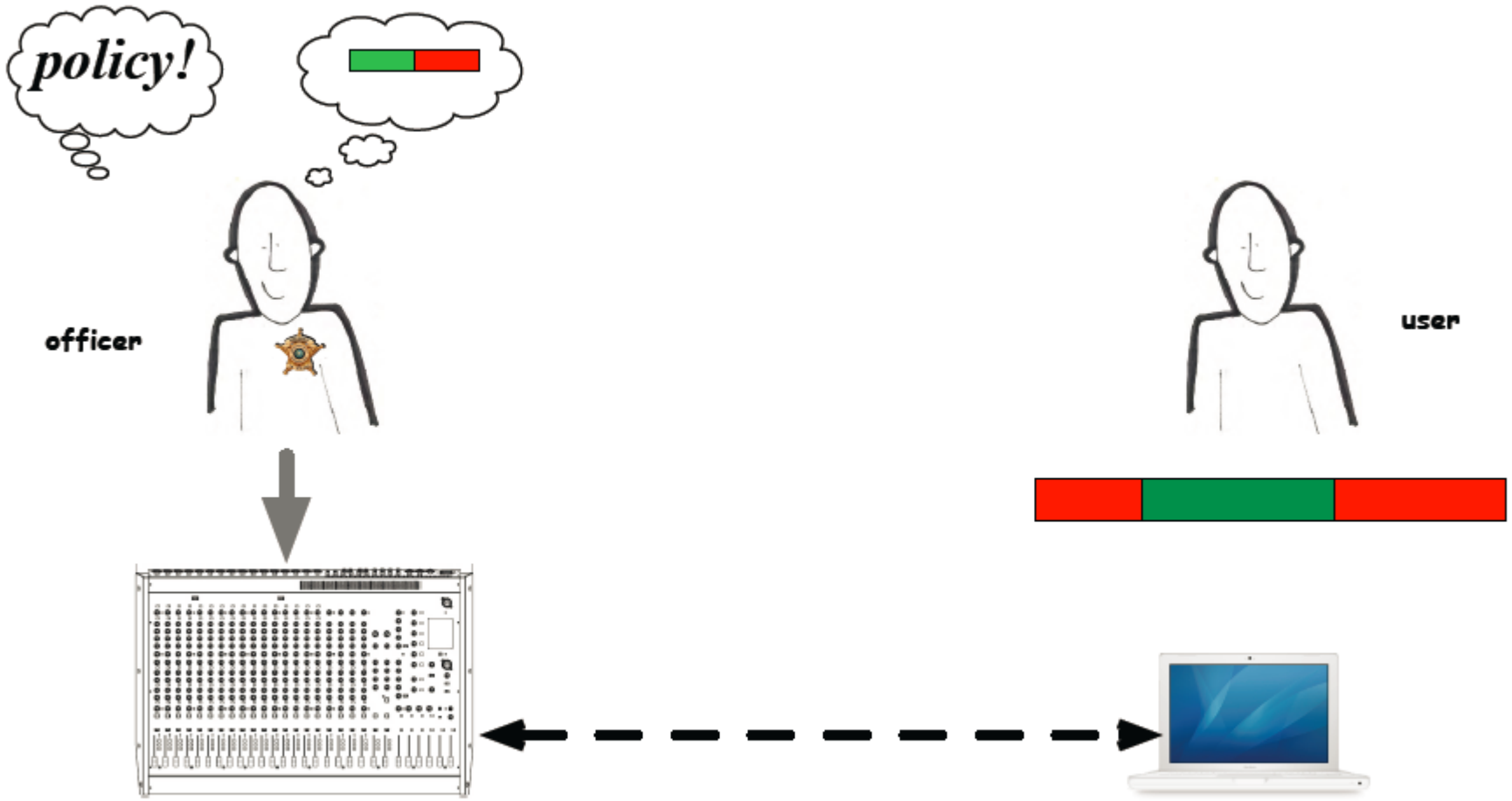
PIs: Tao Xie (Illinois), Jim Blythe (USC),
Ross Koppel (U Penn), Sean Smith (Dartmouth)

Our View of Science of Security: When Human and Machine (Security Control) Meet

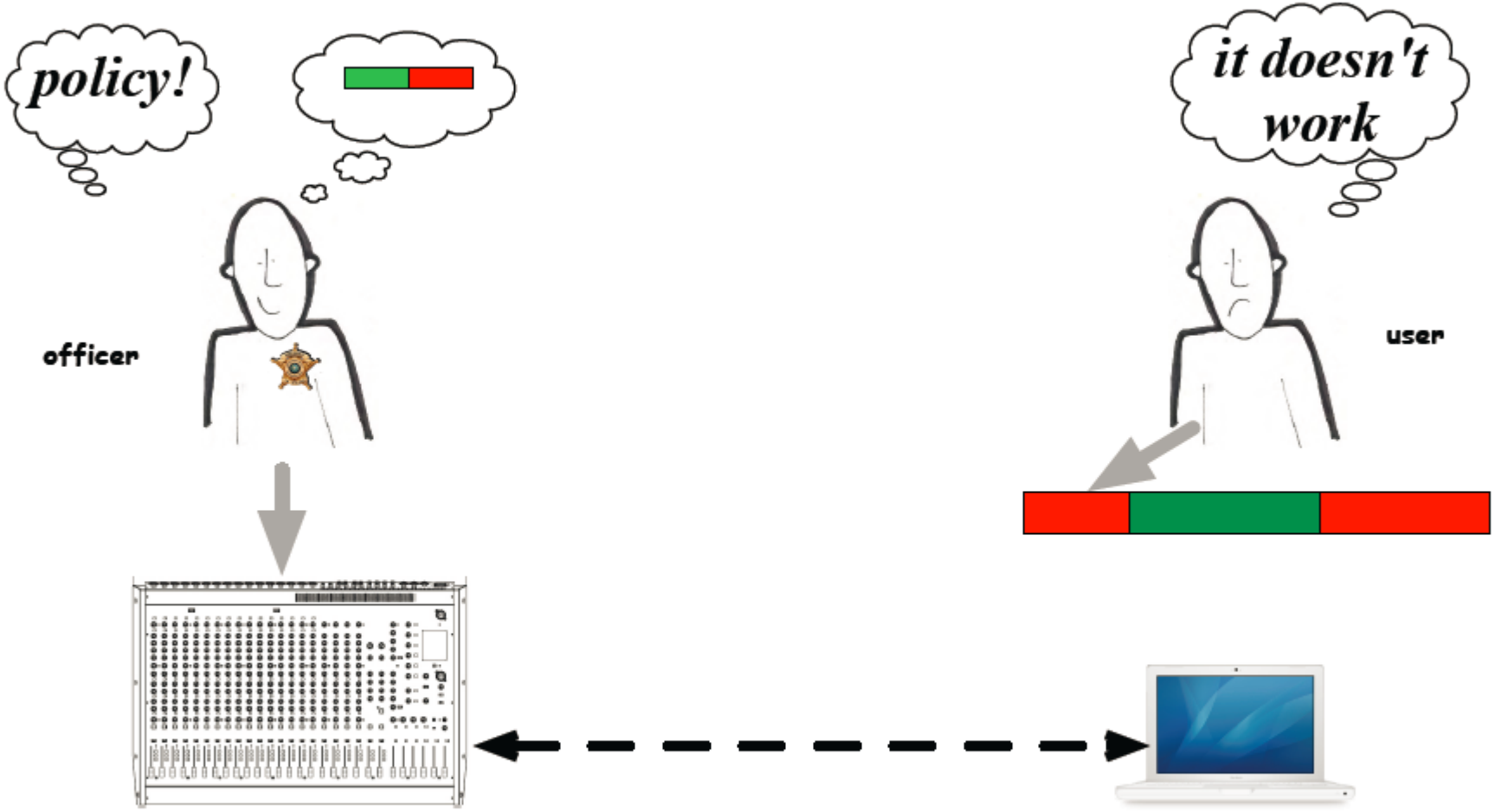
- **Assumption**: human circumvention of security control never happens or human decision on security control is perfect
- **Reality**: well-intentioned human users continually circumvent security controls or make uninformed security decision
- **Consequence**: the pandemic/ubiquitous fact of this circumvention/uninformed decision undermines the effectiveness of security designs

- Our project seeks to develop metrics to enable security engineers and other stakeholders to make meaningful, quantifiable **comparisons**, **decisions**, and **evaluations** of proposed security controls *in light of what really happens when these controls are deployed*.

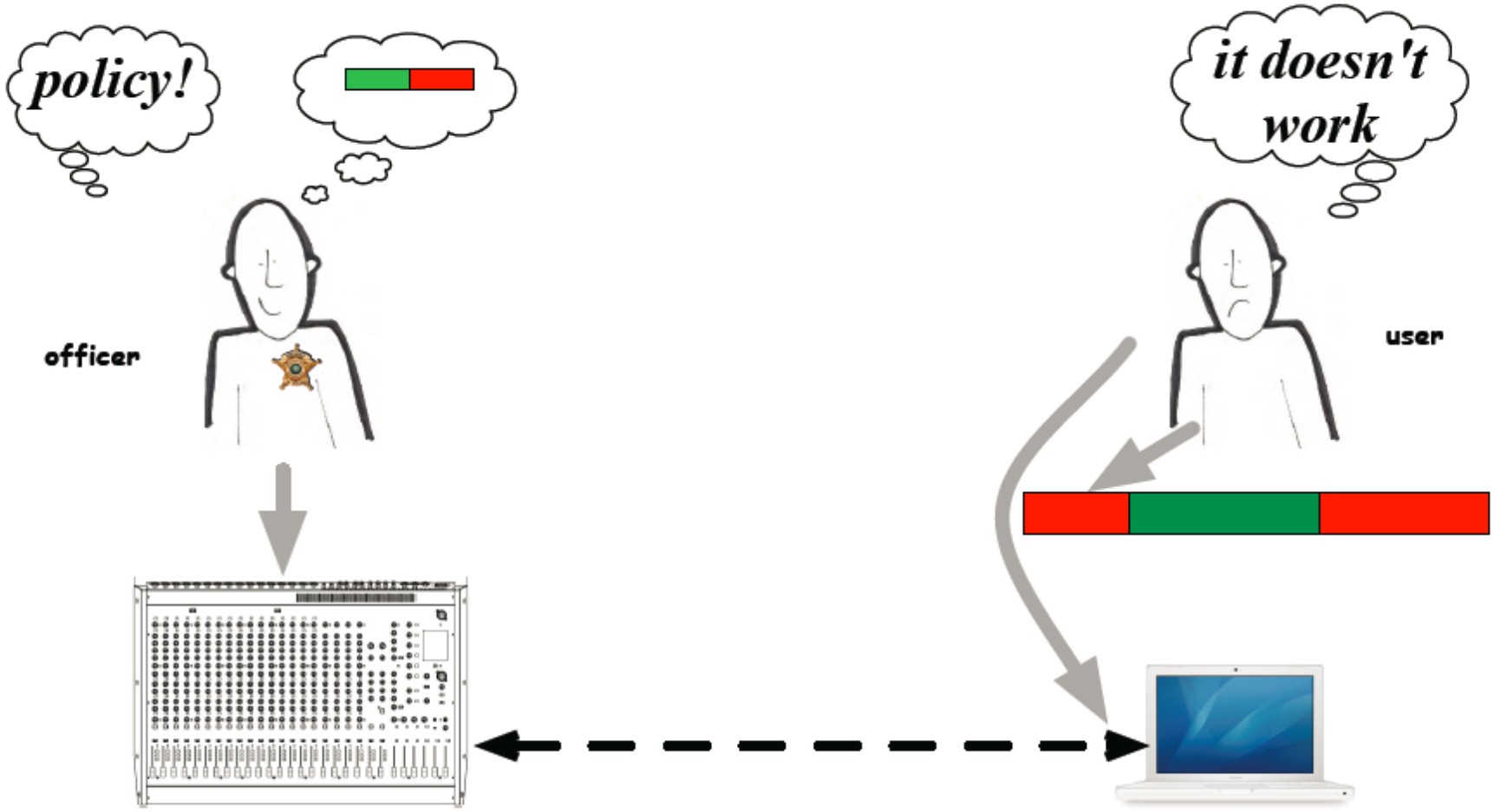
Manageability – Access Control Example



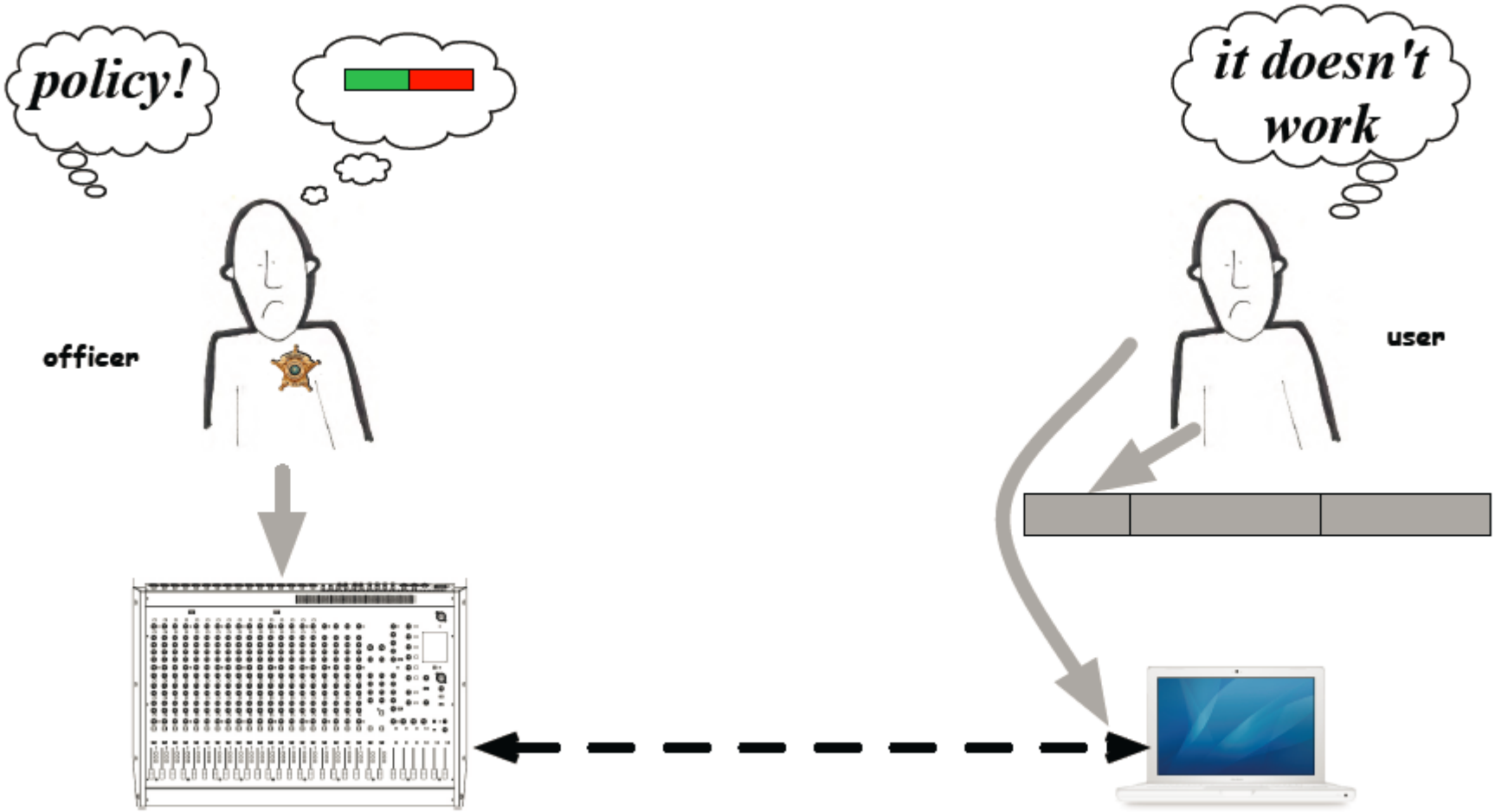
Manageability – Access Control Example



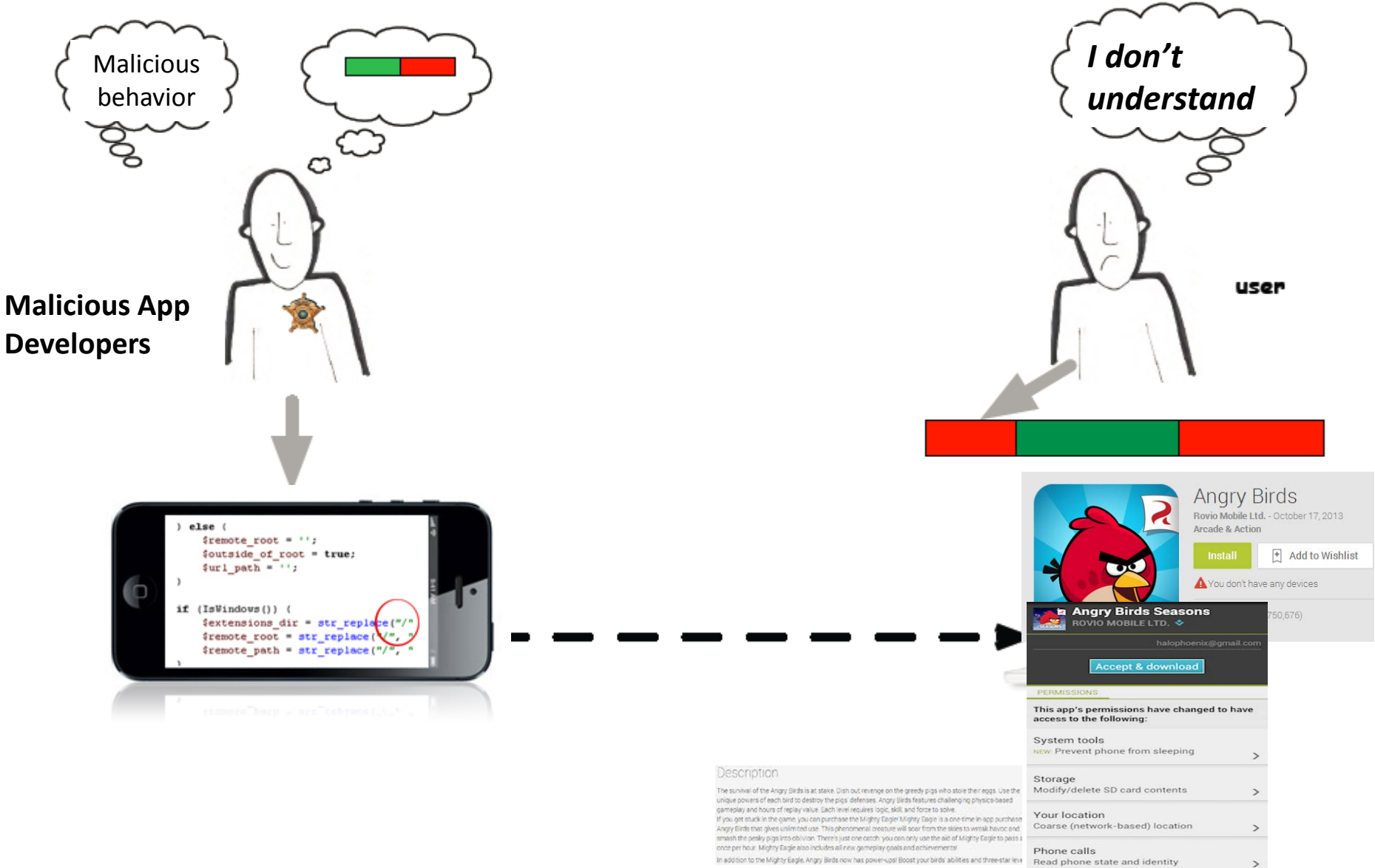
Manageability – Access Control Example



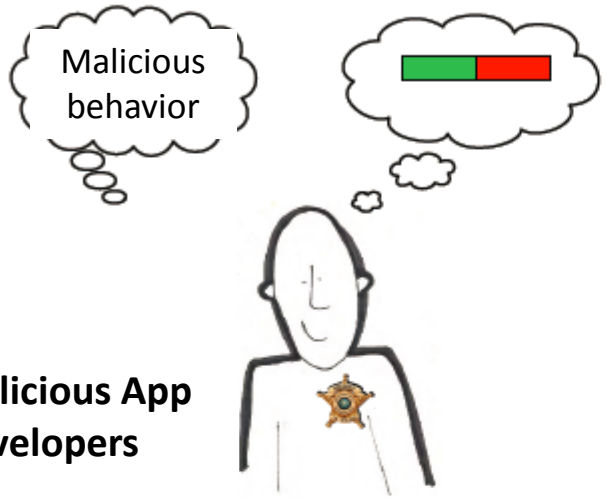
Manageability – Access Control Example



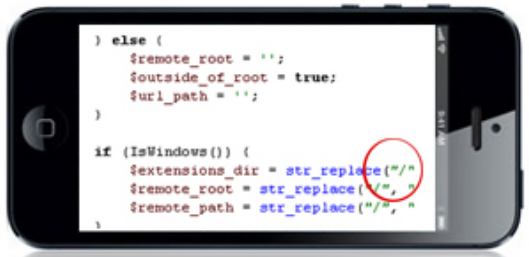
Manageability – Mobile App Permission Example



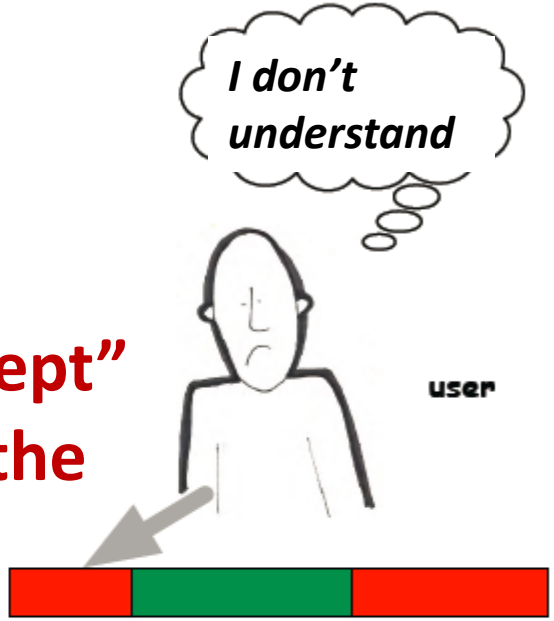
Manageability – Mobile App Permission Example



Malicious App Developers



Click "Accept" to Install the App



White Hats

People just trying to do their work

Workarounds – especially to cyber access

Good intent: unintended outcomes

Usually unfortunate rules: with lousy outcomes: lost productivity, frustration; more circumvention?

Security engineering doesn't work if we base it on the fantasy that all good users fully comply!

Science of Human Circumvention of Security

To better understand and *to model* computer access *workarounds*—their:

- **Reasons, norms, and justifications**
- **Tasks, urgency, and environments**
- **Role in others rule-following behaviors**
- **Methods of discovery**
- **Sensible (responsible & used) controls**

via

- **Fieldwork**
- **Modeling individuals and systems**
- **Validation**
- **Application to hard problems in the real world**

Computer-Access Workarounds in Healthcare

- Workarounds to computer access in healthcare are common but often go unnoticed (clinicians focus on patient care, not cybersecurity)
- Need to do analyses of computer rules, and interviews & observations w/ clinicians
- Conducted Interviews and observations with hundreds of medical workers and with 19 cybersecurity experts, CIOs, CMIOs (chief medical informatics officer), CTO, and IT workers
- Shadowed clinicians as they worked
- **Findings**: dozens of ways workers ingeniously circumvent security rules

Computer-Access Workarounds in Healthcare

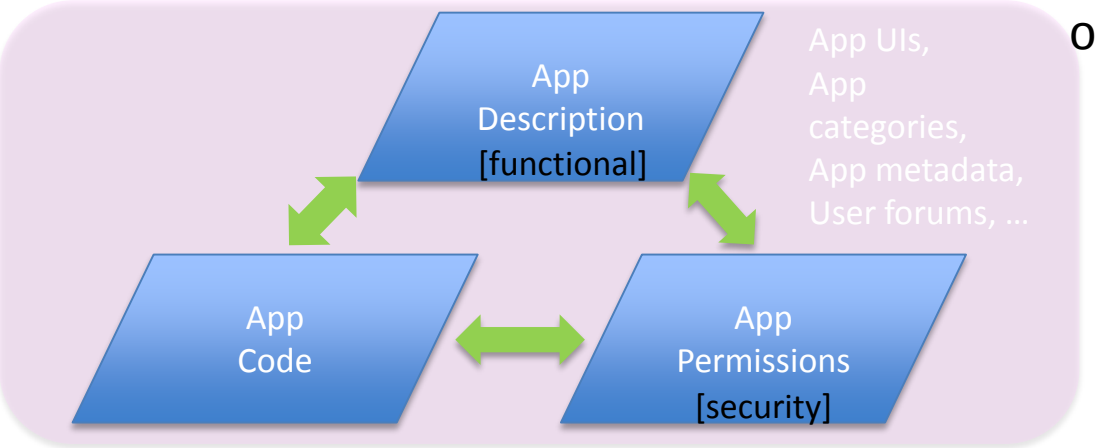
- R. Koppel, S. Smith, J. Blythe, and V. Kothari, “Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?” in Information Technology and Communications in Health (ITCH), 2015
- J. Blythe, R. Koppel, V. Kothari, and S. Smith. “Ethnography of Computer Security Evasions in Healthcare Settings: Circumvention as the Norm”. HealthTech’ 14: Proceedings of the 2014 USENIX Summit on Health Information Technologies, August 2014).
- R. Koppel. “Software Loved by its Vendors and Disliked by 70% of its Users: Two Trillion Dollars of Healthcare Information Technology's Promises and Disappointments”. HealthTech’ 14: *Keynote talk at the 2014 USENIX Summit on Health Information Technologies*, August 2014.
- R. Koppel, J. Blythe, and S. Smith. “Ethnography of Computer Security Evasions in Healthcare Organizations: Circumvention of Cyber Controls”. *Talk at the European Sociological Association Midterm Conference*, August 2014.

Computer Security Perils of Reuse

- System designers routinely reuse existing policies, technologies, and architectures—frequently with little or no changes
- Reuse is good software engineering practice
- **Findings**: Careless reuse in a different or even similar domain can introduce failures and new challenges that subvert security goals and impede organizational objectives

J. Blythe, R. Koppel, V. Kothari, S. Smith. "The Computer Security Perils of Reuse." Submitted for publication, December 2014.

Better Tool Support to Assist Human: User Perception + User Judgment

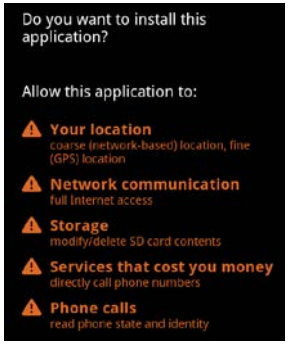


- Reason about user-perceived info, e.g., **WHYPER** [USENIX Security 13]

App Description Sentence

Linkage

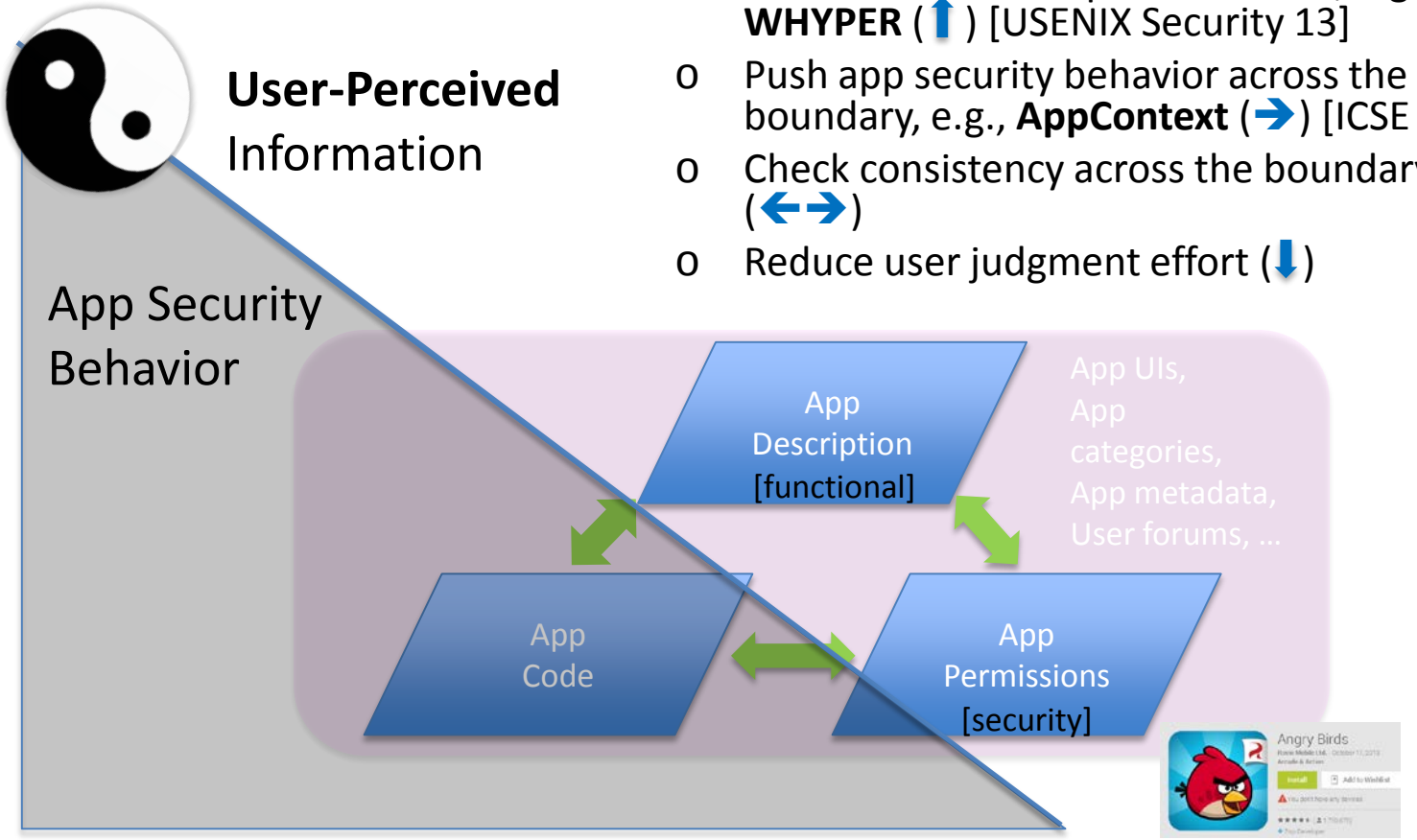
Permission



Rahul Pandita, Xusheng Xiao, Wei Yang, William Enck, and Tao Xie. WHYPER: Towards Automating Risk Assessment of Mobile Applications. In Proceedings of the 22nd USENIX Security Symposium (USENIX Security 2013), 2013.

Better Tool Support to Assist Human: User Perception + User Judgment

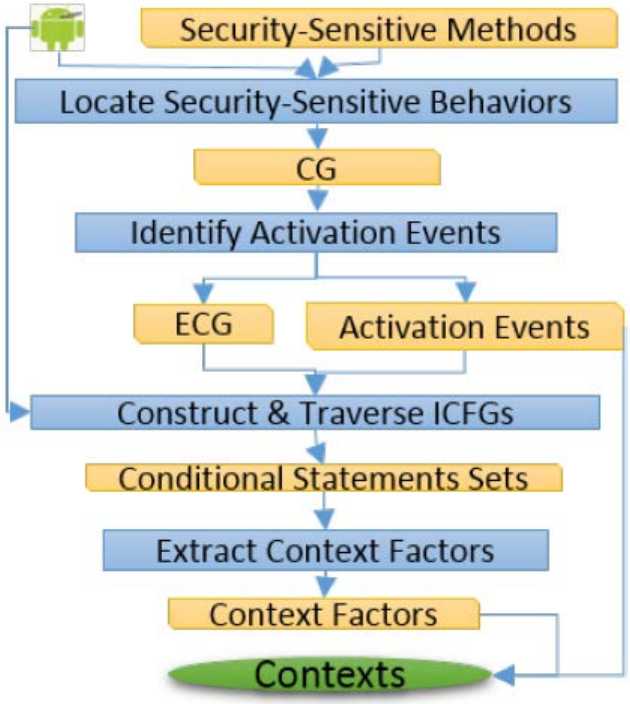
- Reason about user-perceived info, e.g., **WHYPER** (⬆) [USENIX Security 13]
- Push app security behavior across the boundary, e.g., **AppContext** (➔) [ICSE 15]
- Check consistency across the boundary (⬅➔)
- Reduce user judgment effort (⬇)

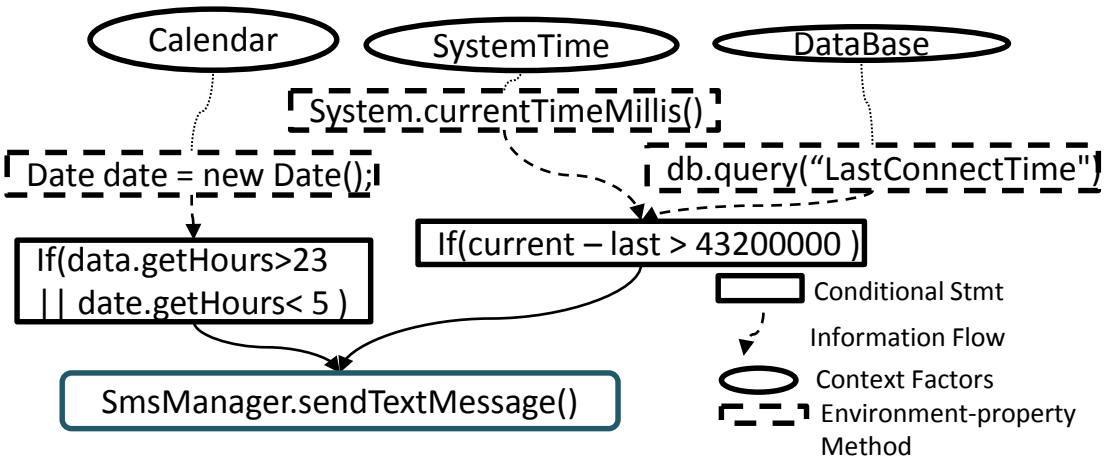


Mobile Malware: Characteristics

- Mobile malware leverage two major mobile-platform features
  - **Frequent** occurrences of **imperceptible** system events
    - E.g., many malware families **trigger** malicious behaviors via background events; in contrast, UI events activate when users using the app ➔ users are **around**!!
  - **Indicative** changes in external environments ➔ users not **around**!!!
    - E.g., DroidDream malware families **suppress**/**trigger** malicious behaviors during **day**/**night** time
- Malware strive to reach a *balance* between **prolonging** life time and **increasing** invocation chance, e.g., malicious behaviors invoked
  - **frequently enough** to meet the need, e.g., a few clicks/day from the device to improve search engine ranking of website X
  - **not too frequently/not wrong timing** for users to notice anomaly

AppContext





Context1: (Event: Signal strength changes), (Factor: Calendar)
Context2: (Event: Entering app), (Factor: Database, SystemTime)
Context3: (Event: Clicking a button)

Context factors: environmental attributes for affecting security-sensitive behavior's invocation (or not)

W. Yang, X. Xiao, B. Andow, S. Li, T. Xie, and W. Enck. AppContext: Differentiating Malicious and Benign Mobile App Behavior Under Contexts. In Proceedings of the 37th International Conference on Software Engineering (ICSE 2015), May 2015.

Context-based Security-Behavior Classification

Step 1. Transform contexts for each app's security behavior as features

Step 2. Label each behavior in training set as malware or benign

Step 3. Learn a predictive model via ML technique, e.g., support vector machine (SVM)

Step 4. Classify an unlabeled behavior as malware or benign via the model

TABLE I
LIST OF FEATURES FOR CLASSIFICATION

Features of Behavior Information		
Permission	Security-sensitive method call	
Features of Activation Event		
SystemUI event	System event	UI event
Features of Context Factors		
List of environmental attributes		

Permission	Method Call	SystemUI	System	UI	F_1	F_2	F_3*	F_4*	F_5*	F_6	...	F_{142}
SEND_SMS	*sendTextMessage*	N/A	SIG_STR	N/A	0	0	1	0	0	0	...	0
SEND_SMS	*sendTextMessage*	EnterApp	N/A	N/A	0	0	0	1	1	0	...	0
SEND_SMS	*sendTextMessage*	N/A	N/A	Click	0	0	0	0	0	0	...	0

* F_3 = Calendar, F_4 = System Time, F_5 = Database

W. Yang, X. Xiao, B. Andow, S. Li, T. Xie, and W. Enck. AppContext: Differentiating Malicious and Benign Mobile App Behavior Under Contexts. In Proceedings of the 37th International Conference on Software Engineering (ICSE 2015), May 2015.

Our View of Science of Security: When Human and Machine (Security Control) Meet

- **Assumption**: human circumvention of security control never happens or human decision on security control is perfect
- **Reality**: well-intentioned human users continually circumvent security controls or make uninformed security decision
- **Consequence**: the pandemic/ubiquitous fact of this circumvention/uninformed decision undermines the effectiveness of security designs

- Our project seeks to develop metrics to enable security engineers and other stakeholders to make meaningful, quantifiable **comparisons**, **decisions**, and **evaluations** of proposed security controls *in light of what really happens when these controls are deployed*.

Science of Human Circumvention of Security

PIs: Tao Xie (Illinois), Jim Blythe (USC),
Ross Koppel (U Penn), Sean Smith (Dartmouth)

Questions??