Progress, Problems, Publications, Plans and Promises of the Group Studying Passwords and Cyber Security Circumvention

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

(False) Assumptions of Security Designers:

Circumvention of security control by humans is:

- Not common
- Only from outside threats
- *Reflects: laziness, skill deficits, or lack of training/understanding*
- Never happens
- **Is solved by technology**
- Or, human decisions on security control are fine ☺

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

- **Reality**: well-intentioned human users continually circumvent security controls or make uninformed security decisions (Why?…just wait)

White Hat

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

- **Consequences**: pandemic/ubiquitous circumvention and uninformed decision:
- Undermines effectiveness of security designs
- *Corrodes* belief in administrators and security rationales
- Creates an environment of workarounds as:
  - **required**
  - **fun**
  - **thoughtful**
  - **consistent with real mission of organization**
  - **"us vs. them."**

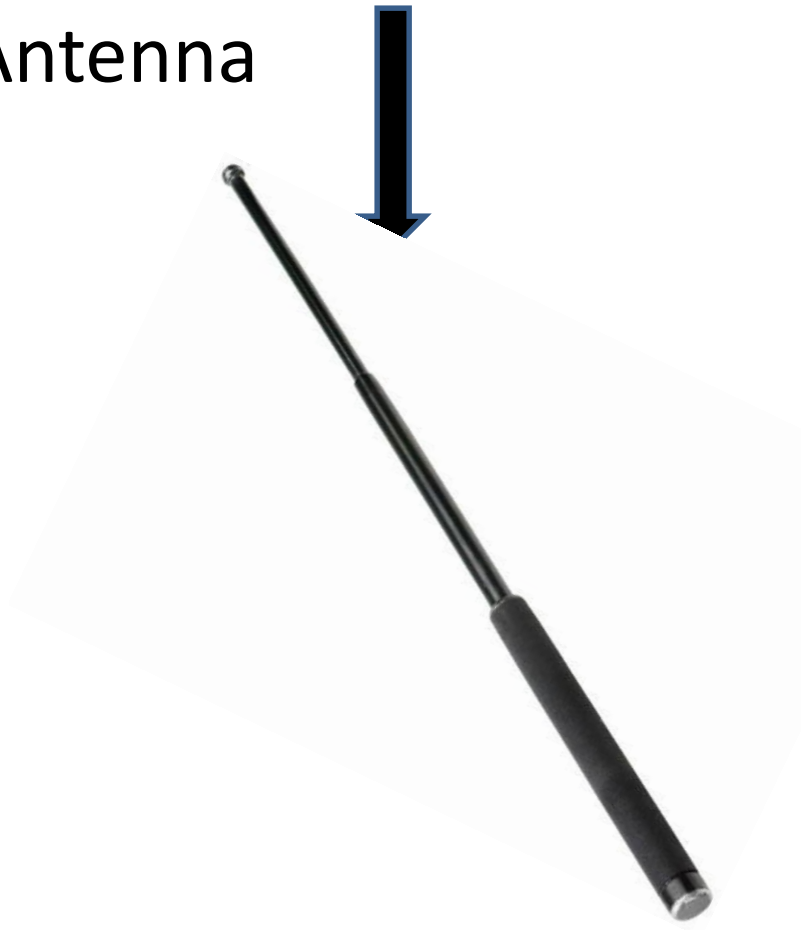
View of passwords inside the supply room

"Simulated" to avoid ethical violations and jail


?
Office DEPOT
matte finish
invisible tape
write on matte surface
write on mail
LSDA

Two Examples for fun: 1. Proximity Indicator

Antenna



Styrofoam Cup

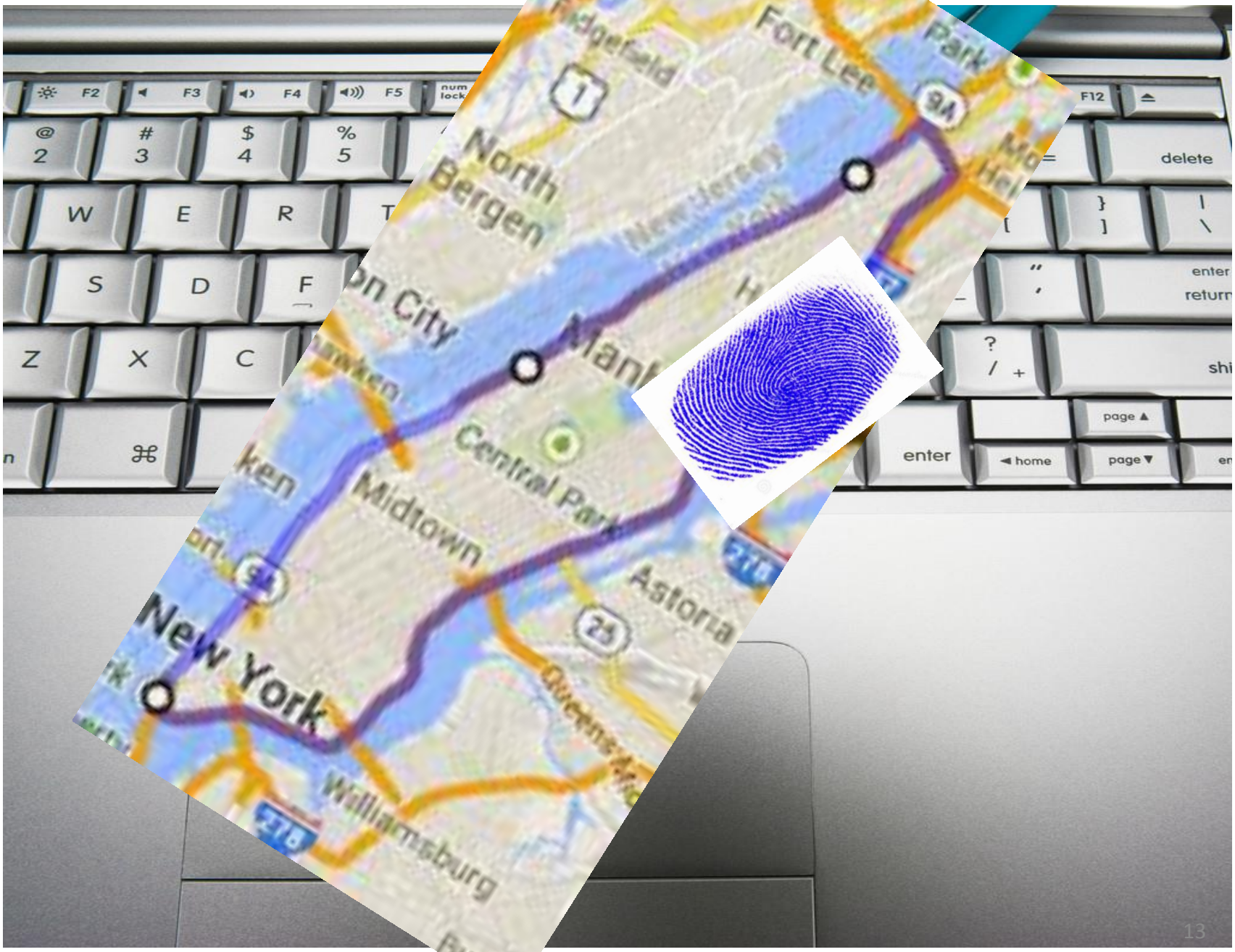
Proximity Indicator: Defeated


Leonia
Fort Lee
Park
North Bergen
Midtown
Central Park
Astoria
New York
Williamsburg

2. Dr. Death and NY Requirements

http://www.omgubuntu.co./2013/03/how-to-get-your-fingerprint-reader-working-in-ubuntu

http://www.amazon.com/Verifi-P2000-Premium-Fingerprint-Reader/dp/B005VF62KG


North Bergen
Fort Lee
Midtown
Central Park
New York
Astoria
Williamsburg


My Passwords


NOT my passwords

Permission management: Who are you?

…And all the men and women merely players.
They have their exits and their entrances,
And one man in his time plays many parts…

- This hour?
- This week?
- Multiple roles: Multiple permissions

Timing….

Too Low Blood Pressure in the ER for… the Computer

Fire Suppression System Code

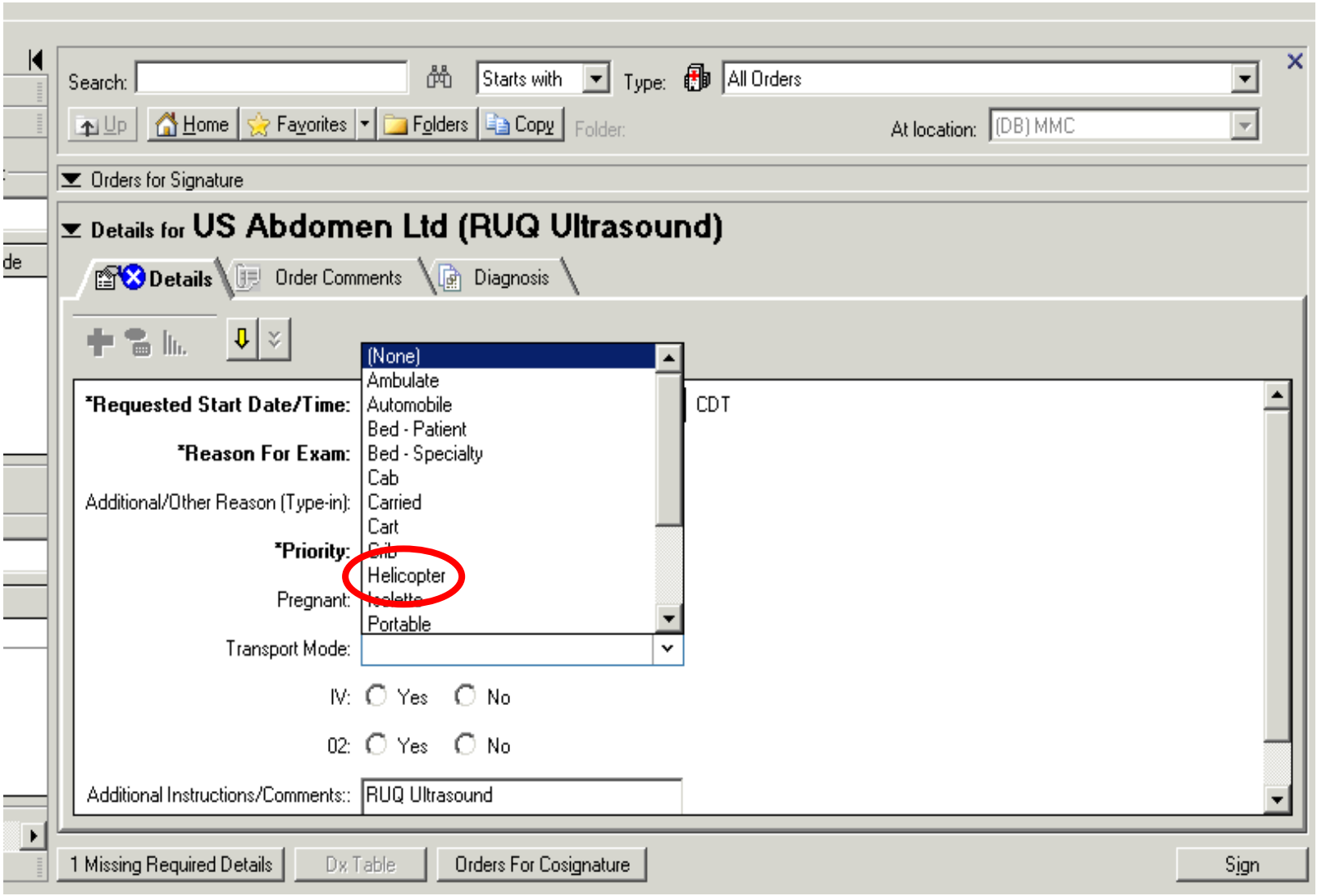
Unnamed US defense agency rules on passwords;

Change every 90 days; 2 capitals, 2 #s, 2 lower case, 2 special characters.

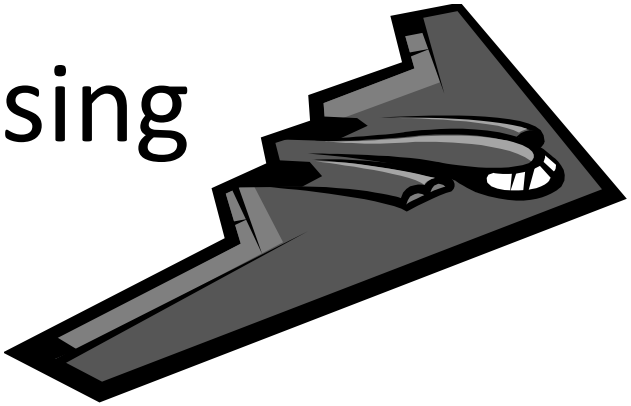
Can't reuse for 5 iterations

Solution: "Forget" password on day 1

Reach behind (in)security


Search:
Starts with
Type:
All Orders
Up
Home
Favorites
Folders
Copy
Folder:
At location:
(DB) MMC
Orders for Signature
Details for US Abdomen Ltd (RUQ Ultrasound)
Details
Order Comments
Diagnosis
(None)
Ambulate
Automobile
Bed - Patient
Bed - Specialty
Cab
Carried
Cart
Helicopter
Portable
*Requested Start Date/Time:
CDT
*Reason For Exam:
Additional/Other Reason (Type-in):
*Priority:
Pregnant:
Transport Mode:
IV: Yes No
02: Yes No
Additional Instructions/Comments::
RUQ Ultrasound
1 Missing Required Details
Dx Table
Orders For Cosignature
Sign

Ex Stealth Dosing



Bug Beeper (Anti Microbial Monitoring Unit)

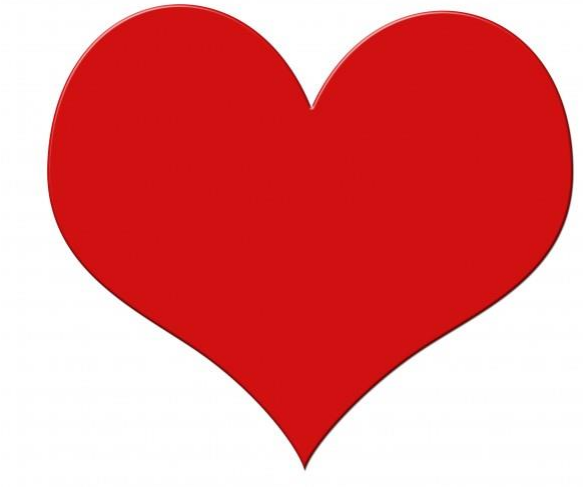
8 AM to 10 PM

Reasons: cost and patient safety

Workaround: Stealth Dosing

When Human and Machine (Security Control) Meet

Our project: 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*.



WORKAROUNDS TO CYBER ACCESS:

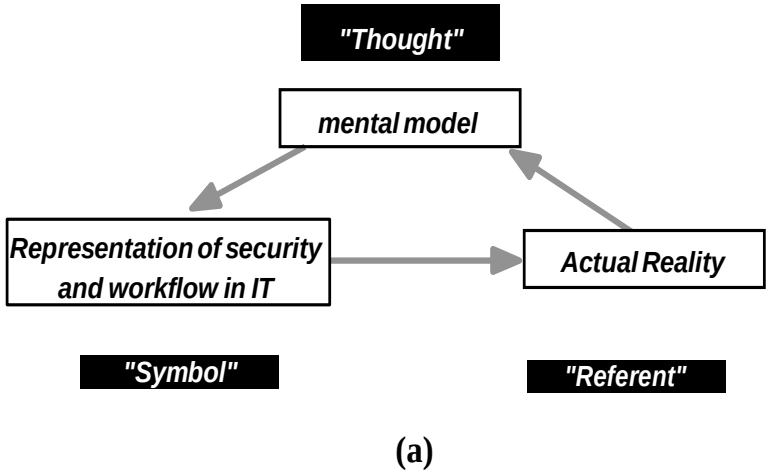
People just trying to do their work

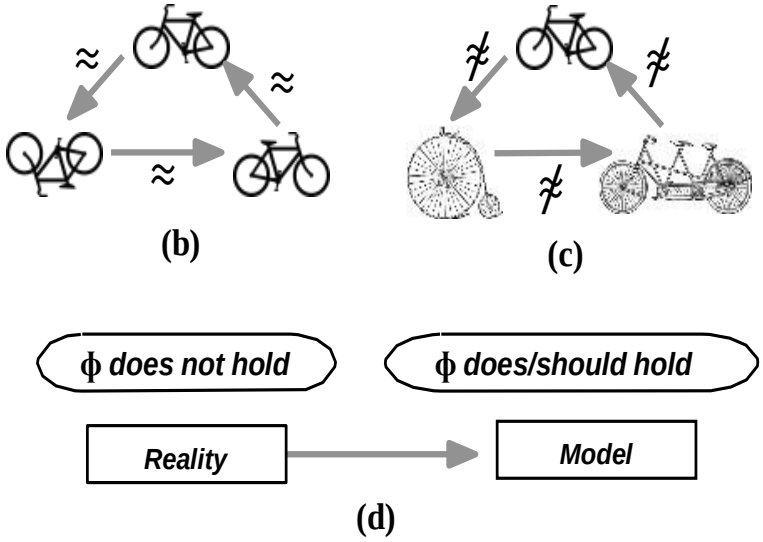
Good intent: unintended outcomes

Usually unfortunate rules: with lousy outcomes: lost productivity, frustration and more circumvention. **Security engineering doesn't work if we base it on the fantasy that all good users fully comply**

Goal: to model and to build science

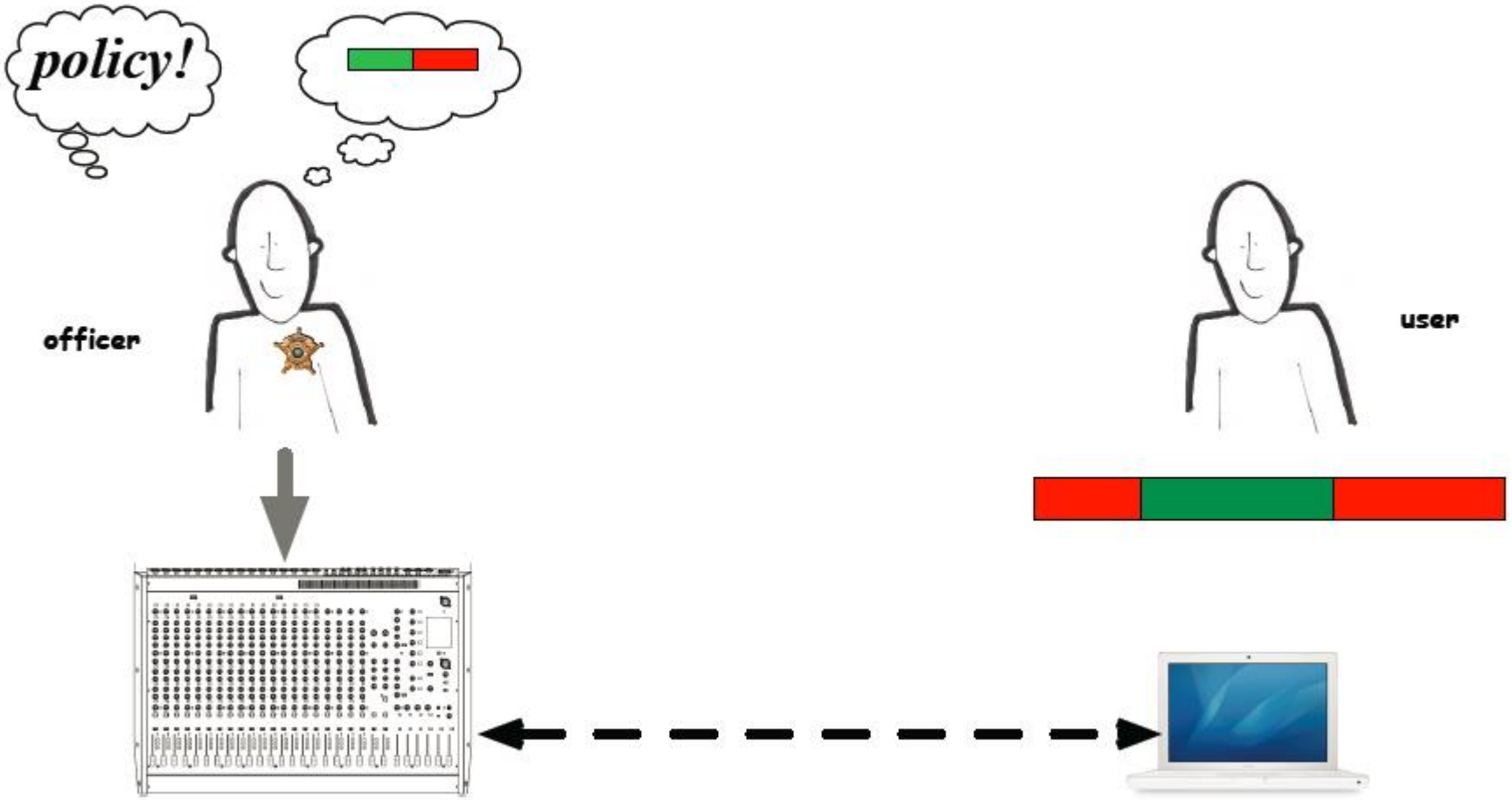
MISMORPHISM (different mental models of users vs. administrators: rules don't make sense)



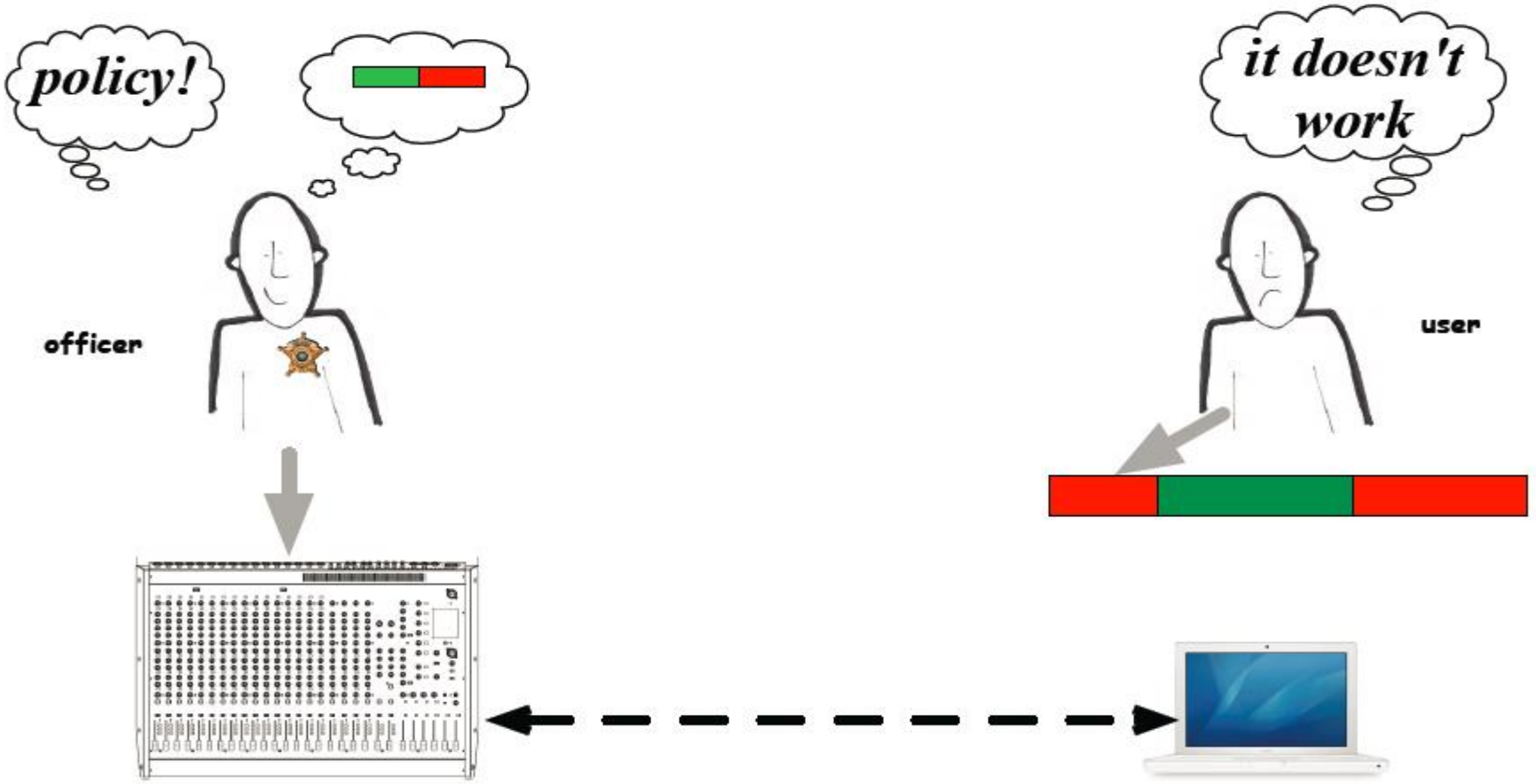


In circumvention semiotics, we think about mappings that fail to preserve structure, e.g., in a standard mismorphism scenario, the generated reality fails to embody a property the user regards as critical.

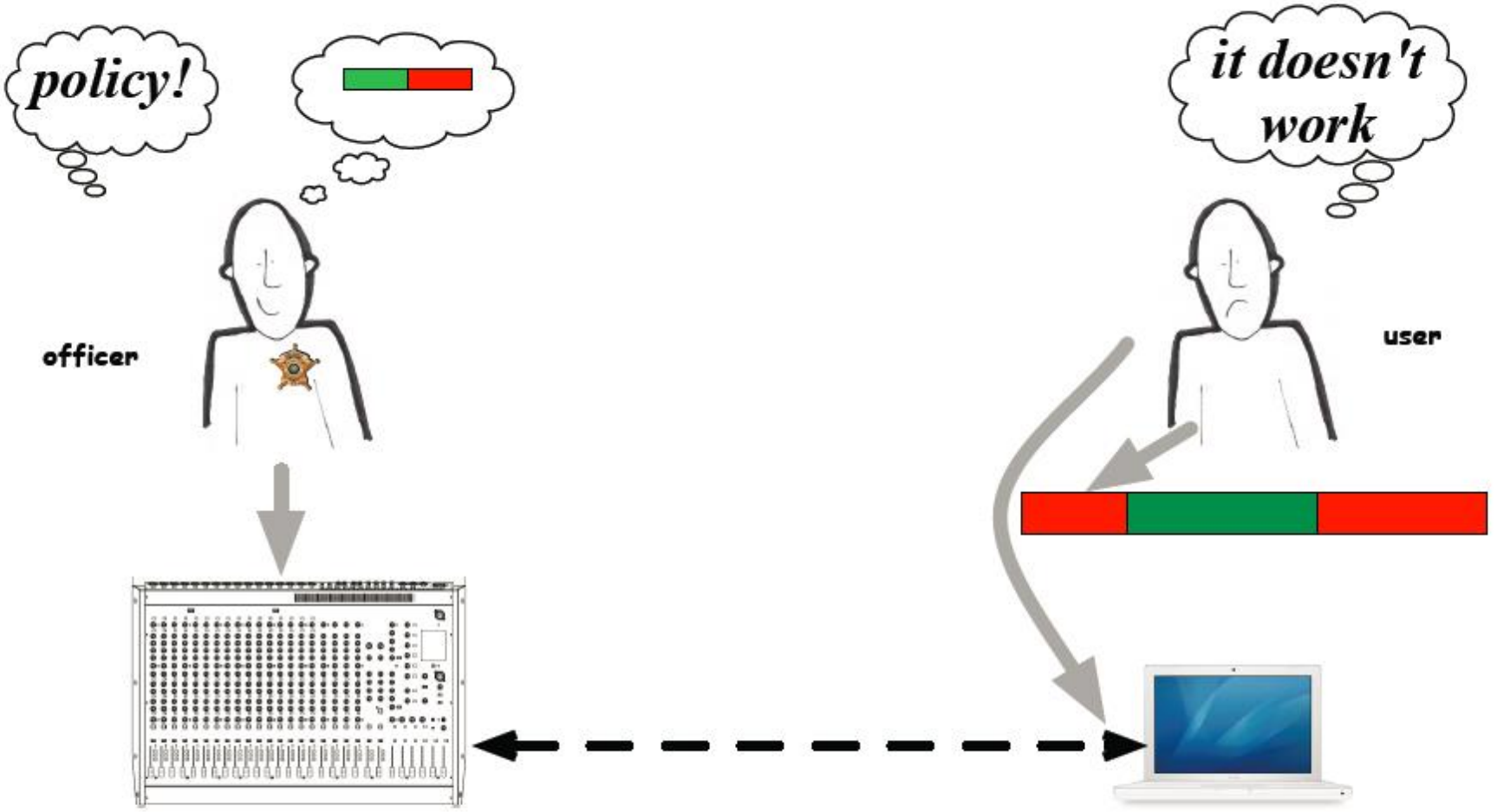
Manageability – Access Control Example



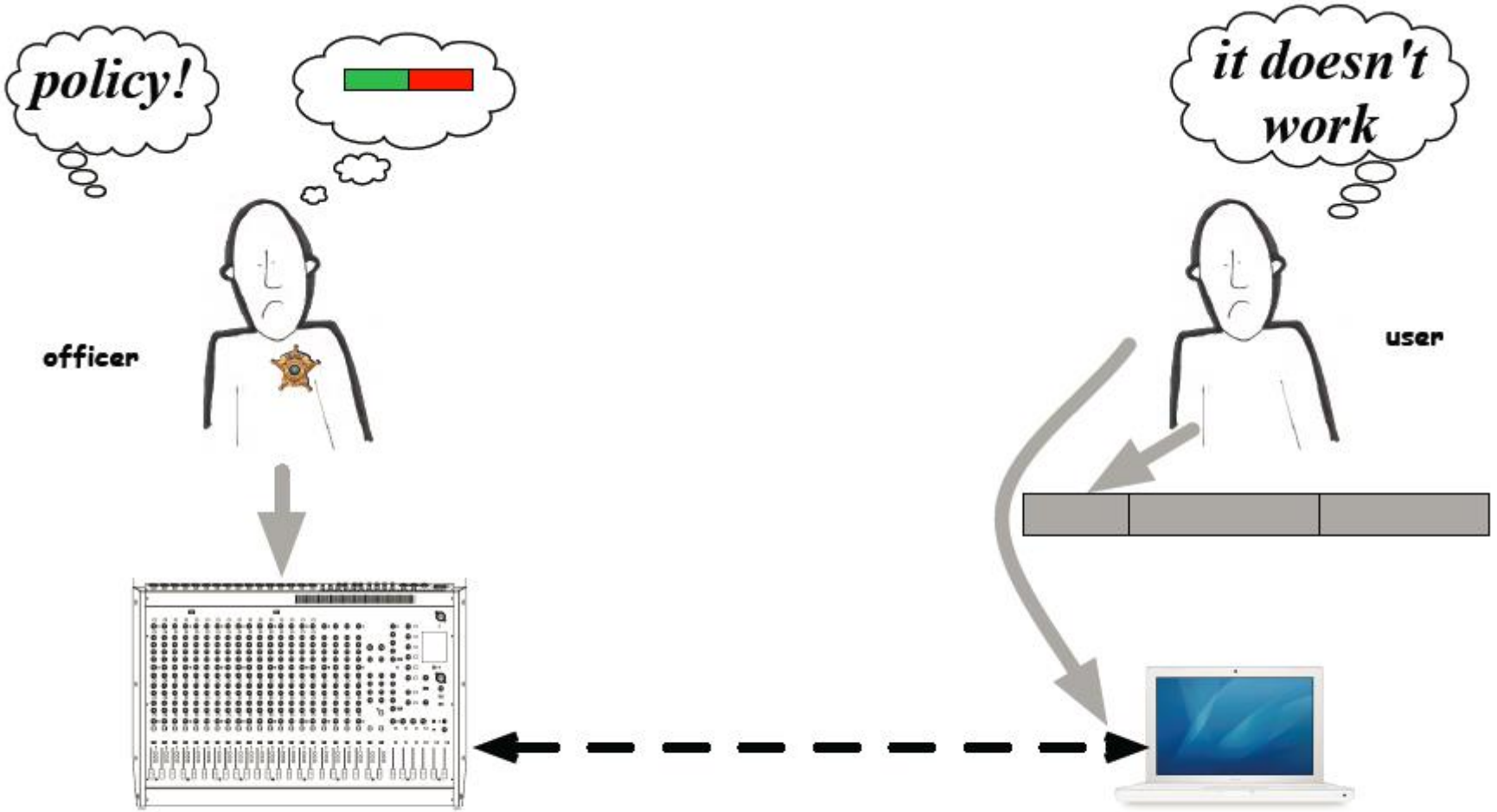
Manageability – Access Control Example



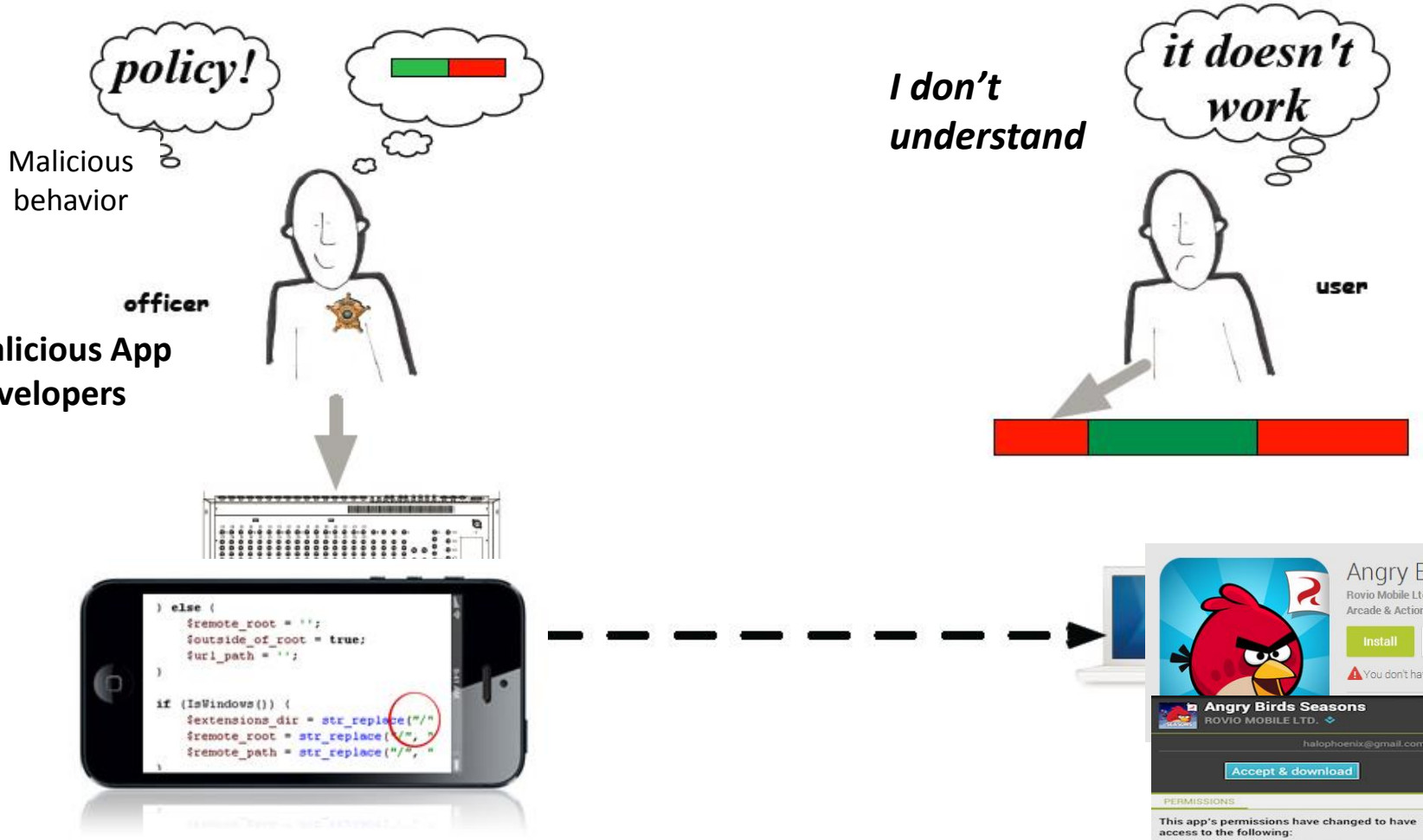
Manageability – Access Control Example



Manageability – Access Control Example



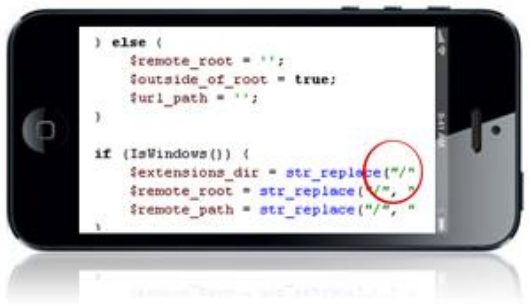
Manageability – Mobile App Permission Example



Manageability – Mobile App Permission Example

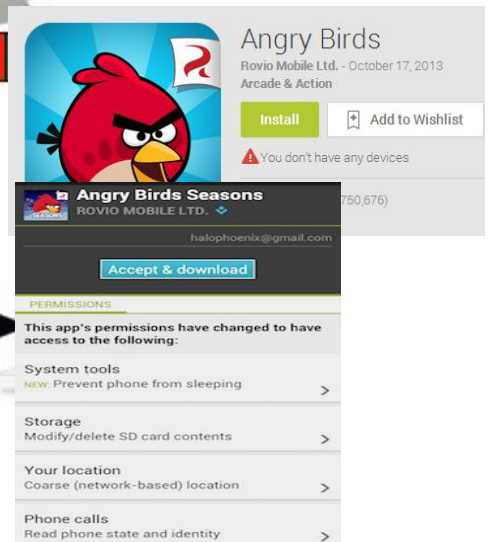
Malicious behavior

Malicious App Developers

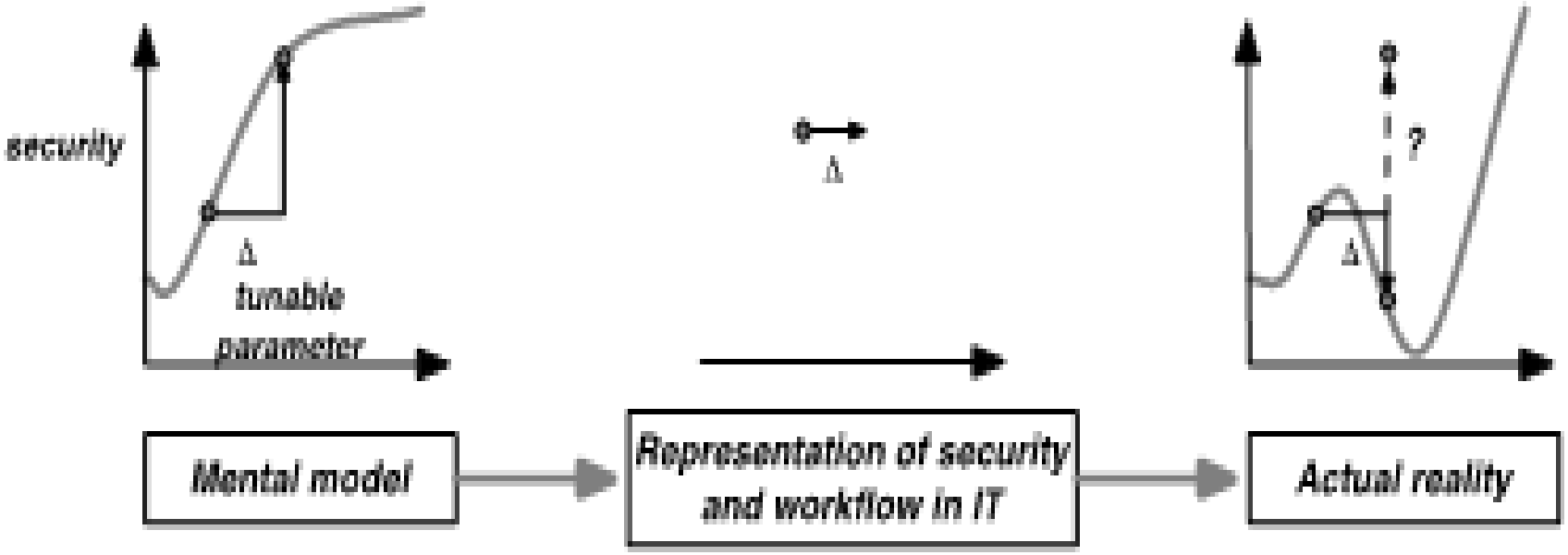


I don't understand

Click "Accept" to Install the App



Uncanny Decent



WHY? Cyber Security Access Workarounds = F

- Perceived importance/criticality of the task and the mission of the organization
- Perceived authority to act outside of the usual boundaries, e.g., I'm a doctor
- Perceived urgency, e.g., patient dying, network about to crash
- Belief that cyber access workarounds are common…or at least common among my group, i.e., everyone else does it/management knows about it/ passwords posted on the walls
- Cybersecurity beliefs carried from previous settings

WHY? Cyber Security Access Workarounds = F

- Perceived insensitivity/misunderstandings of the administrators/security designers:
  - rules don't make sense or **mismorphisms** * (*This is dynamic)
  - "Rules are not for *our* workflow"

  Always satisficing
- Rage/frustration with organization or software
- Perceived probability of not being caught
- Inappropriateness or clunkiness of the software in general
- Exhaustion/time of day (new study)

Modeling individuals and systems

1. Observations
2. Shadowing
3. Logs of access and change requests
4. Surveys
5. Interviews
6. Simulations and Mechanical Turk
7. Altering rules and measuring change
8. Comparison of different settings & rules
9. Understanding workflow in relation to software
10. Agent-based modeling, e.g., DASH
11. Keystroke analysis/ mouse tracking
12. fMRI with assigned tasks

Accomplishments (1)

- Dartmouth Ph.D. student Vijay Kothari and Co-PI Blythe continue to develop **DASH simulations of human agents in workaround settings, to support simulation of password and other security behavior.**
- PI Koppel revised the **survey to examine CISO/CIO attitudes and perceptions**, and submitted to additional populations via Educause group focused on informatics and cyber security. Received completed instruments, which we have analyzed and shared with colleagues.
- PI Blythe is designing **Mechanical Turk experiment to examine users' behaviors when logging in to various accounts**. Experiment (with Dartmouth) will allow us to capture **key strokes, strategies, systems of password reuse and protection**
- Blythe is developing DASH simulations of human agents for capture-the-flag scenarios designed to test the impact of workarounds in an attack, attacker bounded rationality and teamwork among defenders.
- Blythe, Koppel, and Smith **are exploring ways in which lay people don't understand requirements for cyber security** and the implications of that limitation on data and password safety

Accomplishments (2)

- Blythe, Koppel and Smith are exploring **data-driven models of password creation.**
- PI Koppel appointed member of advisory board of the Patient Privacy Rights Foundation (Dallas, TX), an organization that focuses on security of patient information in healthcare institutions.
- PI Koppel working with UC Irvine medical center on software integration and protection of patient data. Conducted interviews with clinicians and administrators and leaders. Also creating survey for use by all clinicians, IT personnel, and administrations on interoperability and data access.
- PhD student Wei Yang advised by PI Xie presented the **AppContext work in ICSE 2015** in May 2015.
- PI Xie led efforts for **designing secure coding duels in Code Hunt for the education and training of secure coding.** Xie presented the initial results as a poster in HotSoS 2015 in April 2015.
- PI Xie led Ph.D. students Wei Yang and Blake Bassett on **developing tool support for analyzing mobile apps**, e.g., to extract contextual information of command-and-control behavior of a bot mobile app so that users of the mobile app can view more detailed information for determining whether the mobile app may be a malicious app or not.

Accomplishments (3)

- Smith/Blythe/Koppel team migrated the **circumvention catalog** from NVivo (a single-site tool) to DeDoose, which allows the entire team to access it.
- PI Koppel is leading a revision of the **survey—to examine CISO/CIO attitudes and perceptions.**
- PIs Smith and Koppel and their research groups met for a face-to-face workshop in 2014 and discussed the ongoing DASH simulation work, the survey work, the corpora of workarounds and other **IT mismatches (now up to about 300), and the analysis of that based on the semiotic framework** that the team used in the earlier JAMIA paper. One consequence of that meeting was the decision to move the corpora into a qualitative research tool (NVivo). Migration and initial coding is now complete; the **team is now planning a follow-on to the JAMIA paper focusing on this analysis.**
- The team presented resulting work [1] at the **USENIX HealthTech Summit** in August, and is also using that to gather more data (by preparing a follow-on survey on circumvention, to send to the participants).
- Dartmouth Ph.D. student Vijay Kothari continued exploring **DASH models** with PI Blythe, with an eye towards choosing the **scenarios to model in a multi-agent setting,** the hypotheses to initially explore, and how to validate the resulting models.

Accomplishments (4)

- PI Blythe led the USC **team developed two agent models that exemplify different kinds of behaviors: multi agent workflow (hospital ward auto-logout) and individual cognitive (password mgmt)**. The USC team has also further developed the design for a human subject behavioral study platform linking mechanical turk users to a network testbed.
- PhD student Wei Yang advised by PI Xie presented the **AppContext work in ICSE 2015** in May 2015.
- PI Xie led efforts for designing secure coding duels in **Code Hunt for the education and training of secure coding**. Xie presented the initial results as a poster in HotSoS 2015 in April 2015.
- PI Xie led Ph.D. students Wei Yang and Blake Bassett on **developing tool support for analyzing mobile apps,** e.g., to extract contextual information of command-and-control behavior of a bot mobile app so that users of the mobile app can view more detailed information for determining whether the mobile app may be a malicious app or not.
- Smith/Blythe/Koppel team is exploring using **NLP/automatic text analysis on problem reports and change logs from partner IT departments (unearthed during our fieldwork), and also using these techniques on the open-ended responses to our questionnaire.**

Accomplishments (5)

- PI Blythe continued working on modeling BCMA workarounds in DASH. PI Smith mined the literature and ideas unearthed during his winter-term "Special Topics" class for circumvention scenarios and motivations. PI Koppel has continued his work with surveys and interviews.
- PI Blythe presented **our agent paper [1] at ACySE** in May, 2014; PI Koppel presented "**Ethnography of Computer Security Evasions in Healthcare Organizations: Circumvention of Cyber Controls**" (Koppel, Blythe, Smith, Kothari) at the European Sociological Association Midterm Conference in August. The JAMIA paper by Smith and Koppel on usability problems with health IT (pre-SHUCS, but related) was named **"among most significant papers of the year."** We are updating that paper to include: mental models of: payers (key), administrators, patients, and to include circumvention triggers.
- Topics" class for circumvention scenarios and motivations. PI Koppel has continued his work with surveys and interviews.

Accomplishments (6)

- PI Xie led efforts for designing **secure coding duels in Code Hunt** for the education and training of secure coding. Xie presented the initial results as a poster in HotSoS 2015 in April 2015.
- PI Xie led Ph.D. students Wei Yang and Blake Bassett on **developing tool support for analyzing mobile apps**, e.g., to extract contextual information of command-and-control behavior of a bot mobile app so that users of the mobile app can view more detailed information for determining whether the mobile app may be a malicious app or not.

Some recent Publications & Presentations by Smith, Blythe & Koppel etc (1)

[1] R. Koppel, S. Smith, J. Blythe, and V. Kothari, "**Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?**" Driving Quality in Informatics: Fulfilling the Promise. K.L. Courtney, Alex Kuo, Omid Shabestari, Eds. Series on Technology and Informatics, 209. Amsterdam, Netherlands: IOS Press, 2015

[2] R. Koppel, S. Smith, J. Blythe, and V. Kothari, "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?" **Presentation by Koppel at International Conference Addressing Information Technology and Communications In Health, 2015. Victoria, BC, Canada**. February/March 2015

[3] S.W. Smith, R. Koppel, J. Blythe, V. Kothari. **Mismorphism: A Semiotic Model of Computer Security Circumvention (Extended Version)**. Computer Science Technical Report TR2015-768. Dartmouth College. March 2015.

[4] **Mismorphism: a Semiotic Model of Computer Security Circumvention** Smith, Koppel, Blythe and Kothari 9th International Symposium on Human Aspects of Information Security and Assurance, 2015 Smith Presented this in July 2015

Some recent Publications & Presentations by Smith, Blythe & Koppel etc (2)

[5] Koppel: **keynote presentation at Royal College of Physicians (Edinburgh) on healthcare software usability and the influence on compliance with cyber security rules** February 2015 (Co-presented with Professor Harold Thimbleby, Computer Science Department, Swansea University) "**Dangers and Frustrations of Poorly Designed and Badly Implemented Healthcare IT: Implications for Medication Errors**"

[6] Koppel gave **presentation to Wales Health Trust at Prince of Wales Hospital**, Swansea, Wales, UK. February 2015.

[7] V. Kothari, J. Blythe, S.W. Smith, R. Koppel. "**Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling**." Symposium and Bootcamp on the Science of Security (HotSoS 2015). ACM. Accepted for publication; to appear April 2015.

[8] S.W. Smith, R. Koppel, J. Blythe, V. Kothari. "**Mismorphism: A Semiotic Model of Computer Security Circumvention** (Poster Abstract)." Symposium and Bootcamp on the Science of Security (HotSoS 2015). ACM. Accepted for publication; to appear April 2015. See [3 and 4] above.

Some recent Publications & Presentations by Smith, Blythe & Koppel etc (3)

[9] 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).

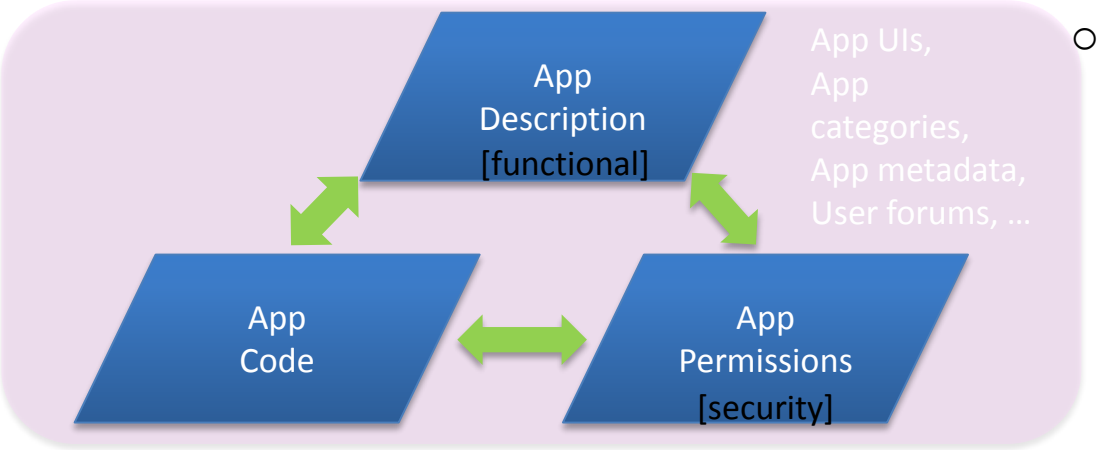
[10] R. Koppel. "Software Loved by its **Vendors and Disliked by 70% of its Users: Two Trillion Dollars of Healthcare Information Technology's Promises and Disappointments**". HealthTech' 14: Keynote talk at the 2014 USENIX Summit on Health Information Technologies, August 2014.

[11] 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.

Recent Papers and Presentations by Xie et al

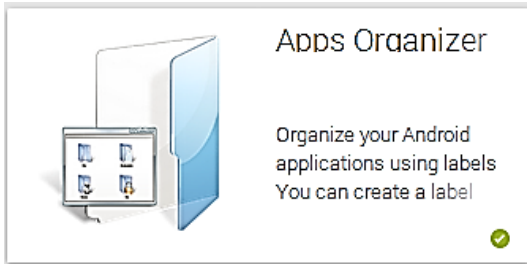
- W. Yang, X. Xiao, B Andow, S. Li, T. Xie, and W. Enck. "**AppContext: Differentiating Malicious and Benign Mobile App Behavior Under Contexts**." In Proceedings of the 37th International Conference on Software Engineering (ICSE 2015), Florence, Italy, May 2015. PhD student Wei Yang presented this in May 2015.
- T. Xie, J. Bishop, N. Tillmann, and J. de Halleux. "**Gamifying Software Security Education and Training via Secure Coding Duels in Code Hunt**". In Proceedings of Symposium and Bootcamp on the Science of Security (HotSoS 2015), Urbana, IL, April 2015.

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



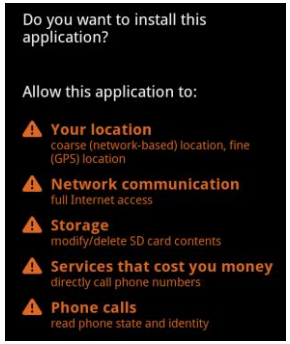
- Reason about user-perceived info, e.g., **WHYPER** [USENIX Security 13]

App Description Sentence



Linkage

Permission

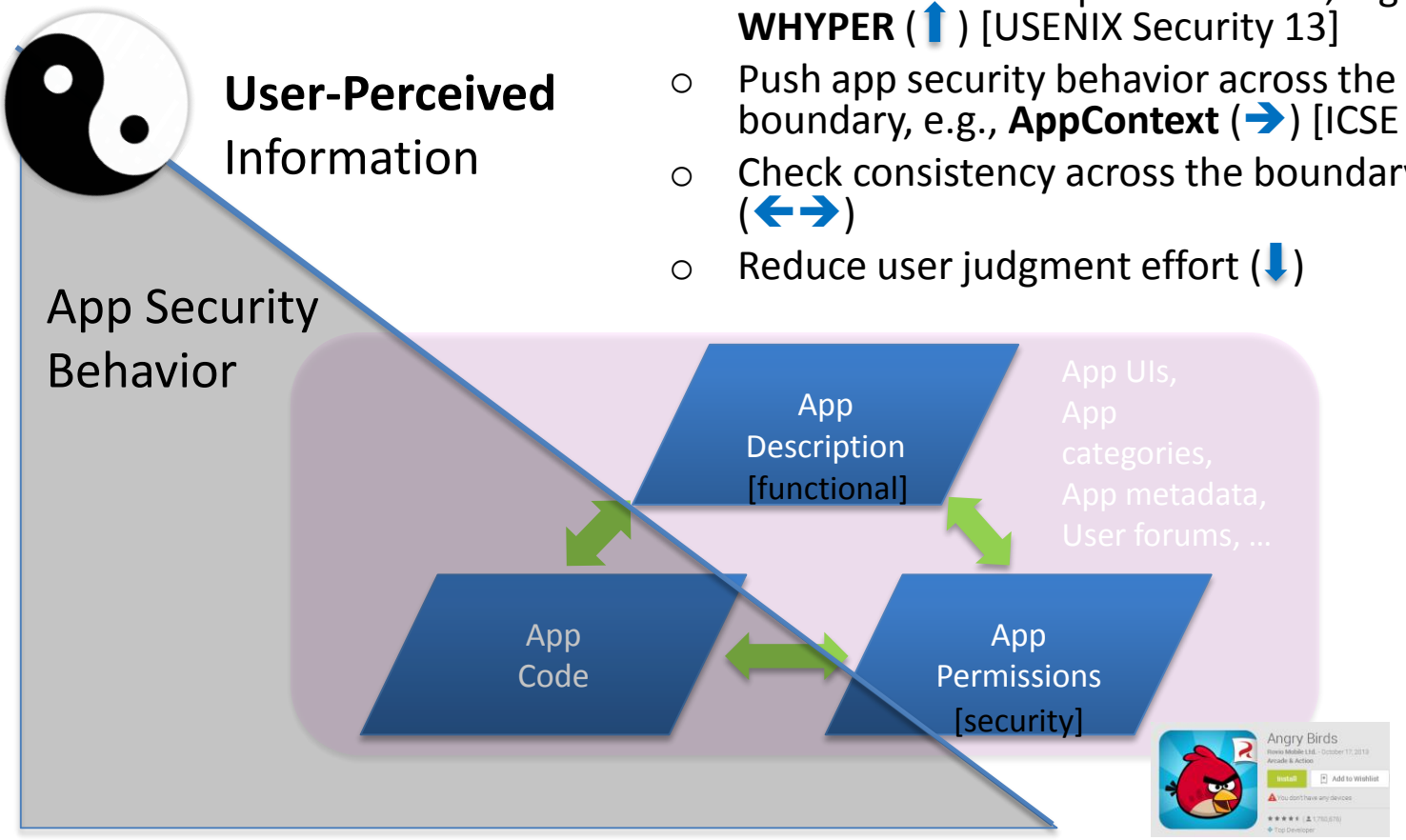


Rahul Pandita, Xusheng Xiao, Wei Yang, William Enck, and Tao Xie. WHYPER: Towards Automating Risk Assessment of Mobile Applications. In Proceedings of the 22nd USENIX Security Symposium (USENIX Security 2013), 2013.

Tao Xie at al:

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

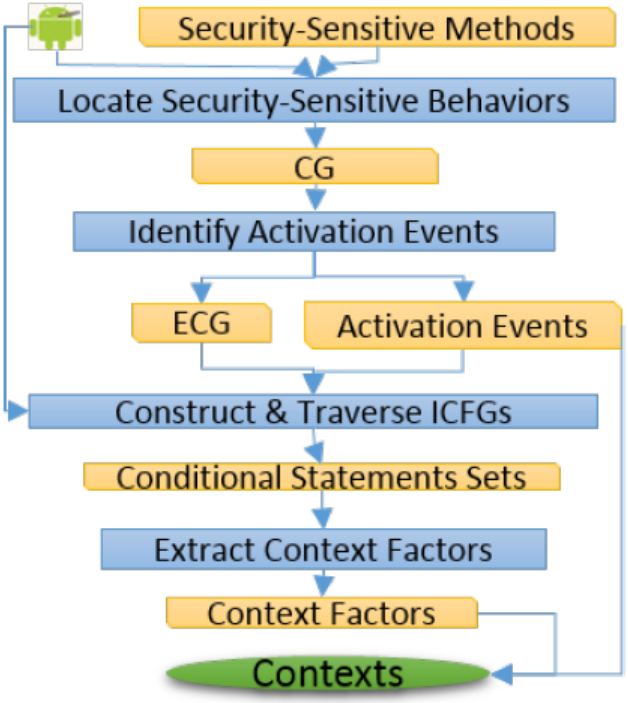
- Reason about user-perceived info, e.g., **WHYPER** (⬆) [USENIX Security 13]
- Push app security behavior across the boundary, e.g., **AppContext** (➔) [ICSE 15]
- Check consistency across the boundary (⬅➔)
- Reduce user judgment effort (⬇)

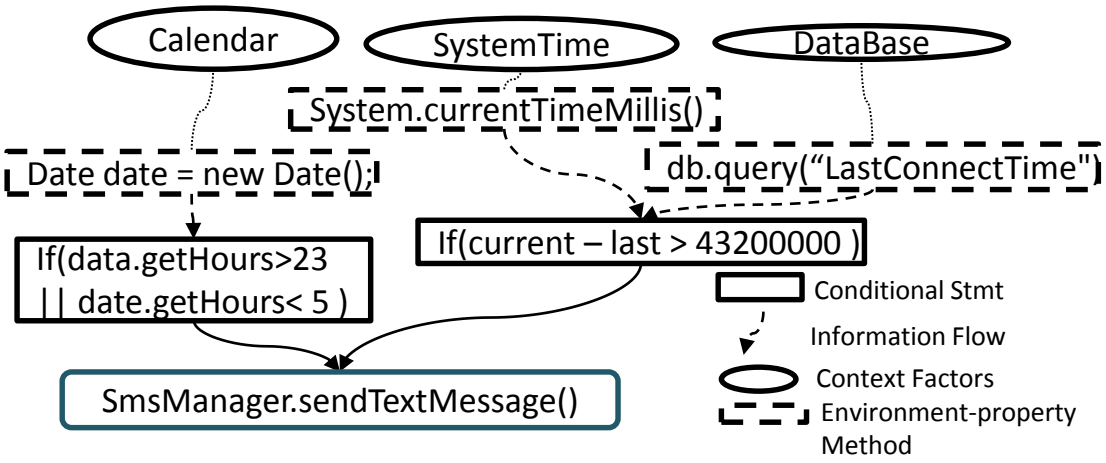


Mobile Malware: Characteristics

- 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

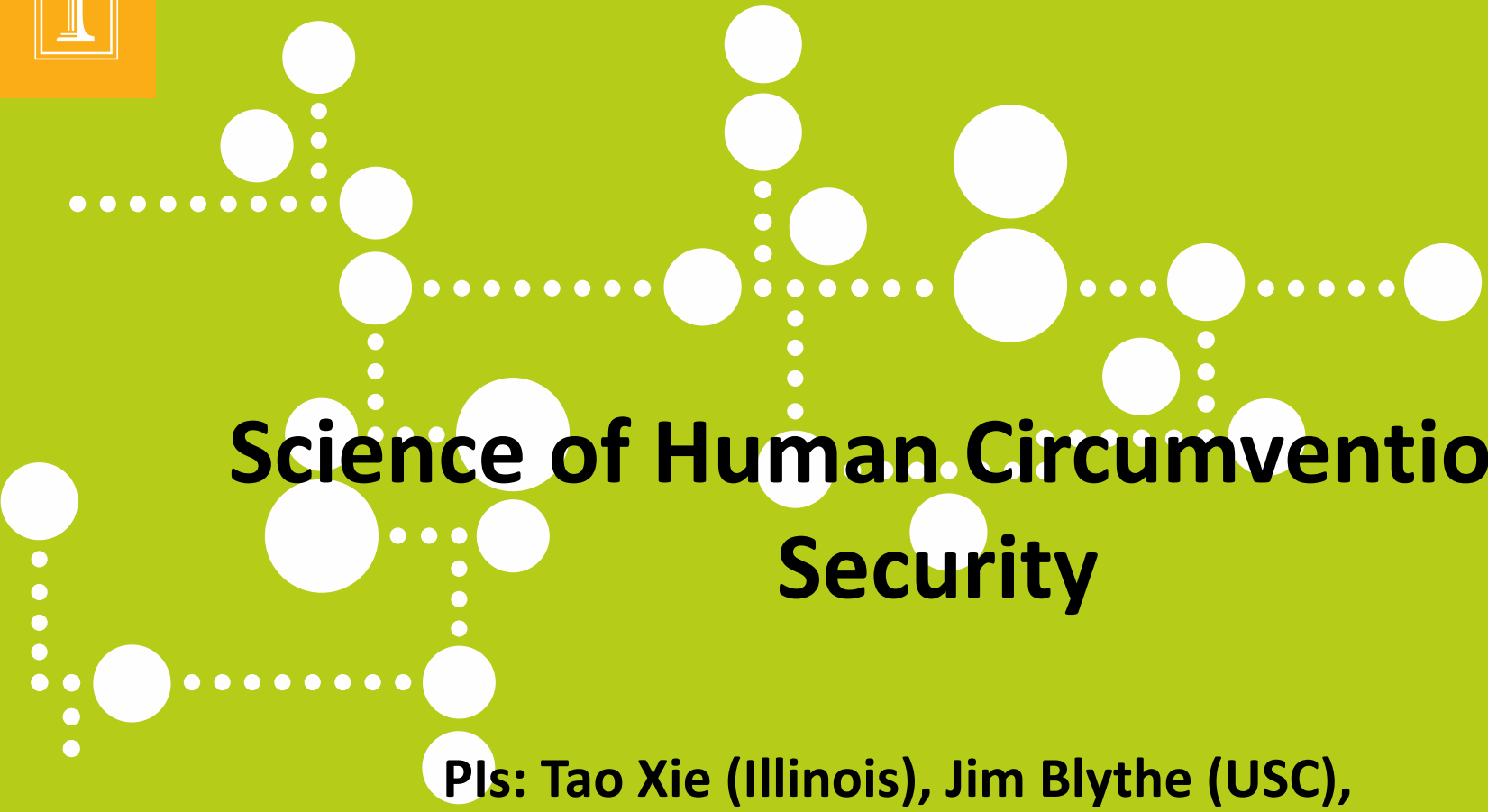
TABLE I
LIST OF FEATURES FOR CLASSIFICATION

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

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.



Science of Human Circumvention of Security

PIs: Tao Xie (Illinois), Jim Blythe (USC),

Ross Koppel (U Penn), Sean Smith (Dartmouth)

rkoppel@sas.upenn.edu

Questions??