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

policy!  

it doesn't work

officer

user

policy!
Manageability – Access Control Example

policy!

officer

it doesn't work

user
Manageability – Access Control Example

policy!

it doesn't work

officer

user

It doesn't work.
Manageability – Mobile App Permission Example

Malicious behavior

Malicious App Developers

I don't understand

Malicious App Developers

I don't understand
Manageability – Mobile App Permission Example

Malicious behavior

Malicious App Developers

I don’t understand

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

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

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

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

App Code

App Description
[functional]

App Permissions
[security]

App UIs, App categories, App metadata, User forums, ...

App Description Sentence

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 (↓)

User-Perceived Information

App Security Behavior

- App Description [functional]
- App Code
- App Permissions [security]
- App UIs, App categories, App metadata, User forums, …
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

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

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

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

<table>
<thead>
<tr>
<th>Features of Behavior Information</th>
<th>Features of Activation Event</th>
<th>List of environmental attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>Security-sensitive method call</td>
<td><img src="" alt="table" /></td>
</tr>
<tr>
<td>SystemUI event</td>
<td>System event</td>
<td>UI</td>
</tr>
<tr>
<td>Features of Context Factors</td>
<td><img src="" alt="features" /></td>
<td></td>
</tr>
</tbody>
</table>

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??