A Cross-Disciplinary Study of User Circumvention of Security

Jim Blythe, PhD
USC ISI
Research Scientist, CS

Ross Koppel, PhD
University of Pennsylvania
Sociology & Senior Fellow LDI

Sean Smith, PhD
Dartmouth College
Professor, CS

Vijay Kothari
Information Sciences Institute
PhD Student, CS

David Harmon
Dartmouth College
Undergraduate, CS

Christopher Novak
Dartmouth College
Undergraduate, CS
Talk Outline

The Problem

How We Approach It

Thrust 1: Fieldwork and Observation

Thrust 2: Analysis

Thrust 3: Towards a Solution

Next Steps
The Problem
The Problem

"good"

officer

user
The Problem

"bad"

officer

user
The Problem

policy!

officer

user
The Problem

policy!

officer

"good"

user
The Problem
The Problem

- policy!
- officer
- user

≠

"good"
The Problem

Good people circumvent security controls to get their jobs done...and to accomplish the mission of their organizations)

“Eppur si muove”….we can’t pretend it doesn’t happen.
How We Approach It

Faculty leads:

- Ethnography and sociology
- Computer security
- Agent-based modeling

Hardworking PhD student

And undergraduate interns
Thrust 1: Sociology, Ethnography, Surveys, Log Analyses

- Observations & shadowing of users in hospitals, offices, banks, Wall St firms, academia, industry.
- Interviews with CSOs and Cybersec luminaries (including leaders at Google, banks, etc)
- Analysis of requests for access, fixes and modifications from IT offices (request logs > 20,000 items)
- Review of password lists
- Analysis of password notebooks/logbooks (thousands sold on Amazon)
- Surveys on cybersec circumvention: general users and cybersec administrators
- Help desk and security logs
- Literature reviews...and our own publications and presentations N >40
- IRB approval for surveys, observations, interviews...and now Mech Turk
- Work with Intel and NSF on IoT cybersecurity
- 20 years of work with medical institutions, medical device makers, medical informatics association.
Thrust 1: Fieldwork & Observation (Simplified Version)

CISO Decisions

User’s understanding

User’s Actions

Aggregate Security
Thrust 1: Fieldwork & Observation (Adding Complexity)

CISOs Decisions (MANY and MANY)

Closer to reality:

User’s understanding

Many and conflicting rules and advice

Users’ actions

Aggregate security across many devices and many networks???
Thrust 1: Fieldwork & Observation

Unuseful Guides to the Perplexed

User now their own CISO(s)
How Common is Circumvention of Password Rules?

From the Pew Survey (2016): Americans Don’t Follow Guidelines:

Sharing passwords  Passwords: Fluffy Fluffy1 Fluffy2 Fluffie Fluffie$ FluFy FluFFies
How Common is Circumvention of Authentication Rules?

How Common is Circumvention of Authentication Rules?

<table>
<thead>
<tr>
<th>Method</th>
<th>Use</th>
<th>Use most often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorize them in their heads</td>
<td>86%</td>
<td>65%</td>
</tr>
<tr>
<td>Write them down on a piece of paper</td>
<td>49%</td>
<td>18%</td>
</tr>
<tr>
<td>Save them in a note on a computer or mobile device</td>
<td>24%</td>
<td>6%</td>
</tr>
<tr>
<td>Save them in their internet browser</td>
<td>18%</td>
<td>2%</td>
</tr>
<tr>
<td>Use a password management program</td>
<td>12%</td>
<td>3%</td>
</tr>
<tr>
<td>Other methods</td>
<td>3%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Note: Results for “use most often” category include those who use only one technique to manage their passwords.
Source: Survey conducted March 30-May 3, 2016. “Americans and Cybersecurity”

PEW RESEARCH CENTER
How Many Worry About Their Online Passwords

Pew Survey:  **Fully 69% of online adults say they do not worry about how secure their online passwords are** (Several months ago.... Pre DNC and last week’s wikileaks-CIA hack)

Nobody Cares
From the Interviews and Observations

The Password for Fire Suppression System is?
From the Interviews and Observations
From the Interviews and Observations
From the Interviews and Observations
From the Interviews and Observations
Our Pilot Surveys

Two Parallel Surveys: CSOs and Regular Users:

Who sets policies? (Anyone know the policies?)

Do they make sense...and to whom?

How often circumvented? (What’s the justifications for that?)
How Frustrated Are You by Access Policies?

<table>
<thead>
<tr>
<th></th>
<th>1 (Not Frustrated)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (Very Frustrated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General users</td>
<td>23%</td>
<td>39%</td>
<td>15%</td>
<td>23%</td>
<td>0</td>
</tr>
<tr>
<td>Cybersecurity pros.</td>
<td>33%</td>
<td>27%</td>
<td>33%</td>
<td>7%</td>
<td>0</td>
</tr>
</tbody>
</table>

Most are frustrated…
What They Say:

Cybersecurity Pros

“Waiting so long when turning on/off the computer as it decrypts/encrypts information.”

General Users

“The work is delayed.”

“Frustration. [Coworkers] not able to do their job. Give up or don't care anymore.”
Are Access Rules Sensible: Pros vs. Users

<table>
<thead>
<tr>
<th></th>
<th>Generally Sensible</th>
<th>Sometimes Sensible</th>
<th>Not Sensible</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gen</td>
<td>Pros</td>
<td>Gen</td>
<td>Pros</td>
</tr>
<tr>
<td>Log on rules</td>
<td>46%</td>
<td>87%</td>
<td>46%</td>
<td>0%</td>
</tr>
<tr>
<td>Password rules for different passwords for each app</td>
<td>30</td>
<td>7</td>
<td>20</td>
<td>53</td>
</tr>
<tr>
<td>Password complexity</td>
<td>23</td>
<td>40</td>
<td>38</td>
<td>20</td>
</tr>
<tr>
<td>Password change frequency</td>
<td>25</td>
<td>13</td>
<td>58</td>
<td>40</td>
</tr>
<tr>
<td>Management’s rules on granting access</td>
<td>8</td>
<td>31</td>
<td>69</td>
<td>23</td>
</tr>
<tr>
<td>Inactivity timeouts</td>
<td>31</td>
<td>53</td>
<td>54</td>
<td>33</td>
</tr>
<tr>
<td>Different rules for different systems</td>
<td>17</td>
<td>21</td>
<td>42</td>
<td>43</td>
</tr>
<tr>
<td>Rules by how/why access is provided</td>
<td>38</td>
<td>53</td>
<td>46</td>
<td>20</td>
</tr>
</tbody>
</table>

Pros a bit more accepting of rules, but most doubt rules’ thoughtfulness.
What They Say:

“Everyone writes down passwords”

Everyone “using alternate spellings to work around the dictionary rule;” eg, ‘boyz’ for ‘boys.’
## When is Circumvention Justified?

<table>
<thead>
<tr>
<th>Reason</th>
<th>General Users</th>
<th>Cybersecurity Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical task, e.g., saving a life, keeping the grid up</td>
<td>83%</td>
<td>79%</td>
</tr>
<tr>
<td>When the rules are so foolish that nothing else makes sense</td>
<td>42%</td>
<td>57%</td>
</tr>
<tr>
<td>Access associated with role(s) make no sense, e.g., members of the same team can’t see all of the information because only some have official access</td>
<td>17%</td>
<td>36%</td>
</tr>
<tr>
<td>When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don’t</td>
<td>28%</td>
<td>9%</td>
</tr>
<tr>
<td>When everyone else is circumventing a specific rule</td>
<td>58%</td>
<td>43%</td>
</tr>
<tr>
<td>When people were officially taught to use a workaround</td>
<td>58%</td>
<td>71%</td>
</tr>
</tbody>
</table>

Answer: When I want to (and we all do it). Pros often more accepting of “cheating”
Security Pros vs. General Users:

General users: cybersec pros not concerned about our work needs

Both general users and cybersec pros tend to see externally imposed rules as unreasonable

Many general users often see cybersec rules as excuse for laziness (as in why we didn’t fix something)

Cybersec pros feel often unloved. And they’re right!
Cybersecurity as conceptualized vs.

As designed vs

As conveyed: with conflicts, contradictions, incomprenesion; across many systems

As understood...and

As acted upon: by individuals, enterprises...

And in relation to the many (interacting) networks and to the IoT
Thrust 2: Analysis

- An organizing model for circumvention: semiotic triads

Smith and Koppel 2014
Thrust 2: Analysis

• An organizing model for circumvention: semiotic triads
• In language: morphisms

• Regular semiotics: morphisms.

• Mappings preserve structure
Thrust 2: Analysis

- In security usability: mismorphism

- Circumvention semiotics: mismorphisms.
- Mappings fail to preserve structure

This project!
Causing Circumvention
Causing Circumvention

\[ \phi_A \text{ should hold} \]

\[ \text{Admin A2's model} \]

\[ \text{IT config at S2} \rightarrow \text{Reality at S2} \]

\[ \text{User's model} \]

\[ \phi_U \text{ should hold} \]

\[ \phi_A \text{ does not hold} \]

\[ \phi_U \text{ does not hold} \]
Trouble: Loss of Monotonicity

\[ S(x) \leq S(x + \Delta) \]
Trouble: Loss of Monotonicity

security

"uncanny valley"

\[ S(x) > S(x + \Delta) \]
Trouble: Loss of Monotonicity

Uncanny *descent*
- timeouts
- password practices
- computerizing medical workflow

Uncanny *ascent*
- "qwertypoqwertyp"  
- executive passwords

Uncanny *nop*
- public/internal wifi
- check diff password via hash
- deleting links, not files 
- education not help
Trouble: Loss of Continuity

\[ |S(x + \delta) - S(x)| < \varepsilon \]

\[ |S(x + \delta) - S(x)| >> \varepsilon \]

+ \delta

Admin A2's model

IT config at S2

Reality at S2
Trouble: Loss of Continuity
Trouble: Loss of Continuity
Trouble: Loss of Continuity
Trouble: Loss of Continuity

- rectal polyps
- accidental tornado siren at 3am
- dead patient---lack of follow-up
- dead patient---extra zero?
Trouble: Action at a Distance
Trouble: Action at a Distance
Trouble: Action at a Distance
Trouble: Action at a Distance
Mismatches between reality and mental models lead to circumvention.

Circumvention leads to significant mismatches between the admin’s mental models and resulting reality.

- What do we do?
- How can we move from fantasy-based cybersecurity to evidence-based cybersecurity?
Once we know the likely behavior of individuals based on survey data and behavioral experimentation,

Agent-based simulation can help explore the consequences of that behavior in organizations.

Principled simulation can help explore policies in silico before paying costs for poor fits in the real world.

Simulations that fail to model known group behavior can point to where more field work is needed.
DASH Cognitive Agents

- Dual process
- Reactive planning
- Mental models
- Spreading activation
Designed for Speed, Reuse and Customization

Reimplemented in object-oriented python.

Have run millions of agents in DETER simulation.
E.g. DASH Agent Model (DASHWords)

Levenshtein measure of cognitive burden

Circumvention models from survey

Direct + reuse measure of security

[Kothari et al. 15]
Demonstrates ‘Uncanny Descent’

As constraints increase, end-to-end security may decrease

[Kothari et al. 15, 16]
Current & Future work: Evidence-based Cybersecurity

- How well do simulation findings reflect reality?
- Link parameters to experimental results and test their impact
Components Explicitly Linked to Supporting Experiments

Component layer
- System 1
- System 2
- Communication
- Human performance

Base DASH agent
- DASH Agent

Reusable domain components
- Password Agent
- Browser Agent
- Attacker Agent
- User Agent
- Insider Agent
- Workflow Agent
- Defender Agent

Agents for experimentation
- MyUser Agent
- Phishable Agent
- ASU Attacker
- Tambe Insider
- Ward Nurse

Caputo et al. 14
FARM Helps User Select Appropriate Settings

- Single most likely scenario:
  - 15 phish emails sent in one day, several hits

- Samples the space of possible scenarios:
  - \(0.5 \leq p(\text{id phish}) \leq 0.8,\)
  - \(0.1 \leq p(\text{open attachment}) \leq 0.\)
  - \(\ldots,\)
  - \(\rightarrow\) number of phish emails from 10--30.
FARM Helps Analyze Results

Reject null hypothesis w prob 0.95, (teaming is better) when there are 15 phishing targets.

Experimenter knows more phish ⇒ teaming less important

FARM can

• estimate probability ≤ 25 phish by sampling parameter space.
• find most likely scenario given > 20 phish by subsampling
Next Steps

Fieldwork, Observations
Surveys, Logs

Empirical Data
Models of behavior and action

Evidence-based cybersecurity and policy

Simulation / DASH
Acquiring More Data

Sources of data:

- Mechanical Turk password experiment
  - Infrastructure in place---and IRB approval just arrived!
- Available data: help-desk logs, server logs, etc.
- Follow-up surveys and experiments to:
  - compare user and expert security behaviors and perceptions
  - determine how users interpret security advice
Revising and Extending Simulations

- Improve simulations based on new data
- Further explore interconnectedness of prescribed behaviors, user decision-making processes, and actual behaviors
- ...and impact on aggregate security
  - What do the curves really look like?
  - Can we help with evidence-based cybersecurity policy decisions?
- Extend from enterprise scenarios to home IoT scenarios
Automatic Reasoning About the Link Between Data and Simulation

• FARM will record the link from data to simulation parameters to:
  • find most likely settings for behavior under test
  • explore dependence of recommendations on data
  • sometimes suggests refined experiments/analysis
Publications

Conclusion (Our Project in a Nutshell)

● Problem
  ○ *Security engineering doesn't work if predicated on the fantasy that good users fully comply!*

● Key Questions:
  ○ Why do users circumvent?
  ○ How does circumvention affect aggregate security?
  ○ How do we improve aggregate security?

● Project Goal:
  ○ To *propose* security solutions and develop metrics to make meaningful, quantifiable *comparisons*, *decisions*, and other *evaluations* of proposed solutions in light of what users do.

Thank you! Questions?