Beyond Pleading With or Restricting Users to Achieve Cyber Security Goals: Approaches to Understanding and Responding to Circumvention

Ross Koppel[a] Vijay Kothari[b] Sean W Smith[b] Jim Blythe[c]
[a] *University of Pennsylvania* [b] *Dartmouth College* [c] *University of Southern California*

Cyber security practitioners and theorists live with the tension between: a) restricting users' unwanted actions by structuring IT systems to enforce safe use and authentication, and b) pleading with users to follow safe security protocols. While the reality of course encompasses both approaches, contrasting the two ends of this spectrum, enables us to explore the strengths, vulnerabilities, and implications of these choices.

We also acknowledge that it's not a fair fight: Humans are ferociously flexible, whereas computers tend to be rather rigid. Humans therefore usually win, but at the cost of security for themselves, their organizations, and everyone's data.

People interact with security mechanisms, learn of new and existing security policies (real, misconstrued, and otherwise), observe other humans' security behaviors, experience new security requirements, hear security advice (both wise and otherwise), and are sometimes or frequently obliged to accomplish their work in the face of security restrictions that appear (and may be) deeply hostile to their tasks and to their organization's mission. Many users view security rules as illogical, as poorly designed, and/or as excuses for administrative laziness or non-responsiveness [1,2]. All of these factors affect users' cyber security beliefs and behaviors as they deal with what they often perceive as incomprehensible and shifting rules. This dynamic interaction with software and hardware makes designing security solutions especially difficult. And therein lies the proposed grand challenge and hard problem: how do we design security solutions when we must simultaneously consider users, users' changing understandings of security, and shifting contexts? Also, we must focus on many organizations and rules simultaneously; users interact with webs of institutions, differing security rules, and different IT systems.

The emergent realities of security solutions are thus always in flux: good security requires that we understand how security needs will change, how those changes affect behaviors and beliefs, and what influences will occasion those changes. We therefore must go beyond improving or expanding our algorithms and rules to incorporate observations, systematic analyses of log-ons, interviews, and even experimentation with differing rules. The work of sociologists and cognitive psychologists can help us understand how users are influenced, how those influences affect their behaviors, and how users make security-related decisions. Armed with that knowledge, we can better prepare emergent security solutions.

There are three interrelated issues that flow from these concerns:

1. Explaining Security Needs and Rules: We need to do a better job of explaining security in ways that encourage users to understand and comply. Here, we reference the W. I. Thomas dictum: "what men believe is true is true in its social consequences." If users view cyber security mainly as an encumbrance rather than as thoughtful and needed protection, then we must improve our efforts (and the technology). Too often, circumvention of security rules is pandemic, and often regarded as essential, even laudatory [1,2]. Communication with users about security must be conceptualized as a dialog, not a command. Enforcing security policies, giving users security advice, and reprimanding users if (when) they circumvent must be tempered and complemented by interaction, listening and observations of actual practice.

2. Responding to Circumvention: How should security practitioners respond to users' circumvention of security? One might argue that security policies should be more heavily enforced to ensure

compliance. Another might argue that security policies should be less strictly enforced, instead relying on security recommendations as the primary means to ensure cooperation; accepting some tradeoffs with full compliance but not alienating the users. Others might even argue that security practitioners should endorse select, benign circumventions to mitigate the risks of users engaging in more harmful circumventions. That is, we might settle: if the user engages in two bad behaviors with different security repercussions it may make sense to endorse the less bad behavior.

3. Circumvention Motivations: Equally important, we must understand users' motivations for circumvention. Few seek to undermine security just for the heck of it. Most just want to do their jobs with minimal hassle. For most users, complying with security policies and mechanisms is a secondary task that too often interferes with or prevents completing their primary tasks. So, users circumvent. The security research literature has shown multiple instances where users routinely circumvent security policies and mechanisms [3]. Users are taught circumvention as part of their job orientations, circumvention may be seen as a sign of innovation and creativity, and circumvention is often rewarded by managers as it may enhance productivity. For some, the struggle to comply manifests as an "us vs. them" confrontation with what they view as insensitive obstructionism by clueless management. Therefore, security researchers, security practitioners, and risk managers must understand not only the risks posed by security circumvention, but also the motivations and rewards for that circumvention. Sociologists and cognitive psychologists can help here, as can observations, data logs, and other data sources. Policy designers and security practitioners in collaboration with other researchers are essential to interrupting dysfunctional interactions that endanger users, the organizations, and its data.

Limitations: We have addressed neither the ethical nor legal concerns that inevitably arise when confronting these challenges. Nor have we confronted the necessity of swift responsiveness to security issues, or the needed managerial structures—with incentive and disincentives for compliance.

Conclusion: We posit two approaches for maximizing compliance with security needs—technological constraints and social (or normative) pressure on users. While acknowledging that both approaches are always employed we expand this dichotomy to include: 1) concerns for understanding users' perceptions of the rules and security needs; 2) how to best respond to users' circumventions; and 3) the need to understand users' motivations for circumvention. We also stress the value of social scientists to better appreciate users' motivations and the most efficacious ways of communicating with them. We argue that successful security policy must encompass user's beliefs and motivations, emerging contextual and experiential changes, and rapid responses to technological and social shifts.

References:

1. R. Koppel, J. Blythe, V. Kothari, S.W. Smith. "Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Vs. Regular Users." *SOUPS 2016 Security Fatigue Workshop.* June 2016.
2. D. Kerin. "New Survey: Businesses Should Begin Preparing for the Death of the Password." GIGYA, May 24, 2016. Accessed September 30, 2016. http://www.gigya.com/blog/new-survey-businesses-begin-preparing-death-password/.
3. Beris O, Beautement A, Sasse MA "Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behavior." ACM International Conference Proceeding Series 08-11-September-2015