Editors: Patrick McDaniel, mcdaniel@cse.psu.edu | Sean W. Smith, sws@cs.dartmouth.edu

Circumvention of Security:
Good Users Do Bad Things

Jim Blythe | University of Southern California
Ross Koppel | University of Pennsylvania
Sean W. Smith | Dartmouth College

Effective security controls are critical for trustworthy operation of large computer systems, which are central to large enterprises and critical infrastructure. This is especially the case if they involve physical distribution of utilities or other essential services. Without tools such as access controls, firewalls, and the like, it's impossible to reason about, define, detect, and prevent adversarial action that violates systems' key security goals.

However, these real-world systems involve large populations of humans who use, configure, and maintain them. Looking at humans and security together is an emerging field.[1,2] Fieldwork and much research consistently find that human users continually circumvent and misuse these security controls.[3–9] (Note that our bibliography offers only some example citations, not a complete list.) Users don't intend their circumventions as attacks, but rather as a way to achieve their job activities and organizational goals. Indeed, workers often learn many forms of security access circumvention as part of their job orientation. Many of these workarounds are so common and viewed as so necessary that they aren't perceived as violations of the norms, let alone security threats.

Many computer security researchers overlook the reality of this circumvention. But such circumvention is ongoing, ubiquitous, often required, and seldom rebuked unless it becomes obvious to leaders or generates a known and exploited vulnerability. Furthermore, because system security depends on correct use and operation of the security tools being circumvented, effective security requires a way to address such circumventions scientifically. Failure to understand and analyze these circumventions means we build and deploy security that doesn't work even though we pretend that it does. This self-delusion deteriorates morale, attenuates workers' beliefs in the organizational leadership's understanding of the mission and tasks, reduces attention to real threats of inappropriate access, and encourages further circumventions.

Textbooks and research literature tend to present a rosy view of the technology that magically solves problems. Academic security experts suggest that all these problems are solved. However, in our many interviews and field examinations, we find that information security appears to be in its own echo chamber.

To bridge the gap between what we read about information security and what we repeatedly find in on-the-floor examination, we talked to users in the trenches trying to get their jobs done despite security technology as well as the enterprise information security officers and consultants trying to make the security technology fit the real world.

View from the Trenches

We interviewed 19 cybersecurity experts, CIOs, chief medical information officers, IT workers, everyday users, and managers to obtain their perceptions of computer security rules, logic, protocols, norms, and actual practice. The interviews were usually face to face, but a few were via the phone. Several involved follow-up calls and emails. A semistructured interview schedule is available from the authors. In addition, each of the authors has been investigating cybersecurity and workarounds for many years. We augment our interviews with the findings from those previous investigations.

Passwords

Let's consider passwords. Ensuring only the right users access various

 Copublished by the IEEE Computer and Reliability Societies

electronic services in the enterprise is important. The standard, textbook first step is to have the system authenticate the user, and the de facto standard is via a username and password. In theory, passwords should be unique to each user, never shared or written down, complex enough to resist automated cracking, and changed regularly; in theory, each user should have few enough passwords that he or she can actually remember them.

However, in practice, things differ radically. In industry after industry, we find users write down passwords. We see sticky notes on monitors, under keyboards, in desk drawers, and occasionally forming sticky stalagmites on equipment. Password tables live in notebooks and spreadsheets (tempting information security officers to beg users to at least store them more securely, even though they shouldn't be storing them at all).

Users share passwords with other users to get their jobs done and make it easier for electronic workflow to match their real-world workflow. Special username-password pairs guarding access to extremely useful services are shared throughout large groups, sometimes because commercial licensing charges the enterprise per password. Critical equipment often ships with default passwords—necessary for emergency maintenance—that are never altered over many years. Clever users even change passwords in ways that work around security checks, thus enabling continued use of the same, easy-to-remember password.

One technique we studied was especially ingenious. All employees in an information technology organization were forced to change their passwords every 90 days. On the 90th day, users would change their passwords in accordance with the rules, including two capital letters, two lowercase letters, two numbers, two special characters, and no dictionary words or previously used passwords. However, on day 91, users would call in and say they forgot their passwords, and the security officer would reset the passwords to something users would be obliged to alter in a few hours. However, the lost-password reset canceled the trace of the previous passwords, so employees could simply reuse their old password.

Timeouts

After authentication comes what practitioners call the *deauthentication problem*: how a system should terminate a user's session. We've seen users putting Styrofoam cups over proximity detectors to trick the system into believing they'd never left. More recently, we've heard senior staffers chortle about how the most junior person on a medical team is responsible for regularly pressing the space bar on everyone's keyboard to prevent the computer from logging off the current user.

Permission Management

For correct matching of users to IT sessions to be truly meaningful, the system's policy of who can do what when must be meaningful, which itself is a can of worms. Defining who is in what role, and thus has access, is a major problem. Workers often shift roles and have joint or multiple responsibilities. Frequently, their work requires full access for one task but only limited access for others. Writing permissions for such complexities is daunting (for example, see "What's Wrong with Access Control in the Real World?"[10]).

Going outside the System—and the Building

Users also react to overly constraining IT security controls by bypassing the enterprise IT entirely. At a government lab, developers writing a filter to enforce enterprise policy by blocking access to pornographic sites needed to go outside the enterprise to test the filter because testing it inside violated policy.

Defense workers lament that a one-size-fits-all approach to policy—applying the same Internet whitelist to a low-level clerk and an analyst—prevents analysts from doing their job while on enterprise machines. Medical workers raise similar objections—Web blacklists can prevent providers from gathering information on the illegal drug use reported by patients. Users in multiple domains report going across the street to a coffee shop (or using Secure Shell tunnels to an external nonenterprise site) to gain access to the Internet so they can perform their jobs. Information security officers report that frustrated users often set up WLANs as a way to work around enterprise firewalls.

Users in a wide variety of domains forward their work material to personal email and third-party repositories. One security officer reported that when telecommuters came into the office, they were surprised that they couldn't access Dropbox, and reported it as a bug.

Going around the Applications

We've also seen many cases of users staying within the enterprise IT system but working around applications and application constraints. A medical clinician was unhappy with the official medical data processing application, so he wrote his own to grab what he really wanted from the raw network packets. Traders will code whatever they feel they need (in VBA spreadsheets or online Web tools) to execute trades when the time is right. In academia, senior users insist on not updating security software because they can't see how the compromise harms them. In the mortgage industry, some users actively disconnect their machines during intranet-driven patching. To circumvent a hospital's rules on

exfiltration of medical images, a doctor takes a screenshot and drops the image into email; in a different industry, to circumvent filters on exfiltration on text, users scan the document into an image and then embed the image in PDF.

Undermining Security Engineering

Because computers and their security controls are technology, the security community tends to think solely in the technological domain. We conceive of correct system behavior under various user actions and construct control systems that let officers specify this behavior. We then reason about what actually happens—the exposure a certain policy permits, different policy choices' relative costs and risks, the best way to modify a given policy to accommodate new enterprise goals or scenarios—as if this technology matches reality.

If a hospital information security officer sets a deauthentication timeout to five minutes, he or she might anticipate the net amount of time that machines may be logged in but unattended to be five minutes times the number of sessions. If a hedge fund client asks about the number of employees who can see his or her data, an investment bank information security officer can simply check the policy and add up the number of subjects that can read those objects. An enterprise information security officer worried about man-in-the-middle attacks on Web sessions can increase assurance that users are protected by insisting that they use fully patched machines and that they check that their browsers report properly blessed SSL sessions with the enterprise's servers.

But what really happens in the trenches doesn't match the technology's underlying assumptions or even purposes. Circumvention renders all this reasoning, designing, and tuning perhaps as effective and relevant as counting angels dancing on a pinhead. If a doctor puts a Styrofoam cup over a detector, the net exposure time of unattended terminals becomes infinite. If standard unofficial practice has all analysts sharing five central passwords, then the total number of employees with access to sensitive data is "all of them." If my superior insists on not using a standard trust root for our enterprise's SSL servers, then every one of my users' work sessions is at risk—as is every one of their personal sessions—because the users were trained to ignore warnings about invalid SSL certificates.

What really happens in the trenches doesn't match the technology's underlying assumptions or even purposes.

Characterizing Workarounds

If we're going to make security work, we need to do better than this.

To start, it might be useful to specify the problem.

We might define a workaround informally as a practice in which users either fail to follow an intended protocol or workflow process, or actively take steps to defeat it. (It's tempting to offer a different, perspective-based definition when the actual use of an information system differs from the information security officer's mental model.) We limit our focus to "white hat" participants: those seeking to improve their efficiency, their group's efficiency, or indeed the mission of their larger organization, rather than external hackers or active saboteurs.

Many access policies aren't communicated clearly enough. We studied a hospital that instituted a new set of permission groups intended to separate access permissions for different roles. Unfortunately, neither the roles nor the groups were clearly defined. In these cases, the designation of a workaround can't be clearer than the official policy's designation and linked groupings.

In some cases, we've observed root causes of workarounds by looking at the complete cycle of IT specification, acquisition, and maintenance. On one hand, we've heard success stories in which information security officers convinced users that compliance with abstract security rules also directly helped further goals they cared about. One officer stopped executives from sharing passwords with their administrative assistants when he pointed out that the passwords also gave access to the executive's private financial information. Another officer stopped users from hiding passwords under keyboards in the trading room when he pointed out that all trades carried out in a user's name would be credited (or, more significantly, debited) to that user's "profit and loss" statement. A third officer increased user compliance with communication rules when he made users realize that their communication logs would make it easier for them to defend themselves in legal audits.

On the other hand, things don't always go so well, as we've indicated.

We might ask how much it ultimately matters whether users know they're engaging in a workaround or how much they know about the workaround's potential bad consequences. Regarding the first part of the question, when access workarounds are taught as part of workers' orientation, it's unlikely many workers know they're engaging in circumventions. In settings in which access workarounds are discussed among groups in the lunchroom,

violations appear to be trivial and arbitrary. Rather than being seen as protective, the rules are seen as annoying, like anti-jaywalking laws.

Regarding the "potential bad consequences," the answer depends in part on how we define this. If we mean, "Does it deteriorate respect for authority figures (because they create annoying and silly rules)?," then yes, but it's probably not a major issue. If you're asking about workers' understanding of cyber risks and vulnerabilities because of their actions, then the implications are far more dire. Organizational leaders have a right to expect their staff to understand that their actions can endanger basic functions and missions. However, organizational leaders have an obligation to ensure the rules make sense, don't prohibit work, and are sensible enough that well-intended workers can follow them. No one should be expected to remember six secure passwords that change every 30 days and aren't standard words or terms. These will be written down or recorded in a spreadsheet marked "passwords," just as we found in our interviews.

So, are workarounds always "bad"? That depends. Workarounds that don't endanger security and that allow more efficient workflow processes should be incorporated into the organization's policies, essentially moving the policy "deviations" to actual policy. But regardless of these sociological and workflow issues, we still have the basic problem that circumvention breaks security engineering.

As two of us observed in a recent analysis,[11]

> Effective cyber security requires that people with authority to effect changes actively seek to discover and remediate the problems and challenges that exist in the workplace but are often unknown to leaders. This requires work by local IT teams, requests to vendors, analyses of linkages with other IT systems, ongoing observations of work, focus groups, interviews, et cetera—or, most probably, a combination of these methods. Remediation will require working with all parties, and, perhaps more important, empowering workers and others who observe problems to request changes and improvements.

According to folklore, after Galileo denied under duress that the Earth rotated around the sun; he then admitted, "and yet it moves." We feel similarly about cybersecurity and circumvention: it's ubiquitous, and we should stop pretending it's not.

We welcome your input. ■

Acknowledgments

This material is based in part upon work supported by the Army Research Office under Award No. W911NF-13-1-0086.

References

1. *Security and Usability*, L.F. Cranor and S. Garfinkel, eds., O'Reilly, 2005.
2. C. Sinsky et al., *Comparative User Experiences of Health IT Products: How User Experiences Would Be Reported and Used*, Inst. Medicine of the Nat'l Academies, 2012.
3. A. Beautement, M.A. Sasse, and M. Wonham, "The Compliance Budget: Managing Security Behaviour in Organisations," *Proc. 2008 New Security Paradigms Workshop*, ACM, 2008, pp. 47–58.
4. E. Felten, "Too Stupid to Look the Other Way," Freedom to Tinker, 29 Oct. 2002; https://freedom-to-tinker.com/blog/felten/too-stupid-look-other-way.
5. M. Harrison, R. Koppel, and S. Bar-Lev, "Unintended Consequences of Information Technologies in Health Care—An Interactive Sociotechnical Analysis," *J. Am Medical Informatics Assoc.*, vol. 14, no. 5, 2007, pp. 542–549.
6. C. Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proc. New Security Paradigms Workshop*, ACM, 2009, pp. 133–144.
7. P. Inglesant and M.A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," *Proc. SIGCHI Conf. Human Factors in Computing Systems*, ACM, 2010, pp. 383–392.
8. B.J. Jansen, A. Spink, and T. Saracevic, "Real Life, Real Users, and Real Needs: A Study and Analysis of User Queries on the Web," *Information Processing & Management*, vol. 36, no. 2, 2000, pp. 207–227.
9. R. Koppel et al., "Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety," *J. Am Medical Informatics Assoc.*, vol. 15, no. 4, 2008, pp. 408–423.
10. S. Sinclair and S.W. Smith, "What's Wrong with Access Control in the Real World," *IEEE Security & Privacy*, vol. 8, no. 4, 2010, pp. 74–77.
11. S.W. Smith and R. Koppel, "Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ," *J. Am. Medical Informatics Assoc.*, 2013; doi:10.1136/amiajnl-2012-001419.

Jim Blythe is a research scientist at the University of Southern California Information Sciences Institute. Contact him at blythe@isi.edu.

Ross Koppel is a professor of sociology at the University of Pennsylvania, Philadelphia. Contact him at rkoppel@sas.upenn.edu.

Sean W. Smith is a professor of computer science at Dartmouth College. Contact him at sws@cs.dartmouth.edu.