Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?

Ross Koppel[a, 1], Sean Smith[b], Jim Blythe[c], and Vijay Kothari[b]
[a] *University of Pennsylvania*
[b] *Dartmouth College*
[c] *University of Southern California*

Abstract. Workarounds to computer access in healthcare are sufficiently common that they often go unnoticed. Clinicians focus on patient care, not cybersecurity. We argue and demonstrate that understanding workarounds to healthcare workers' computer access requires not only analyses of computer rules, but also interviews and observations with clinicians. In addition, we illustrate the value of shadowing clinicians and conducing focus groups to understand their motivations and tradeoffs for circumvention. Ethnographic investigation of the medical workplace emerges as a critical method of research because in the inevitable conflict between even well-intended people versus the machines, it's the people who are the more creative, flexible, and motivated. We conducted interviews and observations with hundreds of medical workers and with 19 cybersecurity experts, CIOs, CMIOs, CTO, and IT workers to obtain their perceptions of computer security. We also shadowed clinicians as they worked. We present dozens of ways workers ingeniously circumvent security rules. The clinicians we studied were not "black hat" hackers, but just professionals seeking to accomplish their work despite the security technologies and regulations.

Keywords. Workarounds, cyber security, computer access, workflow

1. Introduction

A significant gap exists between cybersecurity as taught by textbooks and experts, and cybersecurity as practiced by actual end users [1-9]. In previous work, we looked at the general problem of how users work around security controls in general [10] and in healthcare [11]. Here, we focus on cyber security evasions healthcare and how ethnographic methods help reveal them.

Cyber security efforts in healthcare settings increasingly confront workarounds and evasions by clinicians and employees who are just trying to do their work in the face of often onerous and irrational computer security rules. These are not terrorists or black hat hackers, but rather clinicians trying to use the computer system for conventional healthcare activities. These "evaders" acknowledge that effective security controls are, at some level, important—especially the case of an essential service, such as healthcare. As we observed, earlier, without such tools, the enterprise cannot protect

[1] Corresponding Author

against adversarial cyber action. Unfortunately, all too often, with these tools, clinicians cannot do their job—and the medical mission trumps the security mission.

The problem is the workers humans who build, use, and maintain the systems—often Chief Information or Technology Officers (CIOs/CTOs), Chief Medical Informatics Officers (CMIOs), sometimes cybersecurity experts, and often just IT personnel—did not sufficiently consider the actual clinical workflow. For example, the bolus of passwords, each with specific requirements and time limits, are seen as an annoyance, not as a patient safety effort. Equally important, circumvention of cybersecurity is seldom examined by those concerned with workflow, HIT usability, barriers to teamwork, thought-flow, or user frustration. Cybersecurity and permission management problems are hidden from management, and fall in the purview of computer scientists, engineers, and IT personnel.

We find, in fact, that workarounds to cyber security are the norm, rather than the exception. They not only go unpunished, they go unnoticed in most settings—and often are taught as correct practice. In rare exceptions, when the workarounds become obvious to leaders—such as a security breach involving a patient's record—there may be repercussions. These common forms of ignorance, or willful blindness, or incomprehension allow organizations to continue to deploy security that doesn't work.

2. Methodology

We interviewed medical personnel in their workplace settings--nurses, doctors, chief medical officers, chief medical information officers, cybersecurity experts, CIOs, IT workers, everyday users, and managers--to obtain their perceptions of computer security rules. We collected reports from medical discussion lists and other literature. In addition, we shadowed many clinicians as they conducted their work.

As with our prior research, the interviews were usually face-to-face, but a few were via the phone. Several involved follow-up calls and emails. A semi-structured interview schedule is available from the authors. (We are currently engaged in deeper analysis and experimental work based on our findings.)

Security controls must obviously be addressed in concert with sociological and workflow issues. As Figure 1 sketches, tensions will remain among IT's security needs, IT's security policies (reasonable or otherwise), circumvention "justified" by perceived clinical necessities and actual clinical necessities. In addition, there is a continual dance between cyber security engineers and the clinicians who seek to treat patients; where clinicians view cyber security as an annoyance rather than as an essential part of patient safety and organizational mission. As two of us observed in a recent analysis, workarounds are often the only way essential tasks can be accomplished, the organization's mission can be served, and the conflicting perspectives of the players accommodated [12].

3. Authentication

The standard way to ensure that only the right users access the appropriate files in the hospital, clinic or practice is to have the system authenticate the user. In healthcare (as in most other domains), this is typically done with a username and password.

However, in healthcare, we see endemic circumvention of password-based authentication. In hospital after hospital and clinic after clinic, we find users write down passwords everywhere. Sticky notes form sticky stalagmites on medical devices and in medication preparation rooms. We've observed entire hospital units share a password to a medical device, where the password is taped onto the device. We found emergency room supply rooms with locked doors where the lock code was written on the door--no one wanted to prevent a clinician from obtaining emergency supplies because they didn't remember the code. One vendor even distributed stickers touting "to write your username and password and post on your computer monitor" (Figure 2). A newspaper found a discarded computer from a practice contained a Word document of the employees' passwords—conveniently linked from a desktop icon (Figure 3).

Clinicians share passwords with others so that they can read the same patients' charts even though they might have access in common. A misbehaving hospital technician used a physician's PIN code to create fake reports for patients.

Standard accepted practices for strong password hygiene can be non-existent in healthcare—the US Inspection General notes that NIST will certify EHR systems as secure even if passwords are only one-character long [13]. However, it's not clear that stronger password requirements yield better security. A medical informatics officer lamented that "routine password expiry…forces everyone to write down their password." Dhamija and Perrig [14] observed that users forced to change one password may change all their other ones to match. Observing authentication in medical IT, Heckle [15] noted that clinicians tried to do that but were annoyed when passwords expired at different times.

Expiry can also directly impact patient care: one physician colleague lamented that a practice may require a physician to do rounds at a hospital monthly—but that unfortunate expiration intervals can force the physician to spend as long at the help desk resetting an expired password as he or she then spends treating patients.

4. De-Authentication

After authentication comes what some medical security officers call the *de-authentication* problem. How do we ensure a user's computer session ends when the user leaves? If a user's computer session extends beyond the active need of the user, it leaves the computer vulnerable to misuse by an unauthorized person (say, a passing visitor) or to an authorized user who assumes he or she is entering information for a patient different that the one still logged in on the screen. Koppel et al [16] document physicians ordering medications for the wrong patient because a computer was left on and the doctors didn't realize it was open for a different patient.

Previously, we reported how clever clinicians at one hospital defeated proximity-sensor-based timeouts by putting Styrofoam cups over the detectors, and how (at another hospital) the most junior person on a medical team is expected to keep pressing the space bar on everyone's keyboard to prevent timeouts.

Since then, we've heard a physician complain that a clinic's dictation system had a five-minute timeout, requiring the physician re-authenticate with a password (which takes one minute). During a 14-hour day, the clinician estimated he spent almost 1.5 hours merely logging in.

Heckle offered several relevant observations here [15]. She saw clinicians offering their logged-in session to the next clinician as a "professional courtesy," even during security training sessions. IT personnel added an easy key-sequence to force easy logout—but failed to do this on all machines, so that clinicians attempting to do the right thing would still leave themselves logged in. Nurses would circumvent the need to log out of COWs by placing "sweaters or large signs with their names on them" or hiding them or simply lowering laptop screens.

Failure to have automatic de-authentication is also a usability problem. A nurse reports that one hospital's EMR prevented users from logging in if they were already logged in somewhere else, although it would not meaningfully identify where the offending session was. Unfortunately, the nursing workflow included frequent interruptions—unexpectedly calling a nurse away from her COW. The workflow also included burdensome transitions, such as cleaning and suiting up for surgery. These security design decisions and workflow issues interacted badly: when a nurse going into surgery discovered she was still logged-in, she'd either have to un-gown—or yell for a colleague in the non-sterile area to interrupt her work and go log her out.

5. Breaking the Representation

In our earlier analysis [12], we looked at a set of health IT usability problems as mismatches between the medical reality and its representation in the electronic system. A large number of medical workarounds involved creative clinicians introducing distortions into what should be a direct correspondence. For example: a) In one EHR, patients meeting protocols for blood thinners prophylaxis force clinicians to order blood thinners before they can end their computer session—even if the patient is already on blood thinners. Clinicians must carry out a dangerous workaround of ordering a second dose (lethal if the patient actually receives it), quit the system, then re-log-in to cancel the second dose; b) At a large city hospital, death certificates require the doctor's digital thumbprint. However, only one of the doctors has thumbs that can be read by the digital reader. Consequently, only that one doctor signs all of the death certificates, no matter whose patient the deceased was.

As in other domains, clinicians would also create *shadow systems* operating in parallel to the health IT. Doctors have "shadow notes." Nurses have the "nurse's brain:" a single page with all one's tasks for all of one's patients. "You'd be lost without it, e.g., "at 2:00 I need to do this, later I need to do this, mother is nasty so don't answer phones from her, etc." "Occasionally, information in the *brain* is not information you want in the formal record." Nurses are told to discard paper notes not in the electronic system. A dental hygienist enthusiastically reported keeping a shadow dental record when computer systems did not allow for the desired level of precision.

At one hospital, nurses in pre-op need to physically move patients to the OR, which is 2 minutes away. It's important to the OR people that the time of the transfer into the OR is accurately recorded (to the minute). But the patient record (and the EMR portal) is at pre-op, not in the doorway to the OR. When the hospital had a paper-based EMR, the nurses would enter "current time + 2 min" into the paper record before rolling the patient down the hall. However, the new EMR does not allow future times; consequently, the nurses leave themselves logged in but turn the monitor off--and then come back to the pre-op afterward and record the OR transfer time.

6. Permission Management

We also see many workaround scenarios stemming from the difficulty of permission management in healthcare. Permission management, or *provisioning*, refers to the business process of specifying which individuals or groups are allowed access to which files and data. On paper, it's easy; in reality, it's not [17]. Clinicians often have multiple responsibilities—sometimes moving between hospitals with multiple roles at each one, but accessing the same back-end EHR. Residents change services every 30 days during their training. If access is limited to one service, it needs to be reconfigured that often. However, a resident may be consulted about a former patient, to which he/she no longer has access. More frequent are clinicians who serve in multiple roles: the CMIO may need access to every patient record, not only those in her/his specific medical sub-discipline. A physician who focuses on infectious disease may also be on the committee that oversees medication errors, and thus requires access to the pharmacy IT system and the nurses medication administration system. In some hospitals, nurses sometimes authenticate as nurses and sometimes as doctors.

7. Undermining the Medical Mission

Many workarounds occur because the health IT itself can undermine the central mission of the clinician: serving patients. At a hospital with a "tele-ICU," patients must be monitored from a distant nurse's station, but when bathing the patient, the nurses will cover the camera for patient privacy.

Harrison et al observed "HIT implementation can alter or disrupt oral communication among clinicians, even when talk is faster, more clinically accurate, and safer than transmitting information through the HIT" [18]. Another study found that patients regarded physicians who used EMR as "less capable than a physician using unaided judgment" [19].

In one EHR, a doctor could not find the needed medication in the hospital's formulary (list of available medications)--so entered the drug in a free-text box he thought would be seen. However, the box was not visible; the order was not seen, and the patient suffered loss of half his stomach [16]. (In this case, the failure of the EHR to be sufficiently expressive led to a workaround which did not work.)

8. Conclusion

Understanding circumventions of cybersecurity in a healthcare setting clearly requires more than an analysis of the computer rules and the computer-generated logs of access from those with and without designated permission levels. We found it necessary to conduct interviews, focus groups, and observations; to shadow clinicians, attend meetings, and to conduct surveys of staff. Ethnographic investigation of what happens in the medical workplace emerges as a key method because in the inevitable conflict between even well-intended people vs. the machines and the machine rule makers, it's the people who are more creative and motivated. This is especially true in healthcare settings, with professionals who carry the responsibility of patient care.

Acknowledgements

This material is based in part upon work supported by the Army Research Office under Award No. W911NF-13-1-0086 and partial support from NSF CNS-103715.

References

[1] 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.
[2] L.F. Cranor and S. Garfinkel, eds. *Security and Usability*. O'Reilly, 2005.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] S. Riley. "Password Security: What Users Know and What They Actually Do." *Usability News*. 8(1), February 2006.
[9] 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.
[10] J Blythe. R. Koppel, S.W. Smith. "Circumvention of Security: Good Users Do Bad Things" *IEEE Security and Privacy*. Sept/Oct, 2013. pp.80-83
[11] R. Koppel et al., "Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety," *J. Am Medical Informatics Assoc*., 15(4) 2008, pp. 408–423.
[12] 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.
[13] E. McCann. "OIG: Certified EHRs aren't so secure." *Health Care IT News*. August 5, 2014. http://www.healthcareitnews.com/news/oig-certified-ehrs-arent-so-secure
[14] R. Dhamija and A. Perrig. "Deja Vu: A User Study Using Images for Authentication." *Proceedings of the 9th USENIX Security Symposium*, 2000.
[15] R.R. Heckle. "Security Dilemma: Healthcare Clinicians at Work." *IEEE Security and Privacy*. 9(6):14--19. 2011.
[16] R. Koppel et al. "Role of computerized physician order entry systems in facilitating medication errors." *JAMA: J. Amer Medical Assoc*. Mar 9, 2005. 293:10, pp.1197-1203
[17] 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.
[18] M. Harrison et al. "Unintended Consequences of Information Technologies in Health Care—An Interactive Sociotechnical Analysis." *J. Am Medical Informatics Assoc*. 14(5): 542-549 . 2005.
[19] V. Shaffer et al. "Why Do Patients Derogate Physicians Who Use a Computer-Based Diagnostic Support System?" *Medical Decision Making*. 33: 108 2013.

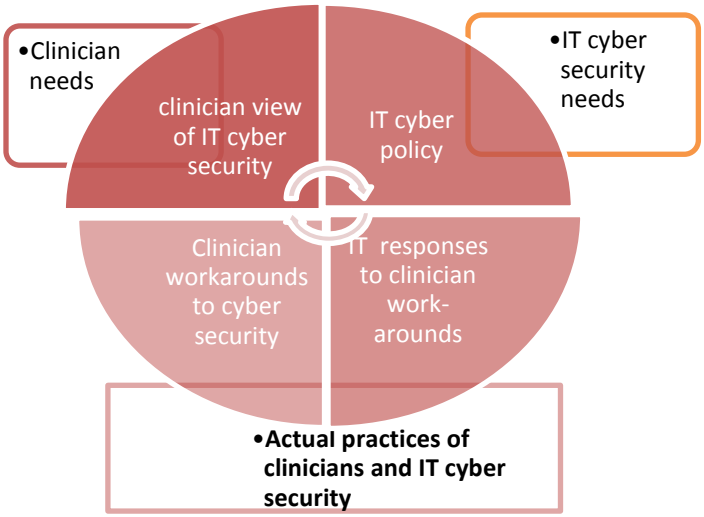

Figure 1: Tensions will remain among IT's security needs, IT's security policies (reasonable or otherwise), circumvention "justified" by perceived clinical necessities and actual clinical necessities

Figure 2: Stickers distributed by a health IT vendor.

Figure 3: Desktop shortcut found on abandoned PC from medical practice.