Dr. Jekyll or Mr. Hyde: Information Security in the Ecosystem of Healthcare

Joseph A. Cooley* and Sean W. Smith†
Department of Computer Science
Dartmouth College
Sudikoff Lab: HB 6211
Hanover, NH 03755 USA
{jac,sws}@cs.dartmouth.edu

Abstract

"Jekyll and Hyde" embodies how information security affects today's healthcare ecosystem. When security works, it promotes patient health and a smooth operating ecosystem (Dr. Jekyll); when it doesn't, privacy and health compromises can occur (Mr. Hyde).

In this paper, we argue that unusable security triggers this split personality and in doing so, compromises the heart of the healthcare ecosystem: the trust relationships that comprise the system. This compromise creates a trust void that ecosystem participants fill with more unusable-security further reinforcing the split personality. To encourage Dr. Jekyll to oust his alter ego and hence, avoid this reinforcement, we postulate a set of usable-security axioms and propose supporting areas of research. We consider both policy and mechanism as important components of usable information security.

1 Introduction

Trust is defined using a three-part relation, *Alice trusts Bob to do X* [3], and we argue that this trust relation forms the cornerstone of the healthcare ecosystem. Clinicians trust peers to diagnose special conditions, patients trust care providers' professional judgments, and hospitals trust business partners to provide services. Sociologists also define a variety of channels through which people build trust, such as expectation of future behavior, third-party guarantees, and past experiences [1]. We argue that ecosystem participants, or actors, rely on these, too.

When security functions properly and fits seamlessly into daily routines, trust-relationships remain intact and Dr. Jekyll [7] visits. When security imposes, actors sometimes change their behavior to skirt security for important practical reasons [6]. Consequently, additional vulnerabilities can arise from adversaries or mistakes creating a trust void and thus an apparent need for more security. The root problem of usable security, however, remains unaddressed. Effectively, Mr. Hyde appears to reinforce unusable security.

2 Motivating Mr. Hyde

Introducing unusable security policy and mechanism into the healthcare ecosystem can motivate Mr. Hyde. Actors adapt their behavior under the forces of new security—not to avoid or align with security, but to maintain a functional environment and achieve new goals that new technology allows [6]. We conjecture that in general, security causes actors to adapt for the following reasons:

a) **Actors bear workflow constraints, liability, and reputation associated with systems that they have limited control over.** For example, healthcare organizations purchase new electronic systems to reduce operational costs or differentiate themselves in a marketplace of care providers. The hidden costs of such purchases arrive when systems slow daily routines or fail entirely in some fashion. Unfortunately, end users have little control over many of these hidden costs, leaving them to the mercy of developers who control software reliability, functionality, and interfaces. Developers, thus, can add burden to care providers' daily routines if code crashes or interfaces do not align with the providers' needs and workflows.

b) **Actors' primary goals and expectations can misalign with practice and promote unintended con-**

*This work is sponsored by the Department of Defense under Air Force contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

†This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under Grant Award Number 0910842. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation.

sequences. Policymakers craft policy but cannot fully understand its operational impact in all situations. For example, some policies slow daily operations to the point where clinicians circumvent policy mechanisms to provide care. In the process, patient privacy may be jeopardized as clinicians trade timely access for weakened security using short or shared passwords, shared logins, or persistent login sessions. Ironically, the letter of a policy can compromise daily activities and consequently suppress the intended spirit of the policy. Also, if security policy does not align with daily routines, new, less-secure practices can evolve [4]. When mechanisms align with needs but don't include proper security interfaces, mechanism users can suffer unintended and unknown loss [5].

3 Enticing Dr. Jekyll

In order to entice Dr. Jekyll, we must carefully define and implement usable security in the healthcare ecosystem. Interfaces of security mechanisms must be usable or users will have little hope of achieving security through them [2]. To achieve this goal, we postulate that usable security will begin with the following three axioms:

a) **Align policy with practice.** Policymakers set high-level goals and practitioners "implement" them. The practical details of each deployment environment affect how well a policy aligns with operational considerations and how well a protected system implements the spirit of the policy. Thus, to improve overall security, we must craft usable security policies that support policy adjustments according to practical considerations. Metrics can help policymakers understand concretely the effects of policy on actors' daily routines and the extent to which actors subvert policy.

b) **Align security mechanisms with practice.** *Usable* security can become *used* security when mechanisms align with practice. To understand alignment, as with policy, we need to collect more quality metrics that define precisely how users interact with security mechanisms on a daily basis in the healthcare ecosystem. In doing so, we can answer questions such as how and why do users subvert existing mechanisms, and which mechanisms work well and why?

c) **Emphasize timely, actionable feedback.** Finally, developers and users must work closely with one another to tune usability and fix bugs in a timely fashion. Policymakers must craft policy to enable timely adjustments on an individual basis, before policy-related problems become large in scale and systematic in nature. All parties can benefit from timely, actionable information. To achieve this nirvana, we need new tools and techniques to automatically collect secure "usability" logs *in situ*. Such logs will provide rich information in useful dimensions and leave the rest anonymized—security mechanisms should protect all ecosystem actors, including the subjects of feedback. Such logs might inform both policymakers and developers.

4 Summary

In this paper, we described how trust relationships form the cornerstone of the healthcare ecosystem. We argued how unusable security reduces the integrity of these relationships and consequently, stimulates a "Jekyll and Hyde" effect on actors in the ecosystem: when security works, it promotes health and a smooth operating ecosystem; when it doesn't, health and privacy compromises can occur, signaling a need for more security that stimulates the problem cycle. We argued that a set of axioms and supporting research can combat the problem cycle, including research at the intersection of security, systems, and daily routine; research in measuring policy effects; and research in secure "usability" logging. Altogether, we argued that carefully engineered, *usable* security promotes *used* security: security that can fit naturally into a practitioners workflow, that is composed of meaningful feedback, and that benefits all actors.

References

[1] D. Anthony. Trust and Technology. http://www.ists.dartmouth.edu/docs/BrownbagT4Tfall08.pdf, 2008.

[2] S. L. Garfinkel and R. C. Miller. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 13–24, New York, NY, USA, 2005. ACM.

[3] R. Hardin. *Trust and Trustworthiness*. Russell Sage Foundation Publications, 2002.

[4] M. Johnson, S. M. Bellovin, R. W. Reeder, and S. Schechter. Laissez-Faire File Sharing: Access Control Designed for Individuals at the Endpoints. In *New Security Paradigms Workshop*, September 2009.

[5] M. E. Johnson, D. McGuire, and N. D. Willey. Why File Sharing Networks Are Dangerous? *Communications of the ACM*, 52(2):134–138, 2009.

[6] S. Sinclair and S. Smith. Preventative Directions For Insider Threat Mitigation Via Access Control. *Insider Attack and Cyber Security*, pages 165–194, 2008.

[7] R. L. Stevenson. *Strange Case of Dr. Jekyll and Mr. Hyde*. Longmans, Green and Company, London, England, 1886.