Panel: Usable Cryptography: Manifest Destiny or Oxymoron?

Zurko, M.E.; Patrick, Andrew

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

*Panel: Usable Cryptography: Manifest Destiny or Oxymoron? **

Zurko, M.E., Patrick, A.S.
July 2008

* published in Lecture Notes in Computer Science (LNCS) 5143. July 2008. NRC 50399.

Canada

Panel: Usable Cryptography: Manifest Destiny or Oxymoron?

Mary Ellen Zurko[1] and Andrew S. Patrick[2]

[1] IBM, Westford, Massachusetts, USA
mzurko@us.ibm.com
[2] Institute for Information Technology, National Research Council of Canada
Andrew.Patrick@nrc-cnrc.gc.ca

Abstract. Outside of SSL, Notes/Domino, and federal PKIs, PK cryptography hasn't caught on. SSL is hugely successful in providing network protection. But its server authentication feature is currently useless in phishing attacks, and its client authentication is largely unused. A number of user studies indicate that while some subset of users know about and notice "the padlock", few know what it really is, and none use it to protect them from phishing. This panel posits that the points where the cryptographic system meets the user are where its success has been blocked (e.g. key mgmt, password for protecting keys, understanding risk, threat, and assurance). We explore that assumption, and the past, present, and future of usable cryptography.

Keywords: User-centered security, cryptography.

1 Introduction

As a conference and a community, the "financial cryptography" conference (which this panel was part of) is obviously dedicated (at least in part) to the practical utility of cryptography in financial applications. A straw poll of the attendees found that the majority believed the notion of "usable cryptography" to be a manifest destiny. Many cryptographic breakthroughs have been targeted at the promise of practical use. Part of the allure of public key cryptography is the promise of deployability and usability. We all get one key pair (or the number we like), and use them with each other. More recently, Identity Based Encryption makes it easier to find or know someone's public key (another deployability and usability concern). Examples of successful use of cryptography include SSL, Notes/Domino, federal PKIs, virtual private networks (VPNs) and wireless protocols.

These examples fall short of the hope and promise of public key (and other sorts of) cryptography. "Why Johnny Can't Encrypt" [1] was foundational usable security research in 1999, covering email encryption. While there has been much follow on research, cryptographically protected email is still not widely deployed. SSL is hugely successful in providing network protection. But its server authentication feature is currently useless in phishing attacks, and its client authentication is largely unused

G. Tsudik (Ed.): FC 2008, LNCS 5143, pp. 302–306, 2008.

and even unknown. A number of user studies indicate that while some subset of users know about and notice "the padlock" (browser indications of when SSL protection is being provided on a page), few know what it really is, and none use it to protect them from phishing [2]. Digital Rights Management (DRM) seems largely stalled, and many big players are actively looking for alternative economic approaches.

This panel posits that the points where the cryptographic system meets the user are where its success has been blocked. These include key management and distribution, passwords for protecting keys, deciding what keys to trust and understanding the risks in trust, understanding threats to the cryptographic protocols, and assurance. The panel (and conference participants) explored that assumption, and the past, present, and future of usable cryptography.

The panelists were Andrew Patrick (NRC Canada & Carleton University), Phil Hallam-Baker (Verisign) and Gene Tsudik (UC Irvine). Below, Mary Ellen Zurko summarizes the positions of Phil Hallam-Baker and Gene Tsudik, and Andrew Patrick outlines his own position on this topic

2 You Can't Make Them Drink

Phil Hallam-Baker's position was, "you can give a user crypto but you can't make them drink". He sees unusable software as insecure shelfware. The way to change this is to not make mistakes, a daunting task. While science generally asks "Did I make a mistake?", Engineering produces rules which, if followed, are meant to minimize mistakes. Phil posits two laws of usable secure interfaces to help minimize mistakes. The first is to avoid providing insufficient information for the user to be usably secure. He sees violating this law as a prime reason for phishing. An example that provides sufficient information to the user to authenticate a bank is Secure Internet Letterhead, which uses cryptography to provide the assurance behind a display of company origin in email. A second law is to minimize complexity. A cryptographic example of that is the encryption of email. Encrypting some, but not all email, or only some of the time, increases complexity, by introducing additional user choice and additional error cases. For example, if the user chooses to encrypt, but the system cannot, due to the system's inability to find a key to use, the user is generally asked if they want to send unencrypted or not send the email. This additional complexity can be done away with by the use of promiscuous encryption; always encrypting email sent.

3 Usable Cryptography: What Is It Good for?

Gene Tsudik asks, "usable cryptography, what is it good for?". He suggests that perhaps we need to strive for useful cryptography, and states that they are not the same (usable <.> useful). He chooses neither manifest destiny nor oxymoron for the notion of usable cryptography, but that it is too early to say. The examples of protected pipes (SSL) and walled gardens (Notes/Domino) are successful because they are either unobtrusive or imposed on users. He outlines two curses. The first is that security is not a service, but an enabler. Security and privacy are not **useful** to the average user. Instant messaging, social networking, web searching and browsing are useful. Even

backups are useful. But we have not convinced users that security is useful. Since it's not **useful**, making it **usable** is **useless**. Our second curse is abbreviations and jargon. Security professionals use the terms "authenticate" and "authentication", but not in the same way it's used in the more common notion to "authenticate a document". Our technical use of "repudiate" and "repudiation" is not the same as the natural language notion, "repudiate this statement by so-and-so". When we use "certificate" and "certification", we don't' mean "course completion" or "quality", as in ISO 9000. And we don't use "revoke" or "revoked" in the same sense as "your authority is revoked". Abbreviations that an average user might encounter include SSL, TLS, HTTPS, CA, CRL, OCSP, PKC, WEP, WPA, IEEE 802.1x, VPN, IPSEC, and IKE. Some jargon makes sense, perhaps accidentally, including "firewall", "spam", and "virus". Gene posits that the curse of abbreviations and jargon can be overcome, perhaps the same way that automotive jargon is coped with. However, the curse of security as an enabler, not a service, is here to stay, and we need to figure out what usable cryptography might mean within that context.

4 "Usable Cryptography" as an Impossible State

When the topic of this panel, "usable cryptography", was proposed, I immediately thought it was a curious choice of words. To me, usability and cryptography don't go together, not because it is hard to make usable cryptography, but because they are really terms from two different domains. It is the usual case of comparing "apples" and "oranges" or worse, it is really talking about an impossible state. Saying "usable cryptography" is equivalent to saying "usable osmosis" or "usable photosynthesis" – it just doesn't make any sense.

Wanting to re-assure myself that my first reactions were correct, I consulted an all-powerful, non-random oracle. I did a Google search on the term "usable cryptography", and Google returned 12 hits. One of the hits was a description of this panel. Another was a paper at the 2004 Swiss Unix Conference on disk encryption that actually said little about usability. Other uses of the term included cryptography that was usable in the real-world and therefore always susceptible to attacks, and cryptography that was freely usable (free as in beer). One corporate site described "usable cryptography" as cryptography that could be defeated by their password recovery and forensic tools, and one patent application used the term to describe any cryptography that was currently available. None of the Google results used the term "usable cryptography" in the sense of information hiding that is easy for people to use.

The reason why "usable cryptography" is an impossible state is that cryptography is a process or method, while users interact with products or services. Rarely is cryptography a product or service of interest. Cryptography and usability occur at different levels in a hierarchy of human-technology interaction, as is shown in Figure 1. At the top level of this scheme are the products and services that users care about, for example banking or shopping or communicating. At lower levels are various technologies that enable these top-level services, and these lower levels provide key functions or features for the applications above (e.g., integrity, transaction security). This hierarchical model of end-user services and enabling technologies was developed as an extension of the traditional 7-layer OSI model by Bauer and Patrick [3] and applied in

a number of areas. In the model, three new human-computer interaction layers are proposed on top of the traditional OSI layers: human needs (10), human performance (9), and display (8).

Users don't want cryptography, they want products and services. Some of these products and services may employ cryptographic methods, and they might even need cryptography to fulfill the users' needs, but rarely do users want cryptography directly. Users value product and services based on their "usefulness", where usefulness is determined by utility and usability. Utility and usability does not happen at the level of "cryptography", but instead at the level of products and services.

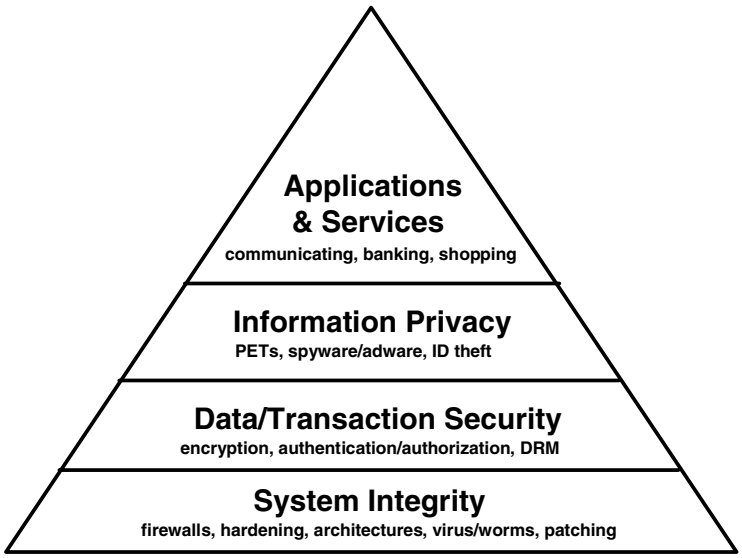

Fig. 1. Hierarchical scheme of human-technology interaction as it relates to security

How does one address, then, the issue of "usable cryptography"? The answer is to think in terms of products and services, and not in terms of processes and methods. What is needed is a top-down approach that begins by understanding users' tasks and goals. From there, we can determine the users' needs and requirements. Only then can we think about particular methods and technologies that can meet those requirements. The process becomes one of product design rather than technology development.

Good products don't just happen. Product design (or industrial design) is a well-established discipline that has developed its own methods for gathering information about people and the things they interact with. Most great products have large product design teams behind them. These teams identify human needs and establish target specifications in terms of utility and usability. Designers develop product concepts, which can be realized in prototypes and tested in a laboratory. Product designers often continue to test their products once they are in the marketplace, to gauge acceptance and assess the competition. Product designers use a variety of methods for gathering data, including ethnography, interviews, surveys, focus groups, usability tests, and secret shoppers. What is needed to build "usable cryptography" is for more people to

adopt a product design perspective. This is in addition to the talented people who are currently developing new, improved cryptographic methods and procedures.

Acknowledgments. Thank you to the FC08 organizers who accepted this panel, and particularly to Ray Hirschfeld, for his hard work and support.

References

1. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th Usenix Security Symposium, pp. 169–184 (1999)
2. Dhamija, R., Tygar, J.D., Hearst, M.: Why Phishing Works. In: CHI 2006 (2006)
3. Bauer, B., Patrick, A.S.: A human factors extension to the seven-layer OSI reference model. IAENG International Journal of Computer Science (in press)