The Human Element
Challenges and Opportunities for Technical Security

Volker Roth
Chief Technology Officer, OGM Laboratory LLC, Omaha, NE

Position Paper
28 June, 2004

The "human element" has always posed a challenge in the design of secure systems — a challenge that increases with the ever growing complexity of networked systems on which modern society depends. We hold the opinion that often over--engineering of security technology inhibits its take--up which leads to the seemingly paradoxical situation that technology with fewer security features may provide greater overall security through superior adoption. In order to illustrate our point, we briefly discuss the case of electronic mail below. However, the limitations of human cognition that often play against the mastering of sophisticated security mechanisms also provide opportunities to design security-critical systems in a fashion that is more secure than what we are currently used to, which we consider an interesting reversal of paradigms. Again, we refer to an example drawn from our recent research.

Support for strong electronic mail security is widely available yet only few communicants appear to make use of these features. Apparently, the operational overhead of security outweighs its perceived benefits. We argue that public key certificates signed by intermediaries (e.g., certification authorities (CA) with limited or nonexistent liability, or peers in PGP's Web of Trust model) and digital signatures account for a considerable cognitive or operational overhead, but they contribute marginally to the practical level of security. By eliminating these primitives, the costs versus benefits ratio can be improved. This may yield a level of security that is less than perfect, but which is still "good enough", as Sandhu puts it. Smetters and Grinter are even more straightforward in this respect, and ask "if you put usability first, how much security can you get?" Towards increasing the benefits versus overhead ratio we suggest an approach that considers security and usability tradeoffs from the outset. We separate key management from key authentication. The opportunistic key management and key update scheme that we suggest should operate transparently for users, and should be complemented by visualization and interaction techniques that communicate the security state of sent and received mail to users in a non-intrusive fashion. Towards a practical assessment of the overheads of key authentication, we conducted a preliminary quantitative analysis of users' mail behavior and found that few communicants account for a majority of exchanged mails. We argue that for individual non-commercial users, out-of-band verification of keys could be more economical than building trust in public key certificates issued by third parties. We are convinced that key verification can be easier explained to humans than the concepts that underpin certificates. In this vein, we argue that human computer interaction (HCI) techniques can support key verification more effectively than e.g., building trust in certificates.

For an area in which limitations of cognitive capacity may play against the adversary, consider personal identification numbers (PINs) and magnetic stripe cards which are in common use for electronic payments and cash withdrawal. Reported incidents document that criminals easily pickpocket cards or skim them by swiping them through additional card readers. PINs are obtained by shoulder surfing, through the use of mirrors or conceiled miniature cameras. Both elements, the PIN and the card, are generally sufficient to give the criminal full access to the victim's account. We investigated alternative PIN entry methods to which we refer as *cognitive trapdoor games.* These methods make it significantly harder for a criminal to obtain PINs even if he *fully observes the entire input and output of a PIN entry procedure.* We also introduce the idea of *probabilistic cognitive trapdoor games,* which offer limited resilience to shoulder surfing even if the criminal records a PIN entry procedure with a camera.