Chapter XI
Security Configuration for Non-Experts: A Case Study in Wireless Network Configuration

Cynthia Kuo
Carnegie Mellon University, USA

Adrian Perrig
Carnegie Mellon University, USA

Jesse Walker
Intel Corporation, USA

ABSTRACT

End users often find that security configuration interfaces are difficult to use. In this chapter, we explore how application designers can improve the design and evaluation of security configuration interfaces. We use IEEE 802.11 network configuration as a case study. First, we design and implement a configuration interface that guides users through secure network configuration. The key insight is that users have a difficult time translating their security goals into specific feature configurations. Our interface automates the translation from users' high-level goals to low-level feature configurations. Second, we develop and conduct a user study to compare our interface design with commercially available products. We adapt existing user research methods to sidestep common difficulties in evaluating security applications. Using our configuration interface, non-expert users are able to secure their networks as well as expert users. In general, our research addresses prevalent issues in the design and evaluation of consumer-configured security applications.

INTRODUCTION

For home consumers, the setup and configuration of new technologies is a daunting experience. The most intimidating configuration interfaces are often feature-based. They list the different technical features that end users can configure. Users select the appropriate radio button or drop-down box option and the product changes its behavior accordingly. This approach is effective — if users know what they are doing. For users unfamiliar with the technology, the obstacles are formidable. First, users must articulate their goals for the configuration. Second, they must map these goals to the product's features. Last, users must configure the product features correctly.

Feature-based configuration interfaces fail to consider how people interact with technology. Reeves and Nass (1996) show that we apply the same social norms that we use for human beings to our "conversations" with computers. Now consider the typical interaction between a person and a security product. It is a dysfunctional conversation. The user states, "I would like to achieve goals 1, 2, and 3." The product declares, "I have features A through Z!" Unfortunately, user goals and product features may not map easily to one another. As a result, many users struggle or give up entirely. For security professionals, we argue these interfaces are psychologically *un*acceptable (Saltzer & Schroeder, 1975).[1]

In the early days of computing, security configuration was a lesser problem. Systems were configured by early adopters, who tend to be expert users. Experts have the ability and the willingness to master psychologically unacceptable configuration schemes. However, the recent explosion of personal computers and mobile devices changes the nature of the problem; home systems are now regularly managed by non-expert users. Today, security configuration is required for each system, in each home. We are beginning to see the consequences of difficult configuration schemes: very few users enable available security features. This problem will only grow as devices proliferate.

Among IEEE 802.11 wireless networks in the home, only 20% to 30% enable some type of security feature (Cohen, 2004). Some security experts interpret this statistic as evidence that home users are too ignorant or too unconcerned about security to enable security measures. However, the problem is more fundamental: the user experience of consumer 802.11 (also known as "Wi-Fi") products is flawed. For approximately every 10 products sold, one consumer calls technical support. Most calls address basic setup issues, such as establishing Internet connectivity. Moreover, representatives of the Wi-Fi Alliance report that up to 30% of all 802.11 equipment purchased for the home is returned (Gefrides, 2004). This is an order of magnitude higher than other electronics products, such as VCRs. Furthermore, the vast majority of returned products—an estimated 90%—is *not* defective. For many home consumers, basic network setup is too difficult—even without considering secure network setup.

In this chapter, we present our design, implementation, and evaluation of a configuration interface for 802.11 access points. The interface enables home consumers to configure their wireless networks securely. Our system acts as an "expert friend," asking simple, high-level questions to elicit users' needs and goals. This information is automatically translated into a security policy for users. By avoiding feature-based questions, our system empowers end users—even novices—to make configuration decisions appropriate to their situation. With existing interfaces, more knowledgeable users are better able to configure secure networks than novice users. Our system levels the playing field, enabling non-experts to perform as well as experts. The lessons that we learned in this domain will apply to other security configuration interfaces.