Mental Models of Home Computer Security

[Poster Abstract]

Rick Wash
School of Information
University of Michigan
rwash@umich.edu

Users of home computer systems are becoming increasingly aware of the need for computer and information security systems. The market for security software for home users is growing rapidly, and includes anti-virus software, anti-spyware software, personal firewall software, personal intrusion detection / prevention systems, computer login / password / fingerprint systems, and intrusion recovery software. This software often requires security-relevant decisions be made by the home users, though most home users have little of the technical training and knowledge needed to make those decisions.

The appearance of botnets has made this a societal problem. Hackers frequently attack large numbers of easy-to-compromise home computers and combine them into a single distributed system called a *botnet*. This botnet can then be used to send spam email, commit fraud, or extort money by threatening denial of service [5]. Through botnets, insecure home computers become security problems for many others.

Though home computer users have little technical training, they do have some idea of the security threats they face and the potential countermeasures; indeed, the market for home security software is quite active. I conducted a series of 23 semi-interviews to better understand how home computer users think about security threats and security software. The respondents were chosen from a snowball sample of home computer users evenly divided between two different midwestern cities. Using these interviews I developed descriptions of the *mental models* [2] that home users use, and analysed these models to determine when these models lead users to good security decisions, and when they leave the users vulnerable. This is in contrast to Camp [1], who proposes using mental models as a method of communicating complex security risks to the general populace. She does not study how people currently think about security; rather she suggests using these models as a communication tool.

In related example of mental models, Kempton [4] studied mental models of thermostat technology in an attempt to understand the wasted energy that stems from poor choices in home heating. He found that his respondents possessed one of two models for how a thermostat works. The valve model works like a faucet, where turning it higher makes more heat come out. In the feedback model, the thermostat just turns the heater on if the temperature is too low and off if it is high enough. One model is closer to an expert's understanding of thermostats, but both models have flaws. Both models lead to some poor decisions by users of thermostats, and both models can lead to correct decisions that the other model gets wrong. Kempton concludes that "Technical experts will evaluate folk theory from this perspective [correctness] – not by asking whether it fulfills the needs of the folk. But it is the latter criterion [...] on which sound public policy must be based." Likewise, we should evaluate the mental models of home computer security not by how correct or complete it is, but by how well it serves the security needs of these users.

Dourish et al. [3] conducted a somewhat similar study of how knowledge workers in corporations handle security issues. They found that most people find some external entity that is more likely to have security expertise, and trust it to provide security. For example, some people have a more technically-savvy friend and trust him when it comes to computer security issues.

EXISTING MENTAL MODELS

We begin with an interesting observation. All of the respondents simultaneously maintained at least two distinct mental models of computer security threats. Different models were used to describe different types of threats. The first model centered around the term *virus* and concerned threats that are conceptually similar to medical contagions. The second model centered around the term *hacker* and concerned threats of malicious people "breaking in" to a computer much like a burglar would break into a house. To the respondents, these models were completely separate and described totally different types of problems that they had to face.

Contagion Models

All of the respondents had a mental model of some set of security threats as a contagion. These threats were all lumped together and described as *viruses*. By this term, respondents really meant a number of different types of malware: viruses, worms, trojan horses, adware, and spyware. But rather than distinguish between these technical categories, they lumped everything together as a computer "virus."

All of the respondents seemed to believe that viruses had a number of important properties. First of all, computer viruses just exist on the Internet. The respondents did not provide any indication that these viruses were created for a purpose. They just exist in the environment, much like biological viruses just exist, and can be "caught."

Different respondents had different conceptions of how computer viruses can be caught. A few respondents felt that viruses "just happen." (Resp. 21) Therefore, it is important to run anti-virus software just in case. The majority of respondents had a slightly more sophisticated model. They felt that computer viruses were much like real viruses in that

you are much more likely to catch a virus from unhygienic or shady places on the Internet. Examples of these shady places include: "websites with lots of ads," (Resp. 1)"unrecognized emails," (Resp. 23) and "MySpaceBook." (Resp. 8) Some respondents talked about how viruses come from downloads, or software that is intentionally acquired from the Internet. One user spoke of how viruses can come from "clicking on the wrong thing." (Resp. 13) Finally, a number of respondents had Macintosh computers, and most of them expressed a belief that Macs were "immune" to computer viruses, continuing the analogy with real viruses.

Even though all of the respondents had some form of anti-virus software installed on their computer, respondents with the less sophisticated model tended to be better protected technically. Users who felt that viruses "just happen" worked hard to keep their anti-virus software up-to-date, and regularly ran full system scans just in case they caught something. Users who felt that viruses primarily came from the unhygienic or shady parts of the Internet frequently did not keep their anti-virus systems up-to-date, or would stop virus scans that they thought would not find anything. They felt that by avoiding the shady parts of the Internet they would not catch many viruses. This can cause these users to be more vulnerable to newer viruses and botnets.

Another interesting part of the virus model is that viruses always have visible symptoms. The respondents spoke of computer viruses mucking with their data (corrupting or deleting data), viruses that slowed down or broke the computer, and viruses that cause strange new behaviors like popups or spam email. Only one respondent talked about viruses that might go unnoticed by the user of the computer. This is interesting because a number of current viruses (such as the Storm botnet) intentionally do not cause user-visible changes in the computer specifically because stealth makes it less likely that the compromise will be discovered and fixed. Since users don't recognize this as a possibility for viruses, they do not feel that they should scan their computer for unseen malware, aggravating the botnet problem.

Burglar Models

The other mental model that all of the respondents had was triggered by the word 'hacker.' When the respondents thought about 'hackers' they conjured up an image of someone 'breaking into' their computer much like a burglar would break into a house. This mental model of hackers had some interesting analogies with the real world. The respondents spoke of hackers breaking in to their computer, but like real burglars, the hackers would never stay in the computer. When they were done, they would leave the computer. Also, most of the respondents expressed a futility in preventing hackers, making statements like "if [hackers] really wanted the data, they would go in and get it anyway" and "if people want stuff they're gonna get it no matter what."

The respondents disagreed widely on how likely it was that hackers would try to break into their computer. One group of people felt that being compromised by hackers was unlikely because hackers tend to target specific things. For example, hackers target "interesting people" (Resp. 16) such as celebrities or other computer people. Hackers might also target "important" computers (Resp. 5) like bank computers or major companies. Also, hackers might choose their targets for the "mental challenge" (Resp. 20) of the attack. The users felt that they were unlikely targets because they were normal, unsophisticated users; they were not "important," "interesting," or "challenging." This is similar to how a burglar tends to target people with lots of money or jewelry. However, since botnets can use any computer with an Internet connection, real hackers tend to target people not for any of those reasons, but because they are *vulnerable* and easy to compromise. Only one respondent (Resp. 11) mentioned this possibility.

The remaining respondents felt that it was very possible that they would be broken into by hackers because they had something that hackers were looking for. A number of people had a model of hackers breaking into computers to look for financial information. This is closely related to the respondents' concerns about identity theft. A few subjects spoke of hackers that would break into computers to rummage around and see what they could find. It is the "equivalent of walking into somebody's attic and seeing how much is there – you know, you thought you threw away all that stuff" according to respondent 11. Often, these users felt that they could prevent hackers by keeping the important information (financial information) from ever being on the computer. These respondents felt that if they never put their bank and credit card information into the computer, then the hackers would have no reason to break into their computer and they would be safe. This is a false sense of security because hackers who use botnets are more interested in the computer itself than any information on the computer.

DISCUSSION

While home computer users did not have the complex, sophisticated mental models of computer security experts, they did have a couple of simple models that helped them make security-related decisions. These models led to a number of good security choices, but also led to a number of vulnerabilities that have been exploited by modern botnets. By understanding these mental models, home computer security technologies can be designed to address the vulnerabilities left by these models, and to take advantage of the knowledge that home users actually do possess.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. CNS 0716196.

1. REFERENCES

[1] J. L. Camp. Mental models of privacy and security. University of Indiana, August 2006.

[2] A. Collins and D. Gentner. How people construct mental models. In D. Holland and N. Quinn, editors, *Cultural Models in Language and Thought*. Cambridge University Press, 1987.

[3] P. Dourish, R. Grinter, J. D. de la Flor, and M. Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, November 2004.

[4] W. Kempton. Two theories of home heat control. *Cognitive Science: A Multidisciplinary Journal*, 10(1):75–90, 1986.

[5] E. Ratliff. The zombie hunters. *The New Yorker*, October 10 2006.