Incentive Design for Home Computer Security

Rick Wash
School of Information
University of Michigan
Ann Arbor, MI 48108 USA
rwash@umich.edu

CHI 2007, April 28–May 3, 2007, San Jose, California, USA.
ACM 978-1-59593-642-4/07/0004.

Abstract
Home computer users frequently lack the skills necessary to ensure proper security. Hackers exploit this to control large networks of computers ('botnets') that are used for spam, extortion, and fraud. I integrate ideas from psychology and economics to design software that provides incentives that induce better security choices by home computer users.

Keywords
Design, Economics, Security, Botnets

ACM Classification Keywords
K.6.5 [Management of Computing and Information Systems]: Security and Protection --- Invasive Software, Unauthorized Access; H.5.3 [Information Interfaces and Presentation]: Group and Organizational Interfaces --- Web-based Interaction

Botnets: An Incentive Problem
People are the weakest link in security [1]. People write their passwords on sticky notes on the screen. People don't patch their home systems and become botnet zombies. People choose whether to label a patch "critical" or just "recommended." My motivating insight is that these actions generally reflect *motivated*

behavior in response to the configuration of incentives confronting individuals.

Since behavior is motivated by the goals and preferences of the individual, this behavior can be altered by designing appropriate incentives. By carefully structuring the benefits received from using a technology, we can induce users to make choices that most benefit the system. Along with some colleagues, I am developing a methodology for incentive-centered design of technology systems that provides guidelines and examples of how to carefully structure benefits to induce appropriate user choices.

I propose to explore applying these technology design ideas to a major open problem in computer security: botnets. Botnets are large collections of computers (called "zombies") that are under the control of a single attacker. Botnets are behind a number of large security problems including spam email, distributed denial of service attacks, and multiple types of fraud and extortion[7]. A significant part of the problem concerns security vulnerabilities inherent in the design of operating systems, network protocols and middleware. I do not address this well-studied issue. Instead, I focus on the problem that many zombies result from home computers that are poorly administered: that is, they are left more vulnerable than necessary given the current state of protective software. Home computer users frequently lack the skills necessary to properly secure their computers to prevent them from becoming zombies, and to properly clean the computer once it has been compromised. By providing appropriate incentives, it may be possible to induce these home users to make better choices in securing their computers.

An individual's use of software is largely driven by his or her perception of the direct benefits and costs of use (including the costs of learning the technology). The problems of non-use and mis-use are especially great for information security technologies for at least two reasons. First, many of the benefits accrue not to the user, but to others. A home computer user rarely suffers from the insecurity he causes; it is the victims of the botnet's use that benefit from increased security. Ratliff[7] describes how botnets can be used for extorting 'protection' money from online businesses. Second, due to the nature of security systems, users are often not well-informed about the benefits to themselves. Most security systems are not directly productive; they exist to prevent productivity losses. As such, there is little feedback to users as to their own benefits (which losses were avoided) from their security choices. On the other hand, costs of recommended security behavior are usually more obvious, and thus receive more weight in user decisions. For example, CERT recommends turning off Java and JavaScript, which will cripple many popular websites such as Google GMail, MSN Games, and most so-called Web 2.0 services.[1]

The motivated behavior framing is more general than it might seem at first blush. For example, security failures due to underinformed users might be investigated as a failure to provide incentives to be better informed. Not every human action can be analyzed as a rational response to incentives, but a surprising number yield usefully to this framework.

---

[1] http://www.cert.org/tech_tips/home_networks.html

Understanding Home Users

To design security technologies that will induce changes in user behavior, it is first necessary to understand how users make security decisions, and then to characterize the security problems that result from these decisions. Thus in the first phase of my project I will perform user studies to map and understand users' existing mental models of attackers and security technologies. Mental models describe how a user thinks about a problem; the model of how things work that the person uses to make decisions about the effects of various actions.

It is well-known that in technological contexts users often operate with incorrect mental models. As an example, Kempton [5] 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, one of which was more 'correct' than the other. While both models lead to some poor decisions by users of thermostats, the 'incorrect' model can lead to correct decisions that the 'correct' 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.'' The same argument holds for technology design: whether the mental models are correct or not, technology should be designed to work well with the users who in fact employ the mental models.

Dourish et. al. [3] conducted a related study, inquiring not into mental models but how corporate knowledge workers handled security issues. They found that most people find some external entity that is more likely to have security expertise, and trust it. For example, some people have a more technically-savvy friend on whom they rely; others depend on the organization's security team.

Economic Modeling and Design Principles

In the second phase of my project, I will use appropriate tools and principles from game theory, economics and social psychology to formally model and design incentive-compatible technology-embedded mechanisms to induce better home computer security behavior. This modeling will identify desirable levels of design trade-offs so that the resulting technology will be effective.

Because of the large external effects of an individual's security decisions on the welfare of others on the network, home security provision is, in part, an instance of the economic phenomenon of public goods. I will draw on the sizable economics literature on the private provision of public goods (e.g., [2]) . This literature investigates techniques to induce individuals to voluntarily choose to provide a public good. In general, most of this work by creatively providing some additional personal benefit that is designed to efficiently align the individual user's interests with those affected by the public good.

In related work, Von Ahn and Dabbish [8] developed a game where randomly matched users try to agree on words to describe an image. The agreed-upon words then are good descriptions of the image, which can then be used for search or other purposes. User contributions are incentivized through the game aspect -- users experience fun from playing, thus motivating

them to contribute further. Google has adopted this technology in their Google Image Labeler[2].

Deployment and Validation

In the final phase of my project I will implement software based on my designs and conduct a human-subjects experiment to test the effectiveness of the design. The system will be evaluated to determine how effective it is at improving the security for home computer users. This experiment will either be conducted in the laboratory or in the field, depending on the technology developed. Field experiments are more appropriate for systems that require long time periods for interaction, but are significantly more difficult to conduct

Incentive-Centered Technology Design

This work is part of a larger effort to design technologies that incorporate incentives into software to improve its effectiveness. Many software systems can benefit from incentive design, such as peer-to-peer systems[4], anti-spam[6], and social software.

Social software faces an important challenge in its design: most social software systems rely on particular user behaviors (such as providing correct and useful data to the system) to function in their prescribed manner for other users. For example, recommender systems require that users provide accurate information about their opinions on various objects to be able to provide good recommendations to others. An ongoing side project includes studying the incentives in a popular social bookmarking website and designing incentives for increased contribution of accurate and useful tags[9].

[2] http://images.google.com/imagelabeler/

References

1. Anderson, R. Why cryptosystems fail *CCS '93: Proceedings of the 1st ACM conference on Computer and communications security*, 1993, 215--227.
2. Bergstrom, T., Blume, L.E. and Varian, H. On the private provision of public goods. *Journal of Public Economics 29* (1). 25--49.
3. Dourish, P., Grinter, R., Flor, J.D.d.l. and Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, *8* (6). 391--401.
4. Feldman, M. and Chuang, J. Overcoming Free-Riding Behavior in Peer-to-Peer Systems. *ACM Sigecomm Exchanges*, *6* (1).
5. Kempton, W. Two Theories of Home Heat Control. *Cognitive Science: A Multidisciplinary Journal*, *10* (1). 75--90.
6. Loder, T., van Alstyne, M. and Wash, R. An Economic Response to Unsolicited Communication. *Advances in Economic Analysis and Policy*, *6* (1).
7. Ratliff, E. The Zombie Hunters *The New Yorker*, 2006.
8. von Ahn, L. and Dabbish, L. Labelling Images with a Computer Game *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2004, 319--326.
9. Wash, R. and Rader, E. Incentives for Contribution in del.icio.us: The Role of Tagging in Information Discovery,, Working paper, University of Michigan, 2006.