**A Cross-Cultural Comparison of u.S. and Chinese Computer Security Awareness**

* It takes time for the level of awareness to reach a critical mass in respect to any malware. Until this point is reached, it is unlikely that users will take the proper precautions to protect themselves from this type of malware.
* Users in the U.S. appear to be reasonably aware of viruses and spyware. However, there is much to be done in terms of achieving that level of awareness for rootkits in both the U.S. and China.
* Consequently, there is no surprise that Chinese users indicated less awareness regarding spyware and viruses relative to the U.S. users
* All malware including rootkits, spyware, viruses, and blended threats are potentially very dangerous to the computing environment. Fortunately, users need not suffer the full effect of malware if the security community can raise awareness to the point where end users will utilize appropriate detection and removal tools as part of their overall computing protection paradigm.
* The survey used in this study is based on the survey used in two previous studies (Jones, Arnett, Tang, & Chen, 1993; Schmidt & Arnett, 2005). Both of these studies examined relatively new malware as it emerged on the computing landscape. The original study (Jones et al., 1993) focused on users perceptions of computer viruses. In the second study, Schmidt and Arnett (2005) utilized a similar instrument to assess users’ perceptions of spyware. The study described herein was similar in that it investigated the relatively new phenomena of rootkits. Specifically, this study examined IT users’ perceptions of rootkits, spyware, and viruses. It further compared the perceptions of users in the United States and China.

This paper is important as it shows a cross cultural analysis of different perceptions of online threats and malware.

**An Exploration of Relations Between Visual Appeal, Trustworthiness and Perceived Usability of Homepages**

Obviously, participants cannot gain a realistic picture of objective usability or reach a true sense of trustworthiness merely from looking brieﬂy at a homepage. One purpose with the preceding experiments was to determine if a relationship can be demonstrated between appeal and other types of judgment that would require additional processing in an experimental paradigm offering only a brief glimpse of each image and no opportunity to interact with the product. Although there are still many issues to be settled, the previous results appear to conﬁrm such a relationship. As visual appeal clearly dominates ﬁrst-impression judgments of other characteristics such as perceived usability and trustworthiness, which are thus subject to a halo effect, it does appear that judgments requiring additional processing are dealt with in a qualitative different manner from those of visual appeal. While lending cautious support to Tractinsky et al.’s [2000] bold assertion that what is beautiful is [perceived to be] usable, the big question of dependence or independence of visual appeal , trustworthiness, and perceived usability remains unresolved . Disentangling these complex relationships remains a very interesting challenge to the HCI community.

This paper shows how important visual design is to recognizing the security of a site among users. It also involves a methodology that compares different sites and their trust worthiness with users

**How HCI Design Influences Web Security Decision**

he findings of the research showed that, based on selfreported security decisions made in their own context of use, by far the biggest, and in some cases “only”, item of tangible security that users based their security decisions on, was whether or not the website’s address was HTTPS, and whether there was a padlock symbol in the web browser. Conversely, the research showed that the concepts of extended validation certificates have not permeated into the general public.

Although this paper provides good reference into creating a mental model, it is not replicable as it relies on users logging their own activities. In local contexts it is preferable to using interveies to probe users about their decisions

**Generative Usability: Security and User Centered Design beyond the Appliance**

**I**n this paper we have outlined some of the current state of security and usability design practice, and pressures that are driving industry towards building appliances. We have expressed some concerns as to why this is problematic, both in terms of whether it is possible to build systems that offer meaningful choice in this way and whether the type of usability that we achieve by appliancisation is what we want to support our technological ecosystem.

This paper is a recommendation on large scale designs and has low relevance to our scope.