A Flock of Birds, Safely Staged

Flinn, Scott

Publisher's version / Version de l'éditeur:

DIMACS Workshop on Usable Privacy and Security Software 2004 [Proceedings], 2004

A Flock of Birds, Safely Staged

Scott Flinn
National Research Council of Canada
Scott.Flinn@nrc.gc.ca

Introduction

Internet users face many threats. Sensitive information leaks out through viruses and spyware, it is bought and sold by organizations that use tracking techniques to build detailed dossiers, and it is given away by users themselves who fall prey to *phishing* scams and other social engineering attacks. At the same time, users pose threats to the systems they use. Infected user machines are used to relay spam, penetrate networks and escalate privileges. Insecure password management leads to increased system vulnerability. Social engineering is becoming the weapon of choice for attackers.

In response, users are advised to install virus filters, spyware detectors and personal firewalls, to browse anonymously, refuse cookies, lie when filling out forms, delete e-mail attachments without opening them, and avoid installing non-essential software. In other words, to shut down the flow of information. Sometimes, however, there are rewards to be gained by taking risks. You may get better service at a Web site if you accept their cookies. In general you may find greater value in on-line services if you are comfortable with the exposure and risk they present. But how can the risk be assessed and managed?

Suppose users were able to quickly and accurately answer the following questions with respect to every choice of action they face: (1) What is likely to go wrong? (2) What damage would result to me or others if it did? (3) How would I know if something went wrong? (4) What reason do I have to believe that it won't? (5) Who is responsible to ensure that it doesn't, and what recourse do I have if it does? We suggest that such users would be better able to negotiate the hazards of cyberspace, confidently seeking its rewards.

We have been experimenting with a system that endeavours to make answers to these questions readily available. A separate paper analyzes the risk management conjecture in greater detail and describes the prototype system [1]. It focuses on how evidence may be gathered over time to address each question. Even if you have ready answers, however, you still face the difficult problem of communicating them effectively to users. This abstract focuses on the communication, proposing a general strategy that is based on a combination of ideas from other researchers.

Of Birds and Staging

The AT&T Privacy Bird (see http://privacybird.com/ for details of its operation) is an agent that assists users in evaluating how closely a Web site's privacy policy conforms to their wishes. It provides ready answers to several of the questions posed above with respect to privacy concerns. The visual and auditory cues provided by the agent consume few cognitive or attentional resources when sites respect the user's privacy preferences. When problems are detected, the user can choose whether to enlist the agent's help in seeking information on which to base a choice of action.

There are other threats, and, in principle, the same idea can easily be multiplied across threat categories to produce a dashboard style display of signals. In our prototype, an HTTP proxy server monitors communication between a Web browser and its targets and injects a dashboard and other instrumentation into web pages. Once caution is signaled and attention has been drawn, there is still the problem of how to communicate further detail. The information should be timely and not overwhelming, and there must be a clear association between any statement of concern and its cause. The *safe staging* technique described by Whitten and Tygar [2] has the potential to address both aspects. The technique seeks to deliver effective security related guidance to users by providing timely answers to a set of questions that clearly resemble the risk management questions listed earlier. In fact, our risk management approach was inspired in part by the safe staging technique.

Consider a scenario in which a page delivered via HTTPS: contains a form that posts to an HTTP: URL. Even though the page containing the form was secured, form data will be sent in clear text. Many browsers detect this, but only after the user has committed to the act of submitting the form. Users will of course react to the warning dialog by simply dismissing it. This situation is easily detected by a user agent, but how should attention be drawn? The solution we have chosen is literally to display a warning label. When a dashboard light turns red, clicking on it causes a box to be drawn around the source of the problem (the input form in our example) with a concise label identifying the potential concern and a hyperlink that will summon a pop-up window to provide additional details, context and assistance, depending on the nature of the warning.

The idea can be applied in other contexts. Consider the e-mail attachments that are currently being used to carry viruses. It is commonly claimed that educating users to not open unknown attachments would significantly reduce the problem, but education has not yet proven effective. A common reaction is to strip attachments at the gateway – to shut down information flow. Sometimes, however, attachments are useful. Would users be educated more effectively if e-mail clients drew warning labels around potentially unsafe attachments?

To summarize, we propose combining the safe staging technique with the design philosophy of the AT&T Privacy Bird as a step towards a general purpose mechanism for guiding users safely and confidently through the hazards of cyberspace. Preliminary experience with a prototype of these ideas applied in a Web browsing context has been encouraging. It is an open question whether the idea has merit in a broader context or in other specific applications.

References

[1] Scott Flinn and Steve Stoyles. Omnivore: Risk Management through Bidirectional Transparency. Submitted to the New Security Paradigms Workshop (NSPW), September 20-23 2004.

[2] Alma Whitten and J. D. Tygar. Safe Staging for Computer Security. Presented at the CHI'03 workshop on HCI and Security Systems, April 6 2003. Retrieved April 30, 2004 from http://www.andrewpatrick.ca/CHI2003/HCISEC/hcisec-workshop-whitten.pdf.