White paper presented to Workshop on Economics and Information Security, May 16-17, 2002, University of California at Berkeley

Improving Information Flow in the Information Security Market

Carl E. Landwehr
Mitretek Systems[1]

The market for information security has long been seen as dysfunctional [1]. The remedy proposed in 1990 by [1] was to create a not-for-profit foundation that would establish Generally Accepted System Security Principles along the lines of similar principles for accounting[2]. The proposed "Information Security Foundation" never really got off the ground, though recent years have witnessed continuing efforts to establish "Best Practices" in the government and elsewhere, and several not-for-profit organizations now offer information security training and guidelines.

Going further back, to the late 70's and early 80's, U.S. government officials correctly recognized that they would be driven increasingly to base defense information systems on commercial-off-the-shelf computers and software. These systems clearly lacked the security properties sought, and so those officials tried to influence the market by creating the Trusted Computer Security Evaluation Criteria (TCSEC, the "Orange Book") and a government-financed scheme to evaluate commercial products submitted voluntarily for review. The idea was to provide a market incentive for commercial vendors to supply improved security throughout their product lines. The Defense Department could then procure competitively the systems it needed.

This attempt to leverage market forces had some good effects, but failed ultimately because:

a) The carrot of lucrative government procurements of evaluated systems never really materialized. Initially, there were few evaluated products and procurements that required them were judged non-competitive. Ultimately, officials controlling the procurements demanded the latest operating systems and features as long as there was some evidence of intention to have the product evaluated eventually; this gave vendors an incentive to start the evaluation process, but not necessarily to complete it. Further, governments often procure systems, not single products, and the evaluation criteria proved difficult or impossible to apply to systems – yet security is fundamentally a system property.
b) As the commercial market for computers boomed, the government's share of that market declined substantially, reducing government leverage overall, and private purchasers did not in general perceive similar security needs.
c) The investment required of the vendors in order to meet the evaluation criteria, in dollars but more importantly in development time, proved more than they could justify economically.

This original scheme of criteria and evaluations has evolved in the past 20 years so that product evaluations at lower, "commercial grade" levels of assurance are now conducted by for-profit commercial firms and paid for by the developers. Government participation is still required to certify the evaluation practices of the commercial firms. Greater flexibility is permitted in the specification of product functions and the levels of assurance evidence to be provided. This flexibility imposes a corresponding specification burden, however.

Rational market decisions depend on good information. All of the attempts to provide security evaluation criteria and to evaluate products can be seen as efforts to improve the flow of information in the market for secure computer systems.

---

[1] Currently on assignment to the National Science Foundation
[2] Whose enforcement seems also to require renewed attention!

The slow rate at which information about the security properties of products is generated impedes improvements in security of deployed systems. More precisely, the lack of specific information about the ability of specific components and system architectures to preserve information availability, integrity, and confidentiality in the face of failures and attacks, and the difficulty of developing this information quickly, is a strong factor in the current state of computer system security, or the lack thereof, in many widely distributed computer systems

Experience shows that information about computer security properties is hard to obtain. The properties are not only difficult to quantify and assess, they are time-consuming to evaluate. Though asymmetric information may be a factor in this market, in that a seller may know more about the security properties of his product than the buyer can, in many cases even the vendor lacks full knowledge of his product. Because it takes significant time and energy to extract the information needed to permit rational decisions, the buyer commonly faces a choice between new, unevaluated products or systems that perform better, but have uncertain security properties, and older products with better known properties but poorer performance.

One way to improve the flow of this kind of information would be to seek measures and assessments of product security that can be obtained quickly and easily. Perhaps security could be viewed as a "hidden variable" and researchers might look for related exposed variables that could be assessed more quickly. For example, a developer might be able to certify that a piece of software is not subject to buffer overflow problems. The concept of proof-carrying code also seems to fit in here: some basic properties of the code can be certified immediately before it is executed.

One might also consider providing tools to help evaluate open source software. Security information about proprietary software often takes longer to develop because only the proprietor has unrestricted access to the code and so the decision of whether to apply resources to security analysis of it is constrained. Opening source permits anyone who cares to apply resources to this task to do so [2]. Some recent efforts under DARPA's Composable High Assurance Trusted Software (CHATS) program aim to encourage security review of open source software [3].

Other kinds of information, beyond the internal properties of components or systems, are lacking from the security marketplace as well. These include reliable information on actual system behavior, actual security incidents, and actual losses. Other mechanisms are needed to foster bringing this kind of information, which is often considered sensitive by the parties who control it, to the marketplace.

Better information will make a better market for computer security. We need to explore how to bring that information to decision makers efficiently.

REFERENCES

1. National Research Council, System Security Study Committee, CSTB, *Computers at Risk*, National Academy Press, 1991. Chapter 6, "Why the Security Market Has Not Worked Well", pp.143-178. Also available at www.nap.edu
2. B. Witten., C. Landwehr, and M. Caloyannides. Does open source improve security? *IEEE Software 18*, 5, (Sept. 2001), 57-61. Also at http://www.computer.org/publications/dlib/
3. Sardonix website: www.sardonix.org