Towards Realistic Assumptions, Models, and Goals for Security Research

(White Paper for NSF Workshop)

Joan Feigenbaum
Yale University, Computer Science Dept.
P. O. Box 208285, New Haven, CT 06520-8285
http://www.cs.yale.edu/~jf

January 18, 2002

Abstract: It is our thesis that a significant amount of the existing security-research literature makes unrealistic assumptions about computing environments and about users' goals. We propose some research directions that we think are more realistic, in the realms of security models, user privacy, and digital copyright. The intent is merely to stimulate discussion and further work, and we make no claim that what follows is scholarly or complete.

Introduction

Decades of research have yielded a vast array of clever techniques that purport to enable many types of "secure" protocols; most of these techniques have been extensively and rigorously analyzed, and some have been commercially developed. However, few are in widespread use. Moreover, even if they were in widespread use, it is far from clear that they would solve the security and privacy problems that users actually have.

Why are the computers and networks that we use everyday apparently so insecure if security research has been so successful? The following answer is offered in [FFSS01]: "Our abstractions don't model our reality. … For instance, the traditional communication-confidentiality model is that Alice wants to communicate with her friend Bob without adversaries Eve and Lucifer being able to read her message. We may abstract general privacy-enhancing protocols by saying that users try to hide information by performing computations in some trusted private environment (the trusted computing base, or *TCB*) and then using the results of these computations to communicate with the outside world. … In a network where businesses bundle valuable content and personalization services, and users want anytime anywhere access from any number of devices, who is Alice, who is Bob, who is the enemy, and what is the TCB? Cryptographic research cannot answer these questions." The emphasis in [FFSS01] is on digital-content distribution, but the fact that our abstractions don't model our reality has broader implications for the research agenda.

Security Models

A typical user has no TCB. Despite steady progress on design, analysis, implementation, and deployment of algorithms and protocols, our computers and networks remain vulnerable to intrusions, denials of service, and other attacks. Indeed, there have been so many successful attacks by so many amateurs on so many major organizations' systems that they are not even front-page news any more. Most of these attacks succeed because of software bugs – and not even interesting or novel software bugs, but rather buffer overflows and other age-old, boring things. ***Research on algorithms and protocols, both theoretical and experimental, is irrelevant to these attacks that actually occur.*** Software-engineering research is certainly important and should be supported, but we have little reason to believe that mass-market software will be free of exploitable bugs during our lifetime. Indeed, some have argued on both economic and technological grounds that attackers will always be able to find technical exploits in complex systems [A01, BAB99].

Therefore, researchers should stop assuming that users have TCBs. The commodity PCs on our desks clearly are not "trustworthy" by any reasonable definition of "trust," and they can only become less so as we continue to install new applications and upgrades every day, some of them provided by vendors and non-commercial websites that make no quality guarantees. Yet, these commodity PCs are quite useful in our everyday lives. Perhaps the definitions of "security" and

"privacy" that researchers typically work with (and that require Alice and Bob to do a lot of computing within the boundaries of their respective TCBs) are too stringent. At least two general research directions suggest themselves:

(1) Take a ***risk-management approach*** to system modeling and "proofs" of security. Individual components of our computing and communications infrastructure may not have any worst-case, provable security properties, but large collections of them may have statistical properties that are "good enough" for the things we want to do with them. The risk-management approach works well in other large, complex systems such as finance. Both mathematical and experimental methods, especially data-collection and data-analysis, will be needed in this project.

(2) For the real-world situations that do require the type of provable security that researchers have already formalized and studied, figure out how to achieve security without "trustworthy" PCs and networks. Can one build simple, inexpensive, trustworthy, special-purpose devices for e-voting or other important tasks that we don't perform every day? These could be auxiliary devices, such as smart-cards, that are used in conjunction with ordinary PCs and networks, or they could be stand-alone "information appliances."

User Privacy

Users of Web-based retailers and other public websites are often called upon to supply PII ("personally identifying information," *e.g.*, names, addresses, phone numbers, *etc.*) in the course of normal use and are justifiably concerned about potential reuse, misuse, or sale of this PII. Note that a technically analogous problem is faced by copyright owners who distribute their works over the Internet. Copyright owners want to sell (or, in some cases, give away) valuable digital content to "untrusted" customers (or, more generally, users) but maintain some control over the use, copying, and modification of that content – even after it has been transferred to the customers' computers. Website users want to supply the PII that is needed for specific transactions that they choose to participate in but maintain some control over how that information is subsequently used by the other parties to that transaction – even after the information has been transferred to the other parties' computers.

Much existing security research focuses on minimizing the amount of PII that must be transferred. Examples of the techniques devised for this purpose include secure, multiparty function evaluation (SMFE) protocols, which minimize the exchange of private data, and anonymizing mixnets, which conceal participants' identities. In the digital-rights-management (DRM) arena, there is also a considerable body of work on copy-protection and related techniques for exercising remote control over digital works, but none of it has withstood concerted attacks by expert circumventers. We believe that, for most ordinary uses of public websites, these techniques are irrelevant. Basic PII is exchanged in the course of normal business transactions, and the parties to these transactions should not have to pay the costs of deploying SMFE, mixnets, or other complex protocols in order to conduct normal business; these costs are considerable, as discussed at length in [FFSS01] and the references therein.

Important questions about protection of PII include:

(3) What is the real goal, and might it be unachievable through purely technological means? For example, should it be legal to use information collected in a consumer transaction for something that is clearly more consequential than consumerism, *e.g.*, employment, law enforcement, health insurance, life insurance, *etc.*

(4) It may be technologically infeasible to *prevent* the misuse of PII once it has been collected, whether "misuse" is defined by law, contract, or digital policies such P3P preferences. (See [CLMPR00] for an overview of P3P.) However, it may be possible to develop auditing tools that monitor compliance with agreed-upon rules for handling PII. Large web-based retailers could be forced, through regulation or competitive pressure, to demonstrate compliance. In this respect, the protection of PII could be made easier than the protection of mass-market copyright material – individual users of the latter could circumvent auditing tools as easily as they could any DRM technology, and they would not be subject to the social forces that large retailers are subject to.

(5) The OECD Fair Information Principles [OECD80] are still the best general guidelines on use of PII. The technical community should develop tools that help organizations implement them.

Digital Copyright

Current US Copyright law is seriously inappropriate for digital works. Many books and articles have been written about this subject, *e.g.,* [DD00, L01, MF01]. For example, the "copy-centric" nature of the current law (*i.e.*, the primacy that it gives to the copyright owner's exclusive right of reproduction) is explored in detail in [DD00, L01, MF01] and shown to be very problematic in the digital realm, where the right to control copying is tantamount to the right to control normal use of a work – something that rights holders cannot do when the work is embodied in a physical object such as a book or CD. The security-research community has put a lot of effort into copy-control and other DRM techniques that attempt to enforce traditional copyright law, but much of the resulting technology has been circumventable. We argue that copy-control is not only hard to achieve but undesirable. [MF01] proposes as an alternative organizing principle of copyright law the right of an owner to control public distribution of the work (whether the distribution is commercial or non-commercial). Copy-centrism is just one example of the anachronistic, logically incomplete, and in some cases inconsistent nature of current copyright law.

The research-agenda item is:

(6) A general overhaul of copyright law may be appropriate, given the fundamental changes that have occurred in the technology for creating and distributing (some) copyrighted works. Computer scientists should be involved in this overhaul, because the new laws should be *feasibly implementable* as well as faithful to the purpose of copyright as put forth in the Constitution ("promoting progress in science and the useful arts"). Recent legal developments, such as the Digital Millennium Copyright Act, are the result of too much attention by the entertainment industry and other well organized stakeholders and too little attention (until it was too late) by the technical community.

References

[A01] R. Anderson, "Why information security is hard – an economic perspective,'' http://www.cl.cam.ac.uk/~rja14.

[BAB99] R. Brady, R. Anderson, and R. Ball, "Murphys's law, the fitness of evolving species, and the limits of software reliability," Technical Report 476, Cambridge University Computer Laboratory, 1999.

[CLMPR00] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," W3C Candidate Recommendation, December 2000. http://www.w3.org/TR/P3P/.

[FFSS01] J. Feigenbaum, M. Freedman, T. Sander, and A. Shostak, "Privacy Engineering for Digital Rights Management Systems," to appear in the *Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management*.

[L01] J. Litman, **Digital Copyright**, Prometheus Books, Amherst NY, 2001.

[MF01] E. Miller and J. Feigenbaum, "Taking the Copy Out of Copyright," to appear in the *Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management*.

[NRC00] National Research Council Panel on Digital Property Rights in the Emerging Information Infrastructure (Randall Davis, chair), **The Digital Dilemma: Intellectual Property in the Information Age**, National Academy Press, Washington DC, 2000.

[OECD80] Organization for Economic Cooperation and Development. "Guidelines on the protection of privacy and trans-broder flow of personal data," September 1980. http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM