Statement by

Steven M. Bellovin

smb@research.att.com
http://www.research.att.com/~smb

AT&T Labs Research

Before The

House Select Committee on

Homeland Security

Subcommittee on

Cybersecurity, Science and Research & Development

Hearing on

“Cybersecurity—Getting it Right”

July 22, 2003

Cybersecurity Research Needs

1 Introduction

It is quite clear that cybersecurity is vital to our nation's safety. A wide variety of National Research Council reports, summarized in *Cybersecurity Today and Tomorrow--Pay Now or Pay Later* [1], have illustrated the threat in no uncertain terms.

Although there are things that the information technology profession -- software vendors, network operators, and end user sites--can and should do today to improve computer security, the simple fact is that there are limits on how good a job it can do. Even with unlimited financial resources, and the best will, we could not do an adequate job. Quite simply, we do not know how to mount an adequate defense. It is usually possible to protect an arbitrary resource; it is not currently possible to protect all critical resources.

2 Threats

The types of defenses that are necessary depend on the nature of the likely attacker. Schemes that will keep out the stereotypical “hacker” -- i.e., the bored teenager with too much time and too few morals--are not very effective against a nation-state. The former typically use tools downloaded from someone more competent; the latter could develop its own custom tools, and combine them with physical world techniques such as “the three B--bribery, blackmail, and burglary”-- or terrorist attacks.

We do not have an adequate categorization of the threat model. Too little research has been done on who launches what kind of attacks. It isn't an easy thing to do; apart from the fact that most attacks are never detected, many organizations are reluctant to disclose their vulnerabilities. But we need to know the attackers' capabilities if we are to devise adequate defenses.

3 Basic Research Questions

Most computer security problems are caused by buggy software [4]. It would be naïve to assume that the problem was solvable now, when it hasn't been solved despite efforts stretching for more than 50 years. Nevertheless, we must continue to focus effort on it. If nothing else, the need now is to solve a subtly different problem: making a small subset of software correct, rather than software as a whole. We may be able to achieve it; today's operating systems are far more reliable than those used a generation ago.

However, if we are to focus our efforts on the critical software, we must learn how to divide up systems appropriately. We have long known how to do that for operating systems, but many of today's problems come from faulty applications. More

generally, we must learn how to build secure systems from insecure components, just as we can produce highly reliable computer systems from unreliable electronic parts.

We need new formal frameworks for analyzing the security of a system, and for specifying its security behavior. We do not have adequate tools for understanding how "strong" a computer system is; at best, we can say that some system can more or less Do certain things reliably. By contrast, civil engineers can tell you how much weight a bridge can hold, while locksmiths can tell you how long it will take to break into a safe using a specified set of tools.

Formal, mathematical statements have proved to be powerful tools in some areas of computer science. We need to be able to apply them to computer security issues.

Although basic cryptographic research is important and should be continued, it is not a high priority. As noted, most penetrations cannot be prevented by cryptographic means. It is more important to do a better job using the cryptographic science we have. Note that I say this as one who has published more than a dozen cryptographic research papers.

Most basic research work is done at universities. But it is not possible to scale up the amount of basic security research very quickly. There are not that many professors who are capable of doing such work; there is a limit to how much money each one can profitably use.

4 The Need for Engineering

Although, as noted, there is a need for more basic research, a great deal of prior research has not yet been translated into practice. For example, we have far more cryptographic science than we have network protocols that use this science. We need to support technology transfer to industry groups and standards organizations; we cannot protect our infrastructure with theoretical constructs. (I note that open standards are better; apart from the "many eyes" notion, with open standards there can be multiple independent implementations of the same function. The National Research Council noted that the lack of diversity in platforms was a major risk factor [4].)

More subtly, much security technology is not employed because it's too hard to use. We need research in the human factors of security technology [2].

Assuming that industry does the necessary cryptographic and human factors engineering, the results must be translated into practice. This may require incentives for software vendors to develop the code, and for end users to employ it.

As noted earlier, most security holes are due to buggy code. That is bad enough; what is worse is that most *penetrations* exploit bugs for which patches are available but

have not yet been applied. The cause is not laziness or incompetence by systems administrators; rather, it's reflective of the immense difficulty of the systems administration task. Patches have a higher bug rate than base code, and may thus be more likely to create new security holes; beyond that, a remarkable amount of code functions because of an implicit reliance on some underlying bug that was present on the development systems. Fixing a bug may, as a side-effect, disable essential applications. No responsible systems administrator will install a patch on a production system without extensive testing, but this behavior leaves the machine vulnerable. We need research to solve this dilemma. Systems administration is not a typical research topic; nevertheless, it is the area with the biggest potential payoff for a relatively modest investment.

It is worth noting that systems administration is often a high stress, low status job. Administrators often struggle to perform basic tasks because of inadequate resources. Measures to improve systems administration, in industry and government, would likely have a significant effect on practical computer security.

5 Privacy

Often, computer security depends on proper authentication of authorized users. Authentication technologies, ranging from passwords to biometrics, are subtle and difficult to use properly. Beyond simple issues of correctness, any authentication technology can be used in ways that violate personal privacy [3]. Both research on cybersecurity and deployment of technology should protect privacy to the extent feasible.

6 Conclusions

There are no simple answers to the problem of cybersecurity. What is needed is a combination of basic research, technology transfer, and applications of new and previously known techniques. We, as a nation, cannot afford to neglect the issue.

References

[1] Computer Science and Telecommunication Board, editor. *Cybersecurity Today and Tomorrow--Pay Now or Pay Later*. National Academy Press, 2002.
[2] John L. Hennessy, David A. Patterson, and Herbert S. Lin, Ed. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. National Academies Press, 2003.
[3] Stephen T. Kent and Lynette I. Millett, editors. *Who Goes There?: Authentication Through the Lens of Privacy*. National Academies Press, 2003.
[4] Fred B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 1999.