The Future of Information Security

John McLean
Catherine Meadows
Center for High Assurance Computer Systems
Naval Research Laboratory
Washington, DC 20375

Preamble

“I confess that in 1901, I said to my brother Orville that man would not fly for 50 years...Ever since, I have distrusted myself and avoided all predictions.” - Wilber Wright, 1908[1]

1 Introduction

Despite Wilber Wright’s warning, the first author of this paper published in the first proceedings of the New Security Paradigms Workshop a view on new research directions for computer security.[3] That paper urged research focused on developing three capabilities: (1) the ability to quantify the value of information assets to determine the resources a penetrator is likely to expend to compromise various types of information, (2) the ability to select a set of system properties that will raise the cost of successfully compromising system security above the value of the assets protected by that system, and (3) the ability to refine these properties into secure implementations.

Not daunted by his lack of prognostic success, the same author co-wrote a paper a couple of years later that urged a second research agenda based on the fact although we seemed to be developing expertise in building systems that could satisfy a single critical property (such as security, dependability, safety, or real-time requirements), we needed to develop expertise in building systems that could satisfy multiple critical properties.[4]

Hoping to get it right the third time around, the same author participated in a 1998 study on high-payoff INFOSEC research opportunities for the Information Research Council’s INFOSEC Science and Technology Study Group. This group focused on policy, availability, privacy/accountability, diversity, and assurance in a world where computing will be ubiquitous, virtually all computers will be networked, and coalitions will frequently form and dissolve.

[1] Cited in *The Book of Predictions* by David Wallechinsky, et al (Morrow, 1980). The authors are grateful to Hilary Hosmer for pointing out this quotation.

In this paper we take a new look at the future of computer security, taking into account the first author's three previous reports and assessing their relevance to the emerging world of security as we see it now.

2 The Future

2.1 Emerging Trends

The future is difficult to predict exactly, but there are a few trends that are becoming clear. The most far-reaching is the trend towards ubiquitous computing. Computers are getting smaller, more powerful, and playing a larger and large part of our daily lives. Moreover, the way in which we interact with computers is changing. As is noted in [5], a few years ago it was common to have a long-term relationship with a small number of computers, for example, one's personal computer or the computers used at work. We might also interact with people who had long-term relationships with their own computers; e.g. booking a flight using a travel agent who had access to a travel database or buying a house using a real-estate agent who had access to the Multiple Listing Service. Now, thanks to the World Wide Web, that is changing and we have short-term relationships with a large number of computers. We can book our flights and shop for houses by accessing them directly. This increasing number of encounters with unknown computers has already started to raise concerns about privacy and security among the general public. Finally, the emerging trend is to have the computers interact with each other directly in short-term relationships on behalf of, but not necessarily at the command of, humans. Here, the concerns about privacy and security become even greater. Although it is difficult to assure one's privacy and security on the Web, it is possible to make a conscious decision as to what to use it for, and whether or not to use it at all. It will be much more difficult to make such a decision in the brave new world of ubiquitous computing.

We believe that this emerging trend will have three major outcomes. One is to make the general public as a whole much more aware of and concerned about reliability issues in general, and security and privacy issues in particular. When computing starts to become a part of everyday life that is impossible to avoid and when computers engaged in short-term relationships with each other exchange information about people on a regular basis, then any failure or security breach can have a major effect on people's lives. Indeed, we already see increased concern about security and reliability with respect to the public's response to the Y2K problem, and with the publicity generated by the recent denial-of-service attacks on government web servers.

The second outcome concerns the role the government will play with resect to these increased concerns. In general, the government will probably play a major role in increasing the security and robustness of the infrastructure since it is a national issue that goes beyond any single corporation. Some of the issues faced here will be purely technical ones, such as how to make the infrastructure resilient in face of the loss of some of its components. Others may be more directly involved with the public's concern for privacy, such as would be the case, for example, in the provision of support for encryption. Of course, the desire for personal privacy will be balanced by the government's desire to monitor electronic transactions for purpose of assessing taxes, detecting criminal activity and fraud, etc. In some cases privacy (in the form of anonymity) may well be provided by private enterprise. Open issues will be how much government intrusion the public will tolerate for the purpose of gaining any benefits that could be achieved by government monitoring and how much privacy the public will be willing to sacrifice to gain these benefits.

The third outcome is that the security problem will become harder than ever. We will not only need to protect relatively long-term interactions between computers that are engaged in at the behest of people (e.g, secure email) but short-term coalitions between computers acting essentially on their own. As coalitions become the norm, the problem of combining different security policies and key management problems will become increasingly pressing issues. Some of these problems will go to the heart of our current paradigm since these coalitions will have neither a natural organizational nor a natural trust hierarchy that can be used for the basis of policy negotiation or for authentication.

Other problems will be more technical. Traditional key management problems (e.g., problems associated with key generation and key revocation) will take on new wrinkles and face problems with scaling. These key management problems will be exacerbated by the increased use of both broadcasting and point-to-multipoint communications. Add key management to the general problem of using encryption for high speed communications and the problem of maintaining key security in the presence of increasingly powerful (possibly, quantum) computers, and we are faced with a world where security challenges will be overwhelming.

2.2 Interaction of Security With Other Concerns

Despite this need for greater security and the increased problems in providing security, we will be forced to continue the current trend of trading off security with other concerns: limited money and limited expertise. For example, we will continue to face financial pressures that will force us to use commercial off the shelf (COTS) and legacy software. We will not have the resources to design custom software to handle every critical application; indeed, with the advent of ubiquitous computing, the distinction between "critical" and "non-critical" applications may become blurred. Thus we will still need COTS. Whether COTS will present us with a monolithic artifice where software is provided by a single vendor is an open issue which will have major security implications. Monolithic artifices reduce cost but increase the severity of security flaws. Likewise, we will no more be able to afford tomorrow to replace system software each time a system's environment changes, than we can afford to do so today. Thus we will still need legacy software. On top of this, limited human resources may well require us to perform system administration over a network from a single point, which will force us to balance security with the need to manage networks at a distance. Again, increases in efficiency must be balanced with decreases in security.

Since we expect the need for security to become more visible, but the security problem itself to become more difficult, it is likely that the computer industry will eventually be facing judicial pressure to take due care in system development. Indeed, we can already such a battle going on with respect to the Y2K problem. We do not believe that this will result in perfect security, for the reasons we gave above, but it should result in the development of best practice procedures to develop security components and architectures using these components that are suitable for protecting various types of information. In order for this to be feasible, it will be necessary to quantify the value of information assets, and thus we believe that point (1) mentioned in the introduction to this paper (the ability to quantify information assets) will become more important in the future.

It is also likely that since the pressure to use COTS and legacy software is not going to go away and since it is unclear how secure general-purpose software can be made, we will see an increasing interest in insertable security, that is security components that can be inserted into an insecure system to provide the necessary security functionality. Indeed, this is a trend that is already growing. Currently popular insertable security components include virus checkers and firewalls. Emerging insertable security components include intrusion detection systems, wrappers, and MLS components such as the NRL Pump [2] and the Starlight Interactive Link [1]. We will expect new applications for insertable security to unfold with the spread of new paradigms such as ubiquitous computing and temporary coalitions. Thus, we believe that points (2) and (3) from the introduction to this paper (the ability to define and implement the appropriate security properties) will still be important, but the focus will shift from the building of secure systems to the building of security components and techniques for securing systems with these components.

Ultimately, however, we must accept the fact that no protection mechanism will keep out the most determined attackers. The future, as a result, will see an increased emphasis on intrusion detection, system reconstitution in the face of intrusion, and, possibly, techniques to make intrusion potentially painful for the perpetrator. All this will require the development of command-and-control-like systems for making decisions about an information battlespace. Who will be controlling this battlespace (individual private enterprise, specialized private information protection agencies, law enforcement, defense departments, other?) is hard to predict.

3 Conclusion

The landscape of information security is going to be altered over the next several decades. While the requirements, pointed out in the first paragraph of this paper, for assessing the value of information and for protecting that information sufficiently will still exist, these will be tempered by a financial environment that will still produce great pressure to use insertable security devices in systems whose functionality will be COTS supplied. Limited human resources may lead to remote system administration. This, coupled with frequently forming and dissolving coalitions will exacerbate an already severe key management problem. The increased presence and connectivity of computers in the future will lead to more severe security, dependability, safety, and timeliness requirements that must be balanced with one another. Finally, we must graduate beyond the fortress mentality that still permeates much computer security research and move to a penetration-tolerant paradigm with a supporting command and control architecture.

References

[1] M. Anderson, C. North, J. Griffin, R. Milner, J. Yesberg, and K. Yiu, "Starlight: Interactive Link," *Proceedings of the 12th Annual Computer Security Applications Conference*, IEEE Computer Society Press, 1996.

[2] Myong H. Kang, Ira S. Moskowitz, and David C. Lee, "A Network Pump," *IEEE Transactions on Software Engineering*, Vol.22, No. 5, 1996.

[3] John McLean, "New Paradigms for High Assurance Software," *Proceedings of the 1992-1993 New Security Paradigms Workshop*, IEEE Computer Society Press, 1993.

[4] John McLean and Constance Heitmeyer, "High Assurance Computer Systems: A Research Agenda," in *America in the Age of Information*, National Science and Technology Council Committee on Information and Communications Forum, Bethesda, 1995.

[5] Mark Weiser, "How Computers Will be Used Differently in the Next Twenty Years," *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 1999.