Summer 1997: Survivability Architectures

Speakers:

John C. Knight, Professor of Computer Science at the University of Virginia

John McHugh, Professor of Computer Science at Portland State University

Panelists:

Mary Jane Bolling, Manager of Information Security, Capital One

Martin Myers, Manager of Contingency Planning, Capital One

Bruce Sommers, Director of Automation Resources, Federal Reserve Automation Services

Synopsis: Challenges Facing the National Computing Infrastructure

Speaker: John C. Knight

The national computing infrastructure is relied upon increasingly to carry out a variety of critical applications with the potential to affect life and property. Applications ranging from financial transactions of all scales to communications to the nationwide control of power and transport systems to wide-area medical information systems are being built.

Significant concerns have been raised about the possible effect of failure in these applications. Increased Business/Social Dependence leads to increasingly serious consequences in the event of failure. There is also concern over the risk of an attack on vital systems by those with malicious intent. Areas of vulnerability include: hardware failure, network failure, operator error, environmental stress, operations error, and software failure. Solutions to these vulnerabilities involve redundant components, backup services, and geographic diversity for systems. While there are many methods for dealing with hardware vulnerabilities, the same cannot be said for software. Improved methods for system development, as well as cooperation between software researchers/developers and end-users may aid in future software survivability.

"Our interest is in how to make these things really dependable, because we really depend on them." -Knight

Synopsis: Principles of Information Security

Speaker: John McHugh

Computers and public networks are increasingly used to hold sensitive financial information, and to transmit this information as well as to exchange items of value. The computer and network systems in use today evolved in an atmosphere where threats to information security were considered to be minimal, and were never intended to provide a high degree of protection for the information they hold or convey. A systematic approach that includes both good systems engineering and careful administration is needed to achieve and maintain a secure system. In design, careful threat analysis and hazard analysis of previous attacks or failures can result in the creation of appropriate countermeasures including cryptography, structural assurance and operational assurance. Ultimately survivability is a life cycle problem.

Roundtable Discussion

Panelists:

Mary Jane Bolling, Manager of Information Security, Capital One

Martin Myers, Manager of Contingency Planning, Capital One

Bruce Sommers, Director of Automation Resources, Federal Reserve Automation Services

Summary of Main Points

There is some question as to the level of requirements and regulations that should be legally imposed on software developers. For the software of critical systems, why are there no regulations that require technical expertise in development, just as there are very specific regulations to be followed in the construction of an airplane? Part of the reason is the difficulty of Government to be on the cutting edge of technology. This then begs the question of who should be responsible for developing industry regulations.

There is a certain Darwinian element to the evolution of industry standards, that can also be applied to software development rules. Currently there may be a slew of different standards and methods of development, but eventually most of those will fall out of use, and a relative few will form the acceptable method for developing survivable systems.

How will security be managed in the face of emerging technologies? An example is fraud detection software used by credit card companies. The software uses historical data of a customer's card use to compare against current card use data to determine the likelihood of fraud because the card has been stolen from the customer. This is a reactive security technique, as the credit card company only acts after a card has possibly been stolen. From a security standpoint, new reactive and proactive methods need to be explored, in order to better protect a system against failure or malicious attack.