TALES FROM THE DARKSIDE:
A Realistic View of Protecting an Organization

Panel Moderator: Ira Winkler, National Computer Security Association, Carlisle, PA
Panelists: Chris Kostick, Project Manager, SAIC
          Fred Rica, Senior Manager, Price Waterhouse
          John Ryan, President, Ryan Net Works

Panel Theme

Most of the research and literature in the security field deals with proposed or actual countermeasures that organizations can use to protect themselves against a variety of threats. Intuitively, most of these countermeasures make perfect sense and seem as if they should be implemented as quickly as possible. Unfortunately there is a cost, such as time, money, training, long term support, etc., in the implementation. Information and Computer Security managers are forced to balance limited resources with a need to protect their organizations from every perceivable threat.

The issue is how does the manager choose which countermeasures to implement given all the "must have" ones out there. This panel addresses these concerns from a unique perspective. The panel members are experts in penetration testing and/or incident response. Basically, we attack computers as an attacker would and we also repel real computer intrusions. This gives us specific knowledge as to what countermeasures are the most useful in preventing, detecting, and responding to real threats.

Surprisingly, many of the most valuable countermeasures are not even considered as options in a standard security program. For example, many organizations debate the need for increased firewall security, while ignoring the advanced password management features freely available on most computer systems. This panel will discuss case studies in detail and talk about the ways that incidents could have been prevented. The recommendations by the panelists are not just relevant, but cost effective as well, making them easy to implement.

Panelists and Their Issues

Ira Winkler

There are two problems that I believe to be the most prominent for allowing crimes to occur: 1) not updating computer systems on a regular basis, and 2) not making use of free and already available security tools. The failure to perform good systems administration is the root cause of almost all computer related intrusions. Good systems administration includes good user administration, watching for new vendor and CERT advisories, actually looking at audit logs, etc. Often, computer professionals fail to make use of the utilities they already have or can freely acquire. Most operating systems have the capability to enforce strong password security, to expire inactive accounts, to tightly control user access, etc. Free utilities can be downloaded from the Internet. These utilities include intrusion detection utilities, such as Tripwire and vulnerability scanners, such as COPS and SATAN.

Chris Kostick

Keeping an intruder out is difficult. The best you can usually hope for is to slow the intruder's progress. If you slow down an intruder enough, they typically give up that avenue of pursuit. If the intruder is not a real enemy, they may give up altogether. Most of the time the best way to keep out an intruder is often by the simplest means. From my observations and experiences with 'breaking in,' I could have been kept at bay for many of my jobs if:

1) Strong (sometimes any) authentication mechanisms were used at the perimeter access points -- i.e. dial-in.

2) The internal systems were not lax in the up keep of their security. Administrators who only perform base installs, fall behind in upgrades, and other things, are easy victims.

By enhancing these two simple aspects, a company can keep out many intruders. Of course, the more determined and experienced the intruder, the tighter the controls need to be. However, the above is a start that most institutions still do not even consider today.

Fred Rica

In over eight years of doing penetration testing, the single biggest lesson learned is that the weakest link will always compromise the strongest. In study after study, supposedly secure systems have been compromised due to the fact that surrounding systems were insecure, or that security was applied inconsistently throughout the network. In an age when the network is the computer, it becomes increasingly
important that all hosts on the network maintain a minimum acceptable level of security in order not to compromise other systems. Given the proliferation of Internet gateways, distributed processing systems, client/server computing, and dial-in connectivity, the exposures will only continue to grow. Constant monitoring is the only way to identify the weak links in the network. Monitoring includes not only producing and reviewing violation logs, but also implementing a program whereby security parameters and settings for each operating system on the network are defined and used throughout the organization. New hosts not in compliance with the security parameters should be identified using automated scanning tools. Scanning also needs to identify hosts whose security parameters may have changed since the last scan and have potentially introduced new vulnerabilities to the network. The fact that no one does this helps explain why our hacker teams never are caught. I will introduce a "model" of a secure network.

John Ryan

I want to lay the blame at the feet of the vendors. Why are there so many after market security products? It seems reasonable to expect IBM, Microsoft, Sun, and others, to produce an out-of-the-box, secure solution. So I propose the following title "The mathematical improbability of security - Why the market can never give us a secure network." Then you draw up some nice charts showing that because of dependency issues, changes in an object's security state, or other reasons, that you would have to spend more time testing say, sendmail, than writing it. This applies in spades to the OS as a hole (pun intended). The result is that Administrators have to pick up the slack and are ill prepared to do so since they, individually, have no more ability than the vendors' to test the product. The only economically viable solution is the one we are stuck with now. Release buggy code to the world and let them pick it apart. That way the vendor gets testing done on the hundreds of thousands of man hour scale required without having to pay for it. The poor systems administrator has to keep abreast as best he can, and good ones do a fair job of it, but novices have a hard time.