Panel Title: How can the Security Community Share Detailed Attack and Vulnerability Information?

Panel Chair: Peter Mell, NIST
Panelists: Matt Bishop, University of California at Davis
Gene Spafford, CERIAS
Kevin Ziese, Cisco

The Case for Sharing:

Computer attackers share attack and vulnerability (AV) information over the Internet while security companies and government agencies keep the information that they have to themselves. While organizations like CERT release AV information, the information helps administrators patch their systems but is not detailed enough for security research. The result is that security professionals must find their AV information from mailing lists, newsgroups, and attack script web sites. This process is extremely expensive because the AV information on the Internet is disorganized, distributed, incomplete, and often incorrect. The expense of gathering the AV information on the Internet inhibits research groups and small companies from using the Internet AV resources.

The future can be much brighter if the security community develops mechanisms by which to share their AV information. The virus checker industry shares all viruses that they discover which results in everyone's computer becoming resistant to all discovered viruses. Likewise, if the intrusion detection industry and the vulnerability scanner industry shared AV information then these products regardless of the vendor will detect all known attacks and vulnerabilities. This same sharing would benefit network penetration testers and software security evaluators. It would provide vendors timely information on when their products are vulnerable to attack and it would provide the security research community with a foundation for their research.

The Case against Sharing:

While the sharing of AV information would greatly aid the security community, little sharing is taking place. In the government world, this is largely the result of an instinctive impulse to hold onto dangerous information. In the corporate world, this is because corporations view sharing AV information as hurting the bottom line. In the security researcher's world, little sharing occurs because researchers want to keep a perceived advantage.

Those that attempt to share AV information are often hampered by not knowing what other's in the community need. Some researchers need attack scripts while others need vulnerability information. Some need general descriptions while others need detailed descriptions. Compounding the problem is that there exists no standard format by which to talk about AV information.

The Panel:

Members of the panel will discuss both sides of the AV sharing debate. The panelists will compare reasons to share AV information with reasons not to share AV information. The panel will end with the description of current AV sharing efforts and how the security community can get involved and benefit from these efforts.

Peter Mell: Why Share AV Information?

Peter Mell will lay a foundation for the panel members by answering the following to questions:

1. Why does the security community need to share detailed AV information?
2. Why are current Internet sources of AV information insufficient?

In answering these questions, he will outline what AV resources are available on the Internet and why these resources do not meet the needs of the security community.

Kevin Ziese: The Case for Corporate Sharing of AV Information

While the arguments that sharing will benefit the security community are convincing, the current corporate mindset is to not share. The rational is that sharing AV information will mean sharing valuable intellectual property and that will hurt the bottom line. Kevin Ziese will explain the reasoning behind this belief and why it is ill founded. He will lay a case for how corporations can share AV information while benefiting themselves and the general security community.

Gene Spafford: A Model for Sharing

Sharing within the security community can succeed only if all parties are convinced that no harm will come of it. Because of this, we need a sharing model structured so that it mitigates the security community’s natural fear of sharing. Gene Spafford will present such a model and describe why it suits the needs of corporations, government agencies, and researchers.

Matt Bishop: Alternate Sharing Models

Matt Bishop will discuss other sharing models, and contrast them to Gene Spafford's model. He will present useful results that could come from widespread sharing in the commercial, government, and research worlds.