Reminder

Workshop on the Active Response Continuum to Computer Network Attacks

March 15, 2005 8:30am to 5:00pm
March 16, 2005 8:30am to 5:00pm
March 17, 2005 8:30am to 3:30pm

George Mason University, Fairfax Campus
Mason Hall D3A&B (located right across the Atrium from the Boardroom).
http://coyote.gmu.edu/map/maphtml/mh.html

Would an active response to a major cyber attack quickly stop the attack and contain damage, or would it reverberate throughout the Internet causing collateral damage that would challenge our ethical, diplomatic, legal, and military standing around the world?

As an expert in the field of cyber security and/or cyber law your input is requested at a workshop to address actions that fall along the Active Response Continuum. The workshop will focus on the problems inherent in responding to large and complex computer network attacks, and to help frame a future that maximizes response to such attacks on networks supporting critical national infrastructure, while at the same time minimizing collateral damage, legal risk, reputational damage, etc. These include, but are not limited to:

- Meaningful communication between organizations' Incident Response Teams that results in rapid and effective response,
- Differentials in incident response resources and skills, and the effect of these differentials on the speed and effectiveness of incident response,
- Meaningful communication between federal law enforcement, the military, and intelligence community agencies,
- The adequacy of state, federal, and international law enforcement to respond to all computer network attacks,
• The risks faced by victims of computer network attack when choosing to respond on their own, beyond their network borders,

• The ethical implications of active response actions,

• The available tools for distributed, coordinated incident response, and the gaps that need to be addressed in order to improve the landscape of incident response,

• Areas of research and development in academia and industry that will contribute to a more effective national response to major cyber attack,

• The risks faced by the nation as a result of failures to respond to a large and complex computer network attack or in addressing collateral damage caused by the range of responses,

The workshop dialogue will focus on problems in the status quo related to today's attack scenarios, and explore various proposals for improving the situation to help find a way to migrate to a trustworthy computer network defense landscape. Your contribution to this discussion is important!

The group we are assembling represents some of the best minds in their fields when it comes to critical electronic infrastructure protection, the law, and private and public cyber security practitioners. The synergy across disciplines can help identify promising ways to move the nation forward in its computer network defense posture. These conversations, which will be captured in a book, will work towards consensus and concrete proposals that can be made to policy makers and decision makers within organizations to move us towards a more effective defensive posture. Elsevier has agreed to publish the proceedings, and we need all participants to commit to writing, or at least reviewing, part of a chapter between the end of the workshop and April 15.

We have permission from Hossein Bidgoli, editor of the forthcoming “Handbook on Information Security” to allow participants in the workshop to read the final draft of an article, “Active Response to Computer Intrusions,” by David Dittrich and Kenneth E. Himma to . (We must ask that you please do not redistribute this article as copyrights are reserved by John Wiley & Sons, Inc.) This Handbook article, directions, hotel information, panelists and subject area assignments, draft daily schedule, and other information important to participants will be updated regularly on this web page: http://staff.washington.edu/dittrich/arc/workshop/

We look forward to your attendance and to a productive and lively discussion!

Dave Dittrich, Program Chair