Workshop on the
Active Response Continuum to
Computer Network Attacks

Introduction

Responses by victims to cyber attacks fall onto a continuum of actions from less to more intrusive, less to more risky, and less to more detectable. They can be ethical or legal at best, perhaps be illegal and represent computer trespass, or at worst may not be clearly legal or illegal. What is more, a future terrorist attack may target computer networks and start as a large number of separate intrusions in the private sector, but later require a military response. The 9/11 Commission's report describes the complexities of response yet barely even mentions cyber attacks or response requirements.

In 1998, the President's Council on Critical Infrastructure Protection published a report that predicted an increase in the amount of computer crime as well as pressure on federal law enforcement and private sector incident responders. Two authors of that report wrote a paper, suggesting that: a coordinated effort to clarify the roles of the public and private sectors with respect to investigations and responsive legal action is warranted.

In 2004, the British All Party Internet Group confirmed these predictions in the PCCIP report: the online gambling industry in the UK had paid out tens of millions of dollars in extortion demands accompanied by massive distributed denial of service attacks. They called for changes in Britain's Computer Misuse Act to create a group of professionals able to assist victims in a way that also supports the needs of law enforcement.

Also in 2004, Europe's Lycos (a search engine company) announced their "Make Love, Not Spam" campaign, which involved a screen saver designed to "slow down" suspected spam related sites. Hundreds of thousands of users willingly downloaded and installed the screen saver to participate. While justified as an effort to change the cost model of spamming, the program was quickly withdrawn when it was found to be disabling sites with what was effectively a coordinated, distributed denial of service attack.

We urgently need to come up with technical and policy guidelines to counter the growing criminal threat in cyberspace and better respond to any future attacks on networked critical infrastructures.

On behalf of the Program Committee, I would like to invite you to participate in a workshop discussing these and other issues of the Active Response Continuum to Computer Network Attacks. More details on this workshop can be found below.

Participants will not be automatically funded to attend this workshop as our grant is limited; however, those who need support and who commit to authoring a document on the discussion for one of the topic areas will be given first priority for support. One
desired outcome of this workshop will be a book reporting on the discussions and providing high-level recommendations to policy makers.

Please reply at your earliest possible convenience. As we are trying to keep the size of this group to a minimum, and wish to include people with established backgrounds in the subject matter who commit to contributing, please do not forward this invitation. However, though we have only a few more openings, you are invited to send names of proposed candidates to ditrich@u.washington.edu and the Program Committee will consider them.

Sincerely,

David Dittrich
Center for Information Assurance and Cybersecurity
University of Washington

**Date/time**
March 15 to March 17, 2005, from 8:30am to 5:00pm.

**Goal**
This workshop will involve various stakeholders from a range of fields in a facilitated discussion of the current issues and the ramifications of different organizational approaches to active responses to advanced and large-scale computer attacks. The intent is to identify and propose workable solutions that can be implemented before large-scale cyber attacks on national critical infrastructures occur.

**Participants**
We will bring together 30-40 experts representing a variety of perspectives on the Active Response Continuum, including research scientists, ethicists, military and law enforcement personnel, and members of the intelligence community. Thus the participants will span the spectrum from the private sector to government policy makers.

**Location**
The workshop will be held on the Fairfax campus of George Mason University in Fairfax VA at Mason Hall D3A&B (located right across the Atrium from the Boardroom). Directions can be found at http://coyote.gmu.edu/map/maphtml/mh.html

**Program**
Participants will examine the ethical and legal implications of active response actions, begin relating active response concepts to information warfare or cyber-warfare, and explore and accentuate the gaps and overlaps between the roles of private and public sector organizations, law enforcement, and the military and intelligence communities. The deliberations are expected to result in the identification of areas needing research,
Governmental and private sector active responders will be able to compare and contrast how they may respond. Ethics experts will discuss the issues surrounding active responses and obtain input from those who deal with developing and possibly deploying such responses on a practical level. The combination of technical, legal, and ethical expertise will allow discussion to focus on outcomes in terms of what can, should, and should not be done.

Topics, based on the third Agora Active Defense workshop held in Seattle, WA, on September 12, 2003 (see http://staff.washington.edu/dittrich/ad/WorkshopSummary.doc) will include:

- Motivations and Goals of active response actions
- Definitions of the Active Response Continuum
- Ethics of active responses
- Domestic (United States) legal issues of active responses
- International legal issues of active responses
- Military and intelligence community perspectives of active responses
- Homeland Security perspective of active responses
- Models for public/private partnerships supporting active responses

The most important outcome will be in informing policy and lawmakers of mechanisms for public/private partnerships; this will be collected and published in a book – the possible outline of which is appended to this invitation. Prior to attending the workshop, participants are asked to read and comment on the proposed chapters and contents of the book and state to which two chapters they expect to contribute material. Those willing to make presentations are asked to send possible slides or commentary to all in the hopes that we shall be well prepared prior to the start of the workshop.

(Support for this workshop is provided by George Mason University and Cisco Systems' Critical Infrastructure Assurance Group, and is being organized in conjunction with the University of Washington’s Center for Information Assurance and Cybersecurity.)