CSEP590tu Whitepaper Project Proposal: "Offense vs. Defense"

Bhavjit Walha, Robert Anderson, Brian Lum, Josefina Valdez

November 11, 2005

1 Proposal

Recent years have seen a proliferation of attacks against corporate networks and individual computers. These include fast-spreading internet worms with malicious payloads; wide-scale distributed denial of service attacks; and penetration attacks designed to steal sensitive personal and corporate information. In addition, nuisances like spam (unsolicited e-mail) are a vexing problem for networks and end users alike, as they consume valuable bandwidth; enervate business productivity; and often act as carriers for internet viruses and vehicles for hoaxes, scams and deceptive phishing solicitations. Traditional ways of protecting against such attacks have focused on passive defensive approaches ranging from firewalls, anti-virus and anti-spyware software, SYN cookies, spam filters and methods like auto-disconnecting servers in the event of attacks. Many of these methods have met with only limited success in thwarting attackers; DDoS attacks, for example, are notoriously difficult to defend against. And, a purely defensive approach does nothing to discourage violators from repeating the attacks elsewhere. Many attackers "troll" for vulnerabilities, knowing that there is little risk of reprisal.

These limitations have given rise to proposals for more reactive and offensive "counter-strike" approaches to cyber-security. Some corporate IT specialists and security researchers feel that, rather than remaining a silent spectator when faced with a cyber-attack, the owners of besieged networks should retaliate. It is believed that "vigilante" measures—and specifically the presence of a ubiquitous and potent deterrent—will change the cyber-security landscape, reducing the frequency of attacks and making corporations, governments and individuals safer.

We propose to discuss some of the possible choices of countermeasures. We will examine the reasons why people want to combine offensive maneuvers with defense ones when it comes to cyber-security. We plan to look into the technical feasibility, popularity and effectiveness of these countermeasures.

Since most of these attacks involve throttling user bandwidth, dropping user traffic or infiltrating and modifying non-owned machines, counterattacking organizations risk the wrath of courts large and small, around the globe. At the same time, the perceived inefficacy of the legal patchwork enforced by these courts has led to a surging interest in counterattack technology. The legal issues are further complicated by the anonymity afforded by the internet, the multiplicity of laws and jurisdictions, and the ability of attackers and counterattacks to wage war in multiple disparate legal jurisdictions simultaneously.

We will gauge the intensity of the counter attack appropriate for an attack of a given scale. We will examine the positive and negative consequences of performing counterattacks,

including the effect on the cyber-ecosystem of the introduction of a deterrent effect, the likelihood of an "arms escalation", and the consequences of mistaking the identity of an attacker.

We also plan to discuss some examples of offensive countermeasures which have been deployed, or are available for deployment as technology solutions in the marketplace today. Thus we plan to discuss the implications of these counter-attacks – both technical and legal. We plan to conclude with an analysis of any policy changes which may simplify the issues concerning these counter-attacks and possibly address the need for them.

2 Principal Authors

The following is our proposed division of research and work on the report. Please note that this is only a rough guideline and this division may evolve as we uncover more material on a particular section or find a particular field lacking.

Bhavjit S Walha(UCSD) will introduce the various 'offense' alternatives and discuss their need and feasibility from a technical view point. **Rob Anderson** (UW) will analyze the wider impacts and social implications of these techniques and elaborate on the various practical and legal issues they raise. **Brian Lum** (UCSD) will present a detailed analysis of specific conter-attacks which have been deployed by government and non-government agencies and discuss their outfall. Finally, **Josefina Valdez**(Berkeley) will talk about where the current law stands and what policy changes might be needed to remove ambiguities raised by this relatively new form of cyber-security.

References

[1] Frank Castaneda, Emre Can Sezer, and Jun Xu. Worm vs. worm: preliminary study of an active counter-attack mechanism. In *WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode*, pages 83–93, New York, NY, USA, 2004. ACM Press.

[2] Dave Dittrich. Active response continuum research project, nov 2005. `http://staff.washington.edu/dittrich/arc/`.

[3] Timothy M. Mullen. Defending your right to defend: Considerations of an automated strike-back technology. `http://www.hammerofgod.com/strikeback.txt`, oct 2002.