Chapter 6
Standing Your Ground:
Current and Future Challenges
in Cyber Defense

Barry V. W. Irwin
Rhodes University, South Africa

ABSTRACT

This chapter explores the challenges facing those involved in cyber defense at a national, organizational, and individual level. As the global economy grows more dependent on the Internet and connected infrastructure, the risk and impact of attack grows. A long-standing response to attacks of various kinds conducted on the Internet has been to filter traffic but not to respond. In some cases, reactive action is taken, but even where attribution is possible, prosecution is rare. In recent months, several countries have stated their policy of military response where they feel that their national infrastructure is threatened. The risk to organizations, civilian populations, and individuals is discussed in the case of such militant response or retaliation. The chapter further considers aspects such as reputation, neutrality, and the concept of Internet “kill switches.”

INTRODUCTION

The realization of cyberwarfare, and cyber attacks has increased since the significant events of May 2007, in what has become termed the Estonian Incident. Denial of Service attacks affecting nation states have subsequently occurred on a number of occasions. In recent months the discovery of the Flame malware has raised more questions in terms of the offensive capability of nation states, with this software exhibiting previously unprecedented sophistication. At the opposing end of the spectrum individuals and organizations often bear the brunt of malicious online activity. This chapter considers the challenges that emerging Internet states need to consider as part of their future development and planning. An integral part of this is to consider the approach taken when individuals and organizations detect and need to decide on an appropriate response to such attacks.

Section 2 briefly explores the evolution of Security on the Internet, considering the substantial changes that have taken place. This is followed in Section 3 by a discussion of current challenges faced in cyber defense. The future challenges from the perspective of the author are explored in Section 4.

DOI: 10.4018/978-1-4666-6158-5.ch006
EVOLUTION OF SECURITY

The Internet has transitioned from its largely academic roots, where the principles of openness and data sharing were paramount to a global network, vital to global commerce and communication. Possibly as a factor of the rapid growth, legal systems globally have failed to keep up, and the ease with which actions may be performed on or against system located in areas geographically distant to the instigator, have made the enforcement of traditional laws difficult. The question of legal jurisdiction in such cross border incidents greatly complicates the resolution from a law enforcement perspective. The long standing principle employed by many network administrators has been to protect the border and implement appropriate technologies to manage the communications of what has become an increasingly hostile, exterior network to those hosts within their organization. This thin veil of security, aptly described by Bill Cheswick as a “sort of crunchy shell around a soft, chewy center” (Cheswick, 1990), has probably never been more apt. The initial approach taken with the widespread adoption of firewall systems was to block the known bad (blacklisting), which has transitioned to largely block everything except what we need (whitelisting). In both approaches, the majority of organizations still focus their defensive efforts outwards. The act of blocking itself takes many forms. Considering the case of the traditional IP Firewall, a block is often differentiated between two states: Deny: in which IP datagrams matching the rule are discarded, and Block: in which prior to the discard a protocol relevant error message is sent indicating this has occurred.

In the case of blocking, the RFC specifications for the ICMP protocol provide for fairly specific signaling as to why a packet may have been dropped (IANA, 2008) (which may not have been only due to security reasons). A similar approach is taken when dealing with email, where spam is either discarded (preferably pre-acceptance) or a notification of the message having been quarantined or tagged is sent.

In recent years many organizations have started to consider the implications of focusing defensive resources inwards on their networks. While in many ways this has been primarily driven by technologies such as DLP (Data Loss/Leak Prevention), a secondary driver has been seen to be the mitigation of risk and liability. Considering the scenario of an administrator detecting repeated port scanning activity from a source, the response has usually consisted of a number of distinct phases.

- **Attribution**: The source(s) are identified, initially as an IP address, and then resolved using various methods to a source organization. This organization may be an endpoint, or in the case of consumer Internet access, an Internet service provider.
- **Action**: The identified sources are blocked, usually at the firewall or routing infrastructure at the point where the administrator has control.
- **Complaint**: A notification of the malicious activity is sent to the responsible organization, usually as an email directed to the abuse@ email address, which is required to exist as per RFC 2142 (Crocker, 1997). This is not always successful, as the addresses often do not exist or no response is received. An escalation path is typically followed with the provider of network access to that organization.

In severe cases such as Denial of Service (DoS) attacks an organization may need to liaise with their upstream network provider(s) in order to perform mitigation actions as close to the ingress point of the traffic as possible. In some circumstances, Network Providers may de-announce targeted network address blocks, resulting in all traffic destined for these ranges of addresses be-
Related Content

Cloak and Dagger: Man-In-The-Middle and Other Insidious Attacks
[www.igi-global.com/chapter/cloak-dagger-man-middle-other/49506?camid=4v1a](www.igi-global.com/chapter/cloak-dagger-man-middle-other/49506?camid=4v1a)

Intrusion Detection Algorithm for MANET
[www.igi-global.com/chapter/intrusion-detection-algorithm-manet/72744?camid=4v1a](www.igi-global.com/chapter/intrusion-detection-algorithm-manet/72744?camid=4v1a)

Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University
[www.igi-global.com/chapter/securing-learning-systems/23214?camid=4v1a](www.igi-global.com/chapter/securing-learning-systems/23214?camid=4v1a)

Applied Cryptography for Security and Privacy in Wireless Sensor Networks
[www.igi-global.com/article/applied-cryptography-security-privacy-wireless/37581?camid=4v1a](www.igi-global.com/article/applied-cryptography-security-privacy-wireless/37581?camid=4v1a)