Possibility Theory in Protecting National Information Infrastructure

Richard Baskerville, Georgia State University, USA
Victor Portougal, University of Auckland, New Zealand

ABSTRACT

Possibility theory is an alternative to probability theory as a basis for security management in settings where information resources are elements of national information infrastructure. Probability theory is founded on the assumption that one cannot totally rule out an intrusion. Possibility theory operates under a contrasting assumption. While persistent, well-supported, and highly professional intrusion attacks will have a higher probability of success, operating instead against the possibility of intrusion places defenders in a theoretical framework more suitable for high-stakes protection. The purpose of this chapter is to introduce this alternative quantitative approach to information security evaluation. It is suitable for information resources that are potential targets of intensive professional attacks. This approach operates from the recognition that information resource security is only an opinion of officials responsible for security.
INTRODUCTION

Probability theory is the most commonly used theoretical base in the process of risk analysis for information systems security. When dealing with multiple intrusion events that justify using probability theory models, certain assumptions are made about distributions of the intruder population and of the intrusion events. For example, commerce settings assume that the intruder population is distributed normally, while the intrusion events have a Poisson distribution (Baskerville & Portougal, 2000). These assumptions are not valid in security settings where the intrusions are rare events; intruders are very highly skilled and intrusion events persistent, that is, attacks that draw on infinite intrusion resources. Such security settings include those where national information infrastructures become enveloped in a battle space subject to information warfare attacks.

Information warfare and the defense of national information infrastructures have become a concern in national defense and law enforcement policies. Information warfare consists of both digital information operations and perception management. Perception management regards information operations that aim to affect the perception of others in order to influence their emotions, reasoning, decisions, and ultimately actions (Denning, 1999). Perception management is closely related to psychological operations (PSYOPS) that influence behavior through fear, desire, logic, and other mental factors. It also is closely associated with propaganda, the spreading of ideas, information, or rumor for the purpose of helping an institution, a cause, or a person or to damage an opposing cause.

The scope of digital information warfare includes the protection and compromise of computer-based technology that bears information. For the purposes of this chapter, we will exclude perception management using a mass communications media and the underlying perception management basis for shaping information content in digital media with lies, distortions, denouncements, harassment, advertising, and censorship. Our focus is mainly on disruptive offensive information operations intended to interfere with proper functioning of computers and networks (Baskerville, 2004).

We are more concerned with how electronic commerce slips into the broader (real) battle space. This slip can occur in at least three ways. (1) Most prevalent are the possible attacks on national critical infrastructures. A battlefield opponent gains advantage when an enemy’s energy supplies, finances, communications, and transportation systems (including both shipment of goods and passengers) are disrupted in such a way as to interfere with their ability to sustain combat operations. (2) The ability to share critical attack information among businesses engaged in such infrastructures forms a second target arena in which information warfare attacks may be levied against electronic commerce. (3) Further, businesses that are developing militarily useful systems, such