Chapter 36
Flow-Graph and Markovian Methods for Cyber Security Analysis

Kouroush Jenab
Embry-Riddle Aeronautical University, USA

Sam Khoury
Athens State University, USA

Kim LaFevor
Athens State University, USA

ABSTRACT

A flow-graph depicts the interrelationships among cyber security and security threats/incidents (i.e., internal, external, and accidental). Using a flow-graph, the manner in which security threats may affect systems can be investigated. This paper reports analytical approaches to analyze time to security threats and probability of security threat occurrence. Considering embedded threat detection functions in a safe-guard unit, the proposed approaches use the flow-graph concept, and Markovian method to calculate time to security threat occurrence and its probability. The threat detection functions are featured by incident detection and recovery mechanisms. The results of this study can be used by all parties (public and private sector organizations, service providers, IT, and insurance companies) to better deal with cyber security issues with respect to utilizing technology, investment, and insurance. An illustrative example is demonstrated to present the application of the approach.

1. INTRODUCTION

The term "cyber security" refers to three things: 1) a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware devices and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security, 2) the degree of

DOI: 10.4018/978-1-5225-5634-3.ch036

protection resulting from the application of these activities and measures, and 3) the associated field of professional endeavor, including research and analysis, aimed at implementing those activities and improving their quality. Cyber security problems exist in Grid/Power System/Distribution, Networks/ Telecom, Computers, Organizations, Information Systems, Industrial Controls, Transportation, Energy, and Healthcare Systems.

In industrial cyber security, the security risk is a function of both the Likelihood of Successful Attack (LAS) against an asset and the Consequence (C) of such an attack. The consequence of a security threat can be classified as financial losses, acute health effects, or environmental impacts. Estimating the LAS is far more difficult. It is a function of three additional variables:

- **Threat (T):** Any indication, circumstance, or event with the potential to cause the loss of or damage to an asset.
- **Vulnerabilities (V):** Any weakness that can be exploited by an adversary to gain access to an asset.
- **Target Attractiveness (AT): An** estimate of the value of a target to an adversary.

These aforementioned terms are more difficult to estimate, particularly with respect to cyber security. In detail, threats to cyber security include the following aspects resulting from data hierarchy as data is transformed into security situation awareness (Figure 1):

- Malware attack with Social Engineering Tactics
- SPAM
- Denial of Service (DoS)
- Phishing and Pharming
- Botnets
- Instant Messaging (IM) attack
- Mobile and Wireless attack
- Root kits
- Web Application attack
- Hacking with Google

As shown in Figure 1, incidents can results in intrusions and cyber security problems. Chou et al. (1999) explored the security problems in an organization that resulted in proposing security frameworks for the cyberspace environment. They also discussed privacy training for users, and the need for procedures and policies for improving cyber security.

Palfrey (2000) studied the interception/surveillance response in the context of other attempts to regulate crime in cyberspace. Napoleon (2007) discussed the needs of modern society for information systems for commerce, communication, and defense. Therefore, security threats to the systems would potentially cost society.

Murphey (2011) described Cyber Anarchism, which means the well-organized and free-wheeling world community of computer hackers. Tsai (2011) reports several probabilistic models with application in social media based on media attributes and classification frameworks. Ling and Masao (2011) introduced potential hazards associated with smart grids that were referred to as a triggering factor to