

Flow-Graph and Markovian Methods for Cyber Security Analysis

Kouroush Jenab, Faculty of College of Aeronautics, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA

Sam Khoury, Faculty of College of Business, Athens State University, Athens, AL, USA

Kim LaFavor, Athens State University, Athens, AL, 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.

KEYWORDS

Block Diagram, Flow-Graph, Incident Detection, Threat Detection

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 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.

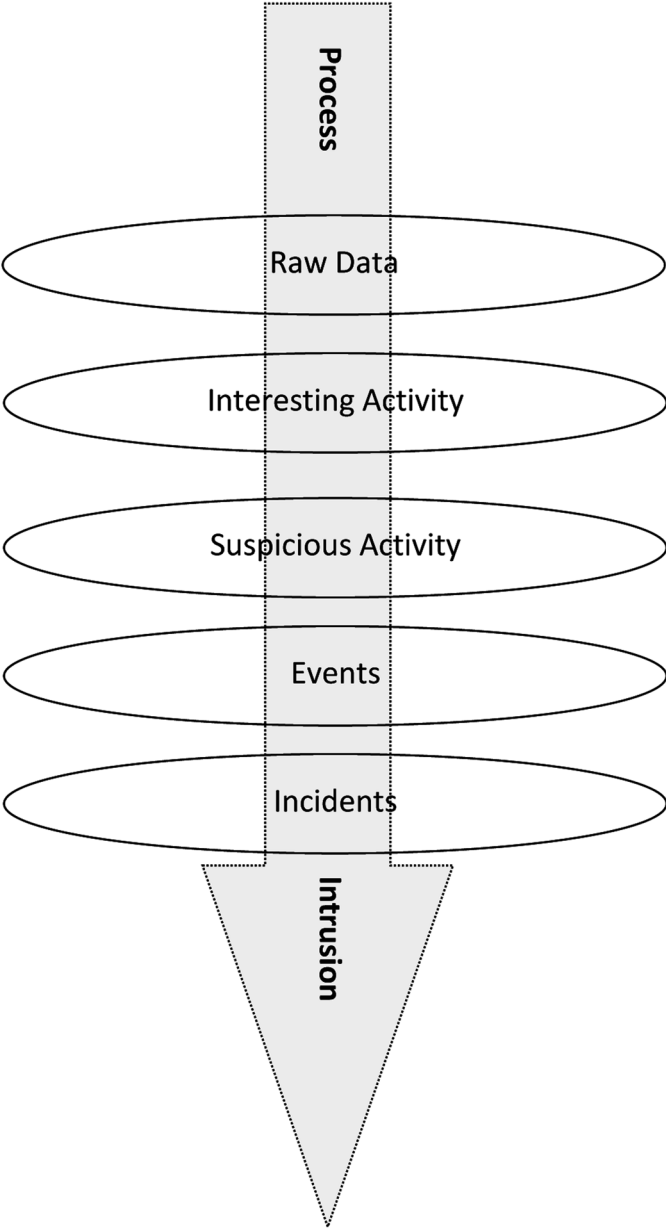
In industrial cyber security, the security risk is a function of both the Likelihood of Successful Attack (LAS) against an asset and the Consequence (C) of such an attack. The consequence of a security threat can be classified as financial losses, acute health effects, or environmental impacts. Estimating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

Figure 1. Security situation awareness



24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/flow-graph-and-markovian-methods-for-cyber-security-analysis/149442

Related Content

IT and Enterprise Architecture in US Public Sector Reform: Issues and Recommendations

Terry F. Buss, Anna Shillabeer and Anna Shillabeer (2012). *Enterprise Architecture for Connected E-Government: Practices and Innovations* (pp. 412-440).

www.irma-international.org/chapter/enterprise-architecture-public-sector-reform/67033

State of the Art Solutions in Enterprise Interoperability

Silke Balzert, Thomas Burkhart, Dirk Werth, Michal Laclavík, Martin Šeleng, Nikolay Mehandjiev, Martin Carpenter and Iain Duncan Stalker (2010). *Enterprise Information Systems for Business Integration in SMEs: Technological, Organizational, and Social Dimensions* (pp. 201-229).

www.irma-international.org/chapter/state-art-solutions-enterprise-interoperability/38200

Principles and Experiences: Designing and Building Enterprise Information Systems

Mehmet S. Aktas (2011). *Enterprise Information Systems: Concepts, Methodologies, Tools and Applications* (pp. 1-20).

www.irma-international.org/chapter/principles-experiences-designing-building-enterprise/48530

A BPM Framework for NPD Process Knowledge Management

Antonio Caforio, Angelo Corallo and Angelo Dimartino (2013). *Enterprise Business Modeling, Optimization Techniques, and Flexible Information Systems* (pp. 127-140).

www.irma-international.org/chapter/bpm-framework-npd-process-knowledge/77965

A Fast-Moving Consumer Goods Company and Business Intelligence Strategy Development

Paul Hawking and Carmine Sellitto (2017). *International Journal of Enterprise Information Systems* (pp. 22-33).

www.irma-international.org/article/a-fast-moving-consumer-goods-company-and-business-intelligence-strategy-development/182431