Chapter 54
Security Visualization Extended Review Issues, Classifications, Validation Methods, Trends, Extensions

Ferda Özdemir Sönmez
Middle East Technical University, Turkey

Banu Günel
Middle East Technical University, Turkey

ABSTRACT

Security visualization has been an issue, and it continues to grow in many directions. In order to give sufficient security visualization designs, information both in many different aspects of visualization techniques and the security problems is required. More beneficial designs depend on decisions that include use cases covering security artifacts and business requirements of the organizations, correct and optimal use of data sources, and selection of proper display types. To be able to see the big picture, the designers should be aware of available data types, possible use cases and different styles of displays. In this chapter, these properties of a large set of earlier security visualization work have been depicted and classified using both textual and graphical ways. This work also contains information related to trending topics of the domain, ways of user interaction, evaluation, and validation techniques that are commonly used for the security visualization designs.

INTRODUCTION

The actions threatening information security have a variety of categories. For example, "web based attacks" is a name given to express a set of harmful activities targeting web-based information systems. The occurrence rates of these harmful events can be gathered from the numeric information provided by vendors of information security protection systems. Symantec programs blocked 190000, 464100

DOI: 10.4018/978-1-7998-7705-9.ch054

and 568700 “web-based attacks” in 2011, 2012 and 2013, respectively, showing a 23% increase between 2012 and 2013 (Symantec, 2014). This single example shows that there is a trend of increase in the occurrence of harmful events threatening information security. The number of actions is not increasing alone; indeed, the type of threats, their sophistication levels and impacts are also getting higher by time. This makes the field of information security very important. A single computing device without any network connections can still have security vulnerabilities. However, as the computing devices get connected to each other and to the Internet, the level of threats increases exponentially. These threats may be unintentional or intentional.

In order to detect and prevent these intentional or unintentional actions, systems such as intrusion detection, intrusion prevention and firewalls are commonly used in enterprises. The security analysts investigate the outputs of these systems either in real time or in a delayed manner. The main source of information provided by these systems is the log files. In order to warn against momentary or future events, some of the IDS systems or firewalls include some visual or audio alert systems.

Although the alternatives and capabilities of protection systems are getting better, there are problems with the usability of these systems. The main source of problems affecting the usability of these systems is the size of the data they process. The log files are often too large to be investigated manually. The frequency of alerts is often high which overwhelms the analysts. Each alert may not point out a correct situation. This results in omissions or ignorance in the long term. Numerous tools and programs are being used in order to overcome security vulnerabilities of the organizations. However, the outputs of these programs are rarely understood clearly.

Security visualization is the act of using information visualization techniques to ease the decision-making process for security analysts. It provides situational awareness. It offers new representations of security data to increase the comprehension and provide an efficient processing of the data. In general, there is a tendency to use the same type of display types for the same use cases, or the same type of display types for the data in similar formats. While this is the result of a consolidated learning in most cases, it may be useful to find alternative combinations of these use cases, display types and data attributes for novel security visualization designs.

To this end, while introducing the selected existing work in this chapter, these works are classified according to display types, use cases and data sources. The objective of this chapter is to classify the existing work which are similar to each other, and by doing so to find out gaps such as data types which are seldomly used for security visualization purposes. In this way, it is expected to find new ways of combining data coming from multiple sources and display types commonly used for some particular scenarios which may also be suitable for some other scenarios. This extended summary of security visualization designs may help researchers who want to solve security visualization problems by applying novel designs and those who investigate current status and trends in the security visualization domain.

The reviews written so far in the security visualization domain focus on a limited number of works. Survey results that depend on few designs can provide only an incomplete perspective of the domain information. In this chapter, the number of designs that are examined in detail is 79. This examination results in a detailed perspective of the security visualization domain. The contribution of this work to the existing literature can be summarized as follows:

- An extended summary of the existing work is given which may help novice researchers find out what has been done so far.