Ontological Framework for Classification of Web Security Attacks

Sarita Sharma¹, Saurabh Ranjan Srivastava²

Department of computer science
SKIT, Jaipur, INDIA
Email: saritasharma1606@gmail.com, saurabhranjansrivastava@gmail.com

Abstract

This paper presents an analytical survey of web security threats using ontological representation. Despite existing methodologies in the field, most threat analysis engineers are not sufficiently trained to define web security threats which ultimately lead to poor encounter mechanisms and eventually loss of resources. This is due to a considerable lack of security knowledge. Some ontologies have been proposed, but a gap still exists between the two fields of threat analysis engineering and their ontological representation. This ontology is focused on classification of web security threats. For evaluation of a security threat, it evaluates parameters as threat type, its origin, and corresponding history of the threat. We expect this work to support in understanding security threats and designing more robust and reliable counter mechanisms.

1 INTRODUCTION

Computers are an integral part of every one's life and so are the web security threats. An optimum level of security to ensure safe and trusted communication of information services between various networks is crucial. Collection and organization of concepts and associations is a challenging process. Similarly, knowledge engineering regarding the design and scaling of a security ontology is a daunting task. A security ontology can act as a standard platform for evaluating and detecting security flaws as well attacks through its comprehensive vocabulary to interpret the available system resources with consistent semantics.

2 THREAT TYPES

2.1 Malware

Programs categorized as Malware [5] pose a significant security risk to the user's system and/or information. Types of programs in the Malware category include viruses, worms and trojans, among other threats. These threats can perform harmful actions such as stealing personal or program data, secretly manipulating the device or installed programs, or completely blocking the user.

Types of Malware

a) Virus: Integrate its own code into program or data files and spreads by integrating itself into more files each time an affected file is run.
b) Worm: Uses computer or network resources to make complete copies of itself and distribute them to other victims. May include code or other malware to damage both the system and the network.

Worms can also be typed more specifically based on the kind of network they use to spread:

- Net-Worm: over a local network or the Internet
- Email-Worm: via emails, either contained in the email itself or as file attachments
- P2P-Worm: in files sent over peer-to-peer (P2P0 networks
- IM-Worm: over instant messaging (IM) networks
- IRC-Worm: over Internet Relay Chat (IRC) channels
- Bluetooth-Worm: via Bluetooth broadcasting
c) Rootkit: Hides itself or other files from the device's security programs and can be used by remote users to manipulate the device
d) Trojan: Uses misdirection, misinformation, omission or outright fraud to trick the user into installing or running it, so that it can perform potentially unwanted harmful actions. It does not replicate.
e) Backdoor: Allows remote users to manipulate a program, computer or network.
f) Rogue: Uses high-pressure, or misleading messaging or outright fraud to pressure users into purchasing antivirus software that may not perform as claimed.
g) Exploit: Takes advantage of vulnerability in a program or operating system to gain access or perform actions beyond what is normally permitted.
h) Packed: Compressed to a smaller size using a packer program known to be used by other malware.
i) Constructor: A utility program send to construct malware.
2.2 Spyware
Programs categorized as Spyware [5] introduce a security risk that may affect the user’s personal data. Types of programs in the Spyware category include trackware and adware. These programs may offer a useful service in exchange for being allowed to gather information from or about the user.

Types of Spyware

a) Spyware: Collects information about the user’s web browsing behavior or preferred applications the data collected may be stored locally or sent out.
b) Trackware: Allows a third party to identify the user or their device, usually with a unique identifier. The most common trackware is tracking cookies.
c) Adware: Delivers advertising content, either in the web browser, on a PC’s Desktop or within an application.

2.3 Riskware
Programs categorized as Riskware [5] are considered safe when used by an authorized person in an appropriate situation. If misused, or used by an attacker, the program may be a security risk.

Types of Riskware

a) Monitoring-Tool

As per Kaspersky report 2012 these are the most active software associated with online threats, the following top 10 account for 95% of all web attacks [3]:

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Number of attacks</th>
<th>% of all attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Malicious URL</td>
<td>1,393,829,795</td>
<td>87.36</td>
</tr>
<tr>
<td>2</td>
<td>Trojan.Script.Iframer</td>
<td>58,279,262</td>
<td>3.65</td>
</tr>
<tr>
<td>3</td>
<td>Trojan.Script.Generic</td>
<td>38,948,140</td>
<td>2.44</td>
</tr>
<tr>
<td>4</td>
<td>Trojan.Win32.Generic</td>
<td>5,670,627</td>
<td>0.36</td>
</tr>
<tr>
<td>5</td>
<td>Trojan-Downloader.Script.Generic</td>
<td>4,695,210</td>
<td>0.29</td>
</tr>
<tr>
<td>6</td>
<td>Exploit.Script.Blocker</td>
<td>4,557,284</td>
<td>0.29</td>
</tr>
<tr>
<td>7</td>
<td>Trojan.JS.Popupper.aw</td>
<td>3,355,605</td>
<td>0.21</td>
</tr>
<tr>
<td>8</td>
<td>Exploit.Script.Generic</td>
<td>2,943,410</td>
<td>0.18</td>
</tr>
<tr>
<td>9</td>
<td>Trojan-Downloader.SWF.Voleydaytor.h</td>
<td>2,573,072</td>
<td>0.16</td>
</tr>
<tr>
<td>10</td>
<td>AdWare.Win32.IBryte.x</td>
<td>1,623,246</td>
<td>0.1</td>
</tr>
</tbody>
</table>

As per CISCO annual report 2014 these threat attacks tie in to the methods malicious actors use to attack networks [4].

Fig. 1 Common Threat Categories Tracked by Cisco IntelliShield [2]

3 IMPLEMENTATION
We created a web security ontology by using protégé tool. This ontology build upon threat classification followed by a detailed
sub classification. The Threat Classification is an effort to classify the weaknesses and attacks that can lead to the compromise of a website, its data, or its users. Threat classification [1] includes:

A. Authentication
B. Authorization
C. Client-side attacks
D. Command execution
E. Information disclosure
F. Logical attacks

3.1 Authentication
The Authentication [2] section covers attacks that target a web site's method of validating the identity of a user, service, or application. Authentication is performed using at least one of three mechanisms: "something you have," "something you know," or "something you are" [1]. This section will discuss the attacks used to exploit the authentication process of a web. The Authentication ontology as given in Fig. 2.

![Fig. 2 Authentication Ontology](image)

1) Brute Attacks: A Brute Force attack [6] is an automated process of trial and error used to guess a person’s username, password, credit-card number or cryptographic key.

2) Insufficient Authentication: Insufficient Authentication [7] occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate.

3) Weak Password Recovery Validation: Weak Password Recovery Validation [2] is when a web site permits an attacker to illegally obtain, change or recover another user's password.

3.2 Authorization
The Authorization [2] covers attacks that target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action. The Authorization ontology as given in Fig. 3.

![Fig. 3 Authorization Ontology](image)
1) **Credential/Session Prediction**: Credential/Session Prediction is a method of hijacking or impersonating a web site user.

2) **Insufficient Authorization**: Insufficient Authorization is when a web site permits access to sensitive content or functionality that should require increased access control restrictions.

3) **Insufficient Session Expiration**: Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization.

4) **Session Fixation**: Session Fixation is an attack technique that forces a user's session ID to an explicit value.

### 3.3 Client-Side Attacks

The Client-side Attacks [2] section focuses on the abuse or exploitation of a web site's users. The Client-Side Attacks ontology as given in Fig. 4.

![Client-Side Attacks Ontology](image)

1) **Content Spoofing**: Content Spoofing is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.

2) **Cross-site Scripting**: Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser.

### 3.4 Command Execution

The Command Execution section covers attacks designed to execute remote commands on the web site [2]. The Command Execution ontology as given in Fig. 4.

![Command Execution Ontology](image)

1) **Buffer Overflow**: Buffer Overflow[8] exploits are attacks that alter the flow of an application by overwriting parts of memory.

2) **Format String Attack**: Format String Attacks alter the flow of an application by using string formatting library features to access other memory space.

3) **LDAP Injection**: LDAP Injection[9] is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.

4) **OS Commanding**: OS Commanding is an attack technique used to exploit web sites by executing Operating System commands through manipulation of =-09876plication input.

5) **SQL Injection**: SQL Injection is an attack technique used to exploit web sites that construct SQL statements from user-supplied input.
6) SSI Injection: SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server.
7) XPath Injection: XPath Injection is an attack technique used to exploit web sites that construct XPath queries from user-supplied input.

3.5 Information Disclosure

The Information Disclosure covers attacks designed to acquire system specific information about a web site. System specific information includes the software distribution, version numbers, and patch levels [2]. The Information Disclosure ontology as given in Fig. 6.

Fig. 6. Command Execution Ontology

1) Directory Indexing: Automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file is not present.
2) Information Leakage: Information Leakage is when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system.
3) Path Traversal: The Path Traversal attack technique forces access to files, directories, and commands that potentially reside outside the web document root directory.
4) Predictable Resource Location: Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality.

3.6 Logical Attacks

The Logical Attacks section focuses on the abuse or exploitation of a web application's logic flow [2]. The Logical Attacks ontology as given in Fig. 7.

Fig. 7 Logical Attacks Ontology

1) Abuse of Functionality: Abuse of Functionality is an attack technique that uses a web site's own features and functionality to consume, defraud, or circumvents access controls mechanisms.
2) **Denial of Service**: Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity.

3) **Insufficient Anti-automation**: Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually.

4) **Insufficient Process Validation**: Insufficient Process Validation is when a web site permits an attacker to bypass or circumvent the intended flow control of an application.

## 4 Conclusion

Web security threats pose a major challenge not only to security professionals but also to common people in modern computing environment. To be able to fight and reduce the chances of successful web attacks, there is a need to educate the masses about various security threats and their counter measures in software/hardware and security policies. This is a long challenging and dynamic process as web threats and counter measures evolves every day. The present work is an effort to classify and analyze various web security attacks using an ontological approach. This ontology is extensible for the upcoming threats in the future. We also aim to capture mobile security attacks in this ontology in near future to enhance its range. Security professionals and rest of the masses need to update their knowledge and implement the best practices in their day to day work. This paper helps to understand various methods of attacks and their relative ranking.

## Acknowledgment

I am very thankful to my co-author who helps me for researching on this project.

## References


## Author(s) Profile

**Sarita Sharma** received the B. tech degree in computer science engineering from the University of Rajasthan in 2007. She is currently pursuing Master degree curriculum in computer science engineering from the Technical University of Rajasthan. Area of research interests includes data mining.

**Saurabh Ranjan Srivastava** received the B. tech degree in computer science engineering from the University of Rajasthan in 2006. He received Master degree curriculum in computer science engineering from MNIT Jaipur in 2013. Area of research interests includes information retrieval, data mining and search engine strategies.