TECHNOLOGY

Early Identification and Prediction of Exploits Using Social Media

OVERVIEW

The number of software security vulnerabilities discovered in recent years has grown significantly. Several of these vulnerabilities, such as Heartbleed and Shellshock, became widely known and reported. However, when these exploits become publicly known, malicious users can create exploits of their own based on known information. Therefore, it is valuable to know when information about an exploit becomes public as soon as possible, especially if the exploit is not yet listed in a vulnerability database such as the Common Vulnerabilities and Exposures (CVE) system.

Researchers at the University of Maryland have developed an algorithm and software that scans publically available tweets and other social media posts to identify potential new exploits of known software vulnerabilities. By searching for relevant information posted to Twitter, it may be possible to find leaked information about an exploit, serving as an early warning system for detecting new proof of concept or actual exploits. Part of this algorithm includes accounting for malicious actors who might attack to 'poison' the data used by the algorithm by posted tweets designed to trigger false positives.

APPLICATIONS

· Identifying new exploits of known software vulnerabilities

ADVANTAGES

· Can find information of exploits faster by two days on average
· Includes mechanisms to resist adversaries' attempts to compromise software with misleading tweets

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Pending

LICENSE STATUS

Available for exclusive or non-exclusive license

EXTERNAL RESOURCES

IS-2015-045