Detecting Mobile Malicious Web pages in Real Time

ABSTRACT:

Mobile specific web pages differ significantly from their desktop counterparts in content, layout and functionality. Accordingly, existing techniques to detect malicious websites are unlikely to work for such web pages. In this paper, we design and implement kAYO,a mechanism that distinguishes between malicious and benign mobile web pages. kAYO makes this determination based on static features of a webpage ranging from the number of iframes to the presence of known fraudulent phone numbers. First, we experimentally demonstrate the need for mobile specific techniques and then identify a range of new static features that highly correlate with mobile malicious web pages. We then apply kAYO to a dataset of over 350,000 known benign and malicious mobile web pages and demonstrate 90% accuracy in classification. Moreover, we discover, characterize and report a number of web pages missed by Google Safe Browsing and Virus Total, but detected by kAYO. Finally, we build a browser extension using kAYO to protect users from malicious mobile websites in real-time. In doing so, we provide the first static analysis technique to detect malicious mobile web pages.

**SYSTEM ANALYSIS**

EXISTING SYSTEM:

The existing system called Content-based and in-depth inspection techniques to detect malicious websites: Dynamic approaches using virtual machines and honey client systems provide deeper visibility into the behavior of a webpage. Therefore, such systems have a very low false positive rate and are more accurate. However, downloading and executing each webpage impacts performance and hinders scalability of dynamic approaches. This performance penalty can be avoided by using static approaches. Static approaches rely on the structural and lexical properties of a webpage and do not execute the content of the webpage.

One such technique of detecting malicious URLs is using statistical methods for URL classification based on a URL’s lexical and host-based properties. However, URL-based techniques usually suffer from high false positive rates. Using HTML and JavaScript features extracted from a webpage in addition to URL classification helps address this drawback and provides better results. Static approaches avoid performance penalty of dynamic approaches. Additionally, using fast and reliable static approaches to detect benign web pages can avoid expensive in-depth analysis of all web pages.

PROPOSED SYSTEM:

In the existing system, the system experimentally demonstrates that the distributions of static features used in existing techniques (e.g., the number of redirections) are different when measured on mobile and desktop web pages. Moreover, we illustrate that certain features are inversely correlated or unrelated to or non-indicative to a webpage being malicious when extracted from each space. The results of our experiments demonstrate the need for mobile specific techniques for detecting malicious web pages.

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.4 GHz (Min)or Later versions.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.(Min)

**Software Requirements:**

* Operating system : Windows Family.
* Coding Language : J2EE (JSP,Servlet,Java Bean)
* Data Base : MY Sql Server.
* IDE : Eclipse Juno
* Web Server : Tomcat 6.0