CS 6262: Network Security - Project Ideas

Akshata Rao
Rituraj Satpute
Rohit Jamuar

January 21, 2014

Introduction

The ideas chosen for the project are

1. Safe Browsing Extension for a Web Browser.
2. Extracting Malware Trends.
3. An Android Malware.

We have enlisted our additional ideas below for the purpose of additional discussion.

4. Certificate Transparency Using The Bitcoin Blockchain.
5. Spam Generating Trojan.

1 Safe Browsing Extensions for Browsers

1.1 Central Idea

Build an extension that is able to

1. Scan accessed webpage against a blacklist of URLs
2. Scan accessed webpage HTML/script content to extract URL links. Evaluate the security of the website based on the URL links it hosts.
3. Evaluate other possible data about the website that can be extracted to perform the same.

1.2 Novelty

There already exist extensions such as AdBlock Plus[3] or Google Safe Browsing[4] that are built into web browsers. Although, they are restricted to deeming a website as insecure on the basis of its reputation alone, and not based on its content.

1.3 What do we intend to learn?

Even though there are similar established extensions out there, building such an extension by ourselves from scratch would help us learn about building security extensions in browsers, web security and blacklists.

1.4 Challenges

1. Finding the scope of deeming a website harmful
2. If the website is harmful and not blacklisted, I still need to download the content to scan it. How can I prevent the harm caused by downloading it?

2 Extracting Malware Trends

2.1 Central Idea

Build an automated system to analyze current malware trends via recently captured PCAPs. An automated system like this could really help in understanding:

1. which malwares are most prominent currently,
2. which (Alexa ranked) sites are actively being targeted, and
3. which ad-networks and / or countries serve as prevalent malware sources.

Furthermore, a system like this could be incorporated by ISPs and / or as a browser extension to prevent the underlying system from infection.

2.2 Novelty

Unlike most other malware analyzers, we intend to analyze PCAP dumps to derive trends. GTISC continually collects PCAPs, which could be employed for building this system. These PCAPs can then be systematically analyzed using WireShark's Python wrapper (pyreshark),for determining packets through which malwares are being served (i.e ones with PE / MZ in their header section). Once located, we can use this for collecting more details about the intermediate sites and the type of malware being served (through API calls to VirusTotal). We will maintain and update a list of malware serving sites (ad sites or otherwise) on a cloud service (Heroku, perhaps), which would be used by this system as a point of reference for operation.

3 An Android Malware

3.1 Central Idea

We intend to create an android malware from scratch and infect a device using one or more of the above methods. There are plenty of malware out there and our malware will most likely end up doing something that has already been done, maybe in a less optimum manner. But the goal is to learn everything about malware from "feet up". If possible, we will try to make the malware do something novel.

3.2 What we intend to learn

A malware has a wide range of aspects to it like its attack vector, the kind of vulnerability it harps on, the actual exploit, the cleanup process and so on. We intend to learn at least one of each one of these aspects and successfully implement from scratch. Building anything from scratch always grants the deepest understanding. And if we intend on creating systems that thwart malware then we need to be thoroughly comfortable with how malware work end to end.

3.3 Challenges

1. Modify existing APK and inject vulnerable code or,
2. Create an APK from scratch with malicious code and install/execute on device.
3. Effectively implementing an exploit which could be keylogging, data extraction, installing adware, rooting etc.
4. Performing proper cleanup post exploitation to remove traces.

4 Certificate Transparency Using The Bitcoin Blockchain

4.1 Central Idea

Researchers have always envisioned a decentralized approach to certificates, but none of them had the luxury of the Bitcoin Blockchain at their disposal. Hopefully, its existence and features can be leveraged to produce a secure and decentralized approach to public key certificates.

4.2 Novelty

There are existing solutions to certificate transparency without a certificate authority like identity based encryption. However, our idea is novel because there is no single unforgeable database where all the public keys are stored. Moreover, the Blockchain suppports the following crucial functions as defined in [8]:

1. Insertion - insertion of a new certificate into the ledger.
2. Revocation - revocation of an existing certificate.
3. Absence - determine if a certificate for a given public key or an entity exists or not.
4. Extension - to be able to prove that the ledger d at time t is an extension of the ledger d' at time t' ¡ t (i.e. d is more recent.)
5. Currency - proof that a certificate is current or not according to d at t.

4.3 Challenges

Apart from implementing the functions given above, there are the following two challenges:

1. If an attacker gains all the capabilities of a CA by compromising it then the attacker can, in no way, affect the validity of legitimate certificates that have already been issued.

2. If an attacker gains all the capabilities of a CA then the attacker, in no way, should be able to issue new and valid certificates for existing entities who have already been issued a legitimate certificate.

5 Spam Generating Trojan

5.1 Central Idea

Build a browser extension/toolbar which is a trojan. The browser extension tracks user activity to find his most popular search results and browsing history. It also tracks the email addresses entered in forms/Auto-Fill etc. The extension then sends this data of the accessed URLs and likely email addresses to a server. The central server extracts the web content of the URL, constructs a spam email message using this content to make the email attractive to the user. It also embeds links of malware links in the email. The email message is then sent to the email addresses collected.

5.2 Novelty

There exist sites like Google that evaluate the user browsing patterns for placing targeted ads. This idea is a twist to the concept. Existing technologies like AdBlock Plus use blacklists of known advertising and spyware sites to automatically block content from them. So it would not be able to block this.

5.3 Challenges

The efficacy of the trojan depends on

1. User must have installed the trojan

2. Firewalls could potentially block the browser extension from contacting the central server, which would render it ineffective.

3. The extension should be able to record the user browsing patterns.

References

[1] Safe Browsing - `http://kb.mozillazine.org/Safe_browsing`

[2] Phishing Protection Utility in Mozilla - -`https://wiki.mozilla.org/Phishing_Protection`

[3] Adblock Plus - -`https://wiki.mozilla.org/Phishing_Protection`

[4] Google Safe Search - http://cyber.law.harvard.edu/archived_content/people/edelman/google-safesearch/

[5] Personalizing Web Search using Long Term Browsing History - Nicolaas Matthijs et. Al - http://research.microsoft.com/pubs/139933/matthijsradlinski_wsdm2011.pdf

[6] Super-safe Web Browsing - http://www.pcworld.com/article/170518/article.html

[7] Extracting user web browsing patterns from non-content network traces - Gabriel Maciá-Fernández et. al

[8] Enhanced Certificate Transparency (Why Johnny could encrypt) : Mark D. Ryan