OREGON STATE UNIVERSITY

CS 373

WINTER 2019

Week 7

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Overview

This week we are diving deeper into web security. In this write up I will include interesting topics that I learned during lecture. I will also include a list of new terms that I learned this week. I will not be including any information about the lab this week as we are turning in the lab as a separate assignment.

II. Lecture topics

A. Computer crime under Oregon law

Below is a quick summary of Oregon's computer law.

- Knowingly accessing or using a computer or network (or attempting to do so) for the purpose of fraud; to obtain money, property or services; or to commit theft of proprietary information.
- Knowingly and without authorization altering, destroying or damaging any computer, network, software data ect. (or attempting to do so).
- Knowingly and without authorization using or accessing a computer or network (or attempting to do so).

The first two offences can be perused as class c felony. The last item is a Class A misdemeanor.

B. Web Delivery Mechanism

The internet is essentially built on the HTTP protocol. The web has evolved quite a bit over the years and now contains many different layers below is a summary of the different layers of the web.

- Content - email, html.
- Search Engine - Google, Archie.
- Browsers - DOS Houdini, Mosaic.
- World Wide web - 1990 Http
- Internet - 1975 TCP/IP
- Networks Ethernet
- Computers - Z3, Apple.

Ages of the internet:

- Stone Age - 1994 - 2000- Generic phishing, Popup-based redirection, script-bombing.
- Bronze Age - early 2000's - Improved Phishing, Cross-site scripting.
- Iron Age - 2005 - 2015 - Spear Phishing, plugin exploit, customized browser exploit.
- Today and Beyond - HTML 5 based attacks, Advanced Spear Phishing, Mt8. Every thing is browser based.

Today 95 percent of all malware is delivered via the web. There are a few other ways that malware is delivered but most of the malware is going through the web. Even the USB based attacks typically end up downloading something from the web to preform an exploit.

C. Web Browser 1.0

The web browser has many different layers because the web browser preforms a lot of different functions. Below are a few layers of the browser.

- Network protocol - this is where the network communication is done. The user or web app provides the Protocol, URL and maybe some data and in return data is delivered to the user.

- DOM - Document Object Model. This is the part that the user actually sees.
- Graphical Interface/input devices - This is the computer hardware which the user interacts with to do things on the web. These devices are also represented in software and interact with the browser using frames, events and various other widgets.

- JavaScript - This used to be the bit that helped the browser render the page. However today the JS exists in every layer.

In this system there are many different injection points into the browser. Below are some of the ways in which a threat may get injected into the browser.

- De-Obfuscated Content - Browser/Extensions
- JavaScript - Script Engine
- HTML - Dom Tree Browser/Extension
- HTML [RAW html] - Winlent ETW/ETL
- HTTP - Network Layer

D. User-Level Attacks

It is important to note that many of the attacks carried out on the web today have nothing to do with technology. Users in general are willing to do a lot of different things that we would note advise. Often time the users clicks on things or will intentionally download software. The weakest link in the chain of security is the user.

There are several different ways in which users may be attacked. Below is a list of different strategies for attcking the users.

- Phishing
- SEO Poisoning
- Fake AV
- Social media Link Insertion
- Forum Link Insertion
- Malvertising

Often times today hackers don't even care about maintaining a presence on someones device. It is possible to get the user to enter their bank information and SSN with out having to add a piece of malware to the users device. This is all they really want so they don't bother to put malware on the users system.

E. SEO Poisoning

In this scheme the hackers use SEO such as google trends to reach a wider audience. They use search results to lure the web searching victim. They do this using Celebrities, pop culture, world event, educational/professional Fake AV/AM. They game the search engine's relevance rules to get their result to show rather than the thing you actually searched for. You then visit this site which it self doesn't have any malicious content but when you click on a link you are directed to the malicious content.

F. Fake AV

Another common attack vector that takes advantage of social engineering is faking Anti-Virus software. This can be done on the computer or via the web. These fake AV's often take advantage of brand recognition by either mimicking windows or mimicking common AV brands that people recognize. Honestly, this is a really good idea. This takes advantage of users recognition of software that should help them maintain their system.

G. WYSIWYG or NOT

Attackers also use URLS that look like url's that you might actually want to visit. For instance microsoft vs rnicrosoft. They look very similar but go very different places. Another good example is http://oregonstate.edu vs http://oregonstate.eclu. The attackers also got really cleaver and started inserting characters that looked the same but were in fact different. This has since been disabled and can't be taken advantage of any more.

H. Social Media Attacks

Social media has been a gift to malware authors. Social media opens a new world for malicious URL delivery and information gathering. I saw this link on social media so it must be ok right? Wrong. Catfishing has become another strategy where some one gathers intelligence by pretending to be your friend but they are actually getting information on you.

I. Malvertising

In this scheme malicious actors use advertising networks as delivery mechanism for malware. The malicious advertiser finds people who they want to attack. Then they seed the advertising network with malicious adds. This may take some money to pay the advertising network to get your add where you want it to go. However, this is very efficient and doesn't require the attacker to have to search out the victim. But rather the advertising network does it for them.

J. Waterhole Attacks

Attackers gathers initial intelligence to determine which sites to target. Attacker then injects exploit into selected sites often visited by targeted victims. Exploit drops the malware on the client machine. Then they infect the network. This is often how attackers attack developers.

K. So what do we do?

Below is a possible list of solutions to the problems listed above.

- URL/Domain Reputation Systems.
- Site Certification Services.
- Client and Gateway AV/AM
- Safe URL shorteners
- Content provider education
- End user education

It has also been suggested that if there were no users that most of these security problems would go away because and I can't stress this enough, The users are the biggest weak point.

L. Security features on Browsers

The modern browser is much more secure than the browsers of 10 or even 5 years ago. Browsers today come with a variety of different features the prevent them from being taken advantage of. This includes the Same Origin Policy where we expect that applications that we want to run on the browser are from the same origin we are currently viewing. This will prevent scripts and malware from being injected into the session. The modern browser also includes URL Scheme access rules. The browser also uses OS Isolation and sand boxing to prevent applications running in the browser from accessing the OS. It also has a certain amount of redirection restrictions that attempt to prevent malicious redirection. The browsers also have built in URL reputation clients as well as content handling and sniffing.

M. Browser Exploits

Even though the modern browser has much more security, it is still possible for the browser to be exploited. Clearly the simplest way that the browser is exploited is that it downloads and runs malicious web content. Another possibility is that there is some sort of day zero exploit that hasn't been found yet. It is also important to note that most of these techniques still require the user to preform some action that the browser cannot reasonably prevent. So why don't we just filter malicious looking content? Well for several reasons, often attackers take advantage of common code obfuscation techniques. Essentially the attackers do the same things that many developers do in order to minimize the size of the client side code that they right. This is call minification. When we minify something essentially all the white space is taken out and the variables are renamed to short names that aren't human readable. This makes if difficult to filter out malicious looking content because it all looks the same.

N. Man in the middle attack

There is also another attack that is used on modern browsers called the man in the middle attack. This is where the attacker intercepts and modifies traffic in real-time. This can be done many different ways such as, DNS poisoning, Wifi Hacking, ARP Attack, Rogue or infected Router, and Rogue Proxy.

O. DNS spoofing

In the is attack the DNS server has a compromised cache. So the attacker has already set up a bad redirect in the DNS cache. At this point the user requests the content that is legitimate but is redirected to the malicious content. I find this kind of attack pretty nasty because the user is requesting good content that they probably know is good but are still redirected to malicious content.

III. Vocabulary

Below is a list of new terms I learned this week during class:

- Malvertising - Using advertising networks to distribute malware
- De-Obfuscated Content - This is the content that the users actually sees and can make sense of.
- Catfishing - Pretending to be someone's friend so that you can gather information about them or their organization.