Department
Computer Science

Project Title
Vulnerabilities of Cookies on the Internet; Analyzing multiple perspectives of Cookie Attacks

Project Objective or Aim
I intend to determine all of the vulnerabilities associated with cookie usage on the internet. This includes various types of cookies, and perspectives of these attacks. How can hackers take advantage of internet cookies? What are tech companies doing about these types of attacks? How do people fall victim to this attack? What makes companies more vulnerable to cookie attacks than others? What methods do hackers use to go around security measures that companies set up?

Project Background and Significance
Cookies are used by websites to identify users uniquely and determine how frequently they are viewing the site and for how long. These are known specifically as HTTP cookies. There are many types of HTTP cookies; broadly speaking, there are first-party cookies and third-party cookies. First party cookies are cookies that are created by the website the user is on whereas third-party cookies are cookies that are not directly on the website but are typically from an advertisement on the webpage. I will be focussing primarily on first party cookies, more specifically session cookies. Session cookies are used by most websites to remember the state of the website while deleting itself when the user closes the website.

While cookies are extremely useful for improving a web page, they prevent many security vulnerabilities to users which can be exploited through various attacks. The most basic attack is called Session Hijacking. This involves sending the user a phishing link to the real website but with a session id already specified within the URL. This gives the attacker full access to the user's session. Another popular method of abusing session cookies is called Sidejacking. Sidejacking is when an attacker is able to obtain a non secure sockets layer (SSL) cookie (a type of session cookie) typically through using a packet sniffer, to monitor the network traffic of the internet connection. Once the attacker has access to this cookie they are then able to access the user's account.

Cyber attacks are very common today, it is estimated that a cyber attack occurs every 44 seconds. Unfortunately when attacks involving cookies happen, the user is never fairly compensated for damages and their information can be sold or their money taken. There are a variety of methods that have been created to secure users from these types of attacks yet they are still common. While these ideas may be difficult to implement in regards to the scale of the web traffic, it begs the question, what are companies doing/have done to protect their users?

Research Methods

My approach to researching session cookie attacks is to collect information from the three main perspectives of the attack: the attacker, the victim, and the cybersecurity engineers for the company whose website is being attacked. By observing all the perspectives from the attacks we can analyze what the attack looked like from all angles. I would be able to reach out to victims of cookie attacks via forums such as Reddit. Many victims have reported their experience online and contacting them would allow me to ask them a series of important questions. It would be important to understand each part of how the victim was taken advantage of to then look for ways the company could have prevented this from happening to the victim. Fortunately, many hackers eventually stop using their skills maliciously and some end up working cybersecurity for companies. There are many hackers all over the internet, by reaching out to many of them I would be able to understand how hackers see the vulnerabilities of HTTP cookies. The hackers might view the use of cookies as irresponsible which would pose questions as to why it is so frequently used by companies. Large tech companies are typically at the forefront of new technologies and techniques becoming popularized. Interviewing cybersecurity experts at large tech companies would allow me to ask them what the companies have done to protect its users. This will allow me to understand how seriously these issues are being taken, because billions of people are victims of these attacks. I would also be able to ask them what they are currently doing to prevent cookie attacks from happening. It would be important to know if they have attempted to implement any of the solutions created by other engineers such as the one time cookie or the two way hash chain to encrypt the cookies. If they have not tried these techniques it would be important to know why not and other techniques they have either implemented or attempted to implement in order to prevent cookie attacks.

Expected Outcome

After completing my research I plan on developing a presentation to submit to the UCFs Showcase of Undergraduate Research Excellence. Through this showcase, I will be able to share the products of my research with others. Through the research from my project we will be able to understand the history of how cookie usage by companies has changed overtime. This would include the techniques that have been implemented and adopted in order to prevent hackers from taking advantage of their websites and their users. Understanding the history is important to understanding that hackers will always be on the lookout for potential exploits to make a profit; no matter what companies will do to try to stop them. This is because of the use of social engineering by hackers which are 90% of hacks. That is why it is important for every person using the internet to understand the risks and how they could be taken advantage of. We would be able to compare the timeline of what companies were doing to prevent cookie attacks, to how hackers were developing new cookie attacks. There will always be a battle between hackers and websites but it is important to know who is winning for users to understand the risks of using these websites. Most people do not understand the risks of using the internet and it is something I believe is dangerous considering how frequently the internet is used for critical purposes. This

research will shed light on the risks of using the internet, specifically how there are bad actors who will take advantage of websites using cookies to take over users' accounts. By interviewing the victims of cookie attacks, we will better understand how they stepped into that situation so we can prevent it ourselves. There are many different ways that have been developed by hackers over the years and it is important to know how they happen so users can prevent it from happening to themselves.

Literature Review

Thawatchai Chomsiri | Research Director | Ph.D. in Computer Systems ...
https://www.researchgate.net/profile/Thawatchai-Chomsiri.

Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History.
https://archive.comsuregroup.com/wp-content/uploads/2018/01/Yahoo-hack_-1bn-accounts-compromised-by-biggest-data-breach-in-history-_-Technology-_-The-Guardian.pdf.

Origin Cookies: Session Integrity for Web Applications.
http://sharif.edu/~kharrazi/courses/40442-952/read/session-integrity.pdf.

"Robust and Fast Authentication of Session Cookies in Collaborative and Social Media Using Position-Indexed Hashing." *IEEE Xplore*,
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6679990.

Smartech Home. https://smartech.gatech.edu/bitstream/handle/1853/.

"Secure Cookies on the Web." *IEEE Xplore*,
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=865085.

Preliminary Work and Experience

I am currently a student at the University of Central Florida working towards a degree in Computer Science. I have completed coursework for Concepts in Computer Science and Intro to Programming in C and which have developed basic programming skills in C and Python. I am an active member of Knight Hacks and The Association of Computing Machinery at UCF in which I partake in workshops, hackathons, and team projects. I have experience working on technical projects and a strong understanding of computers and how the internet works. I have also thoroughly researched the subject of cookie usage on the internet, the various attacks that can take place abusing cookies, and how users fall victim to these types of attacks. My previous research project for the U.S. Government at UCF on the subject of Ghost Guns in the U.S. shows my ability to thoroughly research a topic and develop exceptional writing. Due to this knowledge, I believe I am highly qualified to develop this research project.

IRB/IACUC statement:

My proposal will not require IRB or IACUC approval.

Budget:

Advertising for recruitment- $100.00

- Advertising will be done using Google and Facebook ads to recruit individuals interested in conducting research for the project.

TOTAL COST: $100.00