Romel Cabiling

Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 10 Internet Cookies > Lesson Proper for Week 10

Lesson Proper for Week 10

INTERNET COOKIES

Cookies

o A computer “cookie” is more formally known as an HTTP cookie, a web cookie, an Internet cookie, or a browser cookie is a term for a packet of data that a computer receives, then sends back without changing or altering it.

o Are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.

No matter what it’s called, a ***computer cookie*** *consists of information. When you visit a website, the website sends the cookie to your computer. Your computer stores it in a file located inside your web browser. (To help you find it, this file is often called “Cookies.”)*

When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.

Why internet cookies are called cookies?

Watch this video:

HOW COOKIES WORK

When you revisit the website, your browser sends the information back to the site. Usually a cookie is designed to remember and tell a website some useful information about you.

For example, an online bookstore might use a persistent cookie to record the authors and titles of books you have ordered. When you return to the online bookstore, your browser lets the bookstore's site read the cookie. The site might then compile a list of books by the same authors, or books on related topics, and show you that list.

This activity is invisible to you. Unless you have set your preferences so that you will be alerted when a cookie is being stored on your computer, you won't know about it. When you return to a website, you won't know that a cookie is being read. From your point of view, in the example above, you'd simply visit the online bookstore, and a list of books that might be of interest to you would magically appear.

MANAGING INTERNET COOKIES

Under normal circumstances, cookies cannot transfer viruses or malware to your computer. Because the data in a cookie doesn't change when it travels back and forth, it has no way to affect how your computer runs.

However, some viruses and malware may be disguised as cookies. For instance, "super cookies" can be a potential security concern, and many browsers offer a way to block them. A "zombie cookie" is a cookie that recreates itself after being deleted, making zombie cookies tough to manage. Third-party tracking cookies can also cause security concerns, since they make it easier for parties you can't identify to watch where you are going and what you are doing online.

Here's how to manage your cookies in order to protect your online activity from prying eyes:

1. Open your browser. Because cookies are stored in your web browser, the first step is to open your browser. Popular browsers include Firefox, Chrome, Safari, and Internet Explorer.

2. Find the cookie storage. Each browser stores cookies in a slightly different location. In Internet Explorer 9, for example, you can find them by clicking "Tools," then "Internet Options," then "Privacy." In Chrome, choose the Chrome menu on the toolbar, then click "Privacy." Most browsers store cookie settings under the privacy options.

3. Choose your setting. Every browser gives you a range of options for handling cookies. Internet Explorer, for instance, has a slider that you can adjust for greater or lesser amounts of protection. Chrome both lets you delete existing cookies in a single click and choose how future cookies are collected or stored.

Banning all cookies makes some websites difficult or impossible to navigate. However, a setting that controls or limits third-party and tracking cookies can help protect your privacy while still making it possible to shop online and carry out similar activities.

USES OF COOKIES

1. Session management. For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.

2. Personalization. Customized advertising is the main way cookies are used to personalize your sessions. You may view certain items or parts of a site, and cookies use this data to help build targeted ads that you might enjoy.

3. Tracking. Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.

TYPES OF COOKIES

a. Strictly necessary cookies are cookies that are necessary for correct functioning of our website. They entail cookies allowing you to access our login secured pages, use the cart or online payments.

b. Analytical/performance cookies allow us to identify and count visitors of our website and analyse their use of it. It helps us to improve how our website functions in order to allow you find relevant information as soon as possible.

c. Functionality cookies are used in order to identify you when you come back to our website. That allows us to personalise our content for you and remembers your preferences (e.g. language).

d. Targeting cookies are used to tell us what webpages have your browsed and what links have you clicked on. This information is then analysed to tailor our content and advertisements for your use specifically.

e. Flash cookies are specific cookies for playing video and audio content on our website through Adobe Flash Player. For example, Flash Player uses Flash Cookies to save your pre-sets.

f. Persistent cookies these cookies stay in your device for a time specified within the cookie itself. They are activated every time you visit the domain that created the cookie.

Persistent cookies are used for two primary purposes:

§ **Authentication.** These cookies track whether a user is logged in and under what name. They also streamline login information, so users don't have to remember site passwords.

§ **Tracking.** These cookies track multiple visits to the same site over time. Some online merchants, for example, use cookies to track visits from particular users, including the pages and products viewed. The information they gain allows them to suggest other items that might interest visitors. Gradually, a profile is built based on a user's browsing history on that site.

g. Session cookies these cookies allow websites to connect the user between clicks while browsing a website. Session cookies are created when you open a web browser and deleted after you close it.

When the session ends, session cookies are automatically deleted. They also help the "back" button or third-party anonymizer plugins work. These plugins are designed for specific browsers to work and help maintain user privacy.

FIRST PARTY AND THIRD PARTY COOKIES

Some cookies may pack more of a threat than others depending on where they come from.

First-party cookies are directly created by the website you are using. These are generally safer, as long as you are browsing reputable websites or ones that have not been compromised.

Third-party cookies are more troubling. They are generated by websites that are different from the web pages users are currently surfing, usually because they're linked to ads on that page.

Visiting a site with 10 ads may generate 10 cookies, even if users never click on those ads.

Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads. Consequently, the advertiser could determine that a user first searched for running apparel at a specific outdoor store before checking a particular sporting goods site and then a certain online sportswear boutique.

Zombie cookies are from a third-party and permanently installed on users' computers, even when they opt not to install cookies. They also reappear after they've been deleted. When zombie cookies first appeared, they were created from data stored in the Adobe Flash storage bin. They are sometimes called **“flash cookies”** and are extremely difficult to remove.

Like other third-party cookies, zombie cookies can be used by web analytics companies to track unique individuals' browsing histories. Websites may also use zombies to ban specific users.

ALLOWING OR REMOVING COOKIES

Cookies can be an optional part of your internet experience. If you so choose, you can limit what cookies end up on your computer or mobile device.

If you allow cookies, it will streamline your surfing. For some users, no cookies security risk is more important than a convenient internet experience.

Here’s how to allow cookies:

Find the cookie section — typically under Settings > Privacy.

Click the boxes to allow cookies. Sometimes the option says, "Allow local data.”

If you don’t want cookies, you can simply uncheck these boxes.

Removing cookies can help you mitigate your risks of privacy breaches. It can also reset your browser tracking and personalization.

Removing normal cookies is easy, but it could make certain web sites harder to navigate. Without cookies internet, users may have to re-enter their data for each visit. Different browsers store cookies in different places, but usually, you can:

Find the Settings, Privacy section — sometimes listed under Tools, Internet Options, or Advanced.

Follow the prompts on the available options to manage or remove cookies.

◀ Preliminary Activity for Week 10

Jump to...

Analysis, Application, and Exploration for Week 10 ▶

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 1
Network Attacks: Detection, Analysis & Counter...
Participants
General
06 - Preliminary Examination
09 Internet Protocol Address (Ip Address)
10 Internet Cookies
Preliminary Activity for Week 10

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

- Assignments
- Forums
- Quizzes
- Resources