Session-3: (browser fingerprinting, CSP)

Other tracking methods

Tracking cookies are not a new technology. They've been in use for over a decade and little has changed as far as the way they work. Despite that, they provide a simple, accurate way to track and record user behavior across the web, and they aren't going away anytime soon.

That's not to say tracking cookies are the only way third parties monitor what you do online. Data mongers have several tools at their disposal to stay locked onto you.

IP address

Even before there were cookies, there were IP addresses. Every device connected to the internet is assigned a unique IP address that allows your device to communicate with other devices. IP addresses are a core component of how the internet works. But because they are unique, they can be used to track you.

Your public IP address is made up of a string of numbers and decimals. It changes periodically and is associated with your location. If you connect to a different wifi network, for example, you are assigned a new IP address and your old one is recycled and assigned to someone else. So it's not the most enduring or accurate way to target someone, but it's easy and it works.

To avoid being tracked by your IP address, I recommend using a VPN. A **VPN** encrypts all of the internet traffic on your device and routes it through an intermediary server in a location of your choosing. This masks your real IP address with that of the VPN server, and that IP address is usually shared with dozens, if not hundreds of other users, making it nearly impossible to trace activity back to one individual.

Referrer URLs

A referrer URL is the web address of the previous website where you clicked a link to get to the current website. For example, if you found Privacy.net through a Google search and clicked on a link to this article in the search results, the referrer URL for this page would belong to Google. Referrer URLs can be used for several reasons, and recording your browsing history is one of them.

When cookies are sent to the server that created them, they often contain referrer URLs. But referrer URLs don't require a cookie and the same information can be requested from a website via other means.

Web beacons

Web beacons, also called **pixel tags**, are little segments of code on web pages that check whether you have accessed some content. Web beacon is actually an umbrella term for several similar techniques.

Web beacons can be hidden inside content elements of a web page, making them more difficult to prevent. They can be hidden inside images and other page elements to log user behavior and transmit that data back to the website owner.

Web beacons are commonly used to check whether someone who received an email actually read it. By embedding a pixel tag in an email, the email must load a resource from a third-party. When this happens, the resource can request the recipient's IP address, timestamp, type of browser, and whether the resource owner already set a cookie in this browser. Like cookies, the server can store all of this information and associate it with the user's unique tracking ID.

Browser fingerprinting

Browser fingerprinting is an emerging technique that's getting more and more accessible and is notoriously difficult to shake. A website can glean a lot of information about your web browser through server-side access logs and client-side Javascript and Adobe Flash. This information includes but is not limited to:

- Browser model and version (user agent string)
- Language
- Time zone
- List of plugins/extensions
- Fonts and font size
- Screen resolution
- Do Not Track status
- Several other browser settings
- Whether cookies are allowed
- Protocol
- URL requested
- IP address
- Referrer URL

Even if you connect to a VPN to hide your IP address and block tracking cookies, all of the other information can form a combination so specific that the resulting profile can only plausibly belong to a single person or small group of people. Attempting to alter your browser settings and install more plugins only makes you stand out more.

You can disable Javascript using a plugin like NoScript or ScriptSafe to prevent the collection of most of this data, but many websites rely on Javascript to function, so chances are you'll be forced

to enable it at some point. The only other alternative is to use two browsers: one for private activities and one for day-to-day non-sensitive stuff.

Cookie syncing (CSP)

Most tracking cookies can only be used by the domain that created them. Advertising companies are responsible for many domains that serve tracking cookies, each with its own database of user profiles and audience segments used to target you with ads.

Save for Google, most of these ad companies aren't prolific enough to be everywhere on the web at once, which leads to gaps in their data. Enter **cookie syncing**, the practice of combining advertising data sets to create more accurate and comprehensive tracking profiles.

Cookie syncing occurs when two advertising companies partner up or acquire one another. This consolidation helps them compete with Google, but also has an adverse effect on users' privacy.

Supercookies

Most cookies are tied to specific domains, such as "google.com". Supercookies are associated with top level domains like ".com" and ".org". This allows them to affect requests for cookies from websites that use those top-level domains. For example, a supercookie that uses the ".net" top-level domain could disrupt or impersonate requests from Privacy.net.

Not only could supercookies be used to track you across the web, they can also be used for malicious purposes like changing user information or forging a login. For these reasons, most **modern browsers block supercookies**. They're worth mentioning but probably aren't much of a threat to you.