CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 8: Browser Usage

Web Browsing Dangers

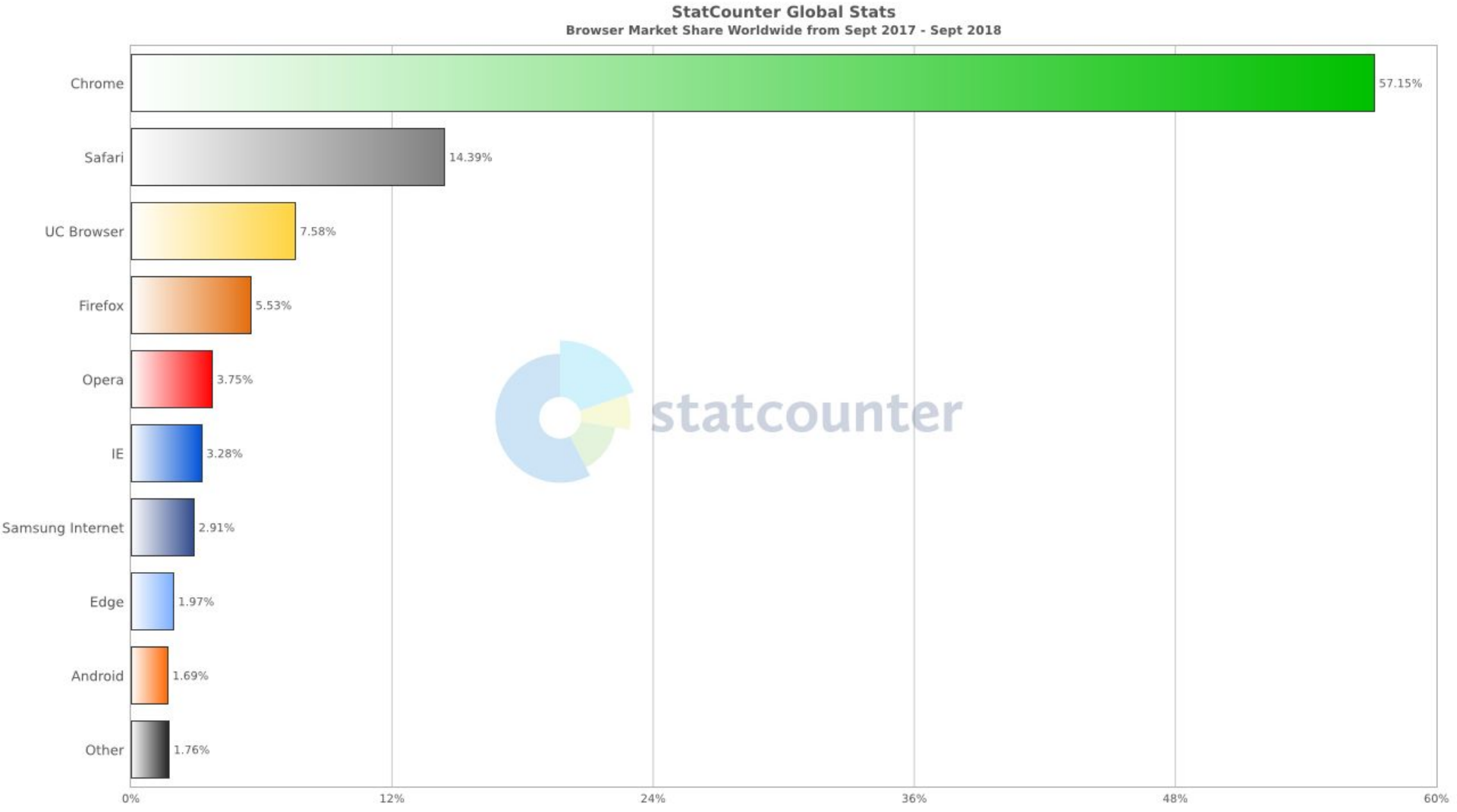
Merely browsing the Web can put you at serious risk.

Drive-by downloads can download all kinds of spyware, pests, and Trojans to your PC without your knowledge.

Malcontents can install Browser Helper Objects on your PC to hijack your home page and spy on your web browsing.

Web sites can invade your privacy by watching every page you visit.

Web Browsers



Web Browsers

In this section, we will look at the three major players in the browser market (Chrome, Firefox and IE) and delve into how we can make them more secure.

Some people have attachments to certain browsers and although they may not be the safest, it may be possible to make them more secure.

The idea is to try and make the browser that you are using more secure.

This can be done through the use of configuring browser settings and add-ons.

Web Browsers

Web browsers can be breached in one or more of the following ways:

1. Operating system is breached and malware is reading/modifying the browser memory space in privilege mode
2. Operating system has a malware running as a background process, which is reading/modifying the browser memory space in privileged mode
3. Main browser executable can be hacked
4. Browser components may be hacked
5. Browser plugins can be hacked
6. Browser network communications could be intercepted outside the machine

Firefox

Firefox has a number of basic security settings but it is the add-ons where Firefox's real security lies.

- Web of Trust
- NoScript
- AdBlock Plus
- Ghostery
- Better Privacy
- Bitdefender Quick Scan
- RequestPolicy

The process of activating security features in a browser and using security add-ons in a browser is called "browser hardening"

Firefox Add-ons

Web of Trust

- WOT warns you about risky websites that try to scam surfers before they enter in them using a safety rating of 21 million websites, WOT combines evidence collected from multiple sources.

NoScript

- NoScript gives you the power to specify the sites you trust and only those sites will be allowed to run active content like JavaScript, Java code and other executable code.
- The add-on protects you from cross-site scripting attacks and clickjacking attacks.

Firefox Add-ons

AdBlock Plus

- Allows you to regain control of the Internet and view the web the way you want to.
- The add-on is supported by over forty filter subscriptions in dozens of languages which automatically configure it for purposes ranging from removing online advertising to blocking all known malware domains.

Ghostery

- Reduces tracking, particularly by advertising companies
- Scans web page to detect trackers, web bugs, pixels and beacons.
- Allows you to opt-out of tracking, block scripts from companies you don't trust, delete and block images & iFrames

Firefox Add-ons

BetterPrivacy

- Is a Super-Cookie Safeguard which protects from usually undeletable Flash-Cookies.
- It blocks long term tracking on Google, YouTube, Ebay to name a few.

Bitdefender TrafficLight

- Provides protection against phishing attacks, safe searching of the Internet. It will identify and report fake website on your search result.
- Identifies trackers that are trying to report on your web behaviours.

Firefox Add-ons

RequestPolicy

- Shows you cross site (XS) request made by web pages you visit, this can protect you from attacks and tracking
- Cross site requests are requests the website you are visiting ask your browser to make to a complete different site. It can be legitimate, but most at times it can allow other websites to track your online behaviour.
- By default RequestPolicy denies such request. Users are notified of this action. Then notification flag at the bottom right hand of your browser turns red. One can click on it to edit.

Google Chrome

Safe Browsing

- If you are about to visit a website which is believed to be associated with malware and phishing, Chrome will warn you with a pop-up dialog box.

Sandboxing

- IE and other browsers run one instance of the browser engine with multiple associated processes. This means that if one of the browser windows runs in to trouble then it will most likely crash all the other windows as well.
- Google Chrome on the other hand runs each instance separately. Malware or issues in one of the tabs does not affect other open browser instances. Also, the browser is unable to write to or modify the operating system in any way - protecting your PC from attack.

Google Chrome

Auto-updates – Chrome checks regularly for updates to ensure that you are protected with the most current security updates. All of this is done without your knowing.

Extensions:

- Web of Trust
- Disconnect
- AdBlock Plus
- Click&Clean
- Site Advisor
- FlashBlock
- HTTPS Everywhere

Google Chrome Extensions

Web of Trust

- Web of Trust is a safe browsing tool, which warns you about risky sites that cheat customers, deliver malware or send spam.

Disconnect

- Blocks third-party tracking cookies

AdBlock Plus

- Blocks ads all over the web and adds to privacy

Click&Clean

- Deletes your browsing history, typed URLs, Flash cookies, all traces of your online activity to protect your privacy.

Google Chrome Extensions

Site Advisor

- This extension will be based on McAfee SiteAdvisor and will warn / inform you about the ratings of the page you are visiting

FlashControl

- This extension automatically blocks flash content on webpages unless allowed

HTTPS Everywhere

- This extension will ensure you always go to the secure site if available

Internet Explorer (& Edge)

Microsoft through IE has a patchy history with security at best

Latest of IE(11) is much more secure than earlier versions (8-) and broadly comparable to Chrome & Firefox in terms of security if still viewed as inferior

IE11

New security features of IE11 include SmartScreen (protects against phishing and malware) and Enhanced Protected Mode (Sandboxing of the browser)

Still has security problems! → serious vulnerabilities still being found (https://www.vulnerabilitycenter.com/#!vul=55645)

Support for legacy MS technologies → this carries over unpatched vulnerabilities

Support Web Cryptography API → allows for secure communications

Edge

Microsoft's latest browser (Edge) mitigates many of the problems of IE by using a separate code base → legacy support and code removed that posed security risks!

Uses Passport technology to prevent phishing attacks → edge authenticates websites and downloads by default in the background

Edge is not built on the OS like IE → operates permanently in a sandbox so if Edge is compromised you are partially protected

MS claims this is the most secure browser

General Safe Browsing Tips

Keep your browser software up-to-date: This is crucial, as new patches are often released to fix existing vulnerabilities in browser software.

Scan files before downloading: It is important to avoid downloading anything until you're confident that it is secure

Watch out for phishing: Phishing attacks use online communications (usually email) to trick users into giving out their sensitive information.

Use HTTPS: The "s" in "https" stands for **secure**, for secure communication over a network.

- In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) (a.k.a. HTTP over TLS)
- HTTP over TLS is more secure than it's predecessor HTTP over SSL (Secure Sockets Layer)

General Safe Browsing Tips

Regularly monitor your bank statements: Keeping an eye on your online statements

Disable stored passwords: Nearly all browsers and many websites in general offer to remember your passwords for future use.

Don't reuse passwords: Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information.

Clean cache regularly → Ccleaner or equivalent can do this for you!

Turn on your browser's popup blocker: Popup blocking is now a standard browser feature

General Safe Browsing Tips

The single greatest danger you face on the Internet is yourself.

More specifically, there is no software that can compensate for your poor Internet safety habits.

Let's start with how much critical information you willingly give away.

This is the Internet - information posted online can be seen by almost anyone and secure websites can be hacked.

Even restricted pages such as your Facebook profile are not entirely safe -- someone with access (such as your "friends") could copy and paste the information to a Web page that isn't truly private.

General Safe Browsing Tips

Issues

- Connecting to unsecure wireless networks
- Accessing secure websites in public
- Saving Personal Information on shopping websites
- Posting Personal Information on Social Networking Sites
- Keep your computer personal
- Do not install software that you do not explicitly want