# Extra Reading- Week 1

## Introduction

HTTP/3 is in its final standardization phase by the IETF, aiming to enhance performance and security.

Key improvements over HTTP/2 include:

* Replacing TCP with QUIC (a UDP-based transport protocol).
* More efficient header compression.
* Mandatory TLS 1.3 for security.

Objective: The paper examines HTTP/3’s adoption, its real-world performance benefits, and its impact on web browsing and video streaming.

## Methodology

* The study conducts a large-scale measurement campaign to analyze:
* Adoption Trends: Using the HTTPArchive dataset to track websites supporting HTTP/3.
* Web Performance: Testing 14,707 websites under different network conditions (latency, bandwidth constraints, packet loss).
* Mobile Browsing: Evaluating HTTP/3 on smartphones and tablets in mobile networks (3G, 4G).
* Video Streaming: Measuring HTTP/3’s impact on adaptive video streaming using controlled DASH-based experiments.

## Key Findings

### 1. HTTP/3 Adoption

* Google, Facebook, and Cloudflare are the early adopters.
* HTTP/3 adoption grew steadily but faced setbacks when Cloudflare briefly disabled support.
* Despite HTTP/3 support, many websites still rely on HTTP/2 or HTTP/1.1 for third-party resources.

### 2. Web Browsing Performance

* High Latency Scenarios: HTTP/3 significantly outperforms HTTP/2.
* Low Bandwidth & Packet Loss: Performance differences between HTTP/3 and HTTP/2 are minimal.
* Websites with fewer third-party connections and fully adopting HTTP/3 benefit the most.

### 3. Mobile Browsing Performance

* Mobile users (smartphones & tablets) see noticeable benefits from HTTP/3.
* Performance improvements are most pronounced on 4G networks.

### 4. Video Streaming Performance

* No significant improvements for adaptive streaming with HTTP/3.
* HTTP/3 results in slower startup times (Playback Startup Delay) under some bandwidth constraints.
* HTTP/3 may cause more frequent resolution downgrades in constrained bandwidth conditions.

## Conclusions

* HTTP/3 adoption is increasing but is mainly driven by large companies.
* Performance improvements depend on network conditions:
* Best improvements in high-latency scenarios (e.g., mobile networks).
* Limited benefits in packet loss or constrained bandwidth conditions.
* Video streaming does not benefit from HTTP/3 in its current form.
* Future work is needed to analyze real-world user experiences, different client-server configurations, and long-term adoption trends.

# Second Reading:

## Introduction

Problem Statement: Many online businesses use third-party web analytics services to track user behavior. However, privacy-focused browser updates have restricted third-party cookie tracking.

To bypass these restrictions, businesses use CNAME cloaking, disguising third-party analytics providers as subdomains of their websites.

This can unintentionally expose session cookies, leading to serious security risks, including account takeover.

## Background and Threat Model

### 1. Web Tracking & CNAME Cloaking

* Traditionally, third-party trackers used their domains and third-party cookies.
* Browsers like Firefox and Safari now block these cookies by default.
* CNAME Cloaking tricks browsers into treating third-party services as first-party subdomains.
* Example: analytics.example.com could be an alias for thirdparty-tracker.com.

### 2. Cookie Security Risks

* Session cookies are used for authentication. If exposed, attackers can impersonate users.
* Poor cookie security settings (e.g., missing Secure and HttpOnly attributes) worsen this risk.

### 3. Attack Model

* A malicious third-party analytics provider could:
* Collect session cookies.
* Hijack accounts by using exposed cookies.
* Compromise banking, e-commerce, and financial services.

## Methodology

The study developed TAFinder, an automated system to detect:

* CNAME cloaking domains on websites.
* Whether first-party cookies are leaked to these third-party services.
* If session cookies are exposed, leading to security risks.

Process:

* Analyzed 100,000 top websites (Majestic Million dataset).
* Captured HTTP and DNS traffic to identify CNAME cloaking.
* Machine learning classified domains as trackers or non-trackers.
* Verified whether session cookies were exposed.

## Findings

### 1. Widespread CNAME Cloaking

* 21.2% (21,184) of analyzed websites used CNAME cloaking.
* 10.7% (2,271) specifically used CNAME cloaking for third-party tracking.
* Large companies like Omniture (Adobe Analytics) were top offenders.

### 2. Cookie Leaks

* 1,195 out of 2,271 websites (52.6%) leaked first-party cookies to third-party trackers.
* 437 websites communicated with trackers over HTTP, further exposing cookies.
* Some financial and banking websites leaked sensitive session cookies.

### 3. High-Risk Websites

* 27 high-profile sites (banks, e-commerce, financial services) exposed session cookies.
* Attackers could hijack accounts, make transactions, and steal data.
* Example: Walgreens.com leaked session cookies, exposing prescription and order history.
* Two major US banks also leaked session cookies, allowing account access.

### 4. Poor Vendor Response

* The researchers disclosed issues to affected websites.
* Many ignored or denied the problem.
* Some silently fixed the vulnerability without acknowledgment.
* Solutions & Recommendations
* Website Owners:
* Stop using CNAME cloaking for tracking.
* Configure cookies securely (Secure, HttpOnly, no broad domain access).
* Audit third-party integrations.
* Browsers & Extensions:
* Enhance CNAME detection.
* Block cloaked trackers like third-party domains.
* Use blacklists to flag CNAME-based tracking.
* Regulators & Security Experts:
* Address CNAME cloaking risks in privacy regulations.
* Raise awareness about hidden tracking vulnerabilities.

## Conclusion

* CNAME cloaking is a major security risk: It enables session cookie leaks, leading to account hijacking.
* Over 50% of analyzed websites leaked cookies to hidden trackers.
* Banks and financial institutions were affected, putting sensitive user data at risk.
* The research highlights an urgent need for better cookie security and third-party tracking controls.