

Web Server Design

Lecture 10 – HTTPS

Old Dominion University

Department of Computer Science

CS 431/531 Fall 2022

Sawood Alam <salam@cs.odu.edu>

2022-11-02

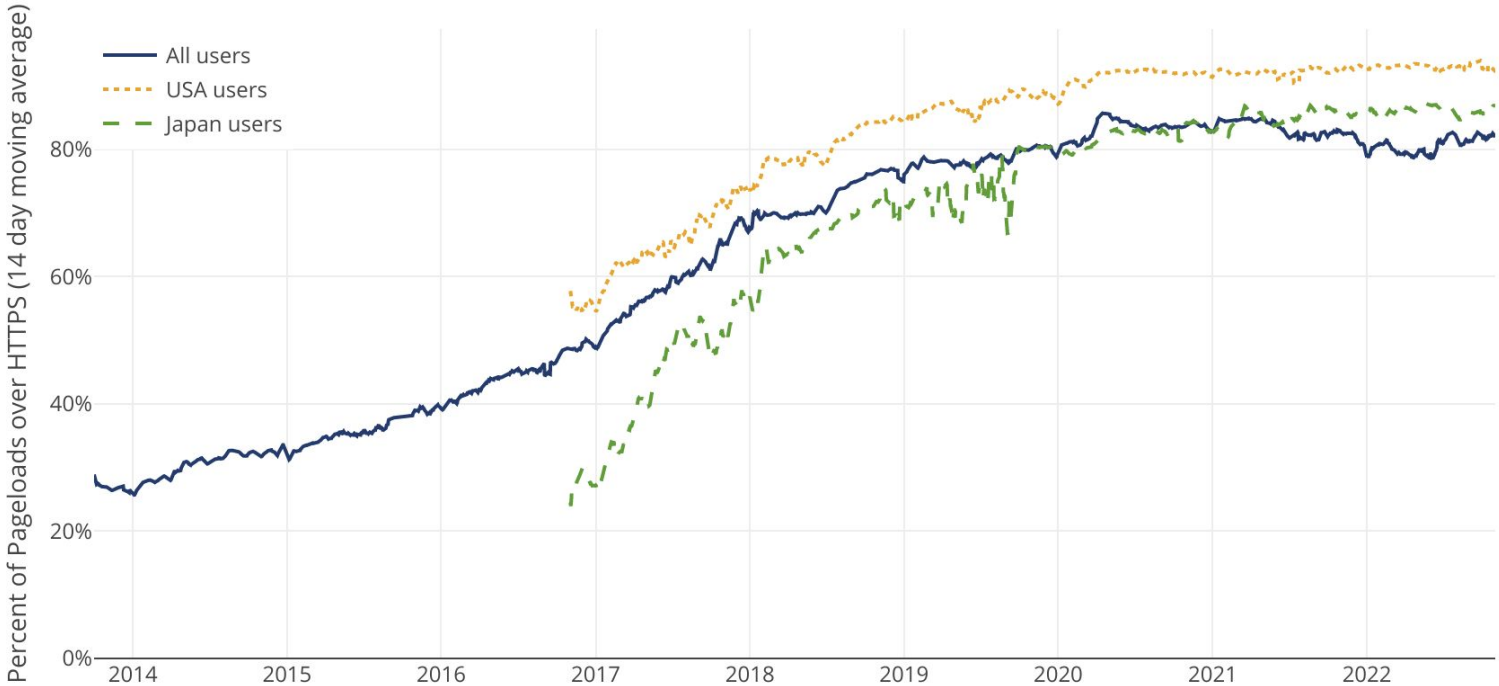
ISPs Inject Ad In HTTP HTML Pages

The image shows a screenshot of the naukri.com website. The top navigation bar includes the naukri.com logo, a search bar, and links for Jobs, Recruiters, Companies, Services, More, and Login. Below the navigation bar, there are tabs for All Jobs, Premium Jobs, Govt. Jobs, and International Jobs. A search bar is present with fields for Skills, Designations, Companies, Location, Experience, and Salary, and a Search button. Below the search bar, there are links for Browse Jobs, All Jobs, Jobs by Company, Jobs by Category, Jobs by Location, Jobs by Designation, and Jobs by Skill. The main content area is partially obscured by a large advertisement for MTNL's Broadband Festive Bonanza. The advertisement features a yellow background with red and green accents, and text that reads: "MTNL's BROADBAND FESTIVE BONANZA", "Save ₹800 on a New Broadband Connection", "₹300/- Waived Off on Registration & Testing charges", "Save ₹500/- on initial charges for Wi-Fi Modem from ₹800/- to ₹300/-", and "For booking type 'mtnl' on your mobile and send it to 9868552121. Offer valid for Limited Period". The advertisement also includes a "Hurry!" badge and a "Register Free" button. At the bottom of the advertisement, there is a "For further details" section with contact information: "Call 1560 7 2221590", "Email at 1560@btl.net.in", and "Contact your nearest Search Head". The MTNL logo is also visible at the bottom of the advertisement.

From: <https://www.medianama.com/2015/06/223-mtnl-isp-advertising-airtel/>

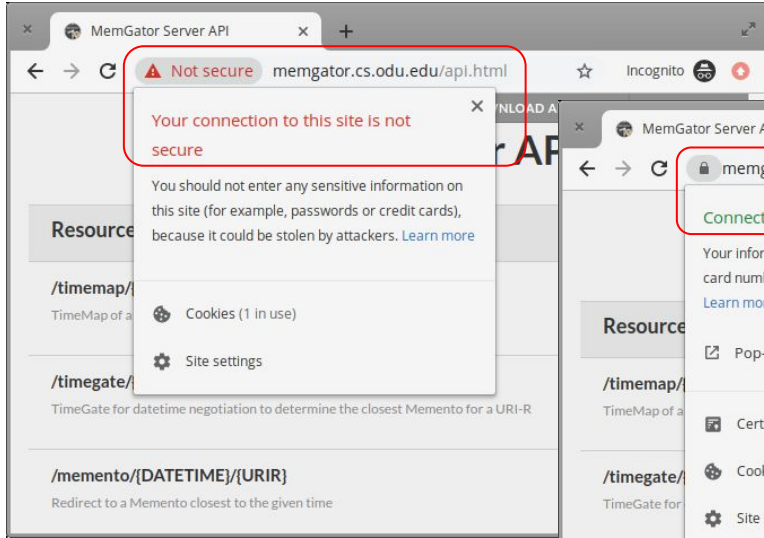
Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: [Firefox Telemetry](#))

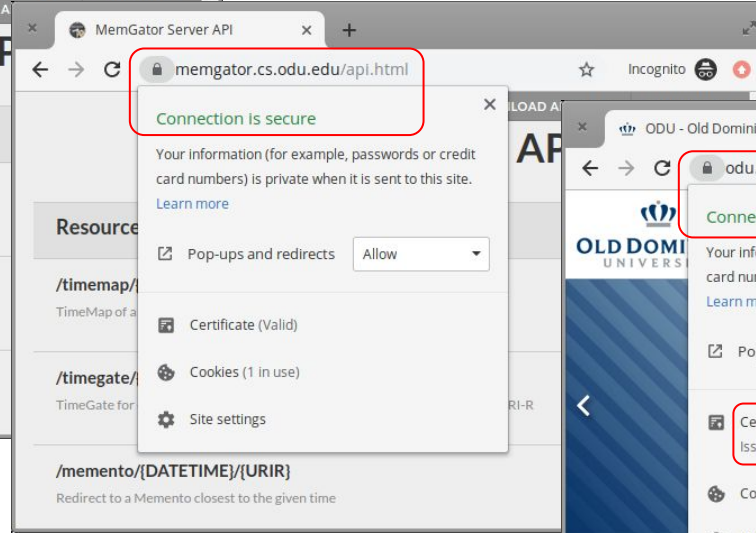


From: <https://letsencrypt.org/stats/>

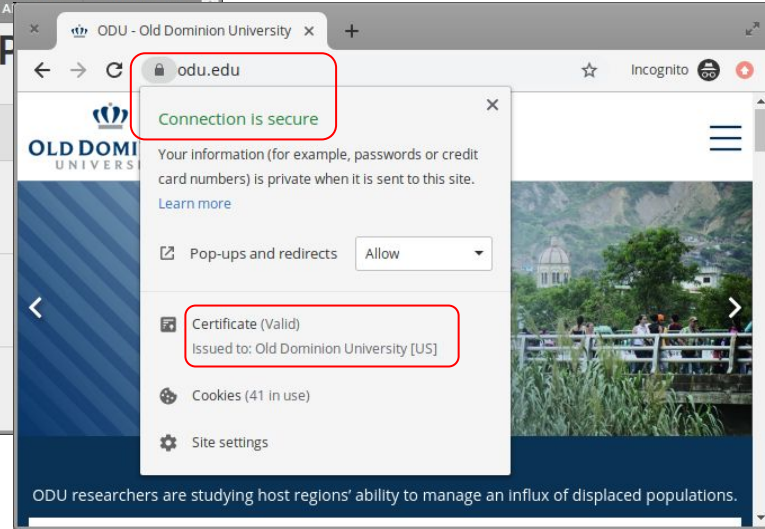
HTTP vs. HTTPS



No Certificate

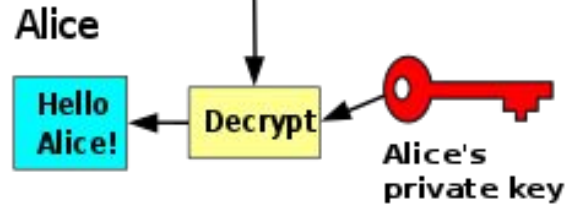
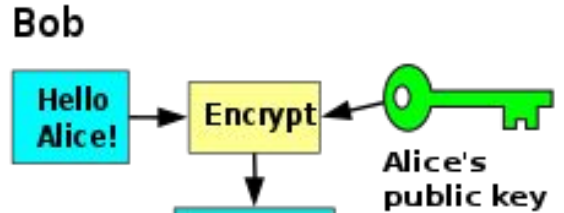


Domain Validation

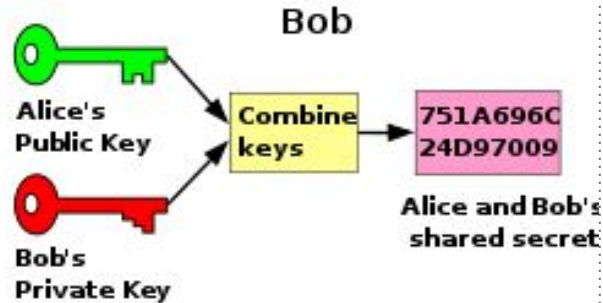
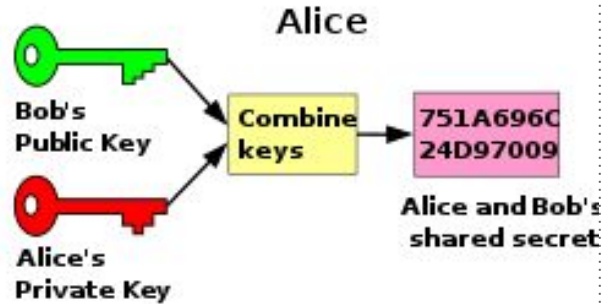


Organization/Extended Validation

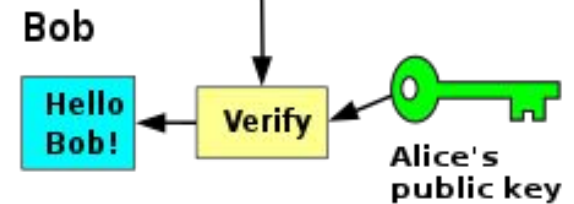
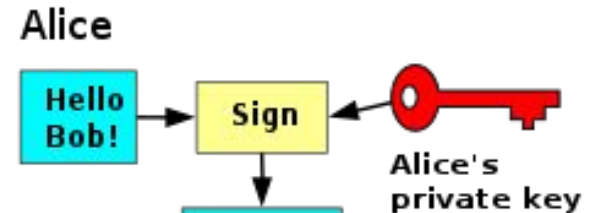
Public-key Cryptography



Encryption

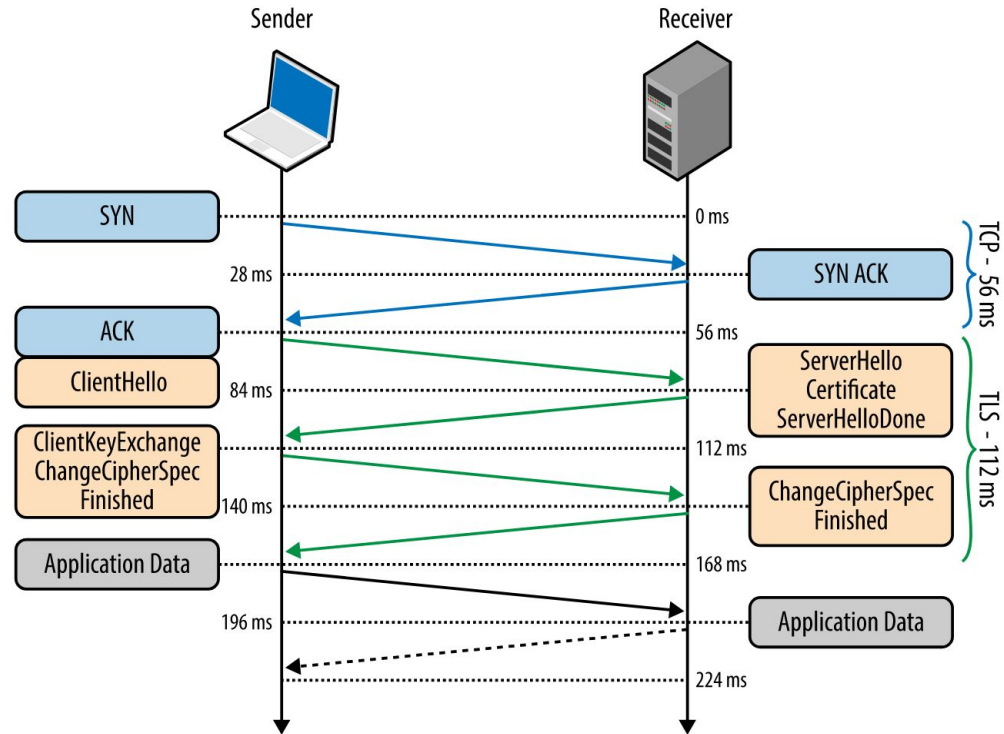
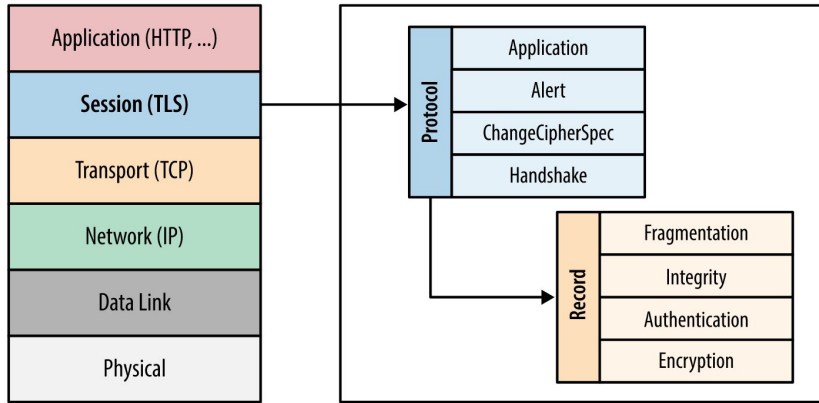


Diffie-Hellman key exchange



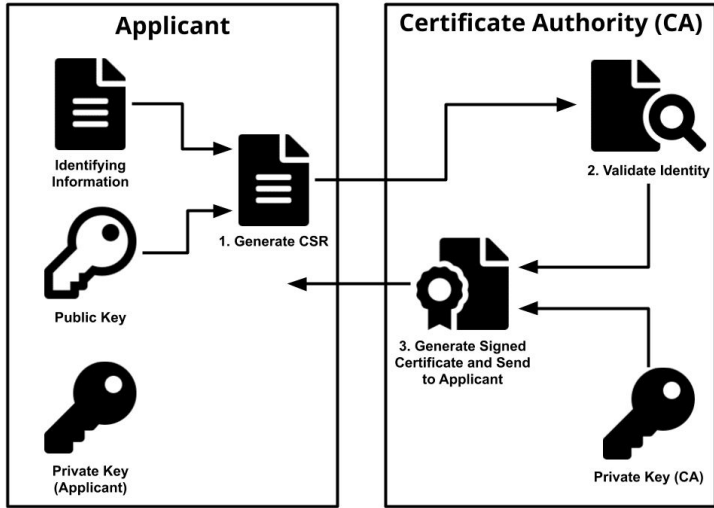
Signing

Transport Layer Security (TLS)

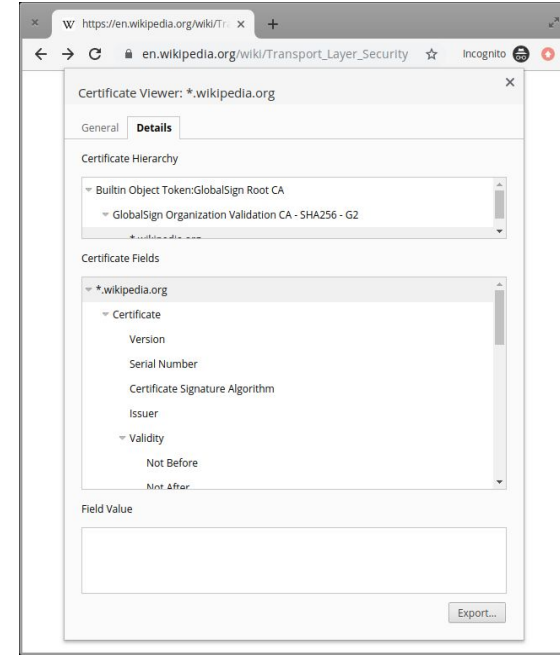
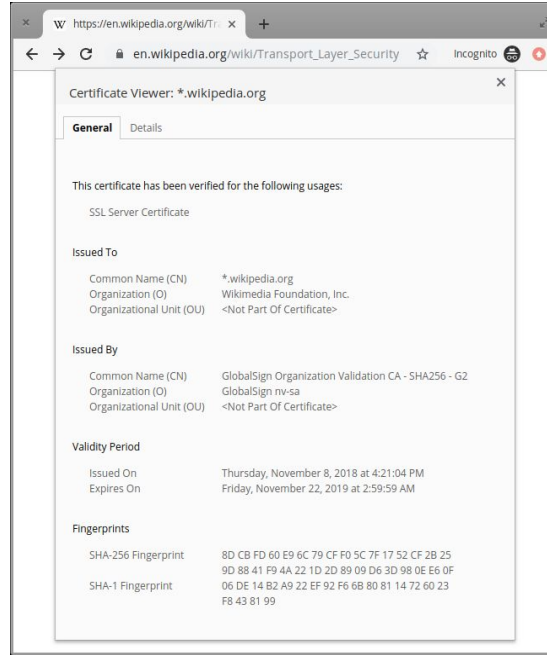


From: <https://hpbn.co/transport-layer-security-tls/>

Anatomy of TLS Certificate

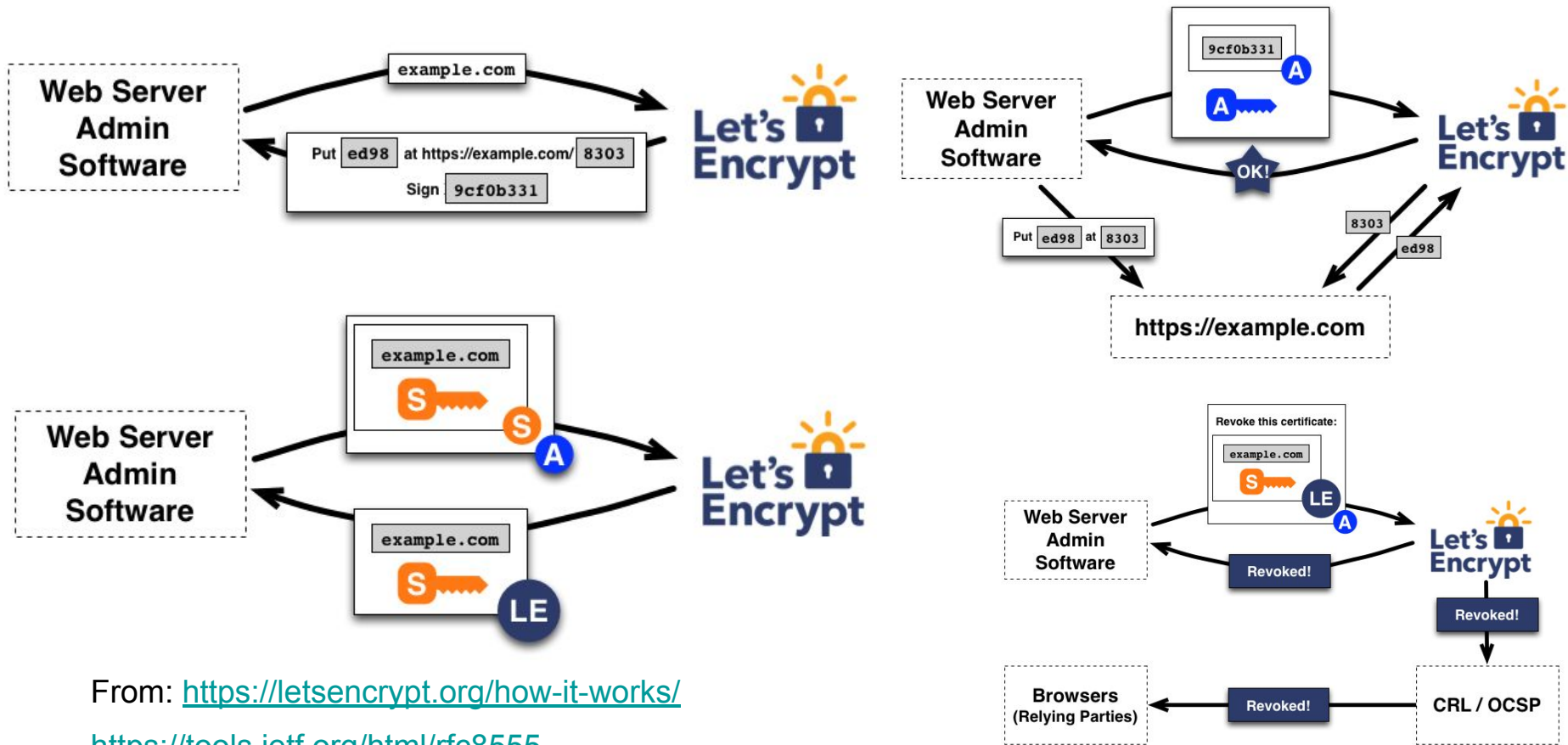


Certificate Issuance from a Certificate Authority (CA)



Certificate Viewer

Automatic Certificate Management Environment (ACME)



From: <https://letsencrypt.org/how-it-works/>
<https://tools.ietf.org/html/rfc8555>