



de.KCD summer school

Technical introduction

Day 4

Berlin Institute of Health Charité - Universitätsmedizin Berlin





Schedule



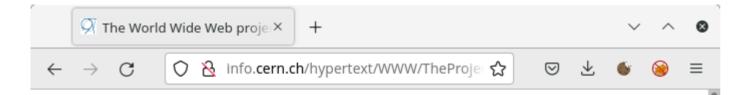
► Certificate architecture



Image by vectorjuice on Freepik







World Wide Web

The WorldWideWeb (W3) is a wide-area <u>hypermedia</u> information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists, Policy, November's W3 news, Frequently Asked Questions.

What's out there?

Pointers to the world's online information, subjects, W3

Ouelle:

http://info.cern.ch/hypertext/WWW/TheProject.html

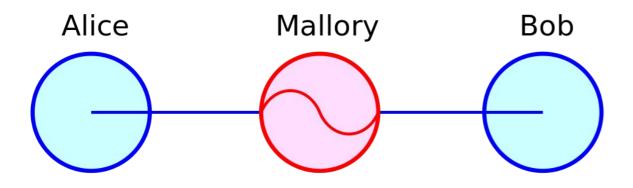
Internet security

- Online services are reachable over the internet
- Default connection protocol is http
- Data is transferred in plain text





Man in the middle attack

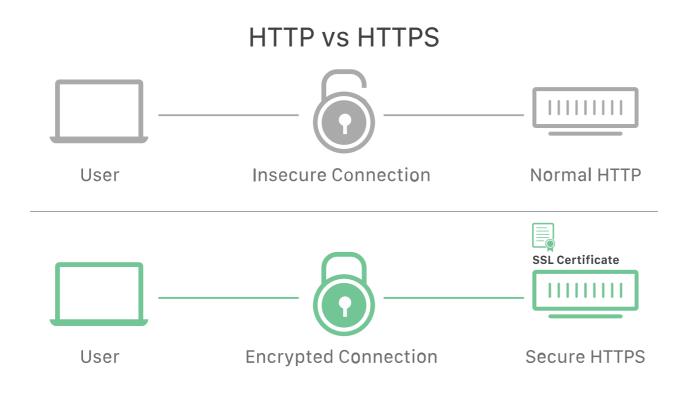


Quelle: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

- An attacker can intersect the plain text communication
- ► The data can be read and changed by the attacker







Quelle: https://www.cloudflare.com/de-de/ssl/

Https with TLS

- Connection between server and browser is encrypted
- Received data must be encrypted before they can be read
- ► The encryption is done via x509 certificates

19.09.2024 de.KCD summer school 5 von 7





Certificate DigiCert Global G2 TLS RSA SHA256 DigiCert Global *.duckduckgo.com Root G2 2020 CA1 Subject Name Country State/Province Pennsylvania Locality Paoli **Organization** Duck Duck Go, Inc. Common Name *.duckduckgo.com Issuer Name US Country **Organization** DigiCert Inc DigiCert Global G2 TLS RSA SHA256 2020 CA1 Common Name Validity Not Before Thu, 02 May 2024 00:00:00 GMT Mon, 25 Nov 2024 23:59:59 GMT Not After

Digital certificates

- ► The public key certificate (x509) proofs the validity of the public key
- Certificate contains:
 - Public key
 - Owners identity
 - Issuer (Certificate Authority or CA)
 - Expiring date





Certificate Authorities (CAs)

- Certificate Authorities (CAs):
 Trusted entities that issue digital certificates to verify online identities.
- Certificate Chain: A hierarchy of trust from end-entity certificates up to root CAs, used by browsers to authenticate identities.
- Public Key Infrastructure (PKI): Manages certificates and encryption, involving CAs, Registration Authorities, and validation mechanisms like CRLs and OCSP.