EP21: Is HTTPs Safe? Also...

THERESA
AUG 27, 2022

In this newsletter, we'll cover the following topics:

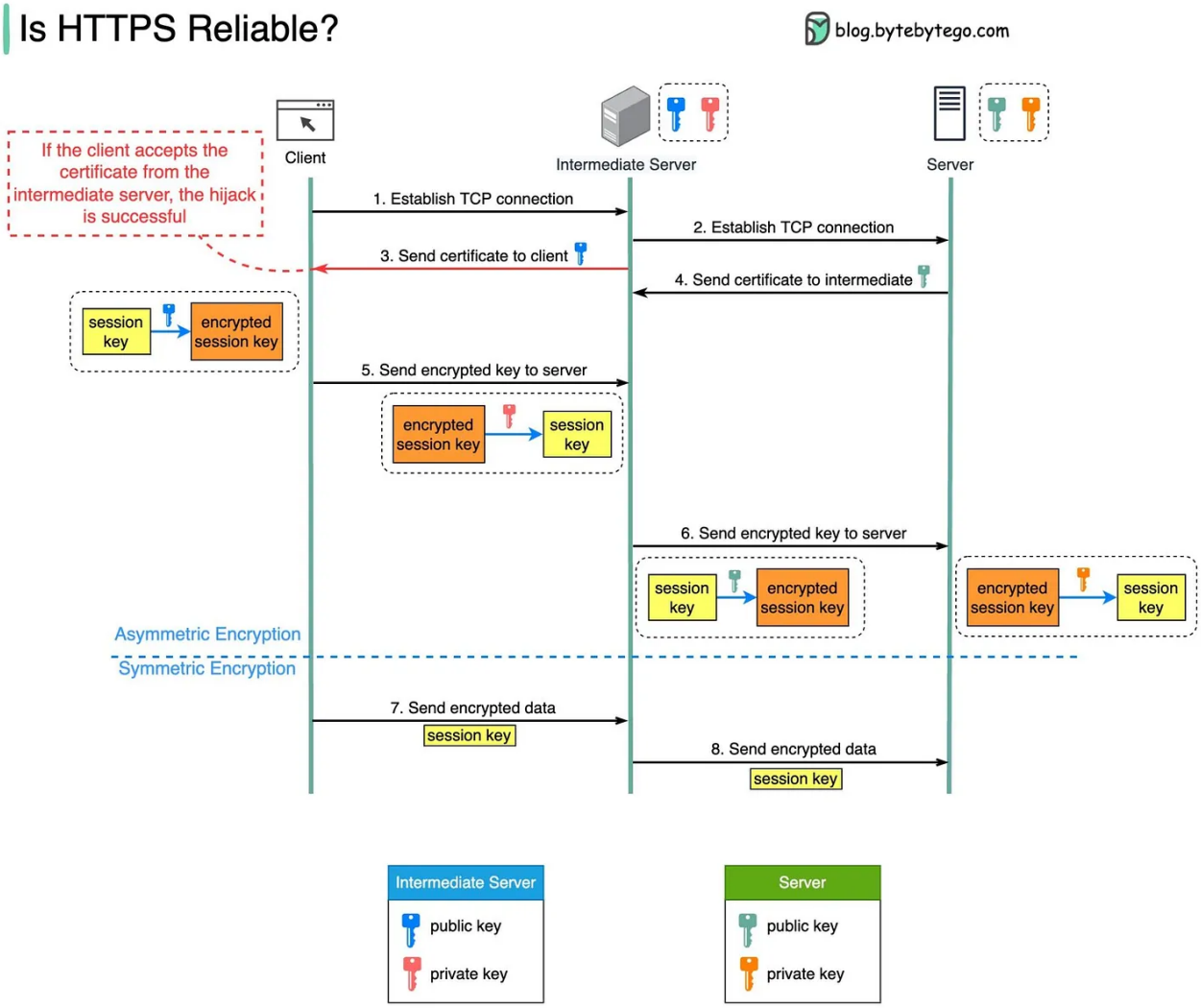
- Reliability of HTTPs
- The CRON Cheatsheet
- Understanding REST API
- ISO standards applied to smart cards

Is HTTPs safe?

If HTTPS is safe, how can tools like Fiddler capture network packets sent via HTTPS?

The diagram below shows a scenario where a malicious intermediate hijacks the packets.

Prerequisite: root certificate of the intermediate server is present in the trust-store.



Step 1 - The client requests to establish a TCP connection with the server. The request is maliciously routed to an intermediate server, instead of the real backend server. Then, a TCP connection is established between the client and the intermediate server.

Step 2 - The intermediate server establishes a TCP connection with the actual server.

Step 3 - The intermediate server sends the SSL certificate to the client. The certificate contains the public key, hostname, expiry dates, etc. The client validates the certificate.

Step 4 - The legitimate server sends its certificate to the intermediate server. The intermediate server validates the certificate.

Step 5 - The client generates a session key and encrypts it using the public key from

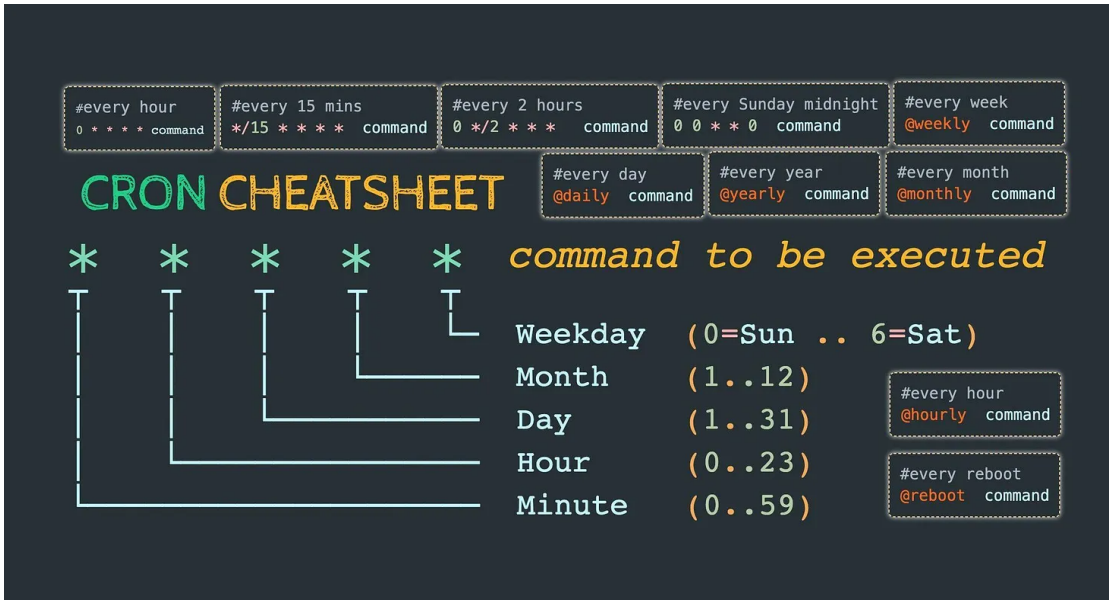
the intermediate server. The intermediate server receives the encrypted session key and decrypts it with the private key.

Step 6 - The intermediate server encrypts the session key using the public key from the actual server and then sends it there. The legitimate server decrypts the session key with the private key.

Steps 7 and 8 - Now, the client and the server can communicate using the session key (symmetric encryption.) The encrypted data is transmitted in a secure bi-directional channel. The intermediate server can always decrypt the data.

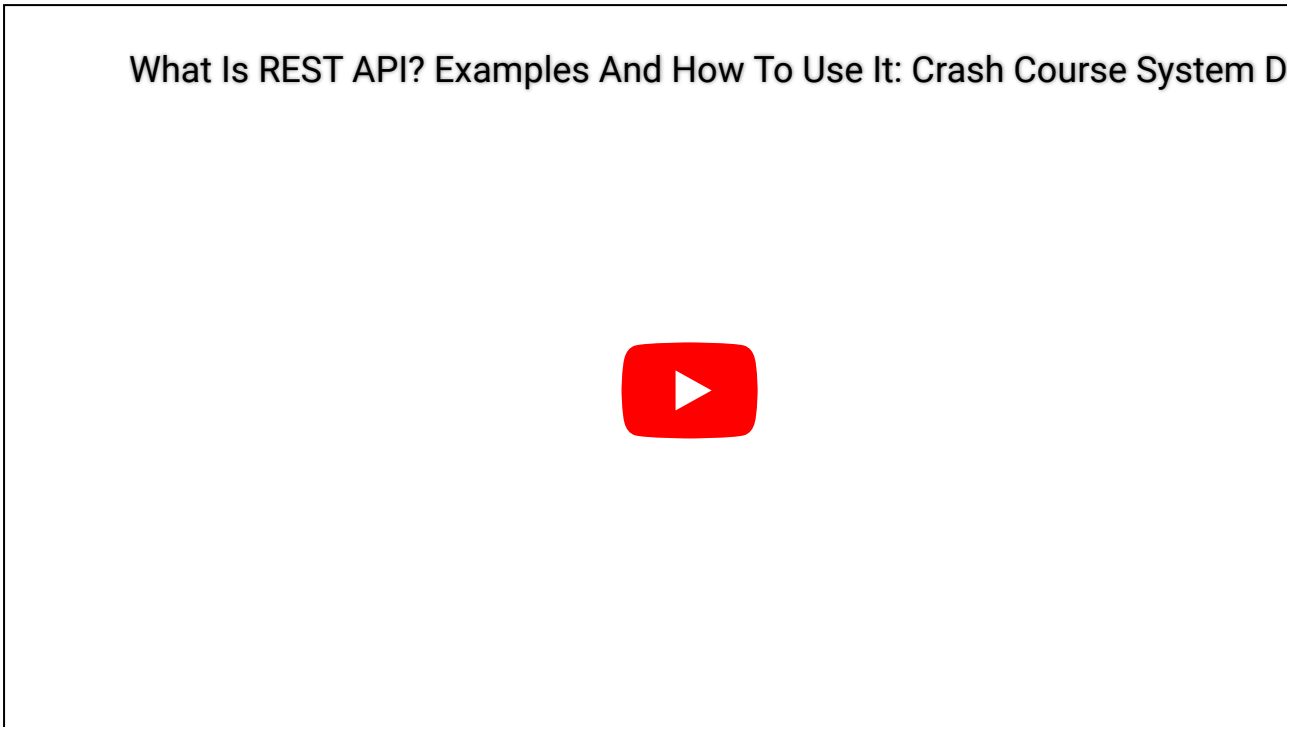
CRON Cheatsheet

CRON cheatsheet by @Handbook on Twitter.



What Is REST API?

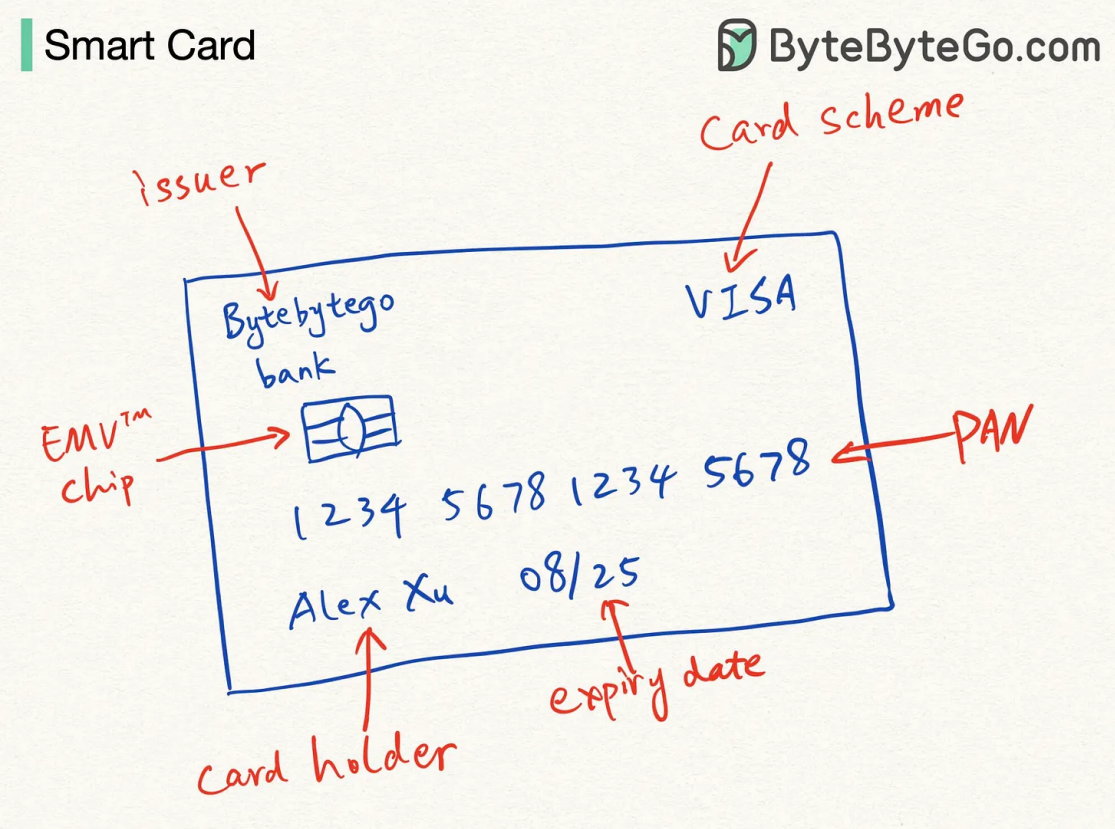
REST is the most common communication standard between computers over the internet. What is it? Why is it so popular?



The ISO standards of smart cards

Do you know how to explain to a 10-year-old what all the symbols/numbers on the smart credit card mean?

Do you know that smart credit cards have ISO standards? Let's take a look:



- ISO 7813: defines the card size and shape
- ISO 7816: defines smart card integrated chips, such as the EMV (Europay, Mastercard, and Visa) chip
- ISO 7812: defines the PAN (permanent account number) structure
- ISO 7811: defines the magnetic stripe details
- ISO 14443: defines contactless card

Thanks for making it this far!

If you want to learn more about System Design, check out our books:

[Paperback edition]

[Digital edition]

105 Likes

7 Comments

Write a comment...

? ! Writes ? ! ? Aug 27, 2022

Your prerequisite to showing how HTTPS is unsafe is that you've already agreed to give your information to the third party.

The answer to the question, is HTTPS safe?, is yes.

This section is misleading at best. The caveats are only: CA hacks (very unlikely) or access to your machine to install certificates.

LIKE (8) REPLY SHARE

Fai C Feb 23

HSTS further improve HTTPS. There is not perfect security in the world, at the end if we need to transact, we need trust.

LIKE REPLY SHARE

5 more comments...