TLS 1.3 Adoption in the Wild

Sajjad Arshad

Some slides are borrowed from the paper published in NDSS 2017
“**The Security Impact of HTTPS Interception**”

About me

- Fourth year PhD student at Northeastern University in **Boston**
  - Winter is Coming!
- Studying Web security/privacy problems by large-scale measurements
- Working with Eric "Ekr" Rescorla as part of Advanced Technology Lab

HTTPS

- Secure Socket Layer (SSL)
  - Developed by Netscape
  - 1.0 (1993) , 2.0 (1995), 3.0 (1996)
  - Deprecated!

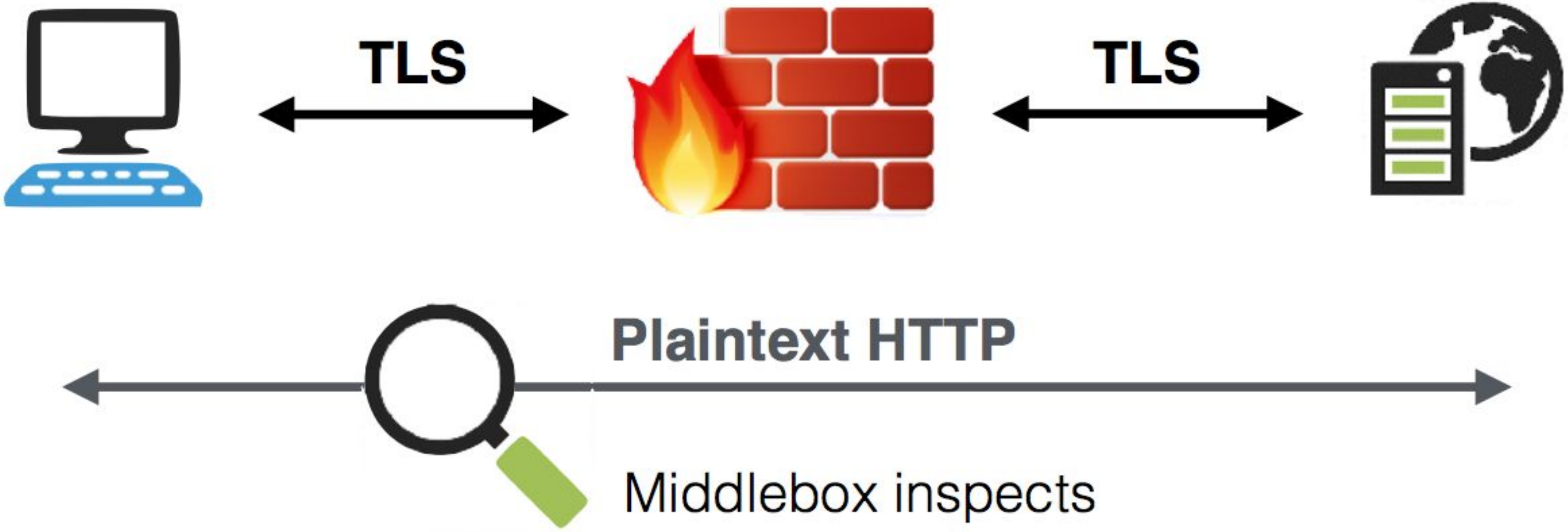
- Transport Layer Security (TLS)
  - TLS 1.0 (1999) was an upgrade of SSL 3.0
  - TLS 1.1 (2006)
  - TLS 1.2 (2008) is now supported by more than 86% of HTTPS-enabled websites
  - **TLS 1.3 (2017)** is faster and more secure than its predecessor
    - Firefox and Chrome enabled it by default
    - But it was disabled due to incompatible middleboxes such as Blue Coat web proxy

Middleboxes

- Some middleboxes (e.g., Firewalls, Antiviruses, Web Proxies) intercept HTTPS connections to inspect the content

Borrowed from “The Security Impact of HTTPS Interception (NDSS 2017)”

HTTPS Interception



TLS

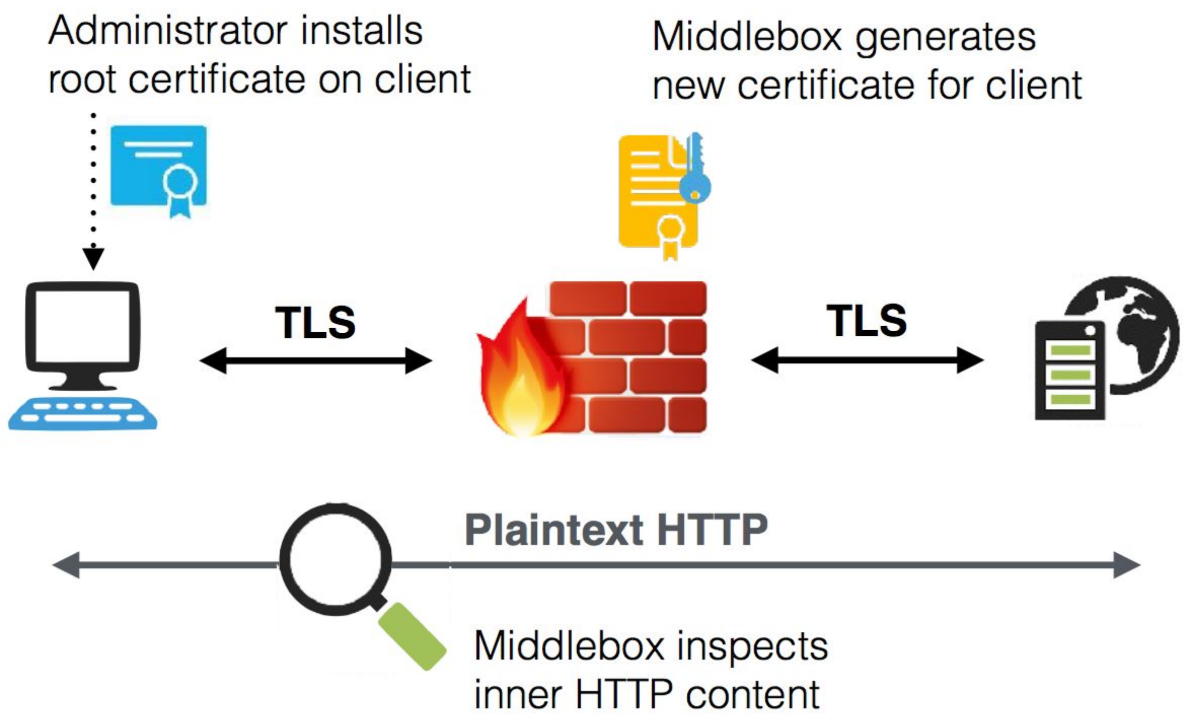
TLS

Plaintext HTTP

Middlebox inspects inner HTTP content

Borrowed from "The Security Impact of HTTPS Interception (NDSS 2017)"

HTTPS Interception



Administrator installs root certificate on client
Middlebox generates new certificate for client
TLS
TLS
Plaintext HTTP
Middlebox inspects inner HTTP content

Borrowed from "The Security Impact of HTTPS Interception (NDSS 2017)"

Experiment

- Developed a Firefox add-on that makes XHR requests to some known websites
    - Change the TLS preferences accordingly
    - Connect to a server NOT supporting TLS 1.3
    - Connect to a server supporting TLS 1.3
    - If the first connection succeeded and the second connection failed, we have a problem!

- Shipped the add-on to 20% of Firefox Beta users

- Collected the results using Telemetry platform

Preliminary Results

- 991,740 clients participated in the experiment
  - The experiment failed for 3,933 clients
- 297,541 (~30%) of the clients had a third-party root certificate installed
- 24,431 (~2.5%) of the clients faced errors initiating a TLS 1.3 connection
  - They succeeded initiating TLS 1.2 connections though
- We observed 31 different error types:
  - NS_ERROR_NET_INTERRUPT (The connection was established, but the data transfer was interrupted)
  - SSL_ERROR_ACCESS_DENIED_ALERT (Peer received a valid certificate, but access was denied.)
  - SSL_ERROR_RX_UNEXPECTED_APPLICATION_DATA (SSL received an unexpected Application Data record.)
  - SEC_ERROR_UNKNOWN_ISSUER (Peer's Certificate issuer is not recognized.)
  - SSL_ERROR_RX_RECORD_TOO_LONG (SSL received a record that exceeded the maximum permissible length.)

Ongoing Work

- Constantly improving the add-on
  - Gathering more reliable data
  - Minimizing the experiment’s side-effects on the users
- Providing more fine-grained access on the TLS configurations to developers
  - Modifying Firefox code base
  - Running the experiments without changing the preferences (no side-effects)

Thank You

Questions?