TLS Information Leakage: CRIME Attack

Noemi Glaeser

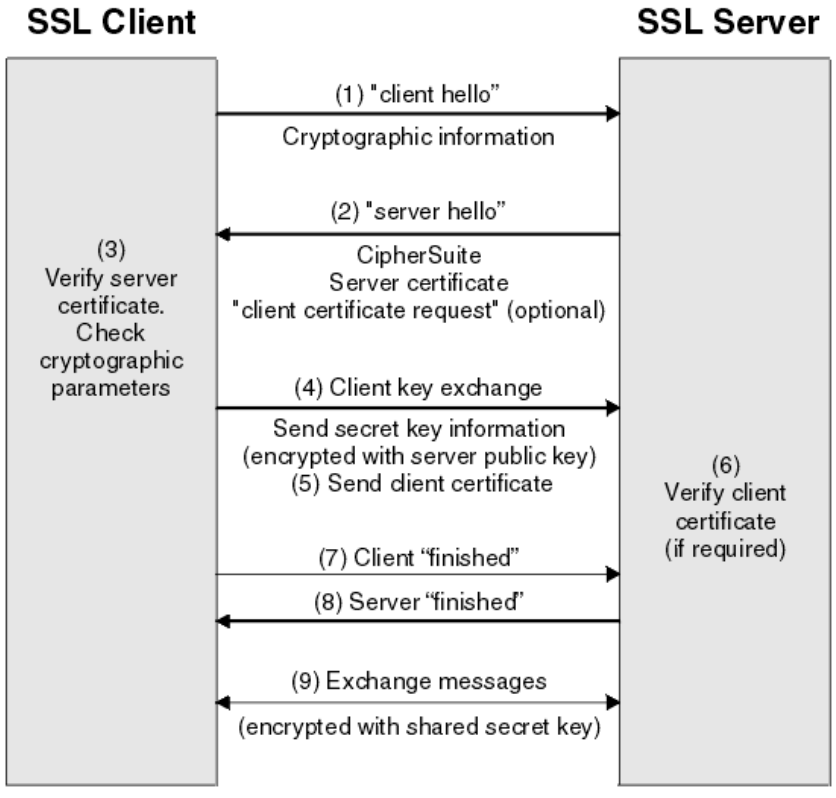
CMSC 818O

October 1, 2019

Overview

Transport Layer Security (TLS)

- Authenticity
  - Verify client and server identities through certificates
- Confidentiality
  - Agree on cipher suite and key



Cookies

- Websites have no memory
- Solution: cookies
  - Small amounts of information stored on your computer by websites, e.g., session ID, login state
  - If session cookies are compromised, your session can be hijacked
- Cookies are sent in every packet header

TLS Browser Compression

- Browsers implemented compression of packets before encryption (i.e., at the SSL/TLS level)
  - Replace repeated byte sequences with pointers

Example

"foobarfoo" $\rightarrow$ "[0]bar[0]"
dict $\rightarrow$ [0: "foo"]

TLS Browser Compression

- **Idea:** If we can inject plaintext, we can use how that affects the length of the encrypted packet to guess the cookie

TLS Browser Compression

Example

Original packet:

"...`Cookie: secret=helloworld`..."

length $= 59$

TLS Browser Compression

Example (Incorrect guess)

Modified packet:

"...Cookie: secret=helloworld...Cookie: secret=x"

$\Longrightarrow$ "...[0]helloworld...[0]x"

length = 47

TLS Browser Compression

Example (Correct guess)

Modified packet:

"...Cookie: secret=helloworld...Cookie: secret=h"

$\Longrightarrow$ "...[0]elloworld...[0]"

length = 45

Compression Ration Info-leak Made Easy (CRIME)

- Client-side attack
- **Main idea:** exploit the packet length property, which isn't hidden, using compression as an attack vector
- Guess one byte at a time and compare packet lengths
  - Can be done in 4-6 tries per byte with a binary search approach
    - Base64: $2^6 = 64$ possible byte values
    - Hexadecimal: $2^4 = 16$ possible byte values
- Various approaches to inject the byte guess:
  - POST body (JS with cross-site scripting attck)
  - cross-domain requests
  - insert into the query string in GET request
  - `<img>` tags
  - probably many others...

Demo

Mitigation

- Turn off SSL compression
  - latest browsers don't even offer it
- The usual: don't access sketchy sites or click on odd links

Other TLS Attacks

- Browser Reconnaisance and Exfiltration via Adaptive Compression of Hypertext (BREACH)
  - Same thing but leveraging HTTP compression
- Browser Exploit Against SSL/TLS (BEAST)
  - Exploits implementation of cipher block chaining (CBC) mode in TLS 1.0
- Lucky 13
  - Timing attack

Conclusion

- As much as stuff gets broken in real life, it's hard to break it on purpose in a specific way
- It's important to pick the right tools from the beginning
- Document your troubleshooting

Questions?