Kleptography in Authentication Protocols: Why is it Still Possible?

Carina Heßeling [1] Jörg Keller [1] Sebastian Litzinger [1]

[1]Faculty of Mathematics and Computer Science, FernUniversität in Hagen, Germany

Network Steganography

- hiding the existence of information
- covert sender (CS) and covert receiver (CR) practise secret communication by hiding messages in overt communication of an established system
- multiple scenarios are conceivable (see *Possibilities for Covert Sender and Receiver Positioning*)

Kleptography

- value from a black box cryptographic device or software is assumed to be random
- in reality, it contains encrypted content when the device is compromised and serves as CS

TLS 1.3

- widely used protocol to secure network connections
- handshake uses random nonce in all versions (see *TLS 1.3 Handshake*)
- opens path to kleptography attacks
- known for 25 years (Young & Yung 1997)
- attack and possible cure presented 16 years ago (Golebiewski et al. 2006)
- practical attack presented 4 years ago (Janovsky et al. 2018)
- TLS still not rectified

Possible Reasons

1. not widely deployed
2. unclear how to exploit
3. unclear how to cure
4. steganographic bandwidth too small

⇒ 1–3 do not apply to TLS

TLS Handshake Covert Channel Bandwidth Estimation

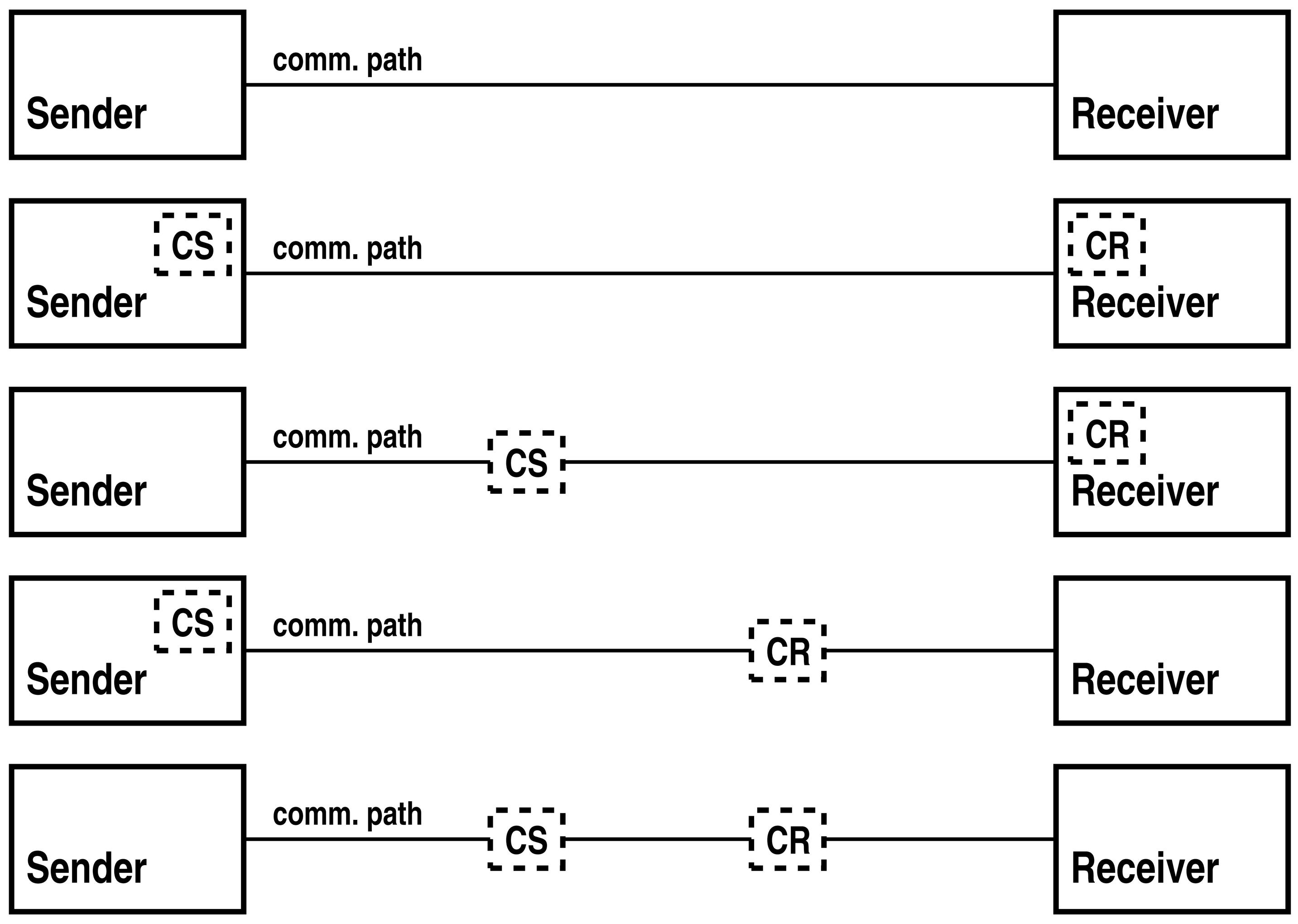
- 32 byte nonce
- hourly handshake and 10 servers

⇒ >60 kbit/day, non-negligible

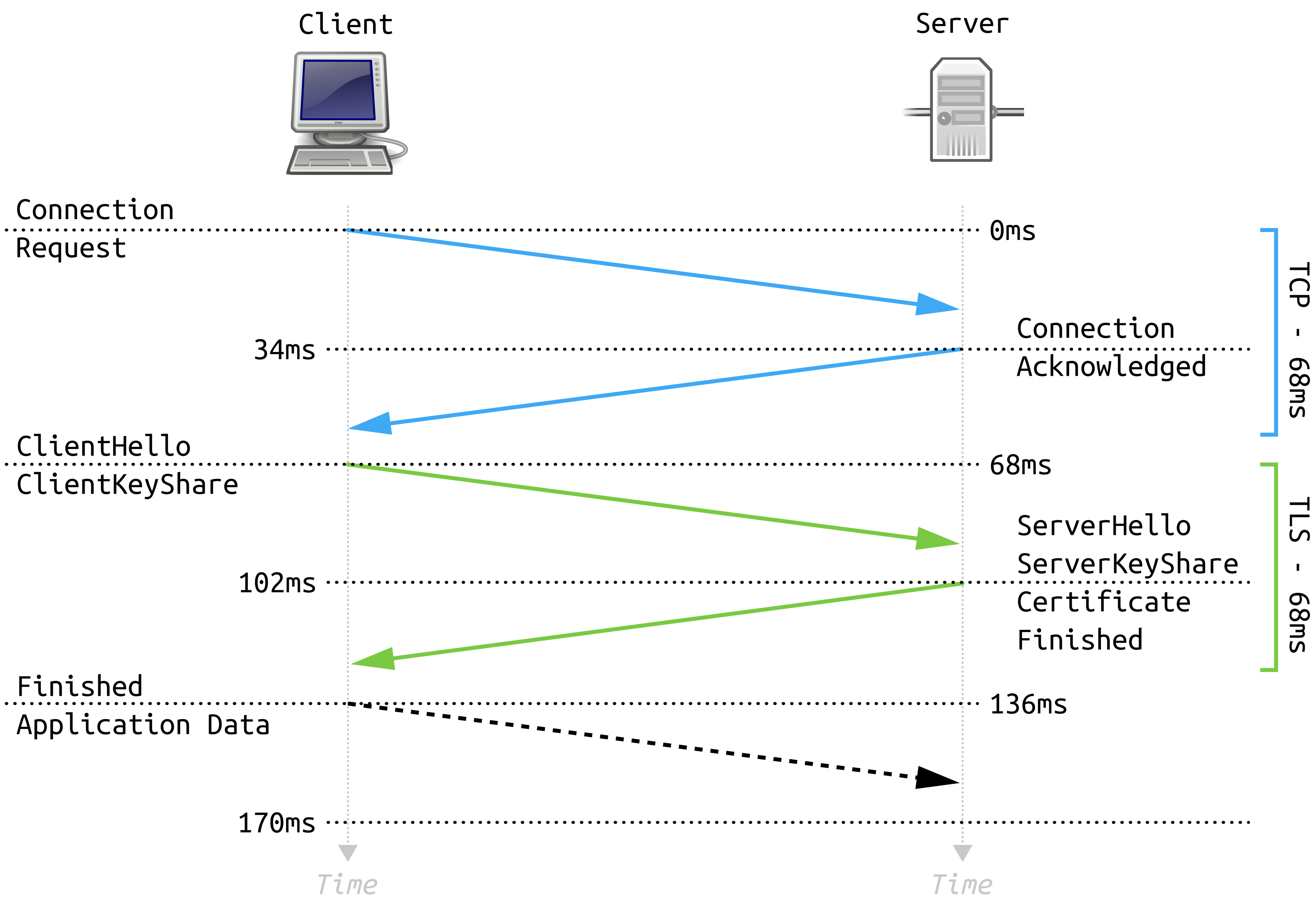
Conclusions

- TLS should be secured against attack
- OCRA and HTTP/1.1 digest access authentication protocols possibly affected

Possibilities for Covert Sender and Receiver Positioning



TLS 1.3 Handshake



ClientHello

```
struct {
   ProtocolVersion legacy_version = 0x0303;
   Random random;
   opaque legacy_session_id<0..32>;
   CipherSuite cipher_suites<2..2^16-2>;
   opaque legacy_compression_methods<1..2^8-1>;
   Extension extensions<8..2^16-1>;
} ClientHello;
```

ServerHello

```
struct {
   ProtocolVersion legacy_version = 0x0303;
   Random random;
   opaque legacy_session_id_echo<0..32>;
   CipherSuite cipher_suite;
   uint8 legacy_compression_method = 0;
   Extension extensions<6..2^16-1>;
} ServerHello;
```

References

[1] Zbigniew Golebiewski, Miroslaw Kutylowski, and Filip Zagórski. Stealing secrets with SSL/TLS and SSH - kleptographic attacks. In *Cryptology and Network Security, 5th International Conference, CANS 2006, Suzhou, China, December 8-10, 2006, Proceedings*, volume 4301 of *Lecture Notes in Computer Science*, pages 191–202, Berlin, 2006. Springer.

[2] Adam Janovsky, Jan Krhovjak, and Vashek Matyas. Bringing kleptography to real-world TLS. In *Information Security Theory and Practice - 12th IFIP WG 11.2 International Conference, WISTP 2018, Brussels, Belgium, December 10-11, 2018, Revised Selected Papers*, volume 11469 of *Lecture Notes in Computer Science*, pages 15–27, Berlin, 2018. Springer.

[3] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[4] Adam L. Young and Moti Yung. Kleptography: Using cryptography against cryptography. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 62–74, Berlin, 1997. Springer.