March 15, 2021
Cryptography

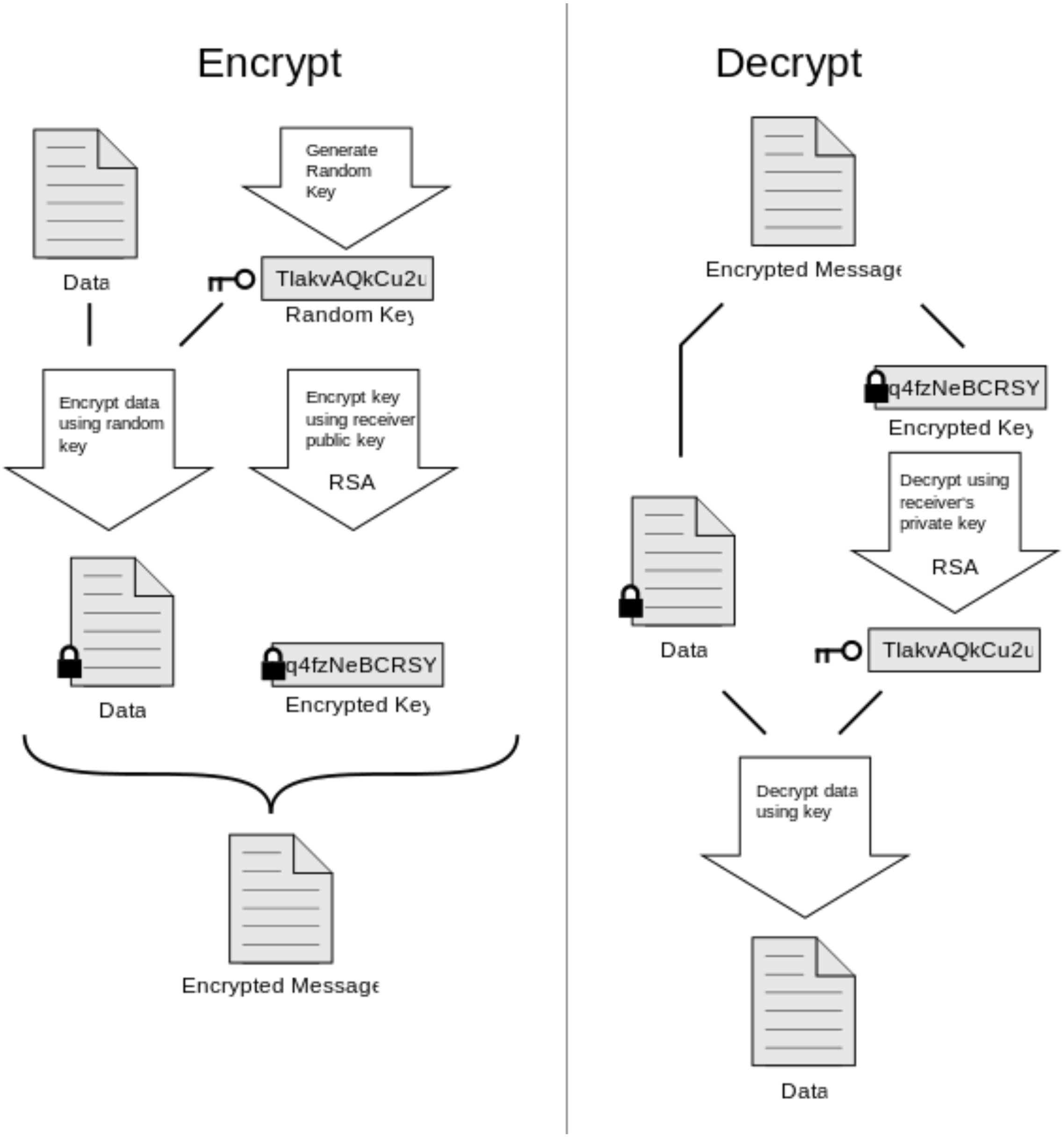
- Today
  - Encryption
  - TLS
- Assignments
  - Project
    - Outline: Due Monday, Mar 29
  - Lab 2
    - Due Monday, Apr 5

Encryption

- Cyphers
- Hashing
- Key Exchange

Pretty Good Privacy

- PGP – Phil Zimmerman
- Why?
- Mechanism


Encrypt
Data
Generate Random Key
TlakvAQkCu2u
Random Key
Encrypt data using random key
Encrypt key using receiver public key
RSA
Data
q4fzNeBCRSY
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
q4fzNeBCRSY
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TlakvAQkCu2u
Decrypt data using key
Data

History

- **Secure Sockets Layer (SSL)** developed by Netscape (remember them?) in 1995
  - Version 1 never released
  - Version 2 incorporated into Netscape Navigator 1.1
  - Microsoft fixes vulnerabilities in SSLv2 and introduces Private Communications Technology (PCT) protocol
  - Netscape overhauls SSLv2, fixing some more security issues, and releases SSLv3
- IETF takes over and releases **Transport Layer Security (TLS)**, a non-interoperable upgrade to SSLv3
  - current version is TLS version 1.3

SSL/TLS Message Types

- Handshake
- Alerts
- Change cipher spec
- Data

Overview

- Alice (client) initiates conversation with Bob (server)
- Bob sends Alice his certificate
- Alice verifies certificate
- Alice picks a random number S and sends it to Bob, encrypted with Bob’s public key
- Both parties derive key material from S
- Client and server exchange encrypted and integrity-protected data

Cryptographic Parameters

- Generated from
  - Rc
  - Rs
  - the master secret K
- *Values* to be generated
  - client authentication and encryption keys
  - server authentication and encryption keys
- Generator functions: ki = gi(K,Rc,Rs)

Cipher Suites

- Includes encryption
  - algorithm, key length, block mode, and integrity checksum algorithm
- ~90 defined cipher suites
- Alice gives Bob a list of supported cipher suites; Bob makes final choice
- Run on a terminal: openssl ciphers -v

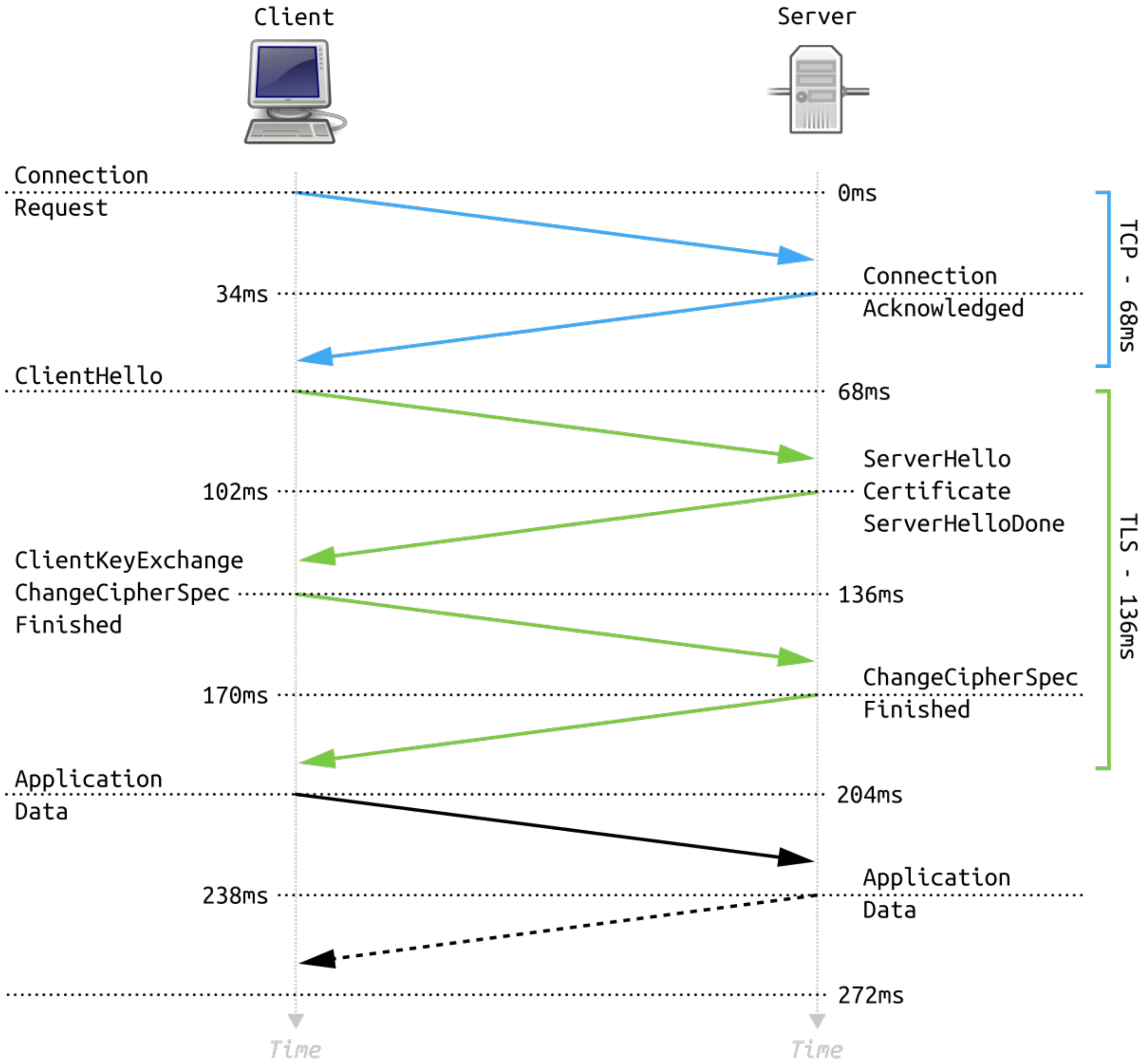
SSLv2 Known Vulnerabilities

- Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)
- SSLv2 doesn't block disabled ciphers (CVE-2015-3197)
- Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703)

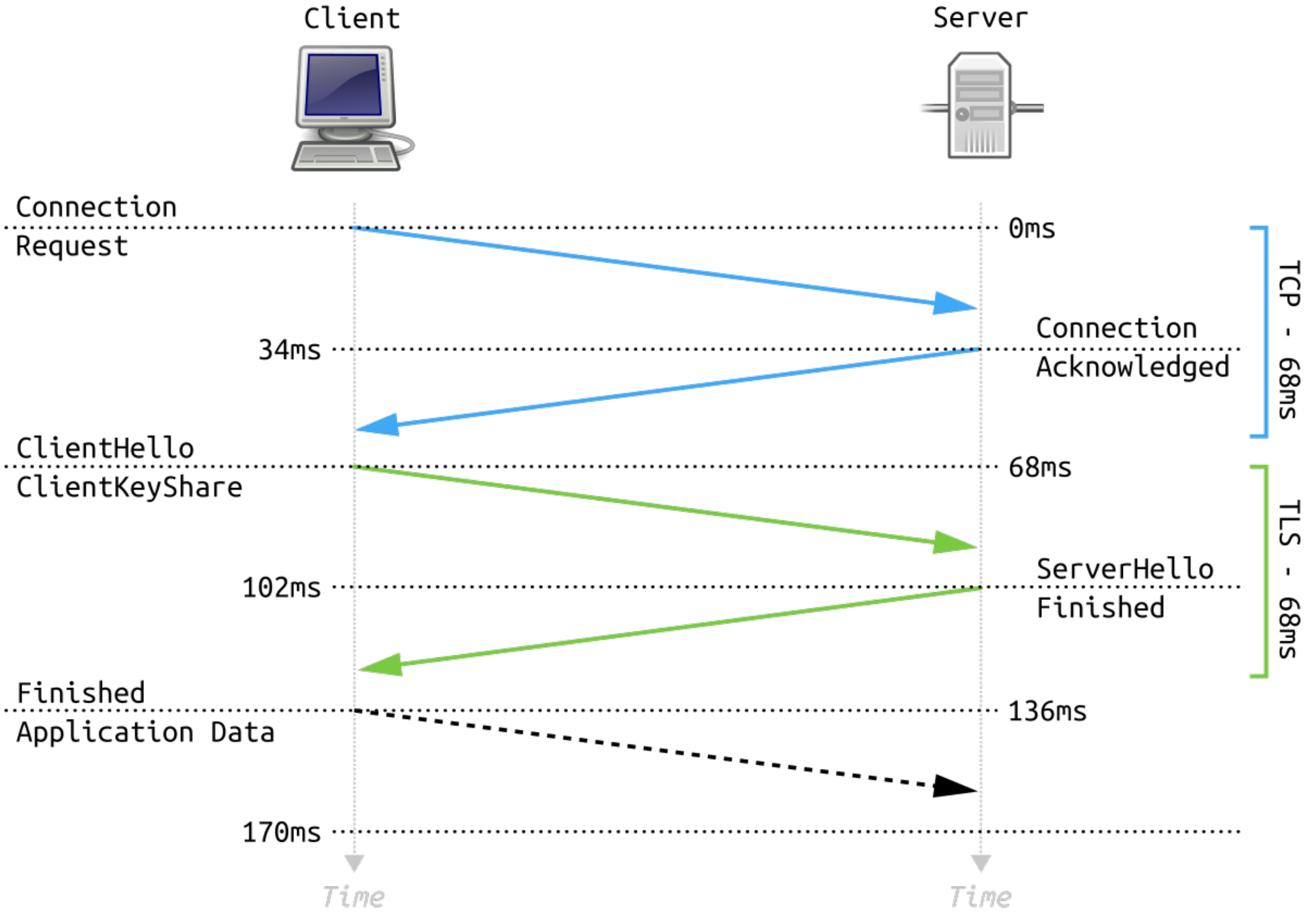
Handshake cost

- Per-session master secret derived using expensive public key crypto

TLS 1.2 Handshake



TLS 1.3 Handshake



Session Resumption

- Allows Alice and Bob to construct new encryption & integrity keys using previously shared pre-master secret (S)
  - uses session-id to continue SSL session over multiple connections
  - avoids having to repeat public-key crypto operations
- If either Alice or Bob don’t remember master secret key, new handshake is required

SSL/TLS in the Real World

- Most (modern) browsers support SSLv3, TLS 1.2
- Client authentication very rare **-- WHY?**
- Implementations:
  - HTTP (80) → HTTPS (443)
  - POP (110) → POP3S (995)
  - IMAP (143) → IMAPS (993)
  - SMTP (25) → SMTP with SSL (465)
  - FTP (20,21)→ FTPS (989,990)
  - Telnet (23) → Telnets (992)

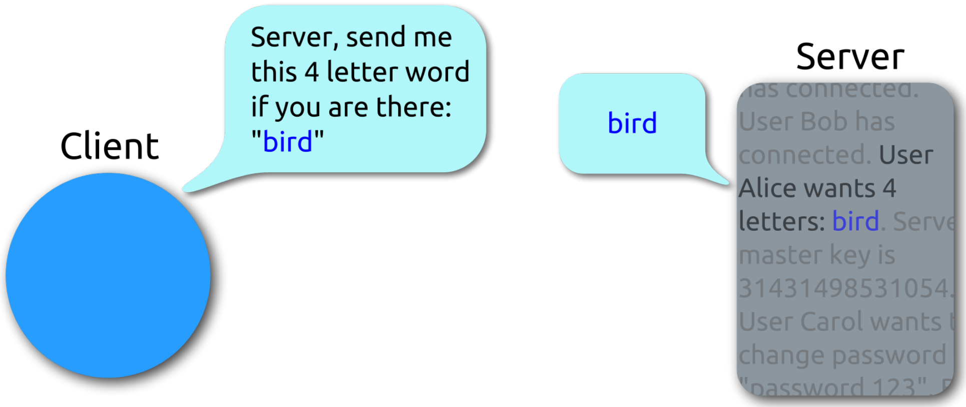
Heartbleed Exploit

- Heartbeat
  - February 2021, RFC 6520
  - Client sends short message and its length
  - Service echo’s message back
  - Allows connections to be maintained

- OpenSSL Library
  - Standard open source SSL/TLS library

Heartbleed

Heartbeat – Normal usage



Client

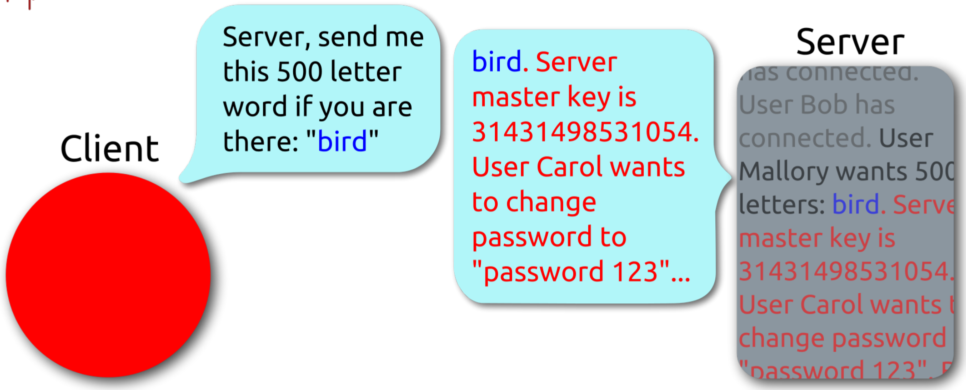
Server, send me this 4 letter word if you are there: "bird"

bird

Server

as connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Heartbeat – Malicious usage



Client

Server, send me this 500 letter word if you are there: "bird"

bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...

Server

as connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P