CSE 484 / CSE M 584 (Spring 2012)

Protocol Rollback and Network Security

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

- Protocol Rollback Attacks (in SSL)
- Network security

- HW2
- Lab 3
- HW 3 (EC)

What is SSL / TLS?

- Transport Layer Security (TLS) protocol, version 1.2
  - De facto standard for Internet security
  - "The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications"
  - In practice, used to protect information transmitted between browsers and Web servers (and mail readers and ...)
  - https://datatracker.ietf.org/wg/tls/
- Based on Secure Sockets Layers (SSL) protocol, version 3.0
  - Same protocol design, different algorithms
- Ubiquitously deployed in commercial Web browsers

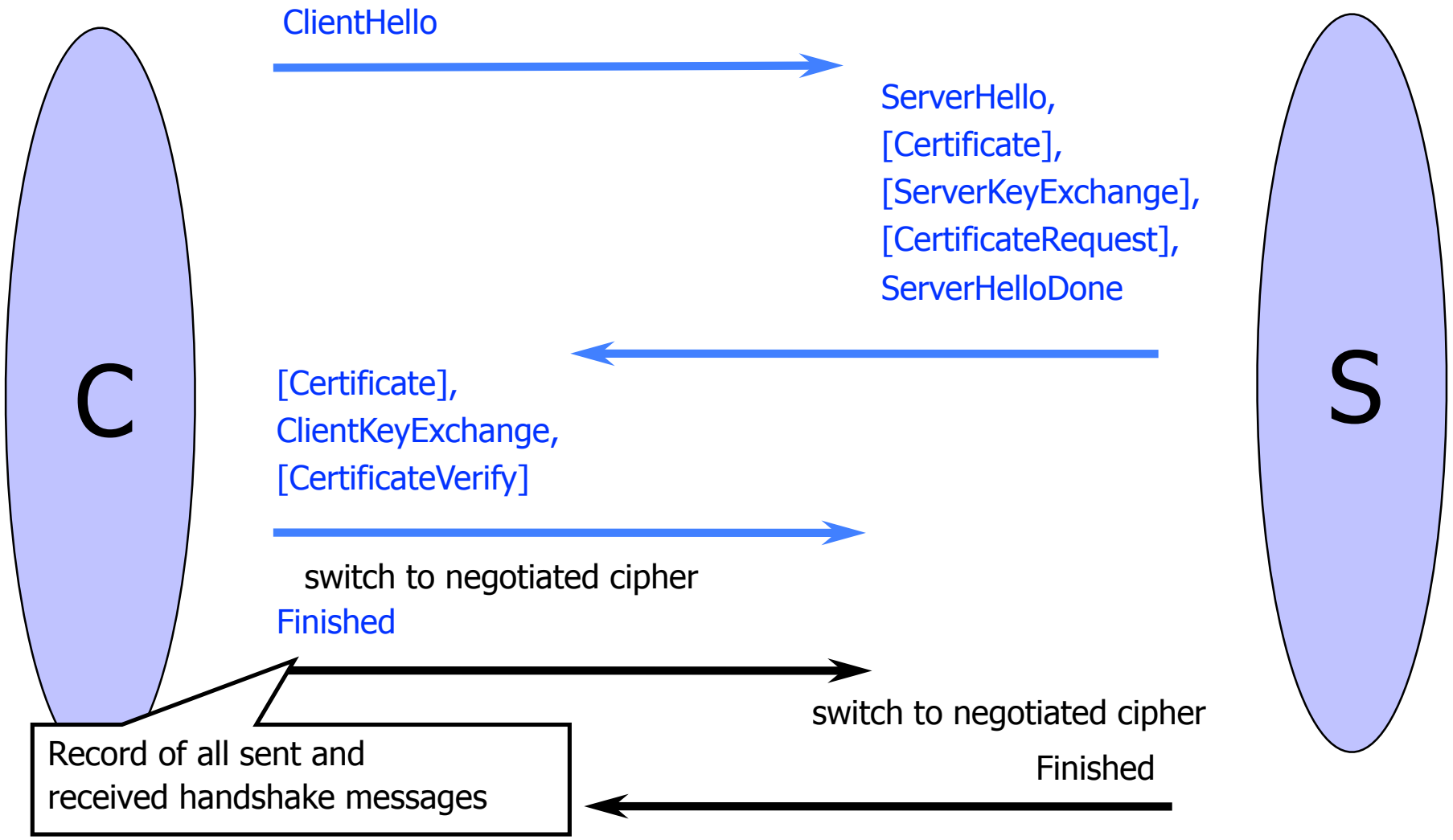
TLS Basics

- TLS consists of two protocols
  - Familiar pattern for key exchange protocols
- Handshake protocol
  - Use public-key cryptography to establish a shared secret key between the client and the server
- Record protocol
  - Use the secret key established in the handshake protocol to protect communication between the client and the server
- We will focus on the handshake protocol

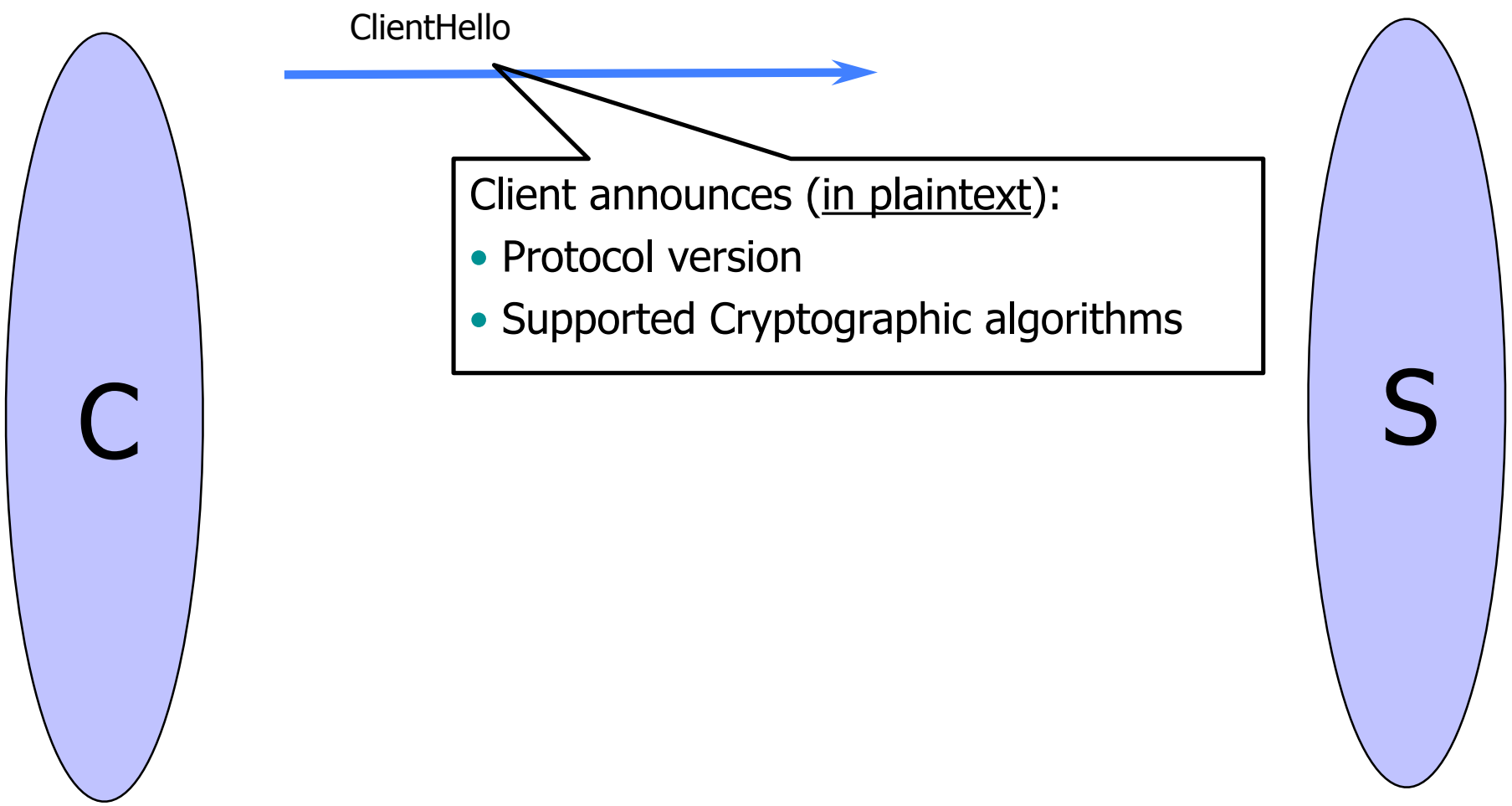
TLS Handshake Protocol

- Two parties: client and server
- Negotiate version of the protocol and the set of cryptographic algorithms to be used
  - Interoperability between different implementations of the protocol
- Authenticate client and server (optional)
  - Use digital certificates to learn each other's public keys and verify each other's identity
- Use public keys to establish a shared secret

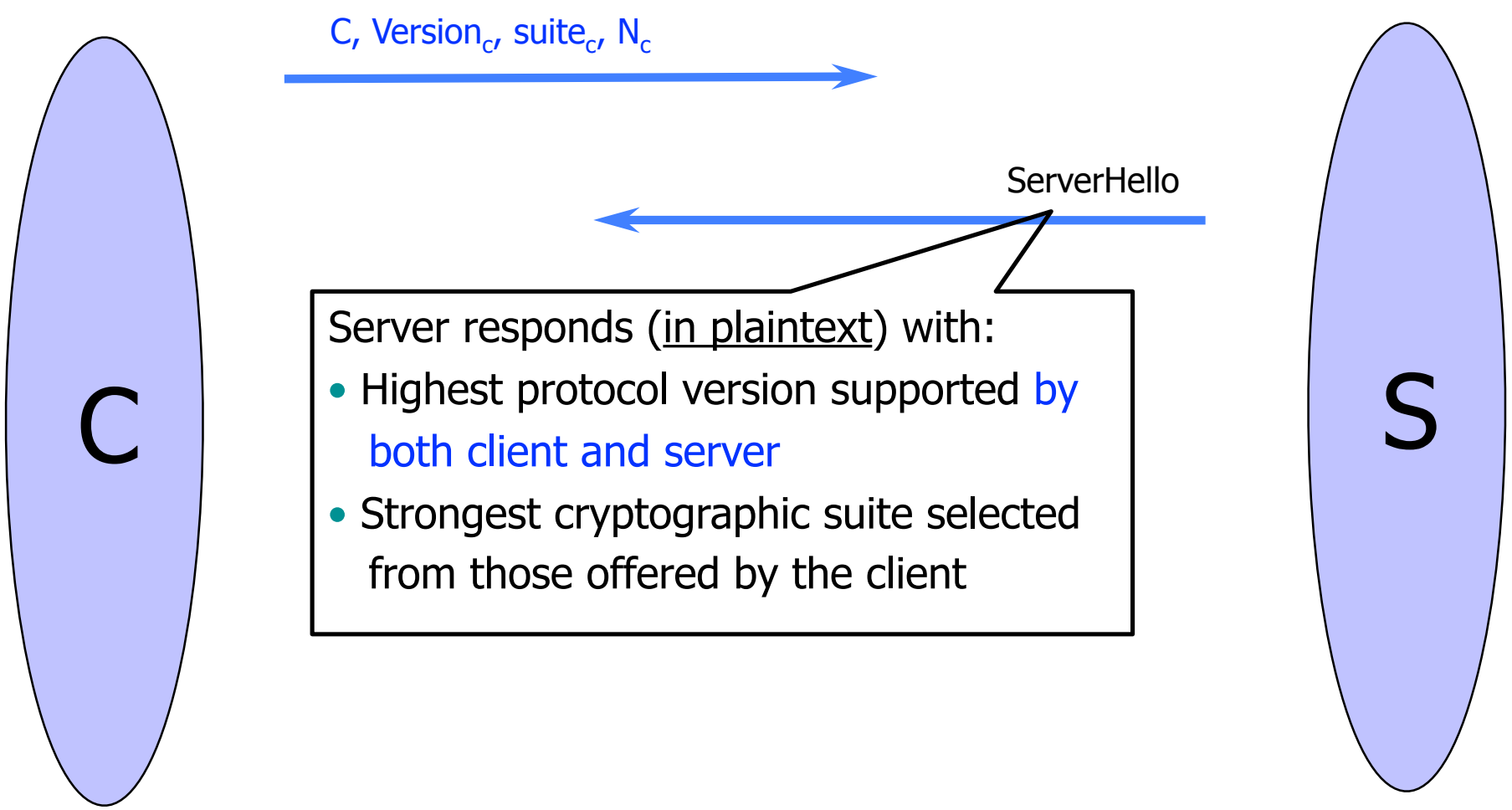
Handshake Protocol Structure



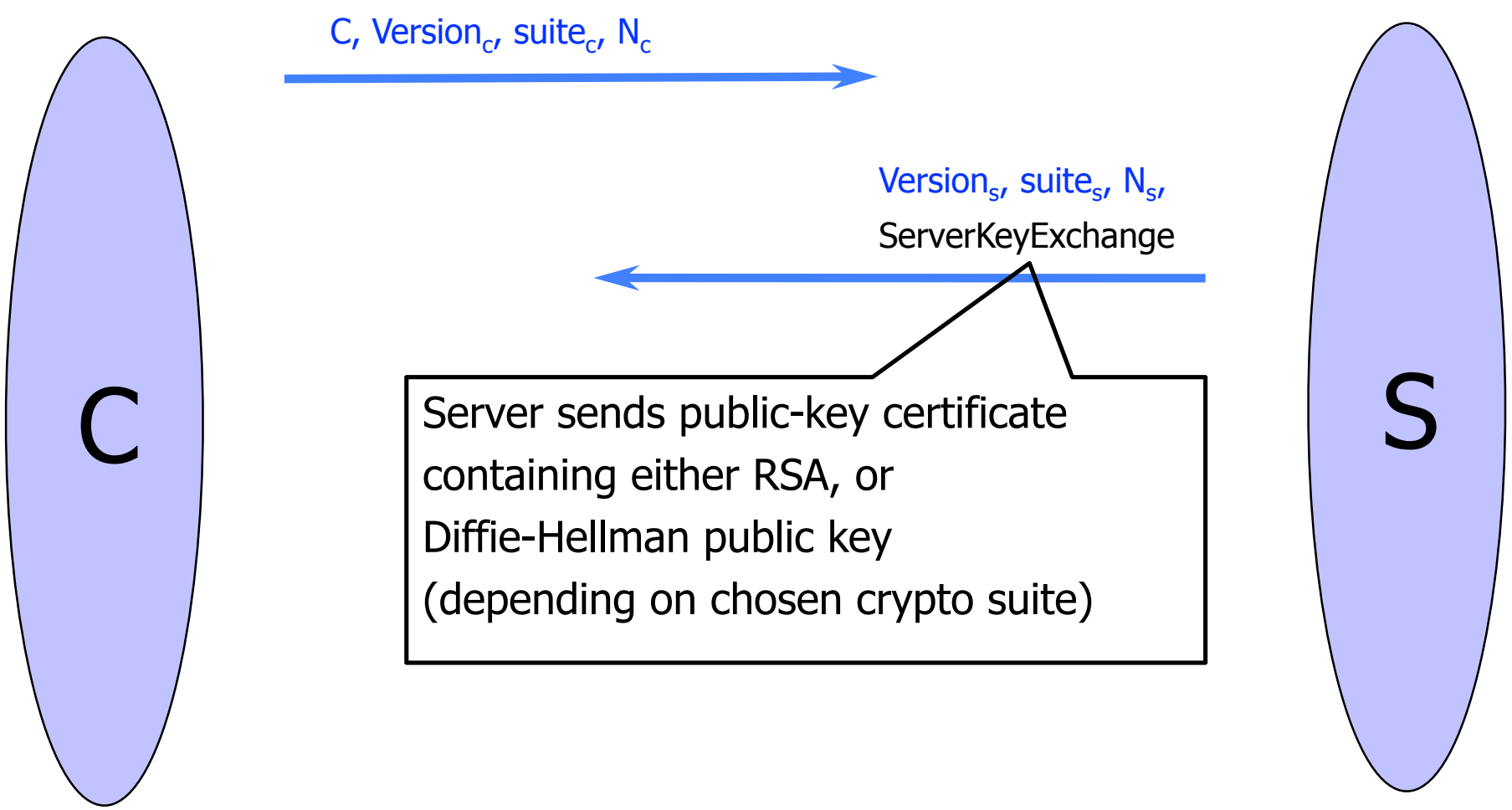
ClientHello



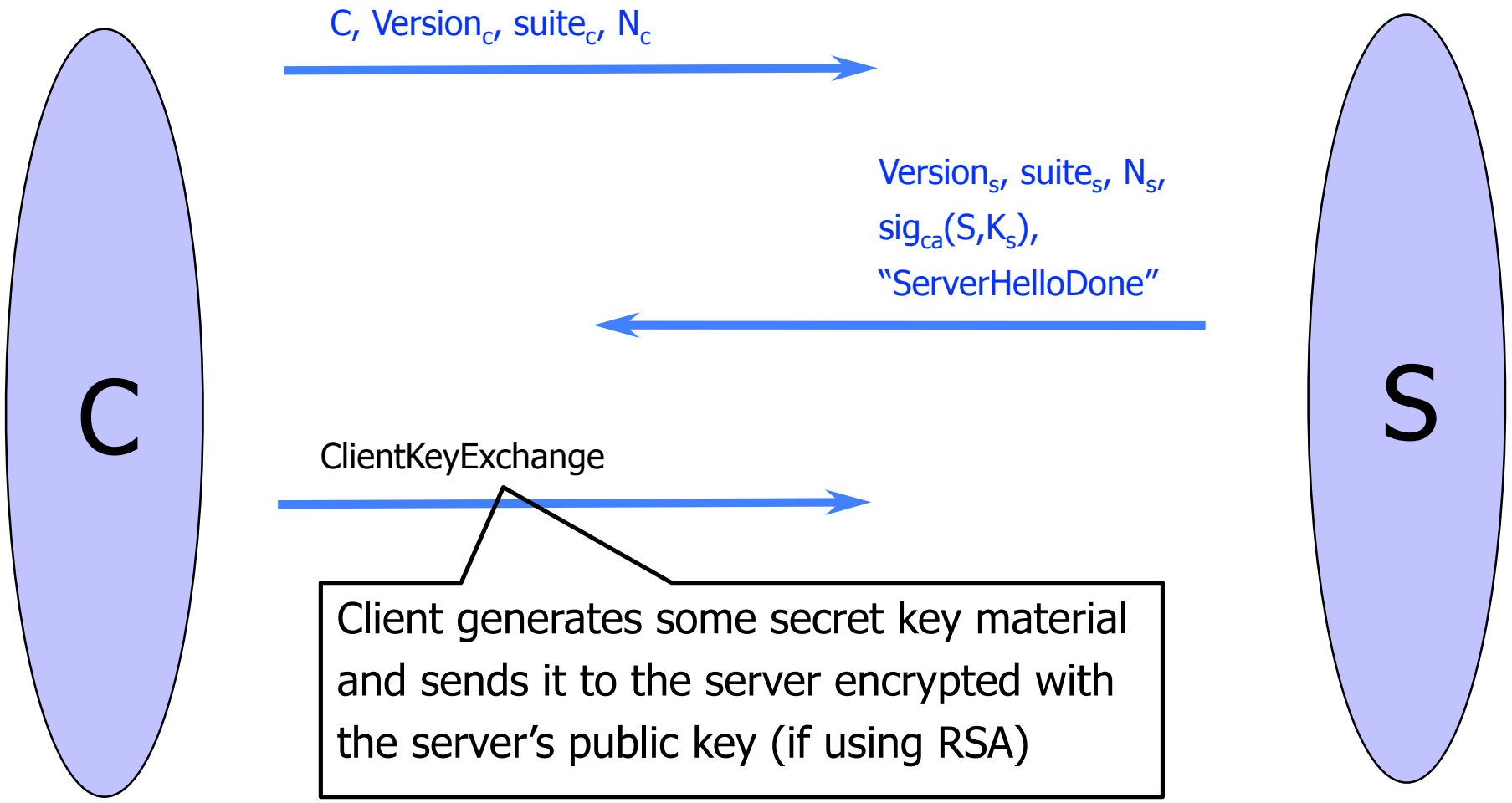
ServerHello



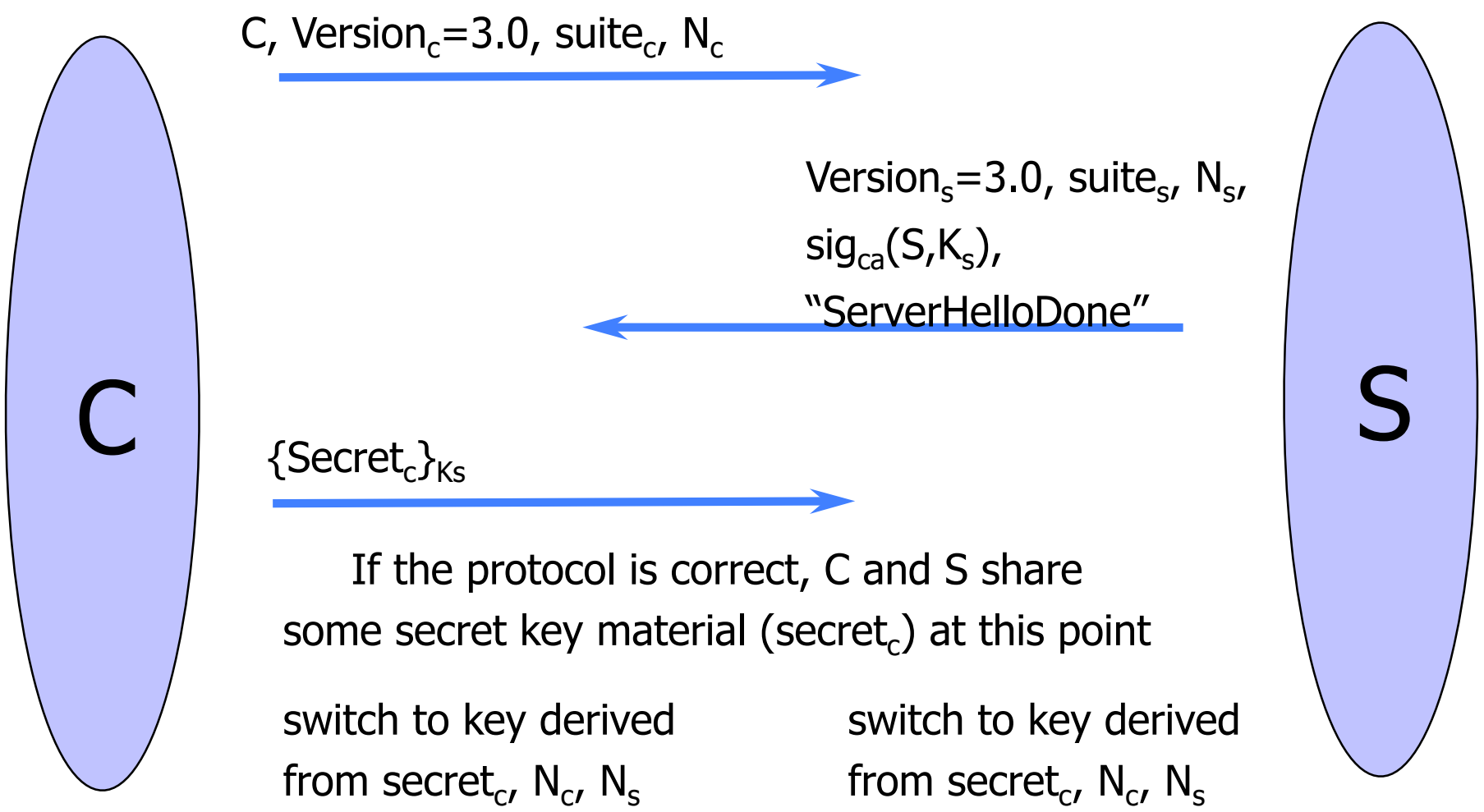
ServerKeyExchange



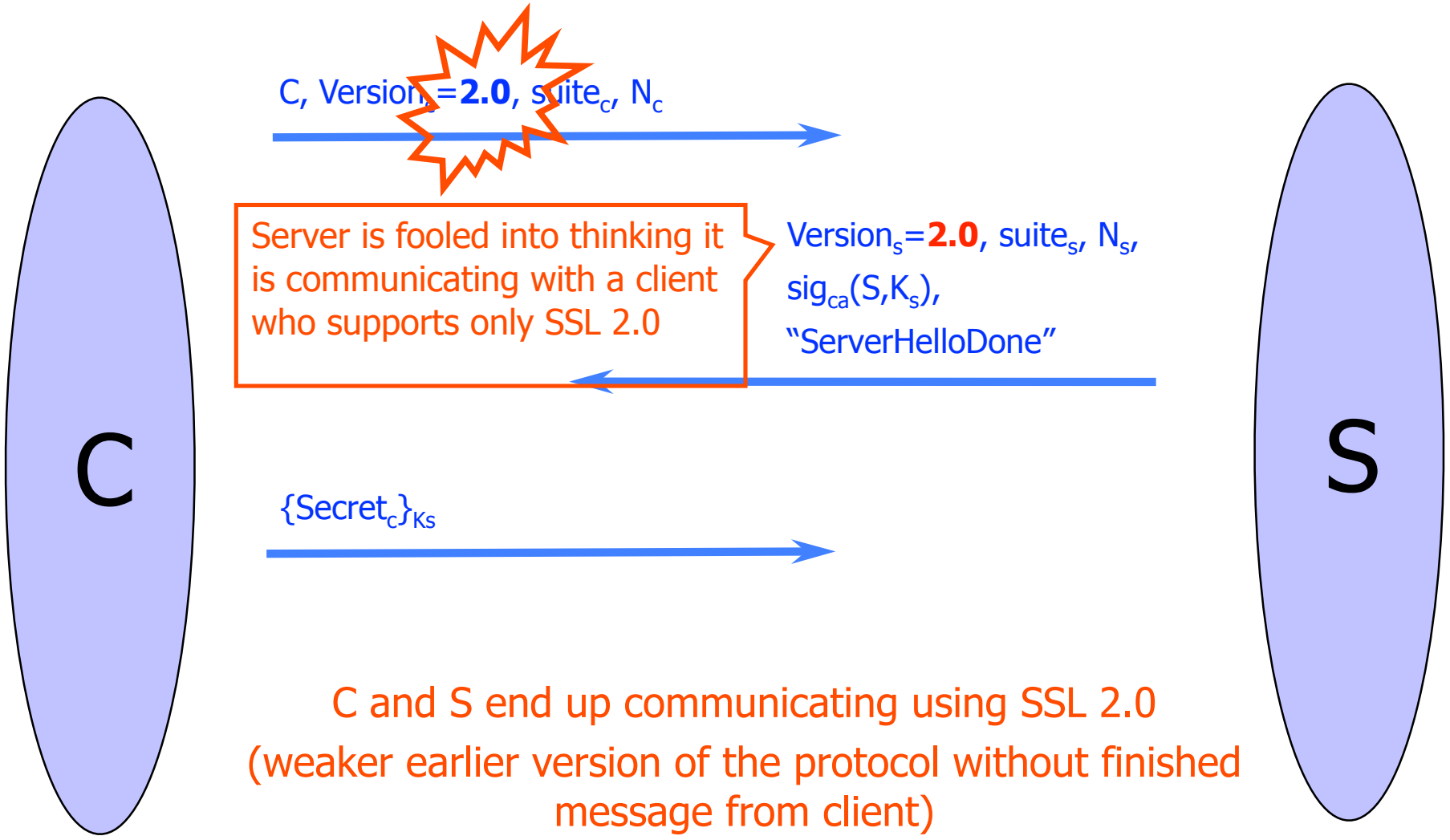
ClientKeyExchange



"Core" SSL 3.0 Handshake (Not TLS)



Version Rollback Attack



C and S end up communicating using SSL 2.0

(weaker earlier version of the protocol without finished message from client)

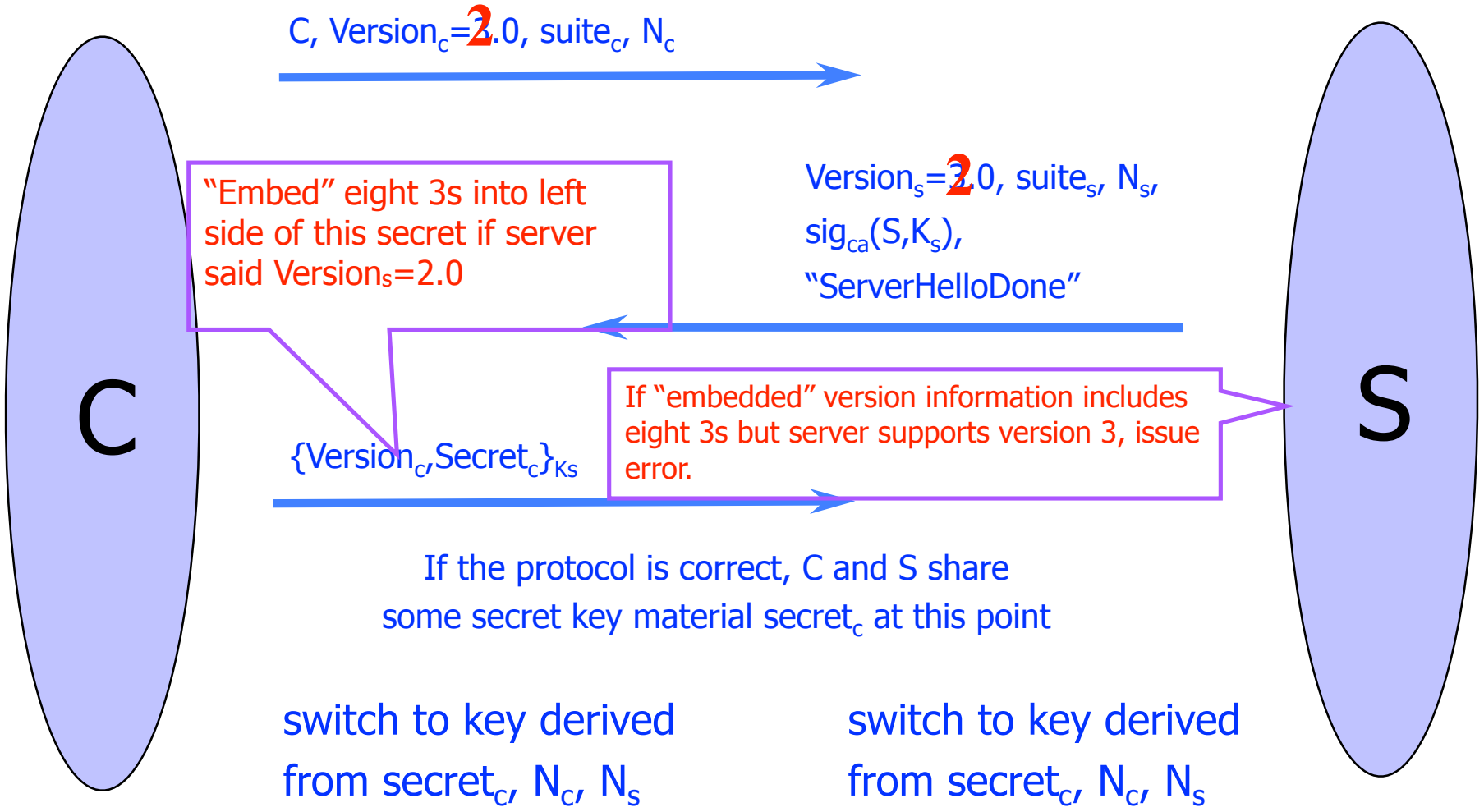
SSL 2.0 Weaknesses (Fixed in 3.0)

- Cipher suite preferences are not authenticated
  - "Cipher suite rollback" attack is possible
- SSL 2.0 uses padding when computing MAC in block cipher modes, but padding length field is not authenticated
  - Attacker can delete bytes from the end of messages
- MAC hash uses only 40 bits in export mode
- No support for certificate chains or non-RSA algorithms, no handshake while session is open

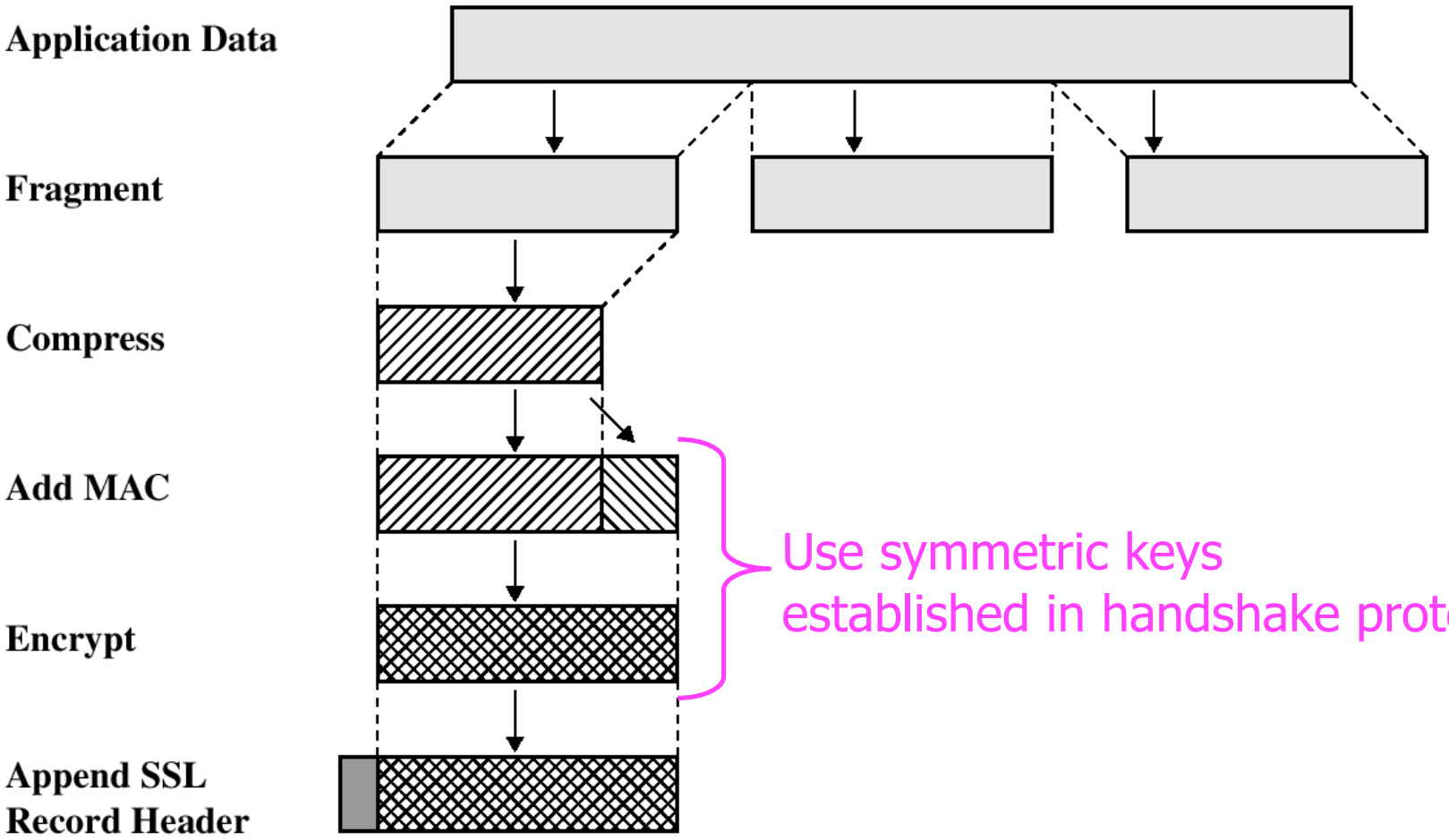
Protocol Rollback Attacks

- Why do people release new versions of security protocols? Because the old version got broken!
- New version must be backward-compatible
  - Not everybody upgrades right away
- Attacker can fool someone into using the old, broken version and exploit known vulnerability
  - Similar: fool victim into using weak crypto algorithms
- Defense is hard: must authenticate version in early designs
- Many protocols had "version rollback" attacks
  - SSL, SSH, GSM (cell phones)

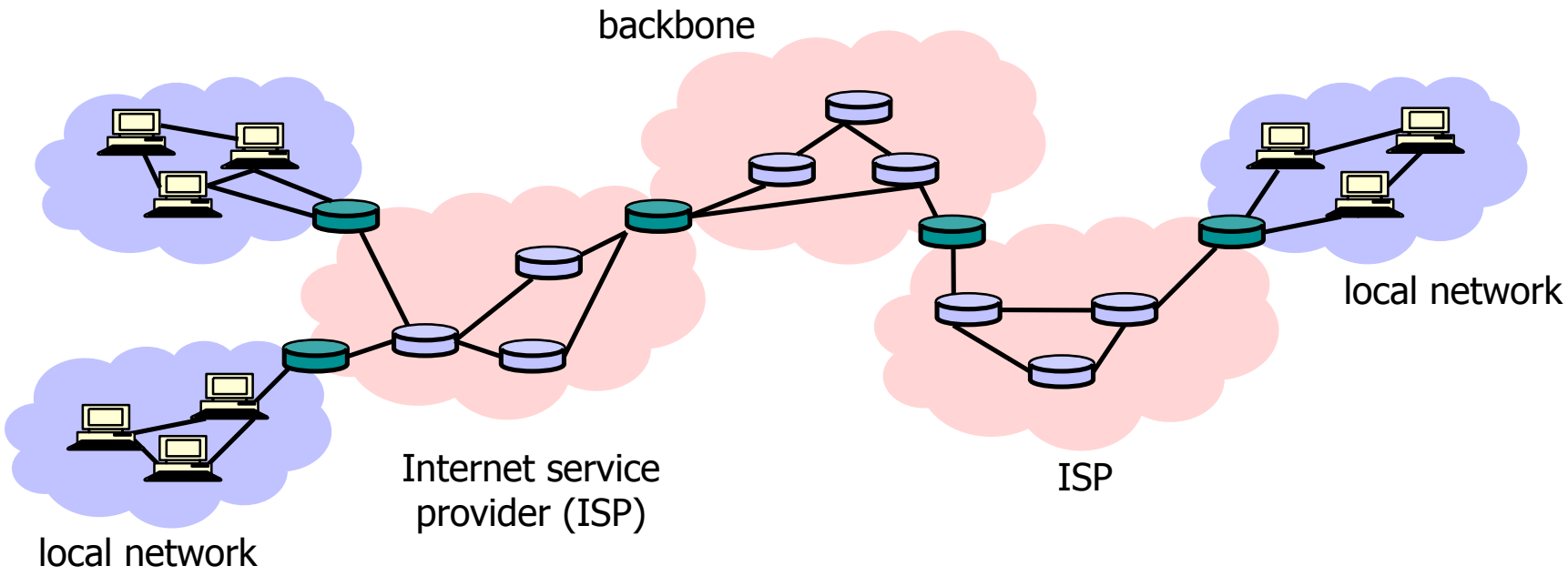
Version Check in SSL 3.0 (Approximate)



SSL/TLS Record Protection

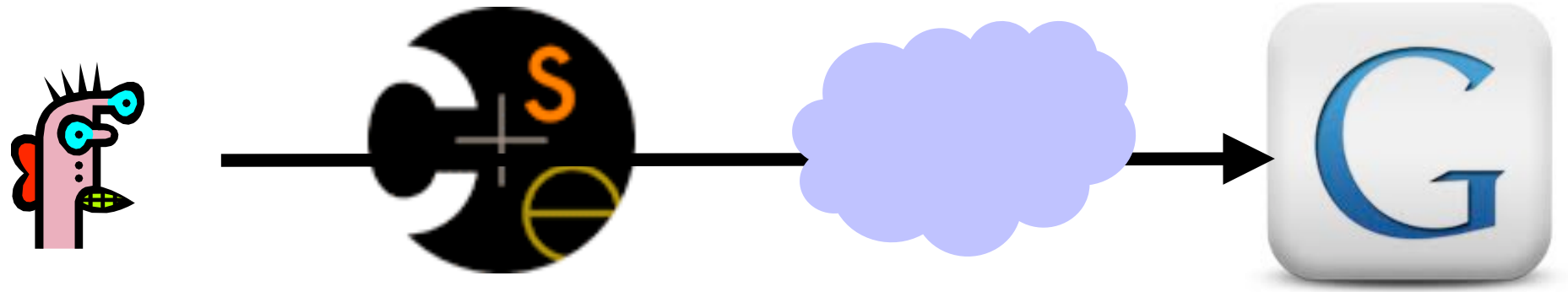


Internet Infrastructure

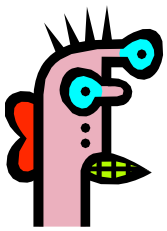


- TCP/IP for packet routing and connections
- Border Gateway Protocol (BGP) for route discovery
- Domain Name System (DNS) for IP address discovery

(Some) Entities



(Some) Goals



User

- Service (can get to Internet)
- Privacy (middle-entities shouldn't know what communicating or with whom)
- Fairness (e.g., get service I paid for)
- Integrity (can't impersonate me, modify my data)
- Safety (network shouldn't attack me)

(Some) Goals

Network Admin

- Service (clients can get to Internet)
- Performance (network works well)
- Identity (know what's on network)
- Safety (no one launching attacks)
- Accountability (can find bad users)

(Some) Goals

Intermediate ISPs

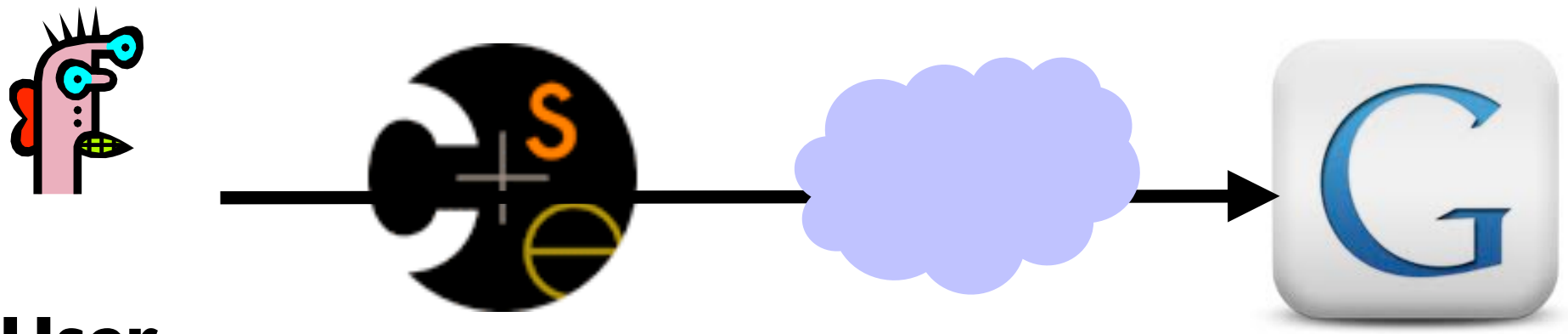
- Service (deliver traffic -> earn $$)
- Reliability & Performance (network works well)
- Integrity of delivered traffic (can bill customers properly, you're not over-charged by providers)

(Some) Goals

Server

- Service (deliver traffic -> earn $$)
- Reliability & Performance (network works well)
- Analytics (better delivery)
- Accounting (can bill customers properly)
- Safety (not being attacked)

(Some) Malicious Goals



User

Network Admin

Intermediate ISPs

Server

Launch undetectable attacks

Probe for vulnerabilities

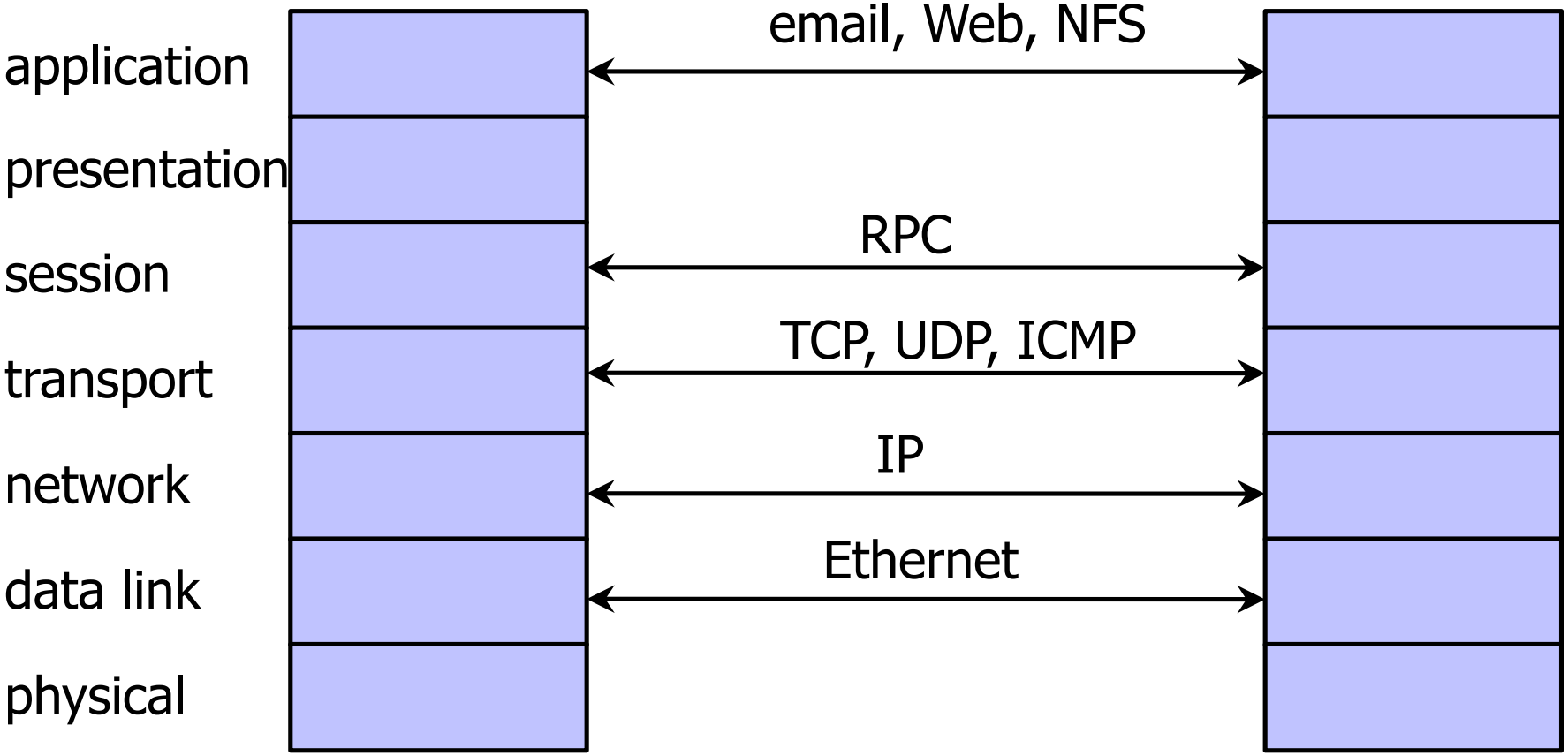
Spy on/tamper with traffic

Impersonate servers/users

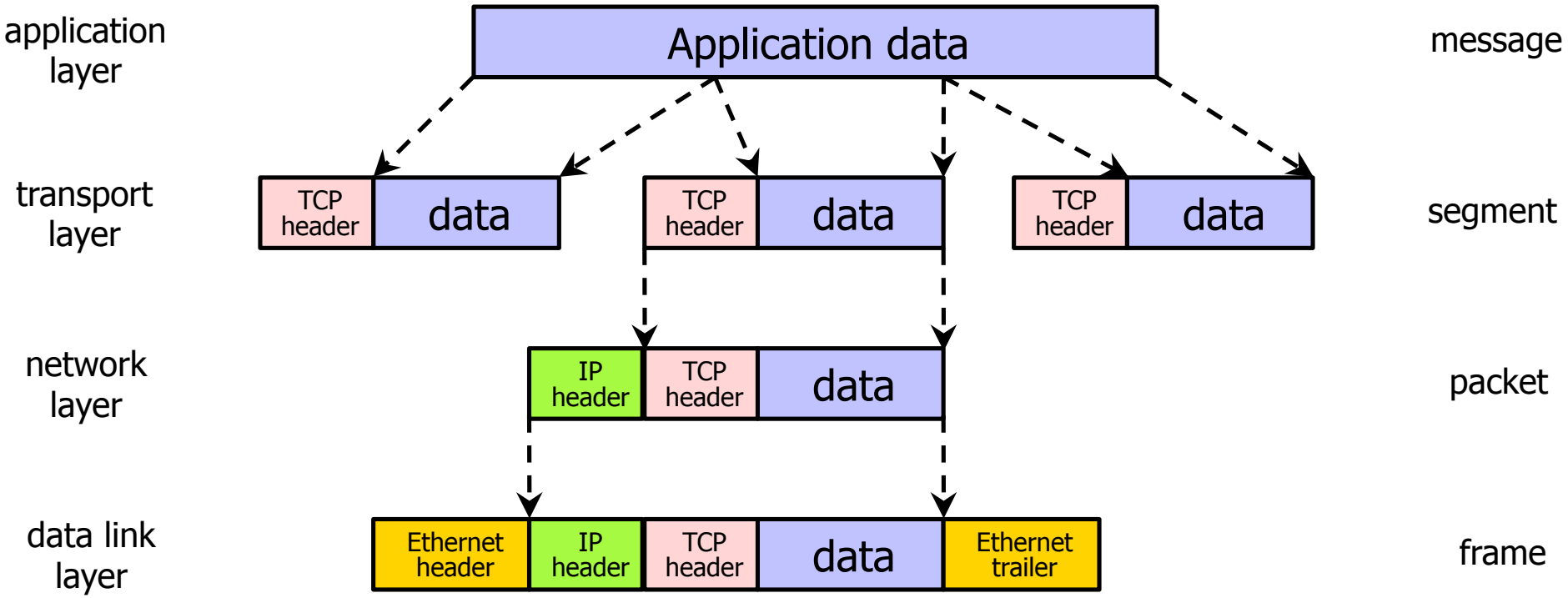
Spy on users

Identify anonymous users

OSI Protocol Stack

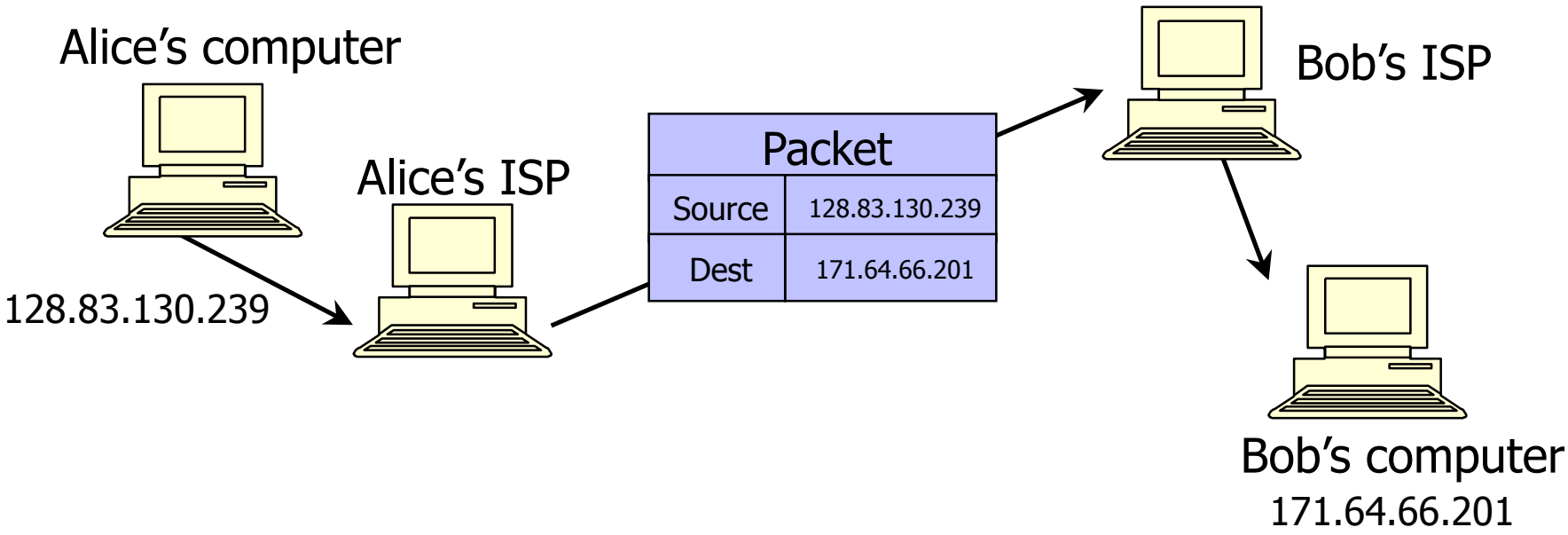


Data Formats



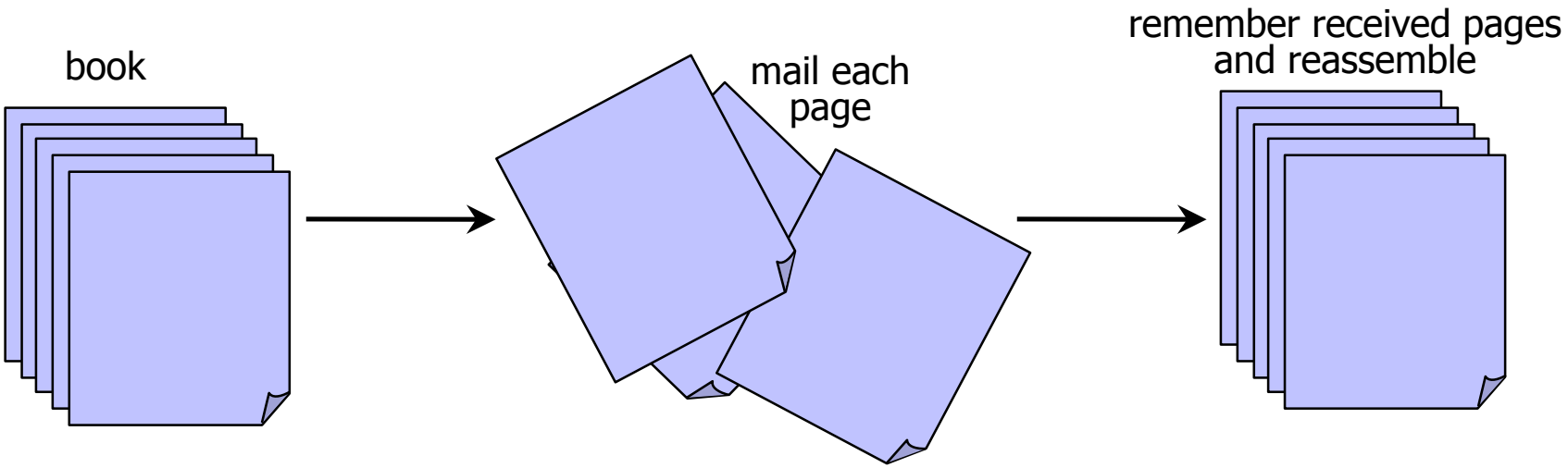
IP (Internet Protocol)

- Connectionless
  - Unreliable, "best-effort" protocol
- Uses numeric addresses for routing
  - Typically several hops in the route



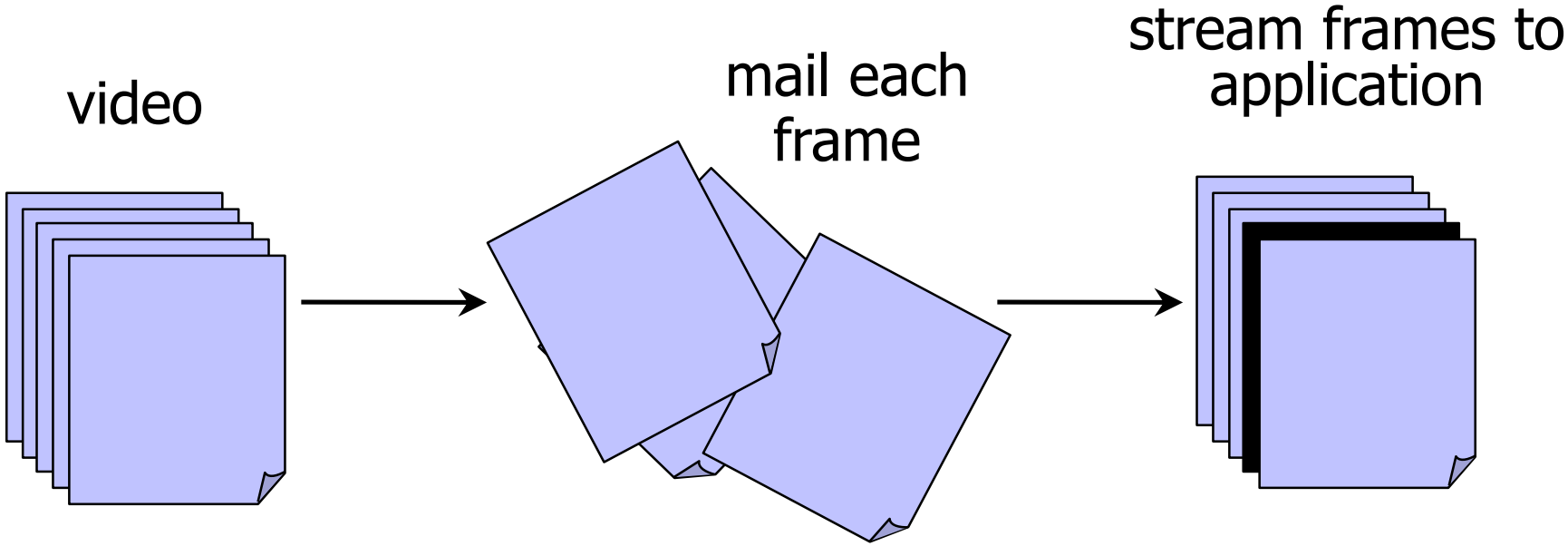
TCP (Transmission Control Protocol)

- Sender: break data into packets
  - Sequence number is attached to every packet
- Receiver: reassemble packets in correct order
  - Acknowledge receipt; lost packets are re-sent
- Connection state maintained on both sides



UDP (User Datagram Protocol)

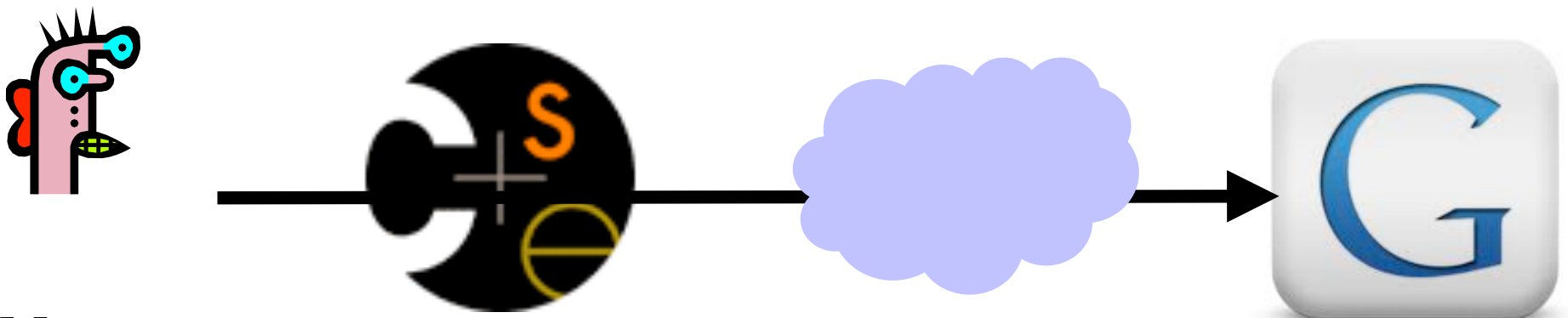
- Sender: break data into packets
  - Sequence number - maybe? If Application wants them
- Receiver: receive packets
  - No acknowledgement
  - Dropped packets are skipped - no retransmission



ICMP (Control Message Protocol)

- Provides feedback about network operation
  - "Out-of-band" messages carried in IP packets
  - Error reporting, congestion control, reachability, etc.
- Example messages:
  - Destination unreachable
  - Time exceeded
  - Parameter problem
  - Redirect to better gateway
  - Reachability test (echo / echo reply)
  - Message transit delay (timestamp request / reply)

(Some) Malicious Goals



User

Network Admin

Intermediate ISPs

Server

Launch undetectable attacks

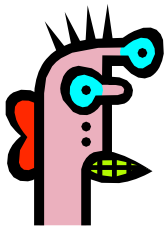
Probe for vulnerabilities

Spy on/tamper with traffic

Impersonate servers/users

Identify anonymous users

Detecting attacks



User

Launch undetectable attacks

- **Problem:** IP packets contain source IP address
- **Solution:** Spoof IP address

Inferring DDOS (Moore, Voelker, Savage '01)