

SSL/TLS

Vitaly Shmatikov

Reading Assignment

◆ Kaufman. Chapter 19.

What is SSL / TLS?

- ◆ Transport Layer Security protocol, version 1.0
 - De facto standard for Internet security
 - “The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications”
 - Security against active, man-in-the-middle network attacker
 - Used to protect information transmitted between browsers and Web servers, VoIP, many other scenarios
- ◆ Based on Secure Sockets Layers protocol, ver 3.0
 - Same protocol design, different algorithms
- ◆ Deployed in nearly every Web browser

SSL / TLS in the Real World

Wells Fargo Account Summary - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Favorites Print Home

Address https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76ax52xltPX8uoCT8rRBfMMdJldx Go Links Yahoo maps Mapblast Dictionary

Home | Help Center | Contact Us | Locations | Site Map | Apply | Sign Off

WELLS FARGO

Account Summary Last Log On: January 06, 2004

> Account Summary

Brokerage

Bill Pay

Transfer

Account Services

My Message Center

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.

Wells Fargo Accounts OneLook Accounts

Tip: Select an account's balance to access the Account History.

NEW [Enroll for Online Statements](#) [My Message Center](#)

Cash Accounts

Account	Account Number	Available Balance
Checking Add Bill Pay		
Total		

To end your session, be sure to Sign Off.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off

Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.

Internet



History of the Protocol

◆ SSL 1.0

- Internal Netscape design, early 1994?
- Lost in the mists of time

◆ SSL 2.0

- Published by Netscape, November 1994
- Several weaknesses

◆ SSL 3.0

- Designed by Netscape and Paul Kocher, November 1996

◆ TLS 1.0

- Internet standard based on SSL 3.0, January 1999
- Not interoperable with SSL 3.0
 - TLS uses HMAC instead of MAC; can run on any port

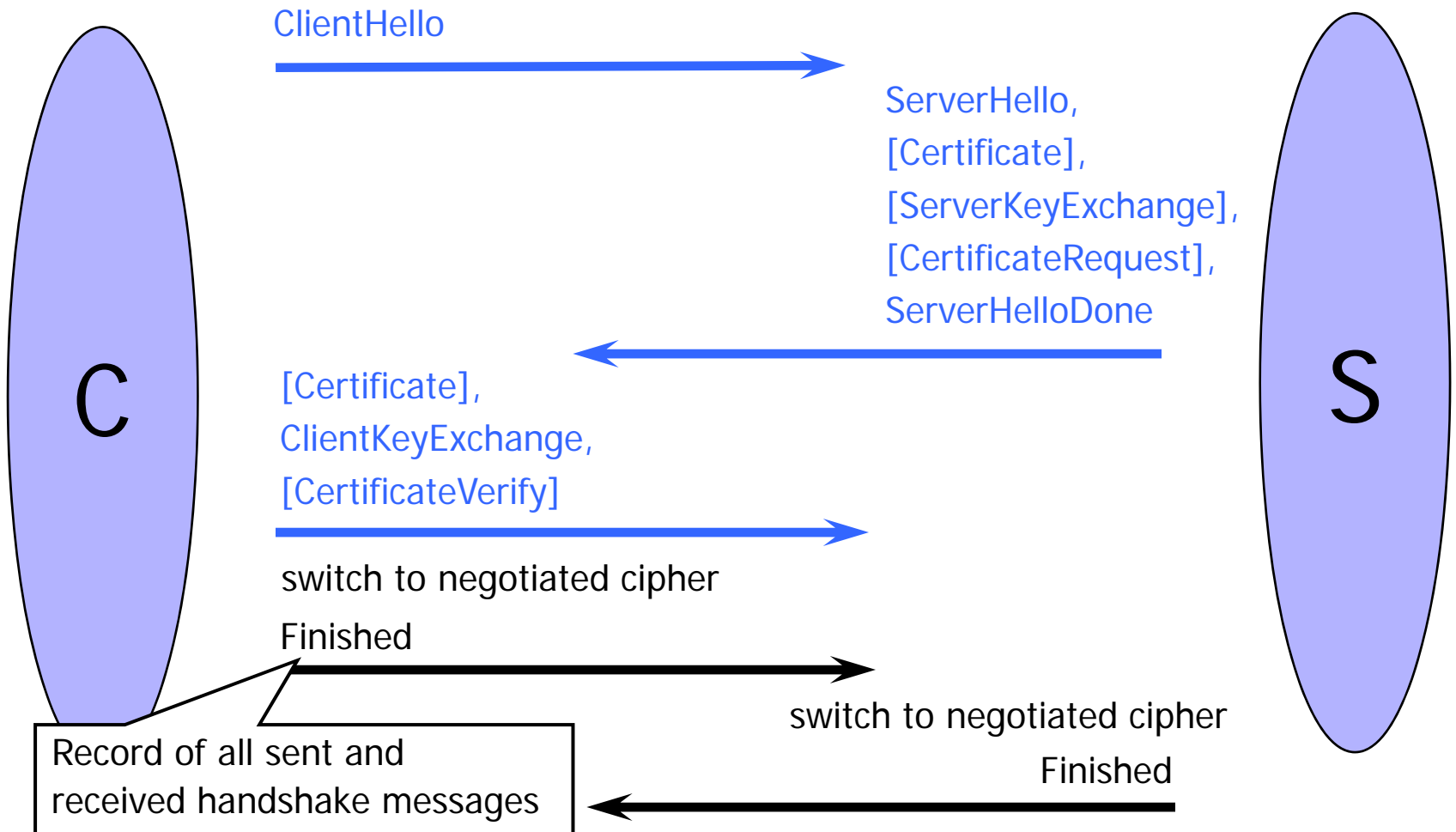
TLS Basics

- ◆ TLS consists of **two** protocols
 - Familiar pattern for key establishment 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

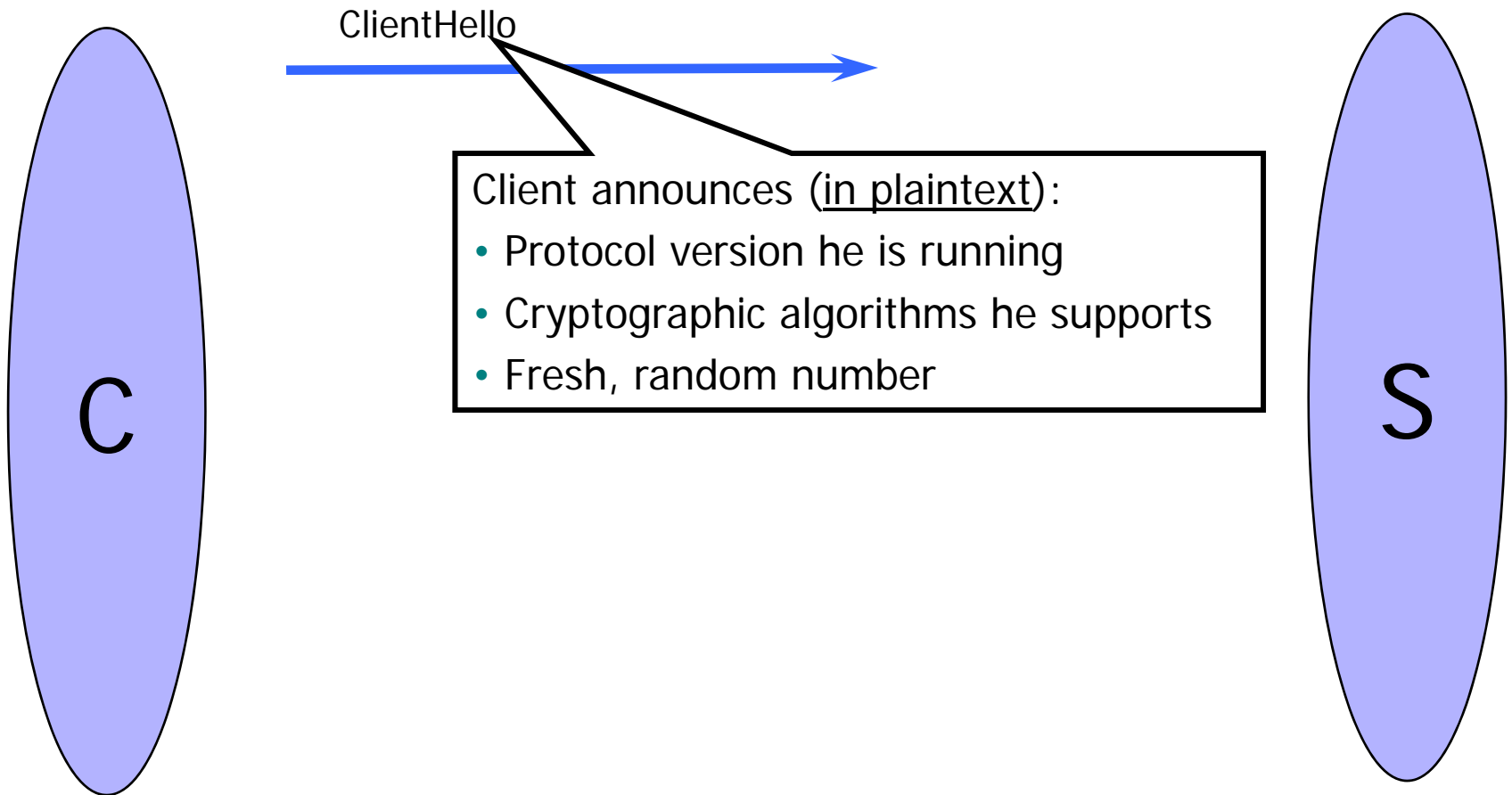
TLS Handshake Protocol

- ◆ 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



ClientHello (RFC)

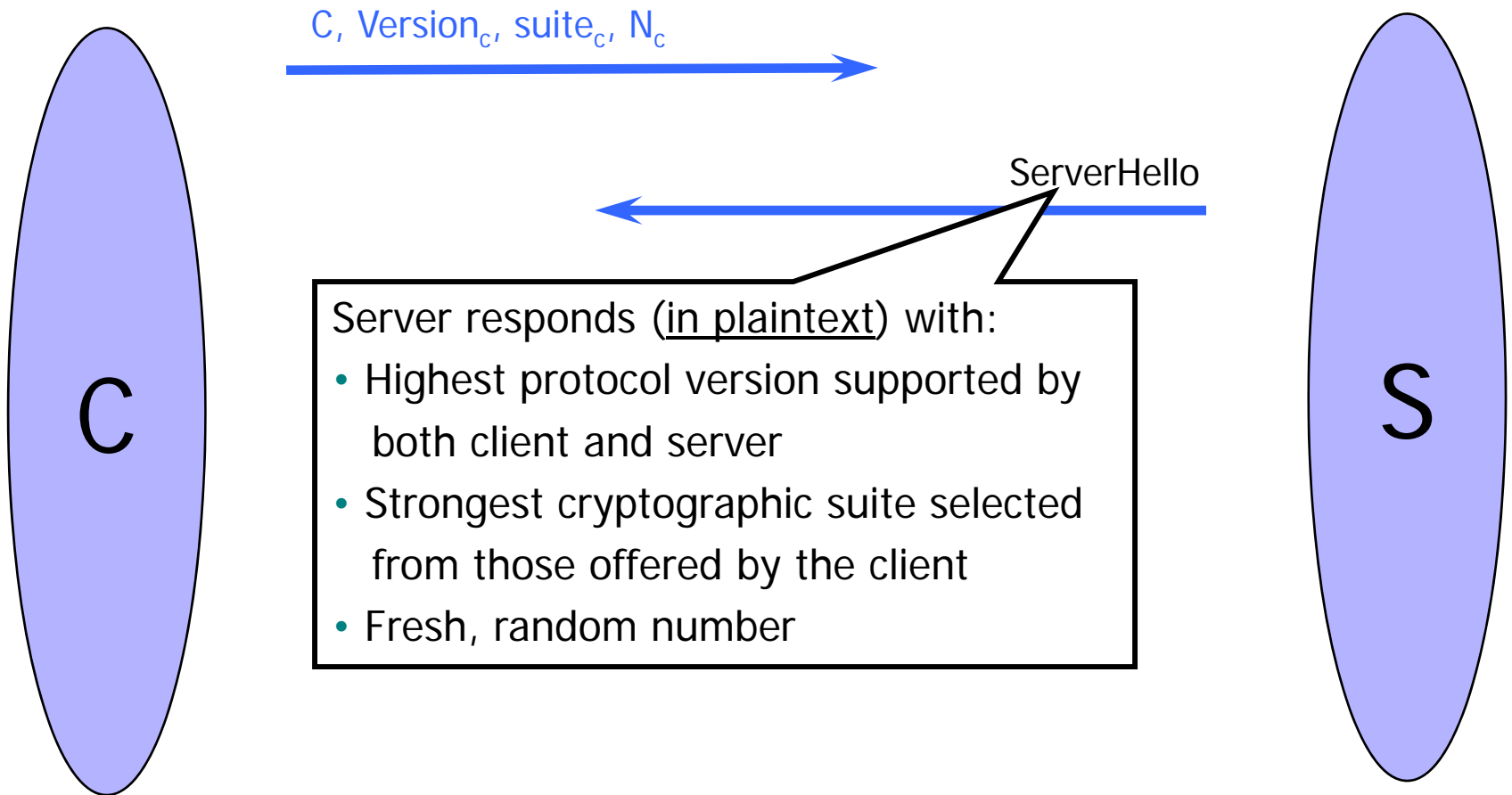
```
struct {  
    ProtocolVersion client_version;  
    Random random;  
    SessionID session_id;  
    CipherSuite cipher_suites;  
    CompressionMethod compression_methods;  
} ClientHello
```

Highest version of the protocol supported by the client

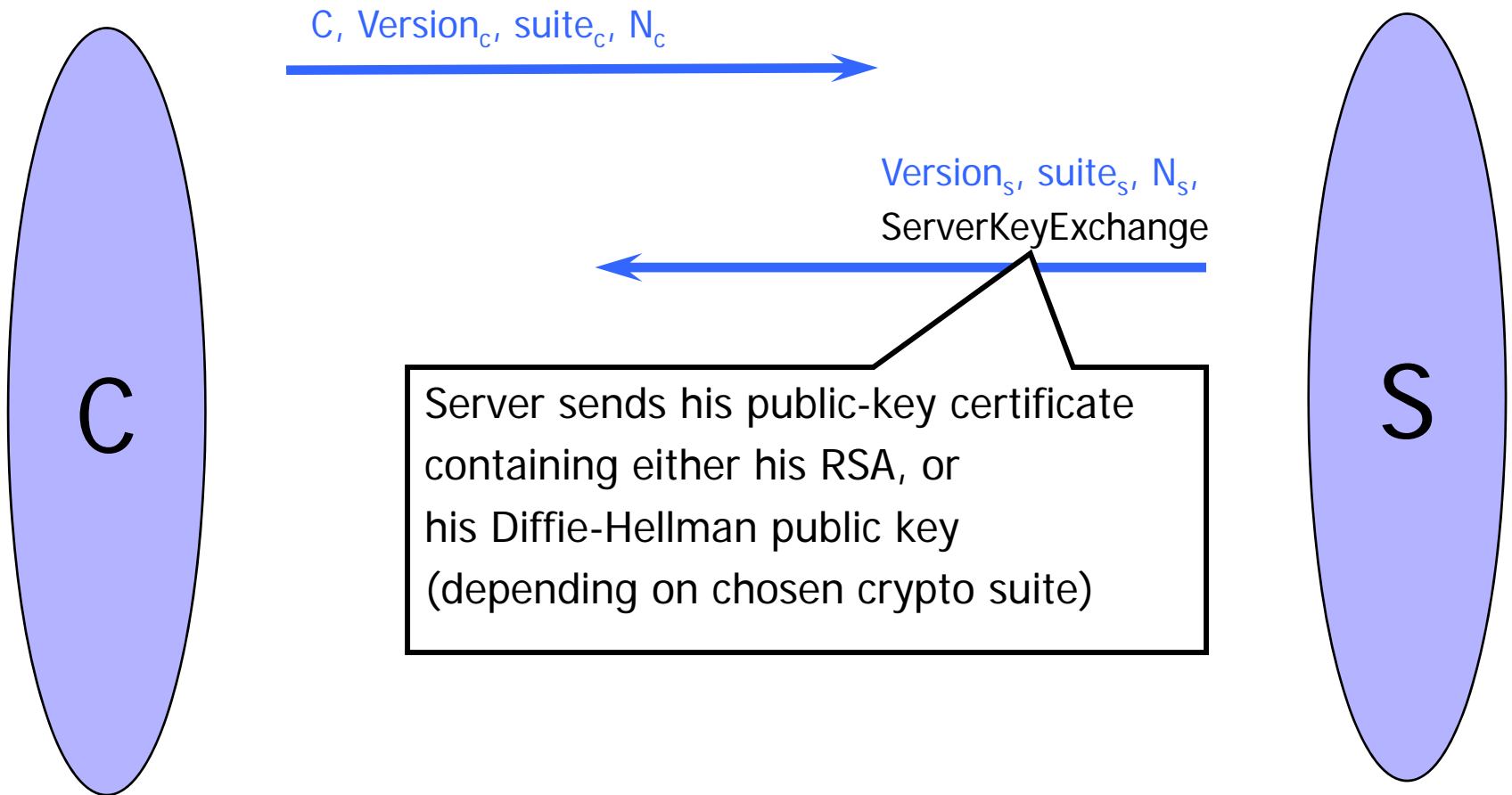
Session id (if the client wants to resume an old session)

Set of cryptographic algorithms supported by the client (e.g., RSA or Diffie-Hellman)

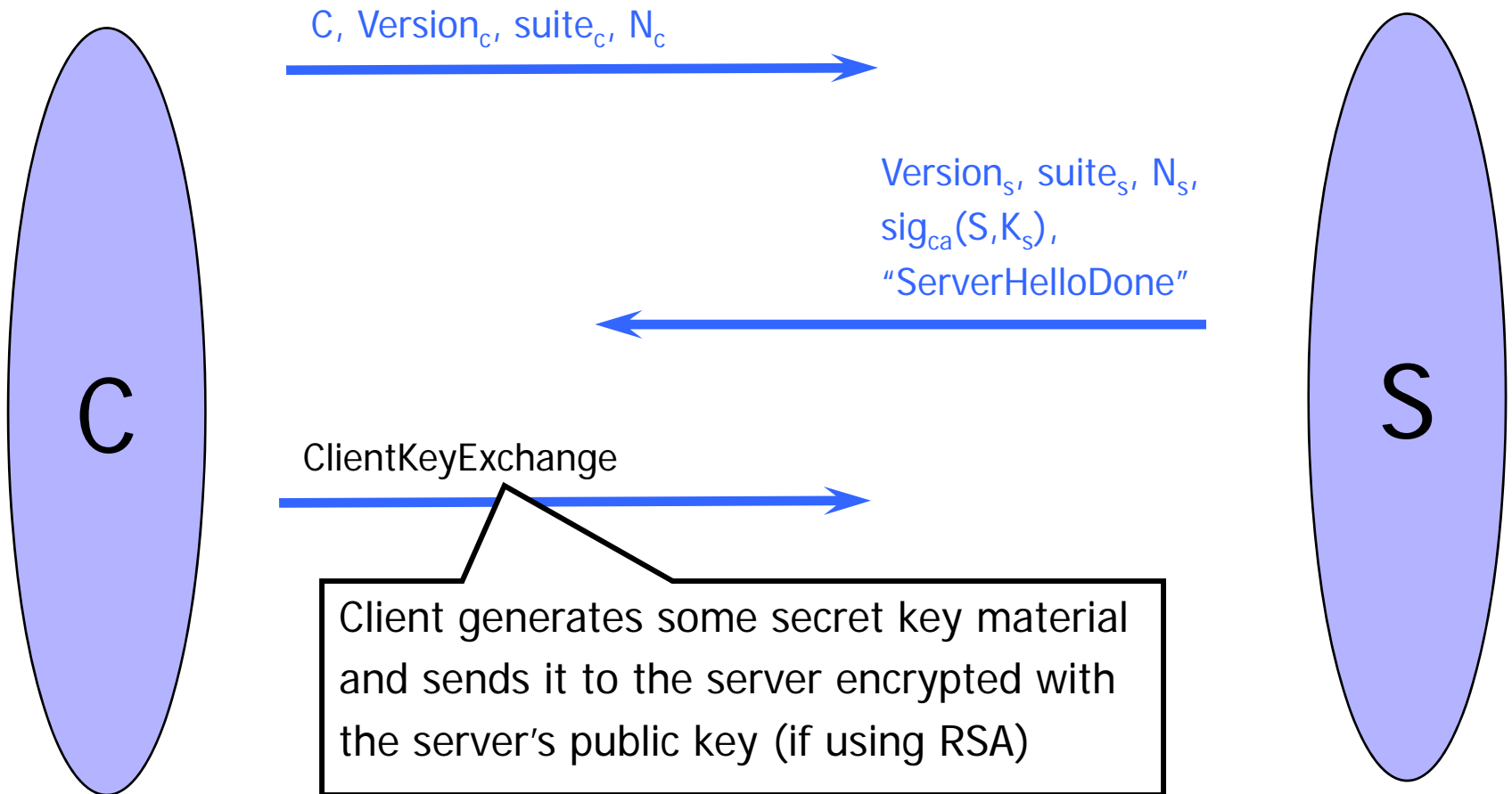
ServerHello



ServerKeyExchange



ClientKeyExchange



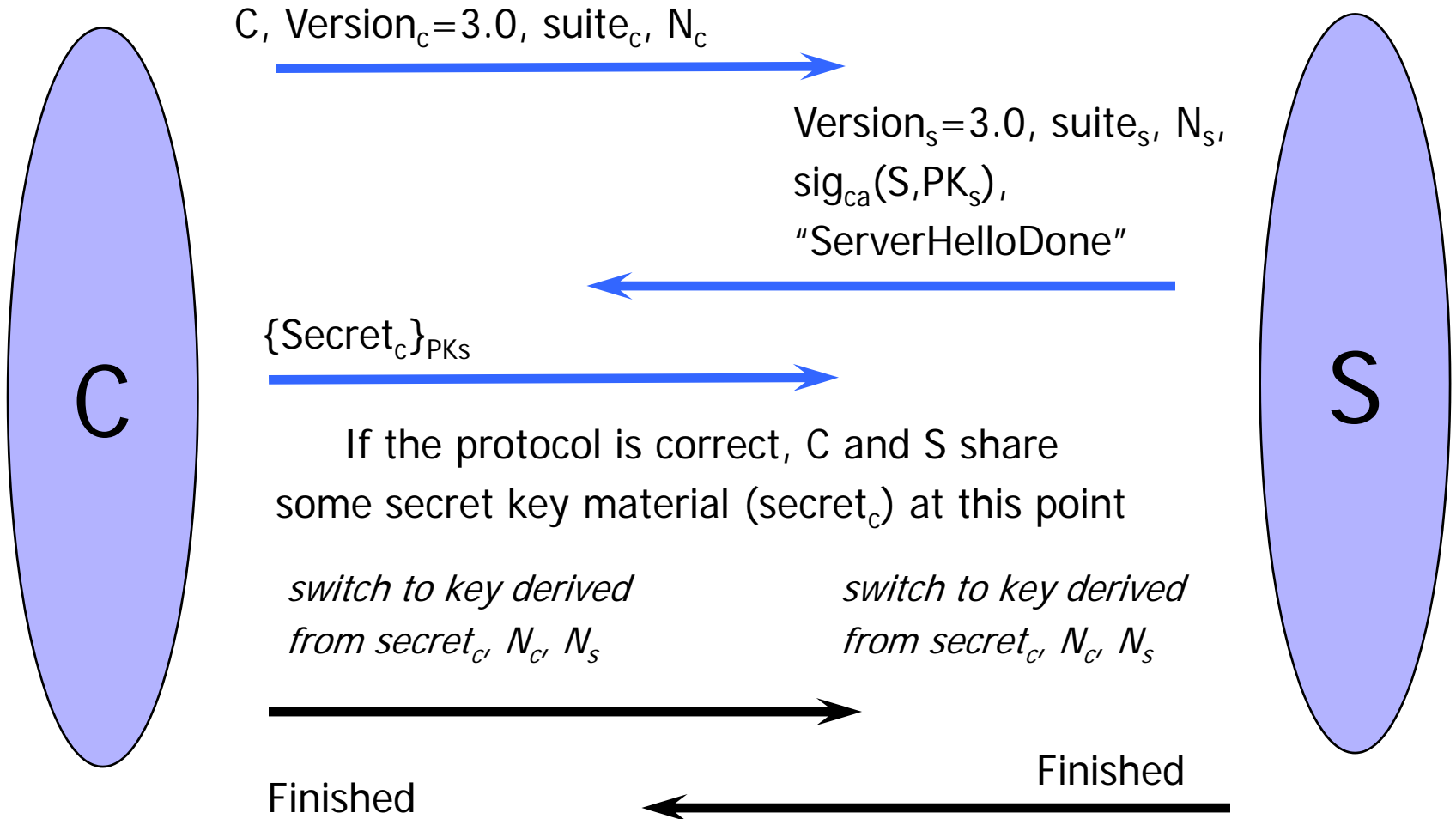
ClientKeyExchange (RFC)

```
struct {  
    select (KeyExchangeAlgorithm) {  
        case rsa: EncryptedPreMasterSecret;  
        case diffie_hellman: ClientDiffieHellmanPublic;  
    } exchange_keys  
} ClientKeyExchange
```

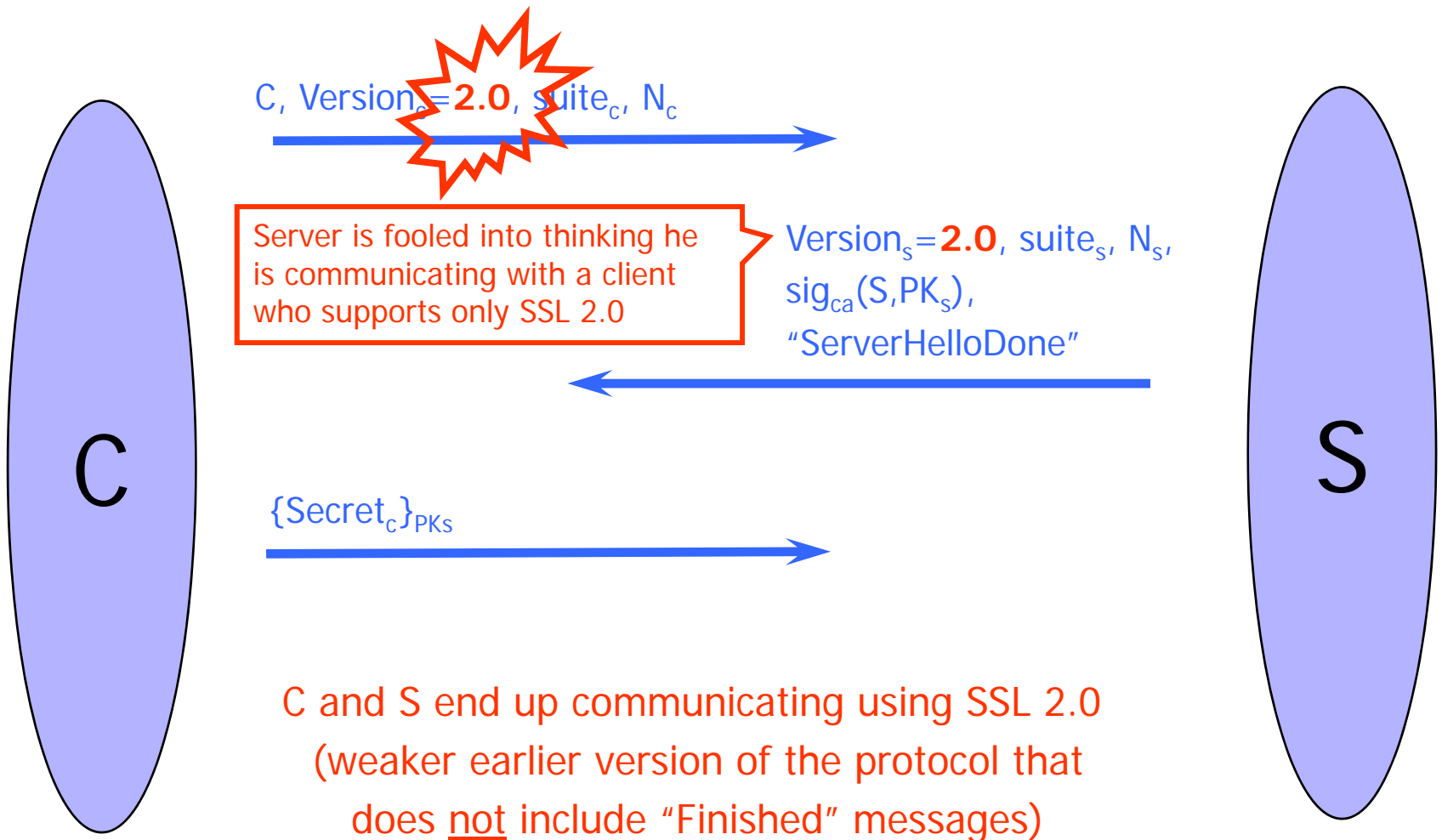
```
struct {  
    ProtocolVersion client_version;  
    opaque random[46];  
} PreMasterSecret
```

Random bits from which symmetric keys will be derived (by hashing them with nonces)

"Core" SSL 3.0 Handshake



Version Rollback Attack



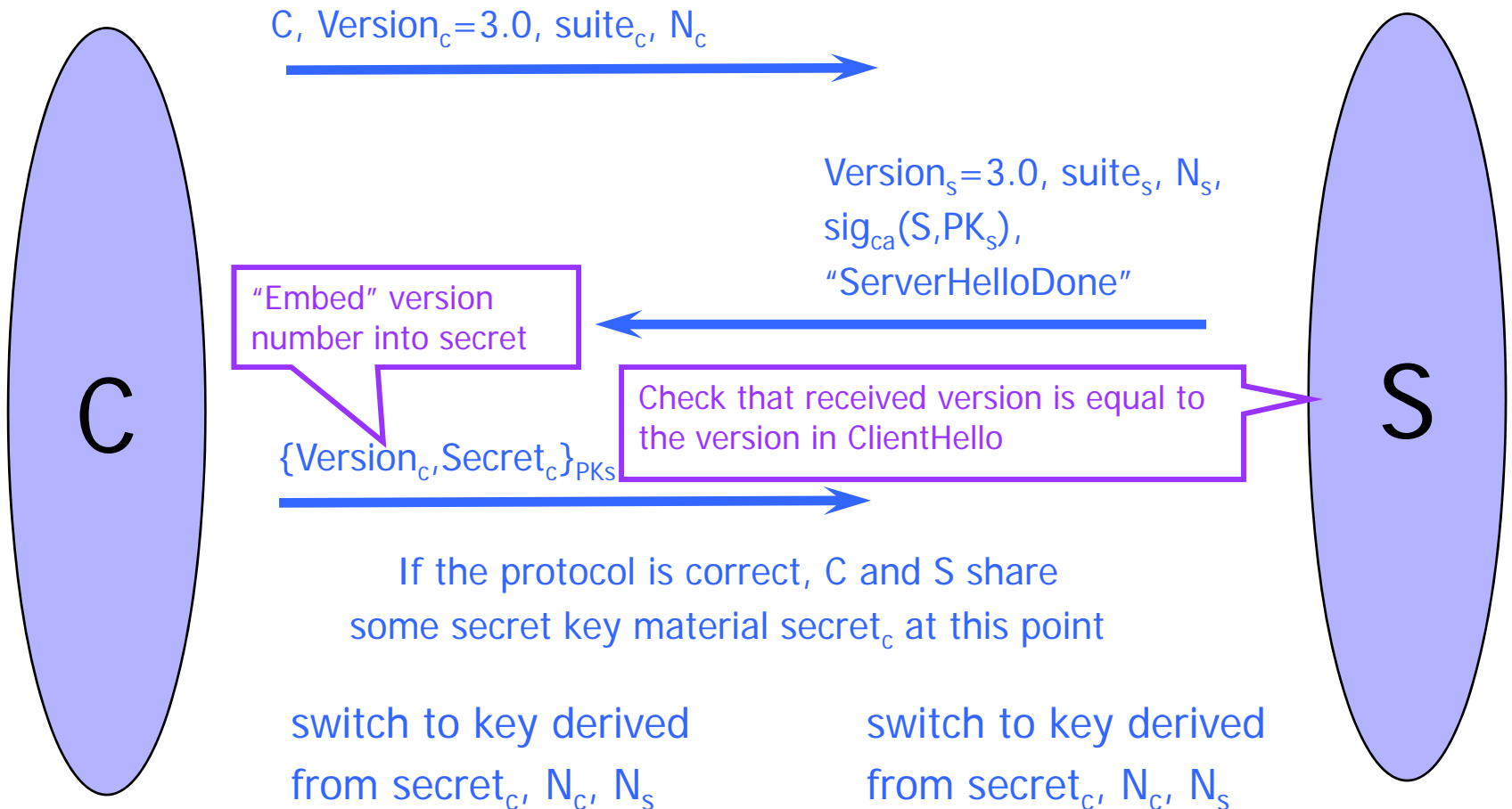
SSL 2.0 Weaknesses (Fixed in 3.0)

- ◆ Cipher suite preferences are not authenticated
 - “Cipher suite rollback” attack is possible
- ◆ Weak MAC construction
- ◆ 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

“Chosen-Protocol” 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 early
- ◆ Many protocols had “version rollback” attacks
 - SSL, SSH, GSM (cell phones)

Version Check in SSL 3.0



SSL/TLS Record Protection

