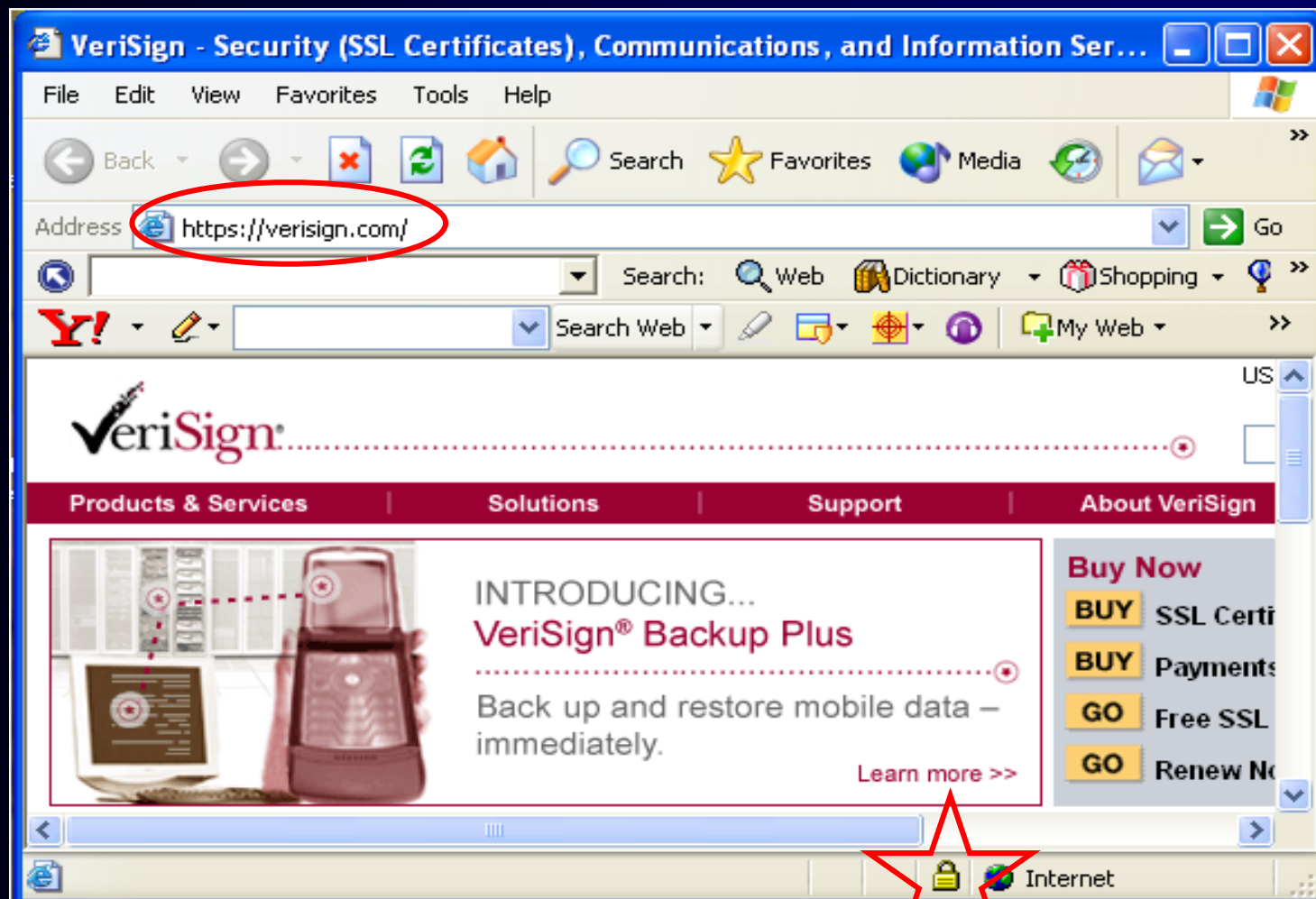

پروتکل SSL

فهرست مطالب

- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

مقدمه



تاریخچه

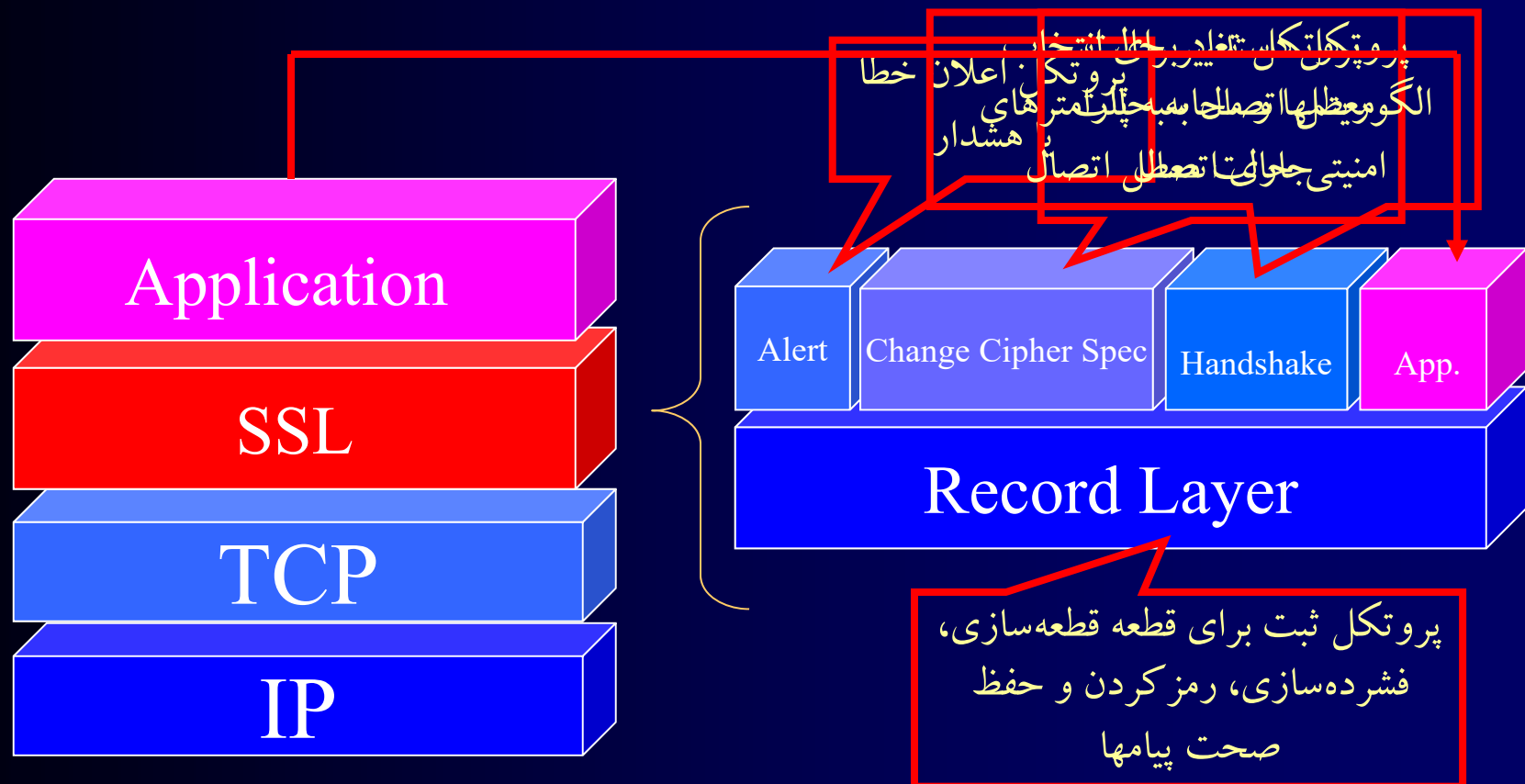
- **SSL1.0** اولین طراحی شرکت Netscape * سال ۱۹۹۴ میلادی.
این نسخه هیچگاه منتشر نشد!
- **SSL2.0** توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۵ میلادی.
- **SSL3.0** توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۶ میلادی.
در ابتدای ماه می سال ۱۹۹۶ میلادی، توسعه SSL تحت مسئولیت IETF در آمد.
- **TLS1.0** اولین نسخه استاندارد پروتکل SSL * اوایل سال ۱۹۹۹ میلادی.
- **TLS1.1** برای رفع ضعفهای TLS1.0 منتشر شد.

فهرست مطالب

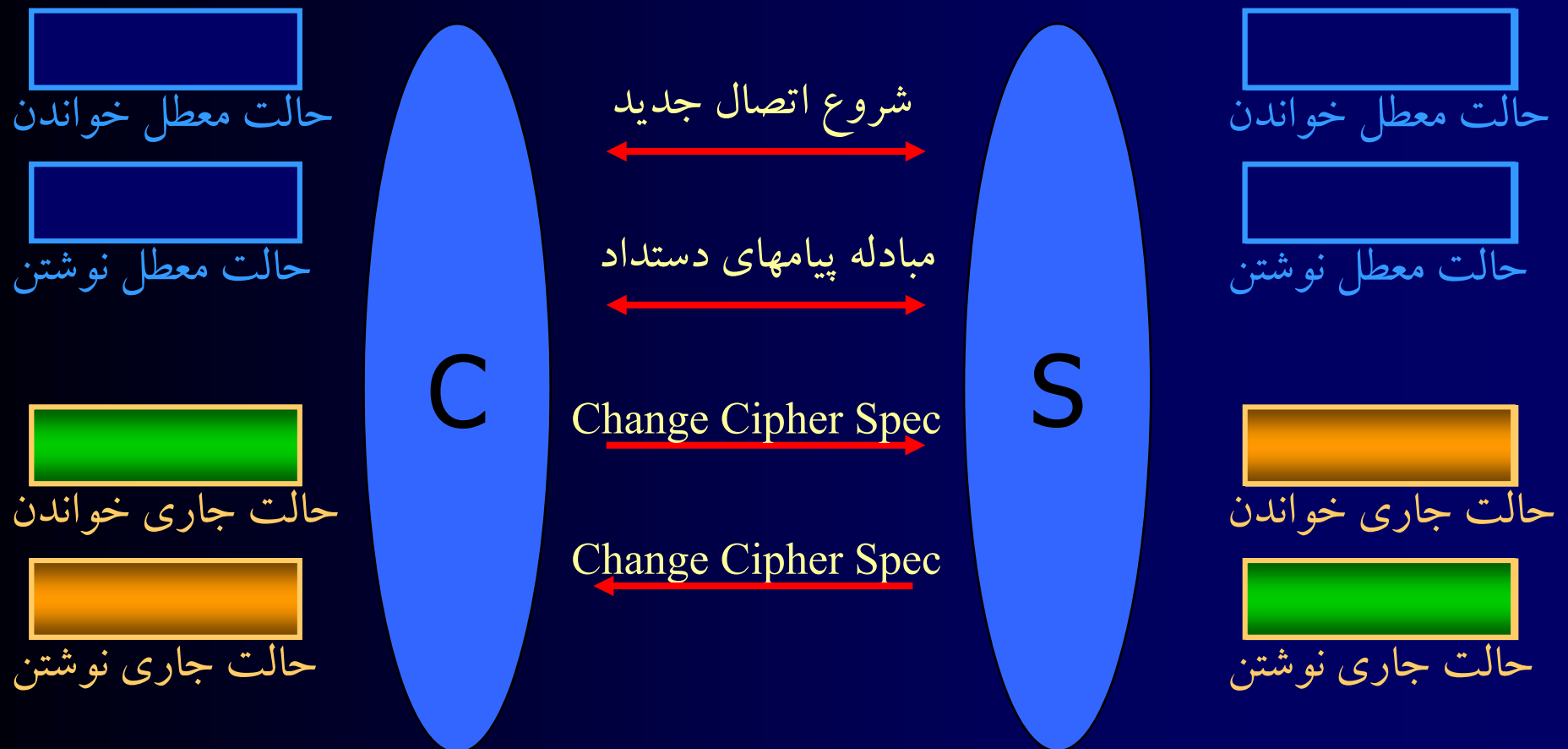
- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

Secure Socket Layer

SSL یک لایه مجزا است که تنها برای برقراری امنیت به معماری اینترنت اضافه می شود.



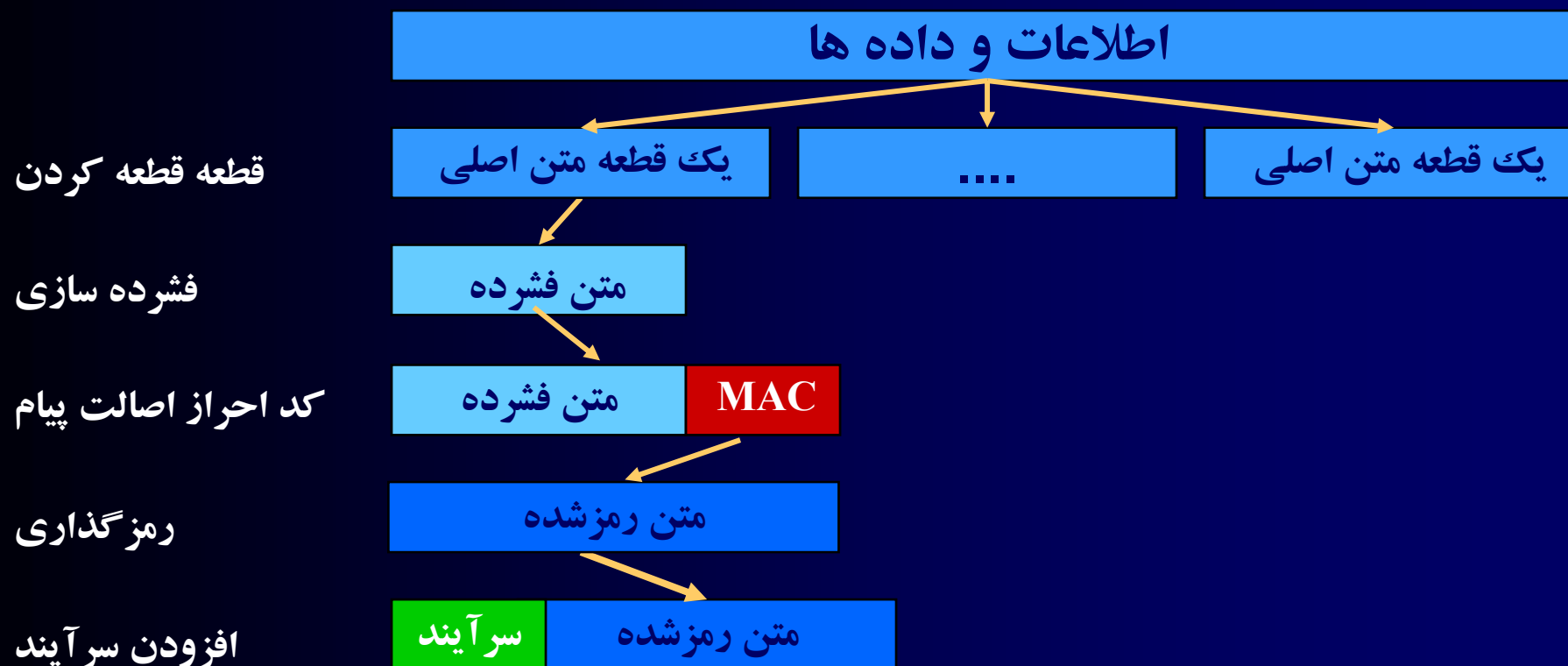
حالات چهار گانه اتصال



پروتکل ثبت

اطلاعات از چهار پروتکل لایه بالایی وارد لایه ثبت می شوند تا به شکل مناسب در آمده و به لایه انتقال فرستاده شوند.

عملیات فشرده سازی، احراز اصالت و رمزگذاری طبق حالت جاری اتصال انجام می شوند.



سرآیند ثبت = طول پیام | نوع پروتکل | نسخه پروتکل

پروتکل اعلان خطا

- پیام این پروتکل شامل دو بات است.


Alert Code	Alert Message	Description
0	close_notify	Notifies the recipient that the sender will not send any more messages on this connection.
10	unexpected_message	Received an inappropriate message This alert should never be observed in communication between proper implementations. This message is always fatal.
20	bad_record_mac	Received a record with an incorrect MAC . This message is always fatal.
21	decryption_failed	Decryption of a TLSCiphertext record is decrypted in an invalid way: either it was not an even multiple of the block length or its padding values, when checked, were not correct. This message is always fatal.
22	record_overflow	Received a TLSCiphertext record which had a length more than $2^{14}+2048$ bytes, or a record decrypted to a TLSCompressed record with more than $2^{14}+1024$ bytes . This message is always fatal.
30	decompression_failure	Received improper input, such as data that would expand to excessive length, from the decompression function. This message is always fatal.
40	handshake_failure	Indicates that the sender was unable to negotiate an acceptable set of security parameters given the options available. This is a fatal error.
42	bad_certificate	There is a problem with the certificate, for example, a certificate is corrupt, or a certificate contains signatures that cannot be verified.
43	unsupported_certificate	Received an unsupported certificate type.
44	certificate_revoked	Received a certificate that was revoked by its signer.
45	certificate_expired	Received a certificate has expired or is not currently valid.
46	certificate_unknown	An unspecified issue took place while processing the certificate that made it unacceptable.
47	illegal_parameter	Violated security parameters, such as a field in the handshake was out of range or inconsistent with other fields. This is always fatal.

پروتکل دستداد

- توافق روی الگوریتمهای لازم برای جلسه
- تبادل پارامترهای رمزنگاری لازم برای توافق طرفین روی یک pre-master-secret
- مبادله گواهینامه به منظور احراز اصالت طرفین
- تولید پارامترهای امنیتی حالت معطل اتصال برای لایه ثبت
- ایجاد اطمینان از درستی محاسبات و مذاکرات

محاسبه پارامترهای امنیتی حالت معطل اتصال

- محاسبه master-secret به کمک pre-master-secret و اعداد تصادفی مبادله شده
- محاسبه پارامترهای امنیتی لازم به کمک master-secret و اعداد تصادفی مبادله شده



کلید رمز کارفرما
کلید رمز کارگزار
کلید MAC کارفرما
کلید MAC کارگزار
بردار اولیه کارفرما
بردار اولیه کارگزار

روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



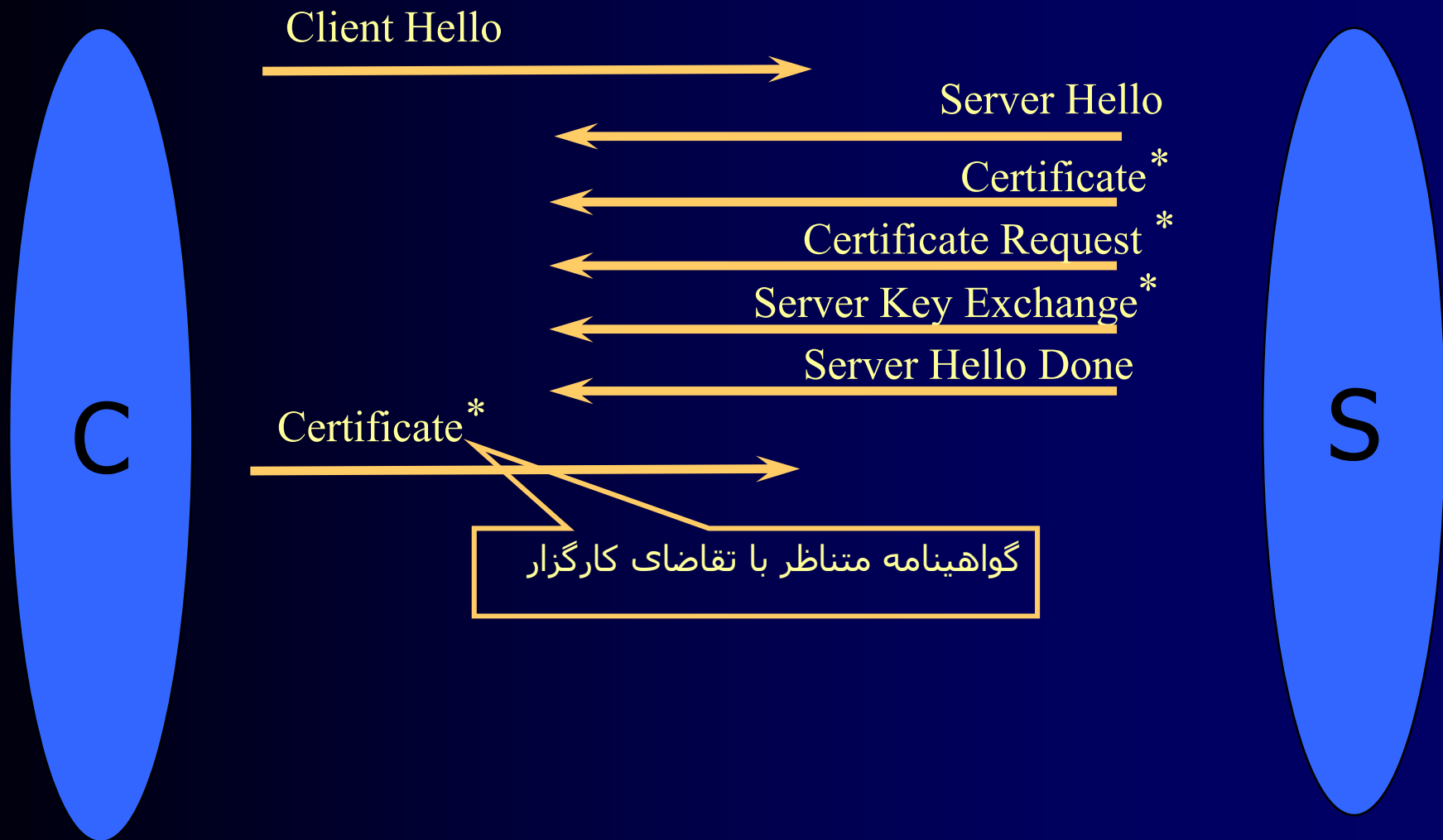
روند تبادل پیامها در یک دستداد کامل



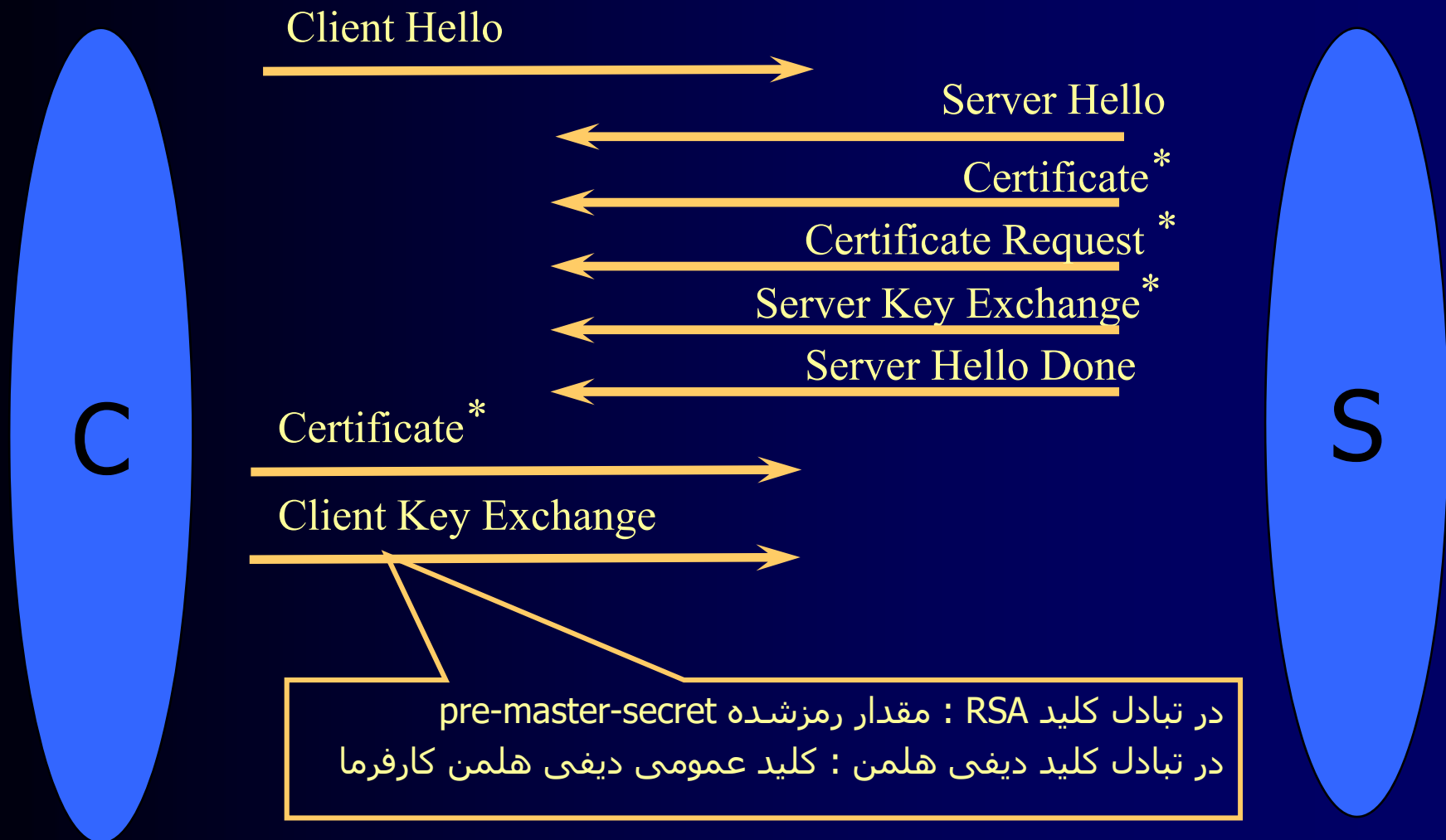
روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



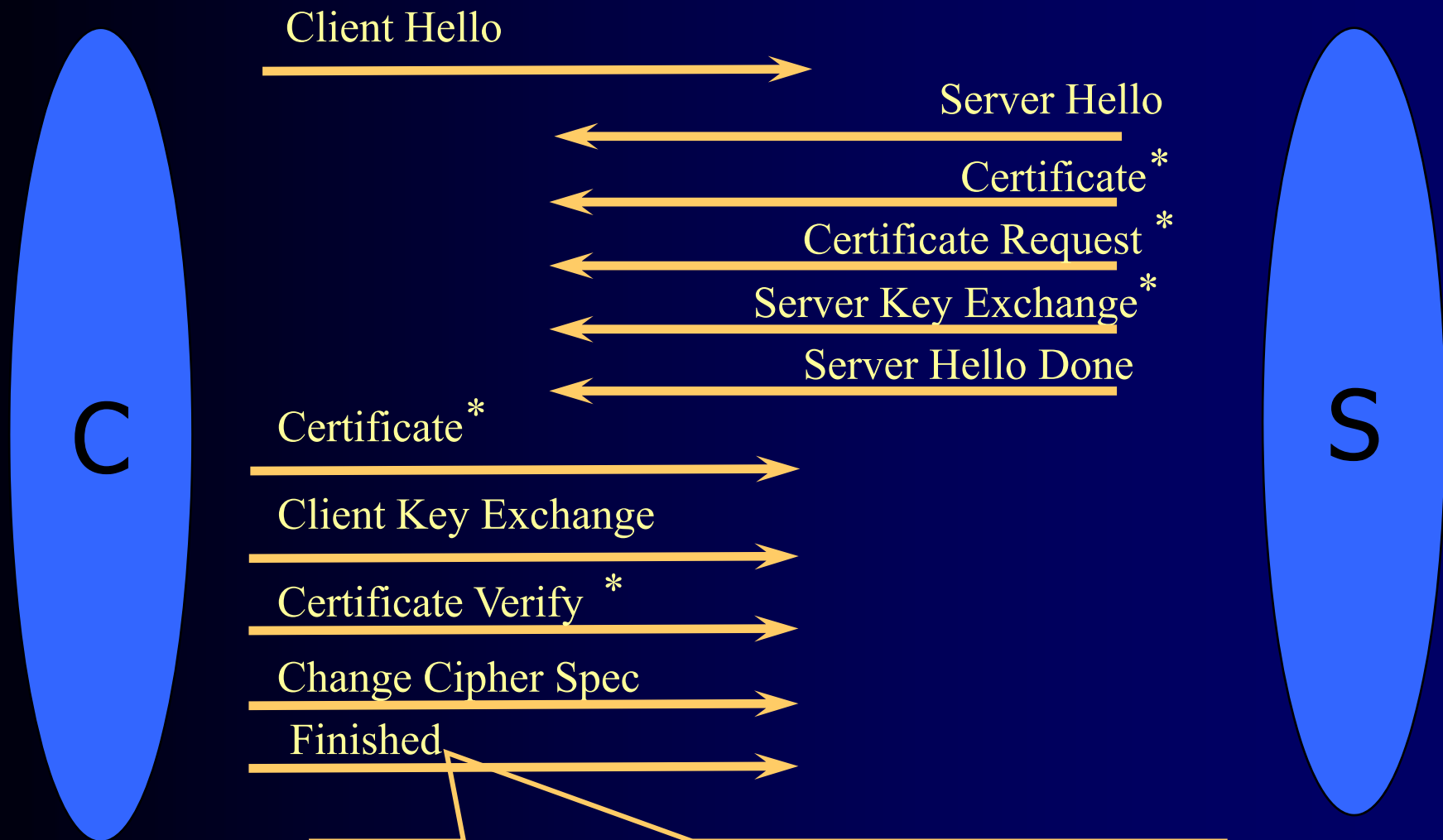
روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل

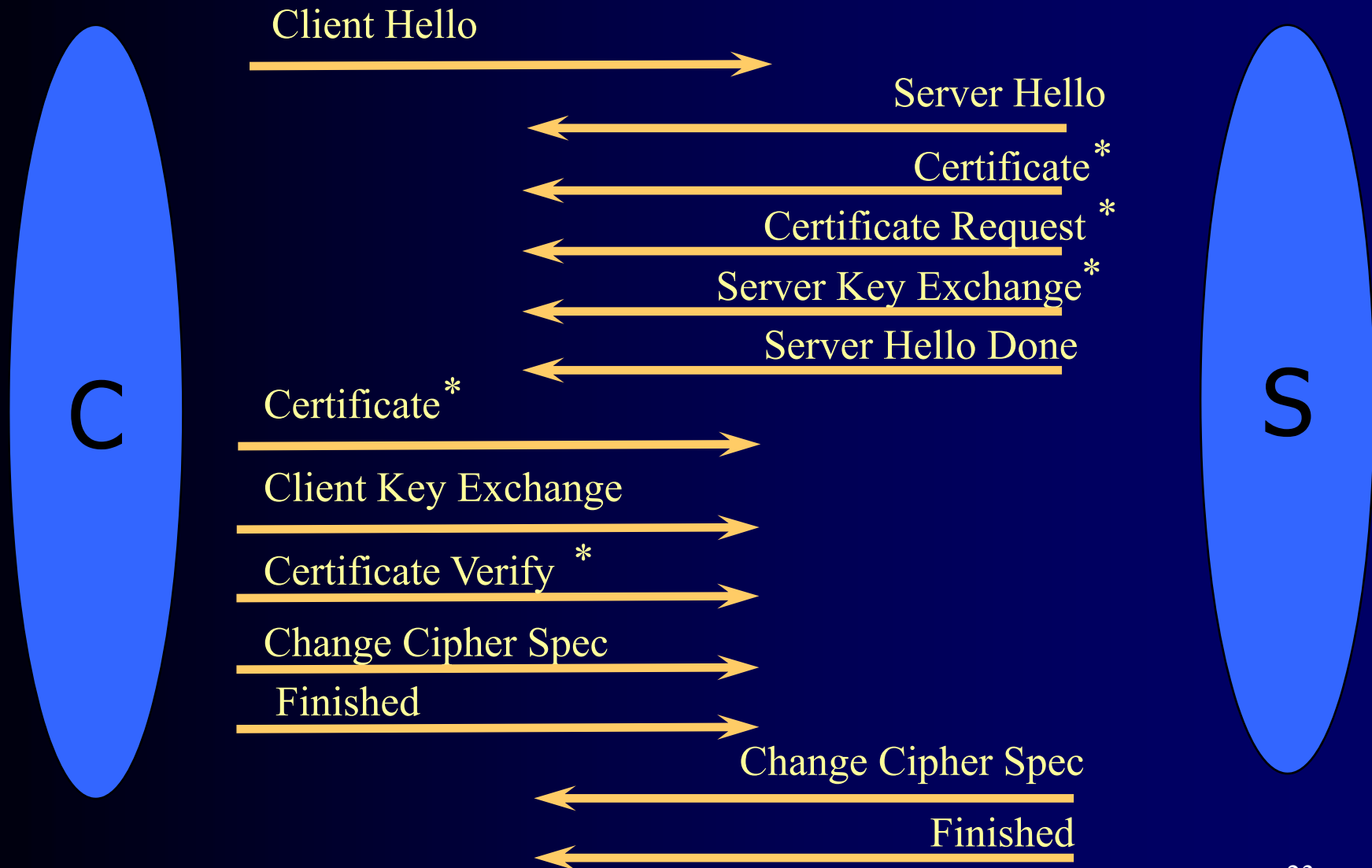


روند تبادل پیامها در یک دستداد کامل



حاصل درهم پیامهای دستداد مبادله شده تا قبل از این پیام

روند تبادل پیامها در یک دستداد کامل



از سرگیری جلسه

- فرآیند تبادل کلید موجب کاهش سرعت برقراری جلسه است.

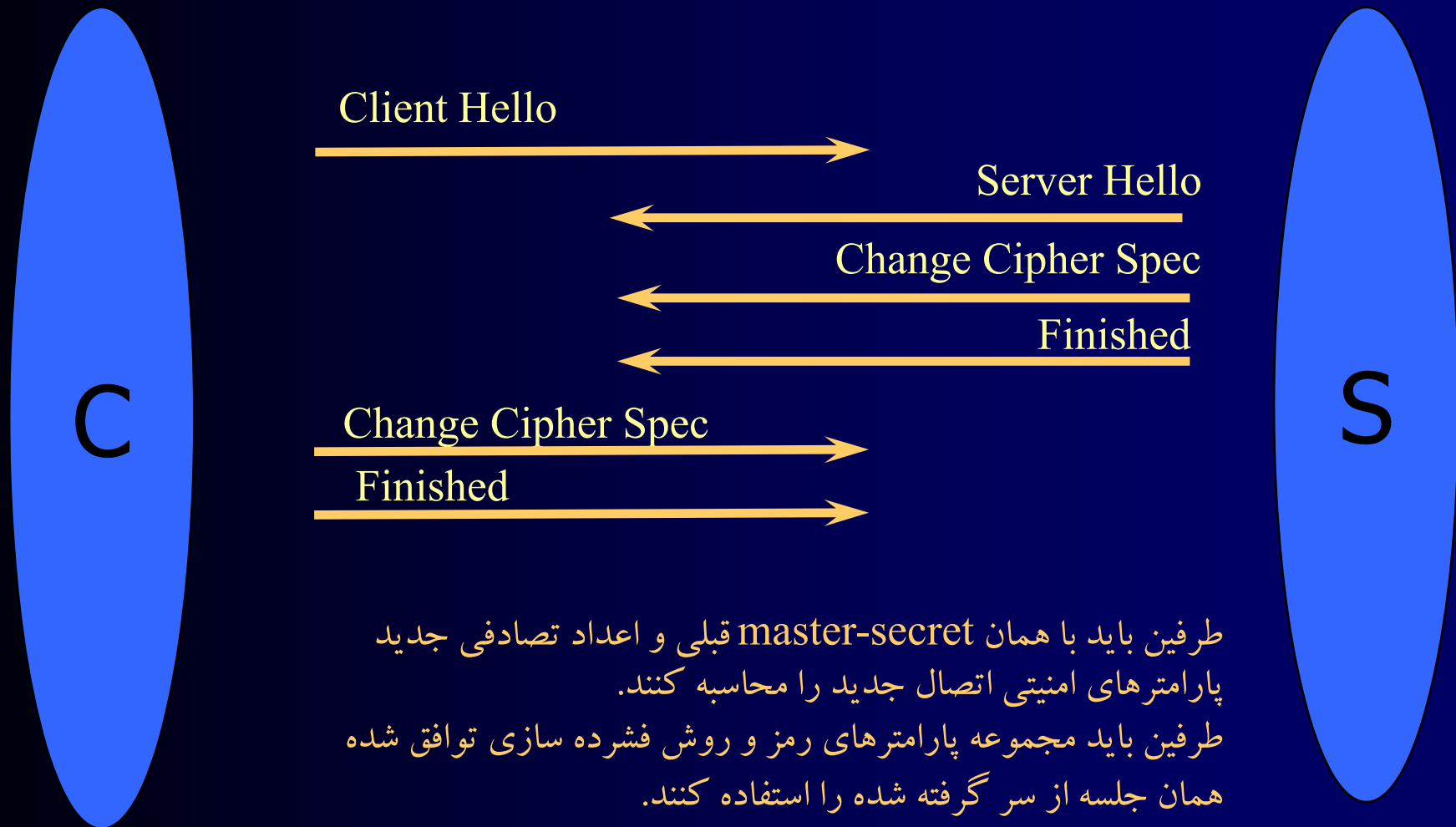


نگهداری pre-master-secret
برای استفاده در اتصالات بعدی

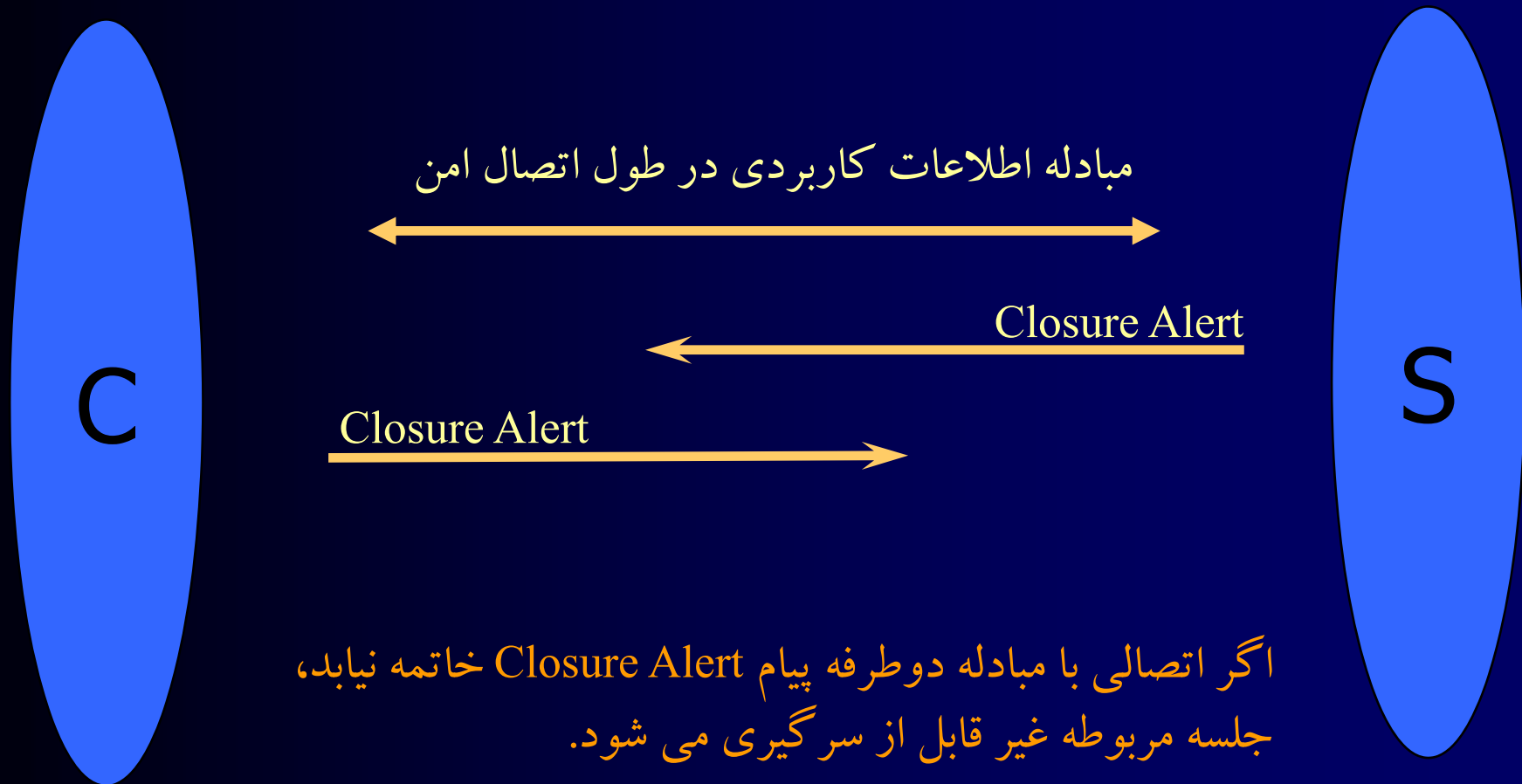


- تفاوت اتصال و جلسه
یک جلسه می تواند چندین اتصال را در بر داشته باشد.

روند تبادل پیامها هنگام از سرگیری جلسه

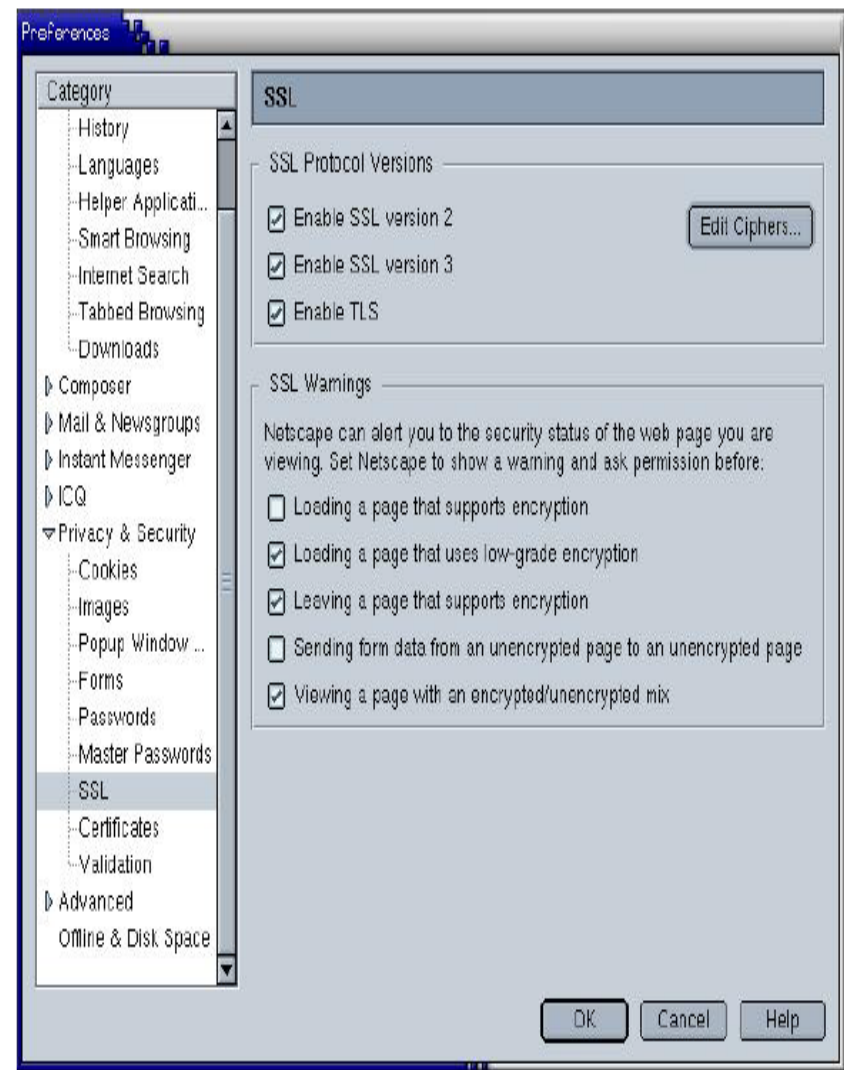
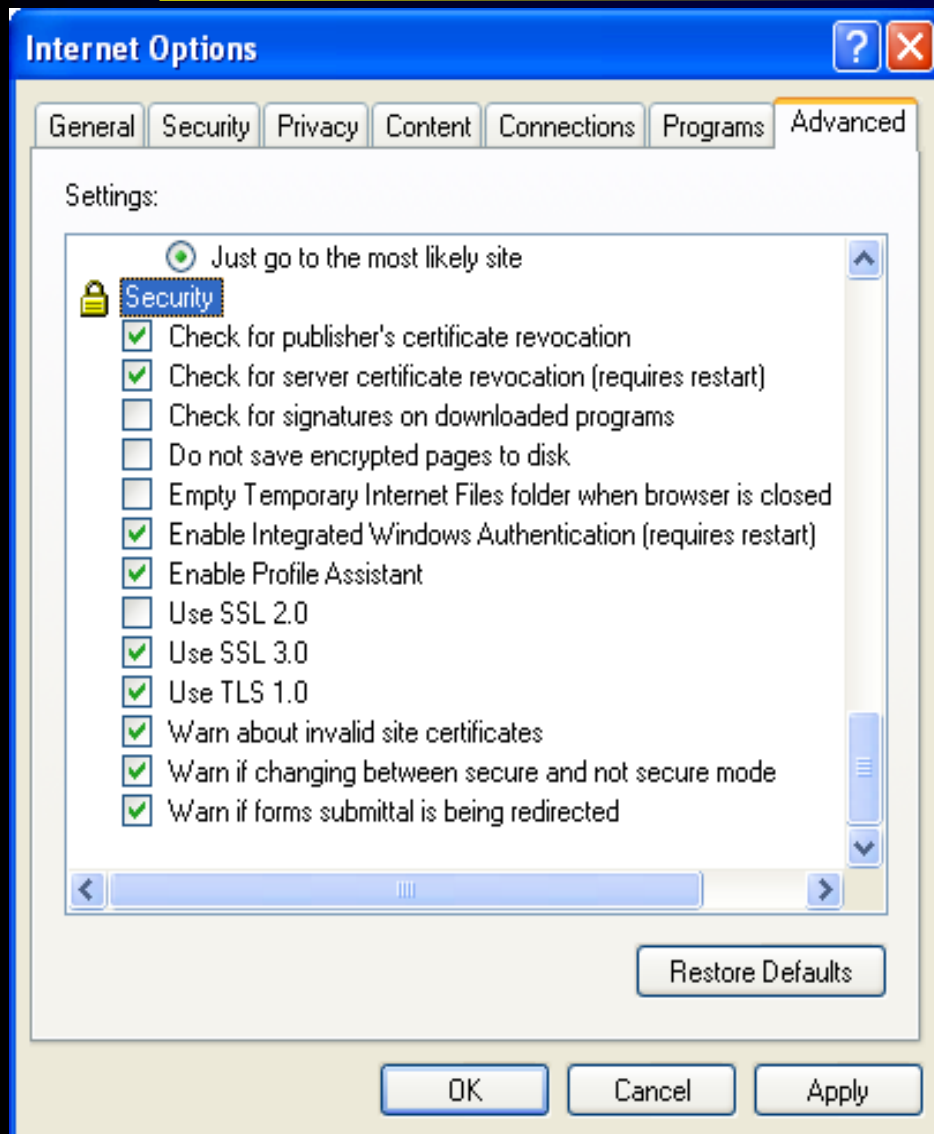


اعلان خاتمه برای پایان دادن اتصال



SSL/TLS Configuration Options

Internet Explorer 6.0 & Netscape



فهرست مطالب

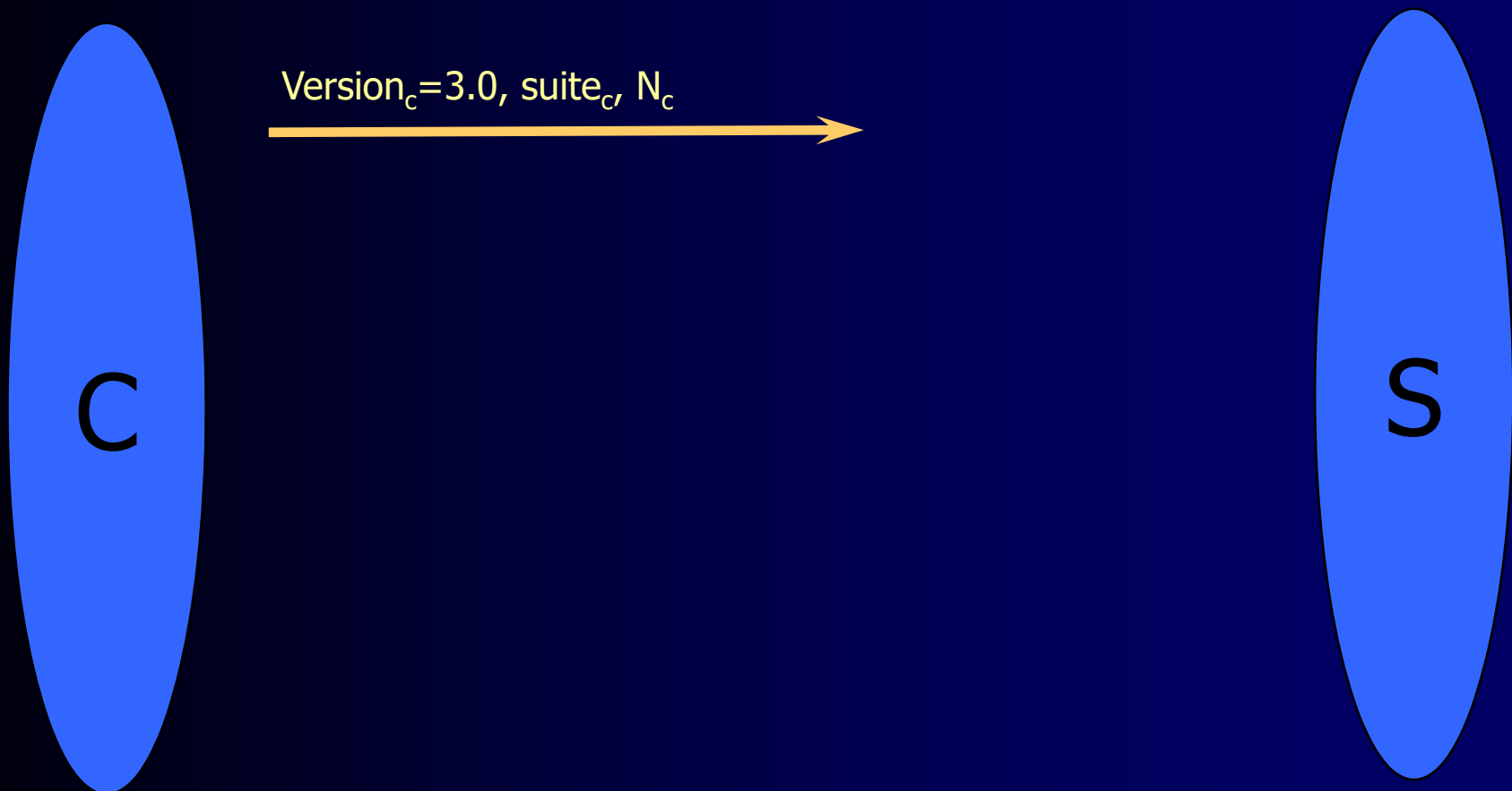
- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

حملات انجام شده با بهره گیری از ضعفهای پروتکل

- تنزل نسخه (۱۹۹۶ میلادی)
- تنزل الگوریتم تبادل کلید (۱۹۹۶ میلادی)
- از قلم انداختن پیام Change Cipher Spec (۱۹۹۶ میلادی)
- دستیابی به محتوای قالبهای رمز شده با بهره گیری از ضعفهای رمز قالبی

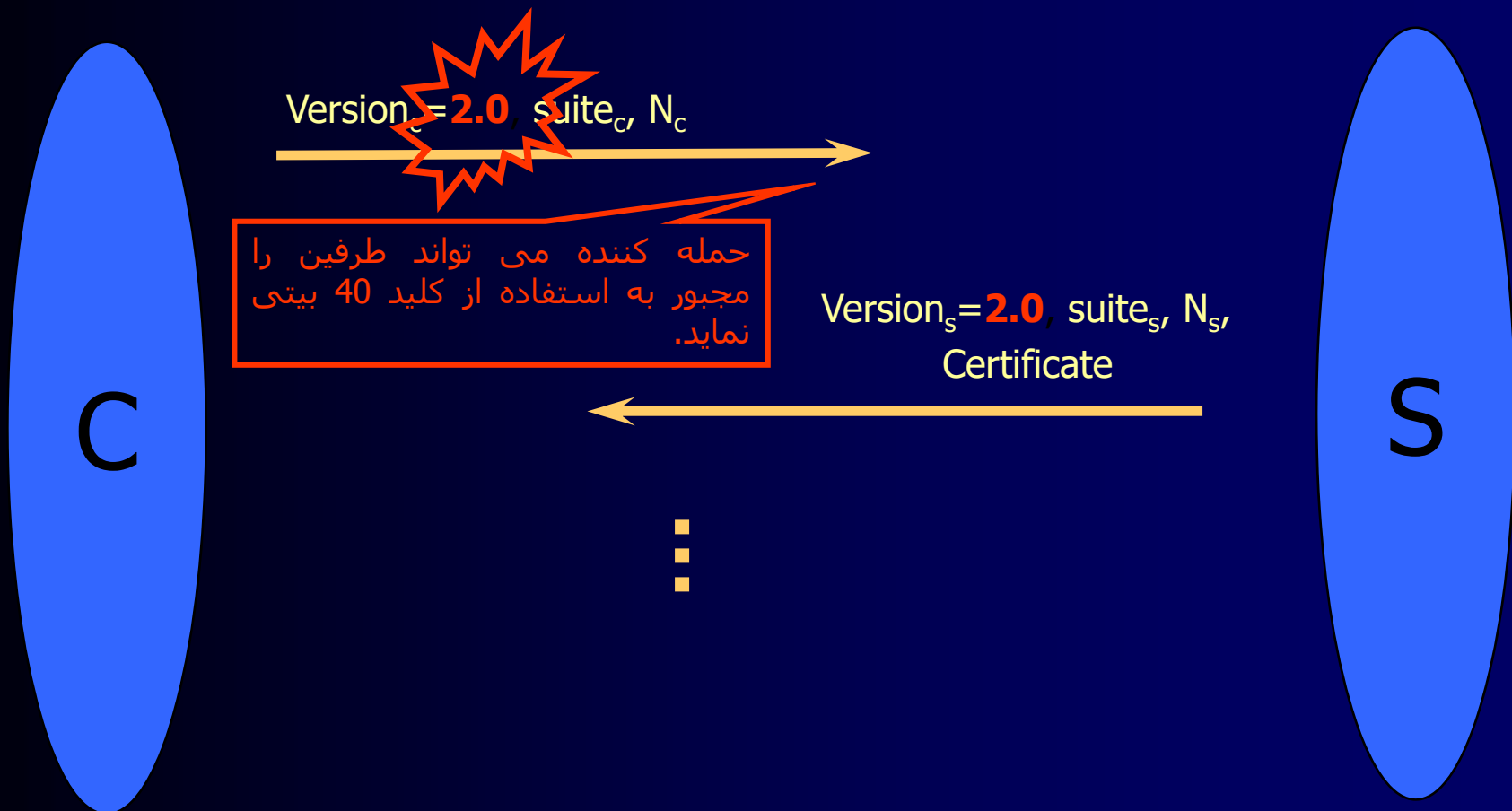
حمله تنزل نسخه

یکی از مهمترین ضعفهای نسخه SSL2.0 این است که پیامها را احراز اصالت نمی کند و حمله کننده به راحتی می تواند طرفین را مجبور به استفاده از کلید ۴۰ بیتی نماید.

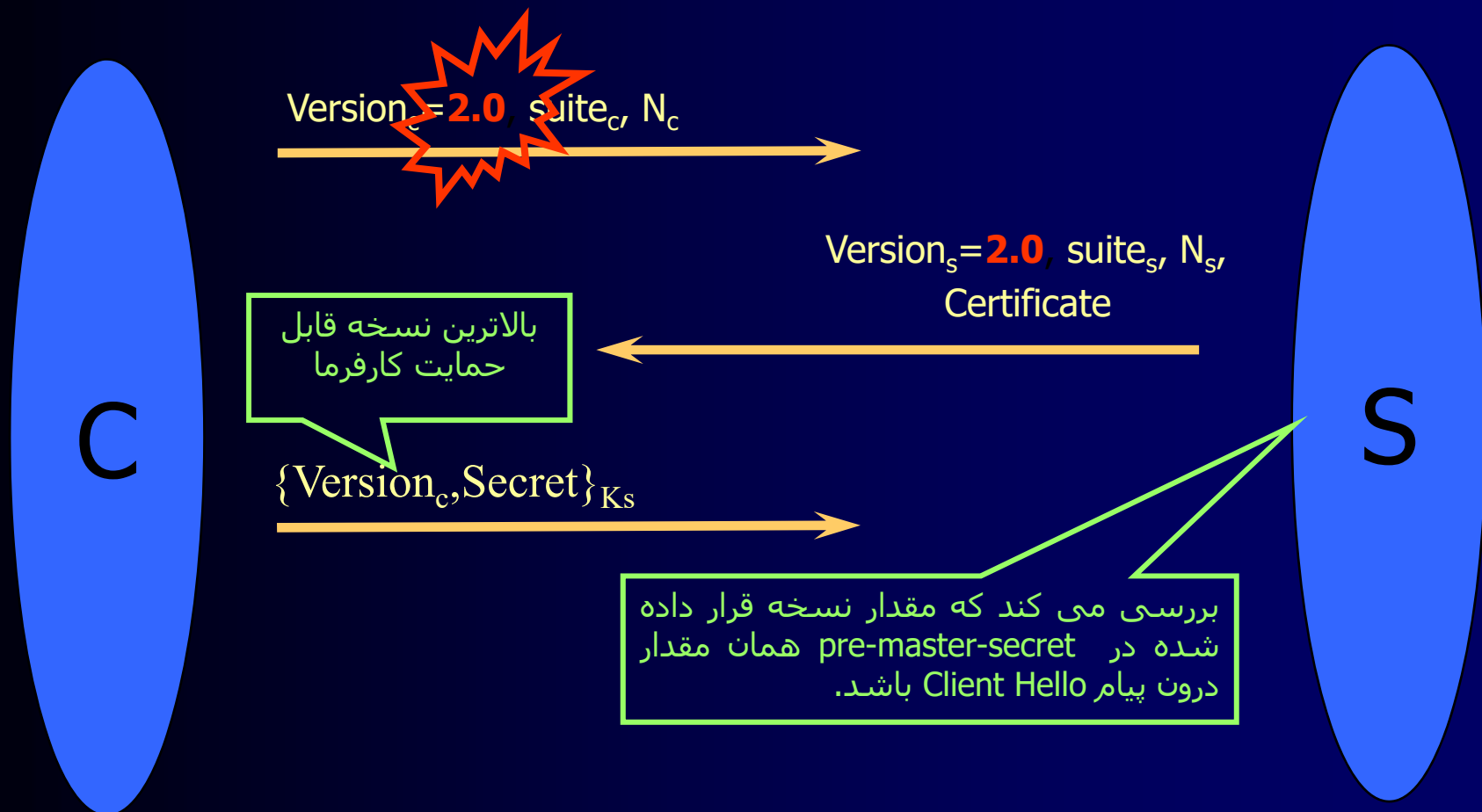


حمله تنزل نسخه

یکی از مهمترین ضعفهای نسخه SSL2.0 این است که پیامها را احراز اصالت نمی کند و حمله کننده به راحتی می تواند طرفین را مجبور به استفاده از کلید ۴۰ بیتی نماید.



آشکار کردن حمله تنزل نسخه



حمله از کاراندازی سرویس

Denial of Service (DoS)

- راهکارهای مقابله با حمله DoS در SSL

۱. استفاده از مکانیزم های مطرح در مقابله با حملات DoS در لایه انتقال
۲. استفاده از روش حل معما

حمله تحلیل ترافیک

- SSL سرآیندهای TCP/IP را رمز نمی کند و در نتیجه اطلاعات مقصد، مبدأ و ساینز بسته ها قابل دسترسی است.

- روند حمله

۱. تهیه یک پایگاه داده از اطلاعات صفحات داخل سایت هدف
۲. شنود بسته های منتقل شده بین کارفرما و کارگزار با استفاده از ابزار شنودگر بسته
۳. جستجوی پایگاه داده برای یافتن صفحه منطبق با اطلاعات شنود شده
یک نمونه خروجی شنودگر بسته:

1460: herland.CS.Berkeley.EDU.1463 > amber.Berkeley.EDU.4243

مبدأ

مقصد

ساینز بسته IP

حمله تحلیل ترافیک (ادامه)

- راهکارهای مقابله

۱. اصلاح خود پروتکلها


مثال: اضافه کردن پوشش تصادفی به بسته ها

۲. اصلاح و بازسازی سایتهای وب

مثال: شکستن صفحه به چندین صفحه کوچکتر

حملات انجام شده با بهره گیری از ضعفهای محیط اجرای SSL

- حملات شخص در وسط ← استفاده از ضعف کاربر



برای انجام حمله شخص در
وسط حمله کننده باید گواهینامه
معتبری ارائه دهد

استفاده از پروتکل SSL

- حمله جستجوی کامل علیه کلیدهای ضعیف

کلیدهای ۴۰ بیتی در مدت زمان بسیار کوتاهی شکسته می شوند.