Secure Sockets Layer
Transport Layer Security
BEAST Attack

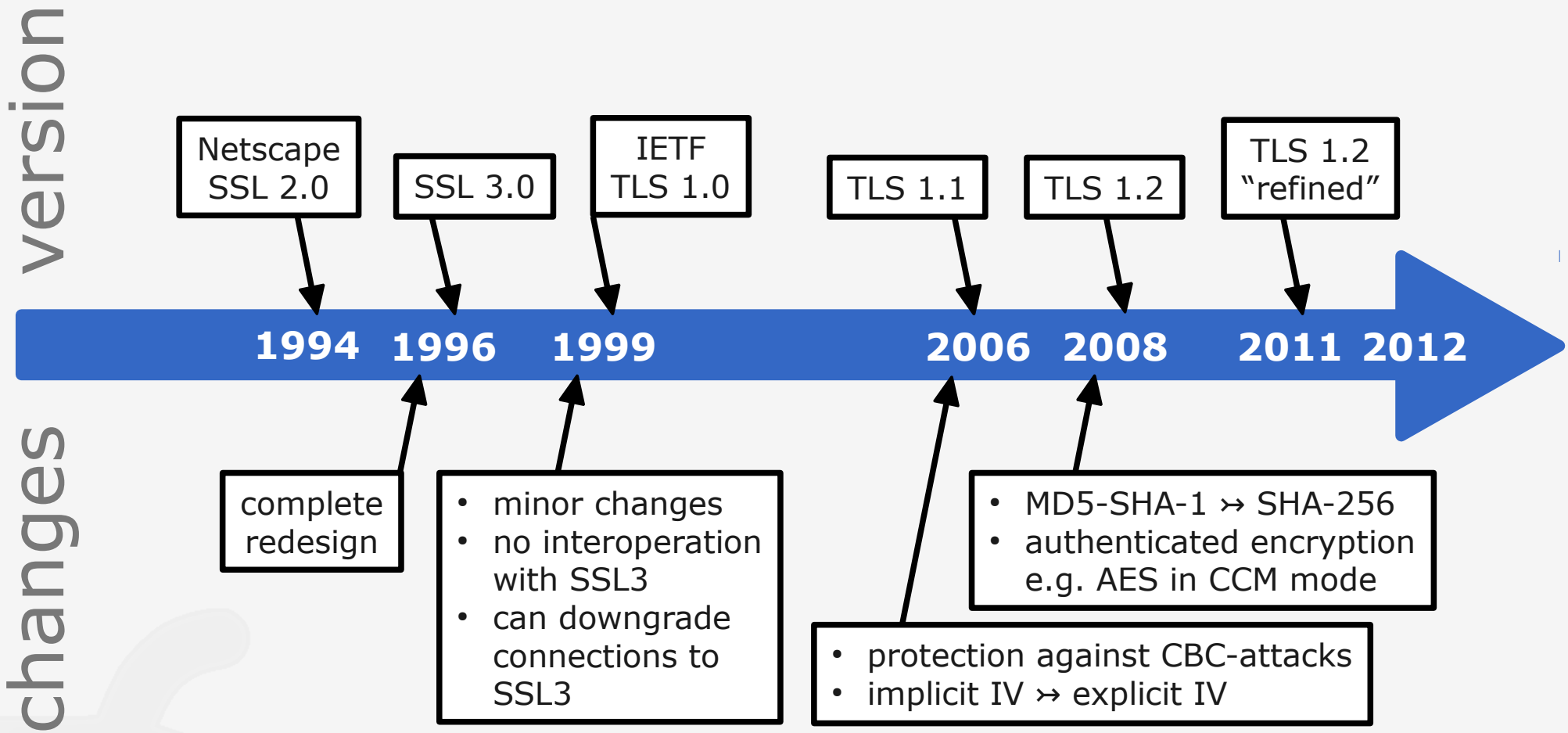
Outline

- History
- Design Goals
- SSL/TLS Stack
- Attacks
  - Attack on CBC
  - BEAST
- Solution

CBC Cipher Block Chaining

BEAST Browser Exploit Against SSL/TLS

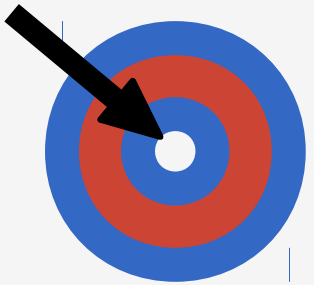
History



MAC	Message Authentication Code
IETF	Internet Engineering Task Force
CBC	Cipher Block Chaining
IV	Initialization Vector
MD5	Message Digest Algorithm
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard
CCM	Counter with CBC-MAC

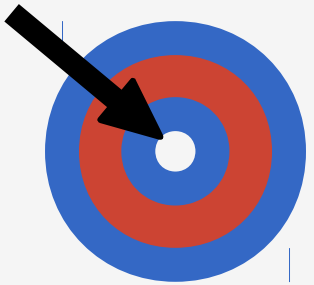
Design Goals

- Cryptographic security
  - establish secure connections
  - secure existing connections
  - data confidentiality
  - authentication
  - reliability
- Interoperability
  - applications exchange parameters with each other
  - applications establish connections with each other
  - specified protocols



Design Goals

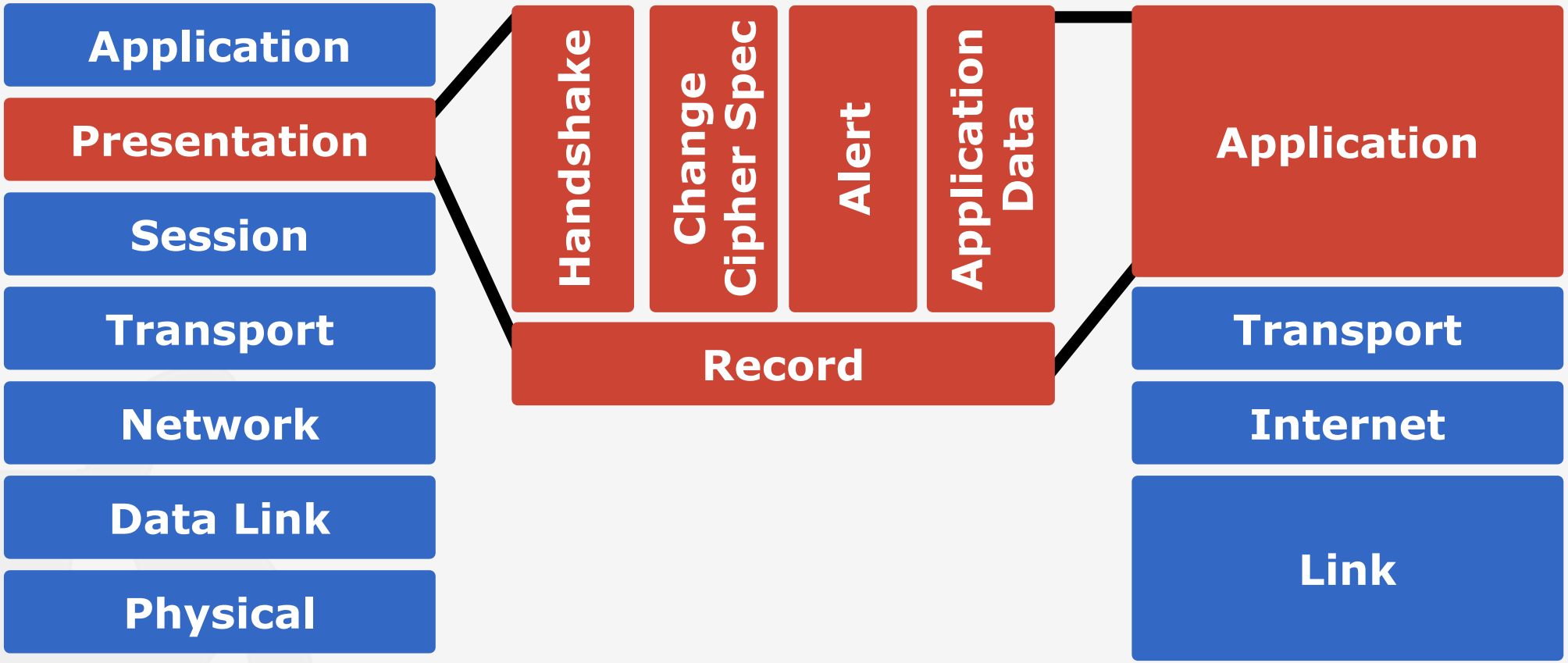
- Extensibility
  - SSL/TLS provides a framework
  - cryptographic methods can be added
    - public key
    - bulk encryption
  - no extensive library/protocol rewriting
- Relative efficiency
  - ability to adopt to its environment
  - session caching (saves CPU)
  - minimal messaging (saves network bandwidth)



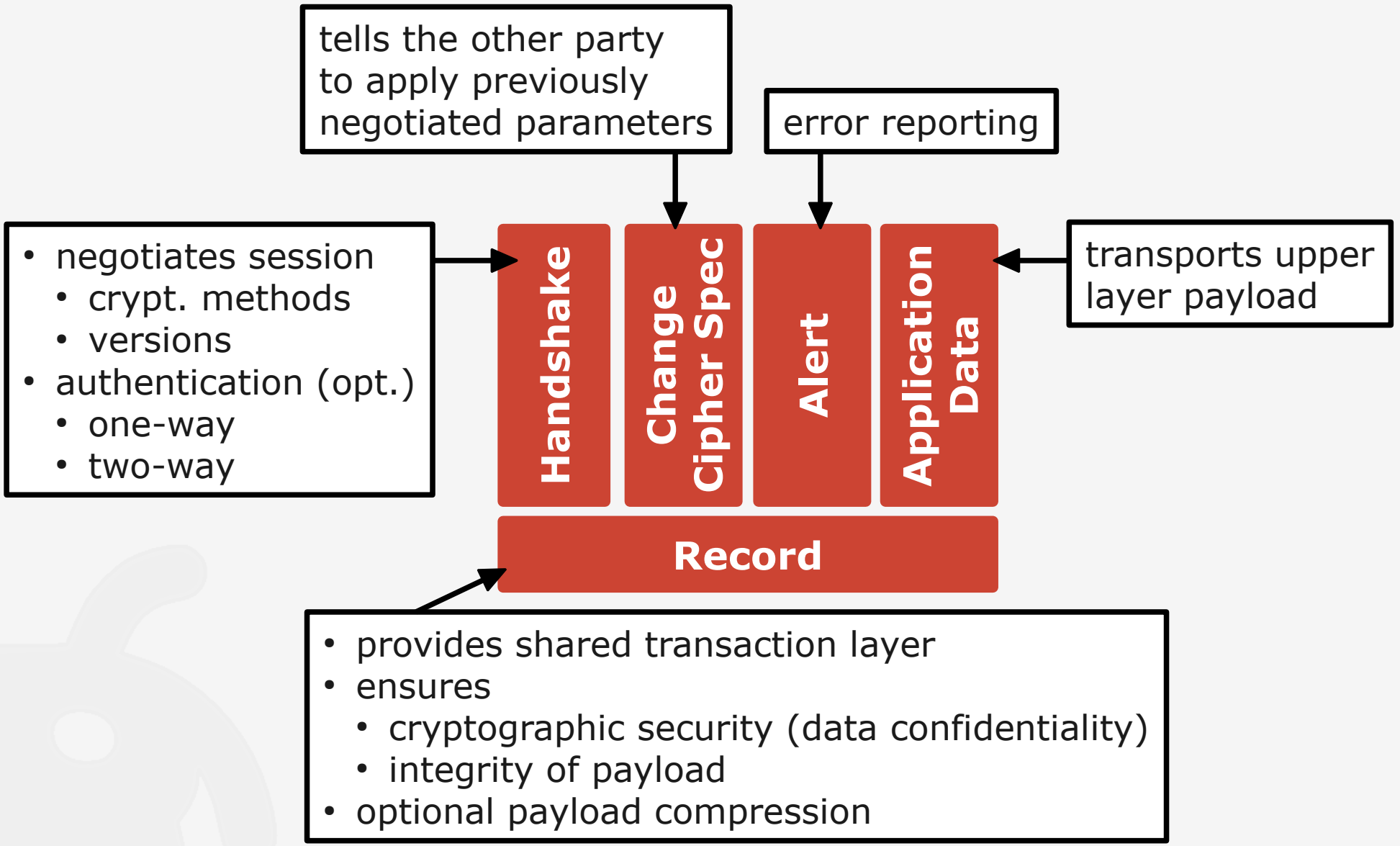
SSL/TLS in Common Models

ISO/OSI model

TCP/IP model



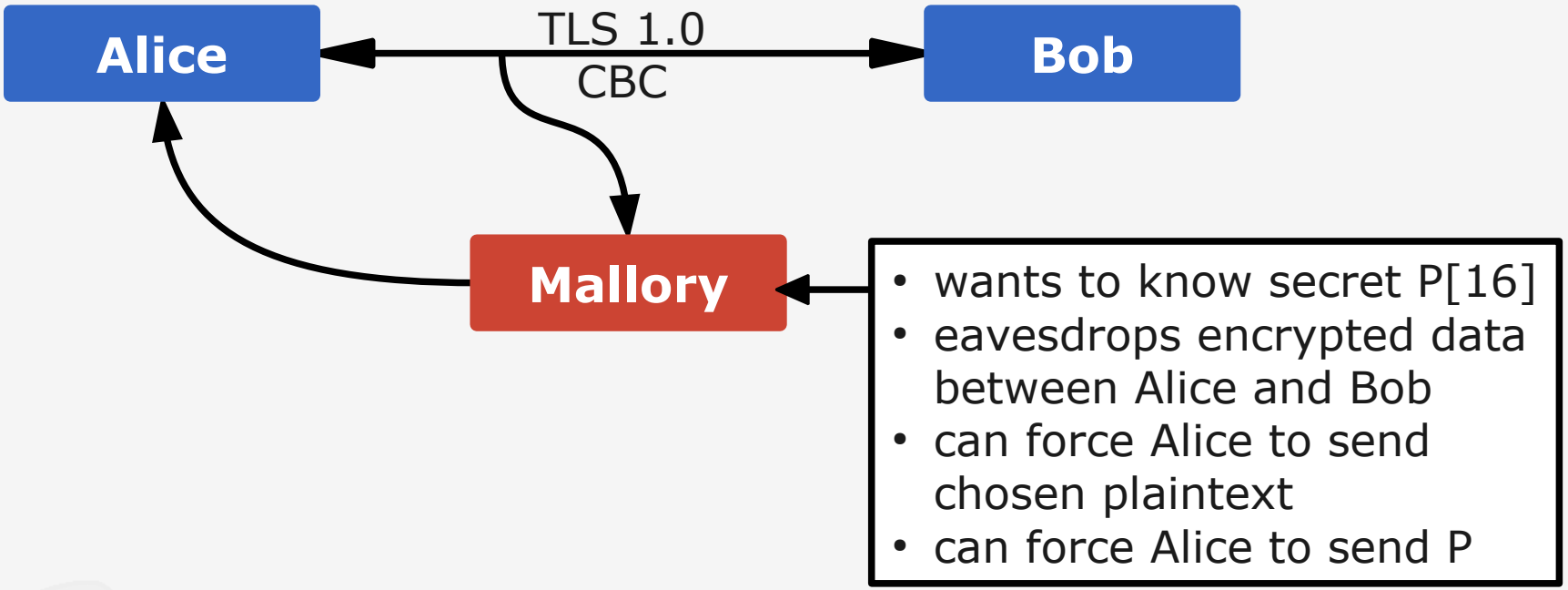
SSL/TLS Protocol Stack



BEAST

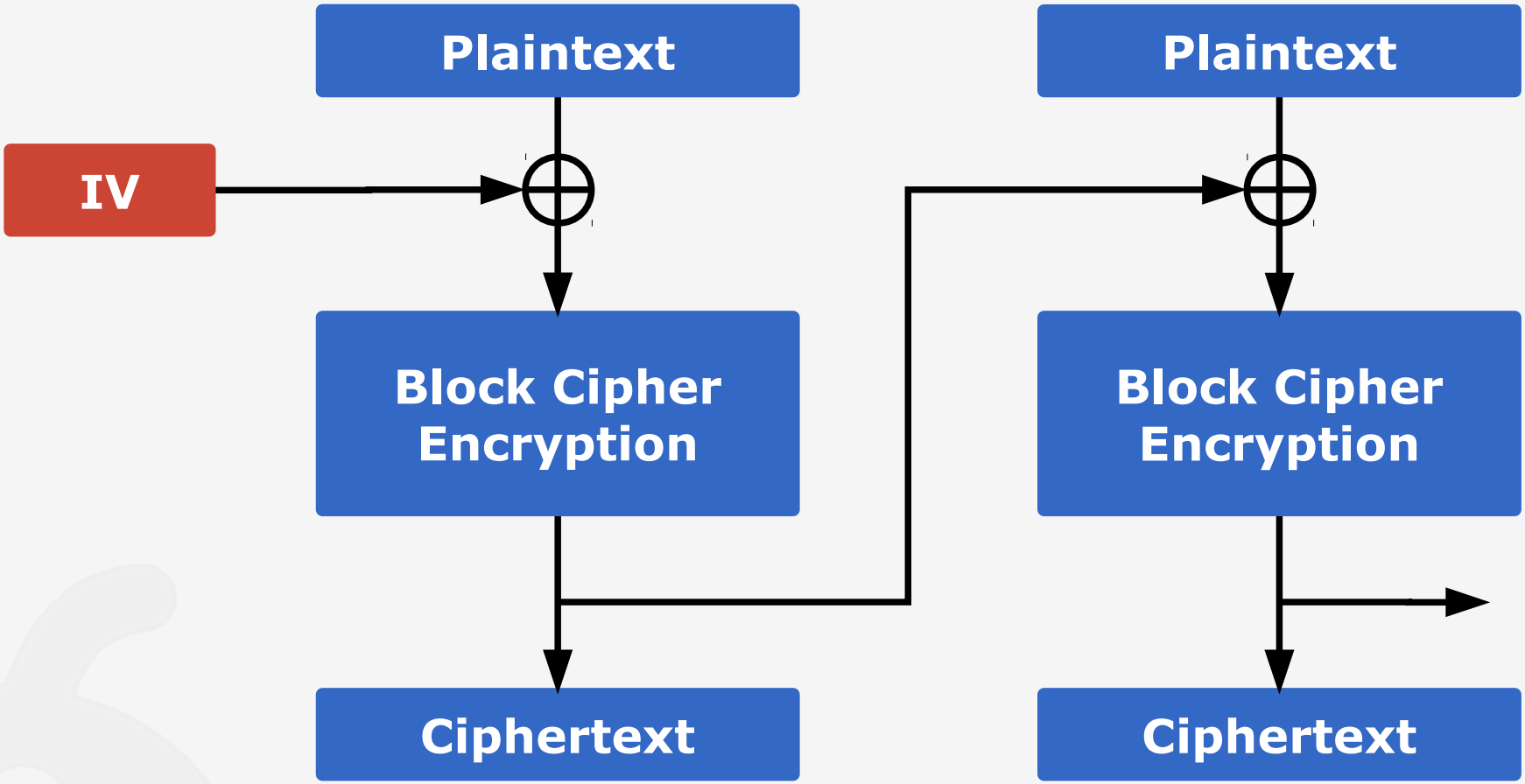
- Browser Exploit Against SSL/TLS (BEAST)
- Chosen Plaintext Attack
- Targets deterministic Initialization Vectors of Cipher-Block Chaining

Attack Scenario



Please note that this is a simplified example, consult reference *Educated Guesswork* for details.

Cipher-Block Chaining



CBC Chosen Plaintext Attack

- Force Alice to send **P**
- Eavesdrop and get $C_p = E(Key, C_{p-1} \oplus P)$
- Let **G** be a blind guess of **P**
- Force Alice to send plaintext $C_{i-1} \oplus C_{p-1} \oplus G$
- Alice sends $C_i = E(Key, C_{i-1} \oplus C_{i-1} \oplus C_{p-1} \oplus G)$
  - $C_i = E(Key, C_{p-1} \oplus G)$
- If $C_i == C_p$ then $G == P$

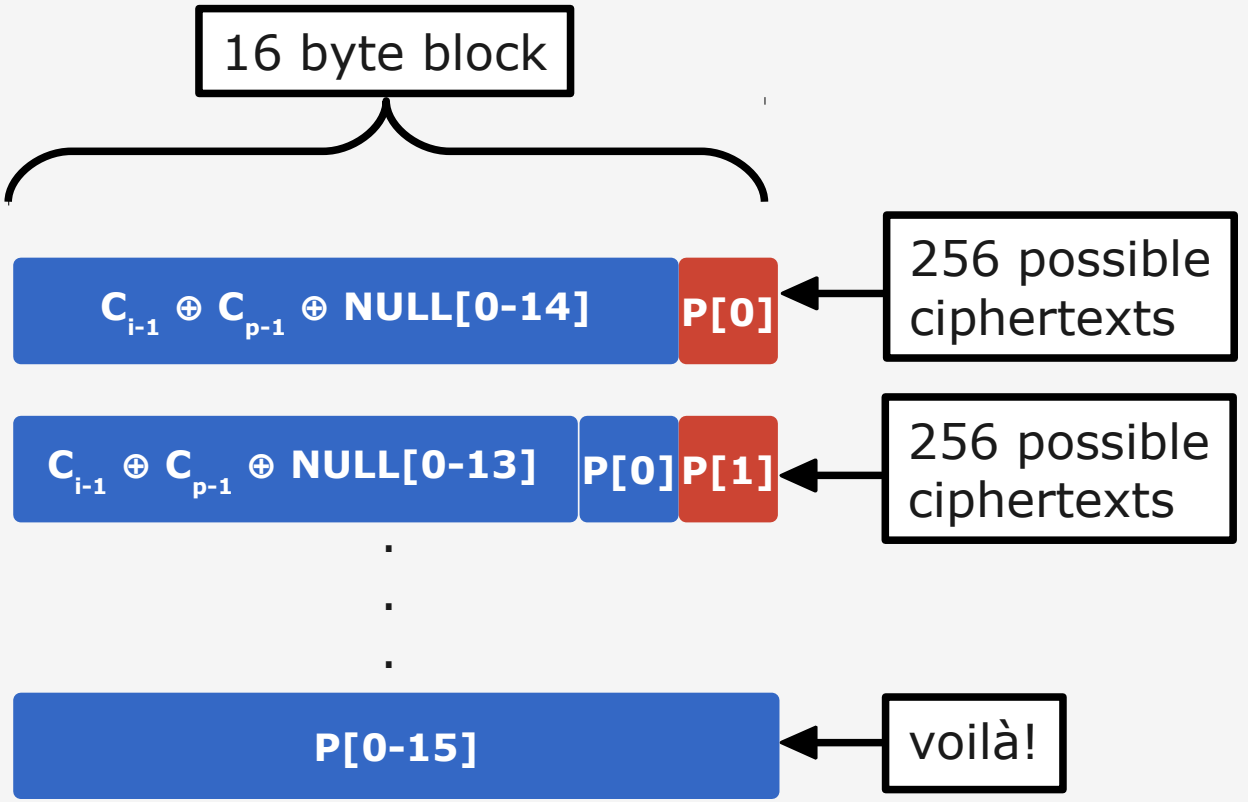
This requires a lot of guessing and it is not very handy!

BEAST

- Force Alice to send **NULL[0-14] P[0]**
- Eavesdrop and get
  C_p = **E(Key,** C_{p-1} ⊕ **NULL[0-14] P[0])**
- Let **G** be a blind guess of **P[0]**
- Force Alice to send plaintext
  C_{i-1} ⊕ C_{p-1} ⊕ **NULL[0-14] G**
- Alice sends
  C_i = **E(Key,** C_{i-1} ⊕ C_{i-1} ⊕ C_{p-1} ⊕ **NULL[0-14] G)**
  C_i = **E(Key,** C_{p-1} ⊕ **NULL[0-14] G)**
- If C_i==C_p then **G==P[0]**

This requires up to 2^8=256 guesses. We can do this!

BEAST

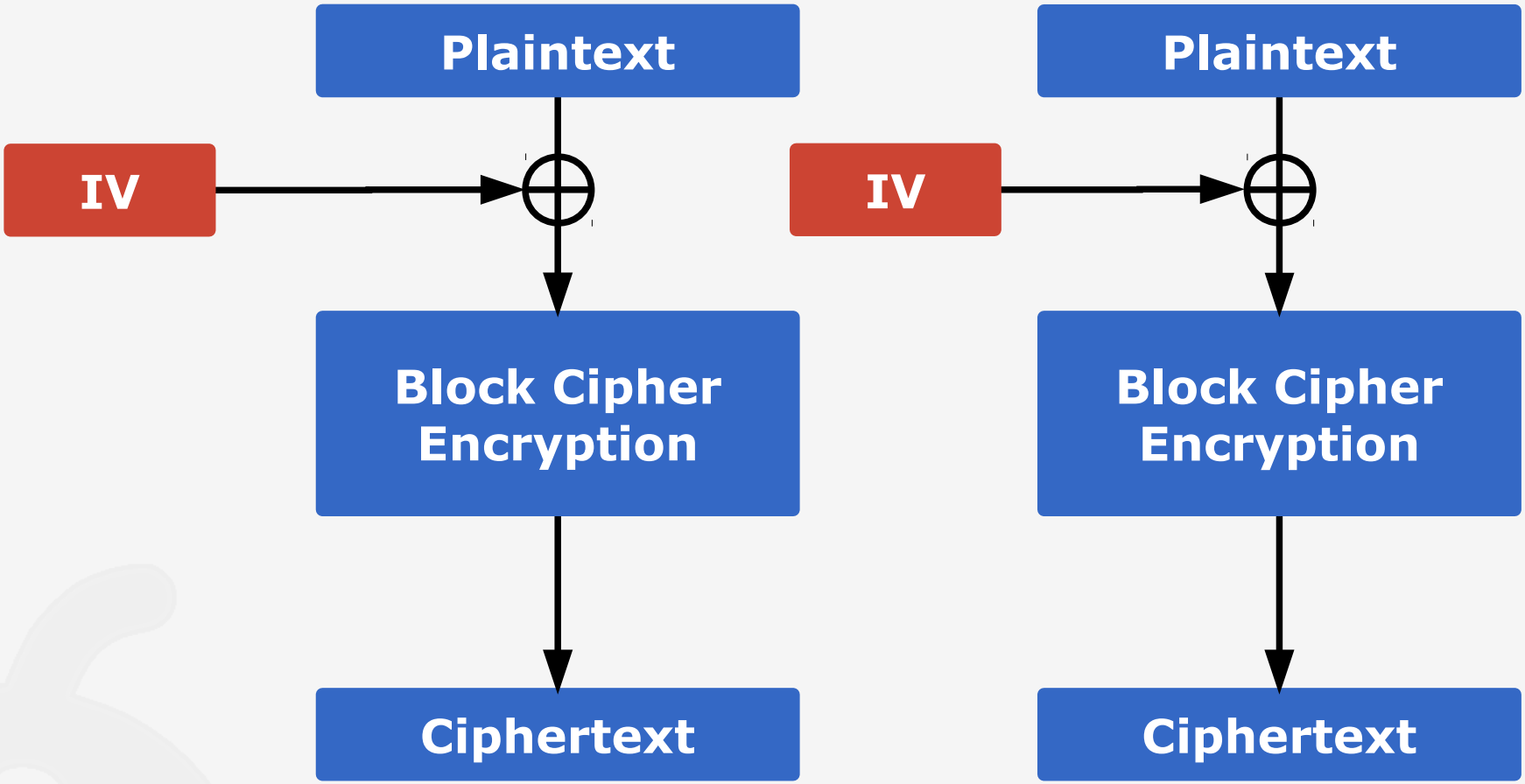


legend:

known

unknown

Solution: Explicit IV



$C_0 = E(Key, IV_0 \oplus M_0)$

$C_i = E(Key, IV_i \oplus M_i)$

Questions?

Thank you for your kind attention.

- References
  - Jörg Schwenk. Sicherheit und Kryptographie im Internet: Von sicherer E-Mail bis zu IP-Verschlüsselung (German Edition). Vieweg+Teubner Verlag, 2010.
  - T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), January 1999. Obsoleted by RFC 4346, updated by RFCs 3546, 5746, 6176.
  - T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (Proposed Standard), April 2006. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681, 5746, 6176.
  - Dan Goodin. Hackers break SSL encryption used by millions of sites. The Register, 2011. http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/ (Retrieved 2012-04-13)
  - Security impact of the Rizzo/Duong CBC "BEAST" attack. Educated Guesswork, 2011. http://www.educatedguesswork.org/2011/09/security_impact_of_the_rizzodu.html (Retrieved 2012-04-13)