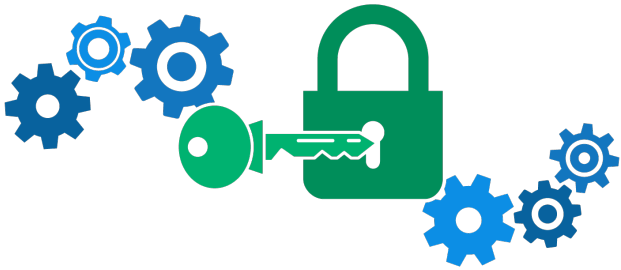


Encryption -> the left, right and what's left

By

Nitin Ramesh

What is Encryption?

Process of encoding particular information so that authorized parties with the correct key can decode and view that information.

Symmetric Encryption

Ex: DES, 3DES, AES, and RC4

Asymmetric Encryption

Ex: RSA

Shared Key Encryption

Public & Private Key Encryption

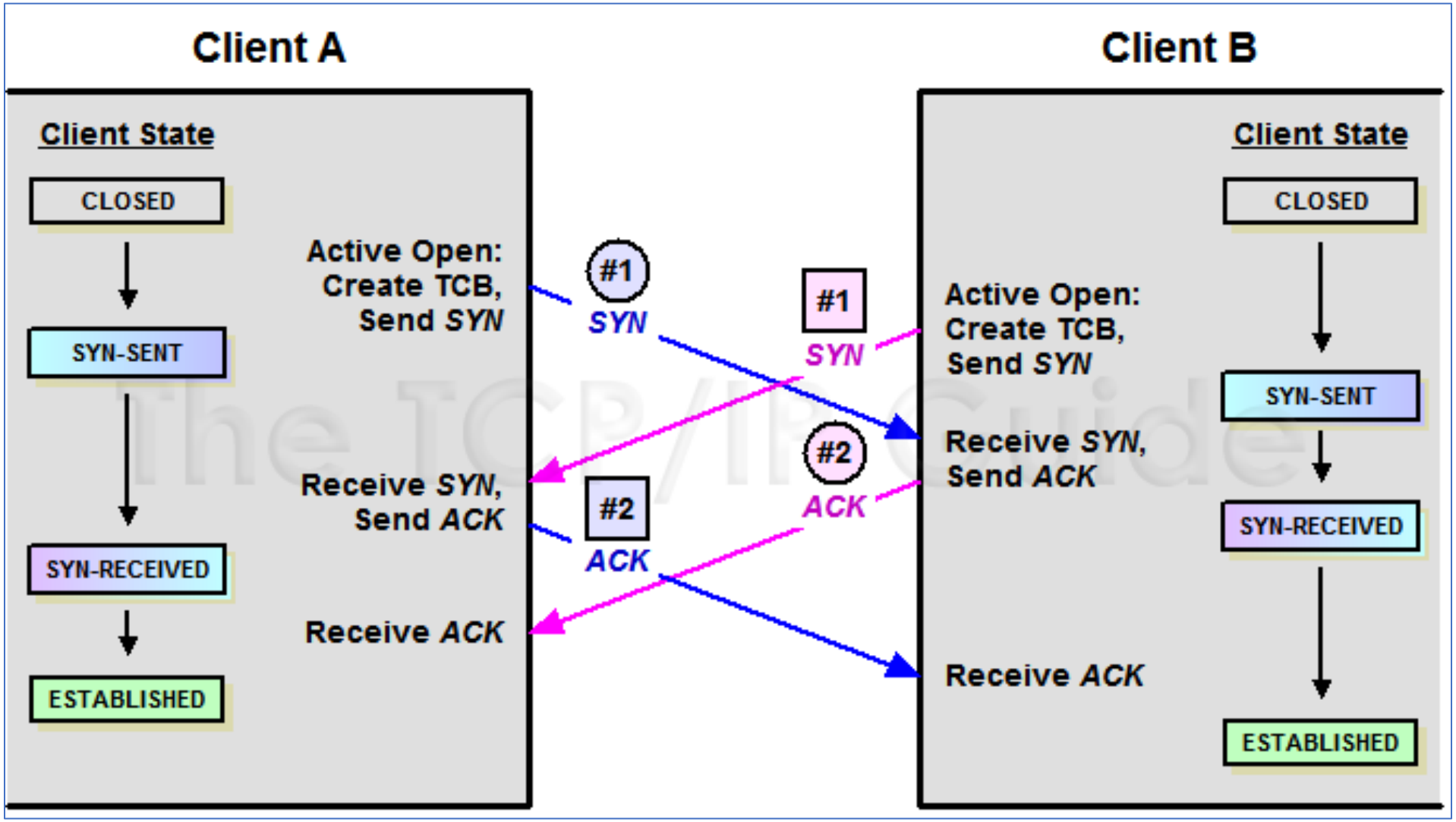
What is a Socket?

IP Address + Port Number

What is a SSL/TLS?

Standard security protocol for establishing encrypted links between a web server and a browser in an online communication

TCP Handshake



TLS Handshake

Request encrypted session + supported ciphers

Agreed Ciphers Suite type + Certificate (with public key)

Verify certificate + create symmetric key & encrypt with public key

Acknowledges successful activation of symmetric key

Secured Connection established

Cipher Suites

What is a Cipher?

A cipher is a technique/method of encrypting text.
Involves an algorithm that ciphers data and a key which defines the method of ciphering.

Block Cipher

Ex: DES, AES etc.

Considers a whole block

Stream Cipher

Ex: RC4, WAKE, Phelix etc.

Considers one bit at a time

Block Cipher

Applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time

---

Consists of 2 pairs of algorithms: E -> Encryption & D -> Decryption

---

Input

- Block of ‘n’ bits size
- Key - > K

Output

- Cipher Block of ‘n’ bits size

#Big Thing Alert 1

Encryption

$$E_K(P) := E(K, P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$ = C

K -> Key used in the encryption process.
k -> Length of the key used in the encryption process.
P -> Info String (Block to be ciphered).
n -> Length of the block.
C -> Cipher block of ‘n’ bits.

Decryption

E = T(D)

$$E_K^{-1}(C) := D_K(C) = D(K, C) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$ = P

Stream Cipher

(a.k.a State Cipher)

Applied to one bit of data at a single go, as a group rather than consider a block at a time.

Faster and less hardware intensive. 2 types ->Synchronous stream ciphers & Self synchronous stream ciphers

---

Input

- ‘n’ bits of information
- Key - > K

Output

- Cipher Block of ‘n’ bits size

What is a Cipher Suite?

A cipher suite is a set of algorithms that help secure a network connection that uses Transport Layer Security (TLS) or Secure Socket Layer (SSL).

Cipher Suite

Key Exchange Algorithm

Bulk Encryption Algorithm

Message Authentication Algorithm

1. Key Exchange Algorithm:
   Method by which cryptographic keys are exchanged between 2 parties to use a crypt algorithm.

2. Bulk Encryption Algorithm:
   Algorithms that encrypts & decrypt all the traffic at the either ends of the communication lines.

3. Message Authentication Algorithm:
   Short piece of information used to authenticate a message. (Verification Hashes)

Cipher Suite Breakdown

Key exchange / agreement	Authentication	Block / Stream Ciphers	Message Authentication
RSA	RSA	RC4	Hash-based MD5
Diffie-Hellman	DSA	Triple DES	SHA Hash Function
ECDH	ECDSA	AES	
SRP		IDEA	
PSK		DES	
		Camellia	

Cipher Suite Block

```
TLSV1_2 Cipher Suites:
  Preferred:
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384          ECDH-256 bits  256 bits      HTTP 200 OK

  Accepted:
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384          ECDH-256 bits  256 bits      HTTP 200 OK

    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384          ECDH-256 bits  256 bits      HTTP 200 OK

    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA             ECDH-256 bits  256 bits      HTTP 200 OK

    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256          ECDH-256 bits  128 bits      HTTP 200 OK

    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA             ECDH-256 bits  128 bits      HTTP 200 OK

    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256          ECDH-256 bits  128 bits      HTTP 200 OK
```

```
TLSV1_2 Cipher Suites:
  Preferred:
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

Key exchange / agreement	Authentication	Block / Stream Ciphers	Message Authentication
RSA	RSA	RC4	Hash-based MD5
Diffie-Hellman	DSA	Triple DES	SHA Hash Function
ECDH	ECDSA	AES	
SRP		IDEA	
PSK		DES	
		Camellia	

Same Algorithms But different Ciphers Suites?

TLS v1.0 -> TLS v1_1

1. Added protection against cipher-block chaining (CBC) attacks.
2. The implicit initialization vector (IV) was replaced with an explicit IV.
3. Change in handling of padding errors.
4. Support for IANA registration of parameters.

TLS v1_3 Cipher Suite

1. New cipher-suites only available in 1_3.
2. Removing support for MD5 and SHA-224 cryptographic hash functions
3. Requiring digital signatures even when a previous configuration is used
4. Prohibiting SSL or RC4 negotiation for backwards compatibility

Anonymous Ciphers

- Generally provides for confidentiality without the need for a certificate authority.
- That means, doesn't need a certificate.
- Provides encryption without authentication.
- Highly vulnerable to MIM attacks.

```
TLS_ECDH_anon_WITH_RC4_128_SHA (0xc016)   INSECURE      128
TLS_ECDH_anon_WITH_AES_128_CBC_SHA (0xc018)   INSECURE  128
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA (0xc017)   INSECURE 112
TLS_ECDH_anon_WITH_AES_256_CBC_SHA (0xc019)   INSECURE  256
TLS_ECDH_anon_WITH_RC4_128_SHA (0xc016)   INSECURE      128
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA (0xc017)   INSECURE 112
TLS_ECDH_anon_WITH_AES_128_CBC_SHA (0xc018)   INSECURE  128
TLS_ECDH_anon_WITH_AES_256_CBC_SHA (0xc019)   INSECURE  256
```

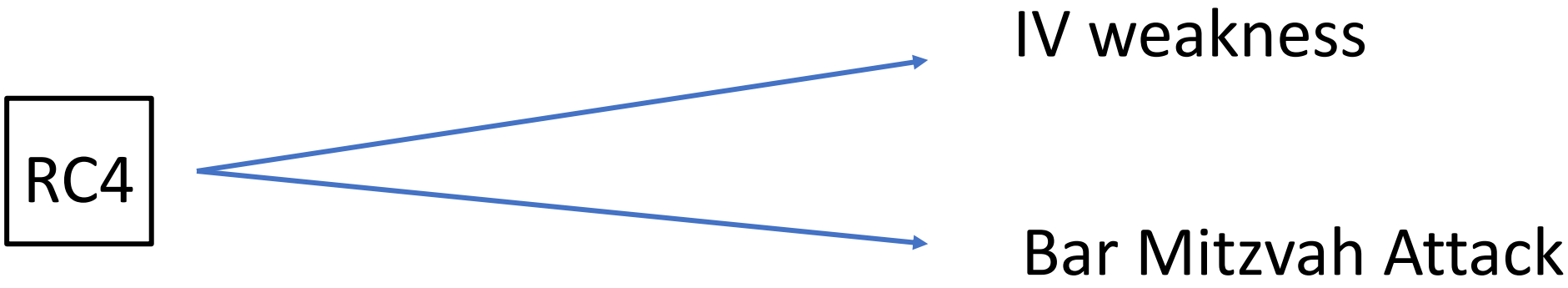
112 bit ciphers

Vulnerable Algorithms

Vulnerable Algorithm I - RC4

- Stream Cipher
- Used in popular security mechanisms like WEP/WPA (Wired Equivalent Privacy).
- Used in ARC4Random number generator.
- SSL (Secure Socket Layer)/TLS (Transport Layer Security)
- Microsoft’s RDP (Remote Desktop Protocol)
- BitTorrent

RC4 - Attacks



Vulnerable Algorithm II - DES

- NSA Approved Block Ciphers
- Superseded by the Advanced Encryption Standard (AES)
- DES uses a 56-bit key = 72,057,594,037,927,936 combinations
- Average of 23 hours to crack.

Website	Category
signin.ebay.com	E-commerce
account.nasdaq.com	Finance
www.bancomercantil.com	Banking
www.unionbankonline.co.in	Banking
ziraatbank.com.tr	Banking
www.state.nj.us	Government
secure.match.com	Dating
amadeus.net	Travel
walmart.com	Corporate
citrix.com	Corporate

High-profile websites that negotiate Triple-DES and accept at least 1 million requests in the same connection.

Vulnerable Algorithm III – 3DES

- Triple DES uses -> three DES keys, K1, K2 and K3, each of 56 bits

  ciphertext = EK3(DK2(EK1(plaintext)))

- DES encrypt -> K1, DES decrypt -> K2, then DES encrypt -> K3.

- Decryption:

  plaintext = DK1(EK2(DK3(ciphertext)))

- DES decrypt -> K3, encrypt -> K2, then decrypt -> K1

Sweet 32 Attack

1. The DES ciphers (and triple-DES) only have a 64-bit block size.

2. Need to run JS on browser -> capture 32 GB of data from single session.

3. Payload to generate a large amounts of traffic during the same TLS connection, creating a collision.

4. With this collision, the attacker is able to retrieve information such as a session cookie.

Vulnerable Algorithm – III - Remaining

- DES, 3DES, MD5, Sha1, AES, Blowfish, Diffie Hellman

Brute Force Search

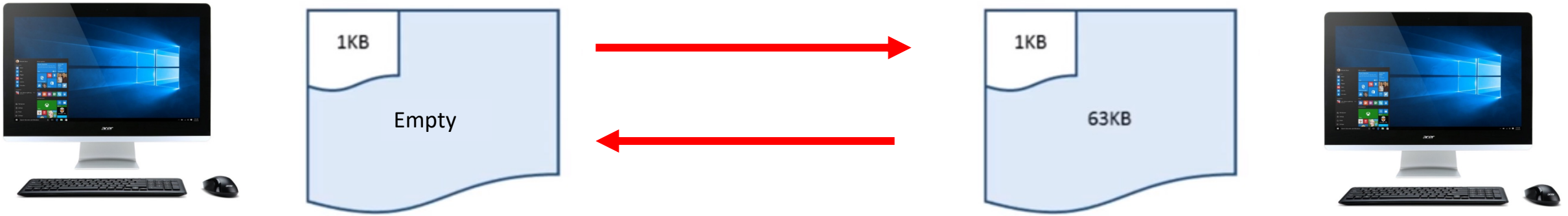
- always possible to simply try every key
- most basic attack, proportional to size of key space
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Attacks on Algorithms

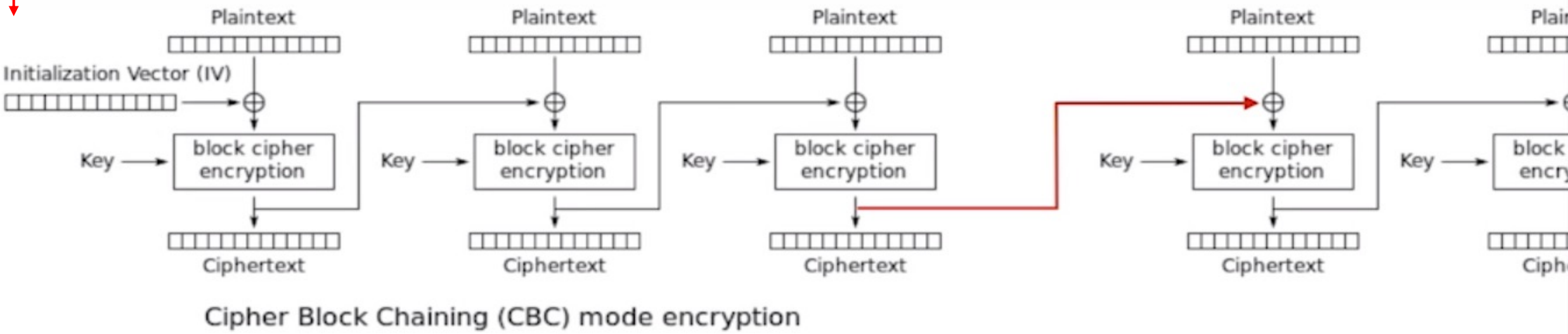
Heartbleed Attack

- Heart Beat is when one computer checks if the other computer listening is still “awake”.
- No sensitive info so usually not encrypted. Usually around 1 kb of data, upto 64kb.
- Send 1kb of data and tell its 64kb instead. Do it multiple times in a single instant.

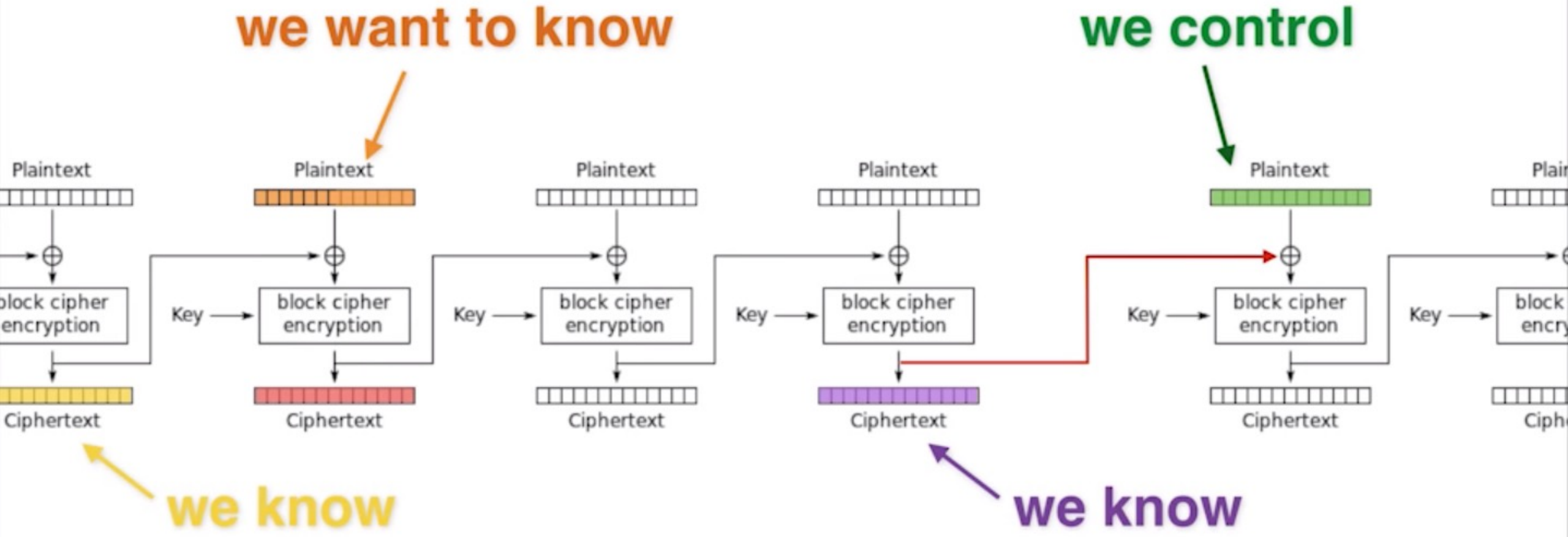


BEAST Attack

- BEAST -> Leverages weakness in CBC -> Exploits the SSL.
- Targets the use of repeated IV(s) -> Initialization vectors.
- More of a proof of concept.
- Requires JavaScript interception to increase request capture.



Cipher Block Chaining (CBC) mode encryption


we want to know
we control
Plaintext
Plaintext
Plaintext
Plaintext
Plaintext
Plain
block cipher encryption
Key
block cipher encryption
Key
block cipher encryption
Key
block cipher encryption
Key
block cipher encryption
Key
block
encry
Ciphertext
Ciphertext
Ciphertext
Ciphertext
Ciphertext
Ciph
we know
we know

POODLE Attack

- Force the backend, by supporting only SSLv3 and rejecting the TLS connections
- Need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages

Message	MAC	PADDING

- Uses CBC mode -> The encrypted block process is incorporated in to the next block.
- Mitigation: Upgrade from SSLV3 and set the TLS_FALLBACK_SCSV to prevent fallback to SSLv3.
- Essentially, TLS_FALLBACK_SCSV allows clients to send a hidden version number in the downgraded connection attempt in a way that doesn't trigger the server bugs.

Renegotiation

What is a Renegotiation?

Starting a new handshake negotiation inside of an existing secure session is called renegotiation.

Client Initiated Renegotiation

- The client side is allowed client to renegotiate new encryption parameters for an SSL/TLS connection within a single TCP connection.
- Handshakes usually involve a high degree of computational overhead.
- Done via a single thread is not very effective.
- But done over a distributed platform over a elongated period leads to DOS attacks.
- Use Rate limiters or don’t support this method.

Insecure Renegotiation

- A flaw in the design of the handshake process of SSL/TLS allows an attacker to inject arbitrary data into the beginning of a client's communication with a server during a man-in-the-middle attack.

Forwards all the requests to and from

Client Handshake request

intercepted

Initiates TLS connection + Payload injected

Payload

Initiates Renegotiation

Send intercepted Client handshake request

Handshake successful + Encrypted connection start

1st Sensitive Operation data sent to the Server

Sensitive Operation + Payload

Payload successful and response sent back

TLS - Certificates

What is a certificate?

Identification passed during a handshake to verify the website the browser is trying to connect to .

Certificate Validation Procedure

1. Step 1: Check public key and parameters.
2. Step 2: Check current date/time against validation period.
3. Step 3: Check revocation status in the CRL.
    - On-hold : Private key compromised
    - Revoked : Error/ misuse
4. Step 4: Checks the name constraints in the certificate.
5. Step 5: The path length is checked to ensure that it does not exceed any maximum path length
6. Step 6: The key usage extension is checked to ensure that is allowed to sign certificates

X.509 Certificates

- Standardized way of generating and validating certificates.
- Certificates confirm the identity of a service.
- Self-Signed Certificate is an identity certificate that is signed by the same entity whose identity it certifies.

The structure of an X.509 v3 digital certificate is as follows:

- Certificate
  - Version Number
  - Serial Number
  - Signature Algorithm ID
  - Issuer Name
  - Validity period
    - Not Before
    - Not After
  - Subject name
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
    - ...
- Certificate Signature Algorithm
- Certificate Signature

Certificates related vulnerabilities

X.509 Certificate About to Expire (SSL/TLS)

- Its about to be invalidated, so renew it

X.509 Certificate Expired (SSL/TLS)

- Its gone, pay the company again for a new one.

X.509 Certificate Not Yet Valid (SSL/TLS)

- Will work some day.

X.509 Certificate with Wrong Hostname (SSL/TLS)

- Who programmed this? Its made for a site with a different host name.

X.509 Certificate Chain Contains RSA Keys Less Than 2048 Bits (SSL/TLS)

- According to industry standards, certificates issued after January 1, 2014 must be at least 2048 bits.

Literally everything required to make a proper certificate:

- https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

TLS - Enforced/Enabled

Connection | **Security** | Birth Message | Will Message

Username

Password

Enable secure (SSL/TLS) connection

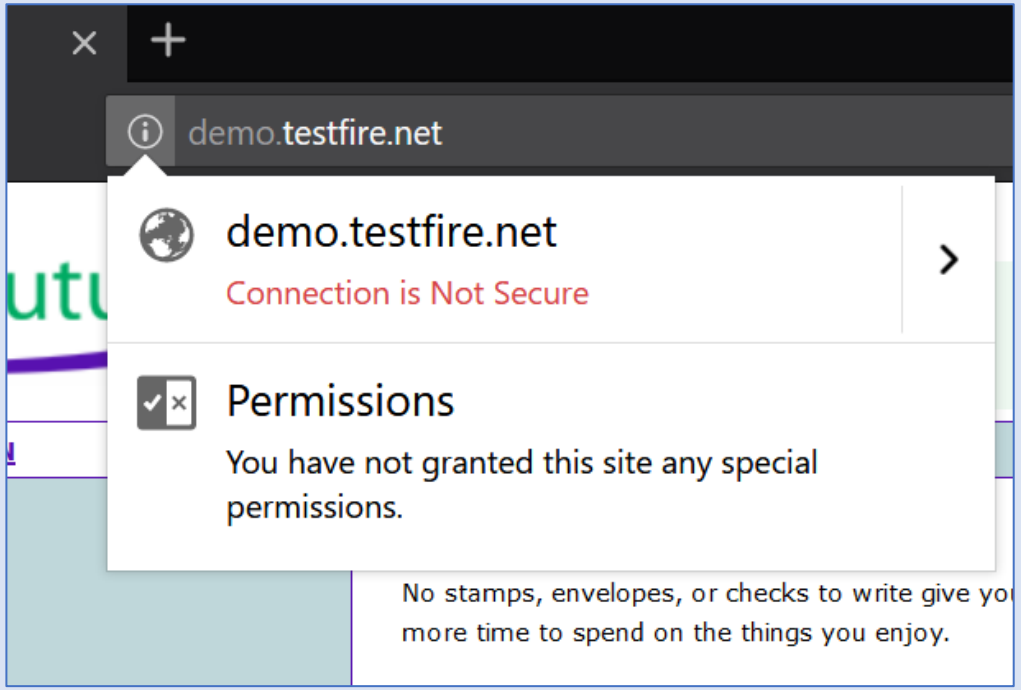
Verify server certificate

Helpful to click this link in the configuration.

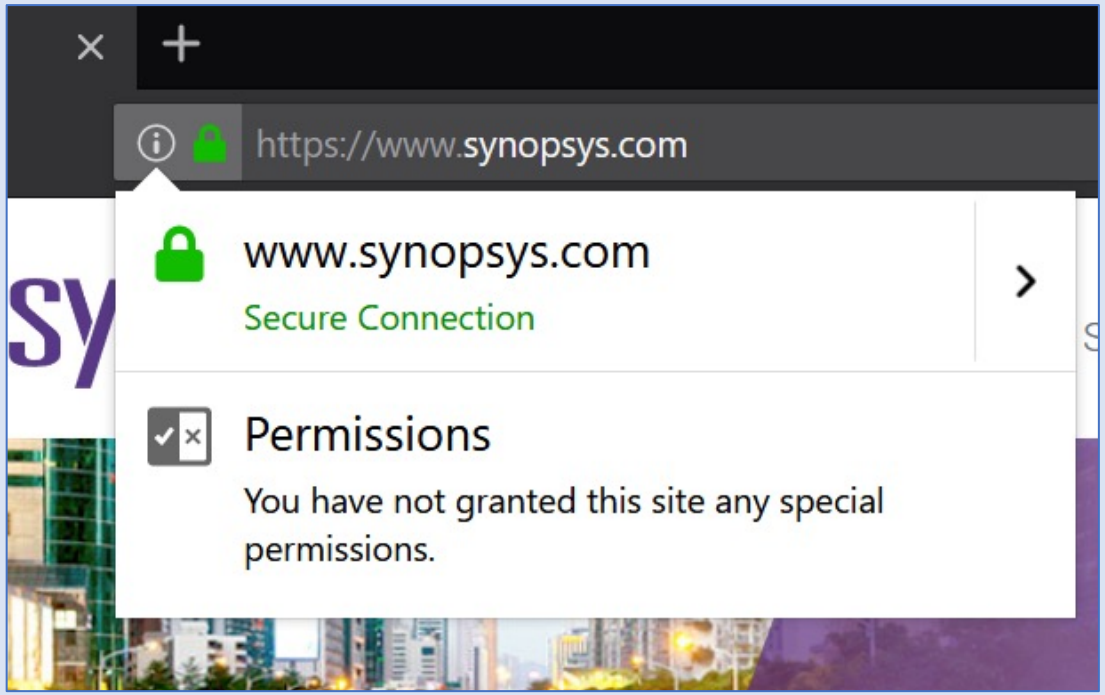
7 nodes use this config

Delete | Update | Cancel

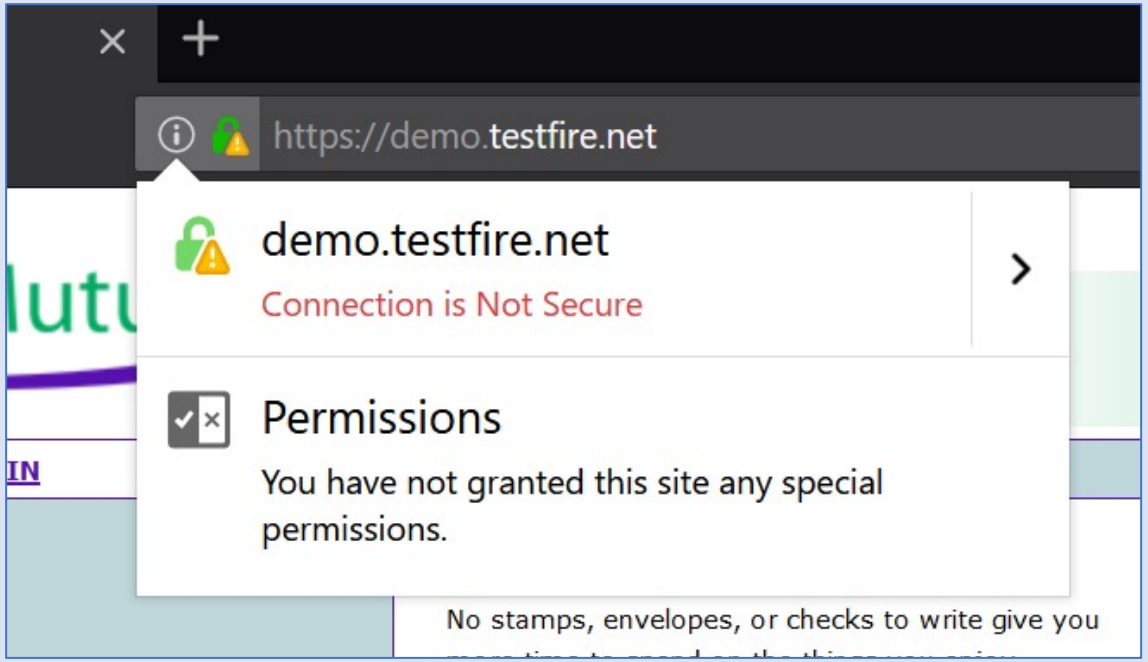
1

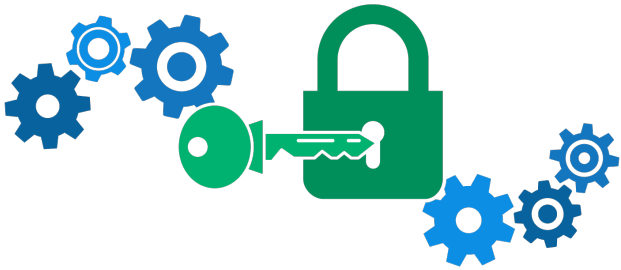

demo.testfire.net
demo.testfire.net
Connection is Not Secure
Permissions
You have not granted this site any special permissions.
No stamps, envelopes, or checks to write give yo
more time to spend on the things you enjoy.

2


https://www.synopsys.com
www.synopsys.com
Secure Connection
Permissions
You have not granted this site any special permissions.

3


https://demo.testfire.net
demo.testfire.net
Connection is Not Secure
Permissions
You have not granted this site any special permissions.
No stamps, envelopes, or checks to write give you



Thank you