Giới thiệu về khái niệm SSL & HTTPS

- SSL là gì?
- - SSL (Secure Sockets Layer) là một giao thức để mã hóa thông tin.

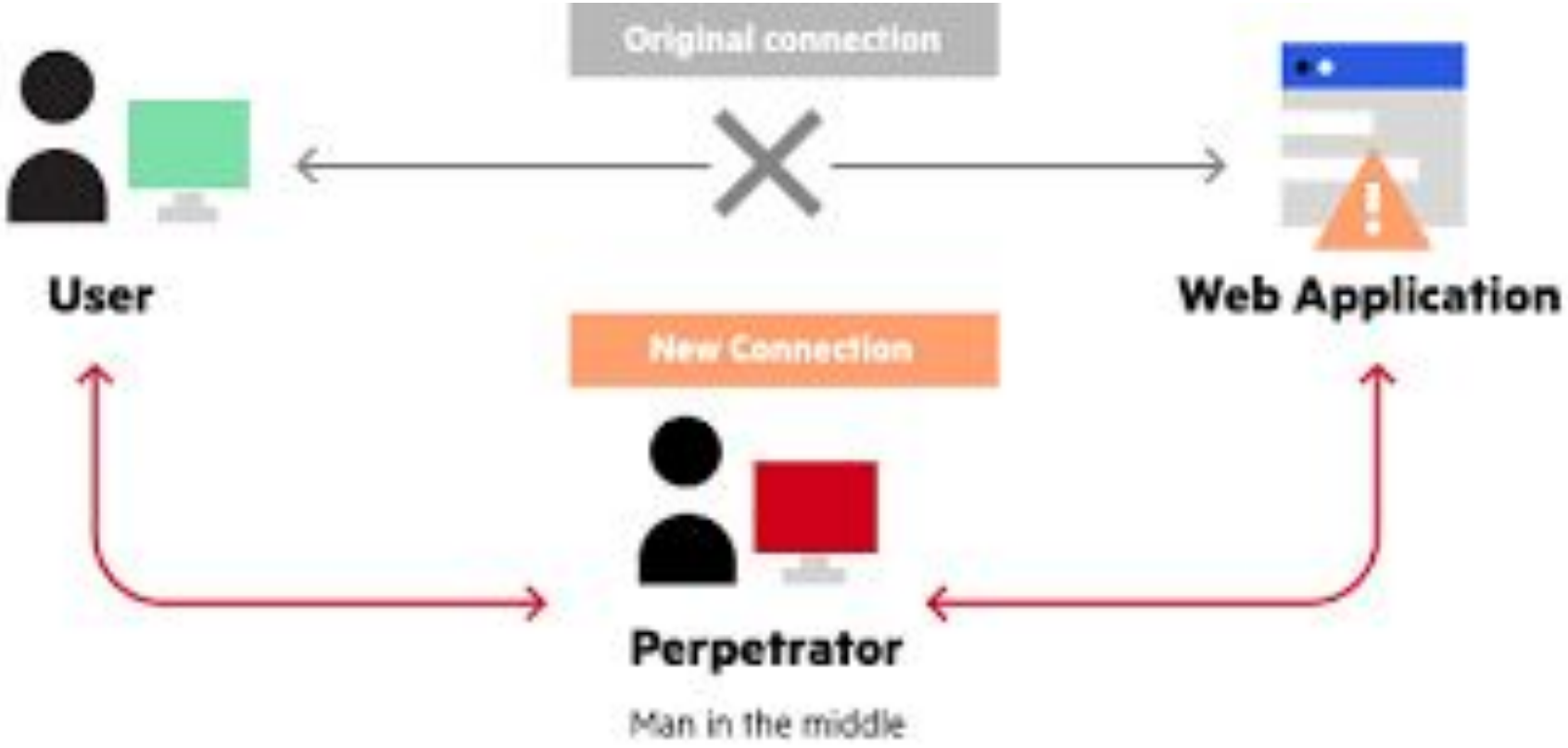
http là gì:
- http là một giao thức truyền tải giúp máy tính có thể giao tiếp với nhau qua mạng

- HTTPS là gì?
- - Cung cấp truyền thông an toàn trên internet.
- HTTPS (HyperText Transfer Protocol Secure) là HTTP kết hợp với mã hóa SSL/TLS.

  - Bảo vệ thông tin nhạy cảm như thông tin đăng nhập, thanh toán.

Các cuộc tấn công HTTP phổ biến

- Tấn công Man-in-the-Middle (MITM)
- Chiếm quyền phiên (Session Hijacking)
- Theo dõi gói tin (Packet Sniffing)
- Tấn công XSS và CSRF


Original connection
User
Web Application
New Connection
Perpetrator
Man in the middle

Wireshark · Packet 7 · wireshark_enp2s0_20171114084337_pMTUlm

```
▸ Frame 7: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
▸ Ethernet II, Src: HewlettP_3d:1a:33 (a0:d3:c1:3d:1a:33),
▸ Internet Protocol Version 4, Src: 192.168.2.146,
▸ Transmission Control Protocol, Src Port: 46432, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
00f0  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0100  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 2a 2f 2a   on/xml;q =0.9,*/*
0110  3b 71 3d 30 2e 38 0d 0a  41 63 63 65 70 74 2d 4c   ;q=0.8.. Accept-L
0120  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
0130  6e 3b 71 3d 30 2e 35 0d  0a 41 63 63 65 70 74 2d   n;q=0.5. .Accept-
0140  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
0150  64 65 66 6c 61 74 65 0d  0a 43 6f 6e 74 65 6e 74   deflate. .Content
0160  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -Type: a pplicati
0170  6f 6e 2f 78 2d 77 77 77  2d 66 6f 72 6d 2d 75 72   on/x-www -form-ur
0180  6c 65 6e 63 6f 64 65 64  0d 0a 43 6f 6e 74 65 6e   lencoded ..Conten
0190  74 2d 4c 65 6e 67 74 68  3a 20 32 35 0d 0a 52 65   t-Length : 25..Re
01a0  66 65 72 65 72 3a 20 68  74 74 70 3a 2f 2f 63 61   ferer:
01b0  73 70 65 72 2e 6a 6f 6e  77 61 74 73 6f 6e 2e 63
01c0  61 2f 6c 6f 67 69 6e 2d  68 74 74 70 2d 74 65 73    /login- http-tes
01d0  74 2e 70 68 70 0d 0a 43  6f 6e 6e 65 63 74 69 6f   t.php..C onnectio
01e0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive..U
01f0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
0200  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 0d 0a 75   Requests : 1....u
0210  73 65 72 6e 61 6d 65 3d  66 6f 6f 26 70 61 73 73   sername= foo&pass
0220  77 6f 72 64 3d 62 61 72                           word=bar
```

Tại sao https có thể giúp ngăn chặn

các cuộc tấn công trên

SSL Termination là gì?

- Sau khi request tới chỗ người vận hành cài cert thì request sẽ được giải mã.
- SSL Termination là quá trình giải mã dữ liệu được mã hóa bằng SSL.
- Thực hiện tại thiết bị chuyên dụng để giảm tải công việc xử lý SSL từ máy chủ.
-
- Tại sao cần SSL Termination?

Vị trí thực hiện SSL Termination (ví dụ trong techcombank)

- Các vị trí thực hiện SSL Termination
- - Load Balancers (ví dụ: F5, NGINX, Citrix ADC)
- - Reverse Proxies
- - Web Servers
- Cách hoạt động: Sau khi giải mã, dữ liệu được chuyển đến các máy chủ nội bộ dưới dạng http.

Lưu ý khi vận hành cert

Kết luận

- Điểm cần nhớ
- - SSL đảm bảo giao tiếp được mã hóa để ngăn chặn tấn công.
- - SSL Termination giảm tải việc giải mã để cải thiện hiệu suất và quản lý chứng chỉ.
- Người vận hành cần nắm rõ ssl để thay đúng hạn