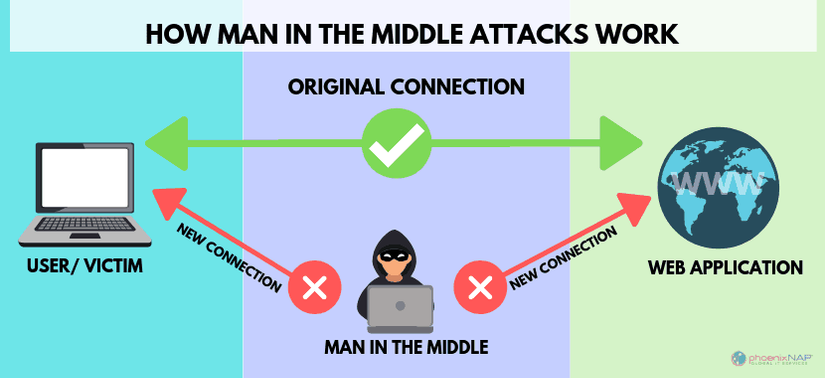
# Man-in-the-Middle Attack (MITM)

[Browser](https://viblo.asia/tags/browser) [Attack](https://viblo.asia/tags/attack) [Information Security](https://viblo.asia/tags/information-security)

Cùng tìm hiểu về kiểu tấn công lấy con người làm trung gian Man-in-the-Middle attack (MITM) trong bài viết dưới đây!

## 1. Key concepts of a Man-in-the-Middle attack



Man-in-the-Middle attack có thể được viết tắt theo nhiều cách: MITM, MitM, MiM hoặc MIM, cách dùng trong bài viết này là MITM.

MITM là một kiểu tấn công bí mật xảy ra khi kẻ tấn công tự nhét mình vào một phiên giao tiếp giữa người hoặc hệ thống (Thường là trình duyệt web và máy chủ web).

Một kịch bản MITM có ba đối tượng tham gia: Nạn nhân, đối tượng mà nạn nhân đang cố gắng kết nối, và kẻ tấn công ở giữa, kẻ tấn công đã chặn kết nối của nạn nhân và nạn nhân không nhận thức được kẻ này, đây là sự điều kiện tiên quyết cho kịch bản đánh cắp này.

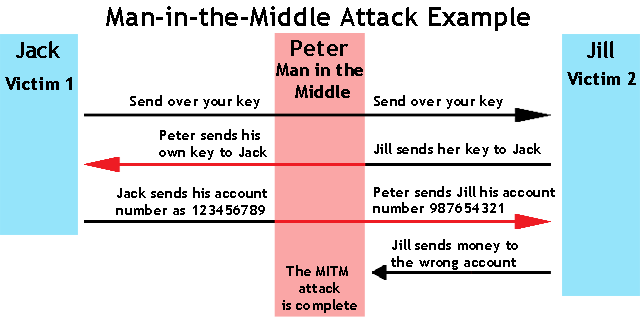
Chi tiết hơn, kẻ tấn công sẽ mạo danh cả hai bên và có được quyền truy cập vào thông tin mà hai bên đang cố gắng gửi cho nhau. Kẻ tấn công có thể chặn, gửi và nhận dữ liệu dành cho cả hai bên, mà không có bên nào biết cho đến khi quá muộn.

Ngoài các website, các cuộc tấn công này có thể chuyển mục tiêu đến liên lạc qua email, DNS lookups và mạng WiFi công cộng. Các đối tượng tiêu biểu của MITM bao gồm: Các doanh nghiệp thương mại điện tử và người dùng các ứng dụng tài chính.

Những kẻ tấn công MITM cũng sẽ sử dụng phần mềm độc hại với hy vọng tạo ra các cỗ máy zombie hoặc xây dựng mạng lưới rộng lớn. MITM có thể được sử dụng như một cách để thực hiện advanced persistent threat (APT).

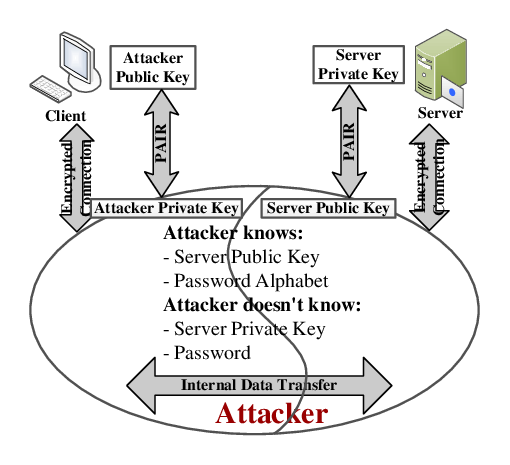
Các tổ chức/người dùng không biết dữ liệu của họ đã bị giả mạo cho đến khi quá muộn. Do đó, nếu MITM thành công, có thể gây ra những thiệt hại nặng nề.

**Ví dụ**



Kẻ tấn công đang mạo danh cả hai bên của cuộc trò chuyện để có quyền truy cập vào tài khoản. Điều này tương ứng với một cuộc trò chuyện giữa khách hàng và máy chủ hay các cuộc trò chuyện giữa người với người. Kẻ tấn công chặn một public key và với key này có thể giả mạo thông tin đăng nhập của một trong hai bên để lừa người dùng ở hai bên rằng họ đang nói chuyện với nhau một cách an toàn.

## 2. How does a man-in-the-middle attack work?



MITM có hai dạng, một dạng liên quan đến sự gần gũi về mặt vật lý và một dạng khác liên quan đến phần mềm độc hại.

Kẻ tấn công thường thực hiện MITM theo hai giai đoạn: interception and decryption.

MITM thành công không dừng lại ở việc ngăn chặn. Dữ liệu được mã hóa của nạn nhân sẽ bị giải mã, kẻ tấn công có thể dựa vào dữ liệu đó để hành động.

Các cuộc tấn công MITM có thể được thực hiện theo nhiều cách khác nhau nhằm khai thác thông tin liên lạc giữa các bên. Cho dù bằng phương tiện thụ động hay chủ động, một cuộc tấn công MITM đều hoạt động theo hình thức: Chặn kết nối giữa các nạn nhân và cố gắng che giấu hành vi của mình.

## 3. Types of Man-in-the-Middle attacks

Kẻ tấn có thể sử dụng các cuộc tấn công MITM để giành quyền kiểm soát các thiết bị theo nhiều cách khác nhau.

**(1) IP spoofing** - Giả mạo IP

Mỗi thiết bị có khả năng kết nối với internet đều có internet protocolt address (IP), tương tự như địa chỉ cho nhà bạn. Với IP spoofing, kẻ tấn công có thể thay thế bạn hoặc đối tượng tương tác với bạn và lừa bạn rằng bạn đang liên hệ trực tiếp với bên kia, kẻ tấn công có thể truy cập vào thông tin mà bạn đang trao đổi.

**(2) DNS spoofing** - Giả mạo DNS

Domain Name Server (DNS) spoofing là một kỹ thuật buộc người dùng vào một website giả chứ không phải trang mà người dùng dự định truy cập. Nếu bạn là nạn nhân của DNS spoofing, bạn sẽ nghĩ rằng bạn đang truy cập một website đáng tin khi bạn thực sự tương tác với một kẻ lừa đảo. Mục tiêu của thủ phạm là tăng lượng truy cập website giả mạo hoặc đánh cắp thông tin đăng nhập của người dùng.

Kẻ tấn công giả mạo DNS bằng cách thay đổi địa chỉ của website trong máy chủ DNS. Nạn nhân vô tình truy cập website giả mạo và kẻ tấn công sẽ cố gắng đánh cắp thông tin của họ.

**(3) HTTPS spoofing** - Giả mạo HTTPS

Khi truy cập website, HTTPS trong URL, chứ không phải là HTTP là dấu hiệu cho thấy website này an toàn. Kẻ tấn công có thể đánh lừa trình duyệt của bạn rằng đang truy cập một website đáng tin cậy bằng cách chuyển hướng trình duyệt của bạn đến một website không an toàn sau khi truy cập, kẻ tấn công có thể theo dõi các tương tác của bạn với website đó và có thể đánh cắp thông tin cá nhân bạn đang chia sẻ.

**(4) SSL hijacking** - Đánh cắp SSL

Khi thiết bị của bạn kết nối với máy chủ không bảo mật (HTTP) máy chủ thường có thể tự động chuyển hướng bạn đến phiên bản bảo mật (HTTPS). Kết nối đến một máy chủ an toàn có nghĩa là các giao thức bảo mật tiêu chuẩn được đặt ra, bảo vệ dữ liệu bạn chia sẻ với máy chủ đó. Secure Sockets Layer (SSL), một giao thức thiết lập các liên kết được mã hóa giữa trình duyệt và máy chủ web.

Tấn công SSL, kẻ tấn công sử dụng một máy tính và máy chủ bảo mật khác và chặn tất cả thông tin truyền qua giữa máy chủ và máy tính của người dùng.

**(5) Email hijacking** - Đánh cắp email

Một cuộc tấn công trung gian phổ biến khác là Email hijacking.

Giả sử bạn đã nhận được một email có vẻ là từ ngân hàng của bạn, yêu cầu bạn đăng nhập vào tài khoản để xác nhận thông tin liên hệ. Bạn nhấp vào một liên kết trong email và được đưa đến trang đăng nhập và thực hiện nhiệm vụ được yêu cầu.

Trong kịch bản này, MITM đã gửi cho bạn email, làm cho nó có vẻ hợp pháp. Nhưng khi bạn làm điều đó, bạn không đăng nhập vào tài khoản ngân hàng của mình, bạn đang bàn giao thông tin đăng nhập cho kẻ tấn công.

Kẻ tấn công nhắm vào email khách hàng của các ngân hàng và các tổ chức tài chính khác. Khi họ có quyền truy cập, họ có thể giám sát các giao dịch giữa tổ chức và khách hàng của mình. Những kẻ tấn công sau đó có thể giả mạo địa chỉ email của ngân hàng và gửi email có chứa một vài hướng dẫn cho khách hàng. Điều này khiến cho khách hàng làm theo hướng dẫn của kẻ tấn công chứ không phải ngân hàng. Kết quả tồi tệ là khách hàng đặt tiền vào tay kẻ tấn công.

Email sẽ có vẻ hợp pháp và vô hại đối với người nhận làm cho cuộc tấn công này rất hiệu quả và tàn phá về tài chính.

**(6) WiFi eavesdropping** - Nghe lén Wi-Fi

WiFi eavesdropping - một cách thụ động để triển khai các cuộc tấn công MITM. MITM thường xuyên xảy ra trên các mạng WiFi.

Với MITM truyền thống, kẻ tấn công cần có quyền truy cập vào bộ định tuyến WiFi (Có thể do không được bảo mật hoặc bảo mật kém). Các loại kết nối này thường là các kết nối công cộng (Các điểm truy cập Wi-Fi miễn phí), hoặc cũng có thể là WiFi cá nhân nếu người dùng không bảo vệ tốt cho chúng.

Tội phạm mạng có thể thiết lập kết nối WiFi với các tên nghe có vẻ rất hợp pháp. Khi người dùng kết nối với WiFi của kẻ tấn công, họ có thể theo dõi hoạt động trực tuyến của người dùng và có thể chặn thông tin đăng nhập, thông tin thẻ thanh toán...

Khi kẻ tấn công tìm thấy bộ định tuyến dễ bị tấn công, chúng có thể triển khai các công cụ để chặn và đọc dữ liệu truyền của nạn nhân. Kẻ tấn công sau đó cũng có thể chèn các công cụ của chúng vào giữa máy tính của nạn nhân và các website mà nạn nhân truy cập để ghi lại thông tin đăng nhập, thông tin ngân hàng và thông tin cá nhân khác.

**(7) Stealing browser cookies** - Ăn cắp cookie trình duyệt

Để hiểu Stealing browser cookies, bạn cần biết: Cookie trình duyệt là một phần thông tin nhỏ mà một website lưu trữ trên máy tính của bạn.

Một tội phạm mạng có thể chiếm quyền điều khiển các cookie trình duyệt. Vì cookie lưu trữ thông tin từ phiên duyệt web của bạn, kẻ tấn công có thể truy cập vào mật khẩu, địa chỉ và thông tin nhạy cảm khác của bạn.

## 4. What are ways to protect against a man-in-the-middle attack?

**Các tương tác dễ bị tấn công MITM:**

* Trang web tài chính - giữa đăng nhập và xác thực
* Các kết nối công cộng hoặc bảo mật kém
* Các website yêu cầu đăng nhập

Rất cần thiết khi thực hiện các bước để giúp bảo vệ thiết bị, dữ liệu và kết nối của bạn.

Vì có khá nhiều cách để thực hiện MITM, không có giải pháp tất cả trong một cho các cuộc tấn công này. Một trong những cách cơ bản nhất, hãy chắc chắn rằng của các website bạn truy cập sử dụng giao thức HTTPS. Các website hiện nay hầu hết đều triển khai HTTP Strict Transport Security (HSTS) - chỉ tương tác thông qua HTTPS

Hãy cảnh giác với các email lừa đảo từ những kẻ tấn công yêu cầu bạn cập nhật mật khẩu hoặc bất kỳ thông tin đăng nhập nào khác. Thay vì nhấp vào liên kết được cung cấp trong email, hãy nhập thủ công địa chỉ website vào trình duyệt của bạn.

Hạn chế kết nối trực tiếp với bộ định tuyến WiFi công cộng. Virtual Private Network (VNP) mã hóa kết nối internet của bạn trên các điểm truy cập công cộng để bảo vệ dữ liệu riêng tư bạn gửi và nhận trong khi sử dụng WiFi công cộng, như mật khẩu hoặc thông tin thẻ tín dụng.

Vì MITM chủ yếu sử dụng phần mềm độc hại để thực thi, bạn nên thực thi một giải pháp bảo mật internet toàn diện trên máy tính của bạn.

Hãy tăng tính bảo mật cho mạng WiFi tại nhà của bạn bằng cách thay đổi tên người dùng và mật khẩu mặc định trên bộ định tuyến và tất cả các thiết bị được kết nối thành mật khẩu mạnh và duy nhất.

Điều thiết yếu là bạn phải ý thức rằng MITM có thể làm tổn hại không nhẹ đến thông tin cá nhân của bạn, để luôn thực thi các biện pháp bảo mật thích hợp với các thiết bị của bạn.

Authentication certificates cũng có thể được sử dụng để bảo vệ chống lại MITM. Một tổ chức có thể thực hiện xác thực rồi cấp chứng chỉ cho tất cả các thiết bị của họ, để chỉ những người dùng có chứng chỉ, cấu hình thích hợp mới có thể truy cập hệ thống của họ.

Để ngăn chặn việc đánh cắp email, có thể sử dụng Secure/Multipurpose Internet Mail Extensions (S/MIME). Giao thức này mã hóa email và cho phép đăng ký email với Digital Certificate duy nhất, cho người nhận biết rằng tin nhắn đã nhận là hợp pháp.

Người dùng có thể tự bảo vệ mình khỏi MITM bằng cách tránh gửi bất kỳ thông tin cá nhân nào qua mạng WiFi công cộng trừ khi chúng được bảo vệ bởi VPN.

***Tham khảo***

[What is a man-in-the-middle attack?](https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html)

[MAN IN THE MIDDLE (MITM) ATTACK](https://www.veracode.com/security/man-middle-attack)

[What is a Man-in-the-Middle Attack?](https://www.forcepoint.com/cyber-edu/man-in-the-middle-attack)

[What is a Man-In-The-Middle Attack?](https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/)

### Tấn công man-in-the-middle

Rate this post

**Là một trong nhiều** [**kỹ thuật**](http://esc.vn) **tấn công mạng, cho phép** [**hacker**](http://esc.vn/tan-cong-man-middle/) **can thiệp vào kết nối Internet của người dùng và thu thập mọi thông tin truyền trên hệ thống mạng đó**

Tấm hình trên có quen với bạn không? Không có gì lạ. Hàng triệu người dùng khắp thế giới kết nối vào mạng Wi-Fi công cộng bằng thiết bị di động của mình khi đi đây đó, và hầu như ai cũng cố gắng giữ kết nối càng lâu càng tốt. Vấn đề ở đây là không phải mạng không dây nào cũng đàng hoàng. Hình ảnh bên trên là một mạng Wi-Fi giả của hệ thống Wi-Fi của một khách sạn, nhưng chúng ta không thể phân biệt được nếu chỉ nhìn vào màn hình.

Kiểu tấn công này trong giới chuyên môn gọi là man-in-the-middle (người đứng giữa), là một trong nhiều kỹ thuật tấn công mạng, cho phép kẻ nào đó can thiệp vào kết nối Internet của người khác và thu thập mọi thông tin truyền trên hệ thống mạng đó. Loại tấn công này đã xuất hiện nhiều năm nay, gây hại với người dùng PC. Nhưng hiện nay, điện thoại di động đang được sử dụng nhiều nên đã trở thành đích ngắm mới.

Một chuyên gia của công ty bảo mật Lookout đã trình diễn những cánh tấn công thông dụng sử dụng kỹ thuật này.

**Diễn ra thế nào?**

Bởi vì người dùng thường làm rất nhiều việc thông qua thiết bị di động, sử dụng Wi-Fi công cộng, nên dữ liệu truyền ra vào thiết bị trở thành rủi ro lớn cho nhiều doanh nghiệp.

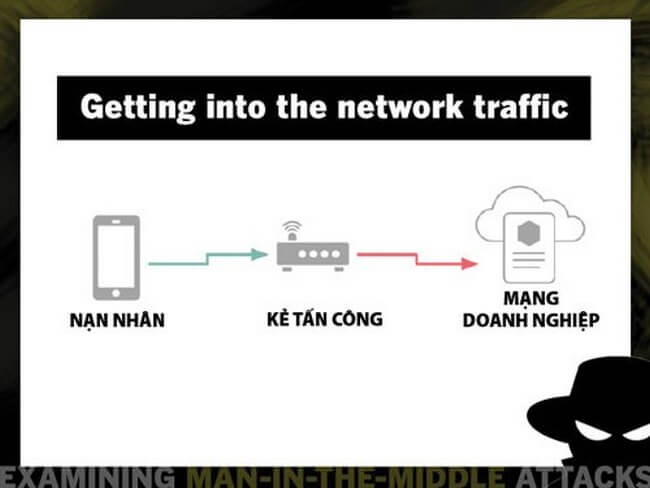
Thông thường, kết nối Internet thông qua các điểm truy cập (access point) hay proxy không an toàn không phải là hiểm hoạ lớn, bởi vì dữ liệu của doanh nghiệp thường được mã hoá. Tuy vậy, có những phương pháp tấn công cho phép kẻ xấu xem được cả dữ liệu mã hoá của doanh nghiệp, như tài khoản đăng nhập hay email nhạy cảm.

Có hai bước để thực hiện tấn công kiểu man-in-the-middle. Đầu tiên, kẻ tấn công phải xâm nhập được vào hệ thống mạng. Thứ hai, kẻ tấn công phải giải mã dữ liệu.

**Xâm nhập vào hệ thống mạng**

Có bốn cách phổ biến mà kẻ xấu thường dùng để xâm nhập mạng:

1. Giả một điểm truy cập Wi-Fi
2. Giả ARP
3. Chiếm proxy /SSL Bump
4. VPN giả

**Giả điểm truy cập Wi-Fi**

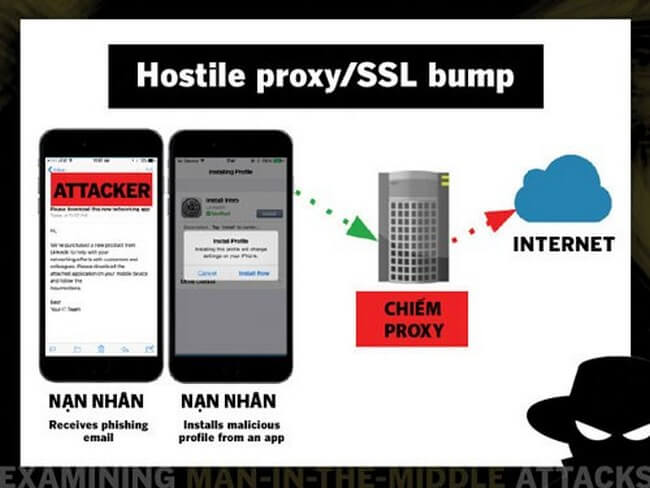
1. Kẻ tấn công thiết lập một access point giả
2. Giả một mạng mà người dùng sẽ tin tưởng là thật
3. Khi người dùng kết nối (hoặc có thể thiết bị tự động kết nối mà không cần người dùng can thiệp), kẻ tấn công đã vào được cùng một mạng với thiết bị của người dùng.

**Giả ARP**

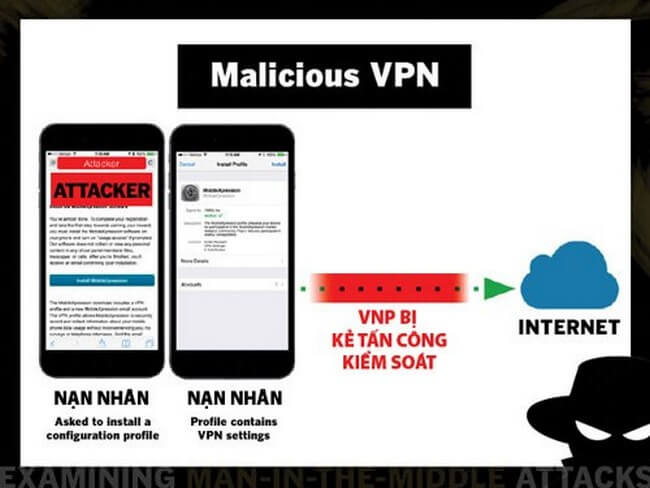
1. Kẻ tấn công thiết lập địa chỉ MAC của chính chúng như là một gateway hoặc thiết bị của nạn nhân.
2. Kẻ tấn công có thể can thiệp hoặc chỉnh sửa mọi luồng dữ liệu.

**Chiếm proxy/SSL Bump**

1. Kẻ tấn công lừa người dùng cài một ứng dụng độc hại hoặc một profile cấu hình nào đó, hoặc sử dụng một phương thức bảo mật khác.
2. Luồng dữ liệu trên thiết bị bị định hướng đến kiến trúc mạng dựng sẵn của kẻ tấn công.

**VPN giả**

1. Một người dùng bị lừa để tải về một ứng dụng hay một profile cấu hình để yêu cầu kích hoạt VPN.
2. Luồng dữ liệu trên thiết bị bị định hướng trỏ vào VPN của kẻ tấn công.

**Giải mã dữ liệu**

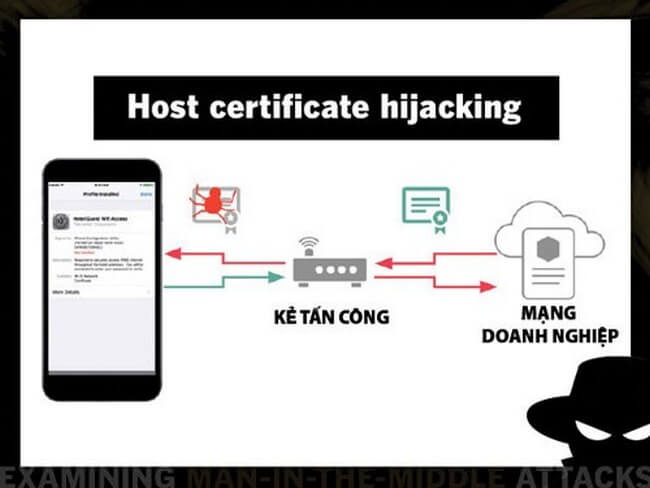
Có vài cách sau để giải mã dữ liệu trong khi dữ liệu đang di chuyển trên hệ thống mạng. Trong đó, ba cách sau là thường gặp nhất:

1. Tấn công chứng thực host
2. SSLStrip
3. Hạ cấp giao thức TLS

**Tấn công chứng thực host**

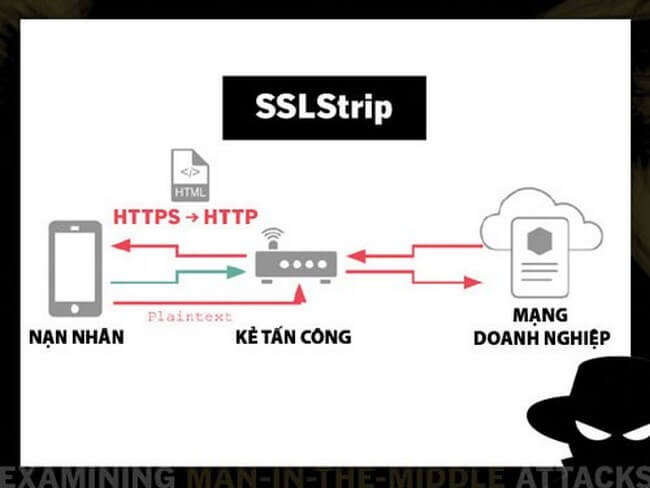
1. Kết nối thông qua man-in-the-middle
2. Kẻ tấn công thiết lập session SSL với host đã nhắm trước
3. Host hồi đáp với chứng thực SSL
4. Chứng thực giả tới người dùng cuối và người dùng chấp nhận

Nếu người dùng bị lừa cài đặt một chứng thực root thì thậm chí hệ thống vô hiệu hoá cảnh báo về chứng thực về sau.

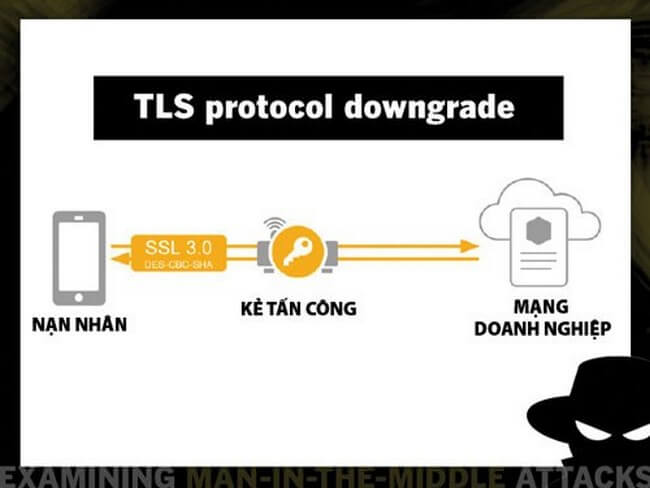
**SSLStrip**

Cách hoạt động:

1. Kết nối thông qua kẻ tấn công
2. Kẻ tấn công viết lại nội dung nhưng không gồm các link HTTPS
3. Thông tin vào ra, như tài khoản đăng nhập, sẽ hiển thị ở dạng văn bản thuần, không hề mã hoá

**Hạ cấp giao thức TLS**

Kẻ tấn công chiếm kết nối để hạ cấp giao thức. Những giao thức lỗi thời như TLS lại rất dễ giải mã nếu kẻ tấn công am tường công nghệ.

**An toàn là trên hết**

Khi kết nối đến Wi-Fi, bạn nên cẩn trọng nếu có bất kỳ dấu hiệu nào yêu cầu bạn thực hiện thêm vài điều để có thể kết nối được đến Internet.

Nhưng nếu mạng Wi-Fi yêu cầu bạn bổ sung thông tin nào khác, như là chứng thực hay phải tải một app nào đó về thì rõ ràng đó là dấu hiệu của kẻ xấu muốn lừa bạn.

Cũng có vài cách an toàn để bạn lướt web khi đi ra ngoài. Sử dụng mạng 3G, tuy có tốn kém nhưng lại an toàn hơn nhiều so với Wi-Fi. Nên nếu cần truy cập dịch vụ ngân hàng trực tuyến hay công việc quan trọng trên mạng, bạn nên chuyển sang dùng 3G. Hoặc bạn có thể bật VPN để mã hoá mọi dữ liệu vào/ra khi đến quán xá nào đó.

Cách tốt nhất là bạn không nên giao dịch điện tử qua Wi-Fi công cộng.

## ****Tổng quan về Tấn công mạng****

### ****Tấn công mạng là gì?****

Khái niệm **Tấn công mạng** (hoặc **tấn công không gian mạng**) trong tiếng Anh là Cyber attack (hoặc Cyberattack), được ghép bởi 2 từ: Cyber (thuộc không gian mạng internet) và attack (sự tấn công, phá hoại).

**Tấn công mạng** là tất cả các hình thức **xâm nhập trái phép** vào một hệ thống máy tính, website, cơ sở dữ liệu, hạ tầng mạng, thiết bị của một cá nhân hoặc tổ chức **thông qua mạng internet** với những mục đích bất hợp pháp.

Mục tiêu của một cuộc tấn công mạng rất đa dạng, có thể là **vi phạm dữ liệu** (đánh cắp, thay đổi, mã hóa, phá hủy), cũng có thể nhắm tới **sự toàn vẹn của hệ thống** (gây gián đoạn, cản trở dịch vụ), hoặc **lợi dụng tài nguyên** của nạn nhân (hiển thị quảng cáo, mã độc đào tiền ảo).

Tấn công mạng **khác với pentest** (kiểm thử xâm nhập). Mặc dù cả 2 đều chỉ việc xâm nhập vào một hệ thống, tuy nhiên tấn công mạng là xâm nhập trái phép gây hại cho nạn nhân, còn pentest là xâm nhập với mục đích tìm ra **điểm yếu bảo mật trong hệ thống** để khắc phục.

Khái niệm an ninh mạng Cybersecurity

### ****Đối tượng bị tấn công****

Có thể là cá nhân, doanh nghiệp, các tổ chức chính phủ hoặc phi chính phủ, cơ quan nhà nước, thậm chí đối tượng có thể là cả một quốc gia. Tuy nhiên, đối tượng phổ biến nhất của các cuộc tấn công mạng là các doanh nghiệp. Đơn giản vì mục tiêu chính của những kẻ tấn công là vì lợi nhuận.

### ****Mục đích tấn công mạng****

Bên cạnh những mục đích phổ biến như trục lợi phi pháp, tống tiền doanh nghiệp, hiện thị quảng cáo kiếm tiền, thì còn tồn tại một số mục đích khác phức tạp và nguy hiểm hơn: cạnh tranh không lành mạnh giữa các doanh nghiệp, tấn công an ninh hoặc kinh tế của một quốc gia, tấn công đánh sập một tổ chức tôn giáo, v.v.

Ngoài ra, một số hacker tấn công mạng chỉ để mua vui, thử sức, hoặc tò mò muốn khám phá các vấn đề về an ninh mạng.

### ****Hacker là ai?****

Ban đầu, những kẻ tấn công mạng được gọi là Cyber-crime (tội phạm mạng), tuy nhiên công chúng thường biết đến họ dưới cái tên **“hacker”** (kẻ xâm nhập), ở Việt Nam gọi là **tin tặc**. Các hacker đều là những người có kiến thức cực kỳ chuyên sâu về an ninh mạng, khoa học máy tính, khoa học mật mã, cơ sở dữ liệu,…Thậm chí, kiến thức của hacker còn được đánh giá là sâu và rộng hơn các kỹ sư CNTT thông thường.

### ****Tấn công trung gian (Man-in-the-middle attack)****

Tấn công trung gian (MitM), hay **tấn công nghe lén**, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Khi đã chen vào giữa thành công, chúng có thể đánh cắp dữ liệu của giao dịch đó.

Loại hình này xảy ra khi:

* Nạn nhân truy cập vào một mạng Wifi công cộng không an toàn, kẻ tấn công có thể “chen vào giữa” thiết bị của nạn nhân và mạng Wifi đó. Vô tình, những thông tin nạn nhân gửi đi sẽ rơi vào tay kẻ tấn công.
* Khi phần mềm độc hại được cài đặt thành công vào thiết bị, một kẻ tấn công có thể dễ dàng xem và điều chỉnh dữ liệu của nạn nhân.

## ****Giải pháp chống tấn công mạng****

### ****Đối với cá nhân****

* Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,… Chi tiết tại: [3 kiểu Tấn công Password cơ bản & cách phòng chống](https://cystack.net/vi/resource/3-hinh-thuc-tan-cong-password-co-ban/)
* Hạn chế truy cập vào các điểm wifi công cộng
* Không sử dụng phần mềm bẻ khóa (crack)
* Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
* Cẩn trọng khi duyệt email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
* Tuyệt đối không tải các file hoặc nhấp vào đường link không rõ nguồn gốc.
* Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
* Sử dụng một phần mềm diệt Virus uy tín.

### ****Đối với tổ chức, doanh nghiệp****

* [Xây dựng một chính sách bảo mật](https://cystack.net/vi/resource/xay-dung-chinh-sach-bao-mat-cho-doanh-nghiep/) với các điều khoản rõ ràng, minh bạch
* Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
* Tuyệt đối không sử dụng các phần mềm crack
* Luôn cập nhật phần mềm, firmware lên phiên bản mới nhất.
* Sử dụng các dịch vụ đám mây uy tín cho mục đích lưu trữ.
* Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: [bảo mật website,](https://cystack.net/vi/resource/bao-mat-website/) bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (CRM), [bảo mật IoT](https://cystack.net/vi/resource/bao-mat-thiet-bi-iot/), bảo mật hệ thống CNTT – vận hành…
* Tổ chức các buổi đào tạo, [training kiến thức sử dụng internet an toàn cho nhân viên](https://cystack.net/vi/resource/lam-sao-de-nang-cao-y-thuc-bao-mat-cua-nhan-vien/).

# Tìm hiểu về tấn công Man in the middle

[07/05/2018](https://ssl.vn/tim-hieu-ve-tan-cong-man-in-the-middle.html) [Hoàng Tùng](https://ssl.vn/author/tunghv)

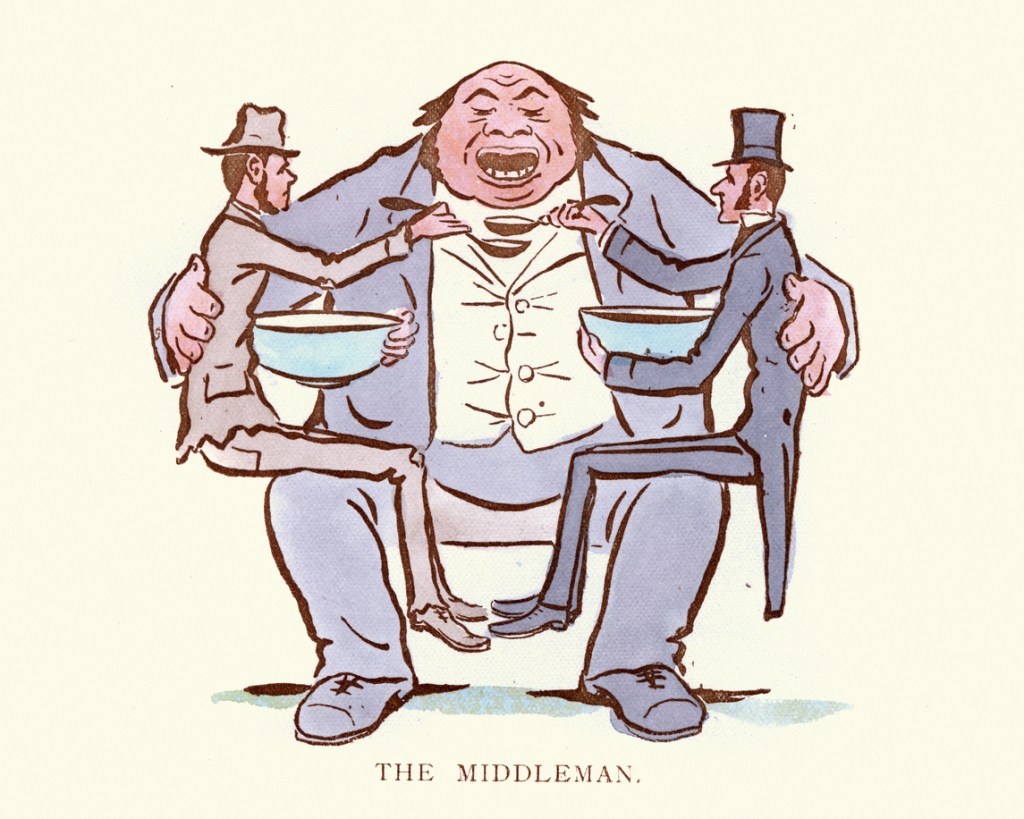


Bạn có thể đã nghe thuật ngữ ‘Man-in-the-middle (MiTM) Attack’ ? Có thể bạn đã mường tượng được phần nào về cách thức tấn công của nó. Nhưng bạn vẫn đang băn khoăn ‘Chính xác thì cuộc Man-in-the-middle là gì?’ Đúng? Hãy để chúng tôi giải thích cho bạn. Như đúng cái tên của nó, loại tấn công xảy ra khi có một thiết bị nằm ở giữa hai hệ thống giao tiếp và cố gắng để ngăn chặn việc chuyển giao thông tin liên tục. Nói một cách đơn giản, một cuộc tấn công MiTM là một phiên bản hiện đại của bugging.

Đầu tiên nhìn xung quanh bạn, nhìn vào chiếc smartphone của bạn, nhìn vào các ứng dụng trong đó, nhìn vào PC của bạn, nhìn vào những thiết bị thông minh kết nối với nhau, nhìn vào trang web bạn đang xem. Những thứ này có gì chung? Điều gì đang thúc đẩy tất cả những điều này phát triển? Câu trả lời sẽ là dữ liệu / thông tin. Cho dù đó là từ một máy tính khác, một máy chủ khác, một quốc gia khác – dữ liệu không biết giới hạn.

Thật không may, tất cả các chuyến đi này mang đến những câu hỏi không thể tránh khỏi về an ninh và riêng tư. Khi dữ liệu rời đi từ điểm cuối này đến điểm kết thúc khác, khoảng thời gian truyền dẫn là nơi kiểm soát nó bị mất phần nào. Khi kẻ tấn công tự đặt mình vào giữa điểm kết thúc và chặn và / hoặc tampers với dữ liệu này trong quá cảnh, nó được gọi là tấn công man-in-the-middle (MiTM). Theo thuật ngữ của công an thì nó tương tự nghe lén vậy.

Đúng vậy, khi bạn cố gắng nghe lỏm được cuộc trò chuyện giữa hai người mà họ không biết, nó giống như một cuộc tấn công **Man in the middle**.

Bạn đã thấy người đàn ông này? Không. Có lẽ là không.

Trong khi truyền dữ liệu đang diễn ra giữa một thiết bị (PC / Điện thoại) và máy chủ web, kẻ tấn công sử dụng các kỹ năng và công cụ của anh ta để đặt một thiết bị vào giữa hai điểm cuối và chặn dữ liệu. Trong khi hai bên tin rằng họ đang nói chuyện với nhau, nhưng thật sự họ đang liên lạc (và thông qua) thủ phạm.

Các cuộc tấn công này không chỉ diễn ra trong quá trình truyền thông giữa các thiết bị, mà còn có thể xảy ra ở bất cứ nơi nào hai hệ thống đang trao đổi dữ liệu.

## Man in the middle hoạt động như thế nào?

Khi nói đến các cuộc tấn công MiTM, không chỉ có một phương pháp duy nhất có thể gây ra thiệt hại – có bốn! Đó là Sniffing, Packet Injection, Session Hijacking và SSL Stripping. Hãy cùng tìm hiểu qua về các phương pháp này

* **Sniffing:** Sniffing hoặc Packet Sniffing là một kỹ thuật được sử dụng để nắm bắt các gói dữ liệu chảy vào và ra khỏi một hệ thống / mạng. Packet Sniffing trong mạng tương đương với việc nghe trộm trong điện thoại. Hãy nhớ rằng Sniffing là hợp pháp nếu được sử dụng đúng cách và nhiều doanh nghiệp làm điều đó vì mục đích bảo mật.
* **Packet Injection:** Trong kỹ thuật này, kẻ tấn công đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp / phần mềm độc hại vì chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.
* **Gỡ rối phiên:** Bạn đã từng gặp lỗi “Phiên hoạt động đã hết hạn” chưa? Nếu bạn đã từng thực hiện thanh toán trực tuyến hoặc điền vào biểu mẫu, bạn sẽ biết thuật ngữ này. Thời gian giữa khi bạn đăng nhập vào tài khoản ngân hàng của bạn và đăng xuất khỏi tài khoản đó được gọi là một phiên. Các phiên này thường là mục tiêu của tin tặc vì chúng có khả năng chứa thông tin kín đáo. Trong hầu hết các trường hợp, một hacker thiết lập sự hiện diện của anh ta / cô ta trong phiên, và cuối cùng nắm quyền kiểm soát nó. Các cuộc tấn công này có thể được thực thi theo nhiều cách khác nhau.
* **Loại bỏ SSL:** SSL Stripping hoặc SSL Downgrade attack là một loài hiếm khi nói đến các cuộc tấn công MiTM, nhưng cũng là một trong những nguy hiểm nhất. Như chúng ta đều biết, chứng chỉ [SSL / TLS](https://ssl.vn/tim-hieu-ve-su-khac-nhau-giua-tls-va-ssl.html) giữ liên lạc của chúng tôi an toàn trực tuyến thông qua mã hóa. Trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL / TLS và giao thức được chuyển từ HTTPS an toàn sang HTTP không an toàn.

## Làm thế nào để ngăn chặn các cuộc tấn công man-in-the-middle?

Hãy nhớ rằng những cuộc tấn công này không dễ dàng như việc tắt tai nghe của bạn, chúng có tính chất rất phức tạp. Bạn cần phải có một số kỹ năng về kĩ thuật và phải được hỗ trợ bởi các công cụ phù hợp.

Dưới đây là các thực tiễn được đề xuất của chúng tôi để bảo vệ chống lại các cuộc tấn công giữa người:

* Đảm bảo rằng các trang web bạn truy cập đã được cài [SSL](https://ssl.vn/tag/ssl)
* Trước khi nhấp vào email, hãy kiểm tra người gửi email
* Nếu bạn là quản trị viên trang web, bạn nên triển khai [HSTS](https://ssl.vn/tag/giao-thuc-hsts)
* KHÔNG mua hàng hoặc gửi dữ liệu nhạy cảm trên mạng Wi-Fi công cộng.
* Đảm bảo trang web của bạn không có bất kỳ nội dung hỗn hợp nào
* Nếu trang web của bạn đang sử dụng SSL, hãy đảm bảo bạn đã tắt giao thức SSL / TLS không an toàn. Bạn chỉ nên bật TLS 1.1 và TLS 1.2
* Không nhấp vào liên kết hoặc email độc hại
* Không tải xuống nội dung vi phạm bản quyền
* Bảo mật mạng gia đình / công việc của bạn
* Có các công cụ bảo mật thích hợp được cài đặt trên hệ thống của bạn