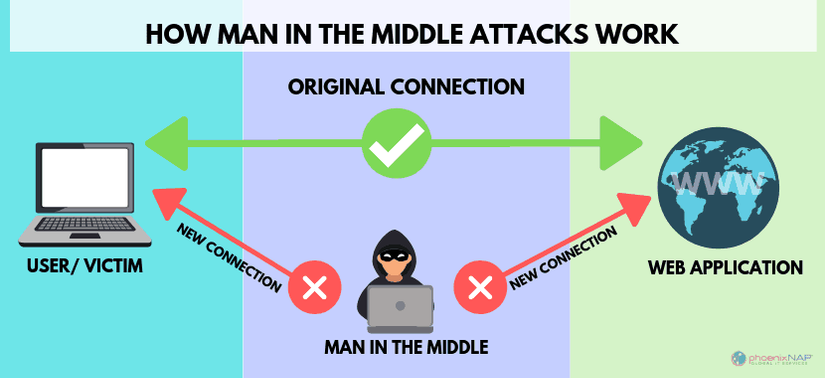
**Man-in-the-Middle Attack (MITM)**

[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.

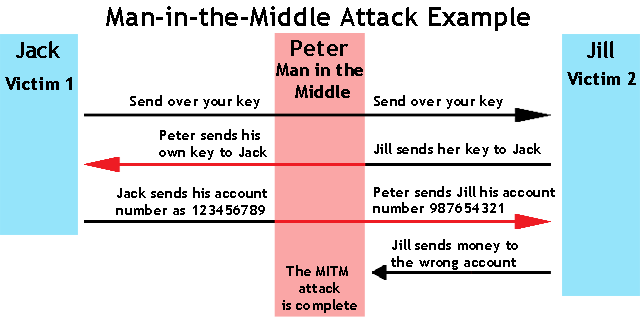
Chi tiết hơn, kẻ tấn công sẽ mạo danh cả hai bên và có được quyền truy cập vào thông tin mà hai bên đang cố gắng gửi cho nhau. Kẻ tấn công có thể chặn, gửi và nhận dữ liệu dành cho cả hai bên, mà không có bên nào biết cho đến khi quá muộn.

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).

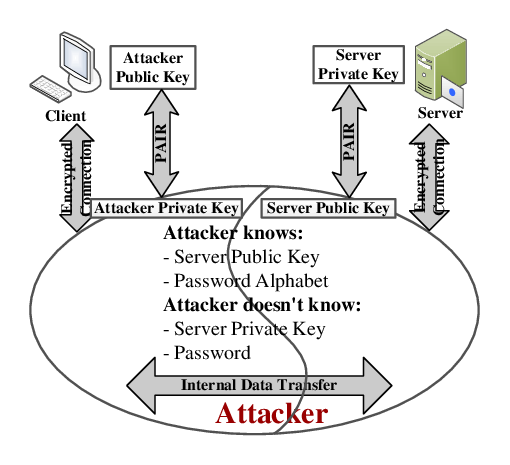
Các tổ chức/người dùng không biết dữ liệu của họ đã bị giả mạo cho đến khi quá muộn. Do đó, nếu MITM thành công, có thể gây ra những thiệt hại nặng nề.

**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.