



Bảo mật trong Công Nghệ Thông tin

Nhóm biên soạn:

1. Lê Ngọc Thành
2. Phạm Trọng Nghĩa
3. Tạ Việt Phương
4. Trương Tấn Khoa

Năm 2022



1 Các Mối Đe Dọa Bảo Mật



Nội dung



Nguyên tắc CIA



Các thuật ngữ liên quan đến an ninh máy tính



Phần mềm độc hại



Tấn công bảo mật

Nguyên tắc CIA

- Nguyên tắc CIA là **bộ nguyên tắc hướng dẫn** thiết kế các chính sách bảo mật thông tin.
- Bộ nguyên tắc CIA gồm:
 - **Tính bảo mật** (**C**onfidentiality)
 - **Tính toàn vẹn** (**I**ntegrity)
 - **Tính sẵn sàng** (**A**vailability)



Tính bảo mật

Bảo mật (confidentiality) nghĩa là giữ mọi thứ được giấu kín.

- Bảo vệ bằng mật khẩu
- Giới hạn quyền truy cập



Tính toàn vẹn

Toàn vẹn (integrity) nghĩa là giữ cho dữ liệu chính xác và không bị can thiệp.



Tính sẵn sàng

Sẵn sàng (availability) nghĩa là **thông tin** có thể dễ dàng truy cập được đối với những người cần nó.



Nội dung



Nguyên tắc CIA



Các thuật ngữ liên quan đến an ninh máy tính



Phần mềm độc hại



Tấn công bảo mật

Rủi ro bảo mật

Rủi ro bảo mật (security risk) là khả năng bị tổn thất trong trường hợp hệ thống bị tấn công.



Lỗ hổng bảo mật

Lỗ hổng (vulnerability) là kẽ hở mà kẻ tấn công lợi dụng để xâm nhập hệ thống.

- Lỗ hổng Zero-day là lỗ hổng mà nhà phát triển không biết nhưng kẻ tấn công lại phát hiện ra.



Khai thác lỗ hổng

Khai thác lỗ hổng (vulnerability exploit) là tận dụng lỗ hổng bằng cách viết mã khai thác nhằm truy cập hoặc gây ra thiệt hại cho hệ thống.



Các mối đe dọa

Mối đe dọa (threat) là những mối nguy hiểm tiềm tàng có thể xảy ra.



Hacker

- Hacker là người cố gắng đột nhập hoặc khai thác hệ thống.
- Có 2 loại hacker phổ biến:
 - Hacker mũ đen: những nhân vật cố gắng xâm nhập vào hệ thống để làm điều gì đó gây hại.
 - Hacker mũ trắng: những người cố gắng tìm ra điểm yếu trong hệ thống và cảnh báo cho chủ sở hữu để kịp thời khắc phục.



Tấn công

Tấn công (attack) là nỗ lực nhằm gây hại cho hệ thống.



Nội dung



Nguyên tắc CIA



Các thuật ngữ liên quan đến an ninh máy tính



Phần mềm độc hại



Tấn công bảo mật

Phần mềm độc hại

Phần mềm độc hại (malware) là loại phần mềm nhằm **đánh cắp thông tin nhạy cảm, xóa, hoặc sửa đổi các tập tin**.



Virus

Virus là loại phần mềm có khả năng gắn vào mã thực thi của một chương trình, tự sao chép chính chúng và thực hiện các công việc gây nguy hại.



Sâu máy tính

Sâu máy tính (worm) là loại phần mềm có thể sống độc lập và lây lan qua các kênh như mạng máy tính.

- Một số sâu máy tính nổi tiếng như ILOVEYOU (Love Bug), Mydoom, Morris, v.v...



Phần mềm quảng cáo

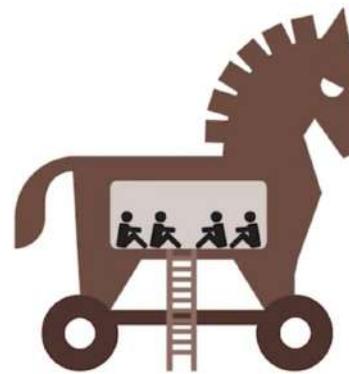
Phần mềm quảng cáo (adware) là loại phần mềm **hiển thị quảng cáo** và thu thập dữ liệu.



adware

Trojan

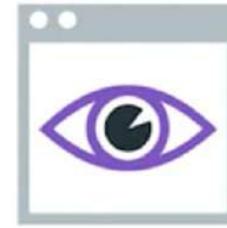
Trojan là loại phần mềm độc hại nhưng tự ngụy trang thành một dạng phần mềm vô hại khác.



Phần mềm gián điệp

Phần mềm gián điệp (spyware) là loại phần mềm **theo dõi người dùng** như màn hình, phím bấm, webcam, v.v...

- Keylogger là loại phần mềm gián điệp **ghi lại mọi thao tác gõ phím.**

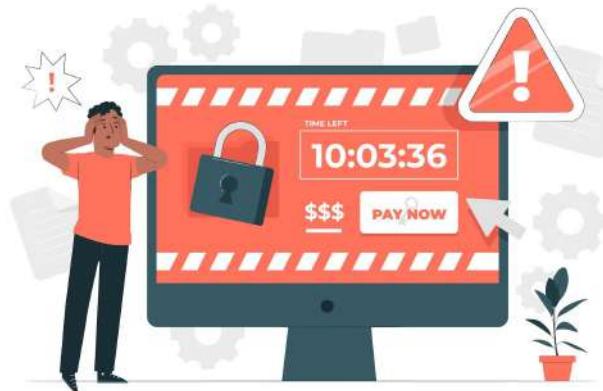


spyware

Ransomware

Ransomware là một kiểu phần mềm tấn công **bắt giữ dữ liệu làm con tin**.

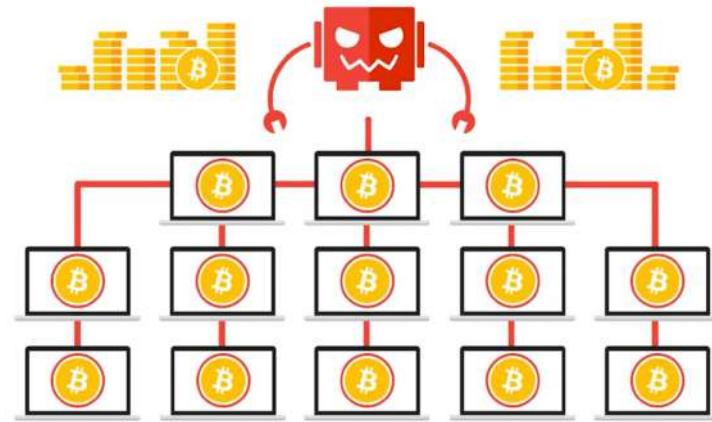
- Một số ransomware nổi tiếng như CryptoLocker, WannaCry, DarkSide, v.v...



Botnet

Botnet là một mạng lưới các máy kết nối Internet bị kẻ tấn công sử dụng thực hiện một số chức năng phân tán.

- Ví dụ: lợi dụng để đào Bitcoin (một loại tiền số)



Cửa hậu

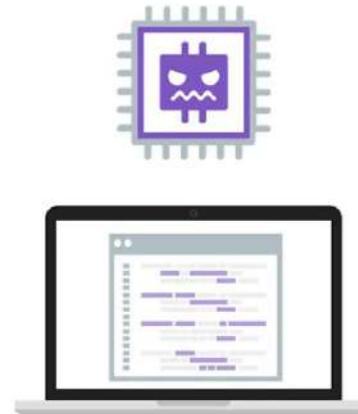
Cửa hậu (backdoor) là một lối xâm nhập bí mật vào hệ thống của những kẻ tấn công.



Rootkit

Rootkit là loại phần mềm **có quyền sửa đổi ở cấp quản lý** đối với hệ điều hành.

- Khi được sử dụng bởi kẻ tấn công thì nó sẽ **chạy nhiều tiến trình độc hại và ẩn chúng khỏi trình quản lý tác vụ**.



Bom logic

Bom logic (logic bomb) là một loại phần mềm sau một sự kiện hay thời gian nhất định, nó sẽ được kích hoạt và chạy các mã độc.



Nội dung



Nguyên tắc CIA



Các thuật ngữ liên quan đến an ninh máy tính



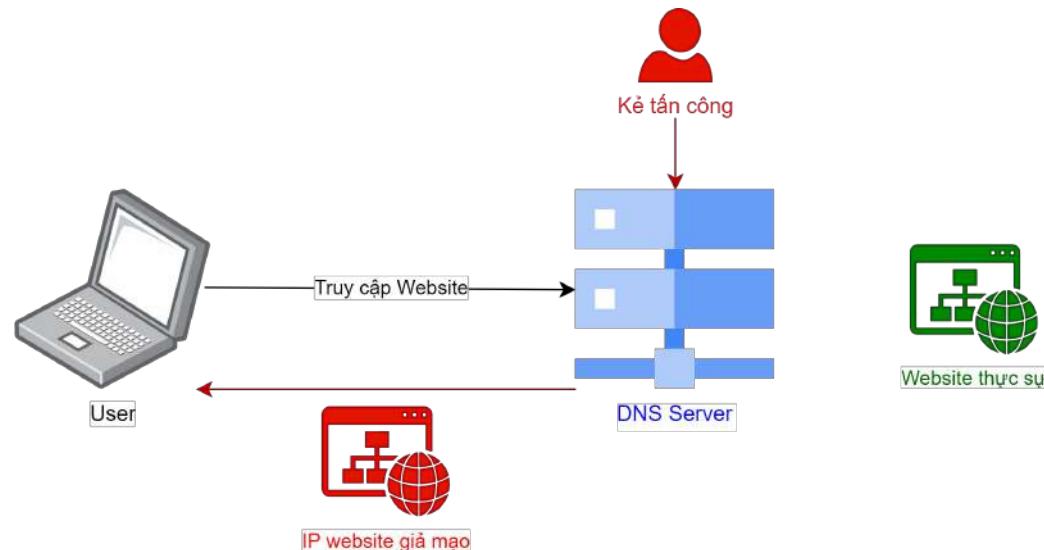
Phần mềm độc hại



Tấn công bảo mật

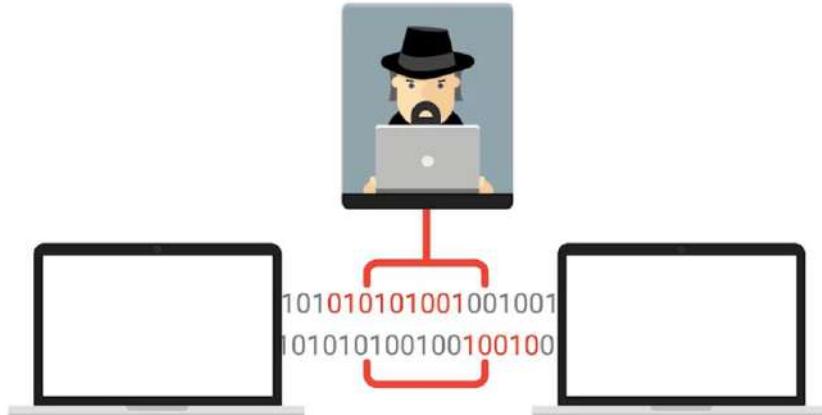
Tấn công giả mạo DNS

Tấn công giả mạo DNS (DNS spoofing, DNS cache poisoning attack) là tấn công lừa máy chủ DNS chấp nhận một bản ghi DNS giả mạo mà nó đã bị kiểm soát.



Tấn công xen giữa

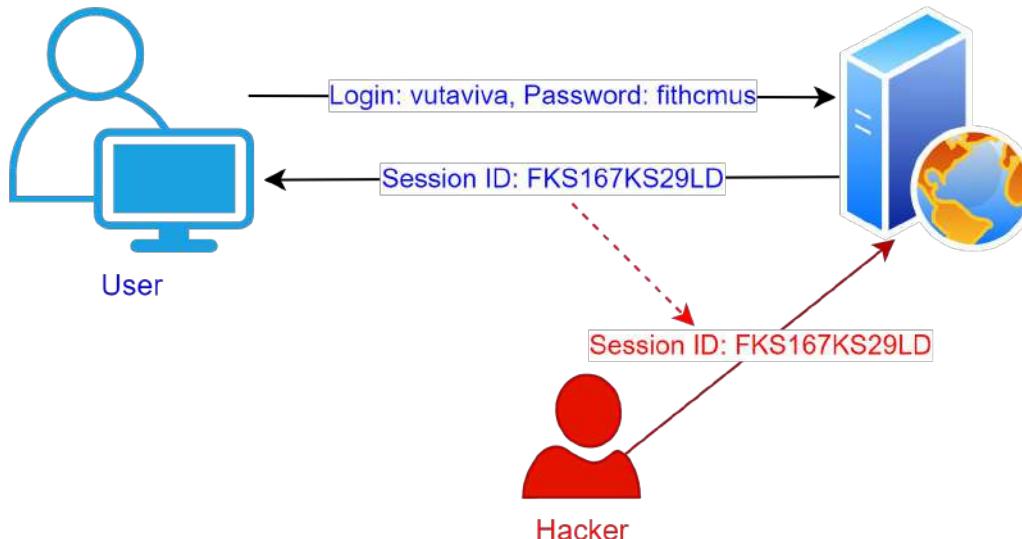
Tấn công xen giữa
(man-in-the-middle attack) là một cách thức mà kẻ tấn công **xen vào giữa giao tiếp của hai đối tượng** mà họ cứ nghĩ rằng đang giao tiếp trực tiếp với nhau.



Tấn công xen giữa

Tấn công xen giữa (man-in-the-middle attack) bao gồm một số dạng:

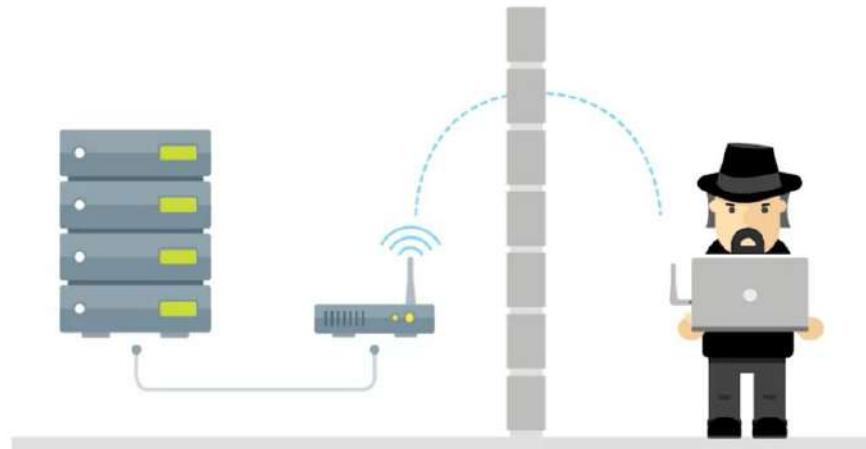
- Tấn công phiên (session hijacking, cookie hijacking): **đánh cắp mã phiên và mạo danh với mã phiên.**



Tấn công xen giữa

Tấn công xen giữa (man-in-the-middle attack) bao gồm một số dạng:

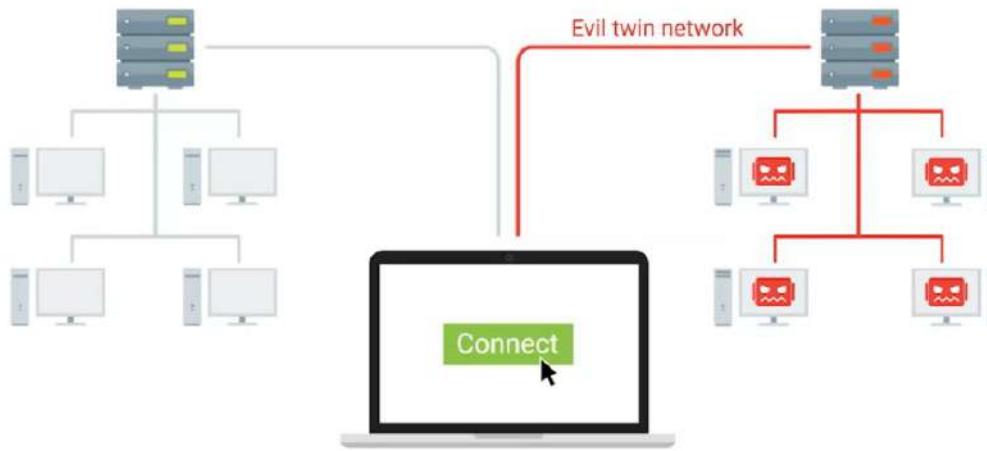
- **Tấn công AP giả mạo** (rogue AP): **tạo điểm truy cập** (access point) và kiểm soát giao tiếp của người dùng trong mạng này.



Tấn công xen giữa

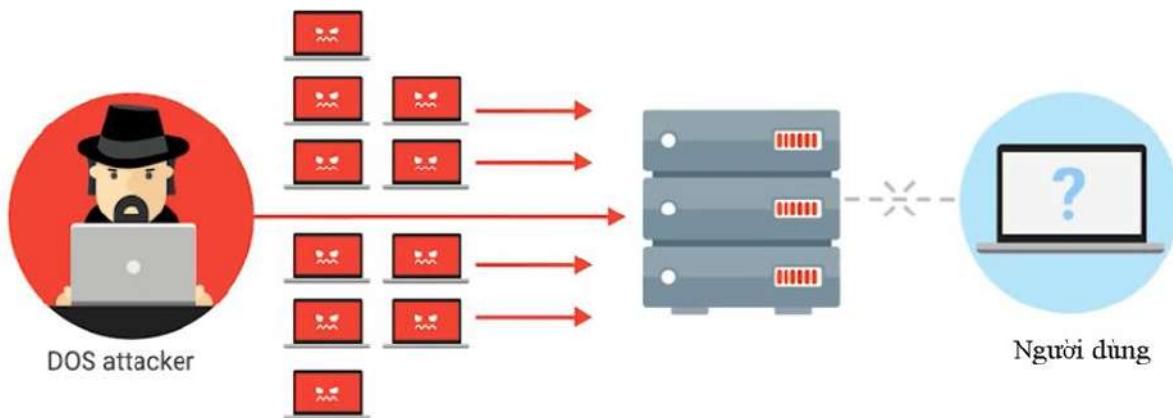
Tấn công xen giữa (man-in-the-middle attack) bao gồm một số dạng:

- **Tấn công Evil Twin:** tạo điểm truy cập (AP) **giống hệt với điểm truy cập hiện có** và kiểm soát giao tiếp của người dùng trong mạng này.



Tấn công từ chối dịch vụ

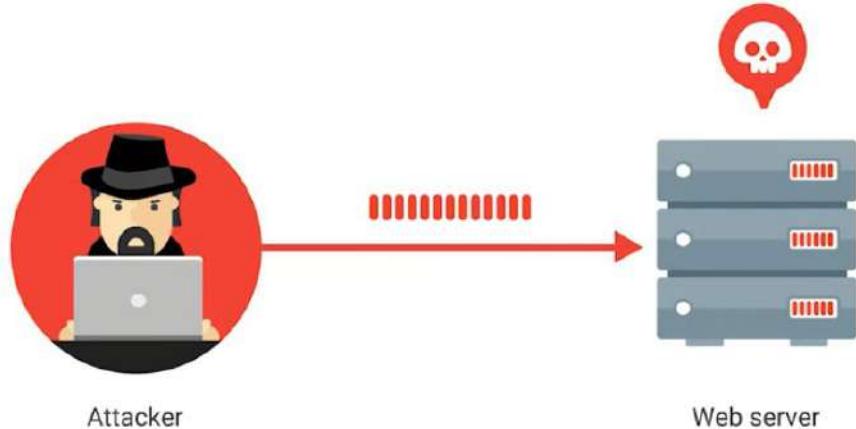
Tấn công từ chối dịch vụ (denial-of-service attack) là dạng tấn công **ngăn chặn quyền truy cập** của người dùng khác bằng cách gây áp đảo mạng hoặc máy chủ.



Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (denial-of-service attack) có thể thực hiện bằng cách:

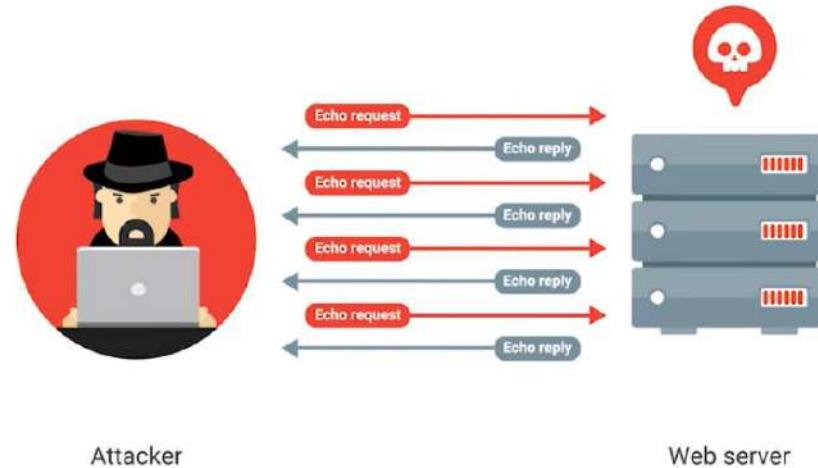
- Ping of Death (PoD): gửi một gói ping có kích thước lớn để gây tràn bộ đệm.



Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (denial-of-service attack) có thể thực hiện bằng cách:

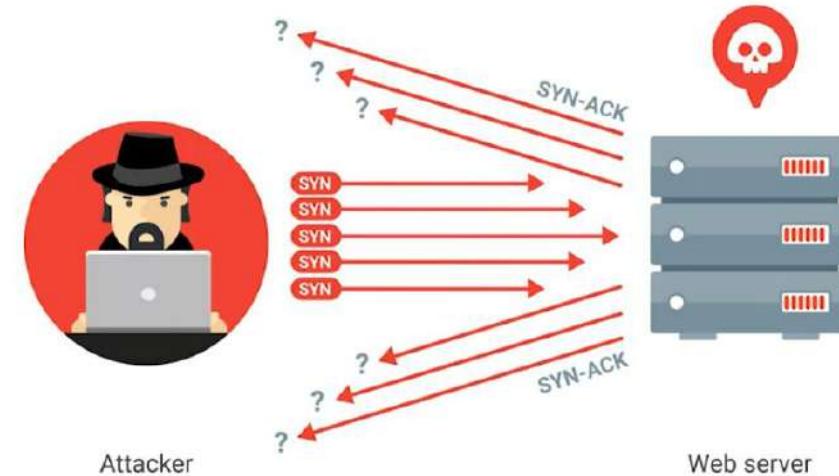
- **Ping flood:** gửi rất nhiều gói ping đến hệ thống.



Tấn công từ chối dịch vụ

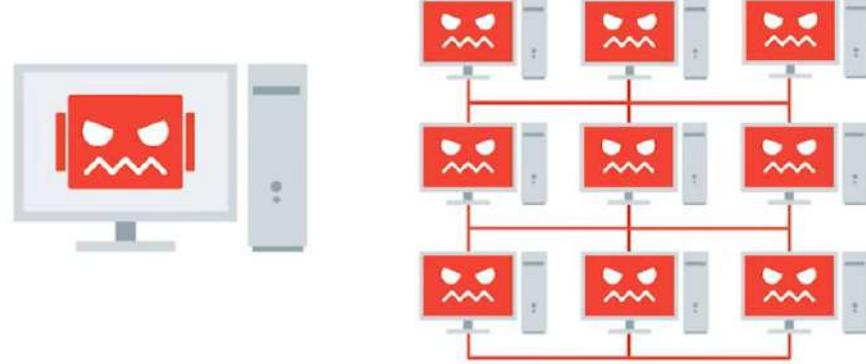
Tấn công từ chối dịch vụ
(denial-of-service attack) có thể thực hiện bằng cách:

- **SYN flood** (half-open attack): gửi rất nhiều gói SYN đến hệ thống và không phản hồi xác nhận.



Tấn công từ chối dịch vụ phân tán

Tấn công từ chối dịch vụ phân tán
(distributed denial-of-service attack, DDoS) là **cuộc tấn công DoS** sử dụng
nhiều máy tính phân tán trên mạng
(botnet).



Tấn công tiêm mã độc

- Tấn công tiêm mã độc (injection attack) là cách thức khai thác lỗi máy tính do xử lý dữ liệu không hợp lệ.
- Hạn chế bằng cách:
 - Kiểm tra kỹ dữ liệu được cung cấp
 - Làm sạch dữ liệu



Tấn công tiêm mã độc

Tấn công tiêm mã độc phổ biến như:

- **Tấn công XSS** (cross-site scripting) là loại tấn công **tiêm mã độc vào trang web** và thường được sử dụng để **lấy phiên đăng nhập** của người dùng dịch vụ.



Tấn công tiêm mã độc

Tấn công tiêm mã độc phổ biến như:

- Tiêm mã độc SQL (SQL injection) là loại tấn công tiêm mã độc cho phép **xóa, sao chép hay chạy các lệnh độc hại** trên cơ sở dữ liệu SQL thực thi trên máy chủ.



Tấn công mật khẩu

Tấn công mật khẩu (password attack) là cách thức sử dụng phần mềm bẻ khóa mật khẩu để thử và đoán nội dung mật khẩu.

- ✗ 000111
- ✗ abc123
- ✗ 01-01-01
- ✗ aBc&!3DoP
- ✗ 10-6-1983
- ✓ 12345



Tấn công mật khẩu

Tấn công mật khẩu (password attack) được thực hiện bằng cách:

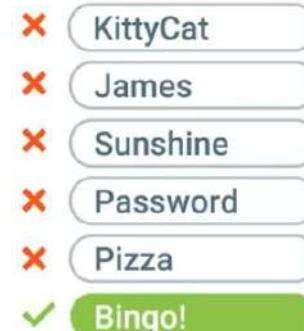
- Tấn công vét cạn (brute force attack): thử tất cả các tổ hợp ký tự và chữ cái khác nhau cho đến khi có quyền truy cập.
 - CAPTCHA là cách thức ngăn chặn tấn công vét cạn bằng cách đưa ra các thử thách để phân biệt người với máy.



Tấn công mật khẩu

Tấn công mật khẩu (password attack) được thực hiện bằng cách:

- Tấn công từ điển (dictionary attack): thử các từ thường được sử dụng trong mật khẩu.
 - Khắc phục bằng cách:
 - Kết hợp viết hoa, số, ký hiệu
 - Ví dụ: s@nDwh1ch
 - Dùng CAPTCHA



Tấn công phi kỹ thuật

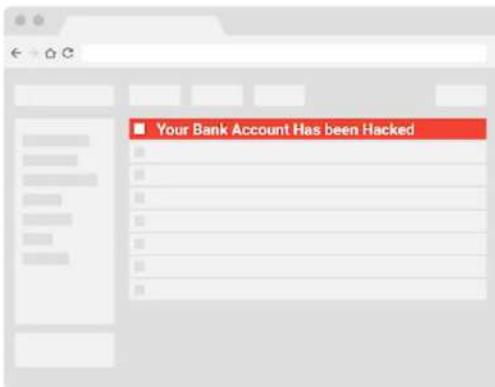
Tấn công phi kỹ thuật (social engineering attack) là cách thức **tấn công nhằm vào con người** để **lừa đảo** quyền truy cập thông tin cá nhân hoặc lừa nạn nhân thực hiện điều nào đó.



Tấn công phi kỹ thuật

Tấn công phi kỹ thuật phổ biến gồm:

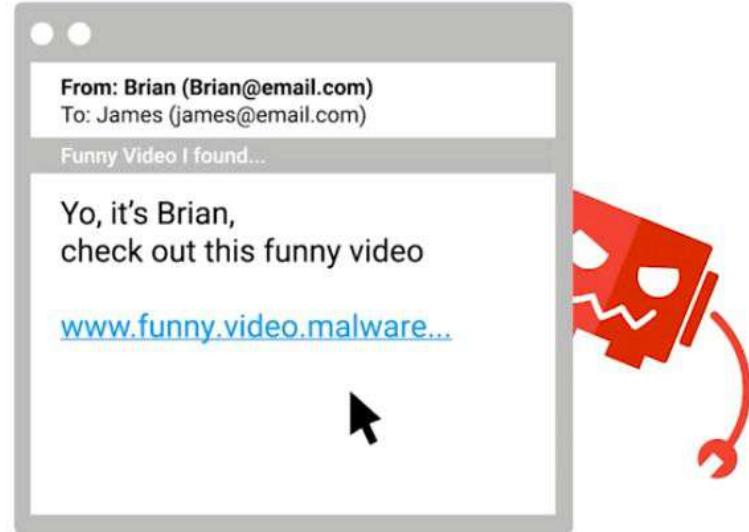
- Phishing: lừa đảo thường qua email
- Spear phishing: lừa đảo qua email nhưng nhắm vào cá nhân/nhóm cụ thể.



Tấn công phi kỹ thuật

Tấn công phi kỹ thuật phổ biến gồm:

- **Spoofing:** giả mạo thành một thứ khác



Tấn công phi kỹ thuật

Tấn công phi kỹ thuật phổ biến gồm:

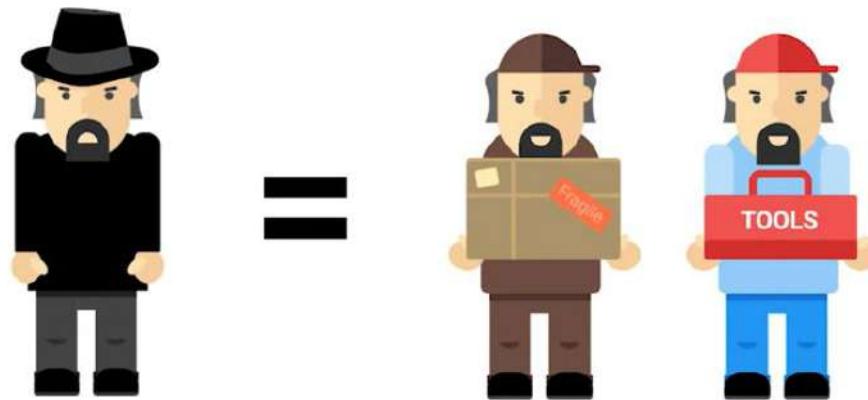
- **Mồi nhử** (baiting): dụ nạn nhân làm điều gì đó.
 - Ví dụ: để lại USB ở đâu đó để nạn nhân nhặt và cắm vào máy của họ.



Tấn công phi kỹ thuật

Tấn công phi kỹ thuật phổ biến gồm:

- **Trà trộn** (tailgating): đóng giả và theo chân người có thẩm quyền để xâm nhập hệ thống.





2 Mật Mã Học



Nội dung



Mã hóa và giải mã



Mã hóa đối xứng



Mã hóa bất đối xứng



Băm



Hệ tầng khóa công khai



Bảo mật mạng



Phần cứng mã hóa

Mã hóa

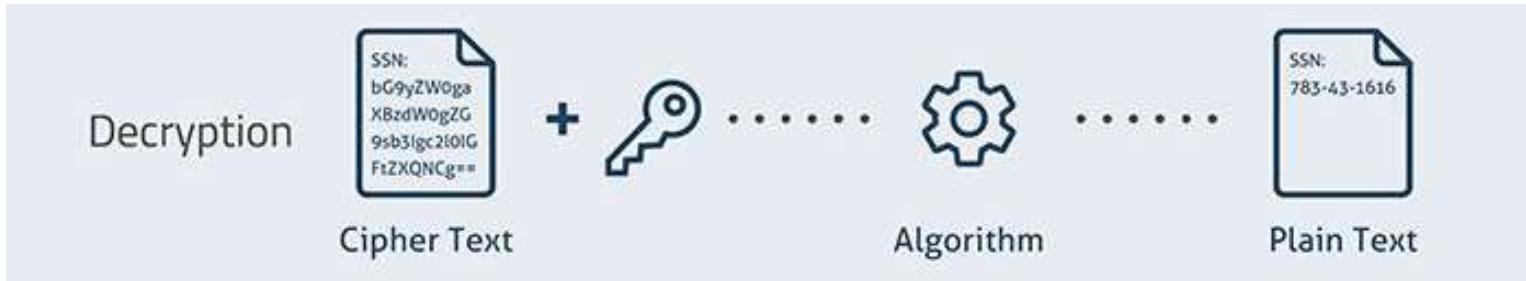
Mã hóa (encryption) là hành động **lấy** một thông điệp và **thực hiện** phép biến đổi trên nó để **được** một thông điệp mới không thể hiểu nội dung.

- Thông điệp trước khi mã hóa được gọi là **bản rõ** (plaintext)
- Phép biến đổi được gọi là **phép mã hóa** (cipher)
- Thông điệp sau khi mã hóa được gọi là **bản mã** (ciphertext)



Giải mã

Giải mã (decryption) là hành động **lấy** một thông điệp đã được mã hóa và **thực hiện phép biến đổi** trên nó để **được** một **thông điệp ban đầu**.



Ví dụ mã hóa và giải mã

Cipher:

$$e = o \quad o = y$$

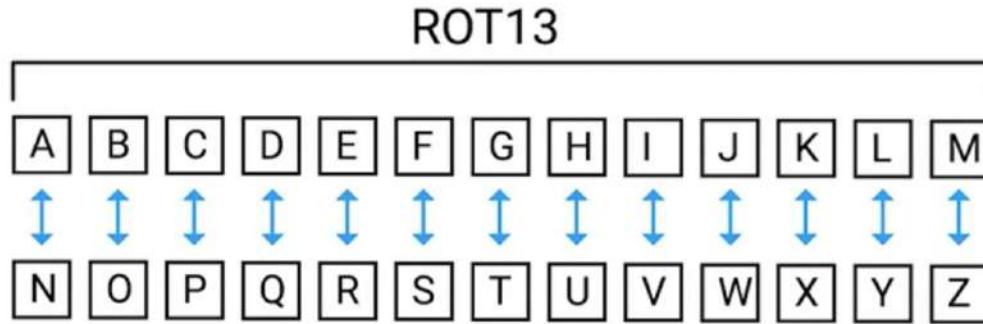
Plaintext:

Hello World

Ciphertext:

Holly Wyrld

Ví dụ mã hóa và giải mã



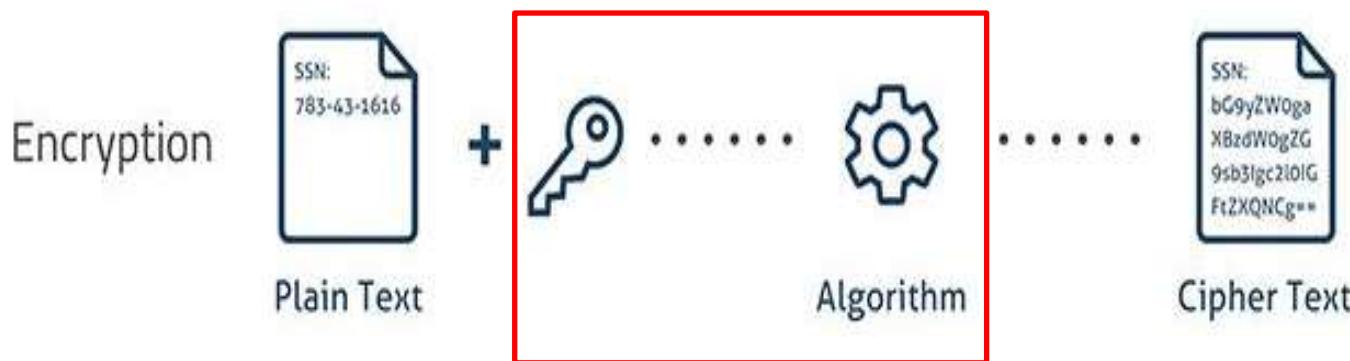
URYYB JBEYQ
=

HELLO WORLD

Phép Mã Hóa

Một phép mã hóa (cipher) bao gồm 2 thành phần cơ bản:

- Thuật toán mã hóa (encryption algorithm): quy trình sử dụng để chuyển bản rõ thành bản mã.
- Chìa khóa (key): thông tin để cá biệt hóa quá trình mã hóa cũng như giải mã.



Bảo mật dựa trên sự mập mờ

Bảo mật dựa trên sự mập mờ (security through obscurity, STO) là cách thức bảo mật thông qua việc **không** cho ai biết thuật toán mã hóa được sử dụng.

- Đây **không phải là cách tốt** để đảm bảo an ninh thông tin hoặc hệ thống.



Nguyên tắc Kerckhoffs

Nguyên tắc Kerckhoffs:

“Độ an toàn của hệ thống mật mã không phụ thuộc vào việc giữ bí mật thuật toán mã hóa, nó phụ thuộc vào việc giữ bí mật chìa khóa.”

“Kẻ thù biết hệ thống” (Shannon)



Mật mã, mật mã học và phân tích mật mã

- Mật mã (cryptology) là quá trình thực hiện mã hóa và ẩn thông điệp.
- Mật mã học (cryptography) là ngành nghiên cứu cách thức thực hiện mã hóa và ẩn thông điệp.
- Phân tích mật mã (cryptanalysis) là ngành nghiên cứu cách phá mã hay phá vỡ sự bảo mật của giải thuật mật mã.



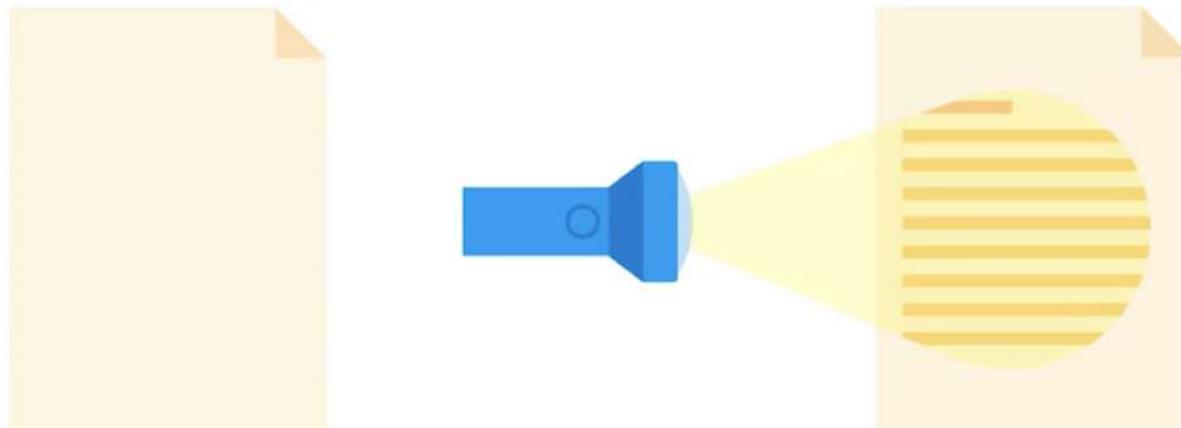
Phân tích tần số

Phân tích tần số (frequency analysis) là quá trình thống kê tần suất xuất hiện của các các chữ cái trong bản mã để từ đó tìm ra chìa khóa hay cách thức phá mã.



Steganography

Steganography là thuật ngữ mô tả quá trình **che giấu thông tin** khỏi những người quan sát nhưng không mã hóa nó.



Nội dung



Mã hóa và giải mã



Mã hóa đối xứng



Mã hóa bất đối xứng



Băm



Hệ tầng khóa công khai



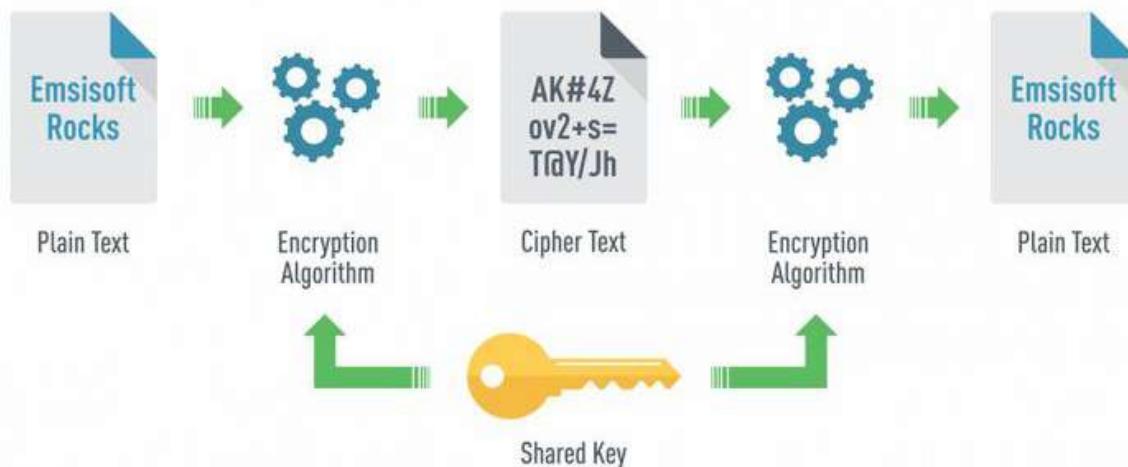
Bảo mật mạng



Phần cứng mã hóa

Mã hóa đối xứng

Mã hóa đối xứng (symmetric cryptography) là cách thức sử dụng cùng một khóa để mã hóa và giải mã thông điệp.



Mã hóa đối xứng

Một số loại mã hóa đối xứng phổ biến:

- Mã hóa thay thế (substitution cipher) là một cơ chế mã hóa thay thế các phần của bản rõ để được bản mã.

Cipher: $e = o \quad o = y$

Plaintext:

Hello World

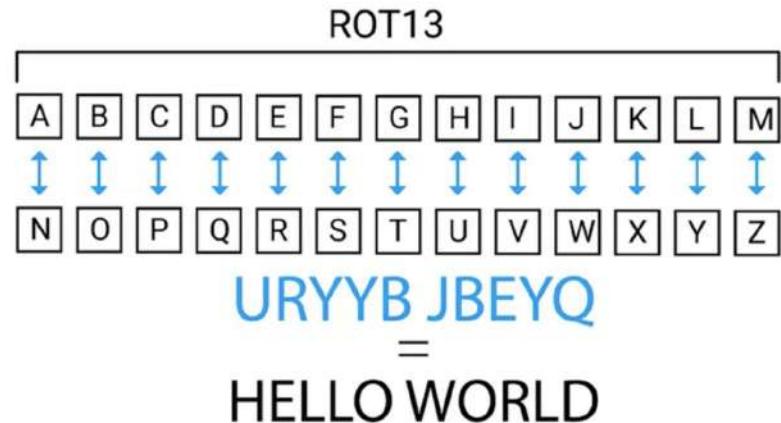
Ciphertext:

Holly Wyrld

Mã hóa đối xứng

Một số loại mã hóa đối xứng phổ biến:

- Mã hóa thay thế (substitution cipher)
 - **Mã hóa Caesar** (Caesar cipher) là thuật toán **thay thế** các ký tự trong bảng chữ cái bằng những ký tự khác thông qua **phép dịch chuyển hoặc xoay bảng chữ cái**.



Mã hóa đối xứng

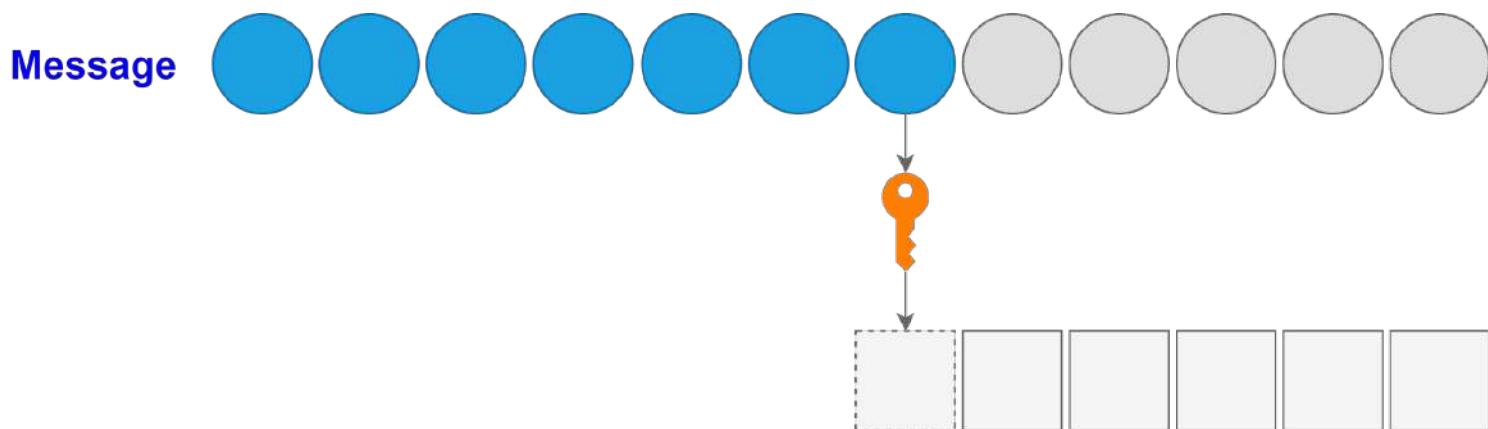
Một số loại mã hóa đối xứng phổ biến:

- Mã hóa dòng (stream cipher)
- Mã hóa khối (block cipher)



Mã hóa đối xứng

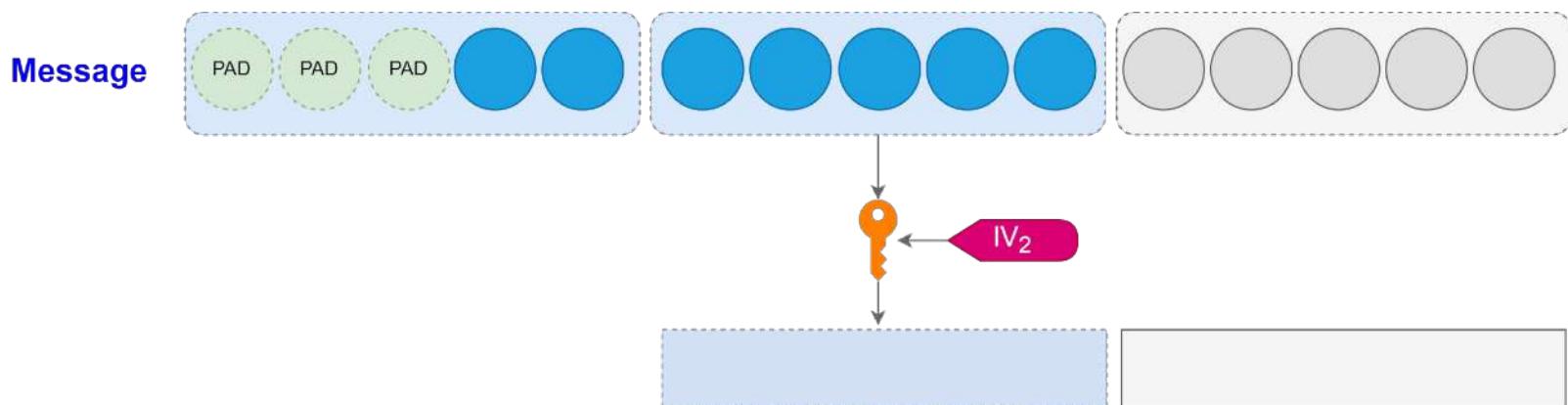
Mã hóa dòng (stream cipher): mã hóa từng ký tự nhận được.



Mã hóa đối xứng

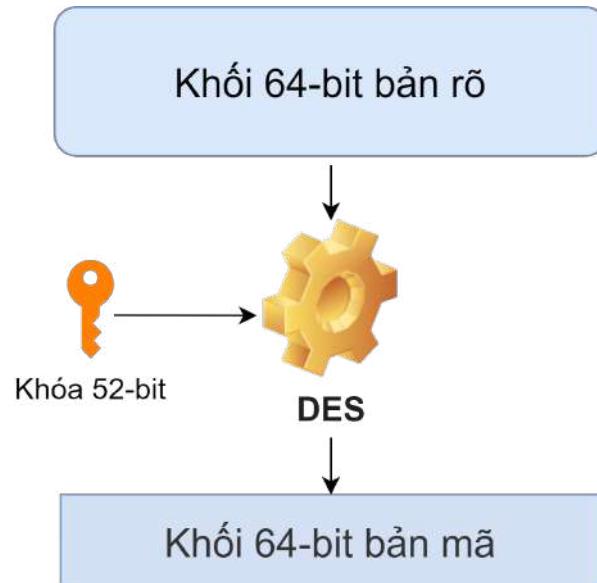
Mã hóa khối (block cipher): chia dữ liệu thành từng khối có kích thước cố định, mã hóa mỗi khối thành một đơn vị xác định.

- Nếu dữ liệu nhỏ hơn kích thước khối, không gian còn lại sẽ được đệm thêm.



Thuật toán DES

DES (Data Encryption Standard) là một mã hóa khối đối xứng sử dụng **kích thước khóa 64-bit** (trong đó, dành 8 bit để kiểm tra lỗi) và **hoạt động trên các khối có kích thước 64-bit**.



Thuật toán DES

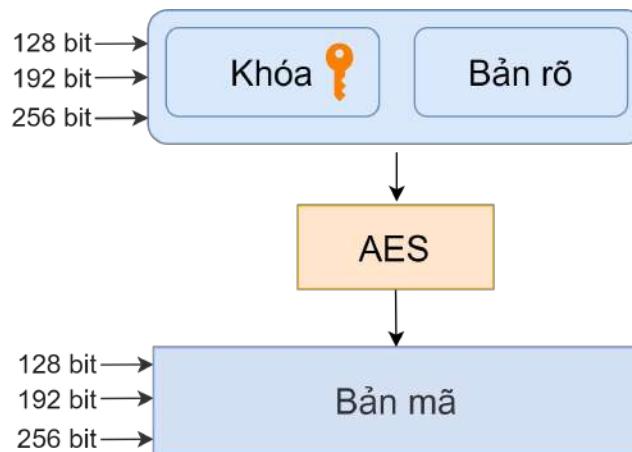
Tấn công thuật toán DES

- Độ dài khóa 56 bit tương đương 2^{56} khả năng
- Một phương pháp tấn công là vét cạn (brute force)
- Năm 1998, tổ chức EFF (Electronic Frontier Foundation) giải mã thành công trong 56 giờ



Thuật toán AES

Thuật toán AES (Advanced Encryption Standard) là một mã hóa khối đối xứng tương tự như DES nhưng sử dụng khối 128 bit và độ dài khóa hỗ trợ gồm 128 bit, 192 bit, 256 bit.



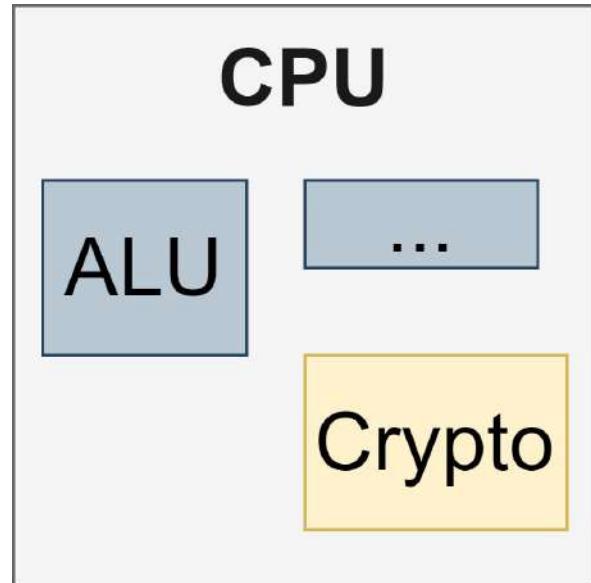
Phần cứng hỗ trợ

Tiêu chí đánh giá thuật toán mã hóa:

- Mạnh mẽ trước các tấn công
- Tốc độ thực thi
- Dễ triển khai

Một số phần cứng hỗ trợ giúp tăng tốc:

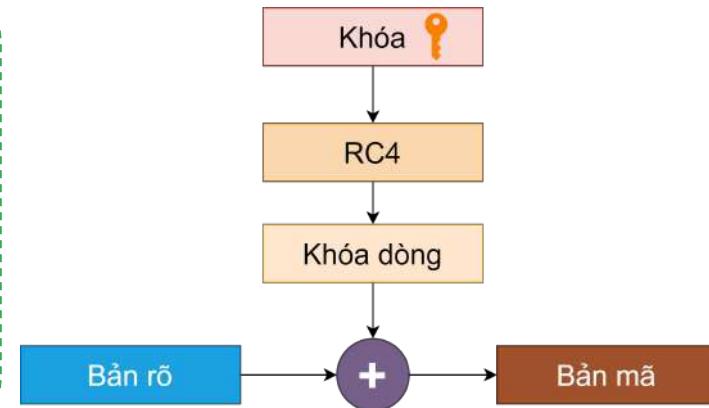
- CPU hiện đại có tập lệnh AES tích hợp sẵn



Thuật toán RC4

Thuật toán RC4 (Rivest Cipher 4) là một mã hóa dòng đối xứng đơn giản và tốc độ nhanh với kích thước khóa từ 40 bit đến 2048 bit.

- Sử dụng rộng rãi trong WEP, WPA, SSL, TLS.
- Thuật toán mã hóa có nhiều điểm yếu khiến nó dễ bị phá.
 - Cuộc tấn công RC4 NOMORE đã phá trong 52 giờ.
- Năm 2015, TSL loại bỏ RC4 khỏi giao thức
 - TLS 1.2 sử dụng AES GCM (Galois/Counter Mode).



Thuận lợi và bất lợi của mã hóa đối xứng

Thuận lợi:

- Dễ thực hiện và bảo trì.
- Thực thi nhanh thậm chí trên dữ liệu lớn.

Bất lợi:

- Trao đổi khóa là điều phức tạp.



Nội dung



Mã hóa và giải mã



Mã hóa đối xứng



Mã hóa bất đối xứng



Băm



Hệ tầng khóa công khai



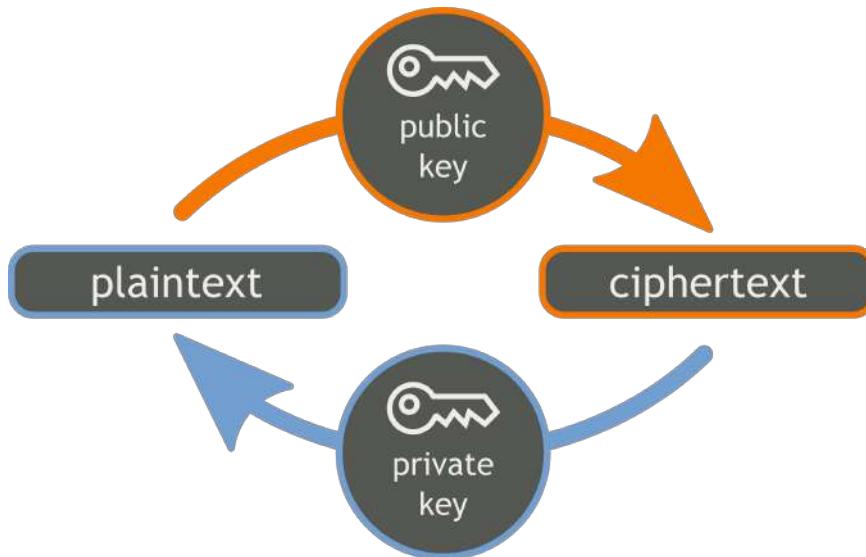
Bảo mật mạng



Phần cứng mã hóa

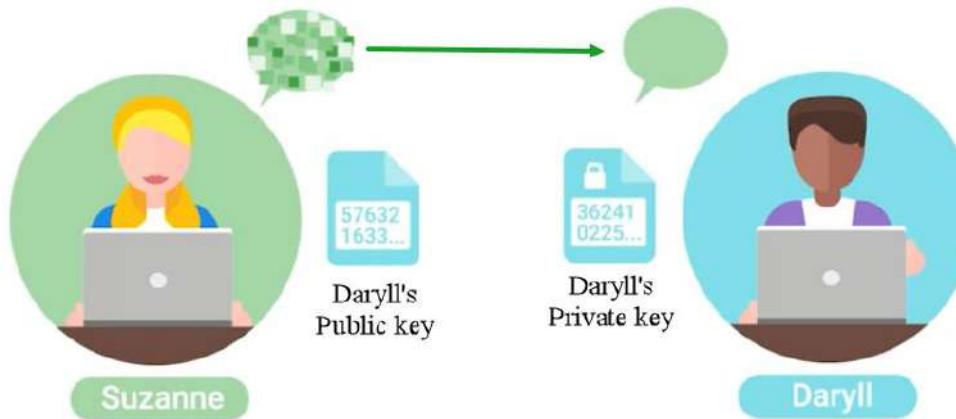
Mã hóa bất đối xứng

Mã hóa bất đối xứng (asymmetric encryption) là cách thức sử dụng **khóa khác nhau** cho quá trình mã hóa và giải mã.



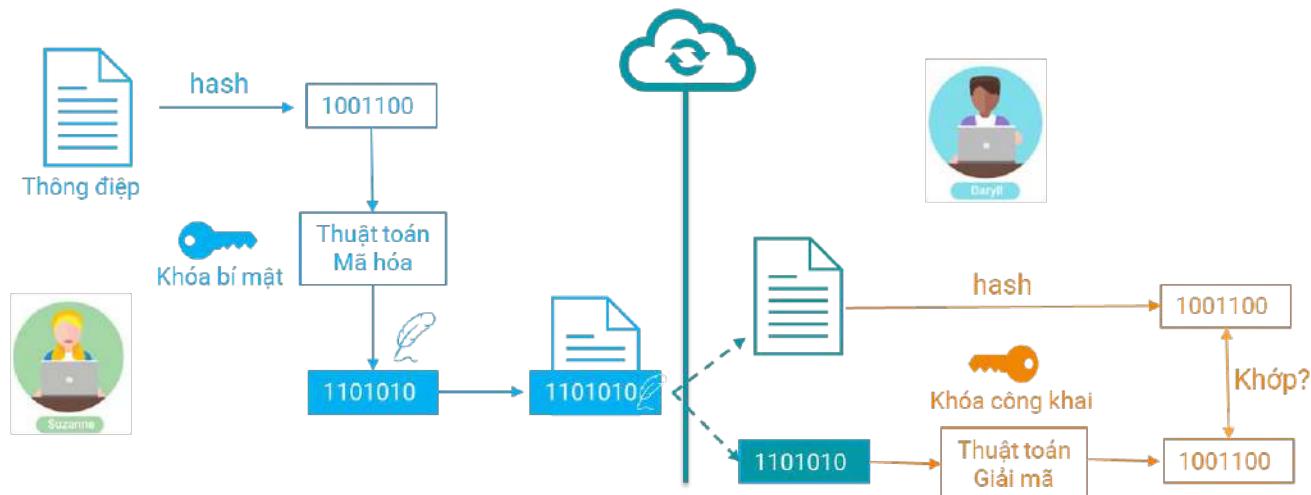
Khóa công khai và khóa bí mật

- Khóa công khai (public key) là khóa dùng để mã hóa dữ liệu.
- Khóa bí mật (private key) là khóa dùng để giải mã dữ liệu.



Chữ ký số

Chữ ký số (digital signature) là một kỹ thuật toán học để **xác thực thông điệp** điện tử.



Tính chất của mã hóa bất đối xứng

Mã hóa bất đối xứng đảm bảo các tính chất:

- Tính bảo mật (confidentiality): thông qua cơ chế mã hóa-giải mã.
- Tính xác thực (authenticity): thông qua chữ ký số.
- Chống thoái thác (non-repudiation): đảm bảo thông điệp đến từ người tự xưng là tác giả.



Confidentiality



Authenticity



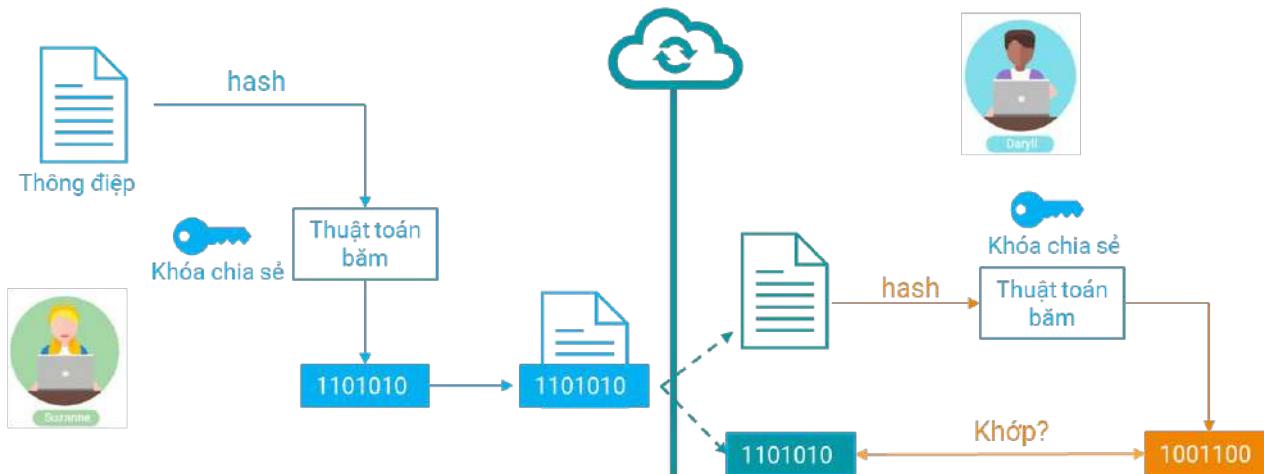
Non-repudiation

Phối hợp mã hóa đối xứng và bất đối xứng

Mã hóa đối xứng	Mã hóa bất đối xứng
Thuận lợi: <ul style="list-style-type: none">Dễ thực hiện và bảo trì.Thực thi nhanh thậm chí trên dữ liệu lớn. Bất lợi: <ul style="list-style-type: none">Trao đổi khóa là điều phức tạp.	Thuận lợi: <ul style="list-style-type: none">Giao tiếp an toàn qua môi trường không tin cậy.Đảm bảo nguồn gốc của thông điệp. Bất lợi: <ul style="list-style-type: none">Tốn chi phí và phức tạp hơn về mặt tính toán
Phối hợp lợi ích của cả hai loại mã hóa: <ul style="list-style-type: none">Mã hóa bất đối xứng dùng để trao đổi khóa hoặc thuật toán mã hóa.Mã hóa đối xứng để mã hóa dữ liệu truyền nhận.	

Mã xác thực thông điệp

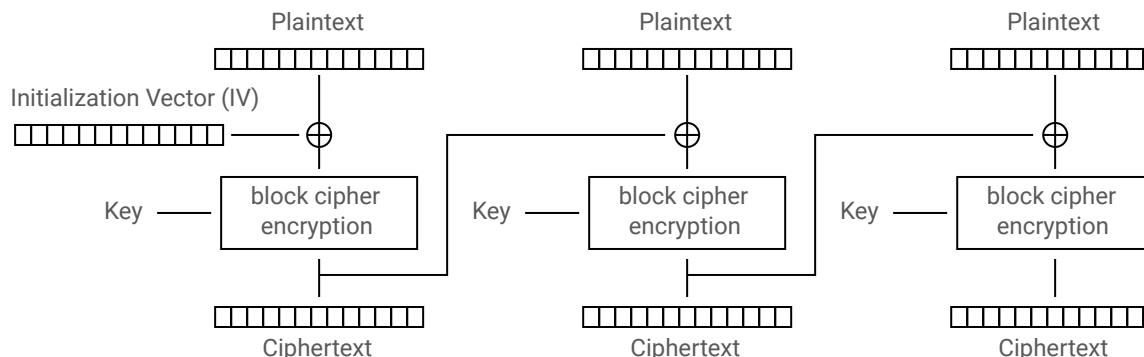
Mã xác thực thông điệp (Message Authentication Codes, MAC) là mẫu thông tin cho phép xác thực thông điệp qua hàm băm mã hóa dùng chung khóa bí mật.



Mã xác thực thông điệp

Một số giải thuật MAC phổ biến gồm:

- **HMAC** (Keyed-Hash Message Authentication Code)
- **CMAC** (Cipher-Based Message Authentication Code)
- **CBC-MAC** (Cipher Block Chaining Message Authentication Code)



Cipher Block Chaining (CBC) mode

Nguồn: Wikimedia

Các thuật toán mã hóa bất đối xứng

Một số thuật toán mã hóa bất đối xứng phổ biến như:

- RSA (Ron Rivest, Adi Shamir, Leonard Adleman): tạo và phân phối khóa dựa trên hai số nguyên tố ngẫu nhiên, duy nhất và rất lớn.



Các thuật toán mã hóa bất đối xứng

Một số thuật toán mã hóa bất đối xứng phổ biến như:

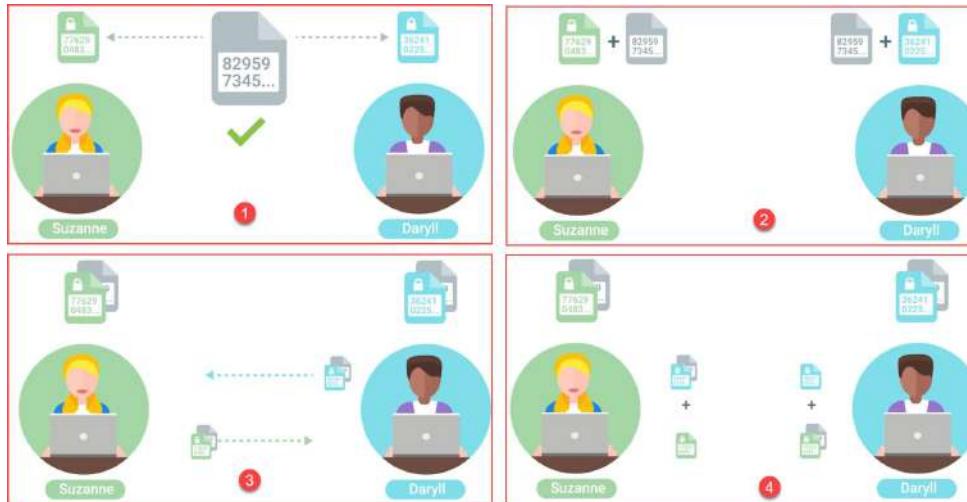
- RSA
- DSA (Digital Signature Algorithm): ký và xác minh dữ liệu dựa trên cặp khóa.



Các thuật toán mã hóa bất đối xứng

Một số thuật toán mã hóa bất đối xứng phổ biến như:

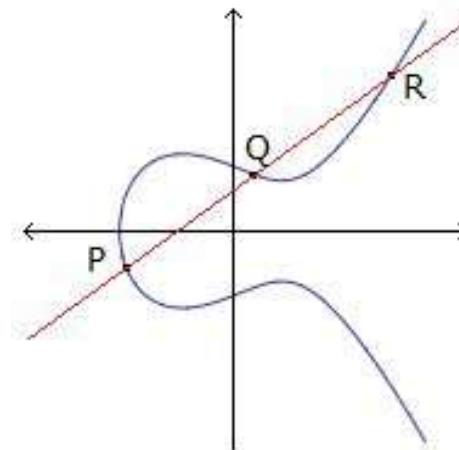
- DH (Diffie-Hellman): trao đổi khóa dựa trên kết hợp các số nguyên tố.



Các thuật toán mã hóa bất đối xứng

Một số thuật toán mã hóa bất đối xứng phổ biến như:

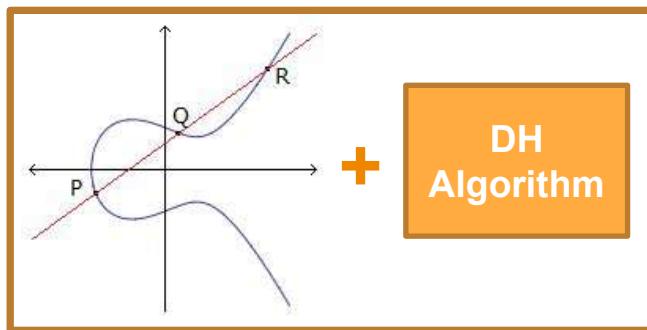
- **ECC** (Elliptic curve cryptography): sử dụng cấu trúc đại số của đường cong elliptic trên các trường hữu hạn để tạo khóa an toàn.
 - Một khóa trên đường cong elliptic 256 bit có thể tương đương với khóa RSA có độ dài 3072 bit.



Các thuật toán mã hóa bất đối xứng

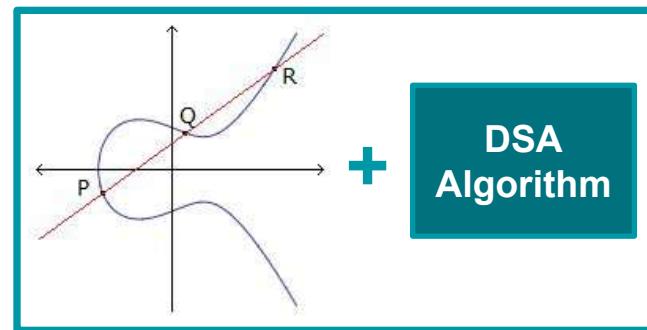
Một số thuật toán mã hóa bất đối xứng phổ biến như:

- ECDH, ECDSA: các biến thể của DH và DSA sử dụng đường cong elliptic.



**DH
Algorithm**

ECDH



**DSA
Algorithm**

ECDSA

Nội dung

-  Mã hóa và giải mã
-  Mã hóa đối xứng
-  Mã hóa bất đối xứng
-  **Băm**
-  Hạ tầng khóa công khai
-  Bảo mật mạng
-  Phần cứng mã hóa

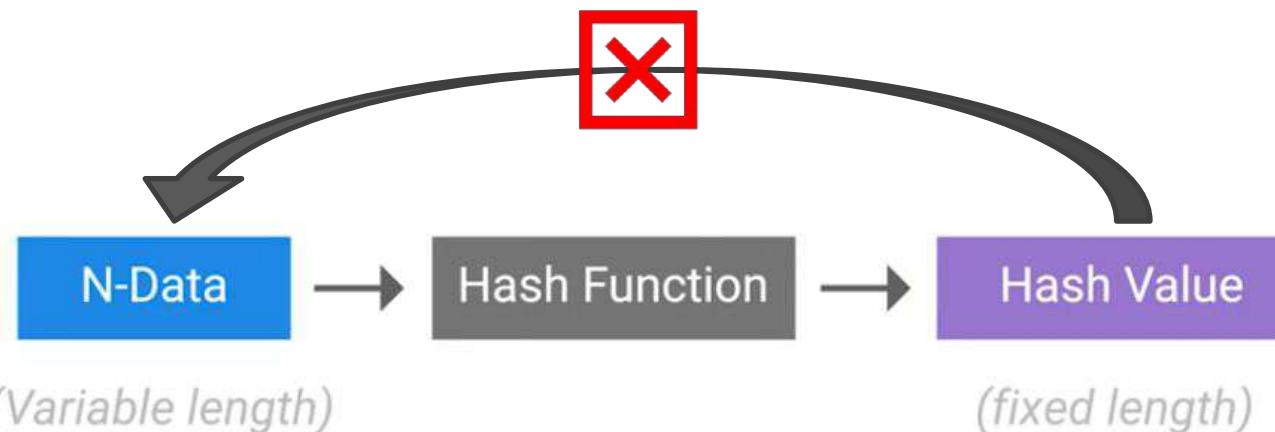
Hàm băm

Hàm băm (hash function) là loại hàm hay thao tác nhận đầu vào dữ liệu bất kỳ và ánh xạ nó thành đầu ra có kích thước cố định.



Hàm băm mã hóa

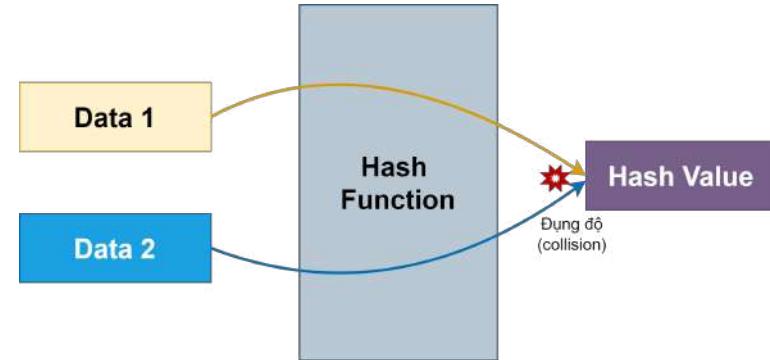
Hàm băm mã hóa (cryptographic hashing) là hàm ánh xạ một chiều.



Tính chất của hàm băm mã hóa

Hàm băm mã hóa cần thỏa:

- **Tính xác định:** cùng giá trị đầu vào sẽ trả ra cùng một giá trị băm.
- **Tính toán nhanh và hiệu quả**
- Không có mối tương quan giữa việc thay đổi một phần dữ liệu với một phần trên giá trị băm.
- Không thể đảo ngược
- Hạn chế xảy ra **đụng độ** (hash collision)
 - Đụng độ nghĩa là hai đầu vào khác nhau ánh xạ đến cùng một đầu ra.



Các thuật toán băm

Một số thuật toán băm phổ biến:

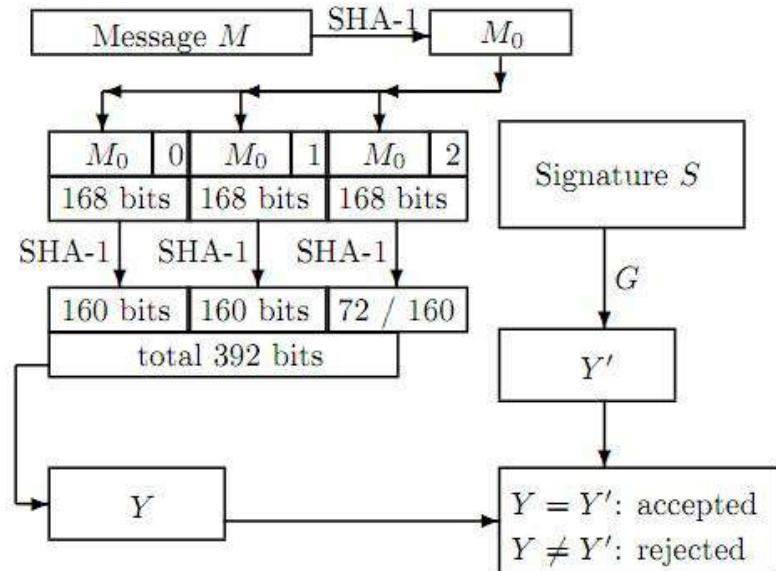
- MD5: hoạt động trên một khối 512 bit và tạo ra giá trị băm 128 bit.
 - MD5 dễ bị đụng độ nên được khuyến cáo không sử dụng cho các tác vụ liên quan đến bảo mật.

```
$ echo 'Hello World' | md5sum  
e59ff97941044f85df5297e1c302d260
```

Các thuật toán băm

Một số thuật toán băm phổ biến:

- SHA-1, SHA-2, SHA-3: hoạt động trên một khối 512 bit và tạo ra giá trị băm 160 bit.
 - Với sức mạnh của máy tính ngày nay, **SHA-1 không còn an toàn** và được khuyến cáo không sử dụng.



Các thuật toán băm

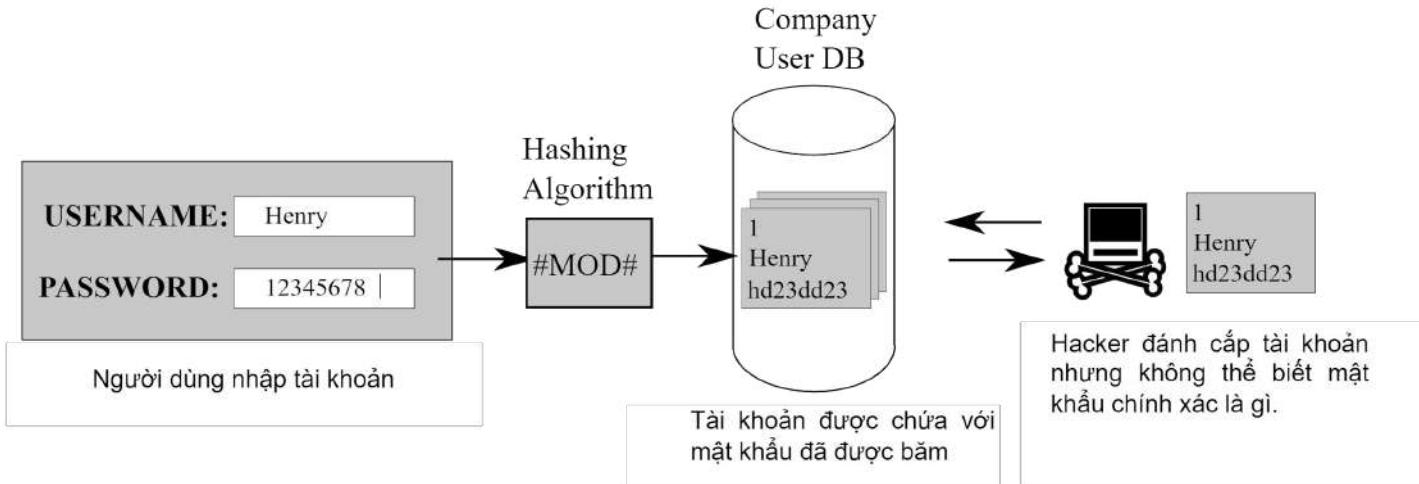
Một số thuật toán băm phổ biến:

- **MIC** (Message integrity check): đóng vai trò như một **giá trị checksum** (tổng kiểm) cho dữ liệu.
 - MIC không sử dụng khóa nên nó không thể bảo vệ chống lại hành động giả mạo.



Ví dụ ứng dụng của băm

Mật khẩu đăng nhập hệ thống cần lưu trữ dưới dạng giá trị băm, không được lưu dưới dạng bản rõ.



Tấn công giá trị băm và cách phòng thủ

Tấn công	Phòng thủ
<p>Để tìm lại bản gốc của giá trị băm, kẻ tấn công có thể:</p> <ul style="list-style-type: none">• Tấn công vét cạn (brute force attack): thủ băm tất cả các giá trị đầu vào có thể có cho đến khi trùng khớp giá trị băm.	<p>Người dùng có thể:</p> <ul style="list-style-type: none">• Cách 1: giới hạn thời gian và tài nguyên cần để thủ.• Cách 2: chạy dữ liệu qua hàm băm nhiều lần.

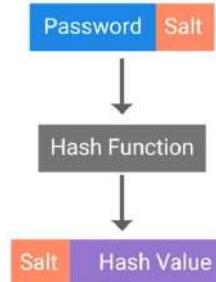


Tấn công giá trị băm và cách phòng thủ

Tấn công	Phòng thủ
<p>Để tìm lại bản gốc của giá trị băm, kẻ tấn công có thể sử dụng:</p> <ul style="list-style-type: none">• Bảng cầu vồng (rainbow table): bảng lưu trữ giá trị tính toán trước của các mật khẩu có thể có.	<p>Người dùng có thể sử dụng:</p> <ul style="list-style-type: none">• Muối mật khẩu (password salt): chuỗi ngẫu nhiên đủ lớn được nối thêm vào mật khẩu trước khi băm.



Password	Hash
123456	e10adc983ad09dca098da02320e
password	09dca09e10a0232dc983ad834ds
qwerty	h566adc983ad09d432fgsdcg432
baseball	123dsa3ad09dca3fer34r4653323
dragon	12409dca098dsa42363412467s2
kittycat	2ws3d4c983ad23wsd34565f4643
000111	344rfwc9834564dca09756324t72



Nội dung



Mã hóa và giải mã



Mã hóa đối xứng



Mã hóa bất đối xứng



Băm



Hệ tầng khóa công khai



Bảo mật mạng

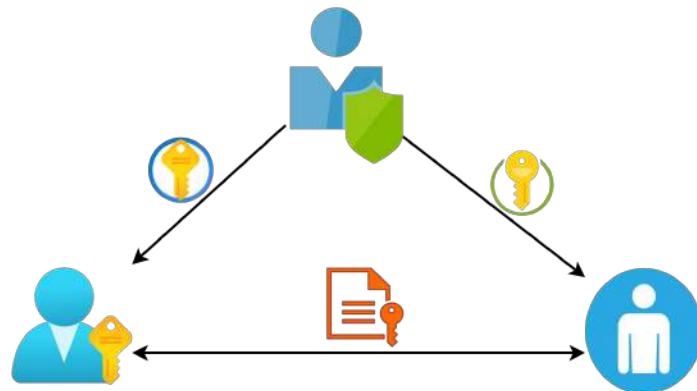


Phần cứng mã hóa

Hệ tầng khóa công khai

Hệ tầng khóa công khai (public key infrastructure, PKI) là một hệ thống để cho một bên thứ 3 cung cấp và xác thực danh tính của các bên tham gia vào quá trình trao đổi.

- Hệ thống PKI định nghĩa việc tạo, lưu trữ và phân phối chứng chỉ số.



Chứng chỉ số

Chứng chỉ số (digital certificate) là một tập tin chứng minh một thực thể sở hữu khóa công khai nhất định.

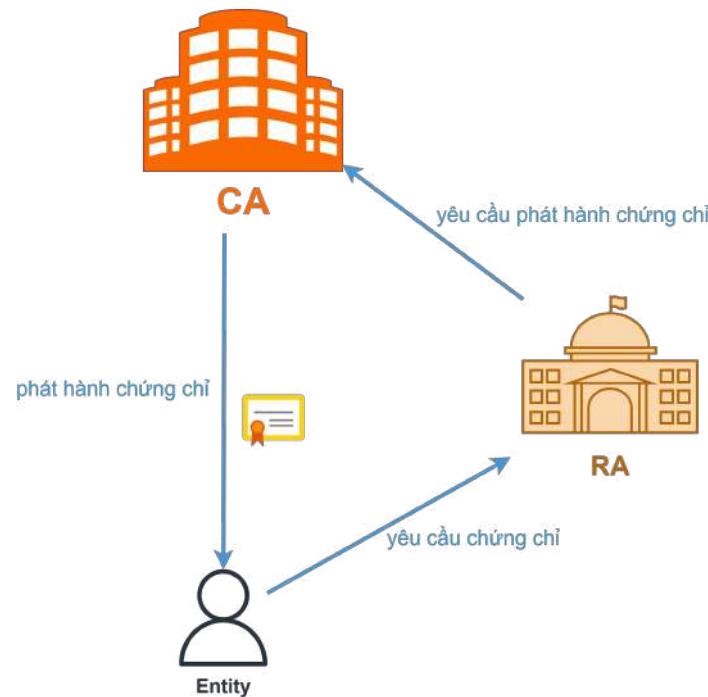
- Chứng chỉ số chứa thông tin về khóa công khai, người sở hữu, chữ ký số.



- INFO ON PUBLIC KEY
- REGISTERED OWNER
- DIGITAL SIGNATURE

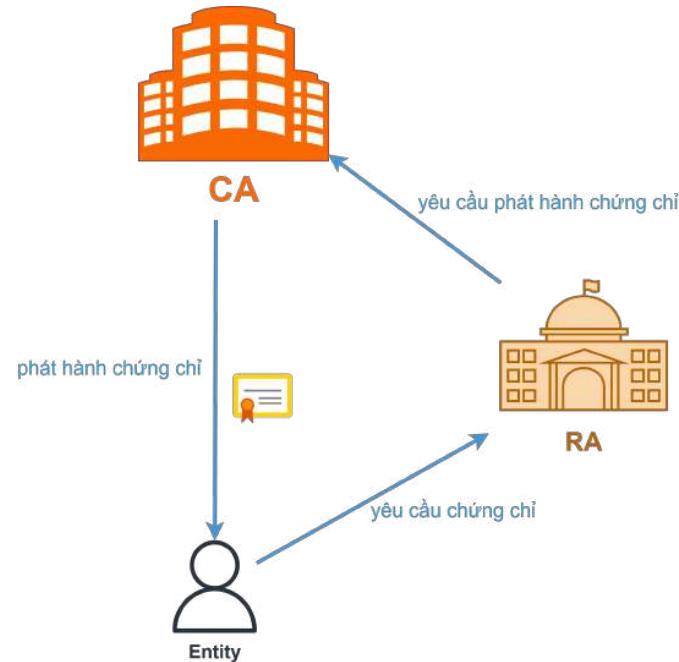
Nhà cung cấp chứng chỉ số

Nhà cung cấp chứng chỉ số (certificate authority, CA) là một thực thể chịu trách nhiệm lưu trữ, phát hành và ký chứng chỉ.



Cơ quan đăng ký

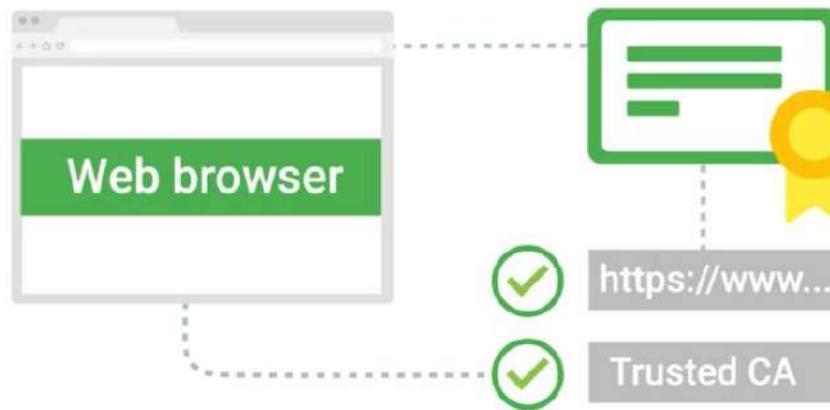
Cơ quan đăng ký (registration authority, RA) là cơ quan chịu trách nhiệm xác minh danh tính của người yêu cầu chứng chỉ và yêu cầu CA phát hành nó.



Các loại chứng chỉ số

Một số loại chứng chỉ phổ biến:

- Chứng chỉ máy chủ SSL/TLS (SSL/TLS server certificate): xác minh thủ chủ chứng chỉ khớp với tên máy chủ đang kết nối đến.



Các loại chứng chỉ số

Một số loại chứng chỉ phổ biến:

- Chứng chỉ máy chủ SSL/TLS
(SSL/TLS server certificate)
- **Chứng chỉ tự ký** (self sign certificate): **sử dụng khóa bí mật** để ký khóa công khai nhằm tự tạo ra chứng chỉ.



Các loại chứng chỉ số

Một số loại chứng chỉ phổ biến:

- Chứng chỉ máy chủ SSL/TLS (SSL/TLS server certificate)
- Chứng chỉ tự ký (self sign certificate)
- **Chứng chỉ máy khách SSL/TLS** (SSL/TLS client certificate): xác thực máy khách khi giao tiếp với máy chủ.



Các loại chứng chỉ số

Một số loại chứng chỉ phổ biến:

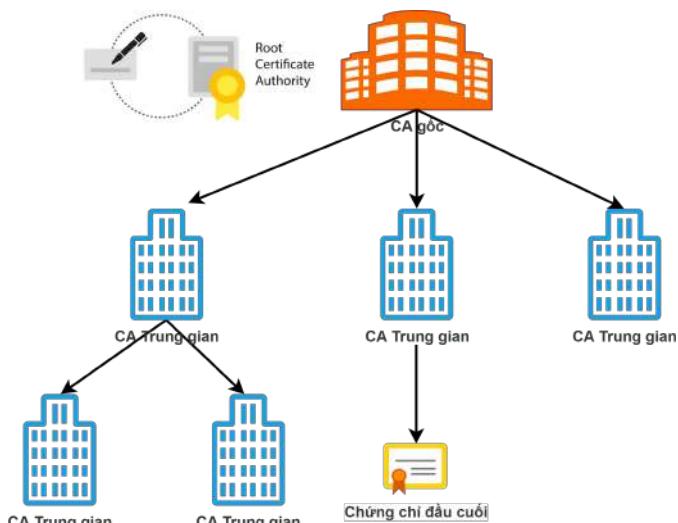
- Chứng chỉ máy chủ SSL/TLS (SSL/TLS server certificate)
- Chứng chỉ tự ký (self sign certificate)
- Chứng chỉ máy khách SSL/TLS (SSL/TLS client certificate)
- **Chứng chỉ ký mã nguồn** (code signing certificate): xác minh ứng dụng không bị giả mạo và đến từ tác giả phần mềm.



Chuỗi CA tin cậy

Mạng lưới các nhà cung cấp chứng chỉ số tin cậy bắt đầu với một **CA gốc** được tin tưởng.

- CA gốc tự ký chứng chỉ của nó.
- CA gốc ký xác nhận cho các CA trung gian với một trường được gán giá trị True trong chứng chỉ.
- Các CA trung gian có thể xác nhận cho các CA trung gian khác.
- Một chứng chỉ mà không được xác thực như CA (không gán True) được gọi là **chứng chỉ lá** (leaf certificate) hay **chứng chỉ đầu cuối** (end-entity certificate)



Cấu trúc của chứng chỉ số

Chuẩn X.509 mô tả cấu trúc của một chứng chỉ số:

- **Version:** phiên bản của X.509.
- **Serial number:** số nhận dạng đơn nhất cho chứng chỉ.
- **Signature Algorithm:** thuật toán ký.
- **Issuer:** tên nhà phát hành.
- **Validity:** khoảng thời gian hợp lệ.
- **Subject:** thông tin pháp nhân được cấp chứng chỉ.
- **Subject public key:** thuật toán khóa công khai và khóa công khai.
- **Fingerprint:** giá trị băm của toàn bộ chứng chỉ.



Web of Trust

Web of Trust là nơi **các cá nhân** thay vì tổ chức đứng ra phát hành chứng chỉ ký các khóa công khai của các cá nhân khác.



Nội dung

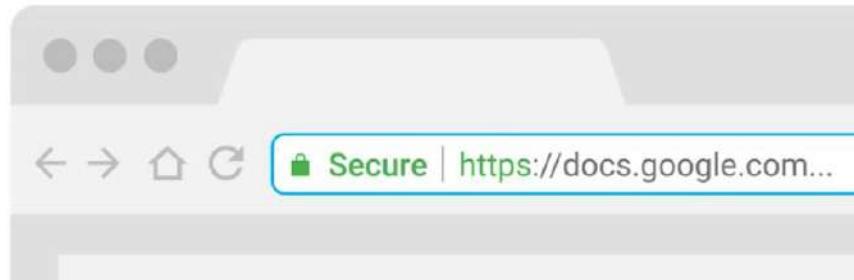
-  Mã hóa và giải mã
-  Mã hóa đối xứng
-  Mã hóa bất đối xứng
-  Băm
-  Hạ tầng khóa công khai
-  **Bảo mật mạng**
-  Phần cứng mã hóa

Giao thức SSL/TLS

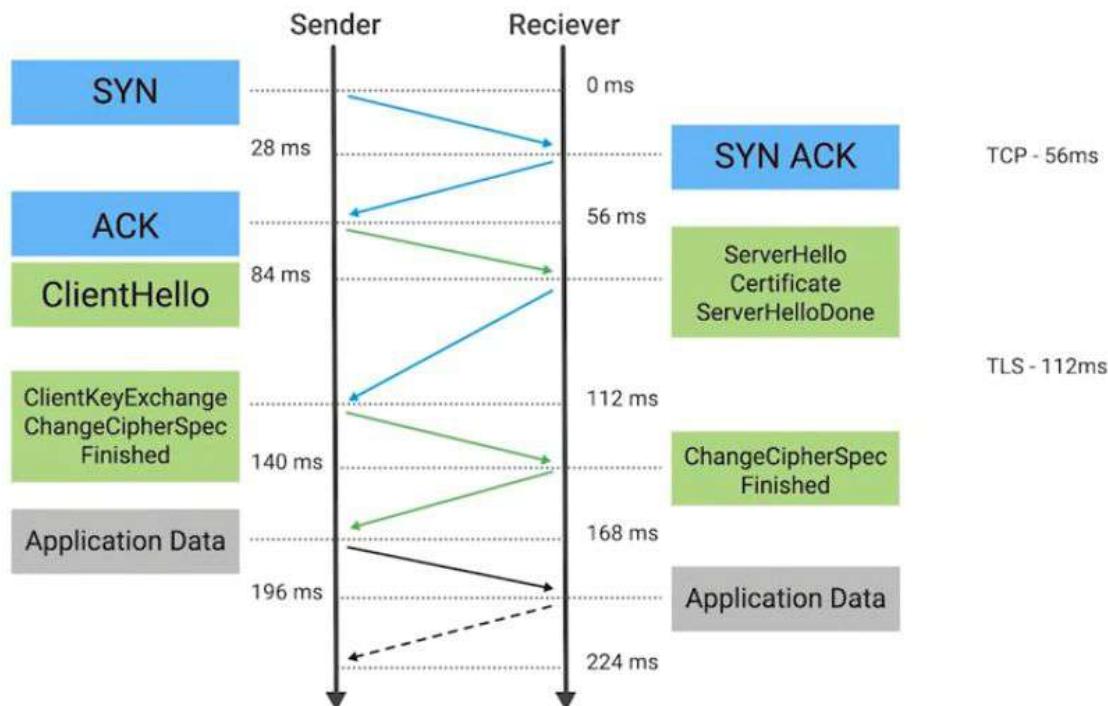
Giao thức SSL/TLS là giao thức giúp **bảo mật** thông tin **liên lạc** giữa các bên trong mạng.

TLS được sử dụng chính hiện tại với ba tính năng:

- Cung cấp đường truyền an toàn.
- Xác thực cả hai bên giao tiếp.
- Bảo đảm tính toàn vẹn của thông tin liên lạc.



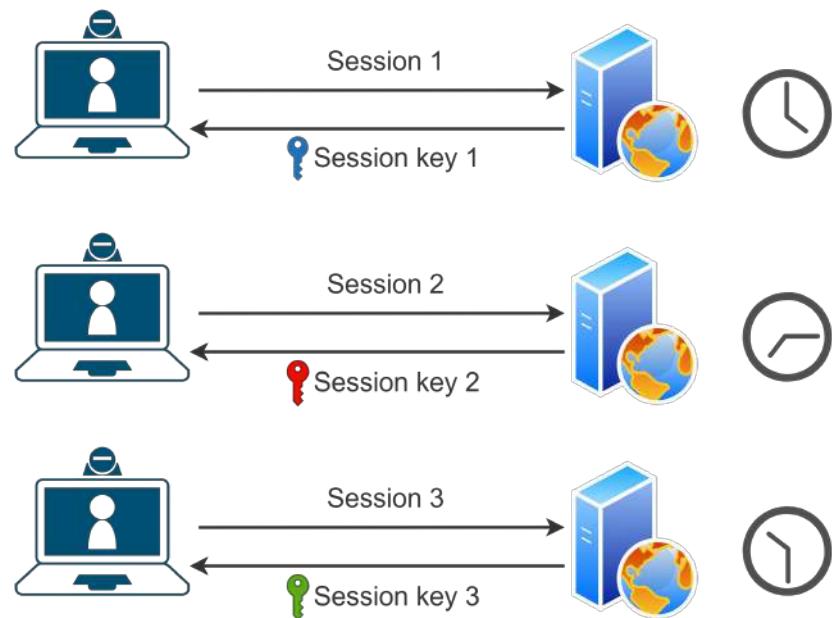
Cơ chế bắt tay TLS



Khóa phiên và bảo mật chuyển tiếp

Khóa phiên (session key) là khóa mã hóa đối xứng được sử dụng để mã hóa chỉ một phiên giao tiếp.

Bảo mật chuyển tiếp (forward secrecy) là thuộc tính của hệ thống mật mã để đảm bảo khóa phiên vẫn an toàn ngay cả khi khóa bí mật bị đánh cắp.



SSH

SSH (secure shell) là một **giao thức mạng bảo mật** sử dụng mã hóa để cho phép **truy cập vào dịch vụ mạng** trên môi trường mạng không an toàn.

- SSH sử dụng **mã hóa khóa công khai** để xác thực máy từ xa.



PGP

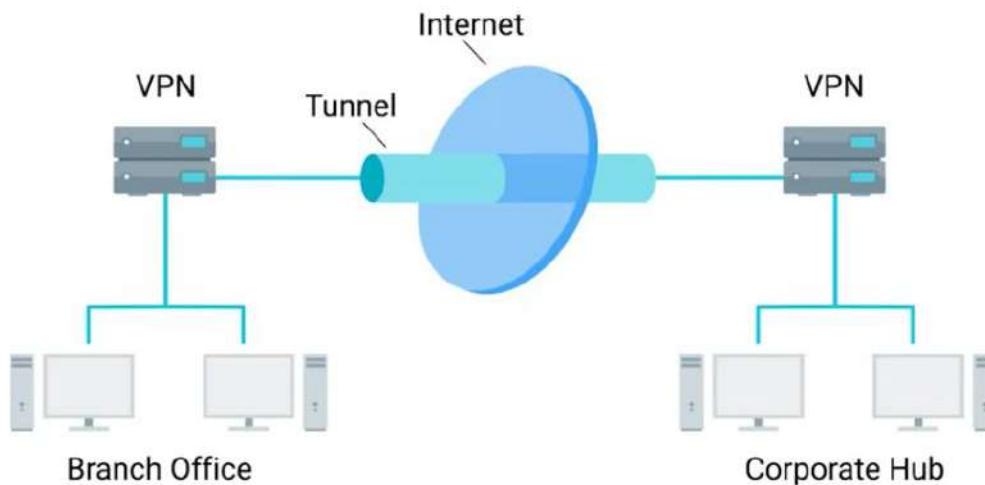
PGP (Pretty Good Privacy) là một ứng dụng mã hóa cho phép xác thực dữ liệu cùng với quyền riêng tư từ các bên thứ ba dựa trên mã hóa bất đối xứng.

- PGP cũng được dùng để mã hóa ổ cứng, tập tin hay thư mục.
- PGP sử dụng khóa không dưới 128 bit và được xem là rất an toàn.



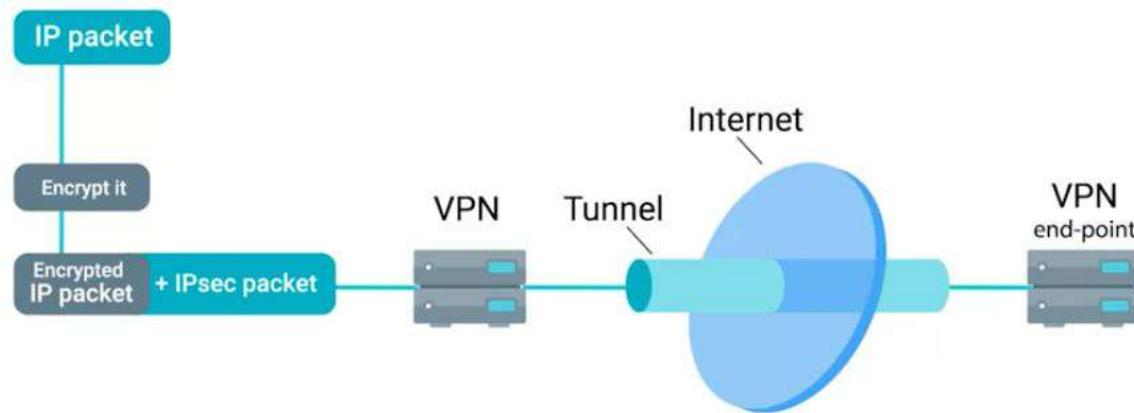
VPN

Mạng riêng ảo (VPN) là cơ chế cho phép kết nối từ xa một máy chủ hoặc mạng nội bộ thông qua một đường hầm được mã hóa.



IPsec

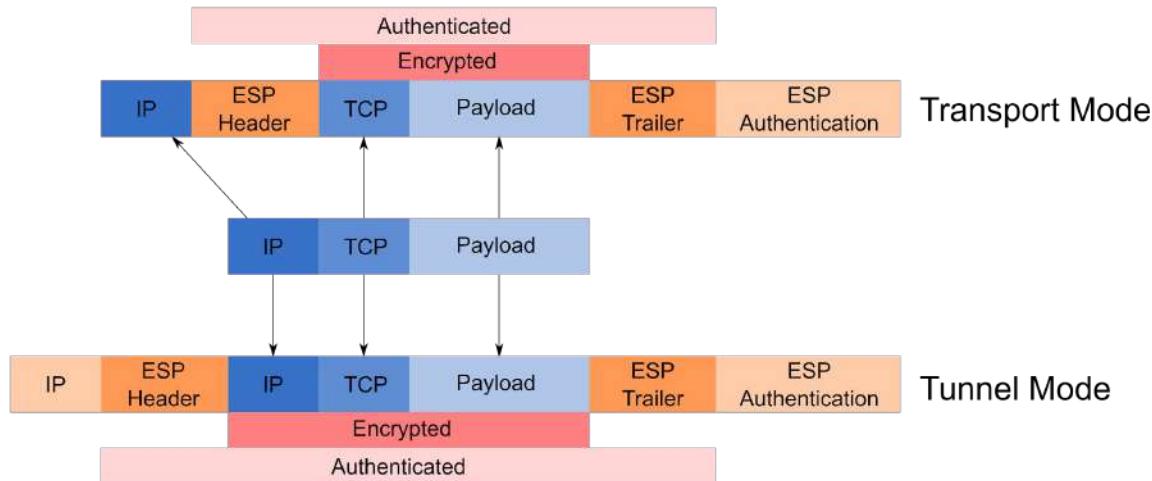
IPsec (Internet Protocol Security) là một giao thức VPN mã hóa gói IP và đóng gói nó bên trong một gói IPsec.



IPsec

IPsec có 2 chế độ hoạt động:

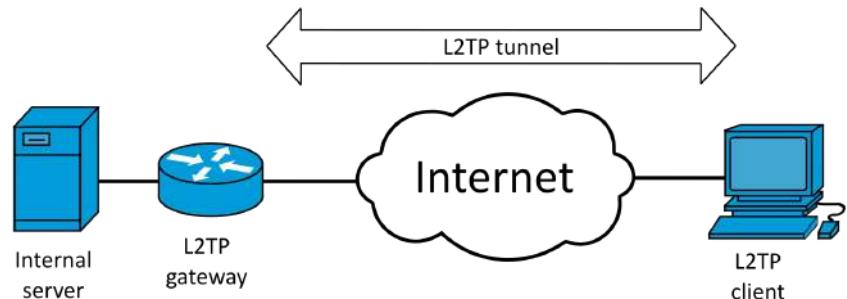
- Chế độ vận chuyển (transport mode): chỉ có dữ liệu của gói IP được mã hóa, IP header thì không.
- Chế độ đường hầm (tunnel mode): tất cả đều được mã hóa và đóng gói trong gói IP mới.



L2TP

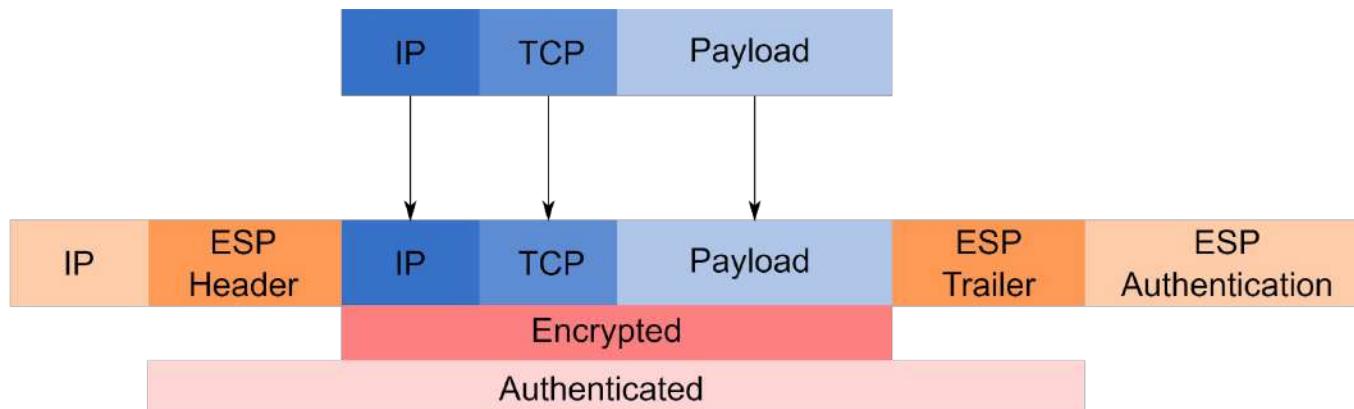
L2TP (Layer 2 Tunneling Protocol) là một giao thức đường hầm cho phép đóng gói các giao thức khác hoặc các lưu thông mà không được hỗ trợ bởi mạng hiện tại.

- L2TP kết hợp với IPSec được gọi là L2TP/IPSec để đảm bảo tính bảo mật cho L2TP.



ESP

ESP (Encapsulating Security Payload) là một giao thức trong bộ giao thức IPsec để đóng gói gói IP, cung cấp tính bảo mật, toàn vẹn và xác thực cho các gói.

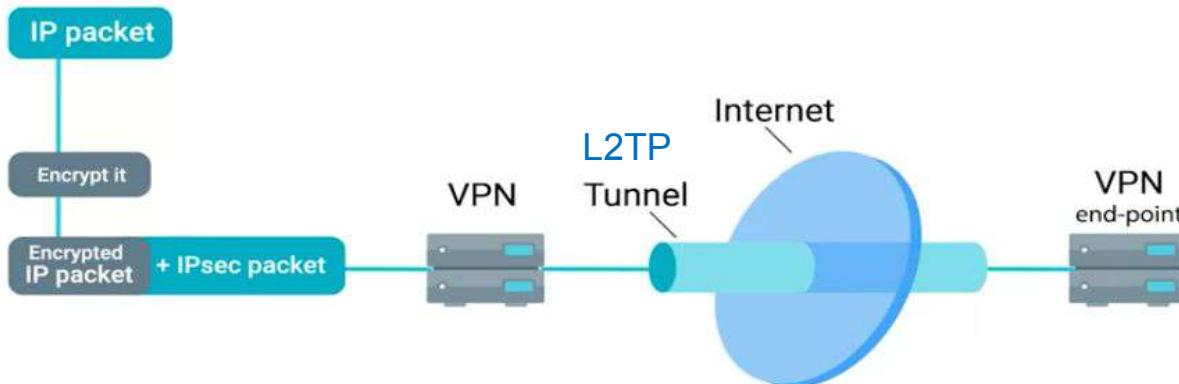


Nguồn: Wikimedia

Đường hầm và kênh bảo mật

Đường hầm (tunnel) được cung cấp bởi L2TP, cho phép truyền các gói tin chưa sửa đổi từ mạng này sang mạng khác.

Kênh bảo mật (secure channel) được cung cấp bởi IPsec để đảm bảo tính bảo mật, toàn vẹn và xác thực dữ liệu được chuyển qua.



OpenVPN

OpenVPN là một VPN sử dụng thư viện OpenSSL để xử lý việc trao đổi khóa và mã hóa dữ liệu cùng với các kênh điều khiển.

- Phương thức xác thực gồm 2 loại: xác thực dựa trên chứng chỉ và xác thực dựa trên tên người dùng-mật khẩu.
- Có thể hoạt động trên TCP hoặc UDP ở cổng 1194.
- Dựa trên đường hầm IP lớp 3 hoặc Ethernet TAP lớp 2.
- Hỗ trợ mã hóa lên đến 256-bit.
- Chạy trong không gian người dùng (user space).



Nội dung



Mã hóa và giải mã



Mã hóa đối xứng



Mã hóa bất đối xứng



Băm



Hạ tầng khóa công khai



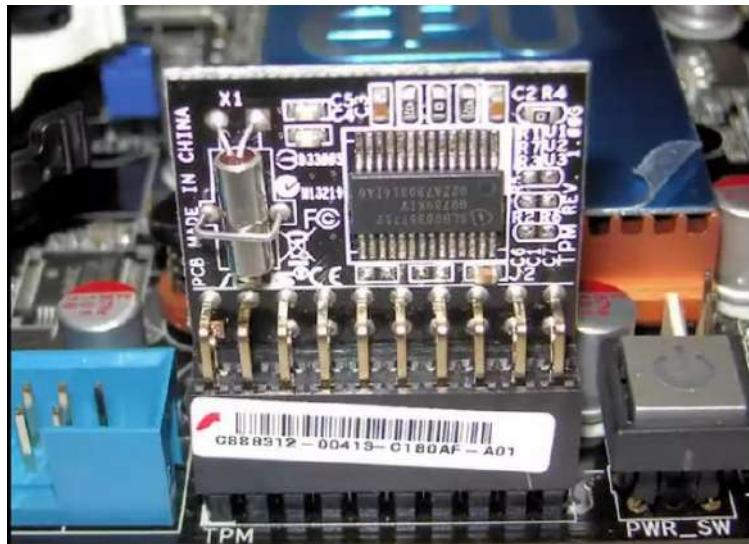
Bảo mật mạng



Phần cứng mã hóa

TPM

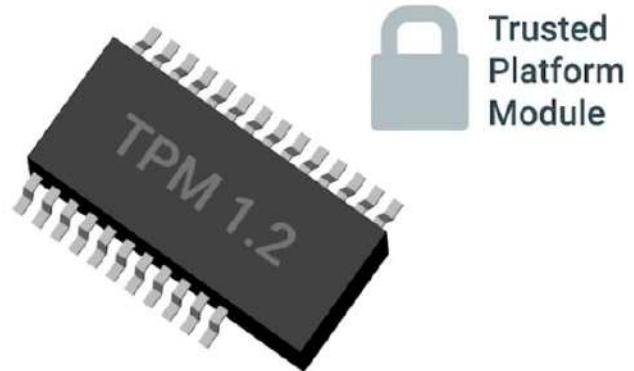
TPM (trusted platform module) là một thiết bị phần cứng thường được tích hợp vào phần cứng máy tính để xử lý các tác vụ liên quan đến mật mã.



Tính năng của TPM

TPM cung cấp các tính năng như:

- Tạo khóa bảo mật (secure generation of keys).
- Phát sinh số ngẫu nhiên (random number generation).
- Chứng thực từ xa (remote attestation).
- Ràng buộc và niêm phong dữ liệu (data binding and sealing).



Triển khai TPM

TPM có thể được triển khai theo nhiều cách:

- Chip phần cứng rời.
- Tích hợp vào một chip khác.
- Triển khai trong phần mềm firmware.
- Ảo hóa bên dưới một phần mềm giám sát máy ảo.



Tấn công TPM

Một số cách thức tấn công TPM:

- Nhà sản xuất có thể lưu trữ các khóa TPM và thực hiện các bản sao TPM về sau.
- Xem mạch TPM bằng kính hiển vi điện tử và thiết bị có độ chính xác ở mức micrômét.



TEE

TEE (trusted execution environment) cung cấp môi trường thực thi cách ly toàn diện chạy cùng hệ điều hành.

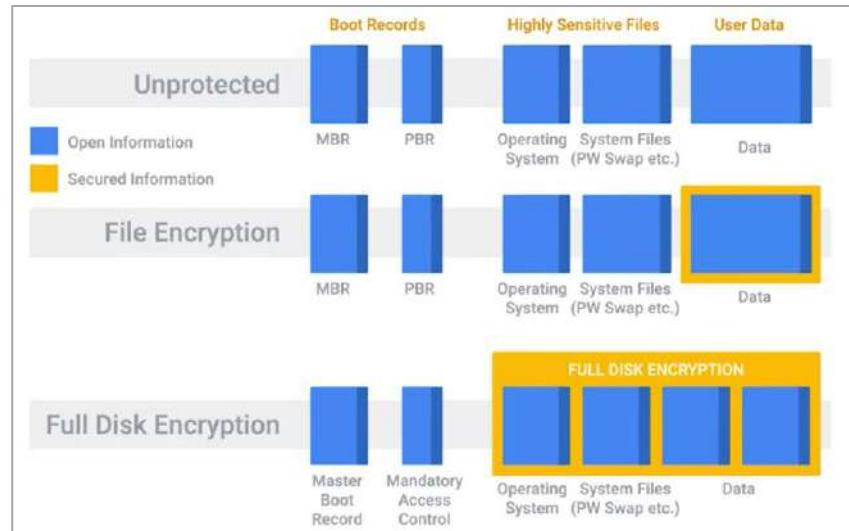
- Cách ly các ứng dụng khỏi hệ điều hành
- Cách ly các tiến trình bảo mật với các tiến trình khác.



Mã hóa toàn đĩa

Mã hóa toàn đĩa (full disk encryption, FDE) là phương pháp mã hóa toàn bộ ổ đĩa trong hệ thống.

- Một phân vùng nhỏ gồm **nhân**, **bootloader**, **initrd** sẽ không được mã hóa để phục vụ quá trình khởi động.



Lựa chọn số ngẫu nhiên

Số ngẫu nhiên đóng vai trò quan trọng trong các thuật toán mã hóa.

- Nếu số không thực sự ngẫu nhiên, có thể tồn tại mẫu có thể bị phát hiện.
- Các hệ điều hành duy trì một hồ entropy để giúp phát sinh số ngẫu nhiên hạt giống.
- Các trình tạo số ngẫu nhiên chuyên dụng và số giả ngẫu nhiên được tích hợp để đảm bảo các số thực sự ngẫu nhiên được chọn khi tạo khóa.





3 Bảo Mật AAA



Nội dung



Giới thiệu bảo mật AAA



Xác thực



Ủy quyền



Kế toán

AAA

AAA là một nền tảng được sử dụng để kiểm soát và theo dõi các truy xuất bên trong một máy tính.

AAA bao gồm:

- Xác thực (Authentication)
- Ủy quyền (Authorization)
- Kế toán (Accounting)

Authentication



A

Authorization



A

Accounting



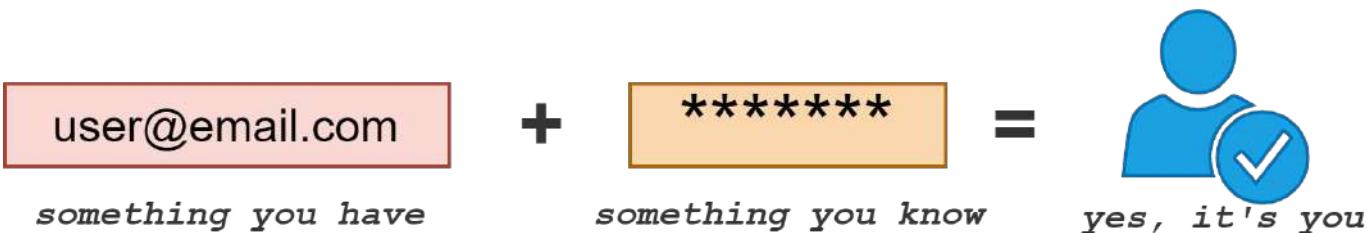
A



Xác thực

Xác thực (authentication) là hành động chứng minh một khẳng định nào đó, ví dụ như chứng minh danh tính của người dùng trong máy tính.

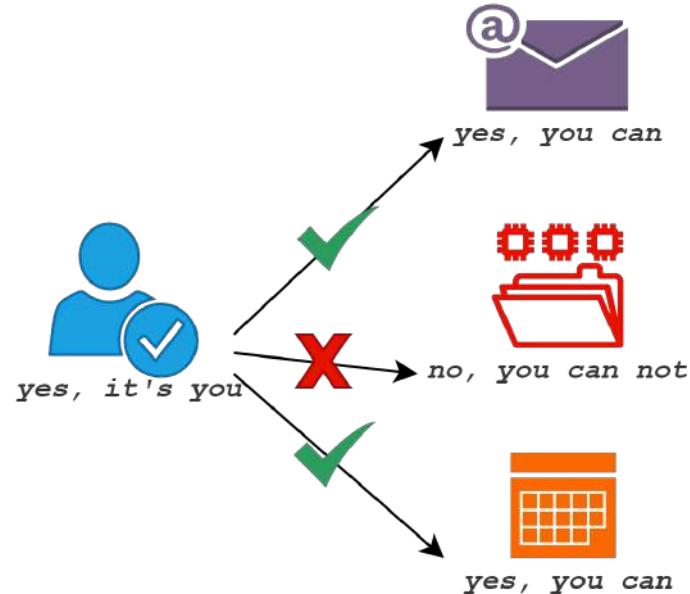
- **Định danh** (identification) là hành động chỉ ra danh tính của một người hoặc một vật.
- Ví dụ: địa chỉ email là định danh, còn quá trình chứng minh email đó là của mình được gọi là xác thực.
- Thường viết tắt là **authn**.



Ủy quyền

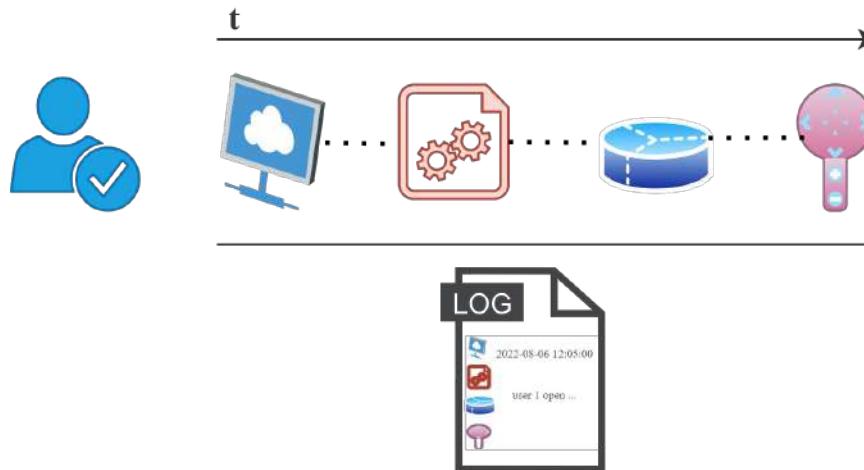
Ủy quyền (authorization) là chức năng chỉ định các quyền/đặc quyền truy cập vào tài nguyên trong hệ thống máy tính.

- Thường viết tắt là authz.



Kế toán

Kế toán (accounting) là quá trình ghi lại các tài nguyên và dịch vụ người dùng đã truy xuất cũng như các thao tác của họ trên tài nguyên này.



Nội dung



Giới thiệu bảo mật AAA



Xác thực

- Mật khẩu mạnh
- Xác thực đa yếu tố
- Xác thực chứng chỉ số
- LDAP, RADIUS, Kerberos, TACACS+
- Đăng nhập một lần



Ủy quyền



Kế toán

Mật khẩu mạnh

Một mật khẩu mạnh cần đảm bảo các yếu tố sau:

- Đảm bảo độ dài tối thiểu nhất định (ví dụ 8 ký tự)
- Sử dụng các ký tự một cách phức tạp
- Không dùng các từ trong từ điển
- Không được viết ra dưới dạng văn bản thô
- Không dùng lại cùng mật khẩu ở nhiều nơi
- Chính sách thay đổi mật khẩu định kỳ (nhưng chu kỳ không nên quá ngắn)

HelloWorld2022



H311oW0rlD2k22

Xác thực đa yếu tố

Xác thực đa yếu tố (multifactor authentication) là hệ thống mà người dùng được xác thực bằng nhiều phần thông tin hay đối tượng.

Bao gồm 3 nhóm yếu tố chính:

- Cái gì bạn biết (something you know)
 - Mật khẩu, mã PIN, ...
- Cái gì bạn có (something you have)
 - Thẻ ATM, điện thoại, ...
- Cái gì bạn là (something you are)
 - Vân tay, mống mắt, ...



Mã Token

Mã token là một dạng mã bổ sung được tạo bởi các thiết bị vật lý hay thiết bị số nhằm cung cấp thêm yếu tố để xác thực người dùng.

Một số dạng của thiết bị token vật lý:

- USB tích hợp khóa token
- Thẻ RFID
- Chìa khóa thông thường
- RSA SecurID
- V.v...

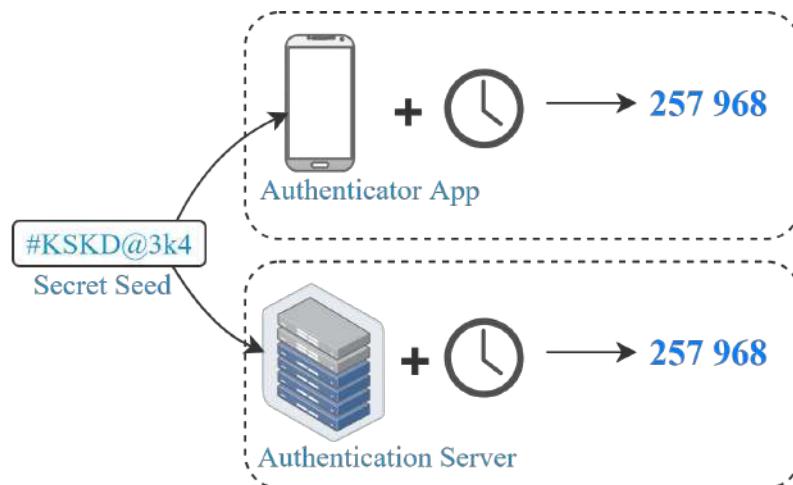


Nguồn: Wikimedia

OTP

Mã OTP (one-time password) là một dạng mã token được sử dụng một lần và tồn tại trong thời gian ngắn.

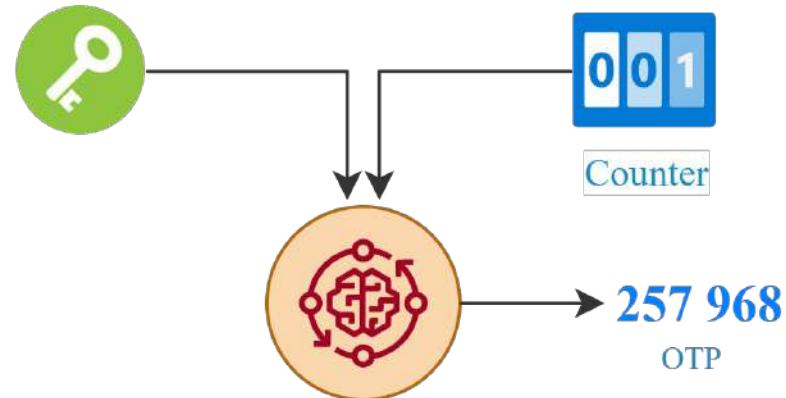
- Mã token này dựa trên thời gian (time-based token) nên nó cũng được gọi là TOTP.
- Cách thức hoạt động:
 - Khởi tạo một giá trị hạt giống bí mật được đăng ký với máy chủ xác thực.
 - Phát sinh OTP dựa trên hạt giống và thời gian hiện tại.
 - Thời gian được đồng bộ với máy chủ bằng giao thức thời gian mạng (network time protocol, NTP).



Token dựa trên bộ đếm

Token dựa trên bộ đếm (counter-based token) sử dụng giá trị hạt giống bí mật và giá trị bộ đếm bí mật để tạo mã token.

- Bộ đếm bí mật được tăng lên mỗi khi mã token được xác thực thành công.

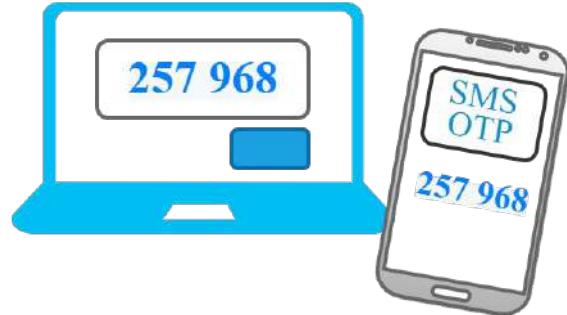


OTP qua tin nhắn SMS

Một số mã OTP được gửi qua tin nhắn SMS mà không cần phát sinh trên thiết bị người dùng.

Điểm yếu của OTP qua SMS:

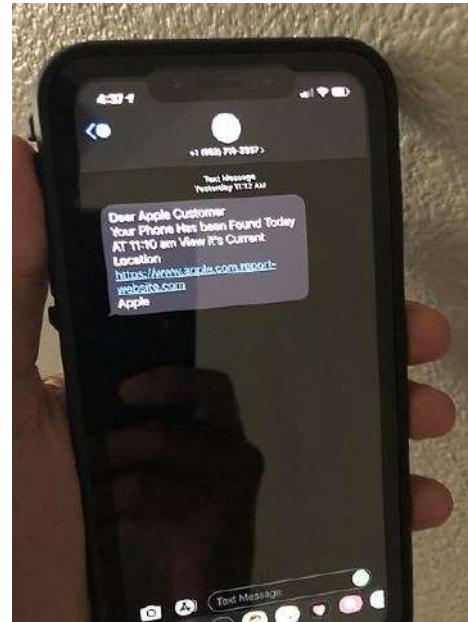
- Phụ thuộc vào quy trình bảo mật của nhà cung cấp dịch vụ di động.
- Tin nhắn SMS thường không được mã hóa.
- Dễ bị mạo danh/mua chuộc để chuyển hướng cuộc gọi đến điện thoại của kẻ tấn công.



Tấn công lừa đảo lấy OTP

Các mã OTP cũng dễ bị tấn công theo kiểu phishing.

- Người dùng bị lừa vào trang xác thực giả thông qua email, tin nhắn lừa đảo.
- Người dùng được yêu cầu nhập mật khẩu và mã OTP.



U2F Token

U2F (universal second factor) là một **chìa khóa bảo mật** kết hợp cơ chế thử thách-phản hồi (challenge-response) cùng với **khóa công khai** để triển khai xác thực yếu tố thứ hai.

- **Chìa khóa bảo mật** (security key) là bộ vi xử lý mã hóa nhúng có khả năng lưu trữ các khóa bất đối xứng và chạy mã nhúng.



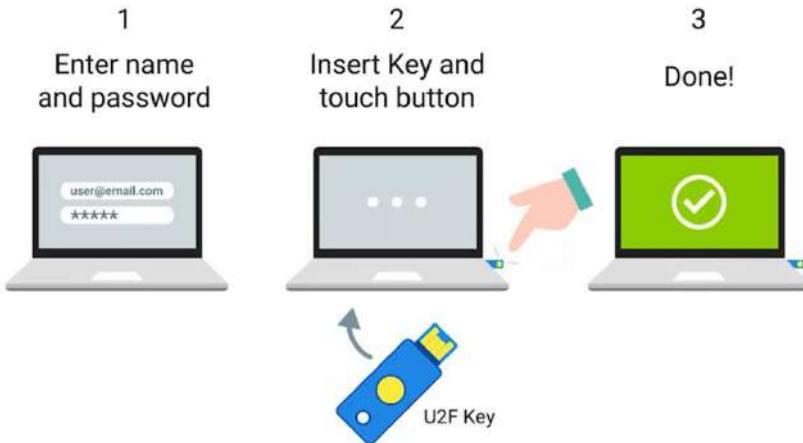
Điểm thuận lợi của U2F:

- Quy trình xác thực được bảo vệ khỏi tấn công lừa đảo
- Chống sao chép và giả mạo
- Thuận tiện hơn so với OTP vì người dùng không cần nhập thủ công

Sử dụng U2F

Các bước để sử dụng U2F:

- Đăng ký từng khóa bảo mật với mỗi trang web/dịch vụ.
- Sau khi đăng nhập bằng tài khoản thông thường, nhấn vào nút khóa bảo mật trên U2F.
 - Bên dưới diễn ra tiến trình thử thách-phản hồi giúp bảo vệ khỏi tấn công phát lại (replay attack)



Xác thực sinh trắc học

Xác thực sinh trắc học (biometric authentication) là quá trình sử dụng các đặc điểm sinh lý độc nhất của một cá nhân để định danh họ.

- Xác thực cá nhân đáng tin cậy hơn so với mật khẩu và mã token.
- Khó để chia sẻ nhưng cũng khó để thay đổi.
- Có thể bị vi phạm quyền riêng tư.



Vân tay



Khuôn mặt



Giọng nói



Mắt

Xác thực sinh trắc học

Xác thực sinh trắc học được thực hiện bằng việc:

- Đăng ký thông tin sinh trắc học.
- Dữ liệu sinh trắc học được mã hóa trước khi lưu trữ.
- Khi xác thực, hệ thống sẽ so khớp sinh trắc học hiện tại với dữ liệu được lưu trữ.



Nội dung



Giới thiệu bảo mật AAA



Xác thực

- Mật khẩu mạnh
- Xác thực đa yếu tố
- **Xác thực chứng chỉ số**
- LDAP, RADIUS, Kerberos, TACACS+
- Đăng nhập một lần



Ủy quyền



Kế toán

Chứng chỉ số

Chứng chỉ số (digital certificate) là một **tập tin** chứng minh **một thực thể sở hữu khóa công khai** nhất định.

- Chứng chỉ số chứa thông tin về **khóa công khai**, **chủ sở hữu**, **chữ ký số**.



Server Certificate

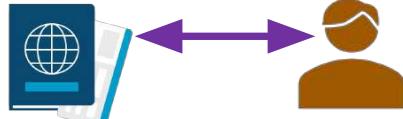
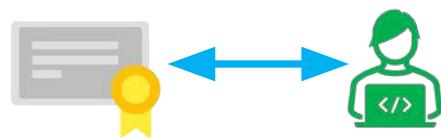
- 👉 INFO ON PUBLIC KEY
- 👉 REGISTERED OWNER
- 👉 DIGITAL SIGNATURE

Client Certificate

Quy trình xác thực chứng chỉ

Bước	Kiểm tra thị thực	Xác thực chứng chỉ
1	Xuất trình giấy tờ tùy thân (hộ chiếu, CCCD) 	Xuất trình chứng chỉ 
2	ID được kiểm tra xem nó có được cấp bởi tổ chức chính phủ tin cậy? 	Chứng chỉ có được CA đáng tin cậy ký không? 
3	Vẫn còn thời gian hiệu lực?	Kiểm tra chứng chỉ có hợp lệ vào thời điểm hiện tại? (Not valid before, not valid after)

Quy trình xác thực chứng chỉ

Bước	Kiểm tra thị thực	Xác thực chứng chỉ
4	ID có nằm trong danh sách bị hạn chế? 	Chứng chỉ có nằm trong danh sách thu hồi (Certificate Revocation List, CRL) không? 
5	Kiểm tra ID có khớp với người xuất trình nó bằng cách kiểm tra khuôn mặt.	Kiểm tra bên trình chứng chỉ có phải là sở hữu hợp lệ bằng cơ chế thử thách-phản hồi.  

Nội dung



Giới thiệu bảo mật AAA



Xác thực

- Mật khẩu mạnh
- Xác thực đa yếu tố
- Xác thực chứng chỉ số
- LDAP, RADIUS, Kerberos, TACACS+
- Đăng nhập một lần



Ủy quyền



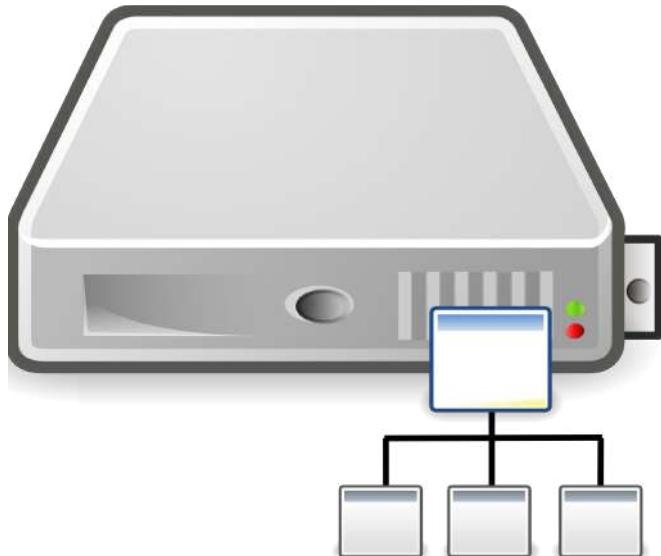
Kế toán

LDAP

LDAP (Lightweight Directory Access Protocol) là một giao thức để truy cập và duy trì các dịch vụ thư mục.

Dịch vụ thư mục (directory service) là một dạng cơ sở dữ liệu chứa và duy trì thông tin về người sử dụng và các tài nguyên trong mạng.

- Ví dụ: khi người dùng truy xuất một ứng dụng, ứng dụng này sẽ tham chiếu đến dịch vụ thư mục để đảm bảo người dùng hợp pháp và có quyền truy cập thư mục.



Cấu trúc của một phần tử trong LDAP

Mỗi phần tử trong LDAP bao gồm
một tập các thuộc tính:

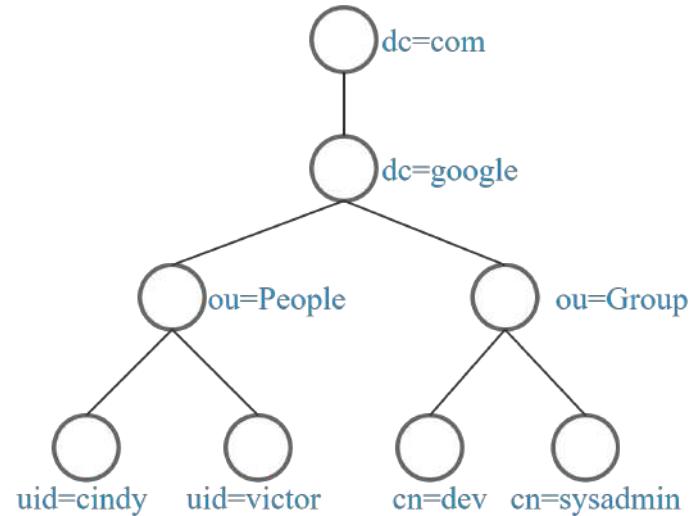
- Họ tên người dùng
- Địa chỉ email
- Số điện thoại
- Shell đăng nhập
- V.v...

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Cấu trúc của một phần tử trong LDAP

Cấu trúc cây trong LDAP được gọi là **cây thông tin dữ liệu** (Data Information Tree).

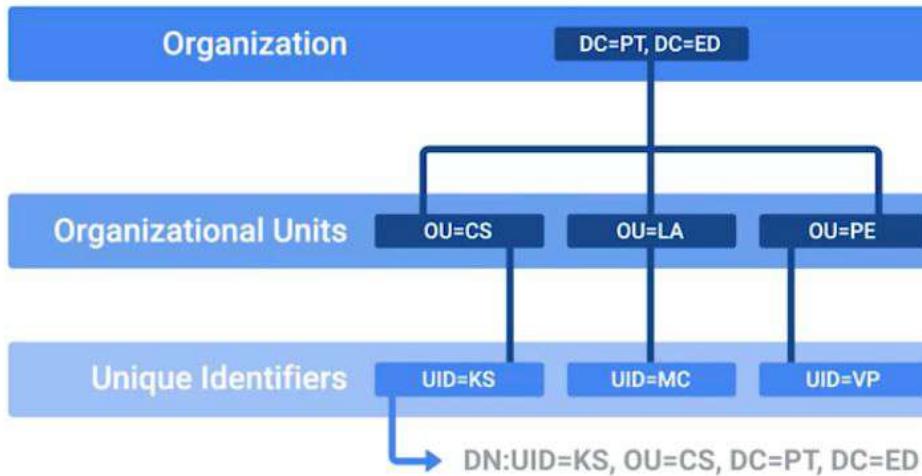
- Thư mục mà một đối tượng thuộc về được gọi là **đơn vị tổ chức** (organizational unit, OU), dùng để nhóm các đối tượng tương tự hay liên quan nhau.
- Thuộc tính đối tượng cha được kế thừa bởi các đối tượng con ở tầng bên dưới của cây.



Định danh cho mỗi phần tử

Mỗi phần tử có một số định danh duy nhất, được gọi là **tên phân biệt** (distinguished name, DN).

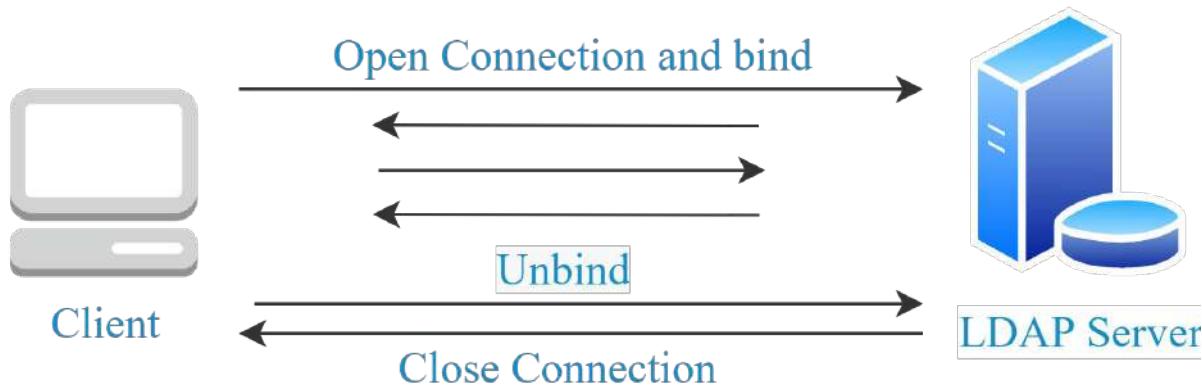
- Tên này là sự **tổng hợp** tên phân biệt tương đối của phần tử và cha của nó.



Kết nối máy khách đến máy chủ LDAP

Máy khách có thể tương tác với máy chủ LDAP thông qua **quá trình liên kết** (bind)

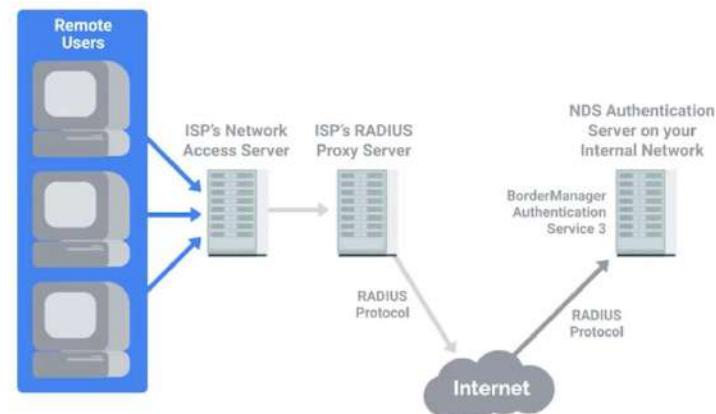
- Đó là **cách máy khách xác thực** với máy chủ.



RADIUS

RADIUS (Remote Authentication Dial-In User Service) là một giao thức cung cấp các dịch vụ AAA cho người dùng trên một mạng.

- Máy khách không trực tiếp tương tác với RADIUS mà xuất trình thông tin xác thực cho NAS (Network Access Server)
- NAS chuyển tiếp thông tin đến máy chủ RADIUS.
- Máy chủ RADIUS xác minh từ một tập tin có sẵn hoặc thông qua các nguồn bên ngoài như cơ sở dữ liệu SQL, LDAP, Kerberos, ...



Kerberos

Kerberos là một giao thức xác thực mạng sử dụng vé để cho phép các thực thể chứng minh danh tính của nhau qua các kênh không an toàn.

- Nó cũng sử dụng mã hóa đối xứng để bảo vệ các thông điệp khỏi các cuộc tấn công nghe trộm và phát lại.



Vé xác thực trong Kerberos

Vé xác thực (authentication ticket) là một loại mã token dùng để xác thực các dịch vụ mà không yêu cầu xác thực tên người dùng và mật khẩu cho từng dịch vụ riêng lẻ.

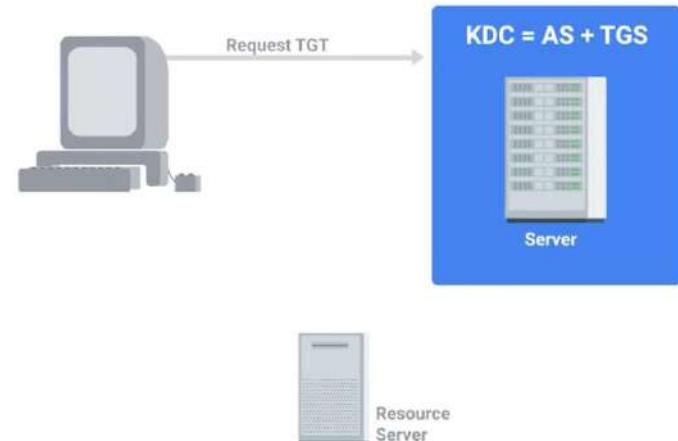
- Vé hết hạn sau thời gian nhất định nhưng nó cũng có thể gia hạn một cách tự động.



Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

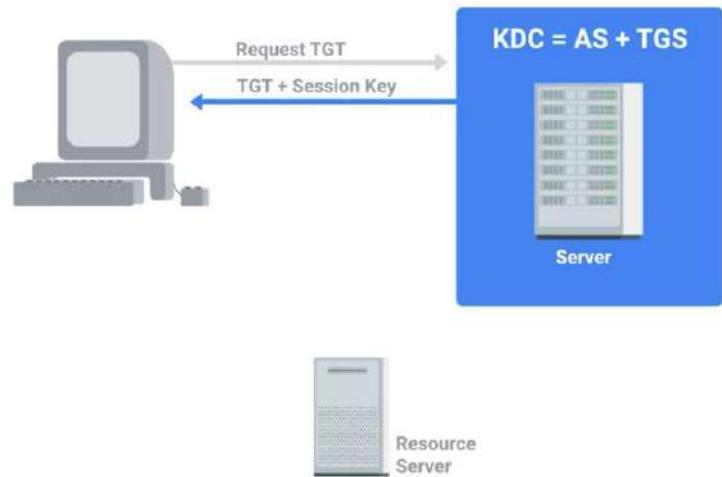
1. Người dùng nhập tên và mật khẩu của họ.
2. Kerberos lấy mật khẩu để tạo khóa mã hóa đối xứng.
3. Gửi một tin nhắn đến Kerberos AS (Authentication Server) với thông tin ID người dùng.
4. Mật khẩu sẽ không được truyền đi.
5. AS kiểm tra tài khoản hợp lệ trong cơ sở dữ liệu.
6. AS tạo khóa bí mật.



Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

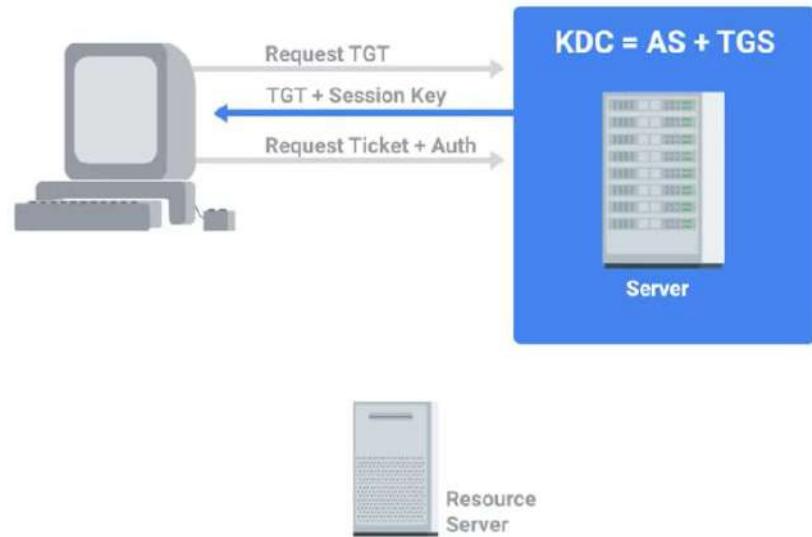
7. AS sử dụng khóa bí mật để mã hóa và gửi thông điệp có chứa khóa phiên TGS máy khách (ticket granting service, TGS).
8. AS cũng gửi một thông điệp thứ 2 với phiếu cấp vé (ticket granting ticket, TGT) được mã hóa bằng khóa bí mật TGS.
9. TGT có thông tin như ID máy khách, thời gian hiệu lực của vé và khóa phiên TGS máy khách.
10. Thông điệp đầu được giải mã bằng khóa bí mật có nguồn gốc từ mật khẩu người dùng.
11. Nó giải mã thông điệp thứ hai chứa phiếu cấp vé.



Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

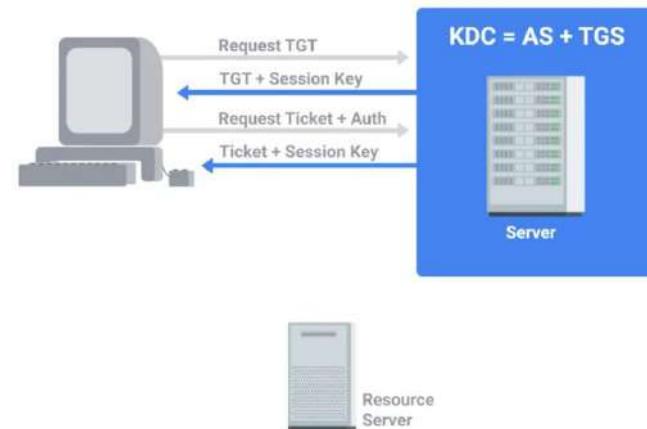
12. Máy khách sử dụng phiếu cấp vé để gửi yêu cầu quyền truy cập vào các dịch vụ bên trong Kerberos.
13. Máy khách cũng gửi một thông điệp có ID máy khách và thời gian được mã hóa bằng khóa phiên TGS máy khách.



Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

15. Dịch vụ cấp vé giải mã phiếu cấp vé bằng khóa bí mật TGS.
16. Nó sử dụng khóa để giải mã thông điệp xác thực.
17. Nó kiểm tra ID máy khách của hai thông điệp xem có khớp nhau không.
18. Nó gửi lại hai thông điệp cho máy khách.
 - Thông điệp 1 chứa vé máy khách đến máy chủ (ID máy khách, thời hạn, khóa phiên máy khách-máy chủ) được mã hóa bằng khóa bí mật của dịch vụ.
 - Thông điệp 2 chứa chính khóa phiên máy khách-máy chủ) được mã hóa bằng khóa phiên TGS máy khách.

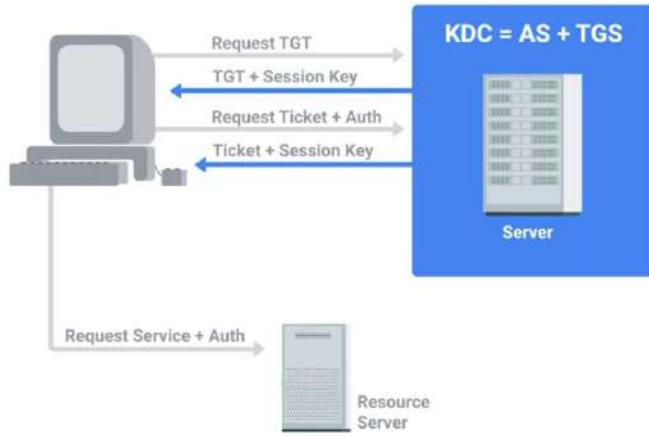


Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

19. Máy khách gửi hai thông điệp đến SS (Service server).

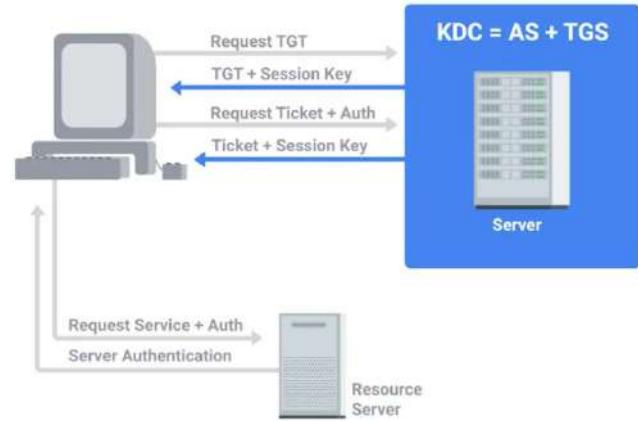
- Thông điệp 1 là vé máy khách đến máy chủ đã được mã hóa
- Thông điệp 2 là trình xác thực mới với ID máy khách và thời gian được mã hóa bằng khóa phiên máy khách-máy chủ.



Cách hoạt động của Kerberos

Kerberos hoạt động như sau:

20. SS giải mã thông điệp 1 sử dụng khóa bí mật của nó để có khóa phiên máy khách-máy chủ.
21. Khóa phiên được sử dụng để giải mã thông điệp 2.
22. Nó so sánh ID ứng dụng khách với ID có trong vé máy khách-đến-máy chủ.
23. SS gửi thông điệp chứa nhãn thời gian từ bộ xác thực cung cấp máy khách được mã hóa bằng khóa phiên máy khách-máy chủ.
24. Máy khách giải mã thông điệp và kiểm tra thời gian có xác thực đúng máy chủ không.



Vấn đề của giao thức Kerberos

Kerberos gặp một số vấn đề như:

- Nếu dịch vụ Kerberos ngừng hoạt động, người dùng mới sẽ không thể xác thực và đăng nhập.
- Nếu máy chủ Kerberos bị chiếm, kẻ tấn công có thể mạo danh bất kỳ người dùng nào.
- Kerberos yêu cầu thời gian nghiêm ngặt nên máy khách và máy chủ cần đồng bộ chặt chẽ.
- Người dùng không thể xác thực bằng Kerberos từ các ứng dụng khách không xác định do cần phải thiết lập sự tin cậy trước.



TACACS+

TACACS+ là một giao thức AAA do Cisco phát triển để quản trị thiết bị, xác thực, ủy quyền và kế toán.

- TACACS+ chủ yếu được sử dụng cho việc xác thực các thiết bị hạ tầng mạng.



Nội dung



Giới thiệu bảo mật AAA



Xác thực

- Mật khẩu mạnh
- Xác thực đa yếu tố
- Xác thực chứng chỉ số
- LDAP, RADIUS, Kerberos, TACACS+
- Đăng nhập một lần



Ủy quyền

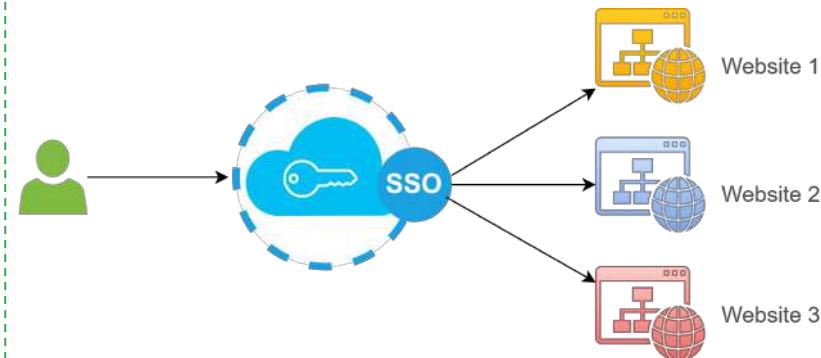


Kế toán

Đăng nhập một lần

Đăng nhập một lần (Single Sign-On, SSO) là công nghệ cho phép người dùng xác thực một lần để được cấp quyền truy cập vào nhiều dịch vụ và ứng dụng khác nhau.

- Người dùng không cần nhiều bộ (username, password) khác nhau trên từng ứng dụng.
- Hoạt động dựa trên xác thực với máy chủ xác thực trung tâm như LDAP.
- Cookie hoặc mã token được trả về để truy cập các ứng dụng.



Hệ thống OpenID

OpenID là chuẩn mở và giao thức xác thực phi tập trung.

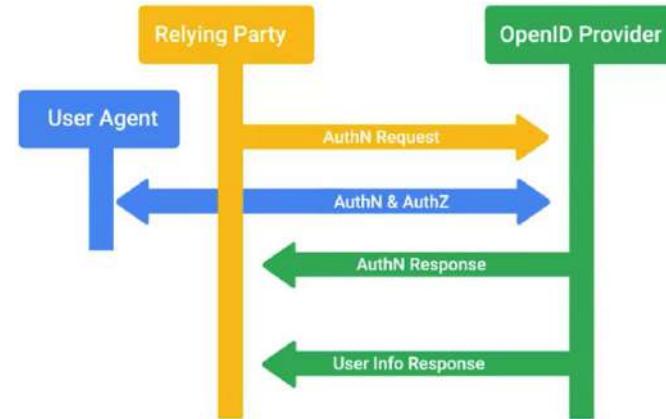
- Các bên sử dụng OpenID được gọi là **bên phụ thuộc** (Relying Party).
- Các bên phụ thuộc **cho phép xác thực người dùng qua bên thứ ba**.
- Các bên phụ thuộc **không cần xây dựng cơ sở hạ tầng xác thực phức tạp**.
- Người dùng không cần tạo tài khoản mới ở bên phụ thuộc mà **chỉ cần có tài khoản của nhà cung cấp định danh**.



Xác thực với OpenID

Để yêu cầu xác thực với OpenID.

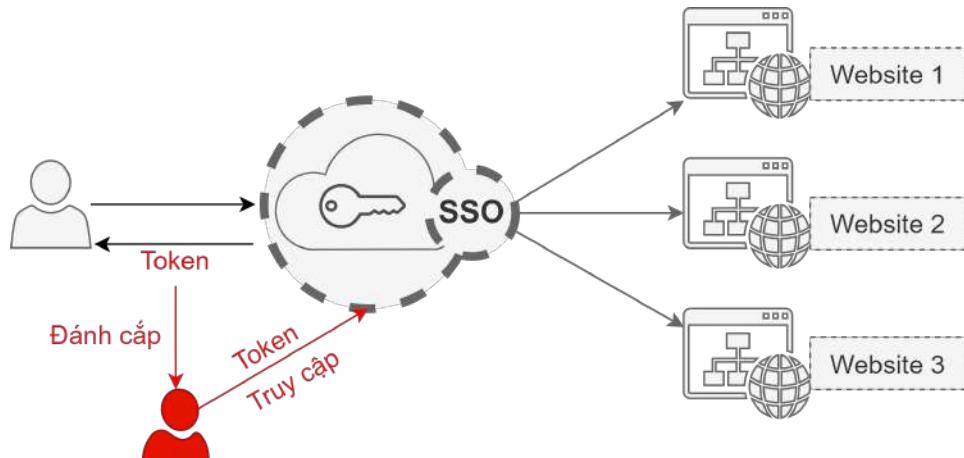
1. Bên phụ thuộc tra cứu nhà cung cấp OpenID và thiết lập bí mật được chia sẻ với nhà cung cấp này.
2. Khóa bí mật được sử dụng để xác thực thông điệp của nhà cung cấp OpenID.
3. Người dùng được yêu cầu xác thực trên một cửa sổ mới dựa trên quy trình của nhà cung cấp định danh.
4. Người dùng kiểm tra và xác nhận tin tưởng bên phụ thuộc.
5. Khi hoàn tất, thông tin đăng nhập được chuyển tiếp đến bên phụ thuộc dưới dạng mã token để cho biết người dùng đã được xác thực.



Tấn công SSO

Nếu bị đánh cắp cookie hay mã token của hình thức đăng nhập một lần, kẻ tấn công có thể:

- Truy cập rộng rãi các ứng dụng ngay cả trong khoảng thời gian ngắn.
- Né tránh được các biện pháp bảo vệ xác thực đa yếu tố.



Nội dung



Giới thiệu bảo mật AAA



Xác thực



Ủy quyền

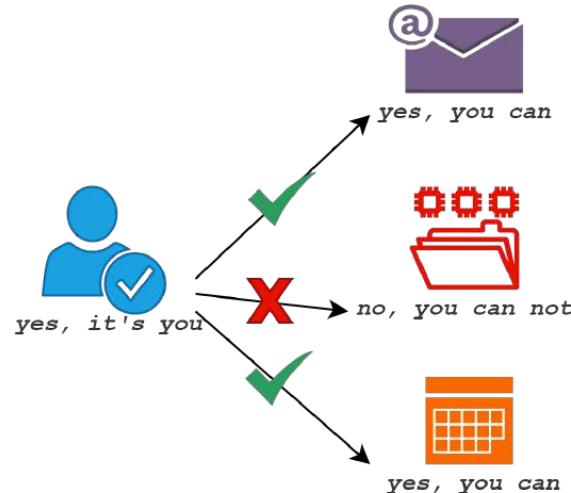


Kế toán

Ủy quyền

Ủy quyền (authorization) mô tả những gì tài khoản người dùng có quyền truy cập hoặc không có quyền truy cập.

- Kerberos kiểm tra quyền truy cập khi xem xét việc cấp vé.



OAuth

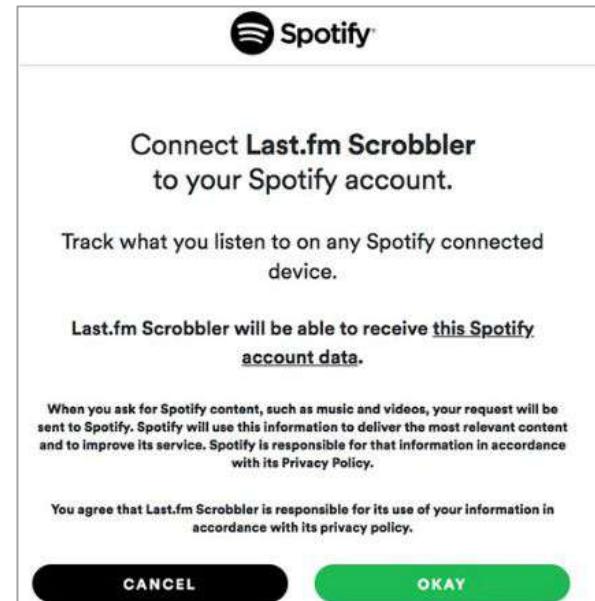
OAuth là một tiêu chuẩn mở cho phép người dùng cấp cho các trang web và ứng dụng bên thứ ba quyền truy cập vào thông tin của họ mà không cần chia sẻ thông tin đăng nhập tài khoản.



Cách hoạt động của OAuth

Cách thức hoạt động của OAuth:

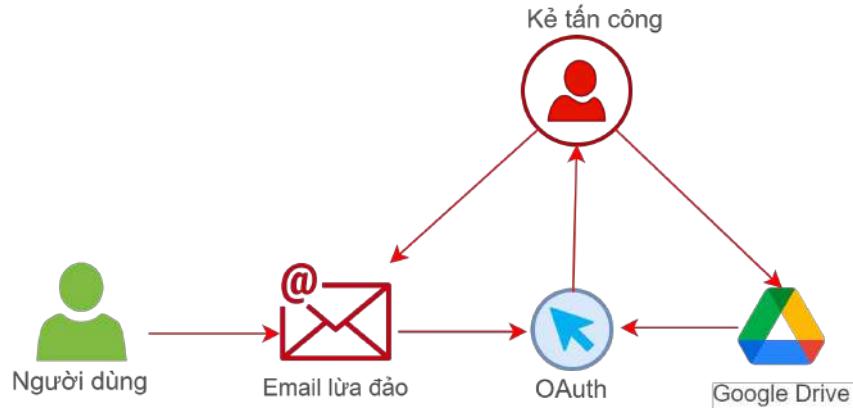
1. Nhắc người dùng xác nhận họ đồng ý cho phép bên thứ ba truy cập vào thông tin nhất định của tài khoản.
2. Sau khi xác nhận, nhà cung cấp định danh sẽ cấp cho bên thứ ba mã token để họ truy cập vào thông tin người dùng.



Tấn công OAuth

Kẻ tấn công có thể thực hiện:

- Gửi email lừa đảo để yêu cầu quyền OAuth hợp pháp.
- Yêu cầu này sẽ hỏi người dùng quyền truy cập vào một thông tin của tài khoản của họ.
- Sau khi được cấp quyền, kẻ tấn công sử dụng mã token ủy quyền Oauth để xâm phạm tài khoản.



OAuth và OpenID

OAuth là một hệ thống ủy quyền và OpenID là một hệ thống xác thực.

- Chúng thường được sử dụng cùng nhau.



Ủy quyền trên TACACS+ và RADIUS

TACACS+ là một hệ thống AAA đầy đủ nên nó cũng xử lý ủy quyền cùng với xác thực.

- TACACS+ cho phép hoặc không cho phép truy cập vào các thiết bị nhất định.

RADIUS cũng có chức năng quản lý cấp quyền truy cập mạng.



Danh sách kiểm soát truy cập

Danh sách kiểm soát truy cập (Access Control List, ACL) là một cách xác định quyền hoặc phân quyền cho các đối tượng.

- Hệ thống tập tin có ACL chứa danh sách các mục chỉ định quyền truy cập của cá nhân/nhóm.
- ACL mạng dùng để kiểm soát lưu lượng đến và đi, hạn chế quyền truy cập từ bên ngoài vào hệ thống hoặc ngăn chặn việc truyền dữ liệu ra bên ngoài.



Nội dung



Giới thiệu bảo mật AAA



Xác thực



Ủy quyền



Kế toán

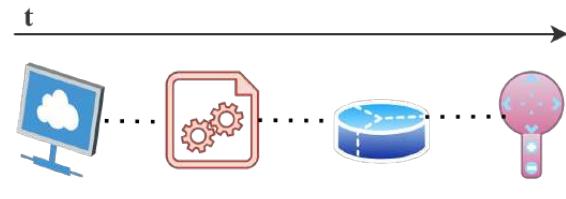
Kế toán

Kế toán (accounting) lưu giữ hồ sơ về những tài nguyên và dịch vụ mà người dùng truy cập hoặc những gì họ đã thao tác.

Mục tiêu:

- Đảm bảo không có gì bất thường.
- Tìm nguyên nhân sự cố.
- Dự báo tài nguyên để nâng cấp.

Thực hiện kiểm toán (auditing, kiểm tra) định kỳ.





4 An Ninh Mạng



Nội dung



Tổng quan gia cố mạng



Gia cố phần cứng mạng



Gia cố phần mềm mạng



Bảo mật mạng không dây

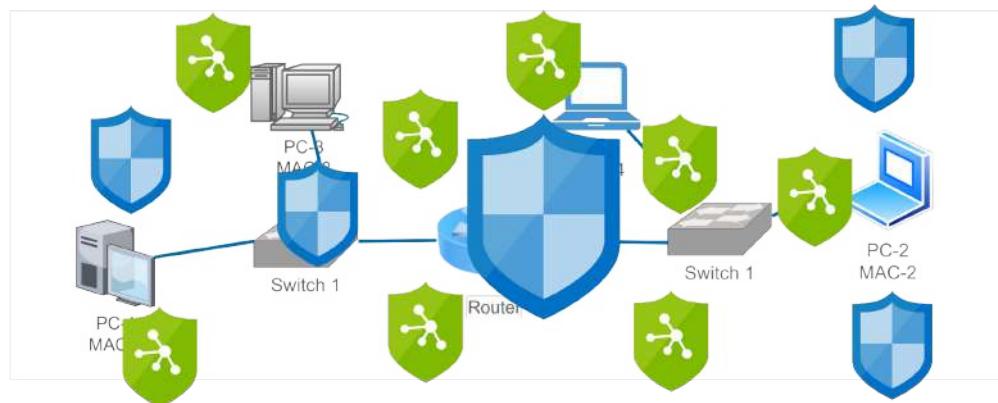


Giám sát mạng

Gia cố mạng

Gia cố mạng (network hardening) là quá trình đảm bảo an toàn cho mạng bằng cách **giảm các lỗ hổng tiềm ẩn** của nó thông qua các **thay đổi cấu hình và thực hiện các bước cụ thể**.

- **Nguyên tắc cơ bản:** vô hiệu hóa các dịch vụ không cần thiết hoặc hạn chế quyền truy cập đến chúng.



Từ chối ngầm

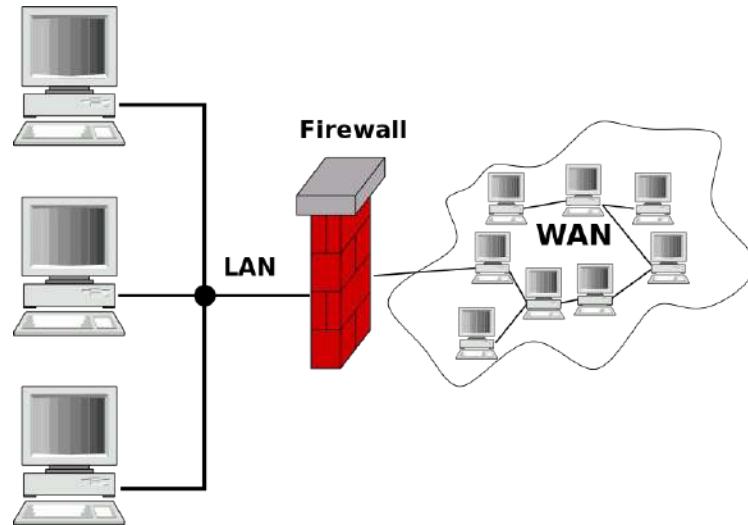
Từ chối ngầm (implicit deny) nghĩa là **bất cứ cái gì không được cho phép một cách tường minh sẽ bị từ chối.**

- Sử dụng ACL (access control list) để cấu hình từ chối ngầm.

Rule	SIP	DIP	Sport	Dport	Proto
1	192.168.*.*	1.2.3.*	*	[2000, 3000]	TCP
2	192.168.*.*	1.2.3.*	*	[0, 1999]	TCP
...

Tường lửa

Tường lửa (firewall) là một hệ thống bảo mật mạng dùng để **theo dõi** và **kiểm soát** các luồng vào ra dựa trên **tập quy tắc** đã được xác định.



Nguồn: wikimedia

Giám sát và phân tích luồng mạng

Giám sát và phân tích luồng truy cập trong mạng là hoạt động quan trọng vì chúng ta có thể:

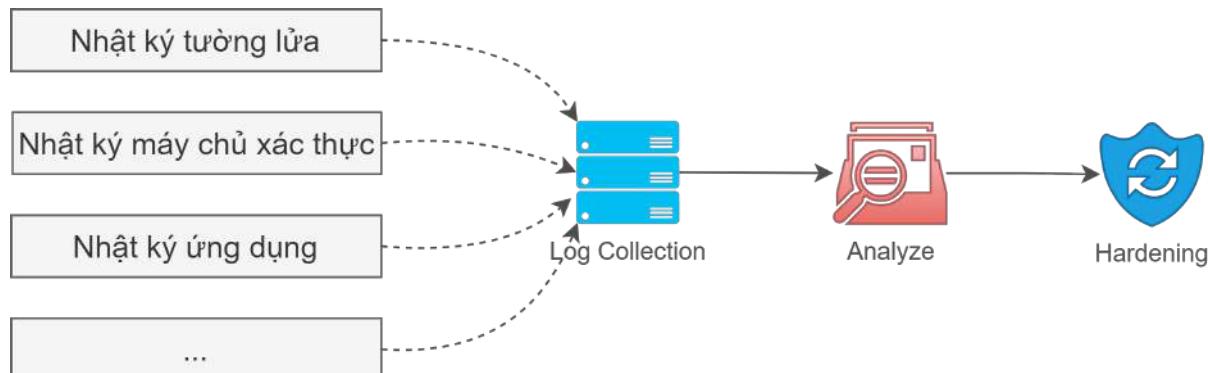
- **Biết được luồng truy cập bình thường trông như thế nào để phát hiện luồng bất thường.**
- **Phát hiện sự cố đang xảy ra.**
- **Gia cố các chỗ bị yếu.**



Phân tích nhật ký

Phân tích nhật ký (analyzing logs) là hoạt động thu thập nhật ký từ các mạng khác nhau và đôi khi là các thiết bị khách trên mạng, sau đó thực hiện phân tích chúng một cách tự động.

- Các nhật ký quan trọng như **nhật ký tường lửa, nhật ký máy chủ xác thực, nhật ký ứng dụng**.
- Ví dụ: các kết nối tới dịch vụ nội bộ từ nguồn không tin cậy, hay các kết nối từ mạng nội bộ đến dải địa chỉ của botnet hay máy chủ điều khiển, v.v...



Hệ thống phân tích nhật ký

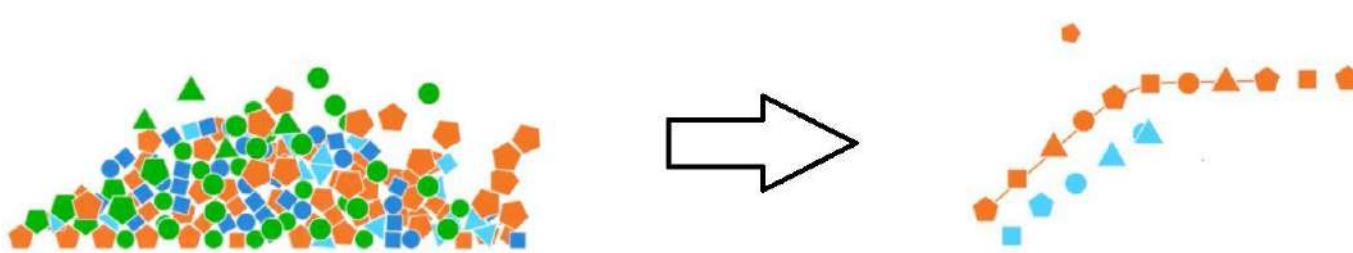
Hệ thống phân tích nhật ký (logs analysis system) cần:

- Thiết lập các quy tắc để khớp với những thông tin nhật ký cần quan tâm.
- Cảnh báo bằng email hoặc SMS khi phát hiện bất thường.
- Thiết lập các chế độ ưu tiên.
- Cho phép tìm kiếm và lọc dữ liệu để phân tích.



Chuẩn hóa dữ liệu

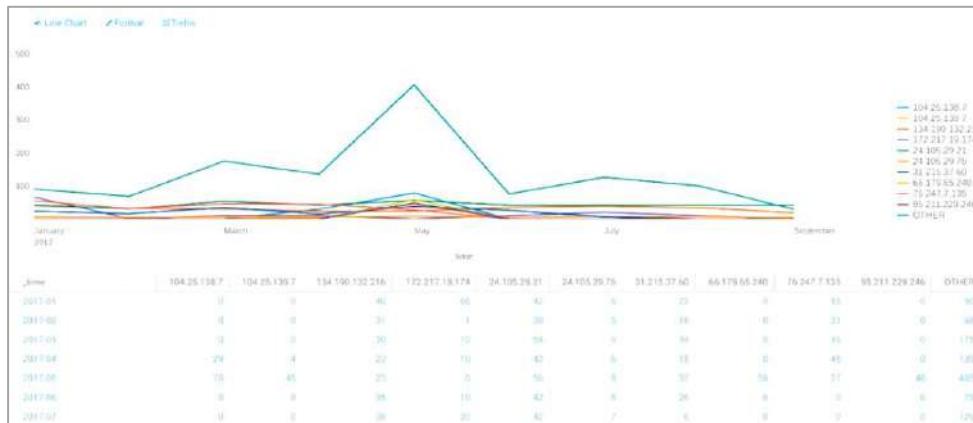
Chuẩn hóa dữ liệu (normalizing log data) là quá trình **chuyển đổi các thành phần nhặt ký thành một định dạng chung** để phân tích dễ dàng hơn.



Nguồn: wikimedia

Phân tích tương quan và post-fail

- Phân tích tương quan (correlation analysis) là quá trình lấy dữ liệu nhật ký từ các hệ thống khác nhau và so khớp các sự kiện giữa các hệ thống.
- Phân tích post-fail (post-fail analysis) là điều tra sự xâm nhập xảy ra như thế nào sau khi phát hiện vi phạm.



Ví dụ hệ thống phân tích nhật ký

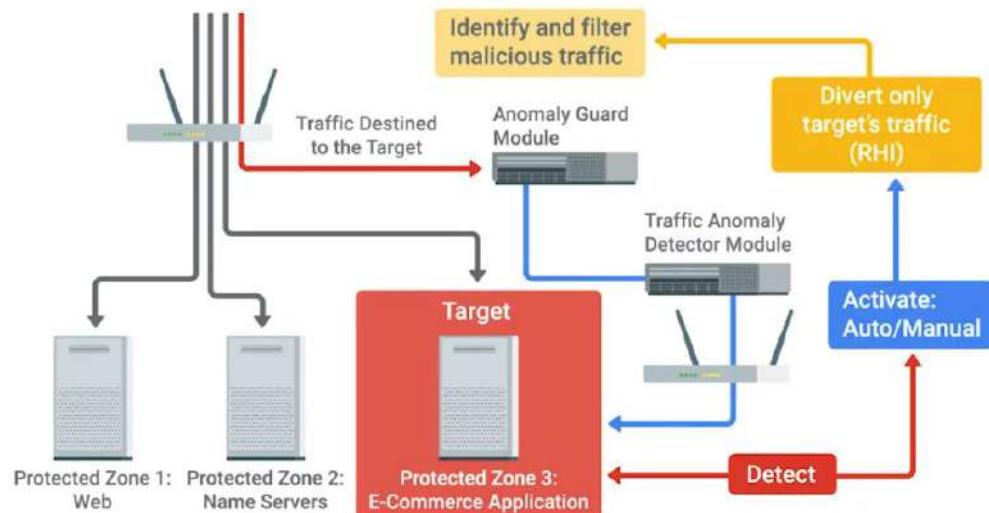
Splunk là một trong những hệ thống phân tích nhật ký phổ biến hỗ trợ:

- Tìm kiếm
- Tổng hợp
- Cảnh báo
- Trực quan hóa



Flood Guard

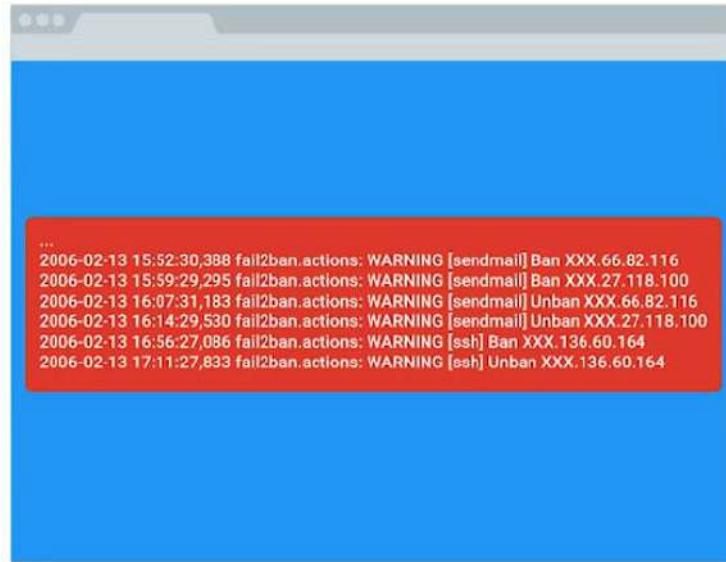
- Flood Guard cung cấp cách thức bảo vệ chống lại tấn công từ chối dịch vụ (DoS) như SYN flood hay UDP flood.
- Nguyên tắc hoạt động:
 - Phát hiện tấn công từ chối dịch vụ.
 - Kích hoạt cảnh báo khi đạt đến ngưỡng được cấu hình.
 - Nếu thiết lập ngưỡng kích hoạt (activation threshold), thì nó sẽ thực hiện một hành động đã định trước như chặn luồng tấn công trong một khoảng thời gian cụ thể.



Công cụ Flood Guard

Fail2ban là một trong những công cụ bảo vệ chống tấn công từ chối dịch vụ:

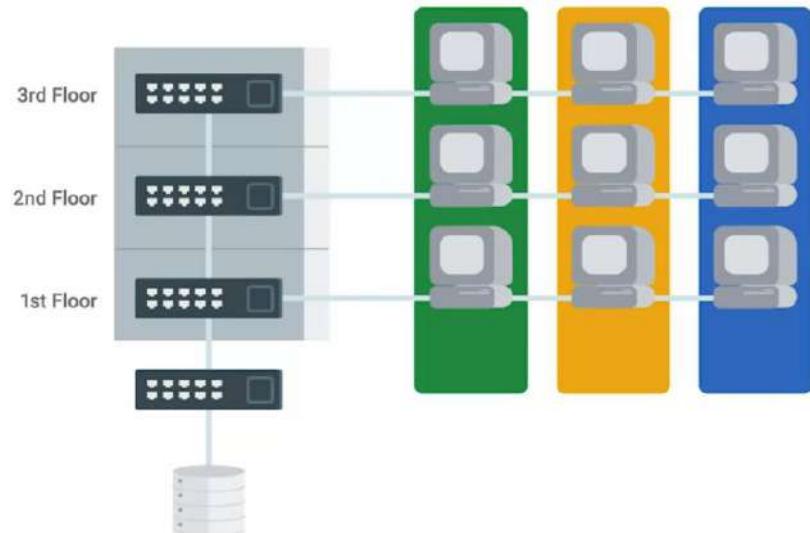
- Theo dõi các dấu hiệu của một cuộc tấn công.
- Chặn địa chỉ bị nghi ngờ tấn công.



```
...
2006-02-13 15:52:30,388 fail2ban.actions: WARNING [sendmail] Ban XXX.66.82.116
2006-02-13 15:59:29,295 fail2ban.actions: WARNING [sendmail] Ban XXX.27.118.100
2006-02-13 16:07:31,183 fail2ban.actions: WARNING [sendmail] Unban XXX.66.82.116
2006-02-13 16:14:29,530 fail2ban.actions: WARNING [sendmail] Unban XXX.27.118.100
2006-02-13 16:56:27,086 fail2ban.actions: WARNING [ssh] Ban XXX.136.60.164
2006-02-13 17:11:27,833 fail2ban.actions: WARNING [ssh] Unban XXX.136.60.164
```

Phân tách mạng

Phân tách mạng (network separation, network segmentation) là **chia mạng thành các mạng con nhỏ** để quản lý linh hoạt hơn và dễ thiết lập cơ chế bảo mật hơn.



Nội dung



Tổng quan gia cố mạng



Gia cố phần cứng mạng



Gia cố phần mềm mạng



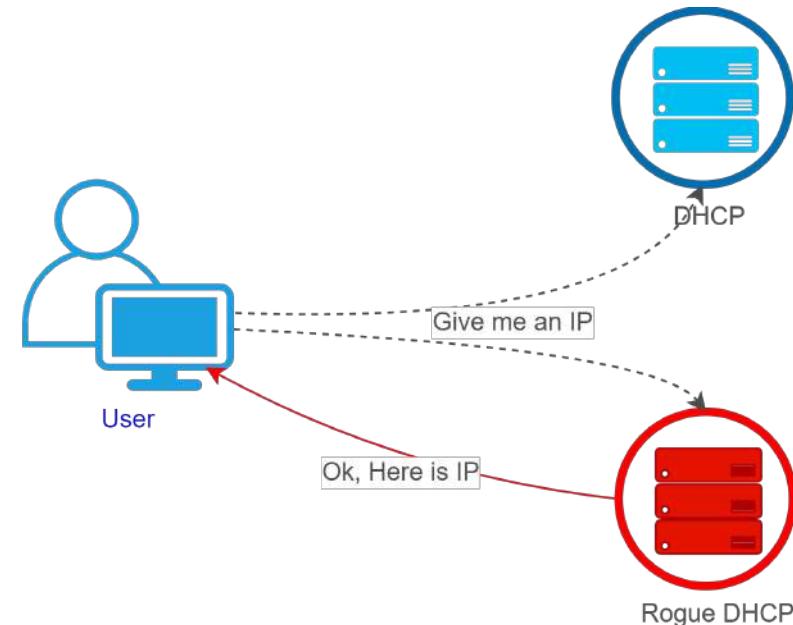
Bảo mật mạng không dây



Giám sát mạng

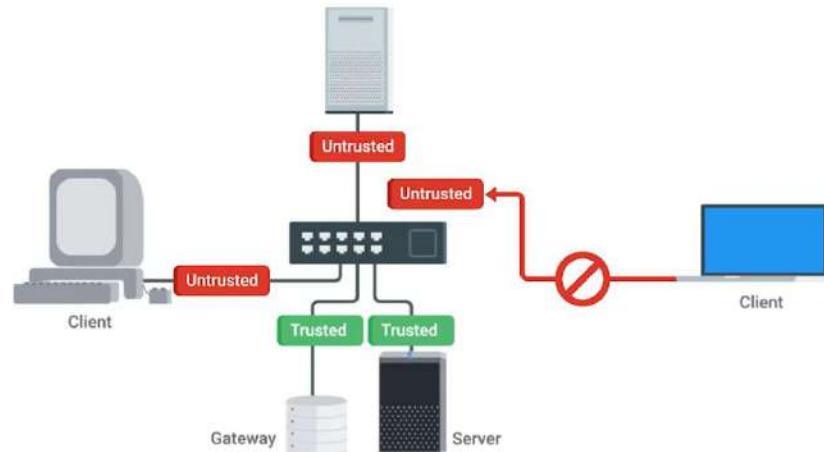
Tấn công giả mạo máy chủ DHCP

Tấn công giả mạo máy chủ DHCP (rogue DHCP server attack) là cách thức kẻ tấn công **tạo một máy chủ DHCP giả** để kiểm soát mạng.



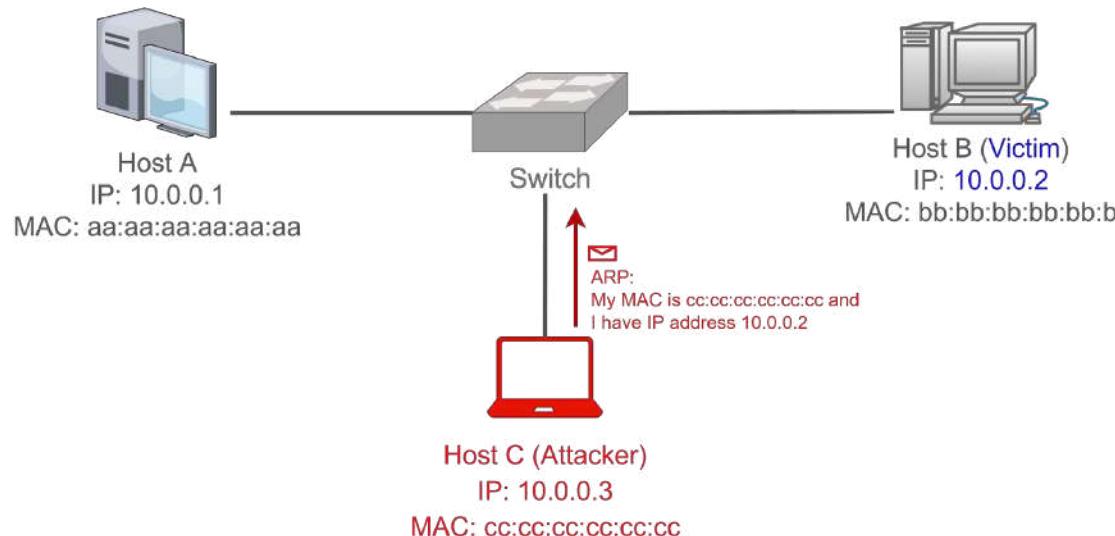
DHCP snooping

- DHCP snooping là **chức năng** trên switch để **chống tấn công giả mạo DHCP**.
 - Giám sát luồng DHCP.
 - Theo dõi việc gán IP.
 - Xây dựng bản đồ địa chỉ IP.
 - **Hỗ trợ chống tấn công giả mạo IP hay đầu độc ARP.**
- DHCP snooping cho phép:
 - **Chỉ định IP của máy DHCP tin cậy.**
 - **Tin cậy cổng uplink để nhận phản hồi DHCP.**



Tấn công giả mạo ARP

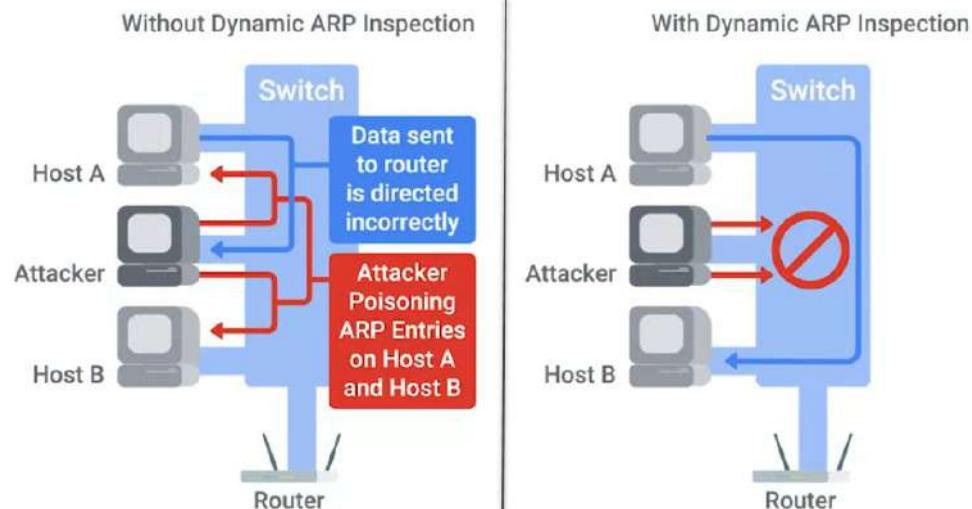
Tấn công giả mạo ARP (ARP spoofing) là một cách thức mà kẻ tấn công giả mạo phản hồi ARP, quảng bá địa chỉ MAC của nó như là địa chỉ vật lý khớp với IP của máy nạn nhân.



Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) là một chức năng trên switch để ngăn chặn tấn công giả mạo ARP.

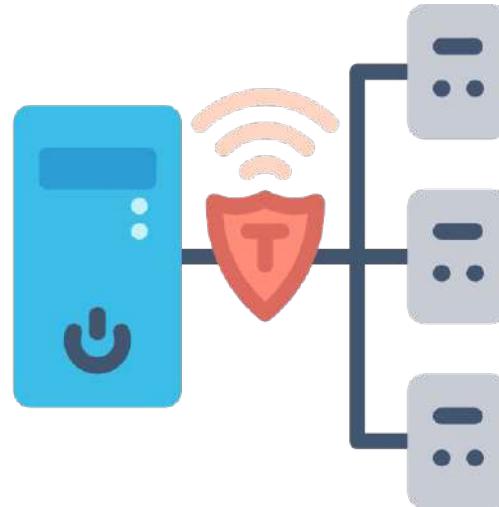
- Sử dụng DHCP snooping để thiết lập bảng ràng buộc tin cậy giữa địa chỉ IP và cổng switch.
- Dùng bảng từ DHCP snooping để phát hiện gói ARP giả mạo.
- Giới hạn số gói ARP trên mỗi cổng để ngăn việc quét ARP.



IP source guard

IP source guard (IPSG) là **chức năng** trên switch để **ngăn chặn tấn công giả mạo IP**.

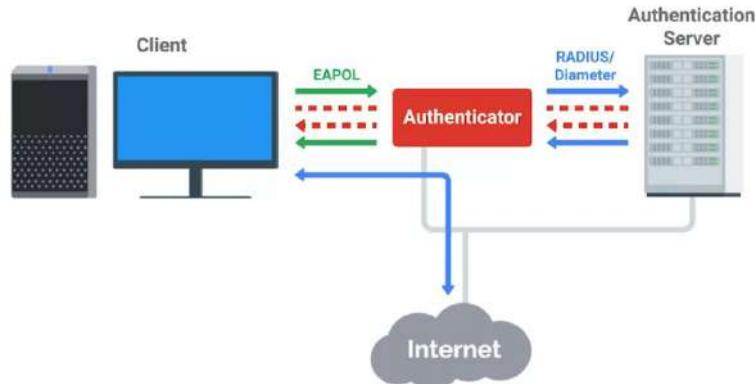
- Sử dụng bảng DHCP snooping để tạo động danh sách ACL cho mỗi cổng switch.
- Loại bỏ các gói không khớp địa chỉ IP với cổng dựa trên bảng DHCP snooping.



Xác thực mạng với chuẩn 802.1X

Khi máy khách muốn xác thực mạng sử dụng 802.1X, có ba bên tham gia:

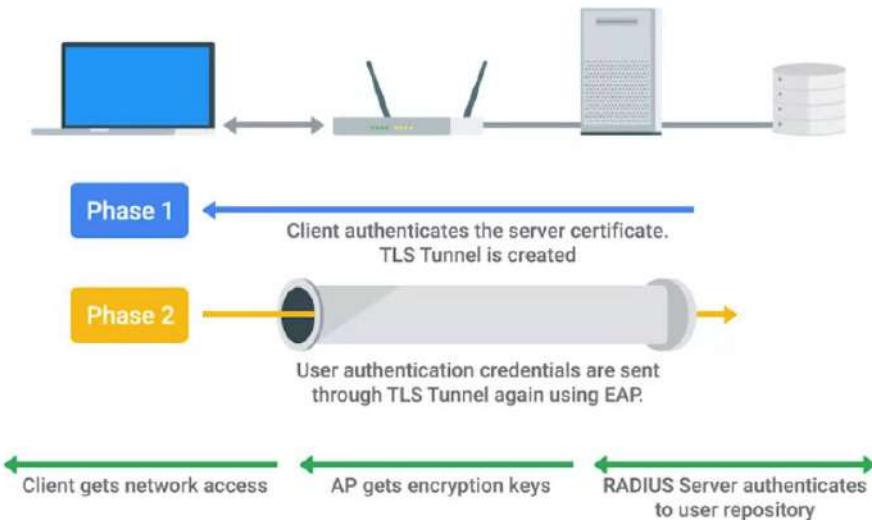
- **Thiết bị/phần mềm trên máy khách:** xử lý quá trình xác thực.
- **Trình xác thực:** yêu cầu máy khách xác thực thành công trước khi giao tiếp với mạng.
 - Trình xác thực có thể là switch đối với mạng có dây hay AP đối với mạng không dây.
- **Máy chủ xác thực:** nơi thực sự xác thực thông tin.



EAP-TLS

EAP-TLS là một loại xác thực được hỗ trợ bởi giao thức EAP (extensible authentication protocol) sử dụng TLS để xác thực máy chủ và máy khách.

- Xác thực dựa trên chứng chỉ.



Nội dung



Tổng quan gia cố mạng



Gia cố phần cứng mạng



Gia cố phần mềm mạng



Bảo mật mạng không dây

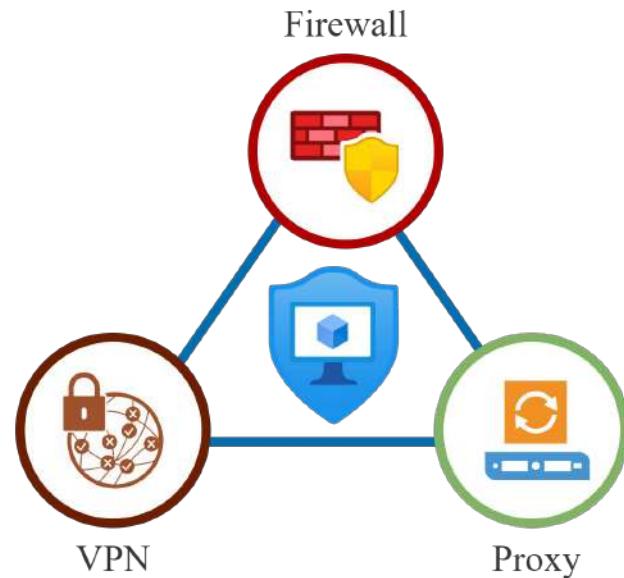


Giám sát mạng

Gia cố phần mềm mạng

Các giải pháp phần mềm bảo mật mạng chính gồm:

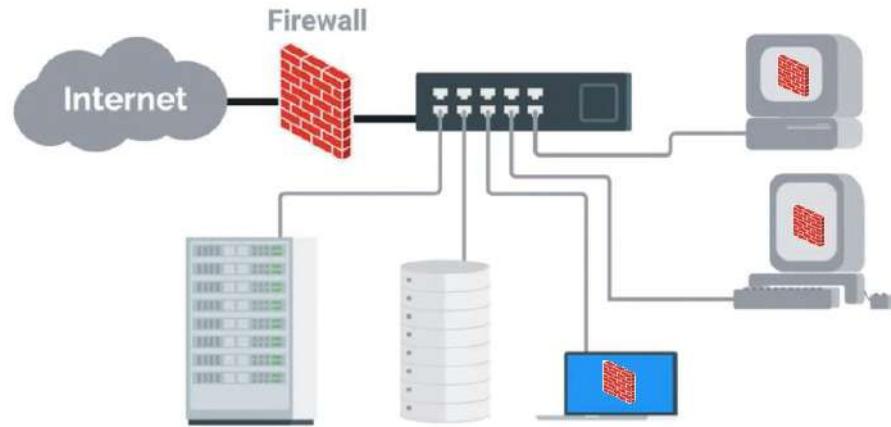
- Tường lửa (firewall)
- VPN
- Proxy



Giải pháp tường lửa

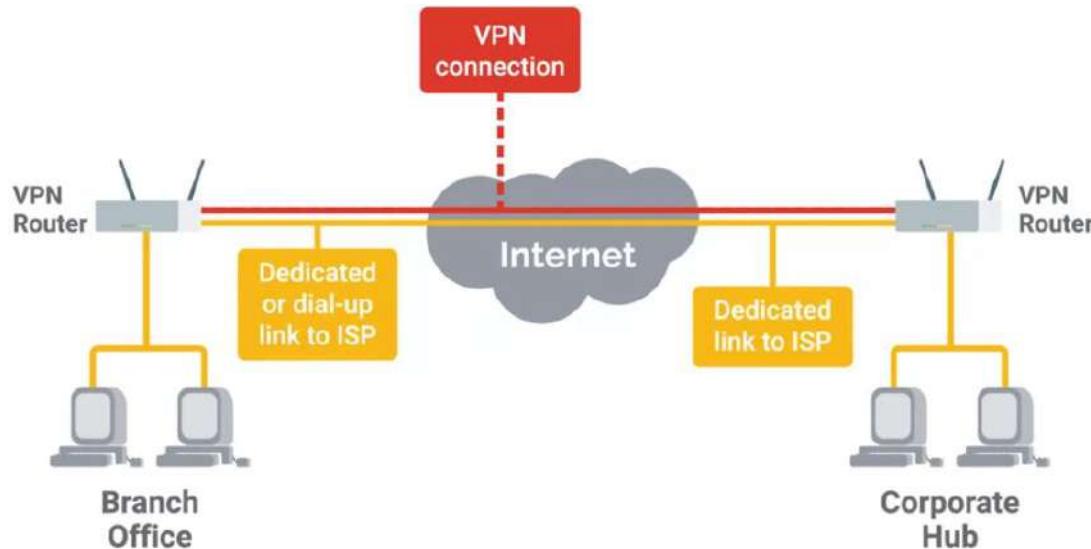
Tường lửa được triển khai theo hai giải pháp:

- **Tường lửa máy trực tiếp** (host-based firewall): phần mềm chạy trực tiếp trên máy tính để bảo vệ khỏi các nguy cơ tấn công, nhất là trong môi trường mạng không tin cậy.
- **Tường lửa mạng** (network-based firewall): bảo vệ ở cấp độ mạng và thường tích hợp trong bộ định tuyến, v.v...



Giải pháp VPN

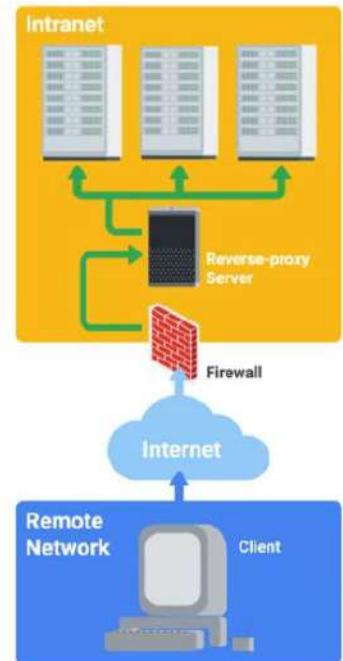
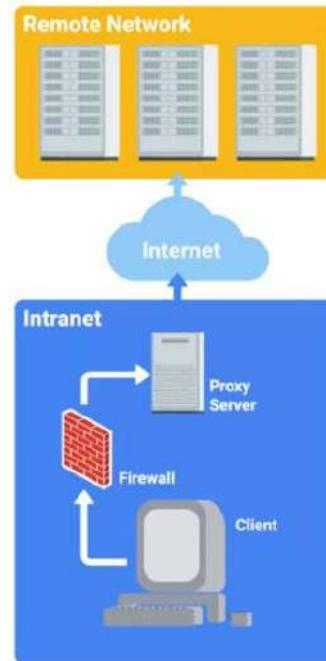
VPN cung cấp truy cập an toàn vào tài nguyên nội bộ cho người dùng di động, đồng thời hỗ trợ kết nối các mạng ở vị trí khác nhau có thể kết nối như một mạng duy nhất.



Giải pháp proxy

Proxy giúp bảo vệ thiết bị khách và luồng truy cập, đồng thời cấp quyền truy cập từ xa an toàn mà không cần sử dụng VPN thông qua reverse proxy.

- Máy chủ proxy giúp ghi lại nhật ký, phân tích lưu lượng và điều tra sự cố.
- Máy chủ proxy có thể chặn nội dung độc hại.



Nội dung



Tổng quan gia cố mạng



Gia cố phần cứng mạng



Gia cố phần mềm mạng



Bảo mật mạng không dây



Giám sát mạng

Giao thức WEP

Giao thức WEP (Wired Equivalent Privacy) là **giao thức bảo mật mạng Wi-Fi** cung cấp quyền riêng tư ngang bằng mạng có dây.

- Gói tin truyền qua mạng sẽ **không được mã hóa**.
- WEP không được sử dụng ngày nay do kém bảo mật.

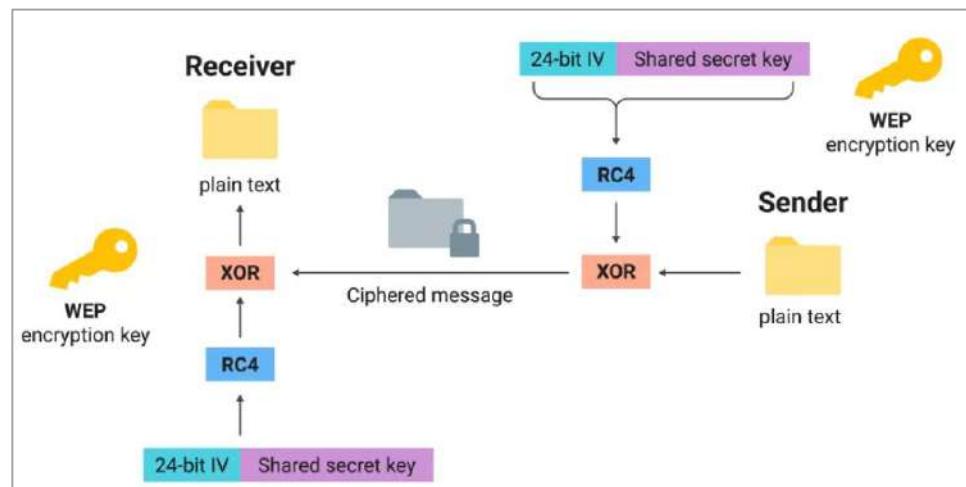


WEP

Kiến trúc WEP

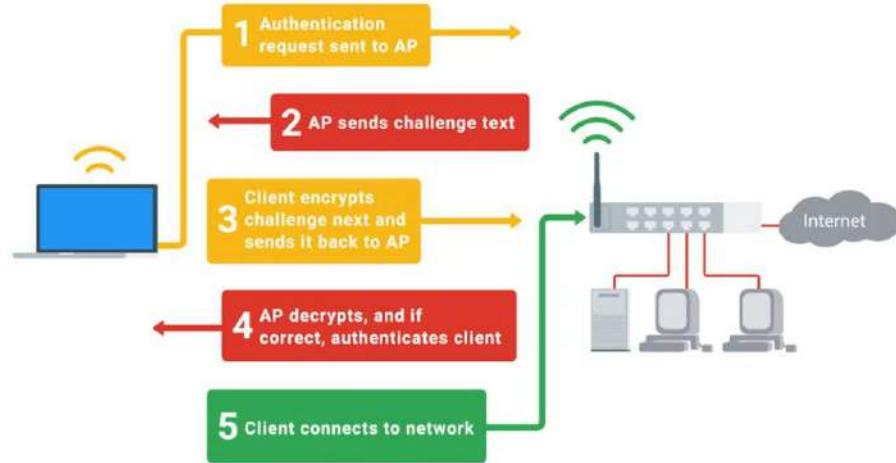
Đặc điểm kiến trúc WEP:

- Sử dụng **thuật toán mã hóa đối xứng RC4.**
- **Khóa chia sẻ 40 bit hoặc 104 bit.**
- **Khóa mã hóa là 64 bit hoặc 128 bit** sau khi nhập với vectơ khởi tạo IV.
- Hai chế độ xác thực:
 - **Hệ thống mở (Open System)**
 - **Khóa chia sẻ (Shared Key)**



Kiến trúc WEP

- Chế độ xác thực hệ thống mở:
 - Không yêu cầu cung cấp thông tin đăng nhập.
 - Giao tiếp với AP(access point) bằng khóa đã chia sẻ trước.
- Chế độ xác thực khóa chia sẻ:
 - Yêu cầu máy khách xác thực qua quy trình thử thách-phản hồi 4 bước.
 - AP gửi văn bản thử thách để máy khách mã hóa bằng khóa đã chia sẻ.
 - Sau khi máy khách trả dữ liệu, AP sẽ giải mã để kiểm tra nếu khớp thì xác thực thành công.



Điểm yếu của kiến trúc WEP

Kiến trúc WEP gộp một số điểm yếu:

- **Bị lộ cả văn bản thô và văn bản mã hóa.**
- **Cách sử dụng mã hóa RC4 và IV để tạo khóa dẫn đến kẻ tấn công có thể khôi phục khóa WEP.**
 - 24 bit khóa IV sinh ra 17 triệu khả năng có thể có và thực sự không lớn cho máy tính ngày nay.
 - Khóa IV được truyền ở dạng văn bản thô.



Phần mềm tấn công WEP

Một số phần mềm mã nguồn mở có thể khôi phục khóa WEP:

- Aircrack-ng
- AirSnort
- V.v...

The screenshot shows a terminal window with a blue background. At the top, there is some status text: "[00:00:19] Tested 6482 keys, 99% 17712 ms". Below this, there is a table-like structure with columns for 'dest' and 'byte(vote)'. The data is as follows:

dest	byte(vote)
0/ 20	33(23552) E2(23552) 08(23296) 07(22528) 36(22224)
0/ 9	38(24832) 93(23808) 80(23808) 9E(22508) 20(22208)
5/ 7	9D(22784) 82(22528) 68(22272) 73(22272) 78(22272)
0/ 1	76(28416) 81(23296) 8E(23040) 93(22784) 26(22232)
0/ 6	65(25856) 70(24832) AA(24576) 2B(24064) FC(23908)

At the bottom of the terminal, there is a large watermark-like text "Aircrack" and two pieces of text in white: "KEY FOUND! [33:38:17:76:65]" and "Decrypted correctly: 100%".

WPA

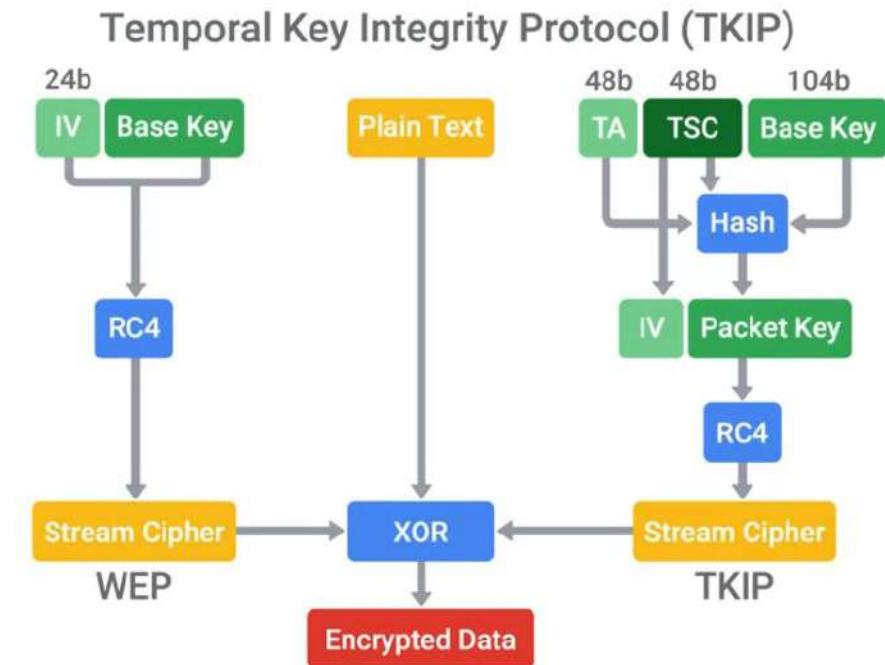
WPA (Wi-Fi Protected Access) là cơ chế bảo mật thay thế tạm thời WEP bằng bản cập nhập firmware.

- **Sử dụng giao thức TKIP** (Temporal Key Integrity Protocol).



Kiến trúc TKIP

- TKIP vẫn sử dụng thuật toán RC4 nhưng hỗ trợ khóa dài 256 bit.
- TKIP có 3 cập nhật:
 - Cơ chế dẫn xuất khóa an toàn hơn.
 - Bộ đếm tuần tự ngăn chặn tấn công phát lại (replay attack).
 - 64-bit MIC (message integrity check) ngăn chặn việc giả mạo hay làm hỏng gói tin.



WPA2

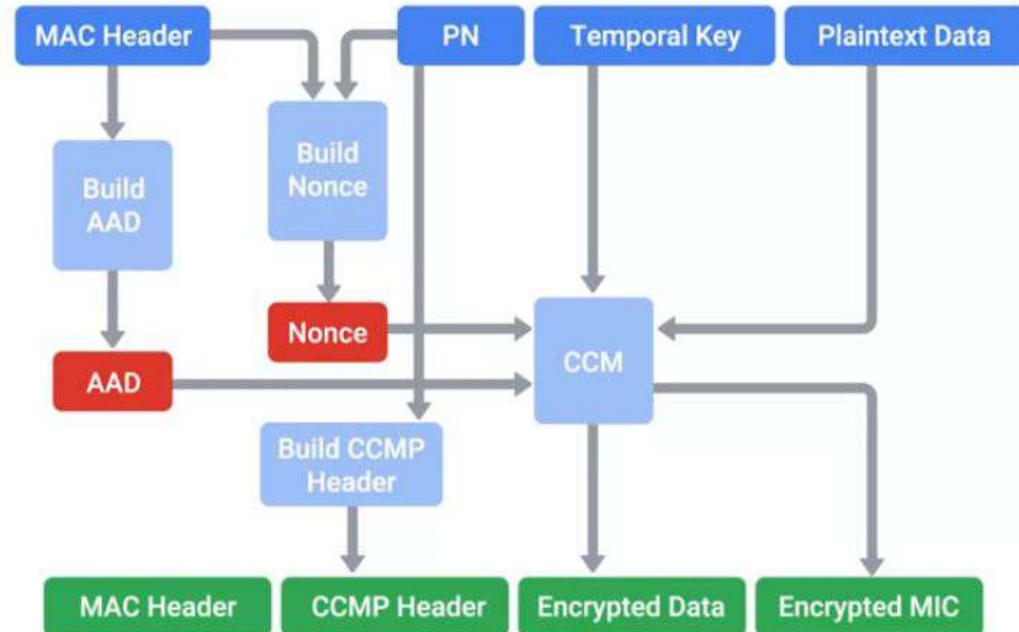
WPA2 cải thiện hơn bằng cách triển khai CCMP (Counter Mode CBC-MAC Protocol) và được xem là bảo mật tốt nhất hiện có cho mạng không dây.

- Sử dụng thuật toán mã hóa AES.



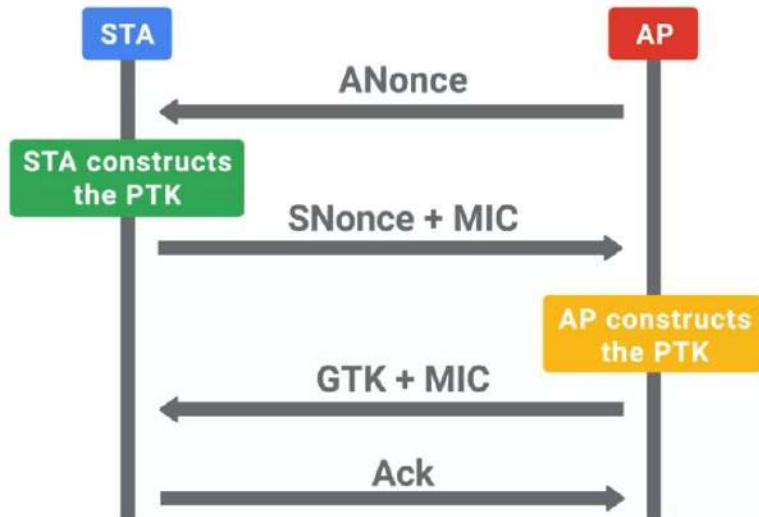
Nguyên lý hoạt động của WPA2

- Quá trình dẫn xuất khóa và yêu cầu khóa tương tự như WPA.
- Điểm khác biệt:
 - Bộ đếm với CBC-MAC là chế độ cho mã hóa khối.
 - Cho phép mã hóa được xác thực.



Cơ chế bắt tay 4 bước trong WPA2

- Quá trình bắt tay 4 bước gồm:
 - AP gửi thông điệp ANonce cho máy khách.
 - Máy khách gửi thông điệp SNonce cho AP.
 - AP gửi ngược lại thông điệp GTK.
 - Máy khách gửi Ack để xác nhận thành công.
- Các khóa được sử dụng:
 - PMK (pairwise master key): khóa chia sẻ.
 - PTK (pairwise transient key): mã hóa dữ liệu.
 - Các thành phần: PMK, AP nonce, Client nonce, AP MAC Address, Client MAC Address



WPA2-Enterprise

WPA2-Enterprise là chuẩn WPA2 áp dụng xác thực 802.1x.

- AP đóng vai trò là bên xác thực.
- Các cấu hình không dùng 802.1x được gọi là WPA2-Personal (WPA2-PSK).



WPA2/802.1x

Tính năng WPS

WPS (Wi-Fi protected setup) là tính năng tiện lợi để giúp máy khách dễ dàng tham gia vào mạng được bảo vệ bằng WPA-PSK.

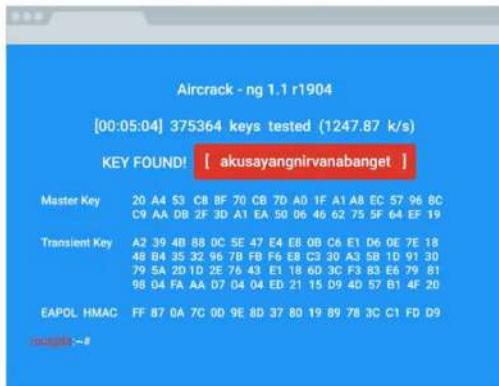
- Không yêu cầu phải nhập trực tiếp khóa chia sẻ trước.
- Hỗ trợ xác thực bằng mã PIN, NFC, USB, xác thực nút nhấn (push-button authentication).



Tấn công WPA2

WPA2 có thể bị tấn công trong quá trình bắt tay 4 bước:

- Tấn công vét cạn hoặc từ điển để đoán khóa PMK từ các nonces, MAC, PTK.
- Sử dụng tài nguyên máy tính mạnh có GPU và điện toán đám mây.
- Bảng cầu vòng có thể được sử dụng để giảm thời gian tính toán.



Password	Hash
123456	e10adc983ad09dca098da02320e
password	09dca09e10a0232dc983ad834ds
qwerty	h566adc983ad09d432fgsdcg432
baseball	123dsa3ad09dca3fer34r4653323
dragon	12409dca098dsa42363412467s2
kittycat	2ws3d4c983ad23wsd34565f4643
000111	344rfwc9834564dca09756324t72

Gia cố mạng không dây

Một số cách để gia cố mạng không dây:

- Sử dụng chuẩn xác thực 802.1x kết hợp với EAP-TLS.
 - Thuận lợi: bảo mật tốt nhất hiện nay.
 - Bất lợi: phức tạp và tốn kém chi phí (máy chủ RADIUS, khóa công khai, chứng chỉ máy khách, v.v....).
- Sử dụng cụm mật khẩu dài và phức tạp.
- Thay đổi SSID thành cụm từ không phổ biến và duy nhất.
- Tắt tính năng WPS trên router.



Nội dung



Tổng quan gia cố mạng



Gia cố phần cứng mạng



Gia cố phần mềm mạng



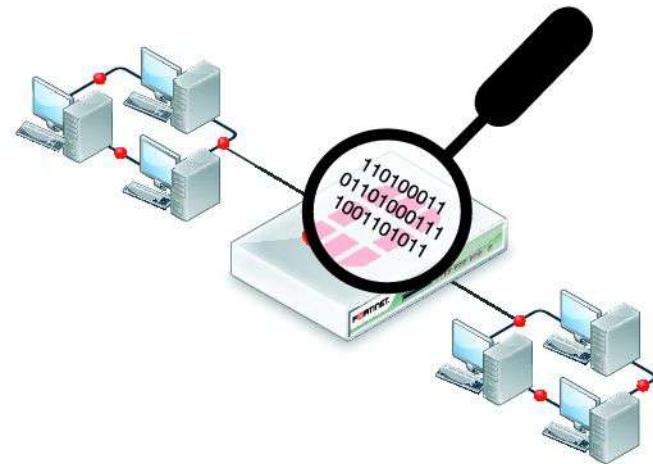
Bảo mật mạng không dây



Giám sát mạng

Bắt gói tin

Bắt gói tin (packet sniffing, packet capture) là quá trình **chặn các gói tin** trên mạng để phân tích.



Nguồn: wikimedia

Chế độ hỗn tạp

Chế độ hỗn tạp (promiscuous mode) là chế độ trên card mạng Ethernet dùng để bắt tất cả gói tin trong mạng.

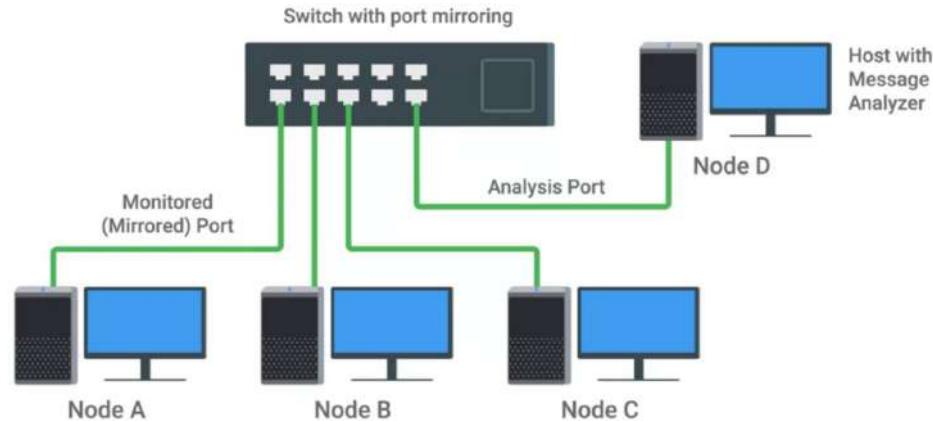


Nguồn: wikimedia

Điều kiện cần cho bắt gói tin

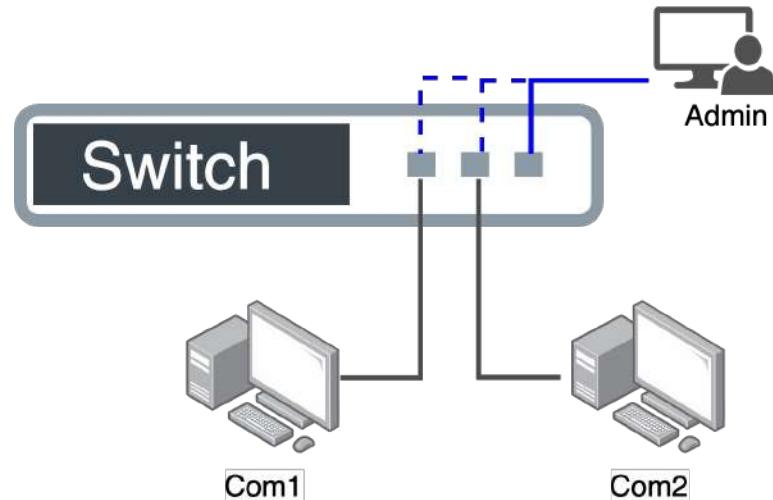
Để bắt được gói tin, điều kiện cần:

- Khả năng xen giữa luồng mạng của switch và các máy trong mạng.



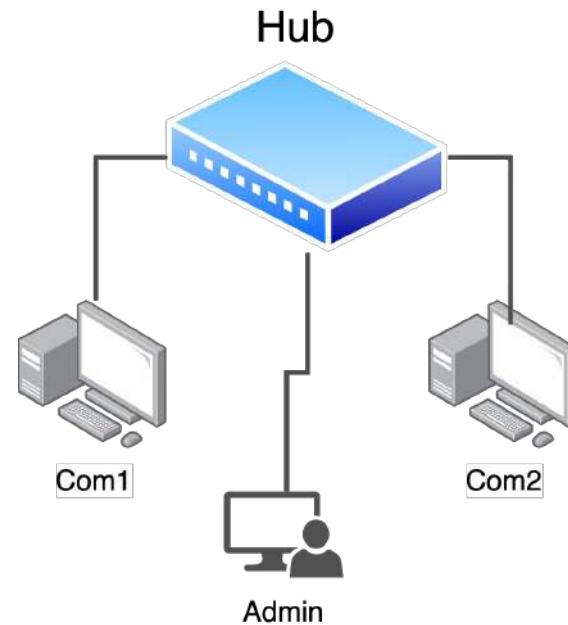
Port mirroring

Port mirroring là một tính năng trên switch cho phép lấy tất cả gói tin từ một cổng, một dải cổng hoặc toàn bộ VLAN và “phản chiếu” (mirroring) đến một cổng xác định.



Bắt gói tin với Hub

- Kết nối các máy tới Hub là cách nhanh chóng và dễ dàng để bắt gói tin.
- Cách này có nhiều nhược điểm:
 - Giảm băng thông trong mạng.
 - Tăng khả năng xảy ra đụng độ.



Bắt gói tin trong mạng không dây

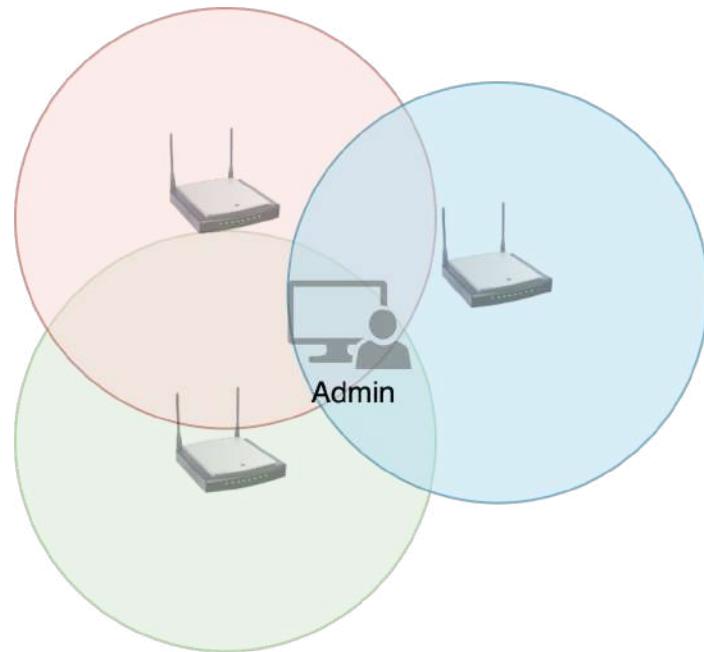
Chế độ hỗn tạp (promiscuous mode) trên card mạng không dây cũng cho phép bắt gói tin trong mạng được liên kết đến.



Bắt gói tin trong mạng không dây

Chế độ giám sát (monitor mode) trên card mạng không dây cho phép bắt gói tin trong tất cả các mạng lân cận.

- Một số phần mềm hỗ trợ như Aircrack-ng và Kismet.



Lệnh tcpdump

tcpdump là lệnh dùng để bắt gói tin.

- Dùng thư viện libpcap mã nguồn mở
- Hỗ trợ ghi gói tin và đọc dữ liệu trở lại.
- Chuyển đổi định dạng sang văn bản để dễ đọc bởi con người.



tcpdump



Lệnh tcpdump

Thông tin gói tin được thể hiện bởi tcpdump gồm:

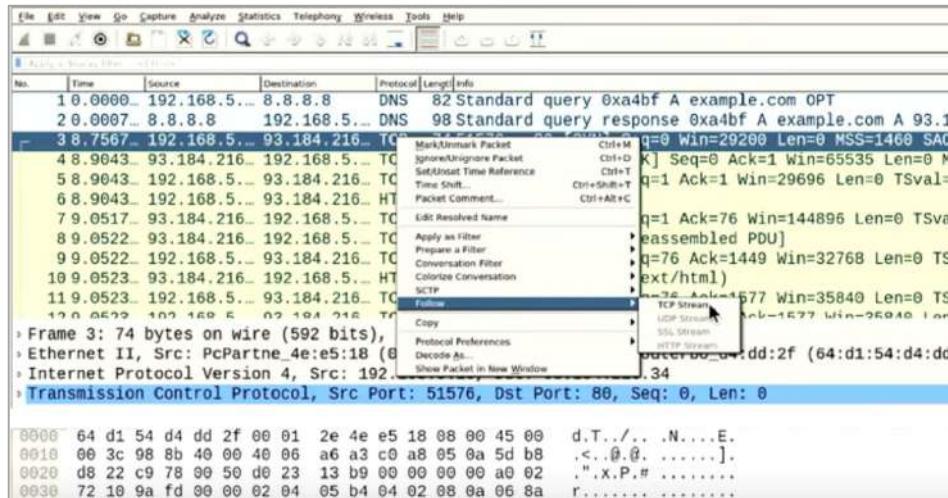
- Thời gian - Giao thức tầng 3 – Địa chỉ nguồn – Cổng nguồn – Địa chỉ đích – Cổng đích – Cờ TCP – Số thứ tự TCP (nếu có) – Số Ack – Kích thước cửa sổ TCP – Tùy chọn TCP – Kích thước gói dữ liệu.

```
spinel [clear] ~                                         17-09-19 4:51PM
spinel% sudo tcpdump -i eno1 ip and host example.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
16:52:00.416978 IP spinel.home.mrant.org.49026 > 93.184.216.34.http: Flags [S], seq 2505083261, win
29200, options [mss 1460,sackOK,TS val 1410827528 ecr 0,nop,wscale 7], length 0
16:52:00.583154 IP 93.184.216.34.http > spinel.home.mrant.org.49026: Flags [S.], seq 1959622244, ac
k 2505083262, win 65535, options [mss 1460,sackOK,TS val 1039848002 ecr 1410827528,nop,wscale 9], l
ength 0
16:52:00.583166 IP spinel.home.mrant.org.49026 > 93.184.216.34.http: Flags [.], ack 1, win 229, opt
ions [nop,nop,TS val 1410827578 ecr 1039848002], length 0
```

Phần mềm Wireshark

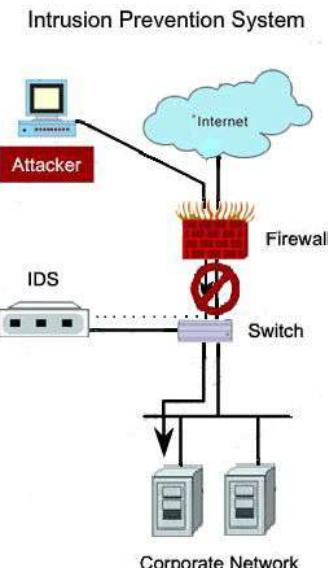
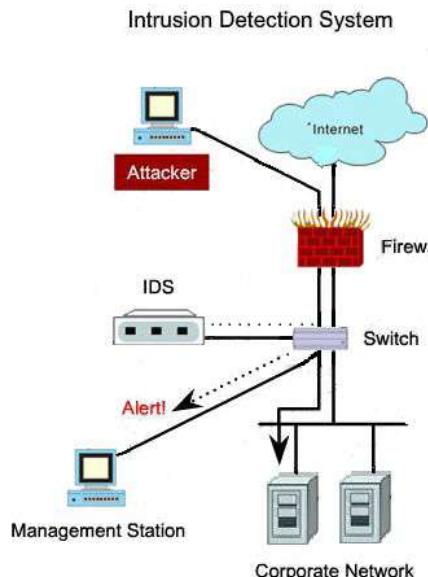
Wireshark là công cụ thu thập và phân tích gói tin với giao diện đồ họa cung cấp nhiều tính năng hơn tcpdump.

- Hỗ trợ giải mã gói tin nếu có được khóa.
- Hỗ trợ hơn 2000 giao thức khác nhau.
- Tích hợp bộ lọc để phân tích dễ dàng hơn.
- Theo dõi các luồng và phiên TCP.
- V.v...



Hệ thống phát hiện và ngăn chặn xâm nhập

- Hệ thống phát hiện xâm nhập (Intrusion Detection System, IDS) là hệ thống phát hiện các xâm nhập và ghi lại các cảnh báo.
- Hệ thống ngăn chặn xâm nhập (Intrusion Prevention System, IPS) là hệ thống điều chỉnh các quy tắc tường lửa để chặn hoặc loại bỏ luồng truy cập nguy hại.



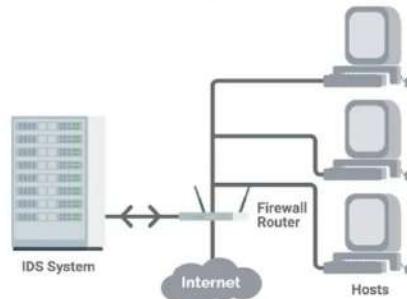
Nguồn: wikimedia

Triển khai IDS/IPS

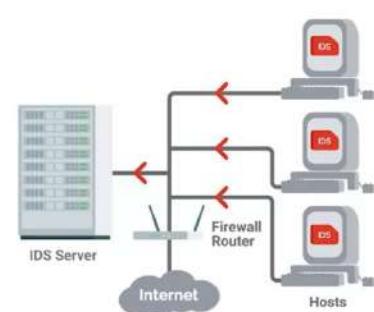
IDS/IPS có thể được thiết kế triển khai theo 2 cách:

- **IDS/IPS triển khai trên mạng** (network based IDS/IPS, NIDS/NIPS): **thiết lập ở một nơi nào đó trên mạng nhằm giám sát luồng truy cập cho một phân đoạn mạng hay mạng con.**
- **IDS/IPS triển khai trên máy tính** (host based IDS/IPS, HIDS/HIPS): **phần mềm được cài đặt trên máy tính để giám sát luồng truy cập đến và đi từ máy tính đó. Nó cũng giám sát các tập tin hệ thống để tìm các thay đổi trái phép.**

Network Based IDS



Host Based IDS



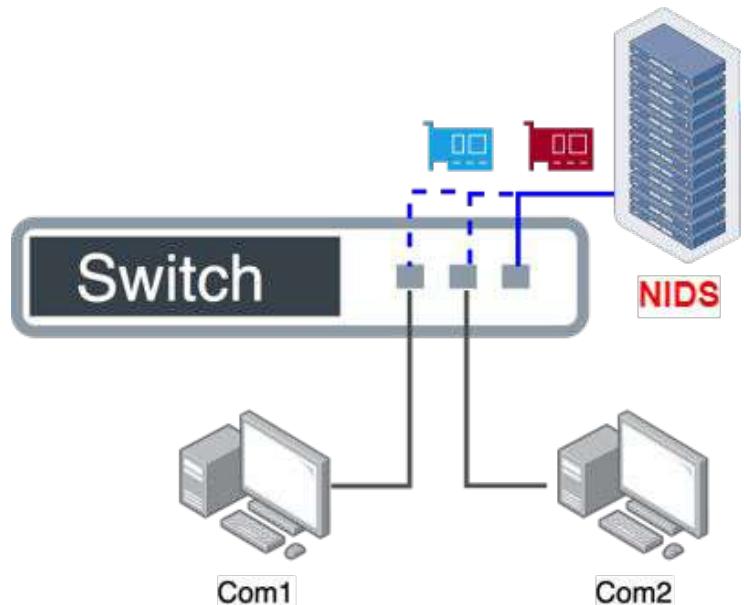
NIDS và Tường Lửa

NIDS	Tường Lửa (Firewall)
Phát hiện và cảnh báo về hoạt động nguy hiểm tiềm ẩn đến từ bên trong mạng .	Ngăn chặn sự xâm nhập bằng cách chặn luồng độc hại tiềm ẩn từ bên ngoài và thực thi danh sách ACL giữa các mạng .
Có khả năng nhìn thấy luồng truy cập giữa các máy tính bên trong mạng .	Chỉ có khả năng nhìn thấy luồng truy cập giữa các mạng mà chúng đã thiết lập để bảo vệ.

Vị trí đặt NIDS

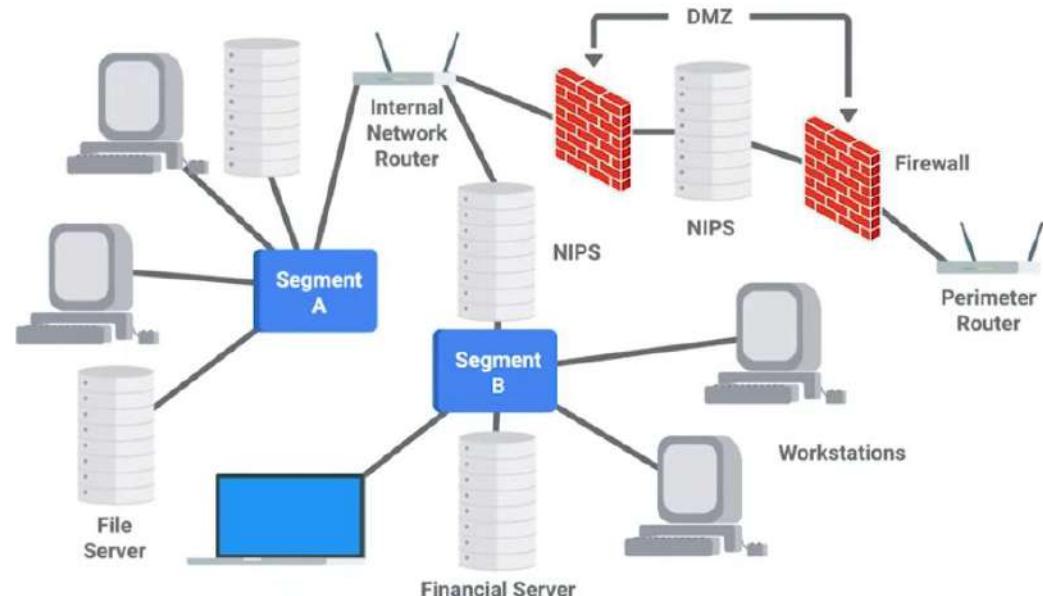
NIDS cần được đặt ở vị trí để có quyền truy cập vào luồng mạng cần theo dõi.

- Thiết lập NIDS với port mirroring trên thiết bị switch.
- NIDS cần có 2 card mạng:
 - Một card dùng để phân tích gói tin nhận từ port mirroring.
 - Một card để quản lý hệ thống mạng.



Vị trí đặt NIPS

Do NIPS ngoài việc giám sát còn ngăn chặn các luồng độc hại nên phải **được đặt sao cho luồng truy cập phải qua thiết bị NIPS trước khi vào mạng.**



Chữ ký luồng tấn công

Chữ ký luồng tấn công là **đặc điểm nhận dạng duy nhất của một luồng truy cập có hại**.

- Có thể là chuỗi gói tin cụ thể hoặc gói tin có trường header xác định đã được nhận diện là có hại trước đó.
- Các chữ ký cần được thường xuyên cập nhật.



Quy tắc tùy chỉnh

Quy tắc tùy chỉnh là quy tắc khi phát hiện luồng truy cập đáng ngờ.

- Ghi lại sự kiện cùng với bản sao toàn bộ gói truy cập nghi ngờ.
- Kích hoạt cảnh báo qua email, vé theo dõi, hoặc gọi trực tiếp cho nhóm phân tích để phân tích và đánh giá luồng truy cập.





5 Phòng Thủ Theo Chiều Sâu



Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



Cập nhật phần mềm

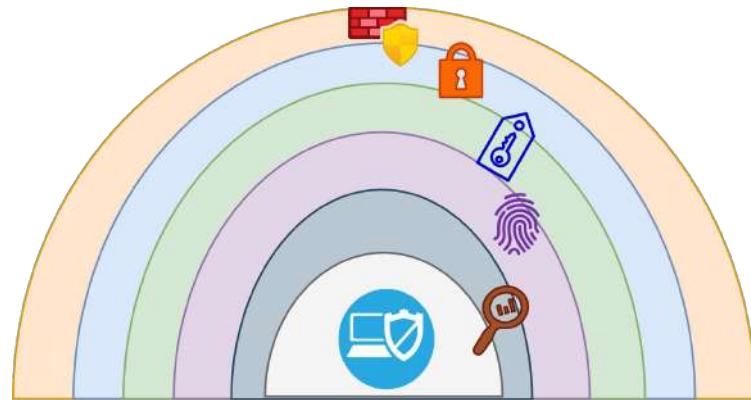


Chính sách ứng dụng

Phòng thủ theo chiều sâu

Phòng thủ theo chiều sâu (defense in depth) là cách thức tổ chức **hệ thống phòng thủ đan xen nhau** để bảo vệ toàn bộ hệ thống công nghệ thông tin.

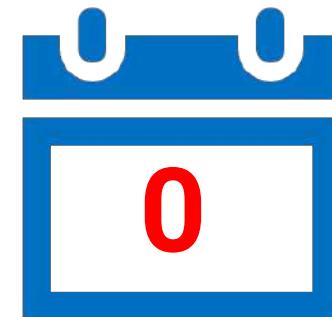
- Nếu lớp này bị đánh sập thì vẫn còn lớp bảo mật khác.



Lỗ hổng bảo mật

Lỗ hổng (vulnerability) là **kẻ hở** mà kẻ tấn công lợi dụng để xâm nhập hệ thống.

- Lỗ hổng Zero-day là lỗ hổng mà **nha phat trien chua biet** nhưng kẻ tấn công lại phát hiện ra.
 - Mặc dù chưa xác định, **vẫn co các bien phap han che va kiem soat chung**.
 - **Mục tiêu cuối cùng là giảm thiểu rủi ro.**



Vectơ tấn công

Vectơ tấn công (attack vector) là phương pháp hay con đường mà kẻ tấn công sử dụng để có được quyền truy cập vào hệ thống.

Một số vectơ tấn công:

- Tập tin đính kèm trong email
- Giao thức mạng
- Dịch vụ mạng
- Card mạng
- Thao tác của người dùng

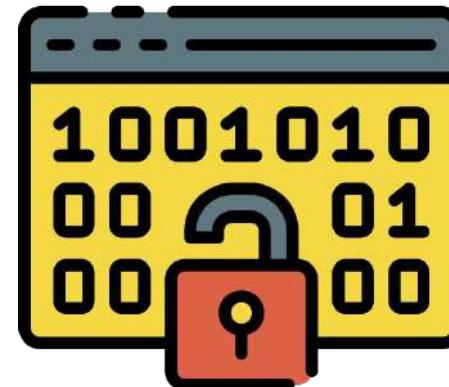


Bề mặt tấn công

Bề mặt tấn công (attack surface) là tổng của tất cả các vectơ tấn công khác nhau trong một hệ thống nhất định.

Nguyên tắc phòng thủ:

- **Giữ cho bề mặt tấn công càng nhỏ càng tốt.**
- **Đơn giản hóa dịch vụ.**



Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



Cập nhật phần mềm



Chính sách ứng dụng

Tắt thành phần không cần thiết

Hướng dẫn phòng thủ:

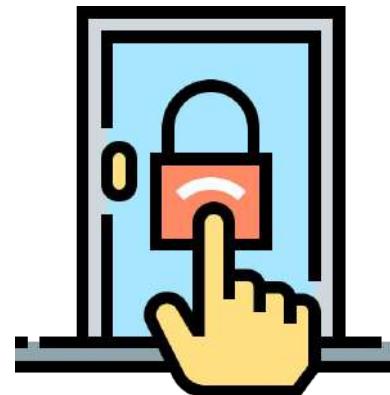
- Tắt hoặc gỡ bỏ các dịch vụ và giao thức không cần thiết.



Tắt thành phần không cần thiết

Hướng dẫn phòng thủ:

- Tắt hoặc gỡ bỏ các dịch vụ và giao thức không cần thiết.
- Ngoài việc giới hạn quyền truy cập, xem xét chỉ cho phép truy cập khi thực sự cần.



Tắt thành phần không cần thiết

Hướng dẫn phòng thủ:

- Tắt hoặc gỡ bỏ các dịch vụ và giao thức không cần thiết.
- Ngoài việc giới hạn quyền truy cập, xem xét chỉ cho phép truy cập khi thực sự cần.
- **Giảm triển khai nhiều gói phần mềm.**



Tắt thành phần không cần thiết

Hướng dẫn phòng thủ:

- Tắt hoặc gỡ bỏ các dịch vụ và giao thức không cần thiết.
- Ngoài việc giới hạn quyền truy cập, xem xét chỉ cho phép truy cập khi thực sự cần.
- Giảm triển khai các gói phần mềm.
- **Tắt các tính năng không cần thiết hoặc không cần dùng trong phần mềm.**



Tắt thành phần không cần thiết

Hướng dẫn phòng thủ:

- Tắt hoặc gỡ bỏ các dịch vụ và giao thức không cần thiết.
- Ngoài việc giới hạn quyền truy cập, xem xét chỉ cho phép truy cập khi thực sự cần.
- Giảm triển khai các gói phần mềm.
- Tắt các tính năng không cần thiết hoặc không cần dùng trong phần mềm.
- **Thực hiện ở mọi cấp độ hệ thống và mạng máy tính.**



Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



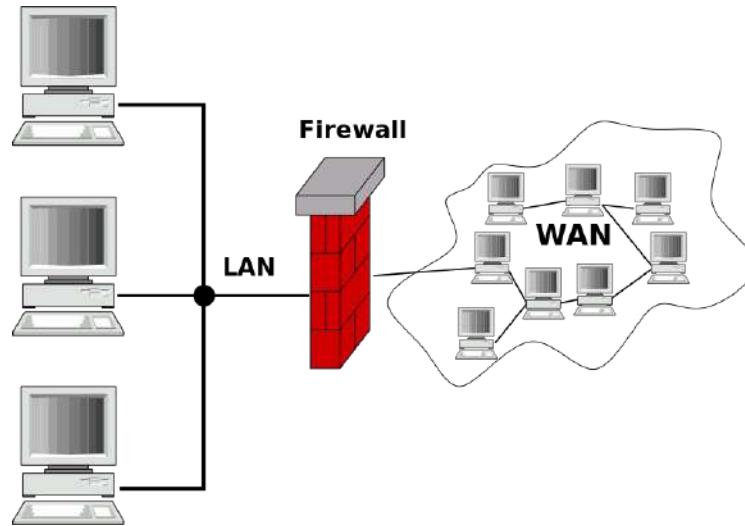
Cập nhật phần mềm



Chính sách ứng dụng

Tường lửa

Tường lửa (firewall) là một hệ thống bảo mật mạng dùng để **theo dõi** và **kiểm soát các luồng vào ra** dựa trên **tập quy tắc đã được xác định**.

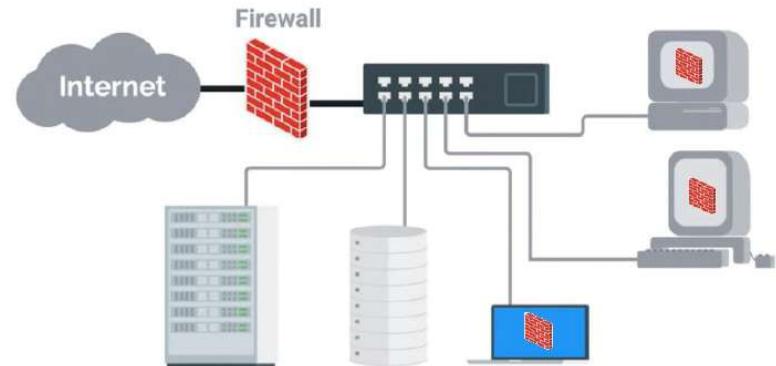


Nguồn: wikimedia

Giải pháp tường lửa

Tường lửa được triển khai theo hai giải pháp:

- **Tường lửa máy tính** (host-based firewall): phần mềm chạy trực tiếp trên máy tính để bảo vệ khỏi các nguy cơ tấn công, nhất là trong môi trường mạng không tin cậy.
- **Tường lửa mạng** (network-based firewall): bảo vệ ở cấp độ mạng và thường tích hợp trong bộ định tuyến, v.v...



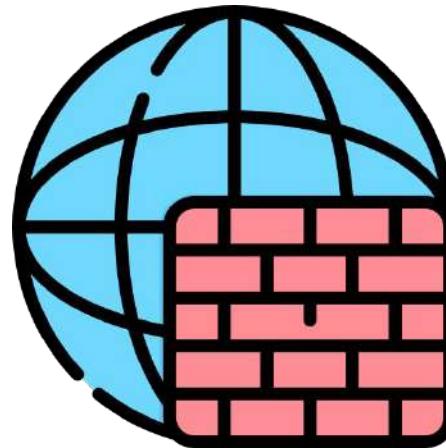
Tường lửa máy tính

Tường lửa máy tính giúp:

- Bảo vệ máy tính trong môi trường không đáng tin cậy.
- Bảo vệ máy tính ngay cả bên trong mạng đáng tin cậy.

Cách thức thiết lập:

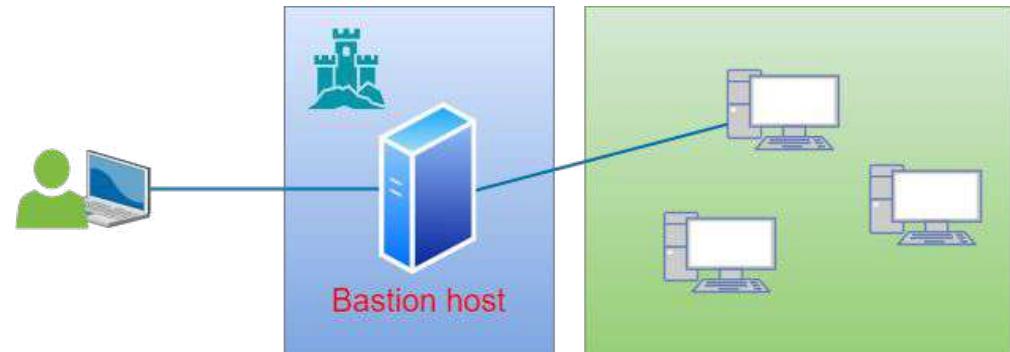
- Bắt đầu với quy tắc từ chối ngầm (implicit deny rule).
- Chọn các dịch vụ và cổng cần sử dụng.



Máy chủ pháo đài

Máy chủ pháo đài (Bastion host) là một máy tính **được gia cố đặc biệt** và **được tối thiểu hóa những gì** **chạy trên nó** để giảm khả năng bị xâm phạm.

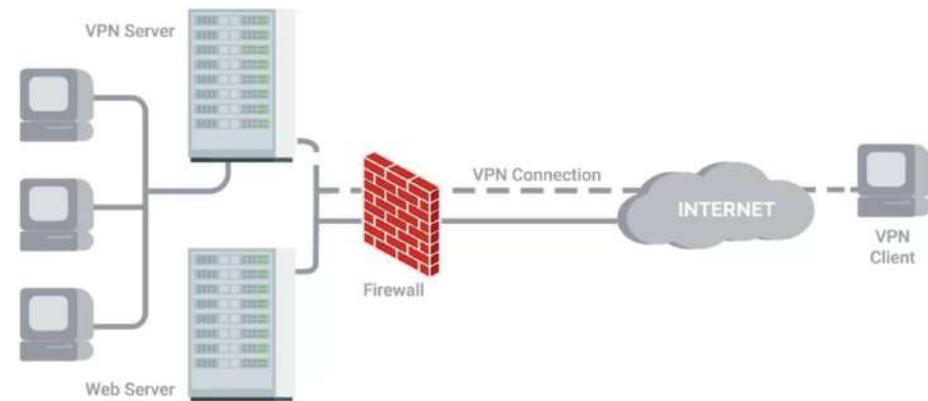
- **Được sử dụng như cổng truy cập vào các dịch vụ nhạy cảm** như máy chủ xác thực trung tâm hoặc bộ điều khiển miền.



Máy khách VPN

Tách biệt mạng mà các máy khách
VPN kết nối đến vì:

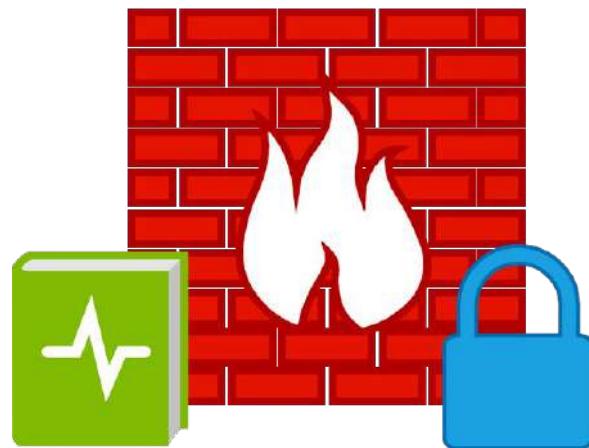
- Các máy khách VPN có thể hoạt động trong môi trường nguy hiểm tiềm ẩn.
- Có thể áp dụng linh hoạt các thực thi bảo mật.



Ngăn chặn tắt hay điều chỉnh tường lửa

Với quyền quản trị máy tính cá nhân, người dùng có khả năng thay đổi cấu hình và quy tắc tường lửa. Do đó:

- Theo dõi bản ghi nhật ký hệ thống.
- Ngăn chặn việc tắt tường lửa trên máy tính.



Nội dung

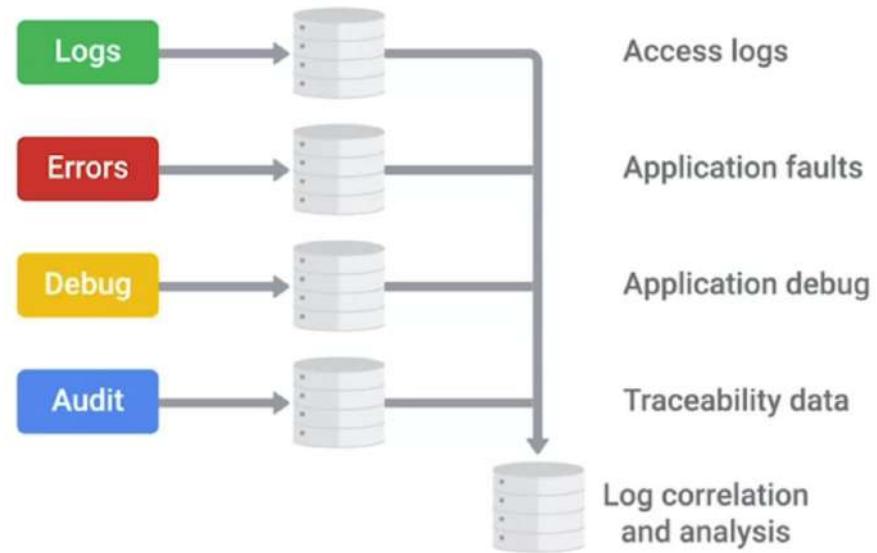
-  Giới thiệu phòng thủ theo chiều sâu
-  Tắt thành phần không cần thiết
-  Tường lửa
-  **Ghi nhật ký và kiểm tra**
-  Phần mềm chống virus
-  Mã hóa toàn đĩa
-  Cập nhật phần mềm
-  Chính sách ứng dụng

Nhật ký và cảnh báo

Nhật ký và cảnh báo là một phần quan trọng trong kiến trúc bảo mật.

Người quản lý cần:

- Xem các nhật ký về luồng truy cập, các thiết bị cơ sở hạ tầng, các ứng dụng.
- Bảo vệ nhật ký.
- Thực hiện các bước để giúp chúng dễ dàng xem và phân tích.



Máy chủ nhật ký

SIEM là mô tả về một hệ thống quản lý sự kiện và thông tin bảo mật:

- Thu thập nhật ký từ các hệ thống khác.
- Hợp nhất các bản ghi.
- Thống kê và phân tích.
- Trực quan hóa.

Lợi ích:

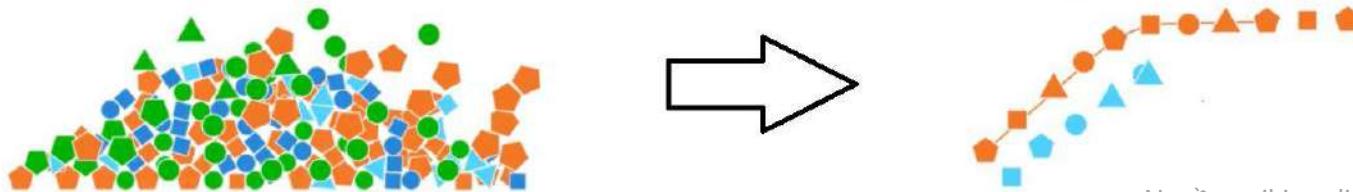
- Tập trung nhật ký trên một máy chủ giúp việc bảo vệ các tài liệu này tốt hơn.



Chuẩn hóa nhật ký

Chuẩn hóa nhật ký là quá trình **chuyển đổi các định dạng khác nhau** của nhật ký **về dạng chuẩn** phù hợp với cấu trúc xác định.

- Giúp cho việc phân tích và so sánh dữ liệu nhật ký của các hệ thống được dễ dàng và thống nhất.



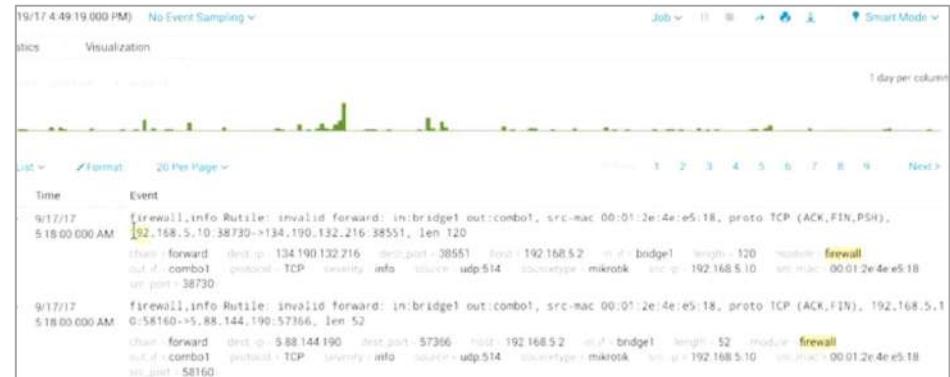
Nguồn: wikimedia

Thông tin cần ghi lại

Thông tin cần ghi lại tùy thuộc vào đặc điểm riêng của hệ thống đang giám sát và loại hoạt động trên mạng.

Thông tin ghi lại cần giúp hiểu những gì đã xảy ra và có thể tái tạo lại sự kiện.

- Thời gian xảy ra
- Sự kiện
- Tài khoản liên quan
- Thiết bị liên quan
- V.v...



Phân tích nhật ký

Khi phân tích nhật ký, cần **chú ý đến các mẫu** và **các kết nối giữa các luồng truy cập** như:

- Nhiều máy trong mạng cùng kết nối đến một địa chỉ bên ngoài.
- Nhiều hành động xác thực lặp đi lặp lại không thành công đến máy chủ xác thực.
- Xem xét các giao thức thường được sử dụng, các trao đổi hàng đầu và các báo cáo lỗi trong mạng.



Lưu giữ nhật ký

Lưu giữ nhật ký (log retention) là khả năng nắm bắt và lưu trữ nhật ký.

Tùy thuộc vào:

- Số lượng hệ thống được ghi
- Số lượng nhật ký và độ chi tiết
- Tốc độ tạo nhật ký
- Thời gian lưu giữ

Một số giải pháp như rsylog, Splunk Enterprise Security, IBM Security Qradar và RSA Security Analytics.



Nội dung

-  Giới thiệu phòng thủ theo chiều sâu
-  Tắt thành phần không cần thiết
-  Tường lửa
-  Ghi nhật ký và kiểm tra
-  **Phần mềm chống virus**
-  Mã hóa toàn đĩa
-  Cập nhật phần mềm
-  Chính sách ứng dụng

Phần mềm chống virus

Phần mềm chống virus dựa trên chữ ký để xác định các phần mềm độc hại.

Chữ ký có thể là:

- Giá trị băm của tập tin virus hay bị nhiễm.
- Đặc điểm luồng truy cập mạng của phần mềm độc hại.



Cách hoạt động của phần mềm chống virus

Phần mềm chống virus hoạt động theo cách sau:

1. Theo dõi và phân tích **những tập tin mới được tạo hoặc được sửa đổi** trên hệ thống để xem bất kỳ hành vi nào khớp với **chữ ký phần mềm độc hại đã biết**.
2. Nếu khớp, tùy thuộc vào loại chữ ký, nó sẽ **cố gắng chặn phần mềm độc hại**.
3. Trong trường hợp quá trình lây nhiễm đã xảy ra, nó có thể **cố gắng cách ly các tập tin bị nhiễm**.
4. Nếu không thể, nó **ghi lại và cảnh báo sự kiện phát hiện**.



Vấn đề với phần mềm chống virus

Có 2 vấn đề lớn liên quan đến phần mềm chống virus:

- Phụ thuộc vào chữ ký để chống virus.
- Phụ thuộc khả năng nhà viết phần mềm trong việc phát hiện virus mới.



Virus & threat protection updates

Security intelligence is up to date.

Last update: 8/8/2022 8:44 PM

Vấn đề với phần mềm chống virus

Phần mềm chống virus cũng là đối tượng bị tấn công.

- Dù vậy, phần mềm chống virus giúp chống lại các cuộc tấn công phổ biến và để chúng ta tập trung vào các mối đe dọa quan trọng hơn.



Nguồn: stockvault

Danh sách trắng nhị phân

Danh sách trắng nhị phân (binary whitelisting) là danh sách các phần mềm được phép chạy trong hệ thống.

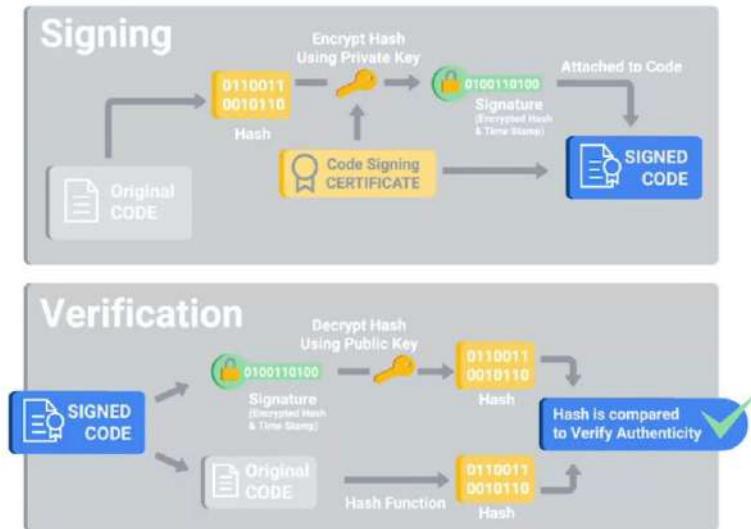
- Mọi thứ khác đều bị chặn.



Cập nhật danh sách trắng nhị phân

Có hai cơ chế cập nhật danh sách trắng nhị phân:

- **Sử dụng hàm băm mã hóa để xác định các tập tin nhị phân duy nhất.**
 - Xác định chính xác tập tin nhưng gây phiền phức, nhất là đối với bản cập nhật phần mềm.
- **Sử dụng chứng chỉ ký phần mềm.**
 - Tiện lợi vì chỉ cần kiểm tra chữ ký nhưng chữ ký có thể bị tấn công.



Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



Cập nhật phần mềm

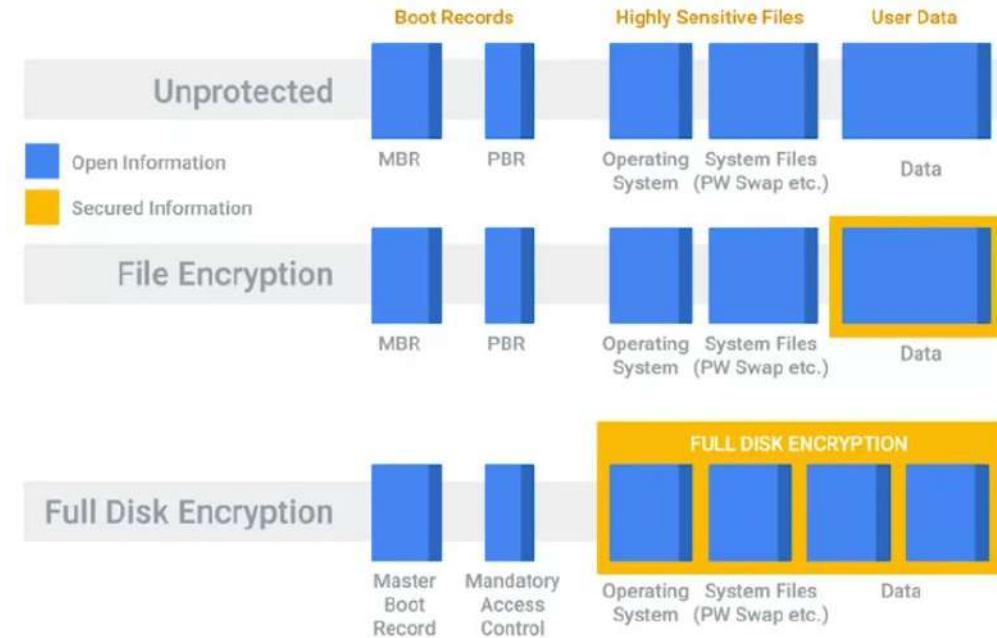


Chính sách ứng dụng

Mã hóa toàn đĩa

Mã hóa toàn đĩa (Full-disk encryption, FDE) là một lớp bảo vệ khỏi hình thức tấn công vật lý.

- **Tính bảo mật:** ngăn việc đánh cắp bí mật trong ổ cứng bị đánh cắp/mất.
- **Tính toàn vẹn:** không thể thay thế các tập tin bằng các tập tin độc hại.



Phân vùng khởi động khi mã hóa toàn đĩa

Khi thiết lập FDE, ổ đĩa cần có một **phân vùng không được mã hóa chứa tập tin dành cho quá trình khởi động** như kernel, boot loader.

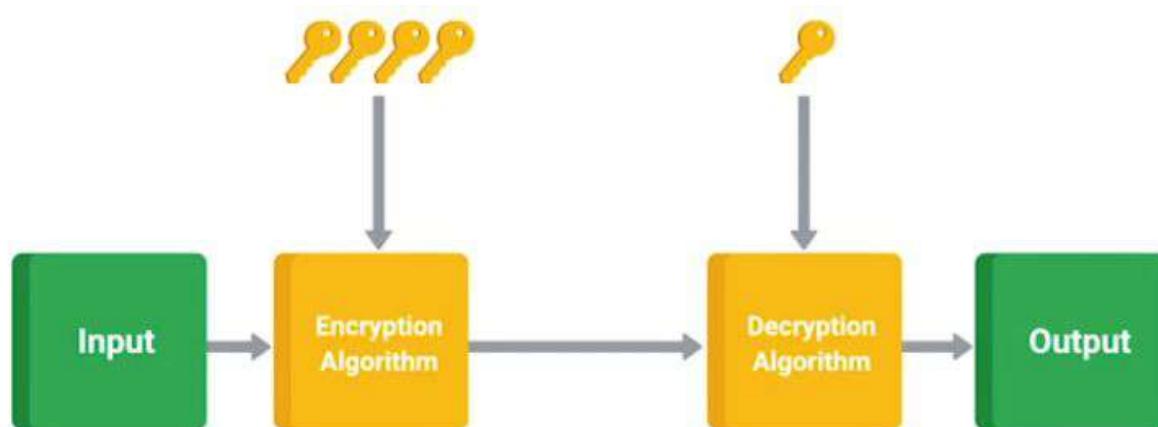
- Các tập tin này cũng là đối tượng để bị tấn công.

Giao thức khởi động an toàn (secure boot protocol) của UEFI giúp **bảo mật các tập tin dành cho khởi động**.



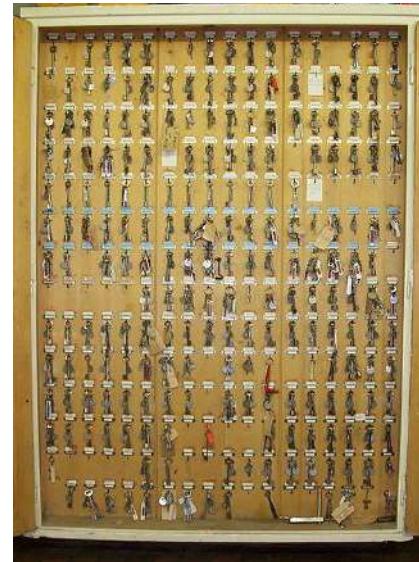
Mật khẩu cho mã hóa toàn đĩa

Khóa bí mật dùng để mã hóa và giải mã ổ đĩa được bảo vệ bằng mật khẩu nhập của người dùng.



Khắc phục quên mật khẩu

Ký quỹ khóa (key escrow) là hình thức cho phép khóa mã hóa được lưu trữ an toàn ở một nơi để nhận lại về sau bởi một bên có thẩm quyền.



Nguồn: wikimedia

Mã hóa toàn đĩa và mã hóa tập tin

Mã hóa tập tin chỉ đảm bảo tính bảo mật và toàn vẹn của các tập tin được bảo vệ bằng mã hóa.

- Kẻ tấn công vẫn có thể xâm phạm hệ thống và truy cập vào dữ liệu này.

Mã hóa toàn đĩa cung cấp mức độ bảo mật tốt hơn.



Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



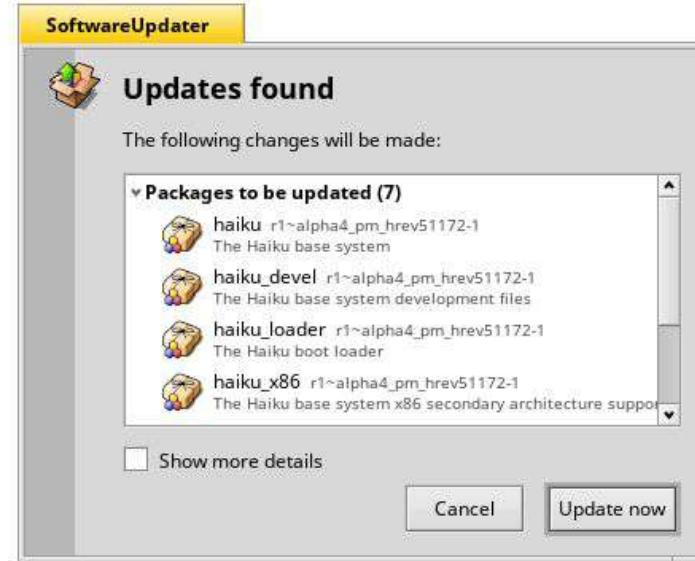
Cập nhật phần mềm



Chính sách ứng dụng

Cập nhật phần mềm

- Các bản cập nhật phần mềm thường:
- **Bổ sung các tính năng mới.**
 - **Cải thiện hiệu suất và độ ổn định.**
 - **Giải quyết các lỗ hổng bảo mật.**



Nguồn: wikimedia

Cập nhật phần mềm trên toàn hệ thống

Kiểm tra, xác minh và cài đặt các bản **cập nhật phần mềm trên toàn bộ hệ thống** các máy tính là điều phức tạp.

- Nhiều giải pháp như SCCM của Microsoft, Puppet Labs hỗ trợ theo dõi và phân tích các gói phần mềm và phiên bản cài đặt trên các máy tính.
- Việc **cập nhật có thể gây ra sự không tương thích hay trực trặc**. Do đó cần có những giải pháp khắc phục để đảm bảo luôn cài đặt các bản vá quan trọng kịp thời.

Nội dung



Giới thiệu phòng thủ theo chiều sâu



Tắt thành phần không cần thiết



Tường lửa



Ghi nhật ký và kiểm tra



Phần mềm chống virus



Mã hóa toàn đĩa



Cập nhật phần mềm



Chính sách ứng dụng

Chính sách ứng dụng

Chính sách ứng dụng (application policy) là các quy tắc chỉ ra những ứng dụng được phép và hướng dẫn mọi người về cách sử dụng phần mềm an toàn hơn.

- Mô tả rõ những phần mềm hợp lệ.
- Xem xét nguy cơ bảo mật đến từ tiện ích mở rộng trong các trình duyệt web.





6 Bảo Mật Trong Công Ty



Nội dung



Mục tiêu bảo mật



Quét lỗ hổng bảo mật



Quyền riêng tư



Người dùng



Bên thứ ba



Văn hóa bảo mật



Xử lý và khắc phục sự cố



Bảo mật điện thoại

Mục tiêu bảo mật

Mục tiêu bảo mật là những yêu cầu về một kiến trúc bảo mật mà công ty mong muốn đạt được để cân bằng giữa mức độ an ninh của hệ thống và năng suất của người dùng.



Tiêu chuẩn bảo mật thẻ thanh toán

PCI DSS là một **tiêu chuẩn bảo mật thẻ thanh toán** mà các công ty cần để ra cho mục tiêu bảo mật khi hỗ trợ khách hàng thanh toán bằng thẻ tín dụng.

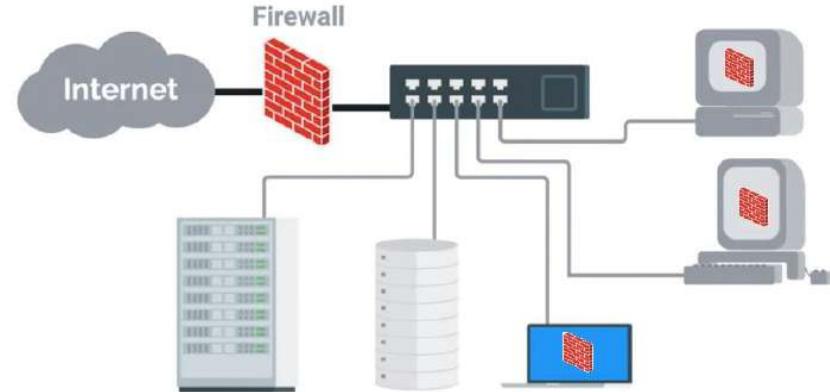
- PCI DSS **gồm 6 mục tiêu lớn**, mỗi mục tiêu có những yêu cầu cụ thể.



Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

1. **Xây dựng và duy trì một mạng và hệ thống an toàn:** cài đặt và duy trì cấu hình **tường lửa** để bảo vệ dữ liệu của chủ thẻ, **không sử dụng mật khẩu và thiết lập bảo mật mặc định** của nhà sản xuất.



Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

1. Xây dựng và duy trì một mạng và hệ thống an toàn.
2. **Bảo vệ dữ liệu của chủ thẻ: bảo vệ lưu trữ, mã hóa việc truyền dữ liệu thẻ, sử dụng mật mã mạnh, các quy định thời gian lưu trữ.**



Nguồn: wikimedia

Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

1. Xây dựng và duy trì một mạng và hệ thống an toàn.
2. Bảo vệ dữ liệu của chủ thẻ.
3. **Chương trình quản lý lỗ hổng**: bảo vệ **chống lại phần mềm độc hại, cập nhật phần mềm, phát triển hệ thống và ứng dụng an toàn**.



Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

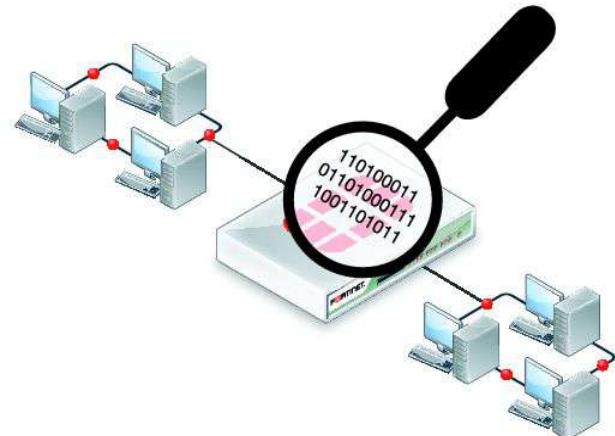
1. Xây dựng và duy trì một mạng và hệ thống an toàn.
2. Bảo vệ dữ liệu của chủ thẻ.
3. Chương trình quản lý lỗ hổng.
4. **Kiểm soát truy cập: giới hạn quyền truy cập vào dữ liệu thẻ, xác thực quyền truy cập, hạn chế quyền truy cập vật lý vào dữ liệu chủ thẻ.**



Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

1. Xây dựng và duy trì một mạng và hệ thống an toàn.
2. Bảo vệ dữ liệu của chủ thẻ.
3. Chương trình quản lý lỗ hổng.
4. Kiểm soát truy cập.
5. **Thường xuyên theo dõi và kiểm tra mạng:**
giám sát các truy cập tài nguyên mạng và dữ liệu thẻ, kiểm tra quy trình bảo mật và khả năng phòng thủ.



Nguồn: wikimedia

Mục tiêu của PCI DSS

Các mục tiêu của PCI DSS gồm:

1. Xây dựng và duy trì một mạng an toàn
2. Bảo vệ dữ liệu của chủ thẻ
3. Chương trình quản lý lỗ hổng
4. Kiểm soát truy cập
5. Thường xuyên theo dõi và kiểm tra mạng
6. **Chính sách bảo mật thông tin: cách thức bảo mật thông tin và hệ thống cho tất cả nhân viên.**



Rủi ro bảo mật

Rủi ro bảo mật (security risk) là khả năng xảy ra các cuộc tấn công hay các mối đe dọa đối với hệ thống.

- **Bắt đầu với việc mô hình hóa mối đe dọa.**
- **Cần xác định các rủi ro bảo mật và gán mức độ ưu tiên** dựa trên mức độ nghiêm trọng và xác suất xảy ra.
- **Tấn công thường nhắm vào các tài sản có giá trị cao** như thông tin tài khoản người dùng, cơ sở dữ liệu xác thực, thông tin liên quan đến thanh toán.



Nội dung

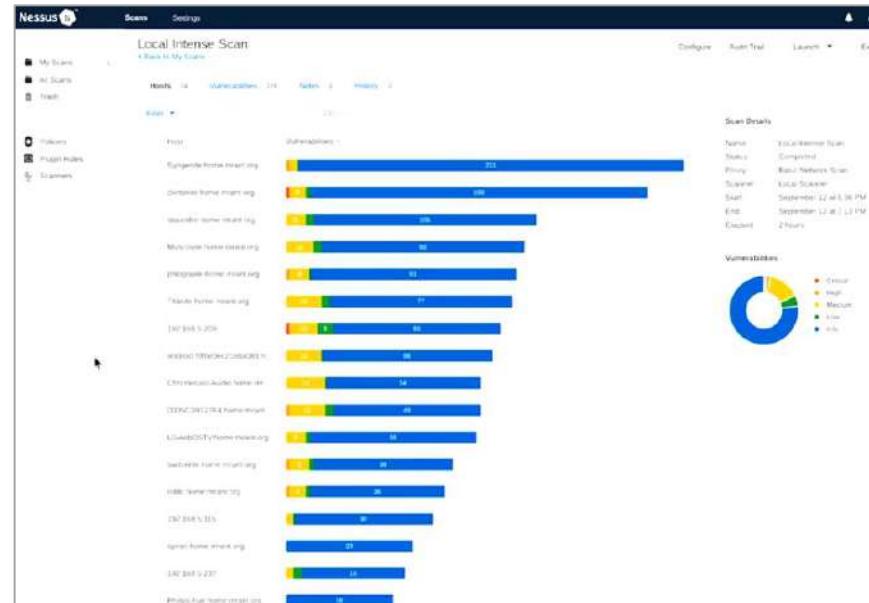


Quét lỗ hổng bảo mật

Quét lỗ hổng bảo mật là quá trình tìm các lỗ hổng bảo mật có thể có trong hệ thống.

Một số phần mềm hỗ trợ như:

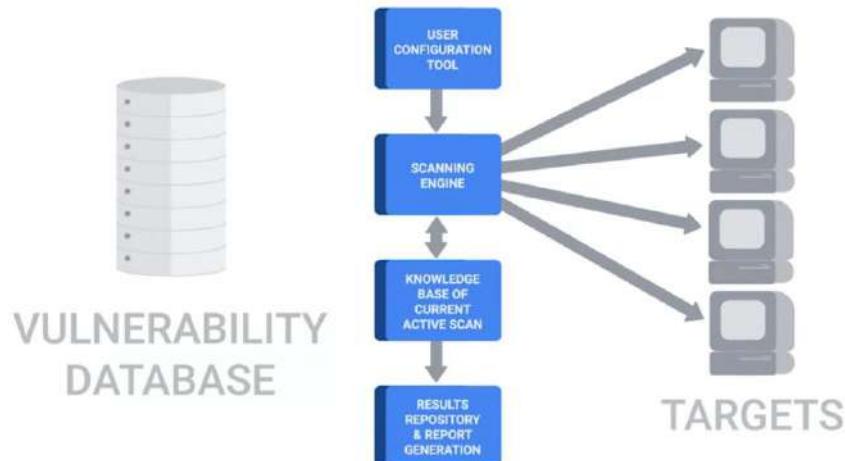
- Nessus
- OpenVas
- Qualys
- V.v...



Quá trình quét lỗ hổng

Quét lỗ hổng bảo mật được thực hiện qua các bước:

1. Tìm và phát hiện các máy tính trên mạng.
2. Quét từng máy tính và xác định các cổng và dịch vụ.
3. Kiểm tra các dịch vụ để khám phá thêm thông tin về loại và phiên bản.
4. Nếu tồn tại trong cơ sở dữ liệu lỗ hổng thì công cụ quét sẽ ghi lại trong báo cáo.



Công cụ quét lỗ hổng

Ngoài chức năng quét, công cụ quét lỗ hổng còn **phân loại theo mức độ nghiêm trọng** như khả năng bị khai thác, có thể khai thác từ xa hay không, v.v...

Công cụ quét chỉ có thể phát hiện các lỗ hổng đã biết và đã lộ diện.

Do đó cần:

- **Cần quét thường xuyên.**
- **Luôn cập nhật cơ sở dữ liệu lỗ hổng bảo mật.**



Kiểm tra thâm nhập

Kiểm tra thâm nhập (penetration test) là **đột nhập thử vào hệ thống hoặc mạng để kiểm tra các vấn đề của nó.**

- Suy nghĩ và thực hiện như cách thức mà kẻ tấn công sử dụng.
- Báo cáo cần liệt kê các điểm yếu và điểm mù tồn tại.
- Có thể thuê một công ty thứ ba cung cấp dịch vụ thử nghiệm xâm nhập.



Nguồn: pxhere

Nội dung



Chính sách quyền riêng tư

Chính sách quyền riêng tư (privacy policy) là các hướng dẫn việc truy cập và sử dụng dữ liệu nhạy cảm, những thông tin cá nhân của người dùng.

- Bảo vệ dữ liệu khỏi việc sử dụng sai mục đích.
- Thường đi cùng với chính sách quyền truy cập (data access policy) để tránh việc người dùng vô tình hay cố ý tác động đến dữ liệu.



Nguồn: pix4free

Thực thi chính sách quyền riêng tư

Quá trình thực thi chính sách quyền riêng tư gồm:

- Kiểm tra định kỳ với các dữ liệu nhạy cảm bị truy cập thông qua nhật ký giám sát.
- Xác định dữ liệu được sử dụng với lý do hợp lý.
- Áp dụng nguyên tắc ít đặc quyền nhất (mặc định không cho phép).
- Việc truy cập cần gửi yêu cầu cùng với lý do chính đáng.
- Giới hạn thời lượng truy cập.
- Điều tra các vi phạm được hệ thống ghi nhận.

Chính sách xử lý dữ liệu

Chính sách xử lý dữ liệu (data handling policy) là các hướng dẫn về **cách thức như thế nào xử lý dữ liệu, cách thức lưu trữ và đảm bảo an toàn trong quá trình xử lý**.

- Hướng dẫn cách thức dữ liệu được phân loại (nhạy cảm/không nhạy cảm, bí mật/công khai).
- Hướng dẫn nơi lưu trữ (máy công ty/phương tiện cá nhân, cố định/di động)
 - Không lưu trữ trên các thiết bị dễ bị mất như USB, ổ cứng di động, CD.



Nội dung



Người dùng

Người dùng được xem là mắt xích yếu nhất trong hệ thống bảo mật nhưng lại thường bị bỏ qua.

- Ví dụ, người dùng có thể viết mật khẩu ra và để nó nơi dễ bị phát hiện.
- Cần có chính sách như **chính sách mật khẩu** (password policy) để tăng cường bảo mật cho hệ thống.



Hỗ trợ công cụ làm việc

- Quan tâm cách nhân viên hoàn thành công việc để hỗ trợ công cụ phù hợp.
- Tránh để họ sử dụng các công cụ gây rủi ro bảo mật.

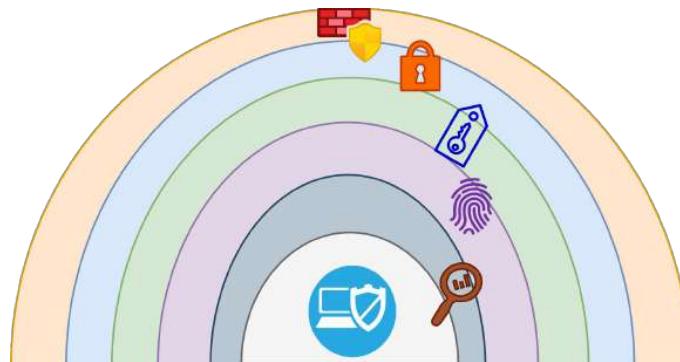


Nguồn: neolite.in

Chính sách mật khẩu

Chính sách mật khẩu (password policy) cần cân bằng với sự thuận lợi của người dùng.

- Nếu yêu cầu mật khẩu quá dài và thay đổi liên tục thì sẽ khiến người dùng viết chúng ra.
- Xác định lý do cần mật khẩu dài và thay đổi để đề ra các cách thức bảo mật tốt mà không cần mật khẩu quá phức tạp.



Mật khẩu dùng nhiều nơi

Sử dụng cùng mật khẩu cho nhiều nơi làm suy yếu tính bảo mật của hệ thống.

Đảm bảo mật khẩu cần duy nhất cho mỗi dịch vụ.

Hệ thống cần kiểm tra nếu người dùng sử dụng mật khẩu đã bị rò rỉ.

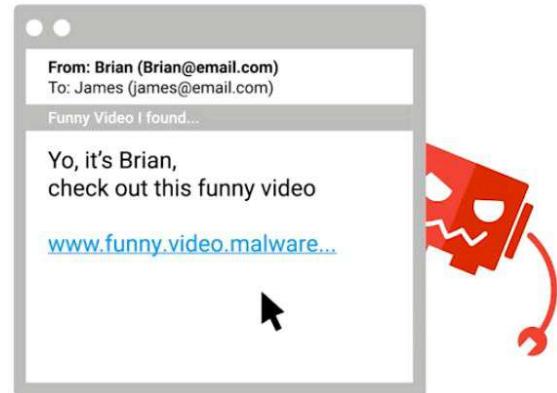


Nguồn: wikimedia

Email lừa đảo

Email lừa đảo lợi dụng khuynh hướng của mọi người mở email mà không cần xem xét chúng kỹ càng.

- Nội dung thường **dẫn đến một trang đăng nhập giả mạo**, người dùng nhập thông tin đăng nhập một cách mù quáng và tiết lộ thông tin này cho kẻ tấn công.
- Tổ chức các buổi **huấn luyện** hay các hình thức cảnh báo giúp người dùng biết **nguy cơ bảo mật** này và **cách phòng tránh**.
- **Thay đổi mật khẩu ngay lập tức** nếu lỡ điền thông tin.



Nội dung

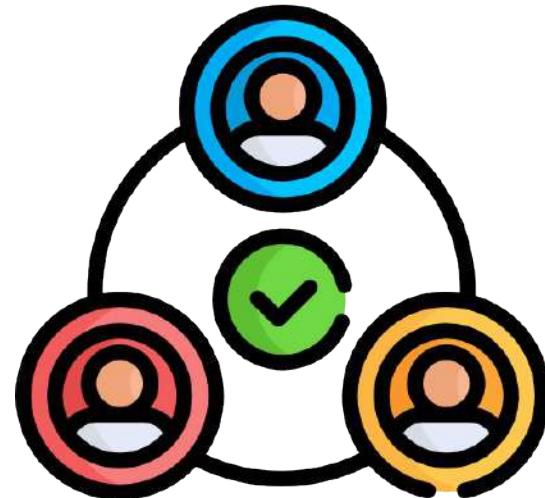


Bên thứ ba

Công ty có thể phải dựa vào giải pháp của **bên thứ ba** và họ **có thể có quyền truy cập đến dữ liệu**.

Do đó, cần:

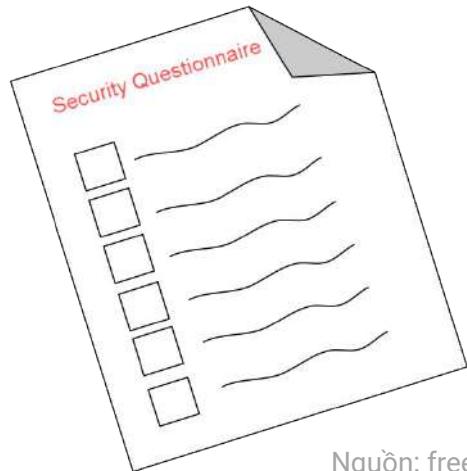
- **Đảm bảo bên thứ ba tin cậy và có uy tín.**
- **Có các cam kết rõ ràng trên bảo mật.**
- **Kiểm soát các cam kết được thực thi.**



Đánh giá bảo mật bên thứ ba

Một số cách để đánh giá bảo mật bên thứ ba:

- Trả lời bảng câu hỏi bảo mật: họ có triển khai bảo mật không, cách họ bảo mật tổ chức của họ, v.v...



Nguồn: freesvg

Đánh giá bảo mật bên thứ ba

Một số cách để đánh giá bảo mật bên thứ ba:

- Trả lời bảng câu hỏi bảo mật
- Xác minh bảo mật thông qua báo cáo kiểm tra
thâm nhập, chạy đánh giá chuyên sâu,
v.v...



Nội dung



Văn hóa bảo mật

Văn hóa bảo mật là cách thức khuyến khích mọi người:

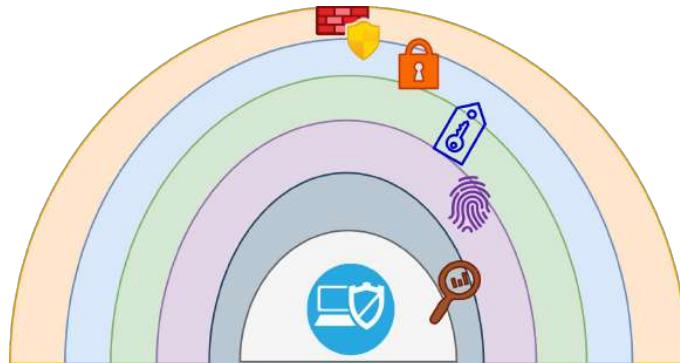
- Lên tiếng khi họ nghi ngờ về điều gì đó là rủi ro bảo mật.
- Tổ chức nơi để mọi người thể hiện các mối quan tâm bảo mật.
- Được nhận câu trả lời rõ ràng.
- Được khen thưởng về những hành động giúp tăng cường an ninh.



Đào tạo, huấn luyện bảo mật

Thường xuyên tổ chức các **khóa huấn luyện** để nâng cao kiến thức và kỹ năng của nhân viên liên quan đến vấn đề bảo mật.

Đào tạo được xem là **tuyến phòng thủ cuối cùng** mà chúng ta cần trang bị.



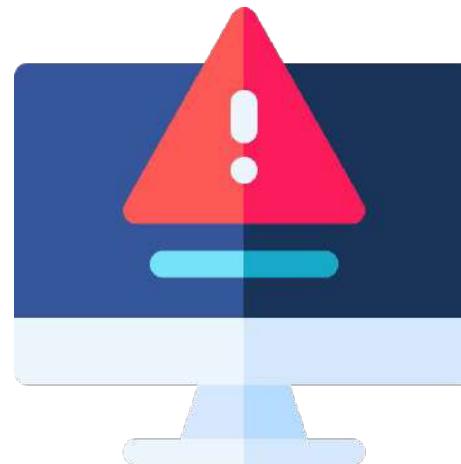
Nội dung

-  Mục tiêu bảo mật
-  Quét lỗ hổng bảo mật
-  Quyền riêng tư
-  Người dùng
-  Bên thứ ba
-  Văn hóa bảo mật
-  **Xử lý và khắc phục sự cố**
-  Bảo mật điện thoại

Khi sự cố bảo mật xảy ra

Khi sự cố bảo mật xảy ra, điều quan trọng là:

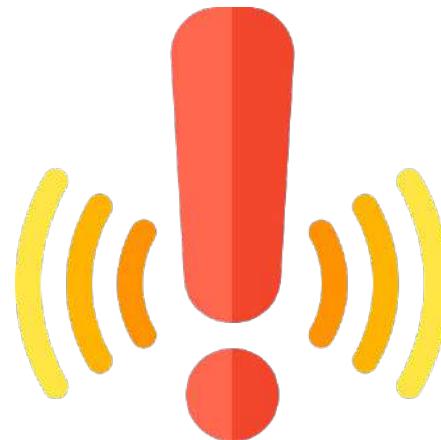
- Biết chính xác những gì đã xảy ra.
- Nó xảy ra như thế nào.
- Khắc phục nó ra sao.
- Làm thế nào để tránh để nó xảy ra lần nữa.



Xử lý sự cố bảo mật

Các bước xử lý sự cố bảo mật:

1. **Phát hiện sự cố**: các hệ thống phát hiện xâm nhập có thể phát tín hiệu cảnh báo, người dùng báo cáo lại những gì nghi ngờ.



Xử lý sự cố bảo mật

Các bước xử lý sự cố bảo mật:

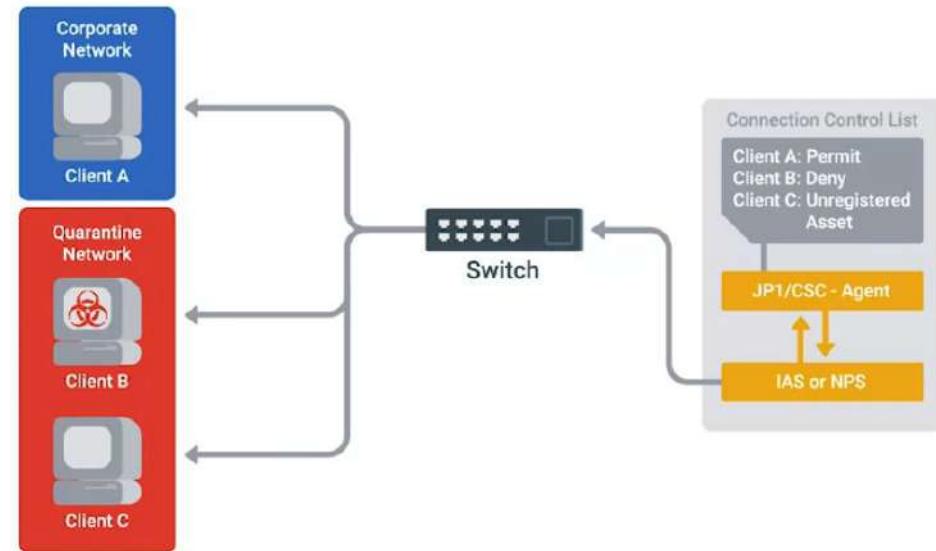
1. Phát hiện sự cố
2. Phân tích, xác định ảnh hưởng và phạm vi thiệt hại: loại sự cố, các máy bị ảnh hưởng, các mối tương quan, v.v...



Xử lý sự cố bảo mật

Các bước xử lý sự cố bảo mật:

1. Phát hiện sự cố
2. Phân tích, xác định ảnh hưởng
3. Ngăn chặn: cách ly hệ thống, khóa tài khoản, thu hồi các mã token, cập nhật quy tắc tường lửa, v.v...



Xác định mức độ nghiêm trọng

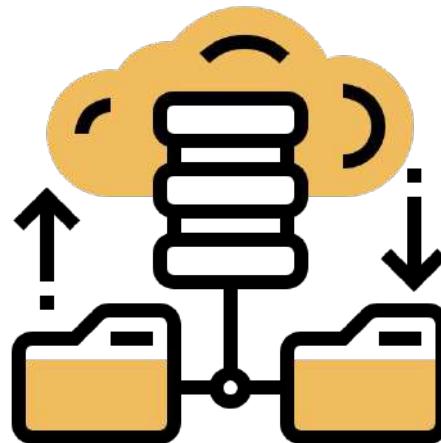
Xác định **mức độ nghiêm trọng**, tác động và khả năng phục hồi của sự cố giúp có các giải pháp phù hợp để khắc phục các vấn đề.



Vấn đề đánh cắp dữ liệu

Đánh cắp dữ liệu (data exfiltration) là việc **chuyển** dữ liệu trái phép từ máy tính.

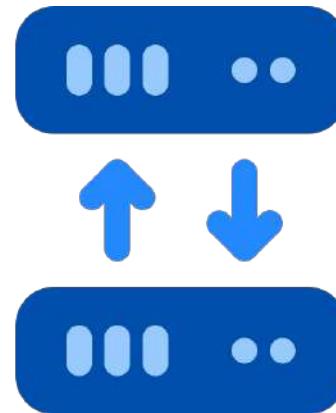
- Bản sao lưu thường xuyên giúp khắc phục một phần vấn đề đánh cắp dữ liệu.



Khôi phục hệ thống

Một số cách để khôi phục hệ thống:

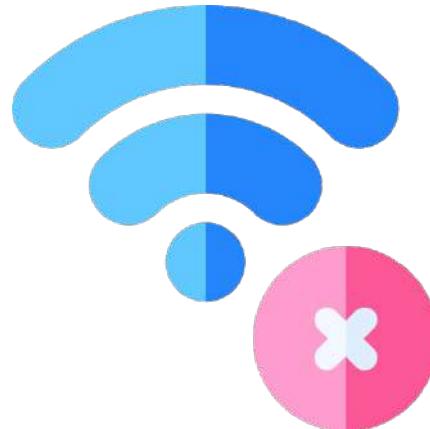
- Xóa phần mềm độc hại.
- Cài đặt lại hệ thống.
- Khôi phục từ bản sao.



Cách ly trước khi khôi phục

Trước khi khôi phục, cần cách ly hệ thống:

- **Tắt hệ thống bị sự cố.**
- **Ngắt mạng, loại bỏ quyền truy cập từ xa.**



Phân tích pháp y

Trong phân tích pháp y, các máy bị ảnh hưởng cần được **sao chụp đĩa trước khi phân tích** để tránh các nguy cơ bị sửa đổi, ảnh hưởng đến bằng chứng pháp y.



Vá lỗ hổng

- Xác định lỗ hổng để khắc phục, tránh bị lặp lại trong tương lai.
- Xem xét kỹ lưỡng để đảm bảo không còn **backdoor** trong hệ thống.



Kiểm tra hồi phục

- Sau khi đã dọn dẹp và vá các lỗ hổng, chúng ta cần **kiểm tra hệ thống** để đảm bảo các chức năng thích hợp đã được khôi phục hoàn toàn.
- **Bật tính năng theo dõi và ghi nhật ký** để đánh giá thêm.



Nội dung

-  Mục tiêu bảo mật
-  Quét lỗ hổng bảo mật
-  Quyền riêng tư
-  Người dùng
-  Bên thứ ba
-  Văn hóa bảo mật
-  Xử lý và khắc phục sự cố
-  **Bảo mật điện thoại**

Bảo mật thiết bị di động

Một số biện pháp để bảo mật thiết bị di động:

- **Bật khóa màn hình.**
- **Mã hóa bộ nhớ trên thiết bị.**
- **Quản lý quyền truy cập của các ứng dụng.**





Tổng kết



Những điều cần nắm

- Xác định và nhận ra được các rủi ro bảo mật, lỗ hổng bảo mật và các mối đe dọa.
- Trình bày được về mã hóa, ý nghĩa, các loại và các ứng dụng mã hóa
- Mô tả được ba thành phần trong bảo mật AAA và chọn lựa được phương pháp thích hợp
- Mô tả được các cuộc tấn công bảo mật phổ biến và các cách để phòng tránh
- Trình bày được các phương pháp xử lý sự cố đến từ hệ thống, thiết bị và con người





THANK YOU

