

Khái niệm về an toàn mạng không dây

An ninh an toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những hiểm họa, lỗi và sự tác động không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất.



Các kiểu tấn công mạng WLAN

Tấn công bị động (Passive attacks)

Đây là loại tấn công mà kẻ tấn công chỉ nghe trộm thông tin truyền qua mạng mà không làm thay đổi dữ liệu hoặc tương tác với các thiết bị.

Tấn công chủ động (Active attacks)

Loại tấn công này liên quan đến việc kẻ tấn công can thiệp vào giao tiếp hoặc dữ liệu truyền qua mạng Wi-Fi.

Tấn công kiểu chèn ép (Jamming attacks)

Đây là loại tấn công mà kẻ tấn công gửi ra tín hiệu nhiễu hoặc tín hiệu mạng giả mạo để làm gián đoạn hoặc ngăn chặn kết nối mạng không dây

Tấn công theo kiểu thu hút (Man-in-the-middle attacks)

Đây là loại tấn công mà kẻ tấn công can thiệp vào giao tiếp giữa hai bên mà không hề được họ biết.

Tấn công lặp lại (Replay attacks)

Đây là loại tấn công mà kẻ tấn công gửi lại một gói tin đã được ghi lại trước đó để tái tạo một hành động hoặc tạo ra sự xâm nhập.

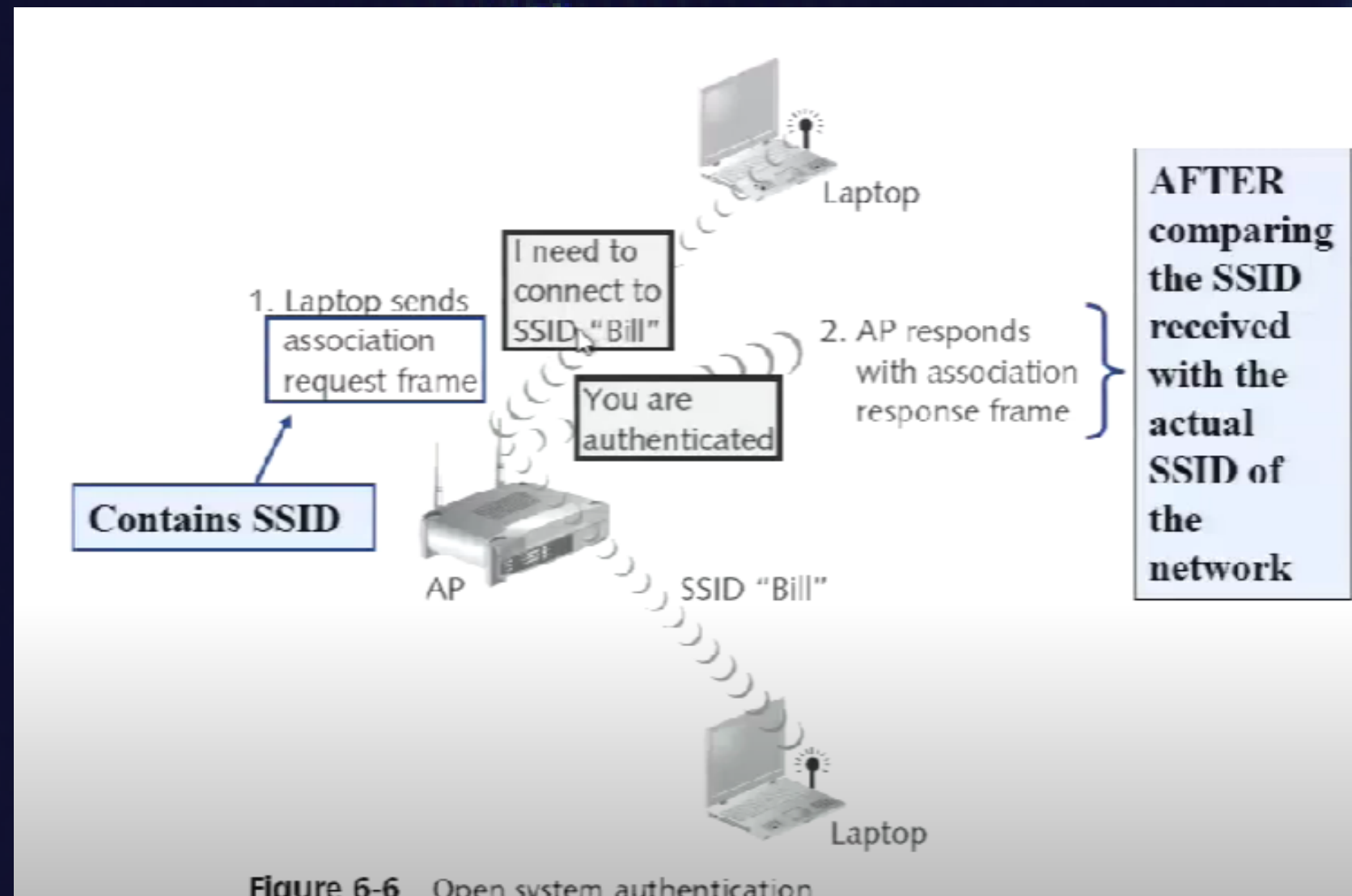
...

Lỗi hồng trong xác thực hệ thống mở.
Lỗi hồng trong xác thực khóa chia sẻ.
Lỗi hồng trong xác thực địa chỉ MAC.

...



LỖ HỒNG BẢO MẬT CHUẨN 802.11



Yêu cầu kết nối: Khi một thiết bị không dây muốn kết nối vào mạng, nó gửi yêu cầu kết nối tới một Access Point (AP) gần nhất.

Yêu cầu SSID: AP phản hồi bằng việc gửi một tin nhắn yêu cầu thiết bị cung cấp SSID (Service Set Identifier). SSID là tên của mạng Wi-Fi mà thiết bị đang cố gắng kết nối vào.

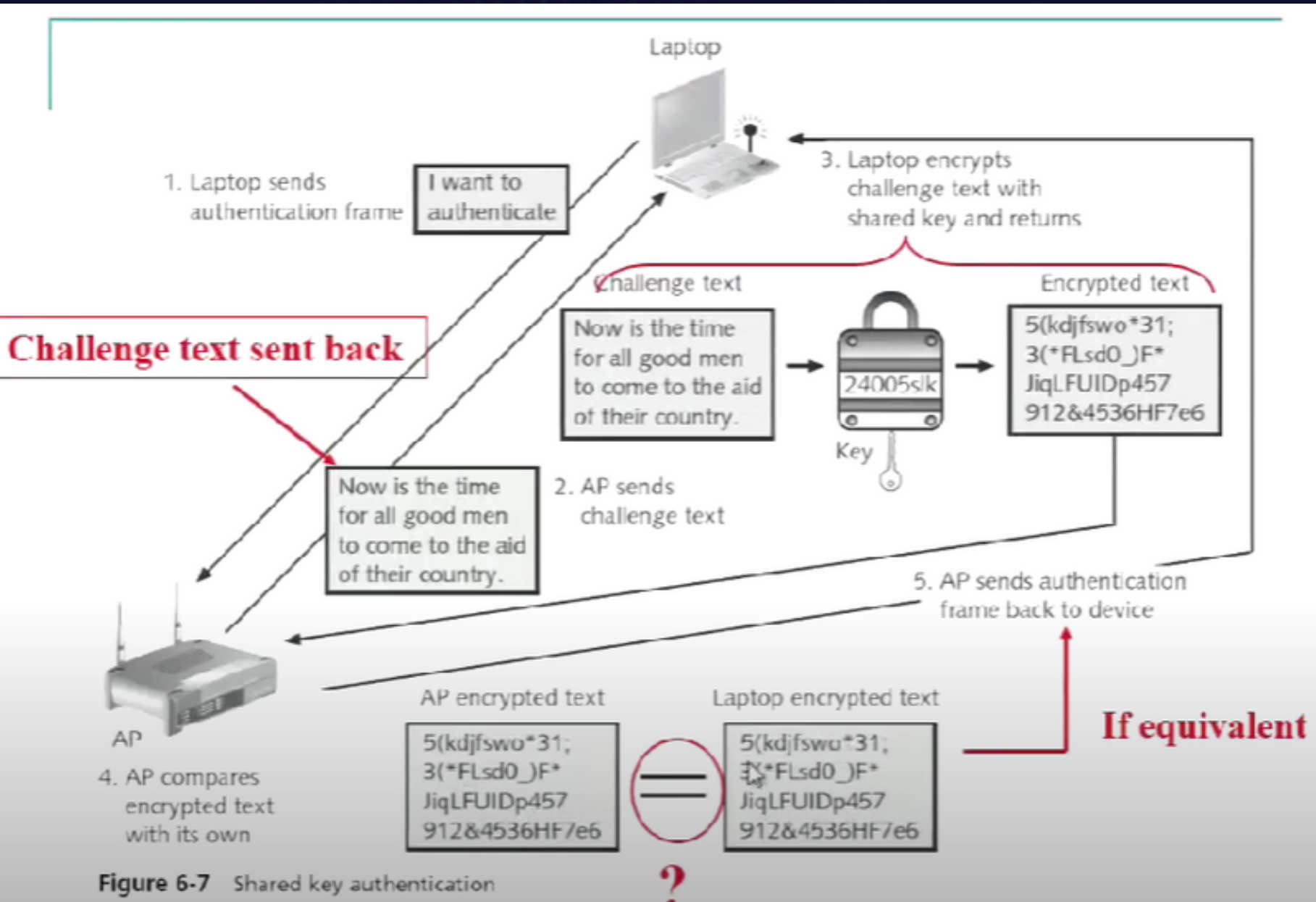
So sánh SSID: Thiết bị gửi lại một tin nhắn chứa SSID mà nó muốn kết nối vào. AP nhận tin nhắn này và so sánh SSID được cung cấp với SSID thực mà nó đang phát sóng.

Xác thực: Nếu SSID được cung cấp bởi thiết bị trùng khớp với SSID mà AP đang phát, AP chấp nhận yêu cầu kết nối và cho phép thiết bị vào mạng. Trong xác thực hệ thống mở, không có bước xác thực bổ sung khác.

Kết nối: Sau khi xác thực thành công, thiết bị được kết nối vào mạng và có thể truy cập vào các dịch vụ và tài nguyên mạng khác nhau.

--> Phương thức này được gọi là "hệ thống mở" vì không có bất kỳ quá trình xác thực mật khẩu hoặc chứng thực nào giữa thiết bị và AP. Nó thường được sử dụng trong các mạng công cộng hoặc mạng không đòi hỏi tính bảo mật cao.

Lỗ hổng trong xác thực hệ thống mở



Yêu cầu kết nối từ laptop: Laptop muốn kết nối vào mạng Wi-Fi và gửi yêu cầu kết nối tới Access Point (AP) trong phạm vi của nó.

Phản hồi từ AP: AP phản hồi bằng việc gửi một gói tin yêu cầu xác thực. Trong quá trình này, AP cũng gửi một chuỗi ký tự ngẫu nhiên, được gọi là "challenge string" đến laptop.

Laptop gửi lại phản ứng xác thực: Laptop nhận được "challenge string" từ AP và sử dụng nó để mã hóa bằng khóa chia sẻ đã được cấu hình trước đó. Sau đó, nó gửi chuỗi mã hóa này kèm theo yêu cầu xác thực tới AP.

AP giải mã và so sánh: AP nhận được phản ứng từ laptop và sử dụng khóa chia sẻ đã được cấu hình trước đó để giải mã chuỗi được gửi từ laptop. Sau đó, AP so sánh chuỗi đã giải mã với chuỗi ban đầu mà nó đã gửi tới laptop.

Xác thực thành công hoặc thất bại: Nếu chuỗi đã giải mã từ laptop trùng khớp với chuỗi ban đầu từ AP, thì quá trình xác thực được coi là thành công và laptop được phép truy cập vào mạng Wi-Fi. Ngược lại, nếu không khớp, quá trình xác thực sẽ thất bại và laptop sẽ không được kết nối.

--> Nếu khóa chia sẻ không được giữ bí mật hoặc bị lộ, thì mạng Wi-Fi sẽ trở nên dễ bị tấn công

Lỗ hổng trong xác thực hệ thống mở

Địa chỉ MAC được truyền mà không được mã hóa trong tất cả frame 802.11 như được yêu cầu trong chuẩn 802.11. Nhờ đó hacker có thể biết được địa chỉ MAC và giả dạng địa chỉ MAC hợp lệ đó để truy cập vào mạng.

Mục đích của địa chỉ MAC: Mục đích chính của địa chỉ MAC không phải là để ẩn thông tin hoặc bảo mật dữ liệu mà thay vào đó là để điều hướng và kiểm soát truy cập vào mạng. Nó giúp AP và các thiết bị trong mạng nhận diện và giao tiếp với nhau.



Lỗ hổng trong xác thực địa chỉ MAC.



Kẻ giả mạo

Đây là những kẻ xâm nhập sử dụng các phương pháp giả mạo để truy cập vào hệ thống mạng hoặc tài khoản của người khác



Kẻ lạm quyền.

Đây là những kẻ xâm nhập sử dụng quyền truy cập hoặc thông tin mà họ không được phép để thực hiện các hành động không đúng đắn hoặc gây hại.



Kẻ bí mật

Một cá nhân nắm được quyền kiểm soát giám sát đối với hệ thống và sử dụng quyền kiểm soát này để lẩn trốn quyền kiểm soát giám sát của administrator.

NGƯỜI XÂM NHẬP (INTRUDERS)

Các mẫu hành vi xâm nhập

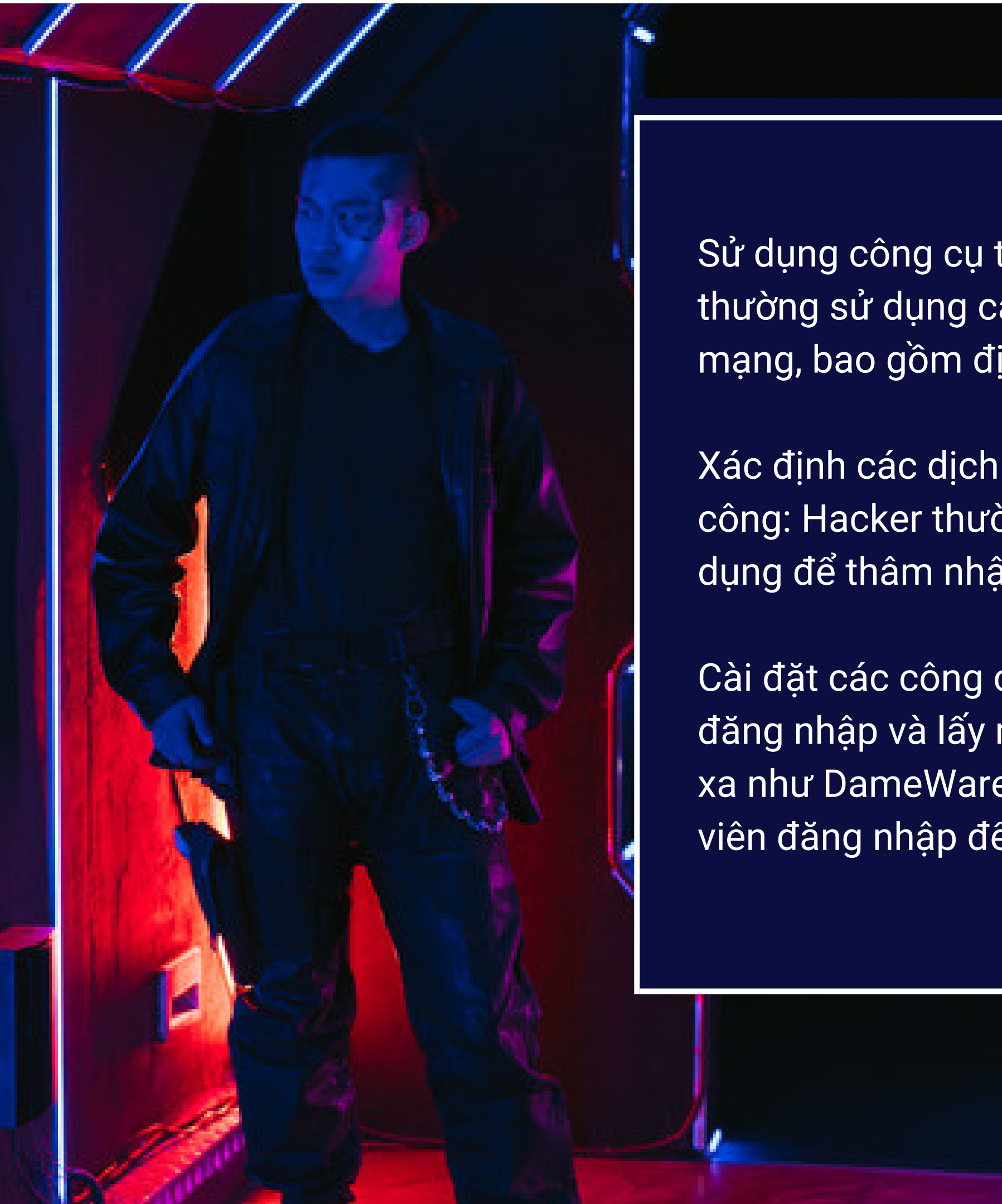
Các kỹ thuật và mô hình hành vi của những kẻ xâm nhập liên tục thay đổi, để khai thác các điểm yếu mới được phát hiện, trốn tránh các biện pháp phát hiện và đối phó

Có 3 mẫu hành vi xâm nhập như sau

Hacker

Tội phạm doanh nghiệp

Tấn công nội bộ

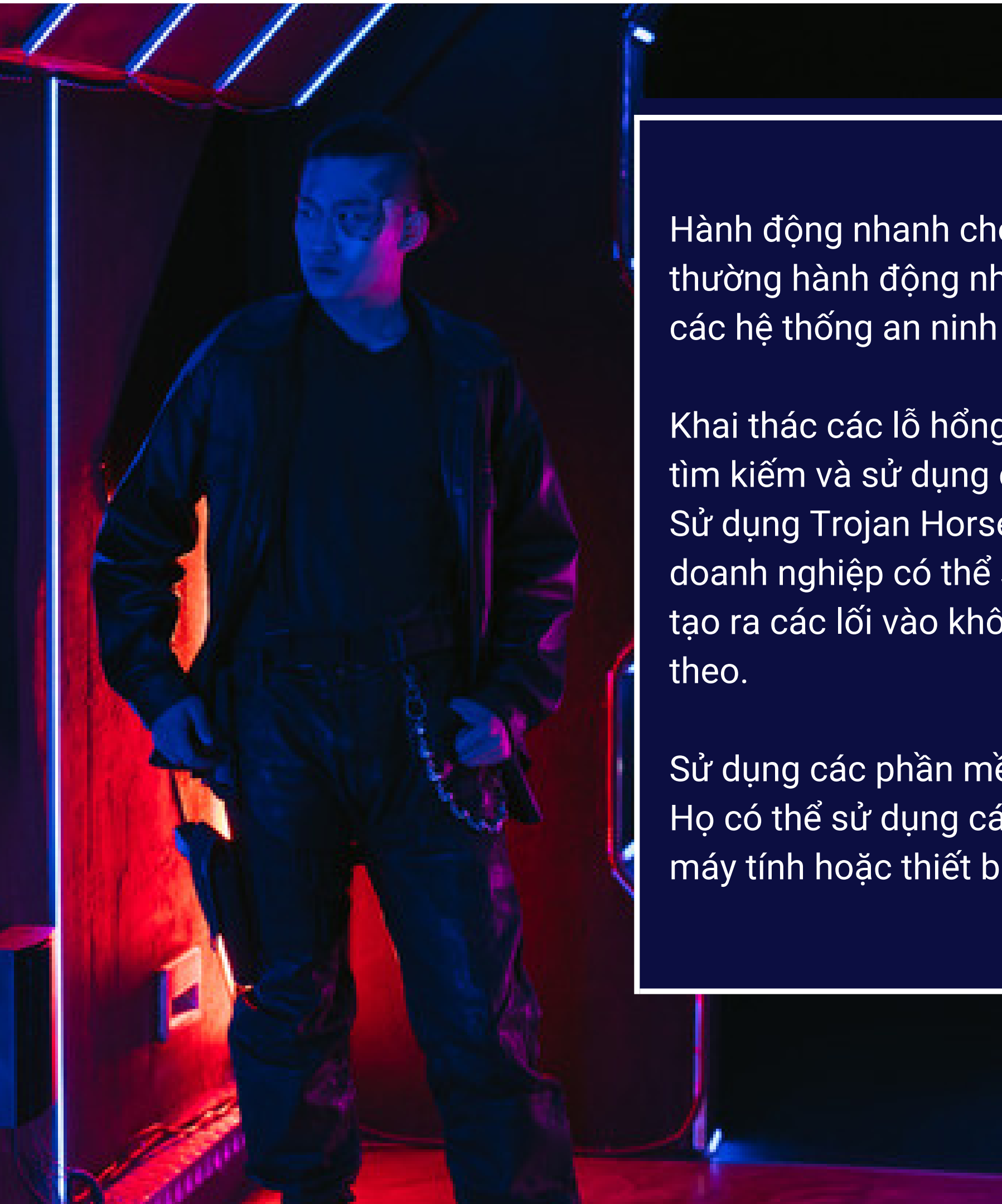


Sử dụng công cụ tra cứu IP như NSLookup để tìm kiếm mục tiêu: Hacker thường sử dụng các công cụ như NSLookup để tìm kiếm thông tin về mạng, bao gồm địa chỉ IP của các hệ thống mục tiêu.

Xác định các dịch vụ có khả năng bị tấn công để tiến hành các cuộc tấn công: Hacker thường tìm kiếm các dịch vụ và ứng dụng mà họ có thể tận dụng để thâm nhập vào hệ thống.

Cài đặt các công cụ quản trị từ xa như DameWare để đợi quản trị viên đăng nhập và lấy mật khẩu: Hacker có thể sử dụng các công cụ quản trị từ xa như DameWare để tạo ra các cửa sau vào hệ thống, sau đó đợi quản trị viên đăng nhập để thu thập thông tin đăng nhập của họ.

Hacker

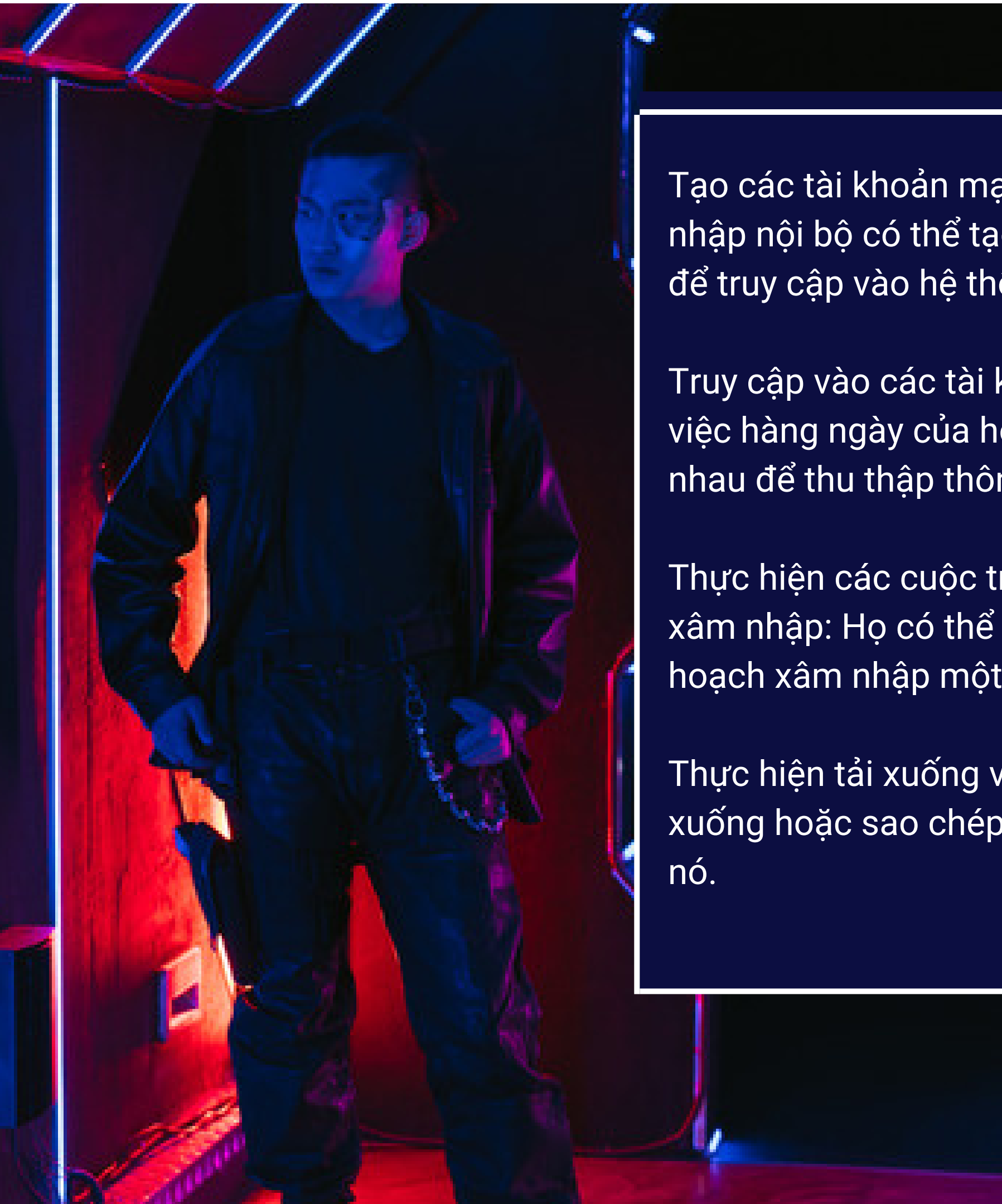


Hành động nhanh chóng và chính xác để tránh bị phát hiện: Tội phạm doanh nghiệp thường hành động nhanh chóng và có kế hoạch cẩn thận để tránh bị phát hiện bởi các hệ thống an ninh mạng.

Khai thác các lỗ hổng trong hệ thống thông qua các cổng dễ bị tấn công: Họ thường tìm kiếm và sử dụng các lỗ hổng trong hệ thống để tiến hành các cuộc tấn công. Sử dụng Trojan Horses để tạo cửa sau cho các cuộc tấn công sau này: Tội phạm doanh nghiệp có thể sử dụng Trojan Horses (phần mềm độc hại được giấu kín) để tạo ra các lối vào không nhìn thấy trên hệ thống để thực hiện các cuộc tấn công tiếp theo.

Sử dụng các phần mềm giám sát để lấy mật khẩu hoặc thông tin đăng nhập khác: Họ có thể sử dụng các phần mềm giám sát để đánh cắp thông tin đăng nhập từ các máy tính hoặc thiết bị mạng trong môi trường doanh nghiệp.

Tội phạm doanh nghiệp



Tạo các tài khoản mạng cho bản thân và bạn bè để truy cập vào hệ thống: Kẻ xâm nhập nội bộ có thể tạo các tài khoản mạng giả mạo hoặc lợi dụng tài khoản hiện có để truy cập vào hệ thống một cách trái phép.

Truy cập vào các tài khoản và ứng dụng mà họ thường không sử dụng cho công việc hàng ngày của họ: Họ có thể truy cập vào các tài khoản hoặc ứng dụng khác nhau để thu thập thông tin hoặc thực hiện các hoạt động xâm nhập.

Thực hiện các cuộc trò chuyện nhắn tin lén lút để trao đổi thông tin hoặc kế hoạch xâm nhập: Họ có thể sử dụng các dịch vụ nhắn tin để trao đổi thông tin hoặc kế hoạch xâm nhập một cách không phát hiện.

Thực hiện tải xuống và sao chép các tệp lớn từ hệ thống: Kẻ xâm nhập có thể tải xuống hoặc sao chép các tệp dữ liệu quan trọng từ hệ thống để sử dụng hoặc tiết lộ nó.

Tấn công nội bộ

- ✓ Sự xâm nhập được phát hiện càng sớm, lượng thiệt hại càng ít và khả năng phục hồi càng nhanh.



PHÁT HIỆN XÂM NHẬP

Các cách tiếp cận để phát hiện xâm nhập

- ✓ **Phát hiện bất thường thống kê**
thu thập các hành vi của người dùng hợp pháp và không hợp pháp. Sau đó, thống kê được áp dụng cho hành vi quan sát được để xác định với mức độ tin cậy cao của các hành vi. Phát hiện bất thường từ thống kê có 2 loại: phát hiện ngưỡng và phát hiện dựa trên hồ sơ.
- ✓ **Phát hiện luật cơ bản**
Đây là một cách tiếp cận cơ bản để phát hiện xâm nhập bằng cách xác định một tập hợp các quy tắc (hay luật) có thể được sử dụng để quyết định rằng một hành vi nhất định là của một kẻ xâm nhập: Phát hiện bất thường (Anomaly Detection), Nhận dạng thâm nhập (Signature Detection)

Phát hiện ngưỡng:

- Cách tiếp cận này liên quan đến việc xác định các ngưỡng hoặc giới hạn cho tần suất xuất hiện của các sự kiện khác nhau trong hệ thống.
- Mỗi loại sự kiện có thể được thiết lập một ngưỡng tần suất tối đa cho phép. Nếu số lần xuất hiện của sự kiện đó vượt quá ngưỡng đã định, hệ thống sẽ cảnh báo hoặc thậm chí ngăn chặn hành vi đó.
- Ví dụ, nếu một người dùng cố gắng đăng nhập vào tài khoản của mình với mật khẩu sai quá số lần cho phép trong một khoảng thời gian ngắn, hệ thống có thể xem xét đó là một hành vi đáng ngờ và thực hiện các biện pháp như chặn tài khoản đó.

Dựa trên hồ sơ:

- Cách tiếp cận này tập trung vào việc thu thập và sử dụng thông tin từ hồ sơ hoạt động của từng người dùng để phát hiện các thay đổi trong hành vi của các tài khoản.
- Mỗi người dùng sẽ có một hồ sơ về hoạt động của họ, bao gồm các mẫu thường xuyên sử dụng, vị trí đăng nhập, và các hoạt động khác.
- Khi có sự thay đổi đột ngột hoặc không bình thường trong hành vi của một người dùng, như đăng nhập từ một địa điểm không phổ biến hoặc truy cập vào các tài nguyên không thường xuyên, hệ thống có thể cảnh báo hoặc thậm chí tạm ngưng hoạt động của tài khoản đó cho đến khi xác minh được.

--> sử dụng các cơ chế tự động để nhận biết các biểu hiện không bình thường hoặc đáng ngờ trong hệ thống

Phát hiện bất thường thống kê

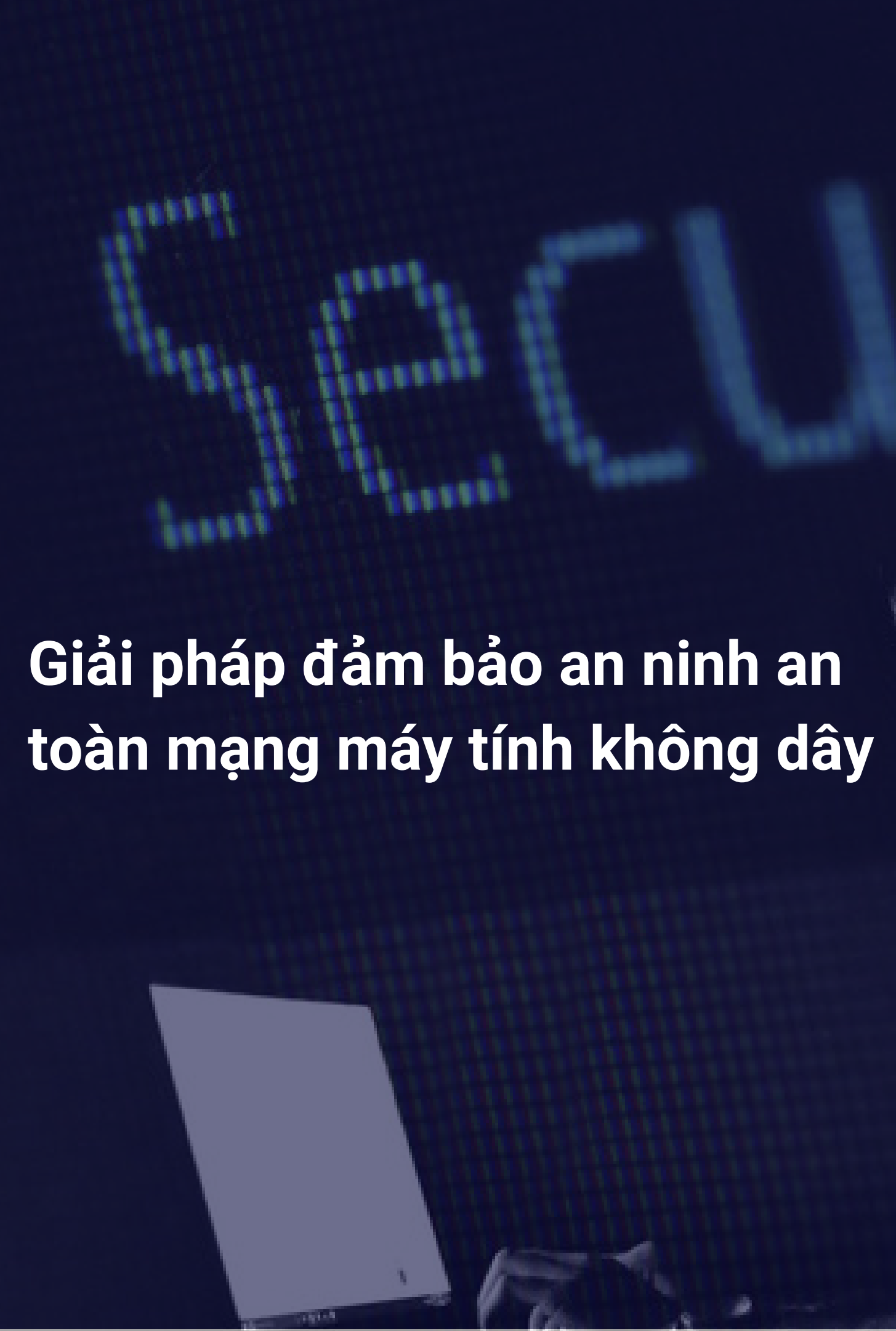
Nhận dạng thâm nhập (Signature Detection)

- Các quy tắc được phát triển để phát hiện sự lệch lạc so với các mẫu sử dụng trước đó (có thể là các mẫu hành vi bình thường).
- Ví dụ, nếu một hệ thống mạng thường chỉ nhận một lượng nhất định các yêu cầu từ một máy chủ trong một khoảng thời gian nhất định, một phát hiện bất thường có thể xảy ra nếu có một lượng lớn các yêu cầu đến từ cùng một máy chủ trong một thời gian ngắn.

Dựa trên hồ sơ:

- Đây là phương pháp tiếp cận chuyên môn nhằm tìm kiếm các hành vi đáng ngờ bằng cách so sánh với các mẫu đã biết của các cuộc tấn công.
- Ví dụ, một hệ thống IDS có thể sử dụng các chữ ký (signatures) của các loại tấn công đã biết để phát hiện và cảnh báo khi gặp phải các hành vi tương tự.

Phát hiện luật cơ bản



**Giải pháp đảm bảo an ninh an
toàn mạng máy tính không dây**

Bảo mật bằng WEP (Wired Equivalent Privacy)

Bảo mật bằng WPA (Wifi Protected Access)

Bảo mật bằng WPA2

Các công cụ bảo mật hệ thống

Bảo mật nhiều lớp

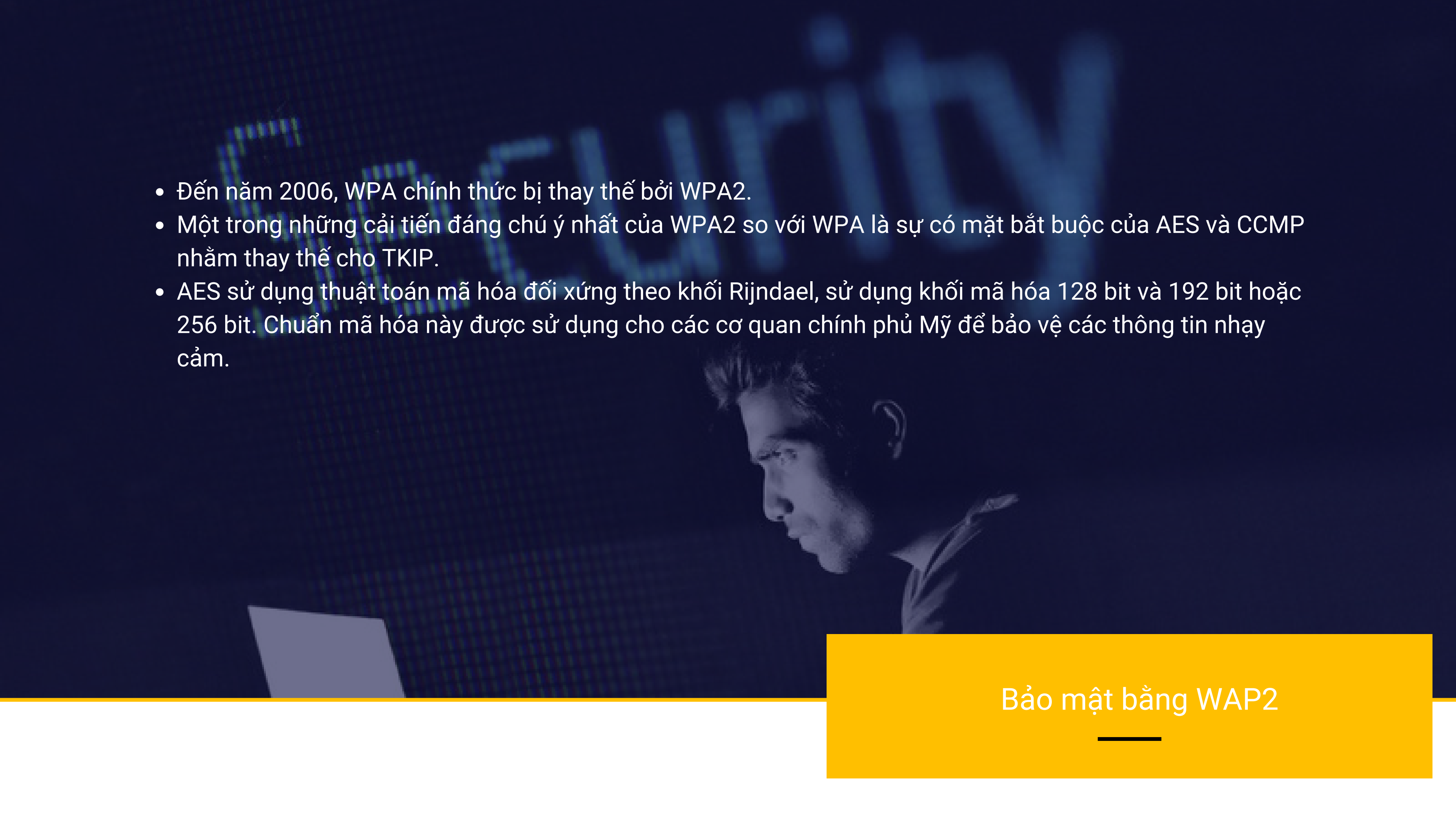
- WEP là một thuật toán bảo nhằm bảo vệ sự trao đổi thông tin chống lại sự nghe trộm, chống lại những kết nối mạng không được cho phép cũng như chống lại việc thay đổi hoặc làm nhiễu thông tin truyền.
- WEP sử dụng stream cipher RC4 cùng với một mã 40 bit và một số ngẫu nhiên 24 bit (initialization vector - IV) để mã hóa thông tin.
- Thông tin mã hóa được tạo ra bằng cách thực hiện phép toán XOR giữa keystream và plain text. Thông tin mã hóa và IV sẽ được gửi đến người nhận. Người nhận sẽ giải mã thông tin dựa vào IV và khóa WEP đã biết trước.



Bảo mật bằng WEP

- WPA là một giải pháp bảo mật được đề xuất bởi liên minh WiFi nhằm khắc phục những hạn chế của WEP. WPA được nâng cấp bằng việc cập nhật phần mềm SP2 của Microsoft.
- WPA cải tiến 3 điểm yếu nổi bật của WEP :
 - WPA cũng mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128 bit và IV có chiều dài là 48 bit. Một cải tiến của WPA là WPA sử dụng giao thức TKIP nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình trao đổi thông tin
 - WPA sử dụng 802.1x/EAP để đảm bảo tính nhận thực lẫn nhau chống lại kiểu tấn công xen vào giữa. Quá trình nhận thực dựa trên một server nhận thực (Radius/Diameter)
 - WPA sử dụng thuật toán kiểm tra tính toàn vẹn của bản tin MIC để tăng cường tính toàn vẹn của thông tin truyền.
- Những điểm yếu của WPA :
 - Điểm yếu đầu tiên của WPA là nó vẫn không giải quyết được kiểu tấn công từ chối dịch vụ. Kẻ phá hoại có thể làm
 - Ngoài ra, WPA vẫn sử dụng thuật toán RC4 mà có thể dễ dàng bị bẻ vỡ bởi tấn công FMS đã được đề xuất bởi những nhà nghiên cứu ở trường đại học Berkeley. nhiều mạng WPA WiFi bằng cách gửi ít nhất hai gói thông tin với một khóa sai mỗi giây

Bảo mật bằng WAP

- 
- Đến năm 2006, WPA chính thức bị thay thế bởi WPA2.
 - Một trong những cải tiến đáng chú ý nhất của WPA2 so với WPA là sự có mặt bắt buộc của AES và CCMP nhằm thay thế cho TKIP.
 - AES sử dụng thuật toán mã hóa đối xứng theo khối Rijndael, sử dụng khối mã hóa 128 bit và 192 bit hoặc 256 bit. Chuẩn mã hóa này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

Bảo mật bằng WAP2

- Các công cụ bảo mật hệ thống :
 - Chứng thực bằng địa chỉ MAC
 - Chứng thực bằng SSID
- Bảo mật nhiều lớp :
 - Dựa trên lý thuyết thì mô hình bảo mật an toàn nhất cho bất cứ mạng vô tuyến nào chính là sự kết hợp các phương pháp bảo mật nhỏ lại với nhau (WEP, WPA, WPA2, Firewall, VPN, Radius Server, lọc địa chỉ MAC). Sự kết hợp giữa các phương pháp bảo mật này sẽ tạo ra cơ chế bảo mật nhiều lớp.
 - Bởi vì mỗi giải pháp bảo mật chỉ nhằm phục vụ một mục đích khác nhất định nào đó nên kết hợp chúng lại thì sẽ giúp dữ liệu được an toàn dưới nhiều dạng tấn công hơn

Bảo mật khác
