**TCVN** **T I Ê U C H U Ẩ N Q U Ố C G I A**

**TCVN xxxx-6:2024**

**Xuất bản lần 1**

**CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – AN TOÀN MẠNG – PHẦN 6: CÁC YÊU CẦU BẢO ĐẢM AN TOÀN THÔNG TIN CHO VIỆC TRUY NHẬP MẠNG KHÔNG DÂY IP**

***Information technology – Security techniques – Network security –
Part 6: Information security requirements for accessing wireless IP network***

**HÀ NỘI – 2024**

Mục lục

[Mục lục 2](#_Toc157156476)

[1 Phạm vi áp dụng 5](#_Toc157156477)

[2 Tài liệu viện dẫn 5](#_Toc157156478)

[3 Thuật ngữ và định nghĩa 6](#_Toc157156479)

[4 Ký hiệu và thuật ngữ viết tắt 7](#_Toc157156480)

[5 Các nguy cơ mất an toàn thông tin đối với mạng không dây IP 10](#_Toc157156481)

[5.1 Thông tin chung 10](#_Toc157156482)

[5.2 Truy cập trái phép 11](#_Toc157156483)

[5.3 Theo dõi gói tin (Packet sniffing) 11](#_Toc157156484)

[5.4 Điểm truy cập không dây giả mạo 12](#_Toc157156485)

[5.5 Tấn công từ chối dịch vụ (DoS) 13](#_Toc157156486)

[5.6 Bluejacking 14](#_Toc157156487)

[5.7 Bluesnarfing 14](#_Toc157156488)

[5.8 Mạng Adhoc 14](#_Toc157156489)

[5.9 Các mối đe dọa khác 14](#_Toc157156490)

[6 Danh mục các yêu cầu an toàn cơ bản cho mạng không dây IP 15](#_Toc157156491)

[6.1 Thông tin chung 15](#_Toc157156492)

[6.2 Tính bí mật 15](#_Toc157156493)

[6.3 Tính toàn vẹn 15](#_Toc157156494)

[6.4 Tính khả dụng 16](#_Toc157156495)

[6.5 Xác thực 16](#_Toc157156496)

[6.6 Phân quyền truy cập 17](#_Toc157156497)

[6.7 Trách nhiệm giải trình (Không thoái thác) 17](#_Toc157156498)

[7 Các biện pháp kiểm soát bảo mật đối với mạng không dây IP 18](#_Toc157156499)

[7.1 Các mục tiêu an toàn cho môi trường hoạt động 18](#_Toc157156500)

[7.2 Kiểm soát và triển khai mã hóa 18](#_Toc157156501)

[7.3 Đánh giá tính toàn vẹn 20](#_Toc157156502)

[7.4 Xác thực 20](#_Toc157156503)

[7.5 Kiểm soát truy cập 22](#_Toc157156504)

[7.5.1 Tổng quan 22](#_Toc157156505)

[7.5.2 Kiểm soát quyền truy cập 22](#_Toc157156506)

[7.5.3 Kiểm soát dựa trên mạng 23](#_Toc157156507)

[7.6 Khả năng phục hồi từ tấn công từ chối dịch vụ (DoS) 23](#_Toc157156508)

[7.7 Phân tách vùng DMZ thông qua bảo vệ tường lửa 23](#_Toc157156509)

[7.8 Quản lý lỗ hổng bảo mật thông qua cấu hình an toàn và tăng cường bảo mật cho thiết bị 24](#_Toc157156510)

[7.9 Giám sát liên tục các mạng không dây 24](#_Toc157156511)

[8 Phương án thiết kế và cấu hình bảo mật cho mạng không dây IP 24](#_Toc157156512)

[8.1 Tổng quan 24](#_Toc157156513)

[8.2 Wi-fi 25](#_Toc157156514)

[8.2.1. Tổng quan 25](#_Toc157156515)

[8.2.2. Xác thực người dùng 26](#_Toc157156516)

[8.2.3. Bảo mật và toàn vẹn thông tin 27](#_Toc157156517)

[8.2.4. Công nghệ Wi-fi không dây 27](#_Toc157156518)

[8.2.5. Các cấu hình Wi-fi khác 27](#_Toc157156519)

[8.2.6. Kiểm soát truy cập – Thiết bị người dùng 28](#_Toc157156520)

[8.2.7. Kiểm soát truy cập – Điểm truy cập cơ sở hạ tầng 28](#_Toc157156521)

[8.2.8. Khả năng sẵn có 29](#_Toc157156522)

[8.2.9. Trách nhiệm giải trình 30](#_Toc157156523)

[8.3 Thiết kế bảo mật cho di động viễn thông 30](#_Toc157156524)

[8.4 Bluetooth 31](#_Toc157156525)

[8.5 Các công nghệ không dây khác 33](#_Toc157156526)

[Thư mục tài liệu tham khảo 34](#_Toc157156527)

1. **Lời nói đầu**
2. TCVN 9801-6:2024 được xây dựng trên dựa trên cơ sở chấp nhận nguyên vẹn một phần tiêu chuẩn ISO/IEC 27033-6:2016.
3. TCVN 9801-6:2024 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

**Công nghệ thông tin – Các kỹ thuật an toàn – An toàn mạng – Phần 6: Các yêu cầu bảo đảm an toàn thông tin cho việc truy nhập mạng không dây IP**

TIÊU CHUẨN QUỐC GIA TCVN 9801-6:2024

*Information technology – Security techniques – Network security – Part 6: Information security requirements for accessing wireless IP network*

* 1. Phạm vi áp dụng

Tiêu chuẩn này là một phần của bộ tiêu chuẩn TCVN 9801 (ISO/IEC 27033) nhằm mô tả các mối đe dọa, các yêu cầu an toàn, kiểm soát an toàn và các kỹ thuật thiết kế liên quan đến các mạng không dây. Nó cung cấp các hướng dẫn cho việc lựa chọn, thực thi và giám sát của các biện pháp kiểm soát kỹ thuật cần thiết để cung cấp thông tin liên lạc an toàn sử dụng các mạng không dây.

Tiêu chuẩn này được áp dụng khi xem xét hoặc lựa chọn các tùy chọn kiến trúc/thiết kế kỹ thuật an toàn liên quan đến việc sử dụng các mạng không dây theo TCVN 9801-2:2015 (ISO/IEC 27033-2).

Nhìn chung, tiêu chuẩn này sẽ hỗ trợ đáng kể cho việc xác định và triển khai toàn diện vấn đề bảo mật cho môi trường mạng không dây của bất kỳ tổ chức nào. Nó nhằm vào người dùng và người triển khai chịu trách nhiệm triển khai và duy trì các biện pháp kiểm soát kỹ thuật cần thiết để cung cấp mạng không dây an toàn.

* 1. Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng đối với tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả phiên bản sửa đổi, bổ sung).

TCVN 11238:2015 (ISO/IEC 27000:2014), “Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và từ vựng”.

TCVN 9801-1:2022 (ISO/IEC 27033-1:2015), “Công nghệ thông tin – Các kỹ thuật an toàn – An toàn mạng – Phần 1: Tổng quan và khái niệm”.

TCVN 9801-2:2015 (ISO/IEC 27033-2:2012), “Công nghệ thông tin – Các kỹ thuật an toàn – An toàn mạng – Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng”.

* 1. Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 11238:2015, TCVN 9801-1:2022 và các thuật ngữ sau:

**Điểm truy cập / Điểm truy cập không dây**

Thiết bị hoặc một phần thiết bị cho phép một mạng không dây nội bộ kết nối đến một mạng có dây.

Chú thích: Kết nối sử dụng một mạng không dây nội bộ (WLAN) hoặc tiêu chuẩn có liên quan.

**Trạm cơ sở / Trạm cơ sở không dây**

Thiết bị cung cấp kết nối giữa điện thoại di động hoặc điện thoại di động và mạng truyền thông lõi.

**Bluetooth**

Chuẩn công nghệ không dây để trao đổi dữ liệu trong khoảng cách ngắn.

Chú thích: “Bluetooth” là nhãn hiệu thuộc quyền sở hữu bởi Bluetooth SIG.

**Mạng lõi**

Một phần của mạng viễn thông di động kết nối mạng truy cập với mạng truyền thông rộng hơn.

Ví dụ: Internet hoặc các mạng công cộng khác là các ví dụ của mạng truyền thông rộng hơn.

**Trạm tế bào (femto cell) / trạm nhà / trạm nhỏ**

Trạm cơ sở di động nhỏ, công suất thấp.

Chú thích: Trạm tế bào thường được thiết kế để sử dụng trong gia đình hoặc doanh nghiệp nhỏ.

**Cứng hóa (Hardening)**

Quá trình bảo mật một hệ thống bằng cách giảm bề mặt dễ bị tổn thương của nó.

Chú thích: Việc cứng hóa thường bao gồm việc loại bỏ phần mềm không cần thiết, tên người dùng hoặc thông tin đăng nhập không cần thiết và việc vô hiệu hóa hoặc loại bỏ các dịch vụ không cần thiết.

**Giao tiếp máy-máy (machine to machine)**

Công nghệ cho phép cả hệ thống không dây và có dây giao tiếp với các thiết bị khác cùng loại.

**Tỷ lệ công suất / Tỷ lệ tín hiệu trên tạp âm**

Thước đo so sánh mức tín hiệu mong muốn với mức nhiễu nền.

Chủ thích: Được định nghĩa là tỷ số giữa công suất tín hiệu và công suất nhiễu.

**Mạng truy cập vô tuyến**

Một phần của hệ thống viễn thông di động triển khai công nghệ truy cập vô tuyến như WCDMA hoặc LTE để cung cấp quyền truy cập cho các thiết bị người dùng cuối vào mạng lõi.

Chú thích 1: Mạng truy cập vô tuyến nằm giữa thiết bị người dùng cuối và mạng lõi.

Chú thích 2: Điện thoại di động là một ví dụ về thiết bị của người dùng cuối.

**Bộ điều khiển mạng vô tuyến**

Phần tử mạng trong mạng di động 3G điều khiển các trạm gốc, giao tiếp với mạng lõi và thực hiện các chức năng quản lý tài nguyên vô tuyến và quản lý di động của mạng.

**Wi-fi**

Công nghệ mạng cục bộ không dây cho phép các thiết bị điện tử kết nối mạng, chủ yếu sử dụng băng tần vô tuyến 2,5 GHz và 5 GHz.

Chú thích 1: “Wi-fi” là nhãn hiệu của Wi-Fi Alliance.

Chú thích 2: “Wi-Fi” thường được sử dụng đồng nghĩa với “WLAN” vì hầu hết các mạng WLAN hiện đại đều dựa trên các tiêu chuẩn này.

**Mạng Wi-fi Ad-Hoc / mạng ad-hoc không dây**

Mạng không dây phi tập trung không dựa vào cơ sở hạ tầng có sẵn.

Chú thích: Ví dụ về cơ sở hạ tầng có sẵn là bộ định tuyến trong mạng có dây hoặc điểm truy cập trong mạng không dây (cơ sở hạ tầng) được quản lý.

* 1. Ký hiệu và thuật ngữ viết tắt

|  |  |  |
| --- | --- | --- |
| 3G | Third Generation of mobile telecommunications technology  |  |
| 3GPP | Third Generation Partnership Program |  |
| 4G | Fourth Generation of mobile telecommunications technology |  |
| AAA | Authentication, Authorization, and Accounting |  |
| AES | Advanced Encryption Standard |  |
| AP | Access Point |  |
| ASE | Authentication Service Entity |  |
| BYOD | Bring Your Own Device |  |
| CCM | CTR with CBC Message authentication code |  |
| CCMP | Cipher Block Chaining Message Authentication Code Protocol |  |
| CISO | Chief Information Security Officer |  |
| DMZ | De-Militarized Zone |  |
| DoS | Denial of Service |  |
| EAP | Extensible Authentication Protocol |  |
| FTP | File Transfer Protocol |  |
| HTTP | Hyper Text Transfer Protocol |  |
| GHz | gigahertz |  |
| ICT | Information and Communications Technology |  |
| IDS | Intrusion Detection System |  |
| IEEE | Institute of Electrical and Electronics Engineers |  |
| IMAP | Internet message access protocol |  |
| IMEI | International Mobile Equipment Identity |  |
| IMS | Internet Protocol (IP) Multimedia Subsystem |  |
| IMSI | International Mobile Subscriber Identity |  |
| IPS | Intrusion Prevention System |  |
| IPsec | Internet Protocol Security |  |
| ISM | Industrial, Scientific and Medical |  |
| ISP | Internet Service Provider |  |
| IT | Information Technology |  |
| LTE | Long Term Evolution |  |
| MAC | Media Access Control |  |
| MIC | Message Interface Code |  |
| NIC | Network Interface Card |  |
| OBEX | Object exchange |  |
| PDA | Personal Digital Assistant |  |
| PEAP-GTC | Protected EAP - Generic Token Card |  |
| PIN | Personal Identification Number |  |
| PKI | Public Key Infrastructure |  |
| PLMN | Public Land Mobile Network |  |
| POP | Post Office Protocol |  |
| RAN | Radio Access Network |  |
| RBAC | Role Based Access Control |  |
| RF | Radio Frequency |  |
| RFCOMM | RF Communication |  |
| SAC | Standardization Administration of China |  |
| SAE | System Architecture Evolution |  |
| SIG | Special Interest Group |  |
| SLA | Service Level Agreement |  |
| SIM | Subscriber Identity Module |  |
| SNMP | Simple Network Management Protocol |  |
| SMTP | Simple Mail Transfer Protocol |  |
| SSH | Secure Shell |  |
| SSID | Service Set Identifier |  |
| STA | STAtion |  |
| TCP | Transmission Control Protocol |  |
| TLS | Transport Layer Security |  |
| TTLS | Tunnelled Transport Layer Security |  |
| UE | User Equipment |  |
| UEA1 | UMTS Encryption Algorithm #1 |  |
| UHF | Ultra High Frequency |  |
| UICC | Universal Integrated Circuit Card |  |
| UMTS | Universal Mobile Telecommunications System |  |
| USB | Universal Serial Bus |  |
| UWB | Ultra-Wide Band |  |
| VLAN | Virtual Local Area Network (LAN) |  |
| VPN | Virtual Private Network |  |
| WAI | WLAN Authentication Infrastructure |  |
| WAPI | WLAN Authentication and Privacy Infrastructure |  |
| WEP | Wireless Equivalent Privacy |  |
| WIDS | Wireless Intrusion Detection System |  |
| WIPS | Wireless Intrusion Prevention System |  |
| WLAN | Wireless Local Area Network |  |
| WMAN | Wireless Metropolitan Area Network |  |
| WNIC | Wireless Network Interface Controller |  |
| WPA | Wi-Fi Protected Access |  |
| WPA2 | Wi-Fi Protected Access 2 |  |
| WPAN | Wireless Personal Area Network |  |
| WPA-PSK | Wi-Fi Protected Access Pre-Shared Key |  |
| WPI | WLAN Privacy Infrastructure |  |
| WRAN | Wireless Regional Area Networks |  |
| WWAN | Wireless Wide Area Networks |  |

* 1. Các nguy cơ mất an toàn thông tin đối với mạng không dây IP
		1. Thông tin chung

Điều 7 liệt kê những rủi ro bảo mật phổ biến đối với mạng không dây. Tuy nhiên, với sự phát triển của công nghệ không dây, các mối đe doạ mới sẽ xuất hiện kèm theo đó những mối đe doạ cũ sẽ không ngừng phát triển. Để đối mặt với thách thức này, người quản trị mạng không dây cần theo dõi sát sao tiến triển công nghệ, áp dụng biện pháp bảo mật mới và kỹ thuật hiện đại để đối phó với những rủi ro tiềm ẩn có thể xảy ra.

Khi ai đó truy cập mạng một cách trái phép, điều đó có thể gây ra những vấn đề nghiêm trọng như rò rỉ thông tin quan trọng, thay đổi dữ liệu, từ chối dịch vụ, và sử dụng tài nguyên mạng một cách bất hợp pháp. Sau khi kẻ xâm nhập đã truy cập được vào mạng, việc theo dõi dữ liệu không được bảo vệ có thể dẫn đến việc thu thập thông tin đăng nhập, như tên người dùng và mật khẩu. Thông tin này có thể được sử dụng cho các cuộc tấn công tiếp theo. Mạng không dây không chỉ phải đối mặt với các vấn đề bảo mật thông thường như mạng dây truyền thống, mà còn phải đối mặt với những nguy cơ đặc biệt liên quan đến việc sử dụng công nghệ không dây. Điều quan trọng là phần lớn các thiết bị không dây không thể giới hạn tín hiệu của chúng chỉ trong một khu vực an toàn. Các tín hiệu này có thể được giấu kín và sử dụng một cách âm thầm. Trong hệ thống mạng dây truyền thống, an ninh được xây dựng thông qua cơ sở hạ tầng vật lý như văn phòng hoặc trung tâm dữ liệu, vì người dùng phải kết nối vật lý để truy cập được tài nguyên, nhưng trong hệ thống mạng không dây, những biện pháp bảo vệ này không còn hiệu quả. Do đó, toàn bộ bối cảnh về mối đe dọa cần được xem xét lại và Điều khoản này mô tả một số mối đe dọa chính liên quan đến mạng không dây.

* + 1. Truy cập trái phép

Mạng không dây cũng phải đối mặt với những rủi ro từ việc truy cập trái phép, tương tự như mạng có dây. Việc truy cập trái phép vào mạng không dây có thể tạo ra những rủi ro về bảo mật, vì thông tin có sẵn có thể bị tiết lộ, mở ra khả năng thu thập thông tin chi tiết hơn. Chẳng hạn, việc biết được tên và cài đặt SSID có thể cung cấp những dấu hiệu quan trọng, giúp kẻ tấn công sau này có thể sử dụng mạng không dây một cách bất hợp pháp. Khi truy cập vào mạng không dây, người tấn công có thể sử dụng nó như một kênh để tiếp cận các tài nguyên khác trong mạng đã kết nối.

Việc ngăn chặn truy cập vào những tài nguyên này không nằm trong phạm vi của tiêu chuẩn ISO/IEC 27033.

* + 1. Theo dõi gói tin (Packet sniffing)

Trong trường hợp mạng Wi-Fi không sử dụng tính năng bảo mật mã hóa, việc nghe trộm kết nối trở nên khá đơn giản. Để thực hiện việc nghe trộm trên một mạng Wi-Fi như vậy, người tấn công cần sử dụng một ăng-ten cùng với các công cụ mạng không dây thông thường, và một chương trình phân tích gói tin mạng. Chương trình phân tích gói tin mạng (a network packet sniffer) là một loại phần mềm cho phép thiết bị mạng của người tấn công chuyển sang chế độ rảnh tay (promiscuous mode). Ở chế độ này, thiết bị sẽ nhận và xử lý mọi gói tin mạng mà nó phát hiện, không chỉ là những gói tin dành cho nó. Chương trình này sau đó hiển thị tất cả các gói tin mạng và giải mã chúng để người tấn công có thể dễ dàng đọc thông tin. Tất cả các dữ liệu truy cập văn bản thuần túy trên mạng có thể được đọc dễ dàng, và người tấn công có thể sử dụng bộ lọc để tìm kiếm từ khóa hoặc giá trị cụ thể. Các giao thức và dịch vụ văn bản phổ biến như HTTP, POP, IMAP, SMTP, FTP và ICQ thường được sử dụng, và người tấn công có thể truy cập dễ dàng vào tên người dùng, mật khẩu, thông tin cá nhân trong các email và tin nhắn.

Có những công cụ đặc biệt được tạo ra để phát hiện những cuộc tấn công mà hacker sử dụng để theo dõi thông tin đang chuyển qua mạng, điều này gọi là tấn công theo dõi gói tin (packet sniffing attacks). Những công cụ này thường xuyên giám sát lưu lượng mạng hoặc quét các card mạng ở chế độ ‘promiscuous’ để phát hiện để phát hiện các thiết bị theo dõi mạng không dây. Ví dụ về những công cụ này có thể kể đến là Wireshark và Snoop.

Khi sử dụng kết nối Wi-Fi và các công nghệ không dây khác như Bluetooth, việc sử dụng ăng-ten hiện đại hơn sẽ tăng tỷ lệ công suất, làm cho việc nghe lén trở nên dễ dàng hơn. Mặc dù nghe lén là một hoạt động thụ động (không can thiệp trực tiếp vào hệ thống), nhưng cuộc tấn công có thể phát triển thành các hình thức khác như tấn công chiếm đoạt phiên (session hijacking) hoặc tấn công trung gian (man-in-the-middle), nơi các tin nhắn giữa người dùng và điểm truy cập không dây bị chặn và sửa đổi với mục tiêu truy cập trái phép vào thông tin hoặc thiết bị.

Trong quá khứ, khi sử dụng các mạng di động, thông tin truyền tải trên các mạng này có khả năng bị nghe lén một cách dễ dàng. Nhưng theo sự phát triển không ngừng của công nghệ mạng và nhu cầu sử dụng ngày càng cao cho việc truyền tải thông tin nhạy cảm và bảo mật, các tiêu chuẩn mã hóa đã được thiết lập để đảm bảo an toàn thông tin người dùng tại các điểm truy cập.

Ví dụ, khi chúng ta nói về việc bảo vệ thông tin trong hệ thống viễn thông di động toàn cầu thế hệ thứ ba (UMTS) chúng ta có thể nhắc đến việc sử dụng một phương pháp mã hóa dữ liệu cụ thể gọi là f8. Để thực hiện việc này, chúng ta sử dụng một loại mã khối được gọi là KASUMI (hoặc UEA1 theo tiêu chuẩn 3GPP). Tuy nhiên, có các nghiên cứu đã chỉ ra rằng mã KASUMI này có thể bị ‘phá vỡ’. Điều này có nghĩa là một kẻ tấn công không cần phải giải mã các mã hóa phức tạp; họ có thể tận dụng những điểm yếu trong hệ thống để đánh lừa và thu thập thông tin. Trong một số tình huống, khi các mạng di động cũ vẫn còn tồn tại, điện thoại thông minh có thể tự chuyển từ một mạng an toàn sang một mạng không an toàn, khiến cho việc nghe lén dữ liệu trở nên dễ dàng hơn. Theo tiêu chuẩn 3GPP, mối đe dọa này được định nghĩa là chuyển đổi bắt buộc sang công nghệ truy cập không dây kế thừa.

* + 1. Điểm truy cập không dây giả mạo

Ngay cả khi tất cả các điểm truy cập mạng Wi-Fi đều được bảo mật, việc triển khai một điểm truy cập Wi-Fi riêng biệt là khá dễ dàng với bất kỳ ai. Ví dụ, một nhân viên hoàn toàn có thể tự ý lắp đặt một điểm truy cập không dây trong phòng làm việc mà không quan tâm đến vấn đề bảo mật. Hành động này không chỉ gây ra các tác động trực tiếp đến các biện pháp bảo mật mà thậm chí gây ra hiện tượng ‘nhiễu sóng’ (hoặc xung đột sóng) với hệ thống chính của tổ chức và/hoặc doanh nghiệp. Điều nguy hiểm là nếu một điểm truy cập không dây "lạ" được cài đặt một cách âm thầm, người cài đặt có thể dễ dàng truy cập vào mạng cục bộ hoặc từ xa. Một tin tặc, hay “evil twin”, cũng có thể thay thế một điểm truy cập không dây hiện tại bằng một cái mà họ có toàn quyền truy cập và kiểm soát; hoặc thậm chí tạo ra một điểm truy cập không dây giả mạo với cài đặt tương tự, nhưng công suất mạnh hơn để vượt qua tín hiệu của điểm truy cập không dây hợp lệ. Khi một người dùng kết nối vào điểm truy cập không dây giả mạo, thông tin kết nối của họ có thể bị thu thập mà không họ biết, đe dọa tính bảo mật của mạng.

Trong Hệ thống Mạng Di động Công cộng Mặt đất (PLMN), việc cài đặt một trạm truy cập hoặc trạm cơ sở giả mạo là một thách thức lớn, chủ yếu do có các rào cản hoặc biện pháp phòng thủ vật lý được thiết lập để ngăn chặn những nỗ lực như vậy. Đa số thiết bị mạng di động được triển khai trong các phòng thiết bị cụ thể hoặc các địa điểm khác nhau, nơi mà việc tiếp cận và cài đặt thiết bị giả mạo trở nên khó khăn.

Tuy nhiên, khi triển khai các trạm di động nhỏ (như trạm di động tại nhà hoặc trạm Femto) tại các doanh nghiệp hoặc nơi ở của khách hàng, có khả năng tin tặc sẽ cài đặt một điểm phát sóng giả mạo, tức là một thiết bị không an toàn vì đã bị tấn công. Nhưng vấn đề ở chỗ, kẻ tấn công cần phải "đánh lừa" mạng để trạm giả mạo này có thể kết nối thành công. Các trạm cơ sở di động này thường được kiểm soát từ xa bởi nhà điều hành mạng di động, và nếu có bất kỳ vấn đề nào liên quan đến bảo mật hoặc hiệu suất mạng xung quanh trạm giả mạo, thông tin này sẽ được báo cáo cho nhà điều hành. Do đó, mặc dù có thể xảy ra tình huống tấn công và làm gián đoạn dịch vụ (DoS) tại một khu vực nhất định hoặc tận dụng một số lợi ích sử dụng di động miễn phí, nhưng phạm vi của một cuộc tấn công thông qua một điểm truy cập không dây giả mạo sẽ bị hạn chế do biện pháp an ninh của nhà điều hành mạng di động.

* + 1. Tấn công từ chối dịch vụ (DoS)

Bản chất của một cuộc tấn công từ chối dịch vụ (denial-of-service hoặc DoS) thường nhằm làm đầy bộ nhớ hoặc làm khả năng xử lý của mục tiêu trở nên quá tải để làm giảm tốc độ hoặc tốt nhất là ngừng hoạt động các dịch vụ được cung cấp. Điều này làm cho máy tính hoặc hệ thống bận rộn phản hồi lại lưu lượng mạng từ kẻ tấn công, từ đó không còn đủ tài nguyên để xử lý thông tin từ người dùng hợp pháp.

DoS chủ yếu nhằm làm suy giảm chất lượng hoặc ngăn chặn việc sử dụng hợp pháp của tài nguyên mạng. Mạng không dây đặc biệt dễ bị tấn công DoS vì tính đặc biệt của nó, như việc truy cập mở, cấu trúc mạng thay đổi linh hoạt, sự hợp tác của thuật toán, giao thức phân tán và sự thiếu rõ ràng trong hệ thống phòng thủ. Điều này không chỉ là một thách thức, mà còn là một vấn đề quan trọng và ngày càng trở nên phổ biến trong thời đại hiện nay. Bên cạnh đó nhiều kỹ thuật phòng thủ được phát triển cho mạng có dây cố định không thể áp dụng được cho môi trường di động này.

Một phương pháp đơn giản để gây ra tấn công từ chối dịch vụ (DoS) là sử dụng kỹ thuật làm phiền sóng radio (RF jamming), trong đó một thiết bị phát ra tín hiệu điện tử hoặc năng lượng ở dải tần số của các mạng không dây ở gần thiết bị tấn công. Khi tín hiệu RF của kẻ tấn công được gửi trong khoảng thời gian ngắn và/hoặc không thường xuyên, điều này được gọi là “scrambling” và có thể khó phát hiện đối với người quản trị mạng.

Một hình thức khác của loại tấn công này được đề cập trong mối đe dọa trước đó là khi một điểm truy cập giả mạo có thể gây ra tình trạng từ chối dịch vụ đối với người dùng cố gắng truy cập vào mạng.

Một tình huống phức tạp hơn có thể xảy ra khi tin tặc liên tục gửi những tin nhắn hợp lệ đến một thiết bị di động có nguồn năng lượng giới hạn, như một thiết bị máy tính từ xa. Điều này khiến cho nguồn cung cấp năng lượng của thiết bị bị tiêu hao nhanh hơn dự kiến, dẫn đến việc mất dịch vụ sớm hơn so với kế hoạch ban đầu.

Các biến thể khác của loại tấn công này có thể bao gồm cuộc tấn công làm mờ (fuzzing attacks), trong đó tin tặc gửi đến thiết bị những tin nhắn hoặc dữ liệu không đúng chuẩn hoặc không đáng tin cậy và theo dõi cách thiết bị phản ứng. Nếu thiết bị phản ứng chậm hoặc bị dừng bởi những cuộc tấn công này, thì đây có thể là cơ sở cho việc thực hiện một cuộc tấn công từ chối dịch vụ (DoS) trong tương lai.

* + 1. Bluejacking

Bluejacking là một hình thức tấn công được thực hiện trên các thiết bị di động có khả năng kết nối Bluetooth, như điện thoại di động. Người tấn công bắt đầu bằng cách gửi những tin nhắn không được yêu cầu đến người dùng của thiết bị có hỗ trợ Bluetooth. Trên thực tế, các tin nhắn này không ảnh hưởng trực tiếp đến thiết bị của người dùng, nhưng có thể kích thích họ phản hồi hoặc thêm thông tin liên hệ mới vào danh bạ của thiết bị. Điều này giống với các cuộc tấn công thư rác và lừa đảo qua email mà chúng ta thường gặp. Tuy nhiên, bluejacking chỉ trở nên nguy hiểm khi người dùng phản hồi với tin nhắn được gửi với ý định gây hại.

* + 1. Bluesnarfing

Bluesnarfing là việc lấy thông tin trái phép từ một thiết bị không dây thông qua kết nối Bluetooth, thường là diễn ra giữa các điện thoại di động, máy tính để bàn, máy tính xách tay và các thiết bị hỗ trợ cá nhân (PDAs). Trong trường hợp tấn công thành công, tin tặc có thể truy cập vào thông tin cá nhân và bí mật của các thiết bị này mà không cần sự cho phép của chủ sở hữu thiết bị.

* + 1. Mạng Adhoc

Nói một cách đơn giản, mạng Wi-Fi thường được tạo ra bằng cách kết nối các thiết bị không dây với điểm truy cập hoặc bộ định tuyến không dây. Tuy nhiên, mạng Wi-Fi Adhoc lại được tạo ra trực tiếp giữa hai hoặc nhiều thiết bị hỗ trợ Wi-Fi mà không cần điểm truy cập trung gian. Thậm chí khi các thiết bị không kết nối trực tiếp, chúng vẫn có thể giao tiếp với nhau thông qua máy tính chung hoặc các máy tính khác.

Với một số hệ điều hành, mạng Adhoc thường được bật mặc định. Điều này có nghĩa là bất kỳ ai ở gần máy tính phát sóng có thể cố gắng kết nối với thiết bị đó và truy cập vào các tài liệu được chia sẻ. Điều này trở nên nguy hiểm nếu người dùng không bật tính năng mã hóa, vì thông tin có thể bị lộ khi truyền qua mạng Ad-hoc.

* + 1. Các mối đe dọa khác

Dưới đây là ví dụ về các mối đe dọa khác:

- Sai định tuyến/tái định tuyến của tin nhắn/gói dữ liệu;

- Tấn công đánh cắp thông tin IMSI (IMSI catching);

- Theo dõi thiết bị di động (UE tracking);

- Ép buộc thiết bị chuyển vùng (forced handover);

- Mối đe dọa đối với bootstrap không được bảo vệ và tín hiệu đa điểm (multicast signalling) trong LTE;

- Các đường hầm IPsec cung cấp tính bảo mật, nhưng không toàn vẹn, có thể bị đồng bộ hoá sai lệch.

Ngoài ra, còn có các mối đe dọa liên quan đến thiết bị người dùng và thông tin được lưu trữ trên đó, chẳng hạn như khóa mã hóa, v.v.

* 1. Danh mục các yêu cầu an toàn cơ bản cho mạng không dây IP
1. Thông tin chung

An toàn thông tin là một phần quan trọng đối với cả mạng không dây và có dây. Tuy nhiên, mạng không dây đòi hỏi các yêu cầu và chức năng bảo mật bổ sung để đối phó với những rủi ro cụ thể của mạng không dây (chi tiết được mô tả trong **Mục 7**) và những yêu cầu bổ sung này sẽ được cung cấp trong Mục 8. Khi đánh giá cách thực hiện những yêu cầu an toàn thông tin cốt lõi này (sẽ được liệt kê trong mục 8.2 đến 8.7), cần phải xem xét cả những rủi ro và bối cảnh của rủi ro đó. Điều này giúp định rõ cách để đáp ứng các yêu cầu an ninh mà không gặp khó khăn.

1. Tính bí mật

Để giảm thiểu rủi ro liên quan đến tính bảo mật của dữ liệu truyền qua mạng không dây, việc sử dụng mã hóa cho dữ liệu người dùng và đôi khi là cả dữ liệu kế hoạch điều khiển và quản lý là cần thiết để đảm bảo rằng dữ liệu không thể bị xâm phạm trong quá trình truyền tải hoặc bị nghe lén. Tùy thuộc vào các loại công nghệ truy cập không dây khác nhau, chúng ta có nhiều cách mã hóa và mức độ bảo mật khác nhau.Đối với việc đảm bảo tính bảo mật, người quản trị mạng cần xem xét việc sử dụng phương pháp mã hóa mạnh nhất có sẵn, đồng thời cân nhắc đến sự đánh đổi giữa hiệu suất của mạng, dung lượng của mạng, quản lý khoá và khả năng sử dụng.

1. Tính toàn vẹn

Việc giữ cho dữ liệu truyền qua các mạng không dây không bị thay đổi là rất quan trọng để đảm bảo tính toàn vẹn của dữ liệu. Để làm được điều này, chúng ta cần sử dụng các biện pháp bảo vệ tính toàn vẹn phù hợp, nhằm đảm bảo rằng dữ liệu của người dùng và cả dữ liệu điều khiển, quản lý đều không bị thay đổi hoặc làm giả mạo. Mỗi công nghệ truy cập không dây có thể sử dụng những cách bảo vệ tính toàn vẹn khác nhau, với mức độ mã hóa cụ thể. Khi quản trị mạng, chúng ta nên lựa chọn sử dụng phương pháp mã hóa mạnh nhất có thể, đồng thời cân nhắc đến các yếu tố như hiệu suất của mạng, khả năng chịu tải của mạng, quản lý khóa và sự thuận tiện trong việc sử dụng.

1. Tính khả dụng

Khả năng sẵn có của mạng không dây sẽ phụ thuộc vào nhiều yếu tố, và hầu hết chúng đều áp dụng cho mọi công nghệ không dây. Chúng bao gồm:

- Các đặc tính RF của công nghệ (băng thông kênh, cường độ tín hiệu, dải tần số, điều chế, mã hóa, vv);

- Môi trường triển khai (địa hình vật lý, khí quyển);

- Hiệu suất của mạng trong điều kiện tải và quá tải;

- Lập kế hoạch mạng (dung lượng, tái sử dụng phổ tần);

- Mức độ dự phòng được thiết kế trong mạng và các yếu tố cấu thành;

- Khả năng phục hồi của mạng và các yếu tố cấu thành của nó đối với các cuộc tấn công DoS.

Những tổ chức cung cấp mạng và dịch vụ, cũng như doanh nghiệp, có thể phải tuân thủ các quy định để đảm bảo cung cấp mức dịch vụ đáp ứng yêu cầu. Một số khách hàng có thể thương lượng Thỏa thuận Cấp độ Dịch vụ (SLA) với nhà cung cấp dịch vụ, điều này có thể ảnh hưởng đến các yếu tố được nêu trên.

1. Xác thực

Việc kiểm tra xem dữ liệu hay các bên liên lạc có đến từ nguồn đáng tin cậy hay không, cũng như xác minh danh tính của các bên tham gia trao đổi thông tin và các quản trị viên, nhân viên bảo trì mạng là cực kỳ quan trọng để đảm bảo an toàn cho mạng không dây. Khác với mạng có dây, mạng không dây truyền tải dữ liệu qua không gian mà không giới hạn bởi các kết nối vật lý.

Mỗi công nghệ truy cập không dây có thể sử dụng những cách xác minh khác nhau cho các thiết bị người dùng đang cố gắng kết nối hoặc truy cập mạng, mỗi cách có giao thức xác minh bắt buộc riêng biệt. Trong nhiều trường hợp, người quản trị mạng không có quyền kiểm soát đối với giao thức này.

Người quản trị mạng nên cố gắng sử dụng tùy chọn xác minh mạnh mẽ nhất có thể, đồng thời cân nhắc đến các yếu tố như hiệu suất của mạng, quản lý khóa hoặc mật khẩu, sự thuận tiện khi sử dụng, mô hình triển khai, và các yếu tố khác.

Chẳng hạn, đối với các mạng di động 3G UMTS, các tiêu chuẩn xác định một số các thuật toán mã hóa và bảo vệ tính toàn vẹn được sử dụng giữa điện thoại di động của bạn và Bộ Điều khiển Mạng Vô tuyến (the Radio Network Controller). Việc chọn một trong những thuật toán này để sử dụng trong mạng được quyết định bởi người điều hành mạng.

Các thuật toán này dựa trên KASUMI và SNOW 3G để thực hiện việc mã hóa và bảo vệ tính toàn vẹn thông tin.

Trong bối cảnh của mạng di động, người điều hành mạng là người quyết định cách các thiết bị người dùng xác thực vào mạng và thậm chí là điểm truy cập mạng cho thiết bị người dùng. Vì vậy, đối với các Mạng Di động Công cộng (PLMN), Giám đốc An toàn thông tin (CISO) hoặc nhân viên Công nghệ Thông tin (IT) cần phải hiểu rõ về tác động của những điều này.

1. Phân quyền truy cập

Kiểm soát truy cập đảm bảo rằng chỉ những người hoặc thiết bị được uỷ quyền mới có thể được truy cập vào các phần khác nhau của mạng, thông tin đã được lưu trữ, dòng thông tin, dịch vụ và ứng dụng.

Mỗi công nghệ truy cập không dây đều xác định các quy định kiểm soát truy cập cho thiết bị cuối và các điểm truy cập vô tuyến, thường được mô tả thông qua các thông số kỹ thuật cho dữ liệu người dùng, kiểm soát và dữ liệu tín hiệu, bao gồm cả quản lý thiết bị và dữ liệu quản lý thành phần.

Ngoài ra, các nhà sản xuất thiết bị cũng sẽ xác định và triển khai các hệ thống kiểm soát truy cập cụ thể cho các điểm truy cập vô tuyến.

Đối với mạng Wi-Fi, Giám đốc An toàn thông tin (CISO) hoặc nhân viên Công nghệ Thông tin (IT) sẽ quản lý việc người dùng nào được phép truy cập vào mạng. Trong khi đó, đối với mạng di động công cộng mặt đất (PLMN), người điều hành mạng quản lý quyền truy cập của các thiết bị người dùng, dựa trên số IMEI của họ, khiến cho quản trị viên của tổ chức và/hoặc doanh nghiệp không có quyền kiểm soát trực tiếp điều này.

Lưu ý rằng, khi công nghệ di động 3G và 4G femto được triển khai rộng rãi hơn, các tổ chức và/hoặc quản trị viên doanh nghiệp sẽ có quyền kiểm soát trực tiếp hơn đối với việc thiết bị người dùng nào có thể truy cập vào mạng truy cập vô tuyến.

1. Trách nhiệm giải trình (Không thoái thác)

Việc đảm bảo trách nhiệm của người dùng mạng không dây là quan trọng để đảm bảo rằng mọi vi phạm chính sách có thể được theo dõi về một người cụ thể.

Quản lý trách nhiệm này giúp ngăn chặn việc một cá nhân hoặc tổ chức phủ nhận đã thực hiện một hành động cụ thể liên quan đến dữ liệu bằng cách cung cấp bằng chứng về các hành động liên quan đến mạng. Điều này bao gồm bằng chứng về nghĩa vụ, ý định hoặc cam kết; bằng chứng về nguồn gốc dữ liệu, bằng chứng về quyền sở hữu, và bằng chứng về việc sử dụng tài nguyên. Bằng cách này, chúng ta có thể đảm bảo sẵn có bằng chứng có thể được trình bày cho bên thứ ba và được sử dụng để chứng minh rằng một sự kiện hoặc hành động cụ thể đã diễn ra.

Đối với mạng Wi-Fi, điểm truy cập có thể được thiết lập để lưu trữ nhật ký truy cập của người dùng. Dữ liệu này không chỉ hữu ích trong việc khắc phục sự cố và giám sát hiệu suất của mạng, mà còn có thể được sử dụng để theo dõi xu hướng. Thông tin về sự cố truy cập của người dùng, sự cố xác thực, và lịch sử kết nối của người dùng cung cấp cho người quản trị mạng cơ sở để theo dõi và xác định nguy cơ về an ninh, đồng thời giúp xác định người dùng chịu trách nhiệm cho một hoạt động cụ thể.

* 1. Các biện pháp kiểm soát bảo mật đối với mạng không dây IP

7.1 Các mục tiêu an toàn cho môi trường hoạt động

Trong việc đánh giá rủi ro của một hệ thống mạng, các mối đe dọa đặc biệt từ mạng không dây, được liệt kê ở Mục 7, sẽ thêm vào những mối đe dọa chung cho tất cả các loại mạng, như việc truy cập không được ủy quyền, đánh cắp dữ liệu lưu trữ, hoặc sự tấn công của phần mềm độc hại. Các yêu cầu bảo mật, được liệt kê ở Mục 8, đã được định rõ cho mạng không dây, nhưng chúng cũng có thể coi là những yêu cầu cơ bản cho mọi loại mạng. Do đó, trong nhiều trường hợp, các biện pháp kiểm soát bảo mật tại Mục 9 có thể áp dụng cho mọi loại mạng truy cập, ví dụ như việc tăng cường bảo mật trên điểm truy cập. Một trong những mục đích quan trọng của Mục 9 là làm nổi bật sự khác biệt giữa việc áp dụng một biện pháp kiểm soát cho mạng không dây so với bất kỳ mạng truy cập nào khác.

Đối với một rủi ro bảo mật cụ thể, mỗi tài sản bảo mật cần được kiểm tra để xác định xem nó có liên quan và ảnh hưởng đến thiết bị hoặc mạng hay không, và dựa vào mức ưu tiên, chúng ta cần xem xét các biện pháp kiểm soát nào có sẵn để giảm thiểu rủi ro đó. Thường thì, hầu hết các rủi ro có thể được giảm thiểu thông qua nhiều biện pháp kiểm soát khác nhau. Ví dụ, kiểm soát truy cập và xác thực có thể được áp dụng để bảo vệ chống lại mã độc. Quyết định về việc chọn lựa các biện pháp kiểm soát hoặc lớp phòng thủ sẽ được đưa ra trong giai đoạn đánh giá hoặc quản lý rủi ro của dự án.

Tương tự như các mạng truyền thông khác, chiến lược bảo mật chính cho các mạng không dây là áp dụng một phòng thủ đa cấp độ.

Dưới đây là một số biện pháp kiểm soát phổ biến:

- Củng cố thiết bị;

- Cập nhật phần mềm cho thiết bị;

- Hệ thống quản lý thông tin dựa trên đánh giá rủi ro của tài sản;

- Đào tạo nhân viên vận hành;

- Tăng cường nhận thức của người sử dụng cuối cùng.

Các biện pháp kiểm soát bảo mật liên quan đến mạng không dây được mô tả dưới đây. Lưu ý rằng không phải tất cả các biện pháp kiểm soát này đều áp dụng cho mọi công nghệ không dây.

7.2 Kiểm soát và triển khai mã hóa

Tại Mục 8, có hai yêu cầu bảo mật chính cần chú ý là bảo mật thông tin và đảm bảo tính toàn vẹn của dữ liệu. Để đảm bảo an toàn cho những yêu cầu này, một trong những biện pháp an ninh quan trọng là sử dụng phương pháp mã hóa dữ liệu. Trong trường hợp mạng không dây, việc mã hóa dữ liệu trên các giao diện không dây được khuyến khích cho hầu hết các trường hợp triển khai. Nhìn chung, các tiêu chuẩn không dây mô tả chi tiết về các loại mã hóa dành cho dữ liệu người dùng, dữ liệu điều khiển và đôi khi là dữ liệu quản lý thiết bị.

Tại Mục 10, có đề cập đến các tiêu chuẩn bảo mật liên quan đến một số công nghệ không dây thường được sử dụng. Dưới đây là những yếu tố mà người chịu trách nhiệm về an toàn thông tin cần xem xét về việc mã hóa thông tin.

- Có những thuật toán mã hóa dữ liệu nào được sử dụng? Các thiết bị hoặc mạng có triển khai những thuật toán mã hóa nào cho người dùng cuối không?

- Người dùng cuối có cần phải chọn loại mã hóa hay chỉ có thể được cấu hình bởi người quản trị mạng?

- Cân nhắc giữa việc sử dụng mã hóa mạnh nhất và hiệu suất của giao diện mạng, thiết bị người dùng cuối, cũng như băng thông khả dụng.

- Làm thế nào người dùng cuối được thông báo về mức độ mã hóa của dữ liệu của họ và mức độ an toàn của nó.

- Hiểu rõ về quản lý khóa mã hóa. Liệu có triển khai cơ sở hạ tầng khóa công khai (PKI) không? Giải pháp không dây có sử dụng cơ quan cấp chứng chỉ cục bộ hay kết nối với cơ quan cấp chứng chỉ công khai/gốc không? Quy trình quản lý khóa càng tự động thì nó sẽ càng thân thiện với người dùng.

- Ở một số địa phương, luật pháp địa phương có quy định về loại mã hóa có thể hoặc không thể triển khai.

- Các Thỏa thuận Cấp độ Dịch vụ (SLA) cũng có thể quy định về loại mã hóa cần được triển khai.

- Tính tương thích với các mạng (không dây) khác, ví dụ: nếu thiết bị người dùng chuyển từ mạng này sang mạng khác, liệu mạng thứ hai có hỗ trợ cùng mức độ mã hóa như mạng ban đầu không?

- Tương thích ngược với các phiên bản thiết bị/máy khác nhau. Trong một số trường hợp, các phiên bản trước đó của một thiết bị người dùng có thể không hỗ trợ cùng mức độ mã hóa.

Các quy chuẩn bảo mật không dây thường chỉ định cơ chế mã hóa dữ liệu theo từng bước hoặc trên một giao diện cụ thể, như giao diện không dây. Khi nghiên cứu về việc mã hóa dữ liệu, người quản lý an toàn thông tin cần xem xét toàn bộ quá trình truyền dữ liệu từ đầu đến cuối. Đôi khi, có thể là lựa chọn khôn ngoan hơn nếu ta xem xét việc sử dụng một kênh bảo mật toàn diện hoặc kết nối VPN an toàn từ đầu đến cuối.

Ngoài quá trình truyền dữ liệu từ đầu đến cuối, việc mã hóa dữ liệu được lưu trữ trong các điểm truy cập không dây và thiết bị cuối cũng là một yếu tố quan trọng. Thông thường, nó sẽ tuân theo những phương pháp thực tiễn tốt nhất để đảm bảo an toàn cho dữ liệu quan trọng.

Về mặt mã hóa, người quản trị an toàn thông tin cần phải nhận biết và nắm được mọi lỗ hổng trong thuật toán mã hóa được công bố. Thông thường, những thông tin như vậy sẽ được công bố rộng khắp trong ngành Công nghiệp Công nghệ thông tin và Truyền thông. Tuy nhiên, quan trọng là phải thiết lập các thỏa thuận tiết lộ lỗ hổng với tất cả các nhà cung cấp hệ thống để đảm bảo rằng Giám đốc An toàn thông tin (CISO) sẽ được thông báo về mọi vấn đề. Điều này đặc biệt quan trọng khi lỗ hổng liên quan đến cách triển khai thuật toán (khác với các đặc điểm lý thuyết của nó), vì khả năng cao là các lỗ hổng như vậy sẽ không được công bố rộng rãi.

7.3 Đánh giá tính toàn vẹn

Để bảo vệ mạng khỏi những tấn công như tấn công chiếm đoạt phiên (session hijacking) hoặc tấn công trung gian (man-in-the-middle), hoặc tấn công lặp lại tin nhắn, các kết nối không dây sẽ sử dụng cơ chế kiểm tra tính toàn vẹn như một tầng phòng thủ chính chống lại những cuộc tấn công này. Các tiêu chuẩn không dây thường xác định cách kiểm tra tính toàn vẹn và có thể có nhiều tùy chọn mà những người quản lý an toàn thông tin cần phải chọn lựa.

Mục 9.2 nêu rõ các yếu tố cần xem xét khi mã hóa dữ liệu, và những yếu tố này cũng có thể được áp dụng để đánh giá tính toàn vẹn.

Khi nhân viên quản lý an toàn thông tin đang xem xét các cơ chế tính toàn vẹn dữ liệu, anh/chị cần xem xét cả dữ liệu người dùng và dữ liệu kiểm soát trong quá trình truyền, cũng như dữ liệu liên quan đến quản lý như tải xuống phần mềm, nâng cấp hay tải xuống cấu hình.

Với sự tinh vi của các cuộc tấn công ngày càng cao, những yếu điểm trong các cơ chế tính toàn vẹn và cách triển khai chúng bởi một nhà cung cấp cụ thể có thể bị lộ ra. Người chịu trách nhiệm bảo mật thông tin cần duy trì sự cảnh giác và đảm bảo rằng họ luôn cập nhật với những tiến bộ trong các tiêu chuẩn an ninh không dây hoặc với bất kỳ vi phạm nào đã được công khai.

7.4 Xác thực

Để bảo vệ chống lại nguy cơ truy cập vào mạng hoặc các điểm truy cập, cũng như truy cập vào dữ liệu một cách trái phép, và nguy cơ chèn các điểm truy cập giả mạo và tấn công trung gian (man-in-the-middle), các tiêu chuẩn công nghệ không dây đã đề xuất những cơ chế xác thực. Những cơ chế này không chỉ đơn giản là việc xác thực bằng mật khẩu, sử dụng khóa chia sẻ hoặc khóa công khai/riêng tư, mà còn bao gồm những kết hợp phức tạp hơn giữa các phương pháp khác nhau. Nhân viên bảo mật thông tin cần xem xét không chỉ cách mà người dùng cuối được xác thực khi kết nối vào mạng, mà còn cách thiết bị của họ được xác thực. Đồng thời, cần quan tâm đến cách điểm truy cập hoặc các cổng kết nối trung gian xác thực chính họ với thiết bị của người dùng cuối, cũng như cách các điểm truy cập xác thực chính họ với nhau hoặc với mạng trung tâm. Nói chung, hầu hết các công nghệ không dây đều đã đặc tả tất cả những khía cạnh này trong các tiêu chuẩn bảo mật tương ứng một cách rõ ràng để đảm bảo an toàn thông tin.

Các cân nhắc sau đây đáng quan tâm đối với một nhân viên bảo mật thông tin:

- Các phương thức xác thực nào được quy định bởi tiêu chuẩn an toàn không dây phù hợp với công nghệ không dây đang sử dụng? Các giao diện nào được đặc biệt xác định trong tiêu chuẩn? Ví dụ, liệu nó chỉ liên quan đến giao diện không dây hay còn liên quan đến quản lý và điều khiển thiết bị và/hoặc điểm truy cập? Tiêu chuẩn có định rõ xác thực lẫn nhau cho tất cả các giao diện không?

- Các phương thức xác thực nào được triển khai trong thiết bị/mạng và thiết bị người dùng cuối? Một số thiết bị và/hoặc trang thiết bị truy cập có thể không hỗ trợ tiêu chuẩn mới nhất hoặc tất cả các tùy chọn bảo mật.

- Người quản trị mạng có những tùy chọn nào để lựa chọn và cấu hình phương thức xác thực?

- Việc sử dụng các cơ chế xác thực mạnh nhất là điều nên làm nhưng nó có thể cần được cân nhắc với sự tiện lợi cho người dùng, khả năng quản lý từ góc độ của người quản trị mạng và chi phí triển khai.

- Việc quản lý thông tin xác thực của người dùng sẽ cần phải được hiểu rõ.

- Các khía cạnh quản lý thông tin xác thực khác cần được hiểu bao gồm: cách xử lý các lần xác thực thất bại; cách thu hồi và/hoặc khôi phục thông tin xác thực; làm thế nào khi thông tin xác thực hết hạn. Những khía cạnh này áp dụng đối với người dùng mà còn cho khía cạnh điều khiển và quản lý.

- Các công nghệ không dây như 2G/3G/4G sử dụng các thiết bị SIM/UICC trong thiết bị người dùng cuối được cung cấp và cấu hình bởi nhà khai thác mạng di động công cộng mặt đất (PLMN) hoặc có thể được cài đặt cố định bởi các nhà sản xuất thiết bị. Nhân viên an toàn thông tin cần hiểu mối quan hệ giữa tất cả các bên. Giám đốc an toàn thông tin (CISO) cũng nên hiểu các cơ chế bảo mật vật lý được sử dụng để bảo vệ thông tin đăng nhập trên các thiết bị người dùng cuối hoặc trong các bộ điều khiển như mạch tích hợp chống giả mạo, môi trường đáng tin cậy, v.v

- Ở một số quốc gia, luật pháp địa phương quy định loại phương thức xác thực có thể hoặc không thể triển khai.

- Thỏa thuận cấp độ dịch vụ (SLA) cũng có thể xác định loại phương thức xác thực nào nên được triển khai.

- Khả năng tương thích với các mạng (không dây) khác, ví dụ: nếu thiết bị người dùng cuối chuyển sang mạng khác, mạng thứ hai có hỗ trợ cùng loại xác thực như mạng ban đầu không? Nhân viên an toàn thông tin nói chung sẽ không thể cấu hình hoặc kiểm soát các khía cạnh tương thích nhưng phải nhận thức được khả năng của các công nghệ an toàn không dây khác nhau.

- Tương thích ngược với các phiên bản thiết bị/thiết bị khác nhau.

* 1. Kiểm soát truy cập

7.5.1 Tổng quan

Các cơ chế kiểm soát truy câpj thông thường như kiểm soát vai trò (RBAC), kiểm soát truy cập hệ thống tệp, tường lửa và phát hiện xâm nhập được coi là những phương pháp tốt nhất khi xây dựng một giải pháp mạng, dù chúng được tích hợp vào một sản phẩm cụ thể hay được đặt ở mức bảo vệ bên ngoài. Đối với hệ thống không dây, nguyên tắc này không thay đổi, nhưng ngoài ra, có những biện pháp kiểm soát cụ thể được định rõ trong các tiêu chuẩn an toàn mạng không dây để tăng cường thêm cho các biện pháp kiểm soát truy cập truyền thống.

Các cân nhắc sau đây đáng quan tâm đối với một nhân viên bảo mật thông tin:

- Cơ chế kiểm soát truy cập nào được quy định bởi tiêu chuẩn bảo mật không dây tương ứng cho công nghệ không dây đã chọn?

- Cơ chế kiểm soát truy cập nào được áp dụng trong các thiết bị/mạng và thiết bị người dùng cuối? Một số thiết bị và/hoặc thiết bị điểm truy cập có thể không hỗ trợ tiêu chuẩn mới nhất hoặc tất cả các tùy chọn bảo mật.

- Người quản trị mạng có những lựa chọn nào về việc chọn và cấu hình cơ chế kiểm soát truy nhập?

- Ở một số vùng, luật pháp địa phương quy định loại cơ chế kiểm soát truy cập có thể hoặc không thể triển khai.

- Khả năng tương thích với các mạng (không dây) khác là gì?

- Nói chung, nhân viên bảo mật thông tin sẽ không thể cấu hình hoặc kiểm soát mọi khía cạnh về khả năng tương thích, nhưng phải nhận thức về khả năng của các công nghệ bảo mật không dây khác nhau.

- Có khả năng tương thích ngược với các phiên bản thiết bị/thiết bị khác nhau là điều cần xem xét.

- Để phát hiện và/hoặc ngăn chặn truy cập trái phép vào mạng không dây, cũng như các tác động tiếp theo của vi phạm bảo mật đó, nên xem xét việc sử dụng hệ thống phát hiện/ngăn chặn xâm nhập không dây.

7.5.2 Kiểm soát quyền truy cập

Ví dụ, trong các hệ thống 802.11, việc sử dụng bộ lọc địa chỉ MAC được thực hiện để đảm bảo rằng chỉ có các thiết bị khách hàng mạng không dây được phép mới có thể kết nối vào mạng không dây. Có thể hiểu đơn giản rằng tính năng bảo mật này một mình không đủ để ngăn chặn tấn công, vì một kẻ tấn công có thể giả mạo thành một thiết bị khách hàng hợp lệ. Tuy nhiên, đây là một ví dụ về một tầng bảo vệ mà hệ thống có thể sử dụng.

Trong các tiêu chuẩn mạng di động, việc sử dụng định danh thiết bị người dùng là một cơ chế để quyết định liệu họ được phép truy cập vào mạng hay không. Nếu IMEI của người dùng (International Mobile Equipment Identity - số nhận dạng quốc tế cho thiết bị di động) bị đưa vào danh sách đen bởi nhà điều hành, họ sẽ không thể truy cập vào mạng.

7.5.3 Kiểm soát dựa trên mạng

Với nhiều công nghệ không dây, khi xem xét về các tiêu chuẩn, chúng ta thấy rằng dữ liệu người dùng và các giao thức kiểm soát thường được định nghĩa và triển khai một cách riêng biệt. Bằng cách xác định và triển khai tiêu chuẩn theo cách này, chúng ta tạo ra một sự phân chia logic, từ đó cung cấp một cấp độ kiểm soát truy cập.

Với tiêu chuẩn 4G LTE, có đề xuất rằng lưu lượng điều khiển nên được bảo mật bằng cách sử dụng các giao thức dựa trên IPsec khi đi qua ranh giới mạng từ một miền an toàn sang một miền khác (nghĩa là qua một mạng không an toàn). Cấu hình mạng như vậy cũng là một lựa chọn cho dữ liệu người dùng nếu các nhà quản lý muốn áp dụng.

* 1. Khả năng phục hồi từ tấn công từ chối dịch vụ (DoS)

Các biện pháp phổ biến để ngăn chặn hoặc xử lý cuộc tấn công từ chối dịch vụ (DoS) thường bao gồm việc sử dụng các kỹ thuật mã hóa an toàn khi lập trình, kiểm tra mã nguồn để phân tích lỗ hổng, và thực hiện đánh giá lỗ hổng. Đồng thời, có thể sử dụng các hệ thống IDS/IPS dựa trên mạng hoặc máy chủ để phát hiện hành vi không bình thường trong lưu lượng IP hoặc ứng dụng. Những biện pháp này áp dụng cho tất cả các mạng thông tin và truyền thông.

Khi nói đến mạng không dây, có một vấn đề khác là gây nhiễu tần số vô tuyến (RF jamming). Điều này chỉ xảy ra trong môi trường không dây, nơi tín hiệu nhiễu RF có thể đến từ kẻ tấn công hoặc nguồn ngẫu nhiên khác. Giám đốc an toàn thông tin (CISO) cần đảm bảo rằng mạng đã được trang bị thiết bị giám sát để phát hiện sự cố và lưu lại thông tin liên quan.

Cuộc tấn công DoS dựa trên các giao thức không dây cụ thể có thể được phát hiện thông qua các hệ thống phát hiện bất thường. Giám đốc an toàn thông tin (CISO) cần nắm rõ những giải pháp đang được triển khai trong mạng, khả năng của thiết bị giám sát, và liên tục cập nhật thông tin về các mối đe dọa mới hoặc tiến triển trong lĩnh vực này. Điều này giúp đảm bảo rằng họ luôn ở trạng thái đề phòng trước những rủi ro an ninh mạng tiềm ẩn.

* 1. Phân tách vùng DMZ thông qua bảo vệ tường lửa

Vì mạng không dây có khả năng bị tấn công thông qua không gian không dây, nên khuyến nghị rằng bất kỳ mạng không dây nào được kết nối với mạng nội bộ bảo mật nên được kết nối thông qua một mạng khu vực phi quân sự (DMZ).

Mạng không dây DMZ này cần được tách biệt khỏi mạng được bảo mật thông qua một tường lửa, nhằm hạn chế một số loại dữ liệu từ mạng không dây có thể truy cập vào mạng được bảo mật.

Một ví dụ điển hình cho việc sử dụng kiểm soát này là mạng không dây dành cho khách trong tổng thể mạng của một tổ chức và/hoặc doanh nghiệp.

* 1. Quản lý lỗ hổng bảo mật thông qua cấu hình an toàn và tăng cường bảo mật cho thiết bị

Một chương trình quản lý lỗ hổng được khuyến nghị nên được thiết lập.Chúng ta có thể sử dụng các công cụ quét lỗ hổng không dây để kiểm tra xem có những lỗ hổng nào trong hệ thống hay không. Những lỗ hổng phát hiện được có thể được khắc phục bằng cách cập nhật ứng dụng, hệ điều hành và thiết bị, hoặc thông qua việc sử dụng cấu hình an toàn và tăng cường bảo mật cho thiết bị.

* 1. Giám sát liên tục các mạng không dây

Mạng không dây nên được tích hợp với hệ thống giám sát an ninh doanh nghiệp. Các công cụ quản lý sự cố và sự kiện bảo mật cũng như các công cụ phát hiện mối đe doạ doanh nghiệp có thể được sử dụng để cung cấp giám sát thường xuyên hoặc liên tục nhằm để phát hiện các cuộc tấn công và rò rỉ dữ liệu.

* 1. Phương án thiết kế và cấu hình bảo mật cho mạng không dây IP

8.1 Tổng quan

Mục 10 cung cấp hướng dẫn nâng cao khi thiết kế và triển khai mạng không dây. Mục này chủ yếu không định nghĩa hoặc mô tả chi tiết về các giao thức hoặc giao diện an toàn không dây vì chúng đã được định rõ trong các tiêu chuẩn công nghệ không dây tương ứng. Một trong những tiêu chuẩn không dây phổ biến nhất là họ chuẩn IEEE 802.11. Mục 10.2 sẽ cung cấp một số chi tiết về các khía cạnh của 802.11. Ở mục 10.2, các tiêu chuẩn khác sẽ được xem xét. Danh sách các công nghệ không dây được bao gồm trong phần này của ISO/IEC 27033 không phải là bản đầy đủ vì ngay sau khi tài liệu được xuất bản, các tiêu chuẩn mới hoặc biến thể của tiêu chuẩn có thể nhanh chóng phát triển và có khả năng thay thế các tiêu chuẩn liên quan đến các công nghệ được liệt kê ở đây.

Trong quá trình lập kế hoạch, có thể sử dụng một số kiểm tra cơ bản để đảm bảo rằng Giám đốc An toàn thông tin (CISO), hệ thống CNTT hoặc kiến sư mạng có thể xem xét và triển khai an toàn các công nghệ mới một cách an toàn.

- Thực hiện đánh giá rủi ro về việc sử dụng các công nghệ không dây mới.

- Như một phần của sự phát triển của tiêu chuẩn không dây và đặc biệt là phần bảo mật, tổ chức phát triển tiêu chuẩn thường hoàn thành một phân tích mối đe dọa mô tả các mối đe dọa áp dụng cho công nghệ và các biện pháp đối phó để giảm thiểu mọi rủi ro. Các biện pháp giảm nhẹ hoặc đối phó sẽ được liệt kê theo khuyến nghị hoặc sẽ được tích hợp vào chính đặc điểm kỹ thuật tiêu chuẩn.

Ví dụ, tài liệu 3GPP TR 33.821 (cơ sở lý luận và theo dõi các quyết định bảo mật trong sự phát triển dài hạn (LTE) của tiến hóa kiến trúc hệ thống RAN/3GPP (SAE) giải thích mối đe dọa cụ thể với công nghệ không dây và cách đối phó, và kết quả của nó được sử dụng trong các tài liệu yêu cầu kỹ thuật bảo mật khác của tổ chức.

- Giám đốc an toàn thông tin (CISO) hoặc chuyên gia bảo mật CNTT cần phải nhận thức được các mối đe dọa cụ thể liên quan đến công nghệ không dây được đề xuất.

- Đảm bảo rằng tổ chức có một chính sách bảo mật không dây, trong đó cụ thể đề cập đến:

* Xác thực người dùng mạng không dây;
* Kiểm soát truy cập mạng không dây cho cả nhân viên và khách;
* Quản lý việc nhân viên truy cập các mạng không dây ngoài sự kiểm soát của tổ chức;
* Xác định ai có thẩm quyền cho phép các điểm truy cập kết nối vào mạng của tổ chức.

Chính sách bảo mật không dây cũng có thể bao gồm các biện pháp an ninh liên quan đến việc mang theo thiết bị cá nhân (BYOD - Bring Your Own Device), mặc dù BYOD không chỉ liên quan đến công nghệ không dây. Quan trọng nhất, chính sách này cần bao quát tất cả các công nghệ không dây được triển khai trong mạng của doanh nghiệp hoặc tổ chức.

8.2 Wi-fi

8.2.1. Tổng quan

Wi-Fi được định nghĩa là bất kỳ sản phẩm mạng cục bộ không dây (WLAN) nào dựa trên tiêu chuẩn 802.11 của Viện Kỹ sư Điện và Điện tử (IEEE).

Phần này cung cấp hướng dẫn về các kỹ thuật và các yếu tố cần xem xét xung quanh mạng và các thiết bị Wi-Fi.

Mạng Wi-Fi là một nhóm gồm hai hoặc nhiều thiết bị mạng không dây trong một khu vực địa lý hạn chế trao đổi dữ liệu thông qua sóng vô tuyến. Các thành phần cơ bản của mạng Wi-Fi theo tiêu chuẩn IEEE 802.11 bao gồm các thiết bị máy khách như máy tính xách tay, máy tính bảng, điện thoại thông minh và các điểm truy cập (AP), có chức năng kết nối logic các thiết bị máy khách với một hệ thống phân phối, thường là cơ sở hạ tầng mạng có dây của tổ chức. Một số mạng Wi-Fi cũng sử dụng các công tắc không dây, hoạt động như bộ truyền đổi giữa các AP và hệ thống phân phối.

Nhóm tiêu chuẩn IEEE 802.11 bao gồm một loạt các kỹ thuật điều chế bán song công qua vô tuyến sử dụng cùng một giao thức cơ bản. Tiêu chuẩn gốc IEEE 802.11-1997 (kế thừa) đã được thay thế bởi hàng tá bản sửa đổi khác nhau, trong đó giới thiệu các sửa đổi và mở rộng hoặc chỉnh sửa các thông số kỹ thuật trước đó, hỗ trợ các tần số truyền khác nhau và các cơ chế bảo mật khác nhau.

Bảo mật của mạng Wi-Fi phụ thuộc nhiều vào mức độ bảo mật của từng thành phần Wi-Fi (bao gồm các thiết bị kết nối, các điểm truy cập AP và bộ chuyển mạch không dây) từ quá trình thiết kế và triển khai ban đầu đến bảo trì và giám sát liên tục. Thật không may, mạng Wi-Fi thường ít an toàn hơn so với mạng có dây vì sự dễ dàng truy cập và thường sử dụng cấu hình bảo mật yếu, có xu hướng ưu tiên sự tiện lợi hơn là tính bảo mật.

Các cơ chế bảo mật cho Wi-Fi được định nghĩa trong các tiêu chuẩn IEEE 802.11 và bao gồm các chức năng như xác thực thiết bị kết nối đến điểm truy cập AP, xác thực AP đến thiết bị, mã hóa dữ liệu người dùng và bảo vệ tính toàn vẹn dữ liệu người dùng. Lưu ý rằng không phải tất cả các chức năng bảo mật đều có sẵn trong mỗi tiêu chuẩn IEEE 802.11.

Đối với doanh nghiệp, bộ phận an toàn thông tin của tổ chức chịu trách nhiệm kiểm soát cách bảo mật được cấu hình trên cơ sở hạ tầng của mình.

Đối với nhân viên sử dụng các mạng khác, điểm truy cập công cộng, v.v., những người này nên được khuyến khích sử dụng các cơ chế bảo mật thay thế, ví dụ như sử dụng VPN khi truyền thông tin nhạy cảm hoặc tuyệt mật.

8.2.2. Xác thực người dùng

Khi mọi người muốn kết nối vào mạng không dây được kiểm soát và quản lý bởi một tổ chức nào đó, họ cần chứng minh họ là người được phép trước khi được truy cập mạng hoặc vào các điểm Wi-Fi cho khách.

Đối với nhân viên, để truy cập vào mạng, họ cần sử dụng xác thực hai yếu tố, ví dụ như SecurID hoặc Safeword Token kết hợp với một mã PIN.

Những điều sau đây cần được xem xét để cho phép khách truy cập Internet.

- Tất cả các khách đăng ký mạng không dây phải được tài trợ bởi một người có trách nhiệm trong tổ chức;

- Các ID của khách hàng cần phải là duy nhất để duy trì tính trách nhiệm. Tuy nhiên, trong trường hợp không thể gán các ID và mật khẩu riêng lẻ (ví dụ: một cuộc họp với nhiều khách hàng), có thể chia sẻ ID và mật khẩu;

- Thời hạn của mật khẩu phản ánh nhu cầu kinh doanh (thường là một tuần);

- Khách hàng nên được cung cấp "thông báo về điều kiện" mô tả các điều kiện và điều khoản để truy cập.

8.2.3. Bảo mật và toàn vẹn thông tin

Dữ liệu phải được mã hóa trong quá trình truyền/nhận thông tin qua mạng của tổ chức. Để mã hóa dữ liệu khi truyền, chúng ta có thể sử dụng các cách sau đây:

- Sử dụng một loại bảo vệ có tên WPA2™ với mã hóa AES (độ mạnh khóa 128 bit hoặc cao hơn);

- Sử dụng VPN (mạng ảo riêng) với mã hóa như 3DES hoặc AES.

WPA2 cũng có tính năng gọi là mã kiểm tra tính toàn vẹn ("Message Integrity Code" hay MIC), giúp đảm bảo rằng những gói tin dữ liệu không bị làm giả mạo. Nó như một bản kiểm tra xác nhận để chắc chắn rằng những gì bạn nhận được là chính xác và không bị thay đổi.

8.2.4. Công nghệ Wi-fi không dây

Tất cả các thiết bị truy cập không dây kết nối với mạng của một tổ chức nên sử dụng thiết bị và cấu hình bảo mật Công nghệ Thông tin được bộ phận an ninh Công nghệ Thông tin của tổ chức phê duyệt.

Các công nghệ đã được phê duyệt bao gồm:

- Điểm truy cập (Access Points): Bất kỳ điểm truy cập nào tương thích với chuẩn 802.11a/b/g/n và hỗ trợ WPA2 sử dụng giao thức xác thực mở rộng (EAP).

- Xác thực thẻ mã thông báo PEAP-GTC (Protected EAP-Generic Token Card) và thuật toán AES hoặc xác thực TTLS (EAP - Tunnelled Transport Layer Security) và thuật toán AES.

- Điểm truy cập không dây nên sử dụng các khung xác thực IEEE 802.1x/PEAP-GTC hoặc EAP-TTLS để xác minh người dùng thông qua máy chủ RADIUS/AAA phía sau.

- Thiết bị máy khách (Client Devices): Bất kỳ card giao diện mạng không dây nào tuân thủ chuẩn 802.11a/b/g/n và hỗ trợ ít nhất mã hóa WPA2 (AES).

Không nên sử dụng WEP (Wired Equivalent Privacy) hoặc WPA như một thuật toán mã hóa do những lỗ hổng về bảo mật được xác định công khai.

8.2.5. Các cấu hình Wi-fi khác

Có những ứng dụng sử dụng cấu hình mạng không đáp ứng được yêu cầu bảo mật trong phần này, ví dụ như máy quét kho hàng sử dụng xác thực AAA.

Do đó, chúng ta cần thực hiện một đánh giá về rủi ro bảo mật để xác định các biện pháp kiểm soát bổ sung, nhằm đảm bảo an toàn thông tin. Dưới đây là một số giải pháp khả dụng:

- Sử dụng WPA-PSK, với việc thay đổi đều đặn mật khẩu có độ dài và tính bảo mật tối đa,

- Sử dụng các SSID đặc biệt cho từng mục đích,

- Hạn chế phạm vi truyền dẫn vô tuyến,

- Giới hạn quyền truy cập vào mạng, có thể thông qua tường lửa TCP hoặc các VLAN cô lập, hoặc;

- Đảm bảo sự có sẵn của nhật ký giám sát.

8.2.6. Kiểm soát truy cập – Thiết bị người dùng

Nhìn chung, kiểm soát truy cập cho mạng không dây nên được thực hiện giống như trong mạng có dây.

Cụ thể, chính sách bảo mật cho mạng không dây nên quy định rõ ràng rằng người dùng khách không được phép truy cập vào mạng nội bộ của tổ chức thông qua mạng không dây.

Ngoài ra, một số quy định bảo mật cụ thể có thể nêu rõ rằng nhân viên của tổ chức không nên thiết lập kết nối không dây đồng thời với mạng nội bộ của tổ chức và một mạng bên ngoài mà tổ chức không kiểm soát được (ví dụ như sử dụng Wi-Fi để thiết lập kết nối đồng thời với mạng LAN của tổ chức và một mạng bên ngoài không dưới sự kiểm soát của tổ chức). Do đó, nhân viên không nên kích hoạt chuyển tiếp IP (IP Forwarding), thiết lập kết nối Wireless Peer-to-Peer, sử dụng chế độ Adhoc hoặc thiết lập các hình thức định tuyến khác.

Hệ thống phát hiện/ngăn chặn xâm nhập không dây (WIDS/WIPS) có thể cung cấp một lớp phòng thủ hiệu quả để chống lại các mối đe dọa như các điểm truy cập giả mạo và các cuộc tấn công từ chối dịch vụ (DoS).

WIDS/WIPS bao gồm các cảm biến quét băng tần RF và truyền lại kết quả về một máy chủ quản lý, sau đó máy chủ này có thể thực hiện hành động dựa trên phân tích thông tin được cảm biến ghi lại. Thông thường, WIDS/WIPS cũng sẽ bao gồm một máy chủ cơ sở dữ liệu làm nơi lưu trữ thông tin.

8.2.7. Kiểm soát truy cập – Điểm truy cập cơ sở hạ tầng

Các điểm truy cập nên tuân thủ theo các hướng dẫn cấu hình sau đây.

- Thay đổi mật khẩu quản lý mặc định cho quản trị điểm truy cập (Access Point) bằng mật khẩu mạnh (không chứa từ trong từ điển, không ít hơn 15 ký tự chữ số và chữ cái, với ít nhất một ký tự số hoặc ký tự đặc biệt).

- Sử dụng hạ tầng thiết bị mạng AAA (Authentication, Authorization, and Accounting) để xác thực các quản trị viên điểm truy cập (Access Point)

- Tắt tính năng quản trị mạng LAN không dây từ xa và chỉ cho phép quản trị qua các giao diện Ethernet, USB, hoặc Serial.

- Sử dụng mã hóa đường truyền cho tất cả các quản trị từ xa (ví dụ: sử dụng https/SSH và vô hiệu hóa http/telnet).

- Thay đổi tất cả các chuỗi cộng đồng SNMP mặc định thành mật khẩu khó đoán.

- Nếu có thể, hãy sử dụng SNMPv3 cho các chức năng quản lý mạng trên tất cả các điểm truy cập.

- Khi cài đặt điểm truy cập, thực hiện khảo sát hiện trường để đảm bảo phủ sóng của điểm truy cập được kiểm soát (ví dụ, tránh phát sóng đến các khu vực không mong muốn như bãi đậu xe). Giới hạn phạm vi tín hiệu của bộ định tuyến vào một khu vực cụ thể để hạn chế quyền truy cập cho người dùng không được ủy quyền.

- Đảm bảo bảo mật vật lý cho tất cả các điểm truy cập một cách đủ mạnh để ngăn chặn mất mát hoặc sửa đổi trái phép.

- Thay đổi SSID (hay ‘Service Set Identifier’) từ tên mặc định sang tên mạng nhất quán và cho phép các điểm truy cập phát sóng SSID của họ.

- Theo tính chất của Điểm truy cập, có thể dễ dàng thiết lập mạng không dây với cùng một SSID và sử dụng ăng-ten hướng có độ nhạy cao để che phủ tín hiệu không dây từ điểm truy cập gốc. Mỗi điểm truy cập được chỉ định trong mạng không dây, dưới sự kiểm soát và quản lý của một tổ chức, nên xác thực các thiết bị không dây khi chúng muốn truy cập mạng.

- Tách biệt mạng không dây ra khỏi mạng nội bộ và mạng Internet của tổ chức.

- Cập nhật bộ định tuyến và các điểm truy cập với phiên bản firmware mới nhất nhằm tăng độ tinh cậy và bảo mật

- Hạn chế quyền truy cập của khách hàng, lý tưởng là bằng cách cung cấp một mạng riêng cho khách.

Khi triển khai các điểm truy cập, có thể xuất hiện nhiều tài khoản quản trị đặc quyền được sử dụng để quản lý các điểm truy cập này (có thể có một hoặc nhiều tài khoản đặc quyền cho mỗi điểm truy cập) và điều này đặt ra vấn đề về cách quản lý những tài khoản quản trị đặc quyền này.

Các tổ chức hoặc doanh nghiệp nên đảm bảo có một cơ chế để quản lý những tài khoản đặc quyền này.

Tổ chức nên xem xét việc thực hiện kiểm định bảo mật bởi bên độc lập thứ ba. Một bên thứ ba chuyên về kiểm định bảo mật không dây có thể có nhiều thông tin cập nhật hơn về lỗ hổng bảo mật hiện có và được trang thiết bị tốt hơn để đánh giá bảo mật của một hệ thống mạng không dây.

8.2.8. Khả năng sẵn có

Nói chung, các kỹ thuật đảm bảo tính sẵn có cho mạng không dây (như bộ định tuyến dự phòng, nguồn điện dự phòng, v.v.) nên tương tự như đối với mạng có dây. Đối với Wi-Fi, sự sẵn có của điểm truy cập và thuật toán mã hóa của chúng được hiển thị đến máy tính của khách hàng.

Một số biện pháp hoặc kiểm tra bổ sung có thể được thực hiện cho các mạng Wi-Fi bao gồm:

- Kiểm tra thường xuyên các cấu hình bảo mật của các thành phần mạng Wi-Fi như thiết bị người dùng và các điểm truy cập để đảm bảo rằng chúng tuân thủ theo mức bảo mật tối thiểu hoặc theo cấu hình bảo mật tiêu chuẩn của tổ chức;

- Giám sát mạng Wi-Fi bằng cách sử dụng các hệ thống phát hiện xâm nhập và bảo vệ không dây được đặt tại các điểm khác nhau trong cơ sở của tổ chức, hệ thống này có thể phát hiện sự bất thường trong các mẫu lưu lượng trên mạng không dây.

Cả hai biện pháp này đều được thiết kế để phát hiện những thay đổi trong đặc tính của mạng Wi-Fi hoặc của các thiết bị người dùng. Điều này có thể là dấu hiệu tiền đề cho một cuộc tấn công. Những điểm yếu như vậy có thể bị tận dụng và từ đó làm giảm khả năng sẵn có của mạng.

8.2.9. Trách nhiệm giải trình

Khi được pháp luật hoặc quy định cho phép, việc kích hoạt ghi nhật ký tập trung trên các điểm truy cập nên được kích hoạt để ghi lại hoạt động của người dùng và sự kiện, chẳng hạn như:

- Thời điểm xảy ra sự kiện,

- Địa chỉ MAC (địa chỉ vật lý của thiết bị mạng),

- Tên người dùng,

- Thành công hoặc thất bại của sự kiện,

- Loại sự kiện, ví dụ như lần đăng nhập,

- Khởi động lại hệ thống,

- Thay đổi cấu hình,

- Kết nối/ngắt kết nối, có thể chỉ ra việc thử tấn công từ chối dịch vụ (DoS),

- Xác định điểm truy cập giả mạo.

Định kỳ, mạng không dây nên được quét để phát hiện các điểm truy cập trái phép trong các cơ sở được quản lý của tổ chức, nhằm hiểu rõ tình trạng an ninh mạng không dây.

8.3 Thiết kế bảo mật cho di động viễn thông

Hệ thống di động viễn thông (còn được gọi là hệ thống di động tế bào) thường bao gồm các trạm cơ sở, bộ điều khiển mạng vô tuyến và các giao diện hoặc cổng kết nối vào mạng lõi của nhà khai thác. Các trạm cơ sở này hỗ trợ một hoặc nhiều ô khu vực mà khi kết hợp lại có thể bao phủ diện tích lớn. Ban đầu, hệ thống được phát triển chủ yếu để hỗ trợ cuộc gọi thoại, đồng thời hỗ trợ một lượng lớn người dùng điện thoại, cho phép chuyển giao giữa các ô khi thiết bị di động của người dùng di chuyển và có khả năng kết nối với các mạng của các nhà khai thác khác. Các hệ thống di động như LTE cũng có thể cung cấp truy cập Internet tốc độ cao cho các thiết bị như máy tính xách tay, điện thoại thông minh và thiết bị di động khác.

Bảo mật trong hệ thống di động viễn thông bao gồm các tiêu chuẩn xác thực tương tác giữa thiết bị người dùng và mạng, cơ chế bảo vệ tính toàn vẹn và tính bảo mật dữ liệu, kiểm soát truy cập vào mạng. Khi việc tích hợp Wi-Fi và hệ thống di động, các mối đe dọa bảo mật cụ thể đối với sự tích hợp này cũng đang được giải quyết theo Tiêu chuẩn Quốc tế.

Nếu nhân viên (của một doanh nghiệp hoặc tổ chức) đang sử dụng các thiết bị di động viễn thông, thì thông thường các thiết bị này sẽ được kiểm soát và duy trì bởi nhà cung cấp dịch vụ, và do đó người dùng có thể không có quyền kiểm soát các tùy chọn bảo mật như mã hóa dữ liệu và xác thực điểm truy cập hay thiết bị.

Dữ liệu truyền tải trên mạng truy cập vô tuyến (RAN, hay “Radio Access Network”) có thể được mã hóa, nhưng không có gì đảm bảo rằng liên kết từ đầu đến cuối là an toàn.

Vì mạng RAN được điều khiển bởi nhà khai thác và mã hóa thông tin, có thể không được đảm bảo, nên người dùng cuối nên sử dụng cơ chế bảo mật thay thế, chẳng hạn như sử dụng VPN khi truyền thông tin nhạy cảm hoặc bí mật.

8.4 Bluetooth

Bluetooth là một tiêu chuẩn công nghệ không dây dùng để trao đổi dữ liệu qua các khoảng cách ngắn (sử dụng truyền vi sóng bước sóng ngắn trong dải tần RF từ 2 400 MHz đến 2 480 MHz) giữa các thiết bị cố định và di động, cũng như xây dựng các mạng khu vực cá nhân (PANs).

Bluetooth được quản lý bởi Bluetooth Special Interest Group (SIG), tổ chức chịu trách nhiệm giám sát quá trình phát triển thông số kỹ thuật và quản lý chương trình chứng nhận. Tất cả các phiên bản của các tiêu chuẩn Bluetooth đều được thiết kế để tương thích với các phiên bản trước đó. Các phiên bản sau của tiêu chuẩn này cung cấp các cải tiến về khả năng Bluetooth, tốc độ truyền dữ liệu cao hơn, kết nối nhanh hơn, phát hiện thiết bị nhanh chóng, kết nối an toàn giữa các thiết bị, hỗ trợ thiết bị tiết kiệm năng lượng và kết nối được mã hóa an toàn.

Đối với Bluetooth, tính bảo mật của một liên kết điểm đến điểm và thậm chí là một Bluetooth PAN lớn phần lớn phụ thuộc vào phiên bản tiêu chuẩn Bluetooth được hỗ trợ hoặc đang sử dụng trên thiết bị. Các điểm yếu đối với từng phiên bản đã được công bố và thông tin chi tiết có thể được tìm thấy trong các tài liệu tham khảo nổi tiếng. Vui lòng tham khảo mục Tham Khảo để biết thông tin chi tiết.

Do các điểm yếu bảo mật vốn có sẵn trong các giao thức Bluetooth, khả năng truyển dữ liệu tồn tại trên các thiết bị Bluetooth (dưới sự kiểm soát của tổ chức) nên được tắt.

Bluetooth có hầu hết các yếu điểm bảo mật như các hệ thống không dây nói chung. Một bộ phát Bluetooth gửi tín hiệu qua không gian tự do đến bất kỳ bộ thu nào, có thể là hợp lệ hoặc không hợp lệ, nằm trong phạm vi. Ngoài ra, Bluetooth hoạt động trong dải tần không được cấp phép 2,4 GHz, và không có hạn chế đối với việc bán các thiết bị truyền và nhận tín hiệu trong dải tần này. Do đó, một thiết bị giám sát trái phép không cần tiếp xúc trực tiếp với một bộ phát Bluetooth có thể chặn tín hiệu của nó. Thiết bị giám sát như vậy dễ giấu kín, không phát hiện được khi sử dụng, và triển khai nhanh chóng hơn so với thiết bị nghe lén truyền thống.

Nhiều cuộc tấn công nhằm vào các lỗi triển khai hoặc thiếu sót về bảo mật trong Bluetooth đã được ghi chéo trong văn bản công khai. Dưới đây là một số ví dụ.

a. Bluedumping: cuộc tấn công nói trên dựa trên tính toán ngược lại mã PIN của người dùng dựa trên các trao đổi ghép nối bị chặn.

b. Bluesmarfing: cho phép kẻ tấn công truy cập vào danh bạ điện thoại và cơ sở dữ liệu cuộc hẹn trên các thiết bị mục tiêu do lỗi thực hiện trong giao thức OBEX Push.

c. Bluebugging: sử dụng các kênh Bluetooth RFCOMM ẩn và cho phép kẻ tấn công từ xa kiểm soát hầu hết các khía cạnh của một thiết bị điện thoại, bao gồm việc thực hiện các cuộc gọi trái phép và bật micrô để biến điện thoại thành thiết bị nghe lén.

d. Bluejacking: thiếu bảo mật trên hồ sơ OBEX trên một số thiết bị cho phép kẻ tấn công thêm các mục tùy ý vào danh sách điện thoại của thiết bị mục tiêu.

e. Bluestabbing: kẻ tấn công sửa đổi tên thiết bị Bluetooth với định dạng sai, gây ra sự cố cho thiết bị mục tiêu khi cố gắng khám phá các thiết bị khác xung quanh.

f. Bluebumping: cuộc tấn công kỹ thuật xã hội tận dụng thực tế là một cặp kết nối không bao giờ biến mất hoặc tự động xóa đi cho đến khi cả hai thiết bị trong cặp xóa kết nối; kẻ tấn công sẽ sử dụng kỹ thuật xã hội để thuyết phục mục tiêu ghép kết nối với thiết bị của họ và sẽ xóa kết nối khỏi thiết bị của mình sau đó, nhưng kẻ tấn công sẽ không xoá, từ đó cho phép kẻ tấn công có một lối "cửa sau" vào thiết bị mục tiêu.

g. Bluesmacking: các chuỗi truy vấn định dạng sai dẫn đến "ping of death", làm sập hệ thống bất kỳ thiết bị nào nhận được tin nhắn đó.

Người dùng nên tuân thủ các nguyên tắc bảo mật sau đây để bảo vệ thông tin cá nhân:

- Chỉ bật chức năng Bluetooth khi cần thiết.

- Sử dụng chế độ bảo mật Bluetooth mạnh nhất.

- Giữ các thiết bị được ghép kết nối càng gần nhau càng tốt khi các liên kết nối Bluetooth đang hoạt động.

- Chỉ để thiết bị ở chế độ khả dụng khi thực sự cần thiết.

- Tránh sử dụng mã PIN cố định yếu (mã mặc định của nhà sản xuất thường là "0000".

- Thiết lập cấu hình thiết bị Bluetooth và phần mềm theo chính sách đã thiết lập.

- Bảo vệ mã PIN khỏi việc bị chặn hoặc giải mã bởi kẻ tấn công.

- Dữ liệu nhận dạng và các khóa của thiết bị cần được bảo vệ.

- Sử dụng bảo mật tầng ứng dụng và hạ tầng khóa công cộng để cung cấp các biện pháp bảo mật bổ sung.

- Thiết lập các nguyên tắc cấu hình thiết bị, chính sách bảo mật, và các cơ chế thực thi cho việc sử dụng các thiết bị Bluetooth.

8.5 Các công nghệ không dây khác

Sẽ luôn có các công nghệ không dây mới được phát triển hoặc các biến thể của các công nghệ hiện có. Một số trong đó sẽ có các cơ chế bảo mật đã được định rõ. Việc đánh giá rủi ro đối với thông tin có thể được truyền qua công nghệ và cách công nghệ vô tuyến tương tác với cơ sở hạ tầng IT của tổ chức luôn được khuyến khích thực hiện. Sẽ là một lợi thế nếu có một Tiêu chuẩn Quốc tế có sẵn bao gồm mô tả hoặc định nghĩa về các biện pháp an ninh được hỗ trợ bởi công nghệ, phân tích mối đe doạ của công nghệ và đề xuất về cách triển khai và tích hợp công nghệ một cách an toàn vào cơ sở hạ tầng IT. Nếu không rõ ràng rằng công nghệ có thể cung cấp các biện pháp bảo mật, thì tổ chức nên đưa ra quyết định về việc liệu có nên sử dụng công nghệ đó hay không và nếu có, thì những biện pháp an ninh bổ sung nào nên được thiết lập để đảm bảo an toàn.

Trong nhiều tổ chức, nhiều công nghệ không dây được hỗ trợ và các thiết bị người dùng có thể được kết nối với nhiều mạng không dây cùng một lúc, chẳng hạn như mạng điện thoại di động, Bluetooth và mạng Wi-Fi, và trong một số trường hợp, thiết bị người dùng cũng có thể được kết nối với mạng có dây. Vì vậy, nếu kẻ tấn công có được quyền truy cập không dây trái phép vào thiết bị người dùng đa kết nối, kẻ tấn công có thể sử dụng nó để truy cập hoặc tấn công các tài nguyên trên mạng có dây. Các tổ chức nên đánh giá rủi ro do việc sử dụng kết hợp các công nghệ không dây và xác định cách giảm thiểu những rủi ro đó. Nếu một hoặc nhiều trong số các mạng không thể giảm thiểu rủi ro ở mức chấp nhận được, thì việc kết nối kép liên quan đến mạng đó có thể tạo ra quá nhiều rủi ro cho tổ chức và có thể cần bị cấm.

Thư mục tài liệu tham khảo

[1] NIST Special Publication 800-153 — Guidelines for securing Wireless Local Area Networks (WLANS), February 2012.

[2] NIST Special Publication 800-121 — Guide to Bluetooth Security, June 2012.

[3] IT Security — Technical Publication — 802.11 Wireless LAN Vulnerability Assessment (ITSPSR-21A), Communications Security Establishment Canada (CSEC), May 2009.

[4] IEEE 802.11, IEEE Standard for Information technology — Telecommunications and information exchange between systems

[5] 3GPP TS 33.821 — Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE) (http://www.3gpp.org/DynaReport/33821.htm)

[6] NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.

[7] IEEE 802.151)Working Group for WPAN

[8] IEEE 802.112)WIRELESS LOCAL AREA NETWORKS

[9] The IEEE 802.16 Working Group on Broadband Wireless Access Standards (http://ieee802.org/16/)

[10] IEEE 802.223)Working Group on Wireless Regional Area Networks

[11] ZigBee Alliance. https://www.zigbee.org/

[12] Wi-Fi Alliance. http://www.wi-fi.org/

[13] Alliance W.A.P.I. http://www.wapia.org/

[14] Bluetooth technology (https://www.bluetooth.com/)

[15] WiMAX Forum. http://www.wimaxforum.org/

[16]. NIST Special Publication 800-48 — Guide to Securing Legacy IEEE 802.11. Wirel. Netw. 2008 July.