Câu 1: Trình bày khái niệm mạng không dây, thành phần và hoạt động cơ bản của mạng không dây

**Khái niệm**

Mạng không dây là một hệ thống các thiết bị được nhóm lại với nhau, có khả năng giao tiếp thông qua sóng vô tuyến thay vì các đường truyền dẫn bằng dây. Vì đây là mạng dựa trên chuẩn IEEE802.11 nên nó còn được gọi là mạng 802.11 network ethernet để nhấn mạng mạng này dựa trên mạng Ethernet. Một tên gọi quen thuộc khác của mạng không dây là: Wifi

**Thành phần**

* Wireless NICs:
  + Là card không dây được tích hợp vào các thiết bị máy tính để kết nối với mạng không dây.
* Wireless Home Router:
  + Kết hợp chức năng của bộ định tuyến và một điểm truy cập không dây (access point). Wireless Router giúp kết nối mạng không dây với Internet và mạng có dây.
* Wireless Access Point:
  + Là thiết bị trung tâm trong mạng không dây, chịu trách nhiệm kết nối các thiết bị không dây với mạng có dây.
* Wireless Antenna:
  + Dùng để truyền và nhận tín hiệu không dây giữa các thiết bị trong mạng. Các loại anten thường sử dụng bao gồm anten tích hợp, enten ngoại vi và anten hướng.

**Hoạt động cơ bản của mạng không dây**

Hoạt động cơ bản của mạng không dây là truyền tải dữ liệu qua không gian bằng cách sử dụng sóng thay vì dây truyền.

* Phát sóng từ thiết bị gửi: Một thiết bị không dây như router hoặc access point sẽ phát sóng tín hiệu không dây
* Thu sóng tại thiết bị nhận: Thiết bị không dây như máy tính được trang bị Wireless NIC để thu sóng
* Chuẩn hóa dữ liệu: Dữ liệu được chuyển đổi thành các fois tin với định dạng chuẩn để truyền qua mạng.
* Truyền dữ liệu qua sóng Radio: gói tind dược truyền qua không gian dưới dạng sóng radio. Sóng radio này có thể hoạt động ở các băng tần nhưu 2.4 GHz hoặc 5 GHz tùy thuộc vào tiêu chuẩn và thiết bị sử dụng
* Điều chỉnh tần số và kênh truyền: Tần số và kênh truyền được chọn để giảm nhiễu và xung đột tín hiệu trong môi trường không dây
* Thu sóng và phục hồi dữ liệu: Thiết bị nhận thu sóng radio, giải mã và phục hồi dữ liệu gói tin.
* Gửi và nhận dữ liệu: Dữ liệu được chuyển đến các thiết bị trong mạng không dây và ngược lại
* Bảo mật và quản lý kết nối: Các giao thức bảo mật như WPA hay WPA2 đượ sử dụng để đảm bảo an toàn dữ liệu truyền qua mạng không dây.

Câu 2: Phân tích các vấn đề an toàn khi sử dụng giao thức WPA2 trong mạng không dây

* Tấn công Brute Force: WPA2 nếu được cấu hình đúng cách với mật khẩu mạng có thể chống lại tấn công Brute Force. Tuy nhiên, nếu mật khẩu yếu đây có thể là một lỗ hổng
* Tấn công từ điểm truy cập giả mạo: Một điểm yếu của WPA2 là khả năng xuất hiện điểm truy cập giả mạo trong mạng. Kẻ tấn công có thể tạo ra một điểm truy cập không dây giả mạng và cố gắng lừa người dùng kết nối từ đó thu tập thông tin đăng nhập
* Replay attack: sự kiểm tra lại có thể xảy ra khi kẻ tấn công ghi lại lưu lượng mạng sau đó phát lai để xâm nhập vào hệ thống. WPA2 sử dụng các kỹ thuật như TKIP để ngăn chặn sự kiểm tra lại.
* Dictionary attack: kỹ thuật tấn công từ điển là một hình thức tấn công mật khẩu nới kẻ tấn công sử dụng một danh sách các mật khẩu phổ biến hoặc từ điển thử nghiệm.
* Lỗ hổng WPS: Nếu WPS được kích hoạt, nó có thể tạo ra lỗ hổng bảo mật nếu không được cấu hình đúng. Kẻ tấn công có thể sử dụng tấn cốn Force WPS để xâm nhập vào mạng.
* Tấn công Key Reinstallation: loại tấn công này có thể tận dụng lỗ hổng trong việc cài đặt khóa để đánh bại hệ thống bảo mật WPA2

Câu 3: Phân tích về hình thức tấn công Deauthentication trong mạng không dây

Tấn công Deauthentication là một hình thức tấn công mạng không dây nhằm làm mất kết nối giữa các thiết bị không dây và điểm truy cập (AP) hoặc giữa các thiết bị không dây với nhau.

**Nguyên tắc hoạt động**

Tấn công deauthentication sử dụng các gói tin Deauthentication để làm thông báo cho các thiết bị không dây hoặc điểm truy cập rằng thiết bị nào đó muốn kết thúc kết nối hiện tại. Gói tin này được gửi đến địa chỉ MAC của thiết bị cụ thể mà kẻ tấn công muốn làm mất kết nối.

**Đối tượng tấn công**

Tấn công Deauthentication có thể nhắm đến cả thiết bị không dây cá nhân hoặc các điểm truy cập trong mạng. Nếu một điểm truy cập bị tấn công, tất cả các thiết bị kết nối đến nó sẽ bị mất kết nối.

**Mục đích tấn công**

* Gây phiến toái: làm mất kết nối liên tục gây ra phiền toái
* Tấn công Man-in-the-Middle: tạo điều kiện cho kẻ tấn công thực hiện tấn công Man-in-the-Middle sau khi làm mất kết nối
* Chống lại các biện pháp bảo mật: gây ra sự cố với các biện pháp bảo mật như WIPS bằng cách làm giảm hiệu suất của chung.

**Biên pháp phòng ngừa**

* Sử dụng WPA3, cung cấp bảo mật cao hơn so với WPA2
* Thực hiện quản lý địa chỉ MAC của các thiết bị truy cập vào mạng.

Câu 4: Phân tích các vấn đề an toàn khi sử dụng thiết bị di động IOS; Trình bày các giải pháp nâng cap an toàn khi sử dụng thiết bị di động IOS trong mạng không dây

Một số vấn đề an toàn khi sử dụng thiết bị di động IOS là

* Phiên bản hệ điều hành cũ: Nếu người dụng không cật nhật hệ điều hành IOS lên phiên bản mới, họ có thể đối mặt với lỗ hổng bảo mật đã được vá trong các phiên bản cật nhật mới.
* Mã điều khiển truy cập: Passcode hoặc mã PIN được sử dụng để mở khóa thiết bị. Sử dụng mật khẩu mạnh để đảm bảo an toàn
* Ứng dụng từ nguồn không đáng tin cậy: ứng dụng này có thể chứa mã độc hại hoặc thu thập thông tin cá nhân mà không được kiểm soát.
* Quyền truy cập ứng dụng: Việc kiểm soát quyền truy cập của ứng dụng đến các thông tin nhạy cảm là quan trọng.

Các giải pháp nâng cao bảo mật

* Luôn cập nhật: Các lỗi bảo mật trên iOS (và sau này còn có thêm iPadOS) một khi được công khai đều chứa nhiều nguy cơ bảo mật, do vậy Apple thường xuyên tung ra các bản vá bảo mật nhằm khắc phục chúng thông qua các bản cập nhật
* Sử dụng Passcode bảo mật hơn, bên cạnh Face ID hoặc Touch ID: - Bảo vệ màn hình khóa
* Không nhấn vào các liên kết đáng ngờ
* Tránh sử dụng các dịch vụ Wi-Fi công cộng không được bảo mật
* Sử dụng mạng riêng ảo VPN
* Cẩn thận khi cấp quyền cho ứng dụng

Câu 5: Android

Các vấn đề bảo mật của Android:

* Sự phân mảnh: là một hệ điều hành mã nguồn mở, Android có nhiều phiên bản sửa đổi được triển khai trên số lượng lớn thiết bị.
* Mã độc:
  + Ước tính trung bình có khoảng 11,7 nghìn mẫu độc Android mới được phát hiện mỗi ngày
  + Phần lớn các cuộc tấn công này nhắm vào các dịch vụ ngân hàng trực tuyến và các ứng dụng di động
* Lựa chọn công cụ quản lý
* Hành vi người dùng
  + Người sử dụng luôn đóng vai trò quan trọng trong việc bảo đảm an toàn cho thiết bị cũng như dữ liệu chứa trong nó
* Rò rỉ dữ liệu: Rò rỉ dữ liệu phát sinh khi người dùng di động không biết về ý nghĩa của việc bảo mật thông tin cá nhâ, cung cấp cho ứng dụng quyền lấy dữ liệu

**Giải pháp an toàn Android**

* Quản lý quyền ứng dụng:
  + Nên gỡ bỏ các ứng dụng High Risk vì chúng có thể đánh cắp mật khẩu hay đọc lén email của bạn.
  + Ngoài ra, hiện còn có ứng dụng di động Anti-Malware của Malwarebytes giúp kiểm tra các ứng dụng và phân loại ứng dụng tùy theo tính năng nào của điện thoại chúng có thể truy cập cho bạn thấy rõ ứng dụng nào có ý đồ gì
* Hạn chế sử dụng Wifi miễn phí
* Bảo mật thiết bị
* Tải ứng dụng từ những nguồn đáng tín cậy
* Cài đặt những bản cập nhật mới nhất
* Mã hóa dữ liệu
* Thường xuyên sao lưu dữ liệu điện thoại

**Câu 6:** Tấn công Man-in-the-Middle trong mạng không dây

Là trường hợp trong đó hacker sử dụng một AP để đánh cáp các node di động bằng cách gửi tín hiệu RF mạnh hơn AP hợp pháp đến các node đó

Các node di động nhận thấy AP phát tín hiệu RF manh tốt hơn sẽ kết nối đến AP giả mạo này, truyền dữ liệu có thể là những dữ liệu nhạy cảm đến AP giả mạo và hacker có toàn quyền xử lý

**Câu 7**: Tìm hiểu về WEP, WPA, WPA2, WPA3 và so sánh các giao thức trên.

- WEP — Giao thức bảo mật Wi-Fi đầu tiên

+ WEP là giao thức bảo mật Wi-Fi đầu tiên

+ Ban đầu nó được kỳ vọng sẽ cung cấp mức độ bảo mật tương tự như mạng có dây. Tuy nhiên, vào thời điểm đó, công nghệ mật mã bị hạn chế và các thiết bị Wi-Fi bị giới hạn ở mã hóa 64-bit.

+Mặc dù giới hạn đã bị phá vỡ và tăng lên 128-bit, nhưng cũng có nhiều vấn đề bảo mật trong WEP khiến khóa dễ bị bẻ khóa.

+ Với tư cách là một giao thức bảo mật không dây rất dễ bị tấn công và không thể chịu trách nhiệm bảo vệ an ninh, cuối cùng đã được thay thế bằng WPA.

- WPA — Cải tiến tạm thời cho WEP

+ Vào năm 2003, khi WEP dần bộc lộ điểm yếu của mình

+ WPA đã được Wi-Fi Alliance thông qua như một giải pháp thay thế cho WEP.

+ Công nghệ mã hóa 256 bit đã được đưa vào WPA

+ Trong tiêu chuẩn WPA, có sự đa dạng giữa hai chế độ: WPA-Enterprise và WPA-Personal, sử dụng các phương pháp mã hóa khác nhau.

- WPA2 — Cải tiến dựa trên WPA + WPA2 đã được phê chuẩn là tiêu chuẩn bảo mật Wi-Fi mới vào năm 2004.

+ Cải tiến đáng kể nhất trong tiêu chuẩn bảo mật WPA2 là việc triển khai Tiêu chuẩn mã hóa nâng cao (AES), cung cấp hiệu suất và bảo mật cao hơn.

+ Vẫn còn một lỗ hổng gây ra các vấn đề về bảo mật vì tin tặc có thể truy cập vào mạng WPA2 bảo mật và có quyền truy cập vào một số khóa nhất định để tấn công các thiết bị khác trên cùng mạng.

- WPA3 — Bảo mật Wi-Fi thế hệ tiếp theo

+ WPA3 đã được Liên minh Wi-Fi đề xuất vào tháng 6 năm 2018.

+ Sự ra đời của WPA3 khắc phục việc bảo vệ chống lại các lỗ hổng trong WPA2 chẳng hạn như tấn công từ điển.

+ Đối với các mạng công cộng như quán cà phê hoặc khách sạn, WPA3 có khả năng bảo mật thực sự tốt vì nó sẽ tự động mã hóa kết nối mà không cần bất kỳ thông tin đăng nhập nào.

- WEP so với WPA so với WPA2 và WPA3: Từ phần giới thiệu ở trên, có thể thấy rằng từ WEP đến WPA3, mọi loại giao thức bảo mật đều là sự cải tiến và nâng cao so với loại giao thức cuối cùng. Sau đây là biểu đồ so sánh sẽ giúp bạn biết bốn thế hệ giao thức bảo mật Wi-Fi thay đổi như thế nào về mọi mặt. Từ phần giới thiệu ở trên, có thể thấy rằng từ WEP đến WPA3, mọi loại giao thức bảo mật đều là sự cải tiến và nâng cao so với loại giao thức cuối cùng. Sau đây là biểu đồ so sánh sẽ giúp bạn biết bốn thế hệ giao thức bảo mật Wi-Fi thay đổi như thế nào về mọi mặt.