Đề cương ôn tập

Câu 1: Tìm hiểu về các công nghệ mạng 1G, 2G, 3G, 4G,5G 2

Câu 2: Tìm hiểu các chuẩn WLAN IEEE 802.11 3

Câu 3: Trình bày định nghĩa macro mobility. Trình bày về giao thức Mobile IP. 4

Câu 4: Trình bày định nghĩa micro mobility. Trình bày về giao thức cellular Ip và giao thức Fast handoff. 4

Câu 6: Tìm hiểu về thành phần của mạng không dây. 5

Câu 7: Tìm hiểu hoạt động của mạng không dây. 6

Câu 8: Tìm hiểu các mối đe doạ và các cuộc tấn công lên mạng không dây. 8

* Các kiểu tấn công trên WLAN 9

Câu 9: Tìm hiểu về WEP, WPA, WPA2, WPA3 và so sánh các giao thức trên. 10

So sánh 4 kĩ thuật xác thực khóa chia sẻ bao gồm WEP, WPA, WPA2, WPA3 11

Câu 10: Trình bày các thách thức bảo mật của Apple. 12

Câu 11: Trình bày các giải pháp bảo mật đối với Apple iOS. 12

Câu 12: Trình bày các thách thức bảo mật của Android. 13

Câu 13: Trình bày giải pháp đảm bảo an toàn của Android. 13

Câu 14: Trình bày về BYOD. 14

Câu 1: Tìm hiểu về các công nghệ mạng 1G, 2G, 3G, 4G,5G

*1G

- Giai đoạn: 1980-1990
- Tốc độ: 2,4 kbps
- Chất lượng gọi thấp
- Pin kém, điện thoại cồng kềnh
- Không bảo mật dữ liệu
- 1G là thế hệ đầu tiên của mạng di động viễn thông với kết nối analog
- thiết bị sử dụng tín hiệu Analog khá cồng kềnh vì nó phải gắn 2 module (thu và phát tín hiệu).

*2G

- Giai đoạn: 1991-2000
- Tốc độ: 9.6 kbps
- GSM/CDMA/edge
- chuyển từ Analog sang Digital network
- Có thêm dịch vụ SMS, trình duyệt web
- là thế hệ thứ hai của mạng di động
- Mạng 2G cho phép người dùng gọi thoại với tín hiệu đã được mã hóa dưới dạng tín hiệu kỹ thuật số (dạng nhị phân 0 và 1). Vậy nên tính bảo mật thông tin của 2G được cải thiện hơn rất nhiều so với mạng 1G.
- 2G cũng hỗ trợ nhiều người dùng cùng một lúc trên mỗi dải tần hoạt động
- 2 phiên bản nữa là mạng 2.5G và mạng 2.75G.

*3G

- Digital network
- Hệ thống viễn thông di động toàn cầu
- Thêm chức năng: cuộc gọi toàn cầu, cuộc gọi video
- cải thiện mạnh mẽ nhất là phần băng thông, cũng như tốc độ truyền dữ liệu so với mạng 2G.
- Tốc độ truyền tải dữ liệu của 3G đạt từ 384 Kbps đến 2 Mbps trong một giây, giúp người dùng có thể gửi và nhận những email có kích thước lớn hơn với tốc độ nhanh hơn.

*4G

- Là thế hệ thứ 4 và vẫn đang phổ biến ở thời điểm hiện tại
- Tốc độ truyền cực nhanh, lý tưởng nhất vào khoảng 1Gb đến 1.5 GB/s
- Có 2 chuẩn 4G phổ biến: LTEA và Giga Lte

*5G

- Là thế hệ thứ 5, Chưa được phổ cập rộng rãi cho tất cả người dùng
- Tốc độ truyền mnhanh gấp 10 lần 4G

Câu 2: Tìm hiểu các chuẩn WLAN IEEE 802.11

* 802.11

- Thế hệ đầu tiên và năm 1997
- Sử dụng tần số tín hiệu vô tuyến 2.4 GHz
- Chỉ hỗ trợ mạng với băng tầng lớn nhất chỉ 2Mbps

*802.11b

- Thế hệ thứ 2 với tên 802.11b ra mắt năm 1999
- Chuẩn mạng mới này hỗ trợ băng thông tối đa lên đến 11Mbps
- Chuẩn mạng 802.11b cũng sử dụng tần số tín hiệu vô tuyến 2.4 GHz
- Tuy tốc độ cao hơn nhưng lại dễ bị nhiễu từ các thiết bị điện tử khác như điện thoại không dây, lò vi sóng, những thiết bị sử dụng dải tần số 2.4 GHz

*802.11a

- 802.11a và 802.11b được IEEE tạo ra cùng một thời gian
- 802.11a thường được sử dụng trong các mạng doanh nghiệp còn 802.11b thích hợp hơn với mạng gia đình.
- Tần số của 802.11a cao hơn so với 802.11b chính vì vậy chuẩn mạng 802.11b dễ dàng xuyên qua các vách tường và các vật cản khác hơn.
- 802.11a hỗ trợ băng thông cao hơn nhiều so với 802.11b lên đến 54 Mbps và tín hiệu trong một phổ tần số 5GHz
- 802.11a và 802.11b hoạt động trên hai tần số khác nhau nên hai công nghệ này không thể tương thích với nhau. Chính vì vậy một thiết bị cùng lúc chỉ có thể kết nối một trong hai mạng.

* 802.11g(wifi 3)

- 802.11g là một chuẩn mạng mới được thiết kế và xây dựng dựa trên những ưu điểm của hai chuẩn 802.11a và 802.11b
- Chuẩn mạng này hỗ trợ băng thông lên đến 54Mbps và sử dụng tần số 2.4 Ghz
- 802.11g có khả năng tương thích với các chuẩn 802.11b

*802.11n

- Thế hệ thứ 4
- Là bảng nâng cấp của chuẩn mạng 802.11g và được thiết kế để cải thiện những nhược điểm của thế 802.11g cũng như thay thế cho tất cả các thế hệ mạng trước đó
- Cung cấp băng thông tối đa lên đến 600 Mbps
- 802.11n có khả năng tương thích ngược với các thiết bị 802.11b, 802.11g

*802.11ac

- Thế hệ thứ 5, là chuẩn WiFi mới nhất, được sử dụng rộng rãi nhất hiện nay
- Mang trên mình công nghệ không dây băng tầng kép
- 802.11ac hỗ trợ các kết nối trên cả hai băng tần 2.4 GHz và 5 GHz. 802.11ac cung cấp khả năng tương thích ngược với các chuẩn kết nối mạng 802.11b, 802.11g, 802.11n
- Tốc độ băng thông đạt tới 1.300 Mbps trên băng tần 5 GHz, 450 Mbps trên 2.4GHz.

Câu 3: Trình bày định nghĩa macro mobility. Trình bày về giao thức Mobile IP.

*Định nghĩa:

- Di động macro (Macromobility) là sự dịch chuyển của MN giữa các subnet trong phạm vi một miền hoặc vùng. - Giải pháp cho di động macro này là các giao thức di động liên mạng (lớp 3) như Mobile IP.

* Trình bày về giao thức Mobile IP

- Mobile IP cho phép một nút mạng thay đổi điểm kết nối POA mà vẫn có duy trì được kết nối IP thông qua các tác nhân di động MA là: Trạm gốc HA và trạm ngoài FA
- Mobile IP sử dụng một cặp địa chỉ để quản lý việc dịch chuyển của người dùng. Mỗi khi một một nút MN trong mạng IP dịch chuyển dẫn tới thay đổi POA, MN sẽ có một địa chỉ tạm cấp gọi là COA
- Sự có mặt của một FA tại một subnet nào đó có thể được MN phát hiện thông qua các thông điệp quảng bá
- Các thông điệp đó được quảng bá bởi FA theo các chu kỳ thời gian nhất định.
- Mỗi lần FA gán một địa chỉ COA cho một MN mới, nó sẽ cập nhật một chỉ mục cho MN này trong một bảng riêng gọi là "danh sách trạm khách".
- Sau khi MN đã có một địa chỉ COA mới, nó sẽ thông báo cho HA của nó về địa chỉ COA mới đó thông qua tiến trình đăng ký
- Ngay khi HA của MN nhận được thông báo về COA mới của MN, HA sẽ chặn các gói tin tới mạng thường trú của MN đang gửi tới MN
- Sau đó, MA sẽ chuyển các gói tin đó tới FA. Tại mạng mà MN đang kết nối, FA nhận được các gói tin đã đóng gói, FA sẽ chuyển các gói tin ban đầu tới MN

Câu 4: Trình bày định nghĩa micro mobility. Trình bày về giao thức cellular Ip và giao thức Fast handoff.

* Định nghĩa:

- Di động micro (Micromobility) là sự dịch chuyển của MN trong phạm vi một BS hoặc giữa các BS nhưng bên trong phạm vi của một subnet và xảy ra rất nhanh.
- Quản lý sự đi động ở mức micro nên thuộc về lớp liên kết (tầng 2)

* Cellular IP

- Một vùng Cellular IP (Cellular IP domain) bao gồm các MA và một trong số đó đóng vai trò như một gateway ra Internet và đồng thời như một Mobile IP FA cho các di động micro.
- Mỗi MA sẽ duy trì một bản lưu các định tuyến
- Bản lưu này được sử dụng bởi MA để chuyển tiếp các gói tin từ gateway tới MN hoặc từ MN tới gateway.
- Các tuyến (router) được thiết lập và được cập nhật thông qua các trao đổi giữa các nút cạnh nhau

* Fast handoff

- Fast Handoff sửdụng lại kiến trúc vànguyên lýcủa Mobile IP phân cấp vàhướng vào giải quyết hai vấn đề:

+ Quản lýquá trình chuyển tiếp nhanh cho các ứng dụng thời gian thực
+ Định tuyến tam giác bên trong các vùng

Câu 6: Tìm hiểu về thành phần của mạng không dây.

* Wireless NICs

- Để giao tiếp không dây, máy tính xách tay, máy tính bảng, điện thoại thông minh và thậm chí cả ô tô mới nhất bao gồm NIC không dây tích hợp kết hợp bộ phát / thu vô tuyến
- Nếu thiết bị không có NIC không dây tích hợp, thì có thể sử dụng bộ điều hợp không dây USB

* Wireless Home Router

- Bộ định tuyến không dây hoạt động như sau:
+ Điểm truy cập: Để cung cấp quyền truy cập dây
+ Chuyển đổi: Để kết nối các thiết bị có dây với nhau
+ Bộ định tuyến: Để cung cấp một cổng mặc định vào các mạng khác và Internet

* Wireless Access Point

- Máy khách không dây sử dụng NIC không dây của họ để khám phá các điểm truy cập (AP) gần đó.
- Sau đó, khách hàng cố gắng liên kết và xác thực với một AP. Sau khi được xác thực, người dùng không dây có quyền truy cập vào tài nguyên mạng.

* AP Categories

- AP tự động: Các thiết bị độc lập được định cấu hình thông qua giao diện dòng lệnh hoặc GUI.
- AP dựa trên bộ điều khiển: Sử dụng Giao thức điểm truy cập nhẹ (LWAPP) để giao tiếp với bộ điều khiển LWAN (WLC). Mỗi LAP được cấu hình và quản lý tự động bởi WLC

* Wireless Antennas

- Đa hướng - Cung cấp vùng phủ sóng 360 độ. Lý tưởng trong nhà và khu văn phòng.
- Định hướng - Tập trung tín hiệu vô tuyến theo một hướng cụ thể.

Câu 7: Tìm hiểu hoạt động của mạng không dây.

* 802.11 Wireless Topology Modes

- Chế độ đặc biệt: - Được sử dụng để kết nối máy khách trong mạng ngang hàng cách thức không có AP
- Chế độ cơ sở hạ tầng: - Được sử dụng để kết nối máy khách với mạng sử dụng AP.
- Tethering: Điện thoại hoặc máy tính bảng có quyền truy cập dữ liệu mạng di động được bật để tạo
điểm truy cập cá nhân.

*BSS và ESS

- Bộ dịch vụ cơ bản (BSS)
+ Sử dụng một AP duy nhất để kết nối tất cả các máy khách không dây được liên kết.
+ Khách hàng ở các BSS khác nhau không thể giao tiếp.
- Bộ dịch vụ mở rộng (ESS)
+ Một sự kết hợp của hai hoặc nhiều BSS được kết nối với nhau bằng một bản phân phối có dây hệ thống.
+ Khách hàng trong mỗi BSS có thể giao tiếp thông qua ESS.

* 802.11 Frame Structure

- Định dạng khung 802.11 tương tự như định dạng khung Ethernet, ngoại trừ việc nó chứa nhiều trường hơn.

* CSMA/CA

- Mạng WLAN là bán song công và máy khách không thể "nghe thấy" khi nó đang gửi, do đó không thể phát hiện ra xung đột.
- Mạng WLAN sử dụng đa truy cập theo cảm giác sóng mang với tính năng tránh va chạm để xác định cách thức và thời điểm gửi dữ liệu
- Máy khách không dây thực hiện những việc sau: Lắng nghe kênh để xem liệu kênh có không hoạt động hay không,
- Gửi tin nhắn sẵn sàng gửi (RTS) đến AP để yêu cầu truy cập
- Nhận thông báo rõ ràng để gửi (CTS) từ AP cấp quyền truy cập để gửi
- Nếu một máy khách không dây không nhận được xác nhận, nó sẽ giả định rằng đã xảy ra xung đột và khởi động lại quá trình

* Wireless Client and AP Association

- Để các thiết bị không dây giao tiếp qua mạng, trước tiên chúng phải liên kết với AP hoặc bộ định tuyến không dây.
- Thiết bị không dây hoàn thành quy trình ba giai đoạn sau:
+ Khám phá AP không dây
+ Xác thực với AP
+ Liên kết với AP
- Để đạt được sự liên kết thành công, một máy khách không dây và một AP phải đồng ý Về các thông số cụ thể:
+ SSID
+ Mật khẩu
+ Chế độ mạng

+ Chế độ bảo mật
+ Cài đặt kênh
* Passive and Active Discover Mode
- Chế độ thụ động
+ AP công khai quảng cáo dịch vụ của mình bằng cách định kỳ gửi khung đèn hiệu phát sóng chứa SSID
+ được hỗ trợ tiêu chuẩn và cài đặt bảo mật.
- Chế độ chủ động
+ Máy khách không dây phải biết tên của SSID.
+Máy khách không dây bắt đầu xử lý bằng cách phát sóng đầu dò khung yêu cầu trên nhiều kênh.

Câu 8: Tìm hiểu các mối đe doạ và các cuộc tấn công lên mạng không dây.

* Các mối đe dọa

- Đe doạ bởi các nguy cơ sau đây:
+ Chặn bắt dữ liệu
+ Tấn công xâm nhập mạng không dây
+ Tấn công từ chối dịch vụ
+ Giả mạo AP

- DoS Attacks
+ Các cuộc tấn công DoS không dây có thể là kết quả của:
. Các thiết bị được cấu hình không đúng
. Kẻ tấn công cố tình can thiệp vào giao tiếp không dây
. Sự can thiệp tình cờ
+ Để giảm thiểu nguy cơ bị tấn công DoS:
. kiểm soát tất cả các thiết bị
. giữ an toàn cho mật khẩu
. tạo bản sao lưu
. đảm bảo rằng tất cả các thay đổi cấu hình đều được thực hiện trong khung giờ hợp lý.

- Rogue Access Points:
+ Giả mạo AP là một AP hoặc bộ định tuyến không giây được được kết nối với mạng công ty mà không có sự cho phép rõ ràng và vi phạm chính sách của công ty
+ kẻ tấn công có thể sử dụng AP giả mạo để chiếm địa chỉ MAC, chặn bắt thông tin, giành quyền truy cập vào tài nguyên mạng hoặc tiến hành một cuộc tấn công trung gian
+ Để ngăn chặn:
. cấu hình WLC với các chính sách AP giả mạo
. sử dụng hệ thống giám sát an ninh mạng.

- Man-in-the-Middle Attack
+ tin tặc ở giữa 2 thực thể hợp pháp để đọc hoặc sửa đổi dữ liệu trao đổi giữa 2 bên
+ Một cuộc tấn công MITM không dây phổ biến được gọi là cuộc tấn công "AP đôi xấu xa – evil twin AP", trong đó kẻ tấn công giới thiệu một AP giả mạo và cấu hình nó với cùng SSID như một AP hợp pháp.
+ Để chống lại:
. xác định các thiết bị hợp pháp trong mạng WLAN
. Người dùng phải được xác thực
. mạng có thể được giám sát để tìm các thiết bị hoặc lưu lượng truy cập bất thường

*** Các kiểu tấn công trên WLAN**

- Tấn công bị động (nghe trộm – Passive attacks).
+ Passive attack không để lại một dấu vết nào chứng tỏ đã có sự hiện diện của hacker trong mạng vì hacker không thật kết nối với AP để lắng nghe các gói tin truyền trên đoạn mạng không dây
+ WLAN sniffer hay các ứng dụng miễn phí có thể được sử dụng để thu thập thông tin về mạng không dây ở khoảng cách xa bằng cách sử dụng anten định hướng
+ Phương pháp này cho phép hacker giữ khoảng cách với mạng, không để lại dấu vết trong khi vẫn lắng nghe và thu thập được những thông tin quý giá

- Tấn công chủ động (kết nối, dò và cấu hình mạng -Active attacks).
+ Hacker có thể tấn công chủ động (active) để thực hiện một số tác vụ trên mạng
+ Một cuộc tấn công chủ động có thể được sử dụng để truy cập vào server và lấy được những dữ liệu có giá trị hay sử dụng đường kết nối Internet của doanh nghiệp để thực hiện những mục đích phá hoại hay thậm chí là thay đổi cấu hình của hạ tầng mạng
+ Bằng cách kết nối với mạng không dây thông qua AP, hacker có thể xâm nhập sâu hơn vào mạng hoặc có thể thay đổi cấu hình của mạng

- Tấn công kiểu chèn ép (Jamming attacks).
+ Jamming là một kỹ thuật được sử dụng chỉ đơn giản để làm hỏng (shut down) mạng không dây
+ Tương tự như những kẻ phá hoại sử dụng tấn công DoS vào một web server làm nghẽn server đó thì mạng WLAN cũng có thể bị shut down bằng cách gây nghẽn tín hiệu RF
+ Những tín hiệu gây nghẽn này có thể là cố ý hay vô ý và có thể loại bỏ được hay không loại bỏ được
+ Để loại bỏ kiểu tấn công này:
. Xác định được nguồn tín hiệu RF.
. Dùng các ứng dụng máy phổ phân tích phần mềm kèm theo các sản phẩm WLAN cho client.

- Tấn công theo kiểu thu hút (Man–in-the-middle attacks).
+ là trường hợp trong đó hacker sử dụng một AP để đánh cắp các node di động bằng cách gởi tín hiệu RF mạnh hơn AP hợp pháp đến các node đó
+ Các node di động nhận thấy có AP phát tín hiệu RF tốt hơn nên 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
+ Để làm cho client kết nối lại đến AP giả mạo thì công suất phát của AP giả mạo phải cao hơn nhiều so với AP hợp pháp trong vùng phủ sóng của nó
+ Điểm cốt yếu trong kiểu tấn công này là người dùng không thể nhận biết được. Vì thế, số lượng thông tin mà hacker có thể thu được chỉ phụ thuộc vào thời gian mà hacker có thể duy trì trạng thái này trước khi bị phát hiện

Câu 9: 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.

So sánh 4 kĩ thuật xác thực khóa chia sẻ bao gồm WEP, WPA, WPA2, WPA3

	WEP	WPA	WPA2	WPA3
Năm phát hành	1999	2003	2004	2018
Phương pháp mã hóa	Rivest Cipher 4 (RC4)	Giao thức toàn vẹn khóa tạm thời (TKIP) với RC4	CCMP và Tiêu chuẩn mã hóa nâng cao (AES)	Tiêu chuẩn mã hóa nâng cao (AES)
Kích thước khóa phiên	40 bit	128	128	128-bit (WPA3-Personal) 192-bit (WPA-Enterprise)
Loại mật mã	Mã dòng	Mã dòng	Khối	Khối
Quản lý khóa	Không cung cấp	Cơ chế bắt tay 4 bước	Cơ chế bắt tay 4 bước	ECDH&ECDSA
Toàn vẹn dữ liệu	CRC-32	Mã toàn vẹn tin nhắn	CBC-MAC	Thuật toán băm an toàn
Xác thực	WPE- Open WPE- Shared	Khóa chia sẻ trước (PSK) & 802.1x với biến thể EAP	Khóa chia sẻ trước (PSK) & 802.1x với biến thể EAP	Xác thực đồng thời các bằng (SAE) & 802.1x với biến thể EAP

Câu 10: Trình bày các thách thức bảo mật của Apple.

- Các vấn đề chính mà Apple gặp phải với iPhone không phải là phần cứng hay thậm chí là phần mềm, mà là các quy trình nội bộ của họ và những khó khăn trong việc duy trì bảo mật trên nhiều nền tảng (di động hoặc nền tảng khác) với một cơ sở mã chung.
- Thứ nhất, trước đây Apple đã chậm cung cấp các bản vá cho các lỗ hổng đã biết được khắc phục trong các thành phần nguồn mở được sử dụng trong OS X
- Thứ hai, Apple cũng vá các lỗi phần mềm của riêng họ theo các lịch trình khác nhau cho các nền tảng khác nhau, có khả năng khiến người dùng gặp nhiều rủi ro hơn. Các sự cố liên quan đến quy trình này có thể là rủi ro bảo mật kết hợp lớn nhất đối với các thiết bị iOS. Mỗi khi một lỗ hổng nào đó được vá trên một nền tảng khác, dù là một thành phần nguồn mở hay một phần mềm độc quyền của Apple, nó có thể cung cấp cho những kẻ tấn công một cách khác để khai thác các thiết bị iOS.
- Apple phải đối mặt với một số thách thức bảo mật bổ sung: Đáng chú ý nhất là bất cứ khi nào một bản bẻ khóa mới được phát hành, nó có thể cung cấp cho kẻ tấn công một cách khác để tấn công các thiết bị iOS
- Việc khai thác pdf (để bẻ khóa và) để chạy các gợi ý mã tùy ý dẫn đến bảo mật iOS không tốt lắm.
- Thêm mã hóa đầu cuối vào các bản sao lưu iCloud, bản sao lưu này sẽ được xóa nếu bạn lâu không hoạt động quá lâu
- Khóa bảo mật vật lý cho tài khoản Apple của người dùng

Câu 11: Trình bày các giải pháp bảo mật đối với Apple iOS.

- 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 12: Trình bày các thách thức bảo mật của Android.

- Sự phân mảnh: Là một hệ điều hành nguồn mở, Android có nhiều phiên bản sửa đổi được triển khai trên một số lượng lớn thiết bị. Tình trạng này có thể tạo ra cơn ác mộng cho nhân viên hỗ trợ và an ninh
- Mã độc: +Ước tính trung bình có khoảng 11,7 nghìn mẫu mã 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 sử dụng: +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: Mặc dù những ứng dụng mới luôn cung cấp các tính năng tuyệt vời và chức năng được cải thiện nhưng chúng cũng gây ra rò rỉ dữ liệu. Trong hầu hết các trường hợp, rò rỉ dữ liệu phát sinh khi người dùng di động không biết về ý nghĩa của việc bảo mật thông tin cá nhân, cung cấp cho ứng dụng quyền lấy dữ liệu.
- Kết nối Wi-Fi không an toàn: Người dùng điện thoại Android thường chỉ chú ý đến việc bảo mật các kết nối Wi-Fi cá nhân của họ khi ở nhà, nhưng họ lại không nghĩ đến việc kết nối với Wi-Fi ở những địa điểm công cộng.
- Mạng truy cập giả mạo: Một chiến thuật phổ biến mà tin tặc thường sử dụng để thu hút người dùng điện thoại được gọi là Fake Access Networks. Họ thiết lập các điểm truy cập giả trong Wi-Fi công cộng có lưu lượng truy cập cao. Vì người dùng có thể không biết sự khác biệt giữa điểm truy cập giả và điểm truy cập thực, nên họ sẽ thường chuyển đến điểm truy cập giả mạo nếu không có ID người dùng hoặc mật khẩu cần thiết để có quyền truy cập
- Lừa đảo: Phishing thường xảy ra thông qua email hoặc dịch vụ sms. Người dùng trả lời email giả và cung cấp thông tin cho tin tặc. Sau đó, tin tặc có thể sử dụng thông tin để truy cập tài khoản trên điện thoại của người dùng.
- Phần mềm gián điệp: Phần mềm gián điệp có thể theo dõi hoạt động của người dùng, lưu trữ lại các bản ghi và thậm chí giải mã tên người dùng và mật khẩu
- Mật mã bị hỏng: Có thể xảy ra khi nhà phát triển ứng dụng sử dụng thuật toán mã hóa yếu hoặc sử dụng mã hóa mạnh mà không tích hợp chính xác vào thiết bị

Câu 13: Trình bày giải pháp đảm bảo an toàn của 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 14: Trình bày về BYOD.

* Định nghĩa: BYOD (Bring your own device) – "mang theo thiết bị của riêng mình", Các công ty cho phép nhân viên sử dụng thiết bị của riêng họ ở nhà, tại văn phòng hoặc bất kỳ vị trí nào khác để công việc trở nên dễ dàng hơn

* Lợi ích của BYOD:

- Tiết kiệm chi phí
- Không cần đến training
- Chủ động cập nhật công nghệ liên tục
- Tăng hiệu quả, hiệu suất
- Sự hài lòng của nhân viên

* Thách thức, rủi ro của BYOD:

- Dễ mất tập trung
- Thiếu nhất quán
- Bảo mật lỏng lẻo
- Lây nhiễm mã độc
- Thiết bị bị mất hoặc đánh cắp
- Việc truy cập mạng không an toàn

*Chính sách bảo mật

- Bảo mật BYOD cần quan tâm đến hai điều:

+ Bảo vệ tài nguyên của công ty (mạng, dữ liệu công ty, ứng dụng, v.v.) khỏi bất kỳ rủi ro an ninh mạng nào

+ Ngăn chặn việc lây nhiễm phần mềm độc hại, chiến dịch lừa đảo và các mối đe dọa bảo mật khác có thể làm tổn hại đến dữ liệu nhạy cảm

- Các yếu tố cần được xem xét trong chính sách bảo mật của BYOD:

+ Các thiết bị và hệ điều hành (OS) cụ thể, bao gồm cả các phiên bản OS

+ Các ứng dụng và trang web chính có trong danh sách chặn và danh sách cho phép của công ty.

+ Quyền sở hữu và quản lý dữ liệu thiết bị

+ Yêu cầu về độ mạnh của mật khẩu

+ Bất kỳ biện pháp bảo mật nào khác như triển khai xác thực đa yếu tố (MFA) và đăng nhập một lần (SSO) người dùng BYOD sẽ phải tuân theo.

+ Cách thức và thời điểm các cấp độ truy cập sẽ thay đổi để đáp ứng với các trạng thái bảo mật của thiết bị