**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**🙠🕮🙢**

**CÁC GIẢI PHÁP BẢO MẬT   
CHO THIẾT BỊ DI ĐỘNG**

GVHD: PGS. TS. Đặng Trần Khánh

Nhóm thực hiện:

Ngành Khoa Học Máy Tính - Cao học khóa 23

1. Đỗ Đặng Minh - 1311015
2. Huỳnh Công Toàn - 1311026
3. Dương Xuân Long - 1311048

*Tp. Hồ Chí Minh, tháng 10 năm 2014*

# Thông tin nhóm

|  |  |  |  |
| --- | --- | --- | --- |
| **MSHV** | **Họ tên** | **Email** | **Điện thoại** |
| 1311015 | Đỗ Đặng Minh | [masterminh219@gmail.com](mailto:masterminh219@gmail.com) | 0168-993-5242 |
| 1311026 | Huỳnh Công Toàn | [alex7huynh@gmail.com](mailto:alex7huynh@gmail.com) | 0121-516-1090 |
| 1311048 | Dương Xuân Long | [xuanlong.8888@gmail.com](mailto:xuanlong.8888@gmail.com) | 097-357-0042 |

# Danh mục các kí hiệu, chữ viết tắt và ý nghĩa

|  |  |  |
| --- | --- | --- |
| **Từ viết tắt** | **Nghĩa tiếng Anh** | **Nghĩa tiếng Việt** |
| CRL | Certificate Revocation List | Danh sách chứng nhận hủy bỏ |
| DoS | Denial-of-Service | Từ chối dịch vụ |
| FINEID | Finnish Electronic Identity | Định danh điện tử Phần Lan |
| GPRS | General Packet Radio Service | Dịch vụ gói radio tổng quát |
| GSM | Global System for Mobile communications | Hệ thống liên lạc di động toàn cầu |
| LAN | Local Area Network | Mạng cục bộ |
| MMS | Multimedia Messaging Service | Dịch vụ tin nhắn đa phương tiện |
| OCSP | Online Certificate Status Protocol | Giao thức trạng thái chứng nhận online |
| PAN | Personal Area Network | Mạng cá nhân |
| PDA | Personal Digital Assistant | Máy trợ giúp cá nhân kỹ thuật số |
| PIM | Personal Information Management | Quản lý thông tin cá nhân |
| PIN | Personal Identification Number | Số định danh cá nhân |
| PKI | Public Key Infrastructure | Hạ tầng khóa công khai |
| POC | Proof of concept | Bằng chứng khái niệm |
| POS | Point-of-sale | Điểm bán hàng |
| RSA | Rivest Shamir Adleman | Rivest Shamir Adleman |
| SMS | Short Message Services | Dịch vụ tin nhắn ngắn |
| WLAN | Wireless Local Area Network | Mạng cục bộ không dây |

# Danh mục các hình

[**Hình 1:** thị phần hệ điều hành di động từ quý 2 2011 đến quý 2 2014 5](#_Toc398099480)

[**Hình 2:** số malware trên di động theo F-Secure Corporation từ năm 2004-2008. 9](#_Toc398099481)

[**Hình 3:** tập tin chính sách mẫu cho PocketPC. 13](#_Toc398099482)

[**Hình 4:** tập tin chính sách mẫu cho Familiar Linux. 14](#_Toc398099483)

[**Hình 5:** mô hình thanh toán POS ảo 15](#_Toc398099484)

[**Hình 6:** tổng quan về giao thức thanh toán thực 17](#_Toc398099485)

Mục lục

[Thông tin nhóm 1](#_Toc398394843)

[Danh mục các kí hiệu, chữ viết tắt và ý nghĩa 1](#_Toc398394844)

[Danh mục các hình 1](#_Toc398394845)

[I. Giới thiệu 3](#_Toc398394846)

[II. Thiết bị di động 3](#_Toc398394847)

[1) Tổng quan 3](#_Toc398394848)

[2) Công nghệ không dây 4](#_Toc398394849)

[3) Mạng cá nhân và mạng cục bộ không dây 5](#_Toc398394850)

[4) Hệ điều hành di động 5](#_Toc398394851)

[5) Phần mềm thiết bị di động 6](#_Toc398394852)

[III. Mô hình nguy cơ 6](#_Toc398394853)

[1) Mất thiết bị 7](#_Toc398394854)

[2) Tấn công từ chối dịch vụ 8](#_Toc398394855)

[3) Tấn công không dây 8](#_Toc398394856)

[4) Tấn công xâm nhập 9](#_Toc398394857)

[5) Phần mềm độc hại 9](#_Toc398394858)

[6) Tấn công dựa trên hạ tầng 10](#_Toc398394859)

[7) Tấn công tính thêm phí 10](#_Toc398394860)

[IV. Tấn công cross-service 10](#_Toc398394861)

[1) Giới thiệu 10](#_Toc398394862)

[2) Tấn công cross-service 11](#_Toc398394863)

[3) Ngăn ngừa tấn công cross-service bằng gán nhãn 12](#_Toc398394864)

[V. Giao thức và chi trả di động 14](#_Toc398394865)

[1) Giao thức thanh toán 14](#_Toc398394866)

[2) Thanh toán POS ảo 15](#_Toc398394867)

[3) Thanh toán POS thực (máy bán hàng tự động) 17](#_Toc398394868)

[VI. Chương trình ứng dụng 20](#_Toc398394869)

[1) Giới thiệu 20](#_Toc398394870)

[2) Mô tả chức năng ứng dụng 20](#_Toc398394871)

[VII. Tài liệu tham khảo 20](#_Toc398394872)

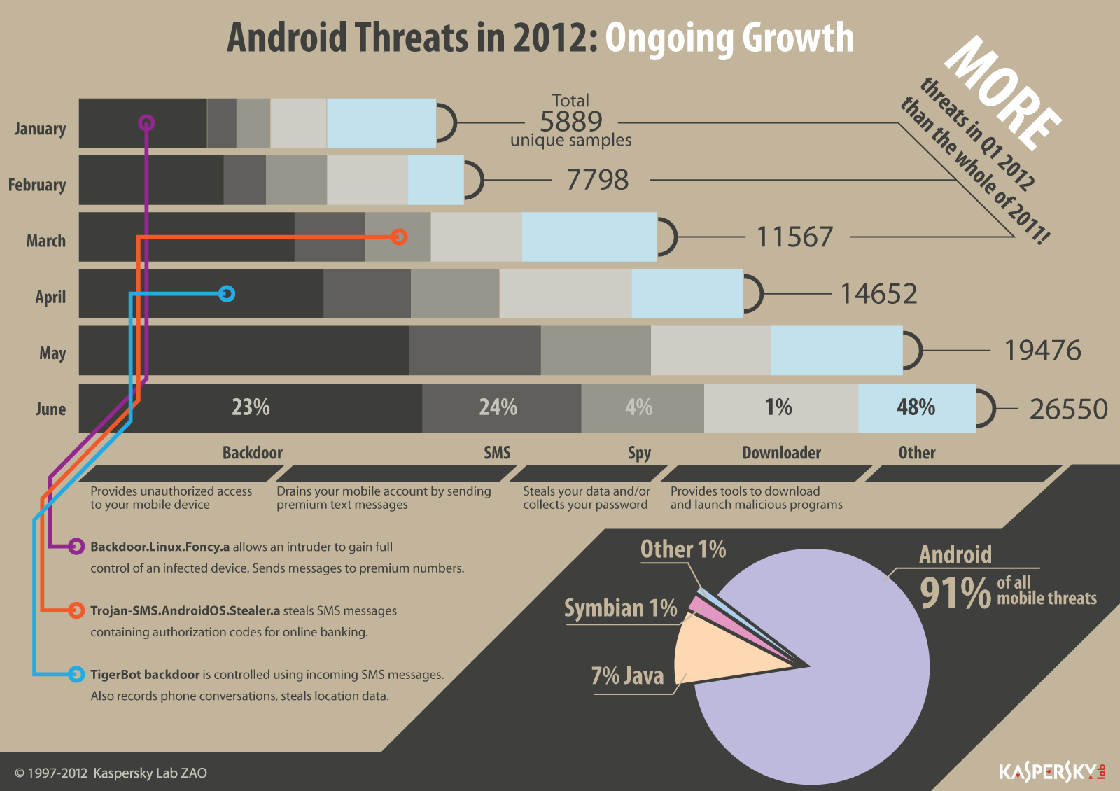
# Giới thiệu

Điện thoại thông minh kết hợp tính năng của điện thoại di động và máy PDA. Những thiết bị này đã trở nên rất phổ biến trong những năm gần đây, dần dần được tích hợp những công nghệ như IEEE 802.11, Bluetooth và GSM. Những thiết bị mới hỗ trợ thêm nhiều tính năng và dịch vụ. Các nhà cung cấp dịch vụ cũng thu được rất nhiều từ các dịch vụ đó.

Tuy nhiên, không may là sự phát triển của thiết bị và dịch vụ chỉ chạy theo nhu cầu thị trường, tập trung vào khía cạnh tính năng mới mà bỏ qua yêu cầu bảo mật. Kết quả là, điện thoại thông minh hiện nay phải đối mặt với rất nhiều vấn đề về bảo mật. Những vấn đề này phát sinh trực tiếp từ việc tích hợp và thường liên quan đến việc gộp nhiều công nghệ không dây vào trong một thiết bị. Một số vấn đề khác do các dịch vụ dành riêng cho điện thoại thông minh gây ra.

Vấn đề đầu tiên liên quan đến điện thoại thông minh là việc truy cập mạng thông qua mạng cục bộ không dây (WLAN). Thường thì việc truy cập mạng phải trả phí, còn mạng cục bộ không dây thì thường miễn phí. Chính vì vậy mà kẻ tấn công có thể tận dụng điểm yếu trong interface mạng miễn phí để truy cập vào mạng trả phí, như mạng điện thoại di động.

Vấn đề thứ hai liên quan đến các ứng dụng chạy trên thiết bị di động. Phân tích tính bảo mật của các ứng dụng này rất khó vì chúng không độc lập hoàn toàn mà còn phụ thuộc và các hệ thống và dịch vụ khác. Chính vì vậy mà các hệ thống phụ này cần phải được xem xét nếu muốn đánh giá tính bảo mật của các ứng dụng này.



**Hình 1:** thống kê các mối nguy hại trên Android (2012) của Kaspersky Lab

Theo báo cáo của Kaspersky Lab vào năm nửa đầu 2012 thì 91% các nguy cơ tấn công vào di động nhắm đến hệ điều hành Android. Các ứng dụng Backdoor chiếm đa số, được dùng để truy cập trái phép vào thiết bị di động. Sau đó là các chương trình tấn công SMS, gửi tin tính phí rất cao để đánh cắp số tiền trong tài khoản của chủ nhân thiết bị. Còn theo báo cáo của Consumer Reports (2014) thì 36% người dùng chỉ dùng mã PIN 4 số để bảo vệ thiết bị và chỉ có 14% người dùng cài chương trình diệt virút.

Mục đích của báo cáo này là tìm hiểu các cách tấn công phổ biến vào điện thoại thông minh, các giải pháp để khắc phục hoặc hạn chế chúng. Chương trình ứng dụng là một chương trình được viết trên Android để bảo vệ điện thoại thông minh khỏi một số cách tấn công phổ biến.

# Thiết bị di động

1. Tổng quan

Thiết bị di động có thể được phân thành tám lớp: Notebook, Máy tính bảng, Máy nghe nhạc di động, Thiết bị di động chơi điện tử, Điện thoại di động, Điện thoại thông minh, PDA và thiết bị di động công nghiệp.

Notebook là những chiếc máy tính nhỏ, dễ đem theo, thường không có bàn phím đầy đủ, nhưng có thể có thêm các tính năng như màn hình cảm ứng. Nhiều notebook chạy các hệ điều hành dành cho máy tính cá nhân, cũng có một số chạy hệ điều hành riêng.

Máy tính bảng hầu hết là những màn hình cảm ứng không bàn phím với kết nối không dây để xem các nội dung online.

Máy nghe nhạc di động thường dùng để truy cập nội dung đa phương tiện. Hầu hết được gọi là máy nghe nhạc và chúng không thể cài đặt phần mềm thêm vào. Đa số đều cài một hệ điều hành đã được tùy chỉnh.

Thiết bị di động chơi điện tử thường dùng để chơi các trò chơi máy tính và cũng có thể chơi các ứng dụng đa phương tiện. Đa số đều cài một hệ điều hành đã được tùy chỉnh.

Điện thoại di động có nhiều loại và hình dáng. Chúng cung cấp rất nhiều tính năng. Đơn giản nhất là tính năng gọi điện và gửi tin nhắn. Tuy nhiên ngày nay những chiếc điện thoại đơn giản nhất đều có thêm tính năng báo thức và xem lịch. Hầu hết điện thoại di động đều chạy hệ điều hành chuyên dụng.

PDA thường có kích thước như điện thoại di động nhưng có màn hình cảm ứng. Cốt lõi của PDA là gói phần mềm để quản lý thông tin cá nhân (PIM). Hầu hết PDA đều cho phép cài thêm phần mềm.

Điện thoại thông minh là sự kết hợp tính năng màn hình cảm ứng của PDA và chức năng của điện thoại di động. Các điện thoại thông minh hiện nay đều cho phép cài thêm rất nhiều ứng dụng cũng như có khả năng truy cập mạng cục bộ cá nhân hay không dây. Đây cũng là thiết bị phổ biến nhất và hiện đại nhất trong các loại thiết bị di động.

Thiết bị di động công nghiệp là thiết bị dành riêng cho thương mại, y tế hay quân đội. Những thiết bị này thường có ít người dùng và tính năng đơn giản.

1. Công nghệ không dây

Công nghệ không dây đóng một vai trò rất lớn trong lĩnh vực di động. Điện thoại di động đã không thể tồn tại nếu không có công nghệ này. Công nghệ truyền thông GPRS đóng vai trò rất quan trọng ảnh hưởng đến thiết bị di động vì chúng là dịch vụ cơ bản cho MMS và kết nối internet.

Công nghệ truyền thông không dây thường được chia thành hai loại: công nghệ phổ biến dành cho điện thoại di động như GSM hay CDMA và công nghệ truyền dữ liệu như GPRS hay EVDO.

Hệ thống liên lạc di động toàn cầu (GSM) là tiêu chuẩn được công nhận cho việc truyền thông di động ở châu Âu, một phần ở Mỹ và châu Á. Ngoài việc truyền dữ liệu và tiếng nói cơ bản, GSM còn cung cấp dịch vụ tin nhắn ngắn (SMS) để gửi tin nhắn và thông điệp điều khiển cho thiết bị di động.

Dịch vụ gói tin radio phổ biến (GPRS) là một công nghệ truyền dữ liệu tiên tiến cho GSM. Người ta nói rằng nó là công nghệ “luôn được bật” vì phí GPRS tính theo lưu lượng (kilobyte) chứ không phải thời gian kết nối. GPRS cũng cung cấp nhiều băng thông hơn so với GSM.

Enhanced Data rates for GSM Evolution (EDGE) là một công nghệ bao quát cả GPRS vì vậy mà tích hợp ngược vào nó. EDGE theo lý thuyết hỗ trợ truyền dữ liệu đến 473.6 kbit/s. EDGE có thể được phân vào nhóm 2.5G hay 3G tùy vào tỷ lệ dữ liệu cài đặt.

Hệ thống Code Division Multiple Access (CDMA) là một công nghệ truyền thông di động khác và được sử dụng rộng rãi trên thế giới ngoài châu Âu. CDMA thực chất là công nghệ cạnh tranh với GSM. Tốc độ truyền dữ liệu tối đa của CDMA là 9.6 kbit/s.

Công nghệ Evolution-Data Optimized (EVDO) là công nghệ truyền thông tiên tiến dành cho mạng CDMA. Giống như GPRS, nó cũng là công nghệ “luôn bật” và tính phí theo lưu lượng. EVDO là công nghệ 3G và truyền dữ liệu được tối đa là 3.1 Mbit/s.

1. Mạng cá nhân và mạng cục bộ không dây

Trong những năm gần đây, mạng cục bộ không dây (WLAN) và mạng cá nhân (PAN) đã trở nên rất phổ biến. Trong đó phổ biến nhất là các công nghệ: LAN không dây (IEEE 802.11), Bluetooth và Hồng ngoại.

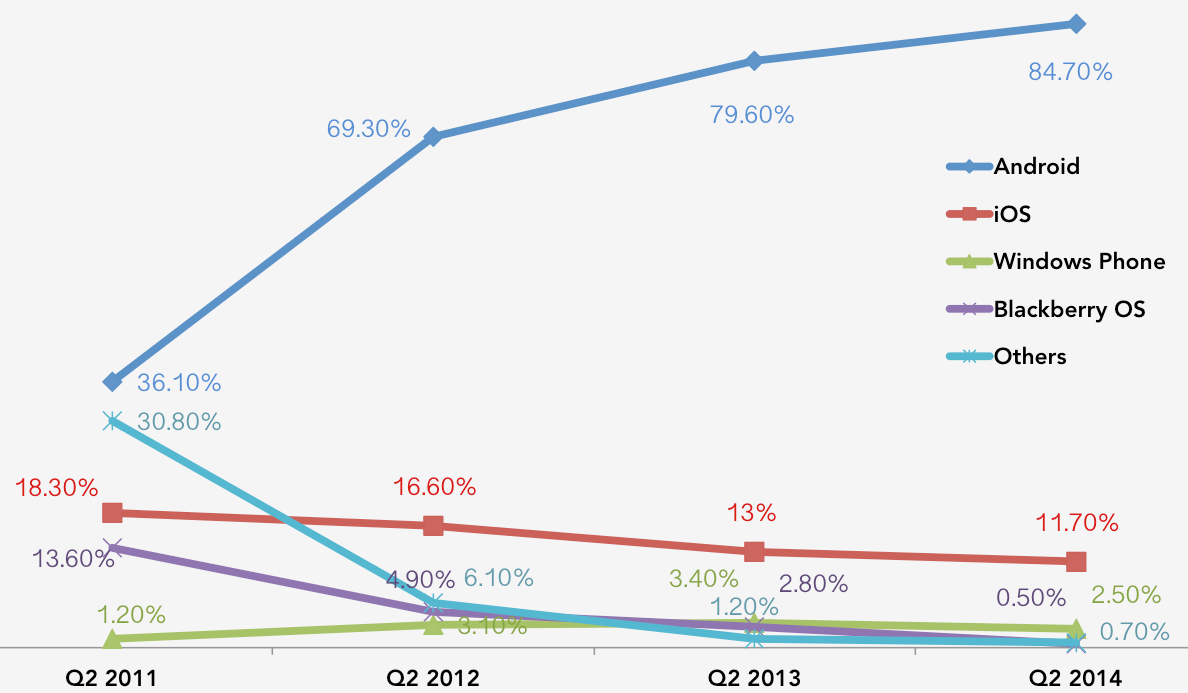
IEEE 802.11 là tiêu chuẩn cho mạng không dây, thường được gọi là Wi-Fi hay WLAN. Phiên bản đầu tiên của tiêu chuẩn 802.11 chỉ có thể truyền 2 Mbit/s, cho tới phiên bản 802.11g đã có thể truyền được 54 Mbit/s. Phổ không dây là một môi trường chia sẻ - mỗi nút gần người gửi đều có thể lắng nghe tín hiệu. Cơ chế bảo mật cơ bản có hai tính năng: hạn chế đường mạng của thiết bị được cấp phép và bảo vệ tính riêng tư của dữ liệu. Công nghệ bảo mật Wired Equivalent Privacy (WEP) được giới thiệu ban đầu dần được thay thế bằng Wi-Fi Protected Access (WPA) và WPA2.

Bluetooth là công nghệ mạng cá nhân. Điểm mạnh của nó là có thể hoạt động trên các thiết bị của các nhà sản xuất khác nhau. Bản chất của Bluetooth không phải là công nghệ mạng mà chỉ là để kết nối giữa các thiết bị.

Hồng ngoại hay IrDA là công nghệ thay thế đường cáp. Nó hỗ trợ việc liên lạc tốc độ chậm, từ điểm tới điểm trong bán kính giới hạn. IrDA đã tạo ra nhiều định dạng truyền dữ liệu mà Bluetooth đã áp dụng sau này. Nói chung, IrDA là công nghệ khá bảo mật vì việc liên lạc cần một đường truyền ngắn giữa hai thiết bị, dù không có cơ chế bảo mật nào cài đặt trên nó.

1. Hệ điều hành di động

Hệ điều hành di động có rất nhiều nhưng phổ biến nhất hiện lại là Android, iOS, Windows Phone và Blackberry. Hình 1 thống kê thị phần các hệ điều hành trên toàn cầu theo IDC.



**Hình 2:** thị phần hệ điều hành di động từ quý 2 2011 đến quý 2 2014

Android thuộc về tập đoàn Google. Nó chiếm thị phần lớn ở mảng điện thoại thông minh. Hầu hết Android miễn phí và mã nguồn mở, nhưng một lượng lớn phần mềm trên thiết bị Android (như Play Store, Google Search, Google Play Services, Google Music,…) đều được cấp quyền và có bản quyền. Các phiên bản trước 2.0 dành riêng cho điện thoại di động. Các phiên bản sau này được phát triển do cả máy tính bảng. Phiên bản hiện tại là 4.4. Hầu hết các nhà cung cấp dịch vụ di động đều có một chiếc Android. Từ quý 2 năm 2009 đến quý 2 năm 2010, thị trường toàn cầu của Android đã tăng trưởng 850% từ 1.8% lên 17.2%. Cho đến tháng 9/2014, thị phần của Android đã lên tới 85%.

iOS thuộc về tập đoàn Apple. Nó chiếm thị phần lớn thứ hai toàn cầu chỉ sau Android. Nó là mã nguồn đóng được cấp bản quyền được xây dựng từ hệ điều hành mã nguồn mở Darwin. Các thiết bị iPhone, iPod Touch, iPad và Apple TV đều dùng iOS. Các ứng dụng của bên thứ ba chỉ được hỗ trợ từ tháng 7/2008. Cho đến tháng 9/2014, thị phần của iOS là 11%.

Windows Phone thuộc về Microsoft. Nó là mã nguồn đóng được cấp bản quyền. Nó chiếm thị phần lớn thứ ba toàn cầu sau Android và iOS. Hệ điều hành này được Microsoft giới thiệu vào ngày 15/2/2010. Nó có khả năng tích hợp với các thiết bị của Microsoft như OneDrive, Office, Xbox Music, Xbox Video, Xbox Live và các dịch vụ khác như Facebook và tài khoản Google. Cho đến tháng 9/2014, thị phần của Windows Phone là 3%.

BlackBerry thuộc về hãng BlackBerry. Người dùng phổ biến chủ yếu là nhân viên chính phủ. BlackBerry 10 là thế hệ kế tiếp dành cho điện thoại thông minh và máy tính bảng, tất cả đều do BlackBerry sản xuất. Đã từng thống trị thị trường nhưng cho đến năm 2014 thì thị phần của nó chỉ còn chưa đến 1%.

1. Phần mềm thiết bị di động

Có nhiều điểm khác biệt giữa các ứng dụng chạy trên điện thoại và các ứng dụng chạy trên máy tính. Hầu hết các khác biệt đều liên quan đến giao diện người dùng (UI).

Thiết bị di động thường có màn hình rất nhỏ, với bàn phím cũng được thu nhỏ hoặc thay thế bằng bàn phím ảo trên màn hình cảm ứng. Hầu hết các giao diện chỉ cho phép tương tác với một ứng dụng tại một thời điểm. Chính UI và việc nhập thông tin khá hạn chế đã ảnh hưởng lớn đến các ứng dụng di động, như nhiều ứng dụng thay vì cho ô nhập liệu đã thay bằng ô chọn lựa. Ngoài ra cũng còn các hạn chế khác như dung lượng lưu trữ và tốc độ CPU, phần nào ảnh hưởng đến hiệu năng và độ ổn định của ứng dụng.

# Mô hình nguy cơ

Khi muốn bảo vệ một hệ thống thì phải biết được các nguy cơ, các cách tấn công vào hệ thống. Một mô hình nguy cơ giúp xác định các nguy cơ hệ thống bị tấn công, các tài sản cần bảo vệ, các đặc điểm của kẻ tấn công và các giải pháp để ngăn ngừa và hạn chế.

Vấn đề bảo mật trên thiết bị di động cũng giải quyết ba tính chất như bảo mật nói chung:

* Tính bảo mật: sự riêng tư, quyết định ai được truy cập những gì.
* Tính toàn vẹn: xác định ai được quyền sửa hay sử dụng tài nguyên nào.
* Tính sẵn sàng: mô tả yêu cầu một người dùng hợp lệ có thể sử dụng tài nguyên nào.

Trong đó có ba mục tiêu chính cần được bảo vệ:

* Dữ liệu: thiết bị di động dùng để quản lý dữ liệu. Vì vậy nó có thể chứa nhiều thông tin nhạy cảm như lịch làm việc, số tài khoản, mật khẩu, thông tin cá nhân,…
* Định danh: thiết bị di động, đặc biệt là với kết nối không dây hoàn toàn mang tính cá nhân. Điều đó có nghĩa là một chiếc điện thoại thường gắn liền với chủ nhân của nó chứ không phải ai khác.
* Tính sẵn sàng: không hẳn là một mục tiêu vì nó không thể bị đánh cắp. Tuy nhiên nó có thể bị từ chối đối với người dùng hợp pháp.

Những kẻ tấn công phổ biến là:

* Chuyên gia: những kẻ tấn công chuyên nghiệp thường nhắm đến cả ba mục tiêu trên. Ngoài việc đánh cắp thông tin, chúng còn sử dụng định danh của điện thoại để chuẩn bị cho các đợt tấn công sau này. Ngoài ra, việc làm cho người dùng hợp pháp không sử dụng được điện thoại cũng là một cách tấn công.
* Lừa đảo: sử dụng định danh trên điện thoại để đi lừa đảo. Những kẻ lừa đảo thường không tập trung vào một cá nhân mà thường tấn công nhiều mục tiêu cùng lúc để thu lợi bất chính.
* Tội phạm máy tính: những kẻ bẻ khóa thường gây hại đến tính sẵn sàng. Chúng thường tạo ra virút hoặc sâu để gây hại cho hệ thống. Ngoài ra chúng còn hứng thú với một số loại dữ liệu cụ thể trong các thiết bị.

1. Mất thiết bị

Theo một báo cáo gần đây, đã có hơn 3,1 triệu điện thoại thông minh đã bị đánh cắp ở nước Mỹ trong năm 2013 so với 1,6 triệu của năm 2012. Đáng báo động hơn, những thiết bị bị mất này phần lớn là thiết bị tài sản công ty, hoặc thiết bị cá nhân được sử dụng cho nhu cầu doanh nghiệp và đều chứa những thông tin nhạy cảm. Theo thống kê của ESET & Harris Interactive, 21% số điện thoại bị đánh cắp thường để trong xe. Còn theo Statista, người sử dụng bị mất điện thoại chủ yếu nằm trong lứa tuổi 18-24, chiếm đến 45% trong thống kê vào năm 2012. Nếu không có những giải pháp bảo mật cơ bản, các kẻ trộm hoặc hacker chuyên nghiệp có thể truy cập vào các thông tin cá nhân hay những thông tin bảo mật của công ty như dữ liệu khách hàng, các báo cáo tài chính… Chính khả năng một thiết bị di động bị mất hay đánh cắp đã làm cho các nhà quản lý hoặc nhà kỹ thuật cần phải lưu tâm tới việc bảo vệ các thiết bị di động.

Nguyên nhân gây ra việc đánh cắp thiết bị di động là sự tăng trưởng không ngừng các thiết bị di động, kết hợp với sự phát triển mạnh mẽ của các dịch vụ đám mây, đã làm cho các các nhân viên sử dụng thiết bị di động cho công việc hằng ngày. Bất chấp những kỹ thuật đã được đưa ra như ẩn giấu thông tin vị trí người dùng, thì những vấn đề về bảo mật thiết bị di động tránh bị đánh cắp vẫn đang gia tăng.

Bên cạnh đó, những dịch vụ đám mây đã phát triển mạnh mẽ đến mức thay đổi cách tương tác giữa các doanh nghiệp và nhân viên với các nhân viên khác và khách hàng. Khả năng truy cập thông tin, chia sẻ tập tin, kiểm tra thư điện tử và hàng loạt các tác vụ doanh nghiệp hằng ngày đều có thể thực hiện thông qua những dịch vụ đám mây với các chức năng mạnh mẽ linh hoạt. Các dịch vụ đám mây, về mặt cơ bản, đã xóa đi việc đánh nhãn ai là người truy cập vào các dịch vụ của doanh ngiệp, từ trợ lý đến giám đốc…

Như vậy, các giải pháp cho vấn đề này cần đưa ra, bao gồm kịch bản giải quyết và các giải pháp đối phó với tình huống. Một vài tình huống cần có thể xem xét tới như: sự mất mát thiết bị của các nhân viên đã nghỉ việc, việc truy cập vào các dịch vụ công cộng (mạng xã hội, blog) của các nhân viên tại công sở, các dịch vụ chính sách cho các thiết bị đánh mất, đánh giá rủi ro, hao tổn về tài chính khi đánh mất thiết bị (cả về giá trị thiết bị và giá trị của dữ liệu mà thiết bị chứa)…

Nhìn chung, các giải pháp cho vấn đề bao gồm:

* Nêu rõ nhận thức với các nhân viên và những người liên quan về tầm quan trọng của thiết bị di động với các dữ liệu doanh nghiệp.
* Xây dựng các chính sách để ngăn ngừa việc thất thoát dữ liệu.
* Xây dựng các ước lượng về đánh mất dữ liệu khi thiết bị di động bị đánh mất.
* Xây dựng các hệ thống kỹ thuật, chống mất cắp thiết bị hoặc đảm bảo tính an toàn của dữ liệu khi thiết bị bị đánh mất.

1. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (DoS) đã tồn tại từ rất lâu, không mới và cũng không riêng cho thiết bị di động. Kẻ tấn công DoS làm cho người dùng hợp pháp không dùng được hệ thống, gây hại đến tính sẵn sàng.

Vấn đề của tấn công DoS thường liên quan đến kết nối và giảm hiệu năng. Ví dụ như cách tấn công phổ biến là gửi một lượng lớn dữ liệu rác đến một mục tiêu thông qua đường mạng. Trong khi kẻ tấn công cần nhiều tài nguyên để tấn công vào máy tính hay máy chủ, một thiết bị di động do có phần cứng hạn chế hơn, rất dễ trở thành mục tiêu của cách tấn công này.

Một cách cụ thể hơn là nhắm đền nguồn pin của thiết bị di động. Trong trường hợp này, mục tiêu của kẻ tấn công là làm cạn kiệt nguồn pin của thiết bị nhắm đến. Đợt tấn công thành công sẽ làm tắt hệ thống hoặc hạn chế đáng kể thời gian hoạt động của mục tiêu. Cách tấn công này có thể khai thác các tính năng khác nhau, như các tiến trình của CPU tốn nhiều năng lượng (quy trình mã hóa phức tạp như bắt tay SSL) hay bắt hệ thống gia tăng sức mạnh cho phần cứng (như màn hình để hiển thị thông tin về một tập tin đang truyền đến).

Các cách tấn công khác như làm nhiễu toàn bộ băng tần (như băng 2.4 GHz mà LAN 802.11 không dây và Bluetooth sử dụng) cũng rất hiệu quả.

1. Tấn công không dây

Có nhiều cách tấn công khác nhau ảnh hưởng đến khả năng kết nối không dây của mục tiêu. Cách phổ biến nhất là nghe lén đường truyền không dây để bắt lấy các thông tin mật như tên tài khoản và mật khẩu. Kiểu tấn công này không dành riêng cho thiết bị di động, nhưng thiết bị di động rất yếu ở điểm này do chúng thường hỗ trợ việc liên lạc qua *kết nối không dây*.

Một kiểu tấn công không dây khác là tận dụng định danh phần cứng duy nhất (như địa chỉ MAC của LAN không dây) tồn tại ở tất cả các đường truyền không dây để theo dõi hay xác định chủ nhân của thiết bị. Loại tấn công này tập trung vào tính cá nhân hóa của thiết bị và nhắm chủ yếu vào thiết bị di động.

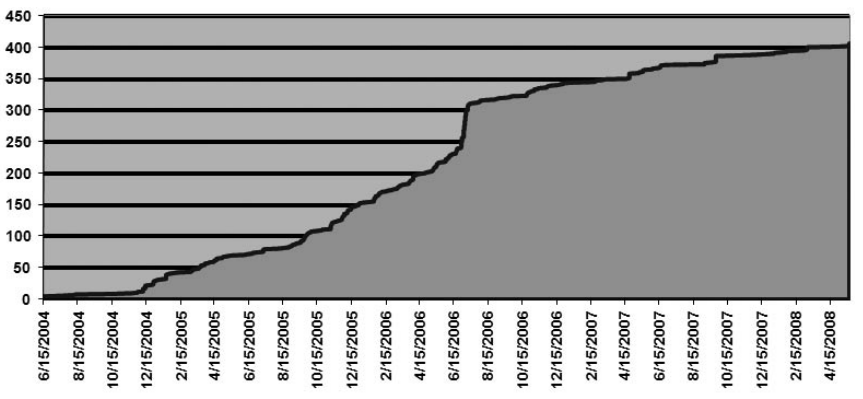
1. Tấn công xâm nhập

Xâm nhập là cách tấn công để chiếm lấy một phần hay toàn quyền điều khiển mục tiêu. Tấn công xâm nhập thường xảy ra theo hai hướng là nhúng mã và tận dụng lỗi logic. Nhúng mã được sử dụng bằng cách khai thác các lỗi lập trình như tràn bộ đệm hay điểm yếu của chuỗi định dạng. Tận dụng lỗi logic thì tinh vi hơn, vì lỗi logic chỉ xuất hiện với một ứng dụng hay thiết bị cụ thể bị tấn công.

Tấn công xâm nhập ảnh hưởng đến tính bảo mật, toàn vẹn và tính sẵn sàng của thiết bị. Mối nguy hiểm thật sự còn tùy thuộc vào mục tiêu của kẻ tấn công. Nói tổng quát hơn, tấn công xâm nhập được dùng để làm nền cho các cuộc tấn công khác như tấn công quá tải hay đánh cắp định danh.

1. Phần mềm độc hại

Phần mềm độc hại (malware) bao gồm virút, sâu và trojan. Chúng phát tán rất mạnh mẽ trong những năm gần đây. Số lượng phần mềm độc hại đối với một hệ điều hành thường có mối quan hệ với thị phần của hệ điều hành đó.



**Hình 3:** số malware trên di động theo F-Secure Corporation từ năm 2004-2008.

Virút và sâu cũng gây nguy hại cho thiết bị di động giống như máy tính. Chúng làm hỏng dữ liệu và làm hệ thống bị tê liệt. Khi sâu tấn công vào điện thoại sử dụng dịch vụ trả phí, nó có thể gửi đến hàng trăm điện thoại khác để gây ra thiệt hại tài chính đáng kể cho chủ của thiết bị bị nhiễm sâu.

Virút có thể tấn công cả thiết bị di động và máy tính. Ban đầu chúng sẽ tấn công vào thiết bị di động và sau đó lây nhiễm qua máy tính (khi đồng bộ hóa thiết bị). Loại virút hay sâu như thế này dễ dàng vượt qua cơ chế bảo mật chỉ bảo vệ khỏi các đợt tấn công từ bên ngoài.

Các loại phần mềm gián điệp khác có thể quan sát và ghi lại hoạt động của thiết bị bằng cách gửi đi báo cáo hàng tuần hay hàng ngày (như mỗi lần người dùng kết nối internet bằng GPRS).

1. Tấn công dựa trên hạ tầng

Hạ tầng dịch vụ, thường được xây dựng từ mạng GSM và ứng dụng máy chủ, đóng vai trò rất quan trọng trong thế giới thiết bị di động. Nó là nền tảng cho các ứng dụng chủ yếu của thiết bị di động như tính năng gọi điện và gửi thư điện tử. Khi thiết bị đã được bảo mật tương đối đầy đủ thì hạ tầng sẽ mở ra để người dùng sử dụng. Vì vậy tấn công vào hạ tầng có thể ảnh hưởng đến hàng trăm hay hàng nghìn người dùng thiết bị. Mặc dù kiểu tấn công này có thể được xếp vào các loại tấn công trên (tấn công DoS hay tấn công không dây), chúng được xét riêng vì tác động đến cơ sở hạ tầng của thiết bị di động.

1. Tấn công tính thêm phí

Tấn công tính thêm phí thường liên quan đến việc chi trả phí dịch vụ, như hợp đồng dịch vụ điện thoại di động. Mục tiêu là tính thêm phí vào tài khoản của nạn nhân, và nếu có thể thì chuyển lượng phí thêm đó cho kẻ tấn công.

Ví dụ như kẻ tấn công có thể tận dụng một sai sót trong hệ thống GPRS để tính thêm phí với những khách hàng của cùng một nhà cung cấp dịch vụ. Hắn tận dụng đặc điểm “luôn bật” của GPRS (trả phí theo lưu lượng thay vì thời gian sử dụng). Kẻ tấn công chỉ cần gửi vài gói tin ngẫu nhiên đến địa chỉ IP của nạn nhân. Nhà cung cấp sẽ không kiểm tra xem đó có phải do nạn nhân yêu cầu hay không và vẫn tính phí.

Một kiểu tấn công khác là dùng tấn công xâm nhập để gọi từ điện thoại của nạn nhân đến một số điện thoại tính phí rất đắt của kẻ tấn công. Kiểu tấn công này rất được ưa chuộng do nó đem món lợi rất lớn.

Kiểu tấn công này cũng thường nhắm đến thiết bị dùng mạng không dây vì dịch vụ không dây thường tính chi phí mỗi lần dùng.

# Tấn công cross-service

Phần này trình bày về tấn công cross-service, một kiểu tấn công mới nhắm đến điện thoại thông minh với nhiều interface không dây và một cơ chế để bảo vệ khỏi cách tấn công này.

Do nhóm không có đủ thiết bị và các điều kiện cần thiết nên nội dung của phần này trình bày lại mô tả và thực nghiệm của Collin Richard Mulliner[2].

1. Giới thiệu

Các điện thoại thông minh hiện nay thường tích hợp nhiều công nghệ không dây như IEEE 802.11, Bluetooth và GSM/GPRS. Tuy nhiên, việc tích hợp nhiều dịch vụ mạng chỉ đơn giản là tích hợp thành phần phần cứng và phần mềm vào trong một thiết bị, không xem xét các đặc điểm khác nhau của công nghệ và dịch vụ đi kèm. Kết quả là một thiết bị tích hợp đời mới dễ bị tấn công tận dụng các tương tác giữa các dịch vụ.

Một ví dụ cụ thể là tương tác giữa các dịch vụ miễn phí và các dịch vụ thuê bao. Người dùng điện thoại thường có hợp đồng với nhà cung cấp trong đó phí được tính thông qua thời gian sử dụng hoặc lượng dữ liệu truyền đi. Mặc dù các nhà cung cấp cũng cài đặt tường lửa và các dạng bảo vệ khác để bảo vệ thiết bị người dùng, tuy nhiên hệ thống ít được bảo vệ khi vào mạng LAN có dây hoặc không dây. Vì vậy một thiết bị tích hợp có thể bị khai thác kết nối mạng cục bộ. Sau đó nó có thể được tận dụng để truy cập các dịch vụ thuê bao gây thiệt hại tài chính cho người dùng.

Tình hình còn tồi tệ hơn do dung lượng và khả năng tính toán được cải tiến. Do có thừa khả năng hỗ trợ dịch vụ truy cập mạng và ứng dụng của bên thứ ba, lỗ hỏng bảo mật càng lớn hơn. Ngoài ra các ứng dụng sử dụng mạng thường được phát triển mà không xem xét vấn đề bảo mật và khả năng tương tác giữa các dịch vụ mạng.

Mặc dù tấn công tràn bộ đệm không có gì mới nhưng nhóm của Collin Richard Mulliner đã mô tả chi tiết lại tấn công cross-service tận dụng kiểu tấn công này. Cơ chế bảo mật triển khai trong thiết bị di động tích hợp không được bảo vệ khỏi kiểu tấn công này. Để xác định các vấn đề liên quan đến thiết bị tích hợp có thể truy cập nhiều dịch vụ mạng, Collin phát triển một cơ chế chia hệ thống tài nguyên thành từng ngăn riêng biệt. Mục tiêu của cơ chế này là ngăn ngừa các tiến trình tương tác với một dịch vụ mạng cụ thể (như mạng không dây dựa trên IP), vượt qua rào cản dịch vụ và truy cập tài nguyên gắn với dịch vụ khác (như dịch vụ dựa trên GSM).

Cơ chế này của Collin theo dõi lời gọi hệ thống thực thi bởi các tiến trình và gán nhãn mã thực thi dựa trên truy cập của nó vào đường mạng (như mạng không dây, GSM, Bluetooth). Nhãn này sau đó được chuyển giữa các tiến trình và tài nguyên hệ thống như kết quả của việc truy cập hoặc thực thi. Khi có một hành động đáng ngờ xảy ra, nhãn của các tài nguyên liên quan (tiến trình hay tập tin) sẽ được so sánh với tập luật. Các luật cho phép xác định điều triển truy cập đã được tinh lọc vào dịch vụ và dữ liệu. Ví dụ như ngăn chặn truy cập của ứng dụng sổ địa chỉ vào API gọi điện, ngăn ngừa truy cập vào API không liên quan (như API socket). Việc gán nhãn và tài nguyên cũng như thực thi các luật được bộ giám sát tham chiếu cấp kernel thực hiện.

1. Tấn công cross-service

Nhóm của Collin cài đặt một kịch bản tấn công POC là tấn công tính thêm phí vào dịch vụ thuê bao của người dùng. Cách tấn công khác cũng có thể sử dụng nhưng cách này có thể đem lại món lợi lớn cho kẻ tấn công nên dễ phát tán.

Minh họa cho đợt tấn công này như sau: một người đưa thư đi vào một quán café tìm một điểm kết nối internet không dây để kiểm tra thư điện tử và lịch trình online. Người đưa thư kết nối thiết bị của mình với điểm kiết nối không dây của quán café. Kẻ tấn công quan sát mạng không dây của quán, nhìn thấy thiết bị vừa kết nối, quét thiết bị mới và phát hiện điểm yếu dịch vụ. Bằng cách khai thác danh sách thư bảo mật đã được công khai cho dịch vụ định danh, kẻ tấn công xâm nhập vào thiết bị. Hắn sử dụng một đoạn mã làm điện thoại của người đưa thư gọi đến một số tính phí của chính hắn, tiêu hết hàng trăm đôla của người đưa thư.

Nhóm của Collin sử dụng i-mate PDA2k để thực hiện kịch bản trên. Thiết bị này có bộ xử lý Intel XScale PXA263 (ARM CPU), chạy hệ điều hành Windows Mobile 2003 Second Edition và có kết nối LAN không dây, Bluetooth, GSM đa dải, dịch vụ GPRS. Collin chọn tấn công tràn bộ đệm để làm ví dụ vì đây là cách tấn công phổ biến, chọn *ftpsvr*, một server FTP mã nguồn mở làm mục tiêu.

Điểm yếu mà Collin dùng để tấn công là tấn công *strcpy* trong hàm *void Session::SendToClient(int mode, LPCSTR msg)* trong *ftpmain.cpp*. Hàm này được gọi để phản hồi lệnh dữ liệu người dùng cung cấp. Đợt tấn công sử dụng lệnh USER và trình xử lý lỗi cho các lệnh khác. Hàm *strcpy* trong *SendToClient* sẽ ghi vào một bộ đệm 256 bytes, cho phép ghi đè lên địa chỉ trả về trong khung ngăn xếp của hàm này. Collin sử dụng trình xử lý lỗi *unknown command* để tải shellcode lên nơi an toàn. Trình xử lý lưu chuỗi không trùng với bất kỳ lệnh nào trong biến toàn cục *m\_szSjis* trước khi gửi lỗi đi cho người dùng, chỉnh sửa bộ đếm của chương trình bằng lệnh *USER* và sẽ ghi đè địa chỉ trả về bằng địa chỉ của *m\_szSjis*.

Khi bắt đầu tấn công, thư viện điện thoại nạp không gian địa chỉ của ứng dụng bằng cách gọi hàm *LoadLibraryW(TEXT("cellcore"))*. Sau đó chức năng gọi điện được thực hiện bằng cách gọi hàm *tapiRequestMakeCall*, gọi đến số cho trước. Số điện thoại là chuỗi Unicode truyền như tham số vào hàm *tapiRequestMakeCall*.

Tóm lại, nhóm của Collin khai thác nền tảng WindowsCE làm tràn bộ đệm trong một ứng dụng mạng và buộc thiết bị của nạn nhân gọi điện.

1. Ngăn ngừa tấn công cross-service bằng gán nhãn

Đế đối phó với kiểu tấn công này, nhóm của Collin phát triển một cơ chế bảo mật dựa trên việc gán nhãn hệ thống và các tiến trình. Cơ chế này định ba loại đối tượng: tiến trình , tài nguyên và interface . Tiến trình và tài nguyên có một nhãn liên kết . Mỗi nhãn này cho biết tiến trình hay tài nguyên liên hệ trực tiếp hay gián tiếp đến một đường mạng cụ thể. là nhãn gán với interface *i*. và là tập nhãn gán với tiến trình *p* và tài nguyên *r*.

Truy cập interace: khi một tiến trình truy cập đến một interface, nhãn của tiến trình được kiểm tra. Tiến trình sẽ đánh dấu nhãn, , trong đó *p* là tiến trình truy cập vào interface *i*. Ví dụ như một tiến trình truy cập vào một interface LAN không dây, gọi hệ thống liên quan đến socket thì tiến trình sẽ được gán nhãn ghi rõ là interface LAN không dây.

Truy cập tài nguyên: khi một tiến trình truy cập đến một tài nguyên (như tập tin) thì nhãn của cả hai sẽ được kiểm tra để các luật cho trước. Nếu truy cập hợp lệ thì nhãn của tiến trình được cập nhật với nhãn của tài nguyên, , trong đó *p* là tiến trình và *r* là tài nguyên.

Tạo tiến trình và tài nguyên: khi một tiến trình *p* tạo một tài nguyên mới hay chỉnh sửa một tài nguyên có sẵn *r* thì tài nguyên kế thừa tập nhãn của tiến trình, . Khi tiến trình *p* tạo ra tiến trình thì cũng tương tự, .

Hành động gán nhãn mô tả như trên giúp kiểm soát được interface nào đang dùng và tiến trình và tài nguyên nào bị ảnh hưởng các hành động liên quan đến bảo mật. Ví dụ như tiến trình gắn với một interface bị nguy hại, tập tin của tiến trình này được gán nhãn liên kết với interface. Khi tiến trình này (hay tiến trình tạo bởi tiến trình này) truy cập đến các interface khác thì hệ thống sẽ xác định và chặn nguy cập vượt rào này.

Cơ chế bảo mật này dùng một tập tin chính sách để cho phép hay từ chối truy cập vào tài nguyên hay interface. Tập tin này chứa các luật. Ngôn ngữ điều khiển truy cập được định nghĩa như sau:

*policy* ⇒ *rule*∗

*rule* ⇒ **access** (*interface*|*resource*) *action label∗*

*action* ⇒ **deny**|**ask**

Hành động *deny* là từ chối truy cập, còn *ask* là đưa ra hộp thoại để người dùng quyết định. Ví dụ như *access i1 deny i2 i3* cho biết sẽ từ chối truy cập vào interface *i1* nếu tiến trình đã gán nhãn với interface *i2* và *i3*.

Ngoài ra để mở rộng thêm, ngôn ngữ này cũng cho phép các ngoại lệ. Trong đó *notlabel* cho biết tiến trình thực thi ứng dụng không cần gán nhãn khi vào interface; *notinherit* cho biết tiến trình không kế thừa nhãn nào khi truy cập đối tượng; *notpass* cho biết tiến trình không truyền nhãn cho tài nguyên hay tiến trình con. Phần mở rộng được định nghĩa như sau:

*rule* ⇒ **exception** *path except∗*

*path* ⇒ */ (dirname/) ∗ filename*

*except* ⇒ **notlabel**|**notinherit**|**notpass**

Biến path chỉ định tập tin chứa ứng dụng có hành vi đã chỉnh sửa.

Ví dụ như luật cho một trình duyệt web chỉ định tiến trình không kế thừa nhãn từ tập tin. Điều này cần thiết vì trình duyệt phải truy cập các tập tin đã tải về trước đó (như cache của trình duyệt). Chính vì vậy mà giúp trình duyệt không bị gán nhãn để tránh việc không được truy cập vào mạng.

# Internet Explorer

exception /Windows/iexplore.exe notinherit

# ActiveSync

exception /Windows/repllog.exe notlabel notinherit notpass

# FileExplorer

exception /Windows/fexplorer.exe notpass

**Hình 4:** tập tin chính sách mẫu cho PocketPC.

# Konqueror (web browser)

exception /opt/bin/konqueror notinherit

# Ipkg (package management tool)

exception /usr/bin/ipkg-cl notlabel notinherit notpass

# multi-purpose binary

exception /opt/QtPalmtop/bin/quicklauncher notpass notinherit

**Hình 5:** tập tin chính sách mẫu cho Familiar Linux.

# Giao thức và chi trả di động

Thương mại di động và thanh toán di động cần được công nhận để không bên nào phủ nhận việc đã tham gia vào một giao dịch. Việc công nhận đạt được bằng mã hóa bất đối xứng sử dụng hạ tầng khóa công khai (PKI). Giả định rằng khóa bí mật của người dùng chỉ có người dùng đó có nghĩa là không ai có thể tạo ra chữ ký số hợp lệ của người dùng đó. Marko Hassinen[7] đã sử dụng một hạ tầng khóa công khai do chính phủ quản trị để cài đặt giao thức cho thanh toán di động. Với những giao thức này, thanh toán di động có thể khả thi ở cả điểm bán hàng (POS) thực và ảo. Sử dụng PKI chính phủ, giao thức sẽ chứng thực công dân thay vì khách hàng của một doanh nghiệp nào đó. Điều này cũng có nghĩa là hệ thống mở ra cho mọi thương nhân, nhà cung cấp dịch vụ và doanh nghiệp. Phần này sẽ trình bày về giao thức này của Marko.

Bảo mật lưu trữ các thông điệp trao đổi rất quan trọng trong trường hợp thiết bị bị truy cập bởi một bên không cấp phép. Điều này có thể xảy ra khi thiết bị bị mất hay bị đánh cắp. Bảo mật trong liên lạc di động hoàn toàn có thể đạt được với công nghệ và thiết bị hiện tại. Cấp độ bảo mật có thể thiết lập đủ cao để cung cấp giao dịch tài chính an toàn sử dụng điện thoại di động.

Nhóm của Marko đã phát triển ứng dụng FINEID (Finnish Electronic Identification) để quản lý thẻ định danh điện tử và cung cấp giao diện điều khiển để thực hiện các hành động khóa bí mật như tạo chữ ký số. Xác thực người dùng bằng cách sử dụng mã PIN (Personal Identification Number).

1. Giao thức thanh toán

Kế hoạch thanh toán di động bao gồm các bên sau: khách hàng, thương nhân và ngân hàng.

*Khách hàng* là người dùng thiết bị di động. Khách hàng nhận được một thẻ SIM và ứng dụng FINEID, bao gồm chứng thực khóa công khai của người dùng và một khóa bí mật tương ứng. Định danh của người dùng là Finnish Electronic User ID (FINUID) của họ.

Một *thương gia* là một sở hữu máy điểm bán hàng (hay máy bán hàng tự động) hoặc là một nhà cung cấp dịch vụ chấp nhận thanh toán di động. Thương gia có một khóa bí mật và một chứng thực khóa công khai tương ứng trong hệ thống FINEID.

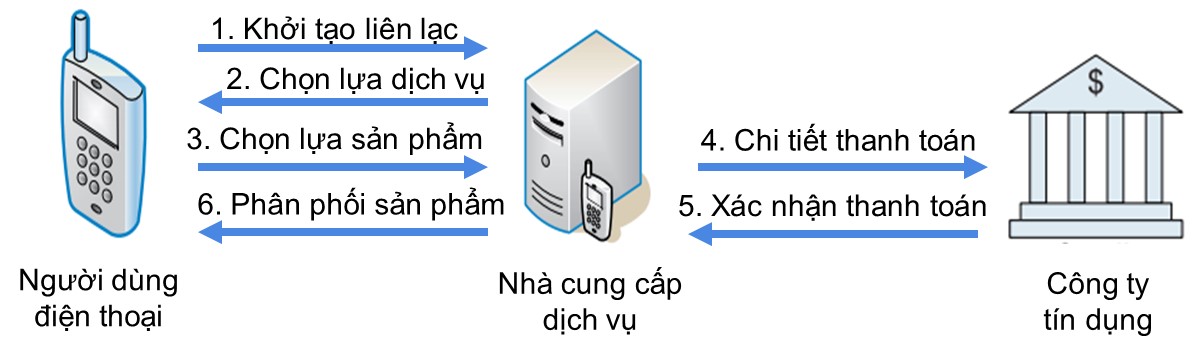
Một *ngân hàng* hay một tổ chức tín dụng như VISA hay MasterCard là một doanh nghiệp hoạt động như một bên xử lý thanh toán. Khách hàng có tài khoản trong ngân hàng hoặc có thẻ tín dụng. Nếu khách hàng có nhiều tài khoản hay thẻ trong ngân hàng, ngân hàng sẽ được thông báo cái nào trong số chúng sẽ được dùng để thanh toán di động. Ngân hàng có quyền tính phí vào tài khoản hay thẻ của khách hàng khi nhận được đơn thanh toán ký bởi khóa bí mật của khách hàng.

Các phần tiếp theo sẽ mô tả việc thanh toán POS ảo và thực (máy bán hàng tự động). Các ký hiệu sau sẽ được dùng để mô tả: *C* là khách hàng, *M* là thương gia, *B* là ngân hàng. là định danh của chủ thể *X*. là khóa RSA bí mật của chủ thể *X* và là khóa công khai tương ứng. là chứng thực khóa công khai của chủ thể *X*. cho biết mã hóa RSA thông điệp *m* bằng khóa *K*. là chữ ký số do *X* tạo, được kiểm tra bởi *Y*. *H* là hàm băm, giao thức là SHA-1.

1. Thanh toán POS ảo

Giao thức cho thanh toán POS ảo bằng di động bao gồm các bước sau:

**Yêu cầu dịch vụ.** Trong bước 1, khách hàng khởi tạo giao thức với thương gia bằng việc yêu cầu chọn lựa dịch vụ. Yêu cầu có thể chứa thông tin giới hạn chọn lựa có thể có, như ngày và thời gian.



**Hình 6:** mô hình thanh toán POS ảo

**Chọn lựa dịch vụ.** Trong bước 2, thương gia gửi danh sách chọn lựa cho thiết bị di động. Danh sách này sẽ mô tả ngắn sản phẩm và giá cả. Thương gia cũng đính kèm chứng nhận với danh sách chọn lựa.

**Chọn lựa sản phẩm.** Trong bước 3, khách hàng phải chọn lựa sản phẩm từ danh sách. Thông tin chọn lựa của khách hàng sẽ được gửi qua cho thương gia. Chọn lựa này được ký bằng bằng khóa bí mật của khách hàng. Thông điệp là:

Trong đó là chuỗi mô tả chi tiết sản phẩm. và là số nonce ngẫu nhiên và nhãn thời gian do khách hàng *C* tạo. *AM* là số tiền mà sản phẩm tiêu tốn.

**Yêu cầu thanh toán.** Bước 4 của giao thức bao gồm việc thương gia gửi chi tiết thanh toán cho công ty tín dụng. Thông tin thanh toán được ký bởi khóa bí mật của thương gia và mã hóa bằng khóa công khai của công ty tín dụng. Thông điệp của bước 4 bao gồm chi tiết của thương gia và thanh toán như số lượng, định danh của khách hàng và thông điệp đã ký nhận được từ bước 3.

Trong thông điệp này là chữ ký ở bước 3. Sau khi nhận được thông điệp này thì công ty tín dụng *B* kiểm tra nhãn thời gian có mới hơn nhãn thời gian của lần liên lạc trước đó hay không, để phát hiện tấn công lặp lại (relay attack).

**Xác nhận thanh toán.** Lượng tiền được chuyển từ tài khoản của người mua sang tài khoản của người bán. Bước 5 do công ty tín dụng bắt đầu nếu giao dịch được xử lý và thông qua lần cuối. Công ty tín dụng sẽ gửi thông điệp xác nhận cho thương gia. Thông điệp này được ký bởi khóa bí mật của công ty tín dụng.

Từ thông điệp này, thương gia có thể kiểm tra thanh toán là lượng *AM* và từ tài khoản của *C* chuyển vào tài khoản của *M*. Giá trị băm là để khách hàng chắc chắn rằng thương gia không thể cáo buộc khách hàng đã mua một sản phẩm nào khác so với sản phẩm ban đầu.

**Phân phối sản phẩm.** Cuối cùng, trong bước 6, thương gia kiểm tra thông điệp nhận được ở bước 5. Nếu thông điệp hợp lệ và việc thanh toán đã thực hiện, thương gia sẽ phân phối sản phẩm đến cho khách hàng. Thương gia cũng gửi thông điệp cho khách hàng việc thanh toán đã hoàn tất và sản phẩm đã được chuyển đi.

Khách hàng có thể kiểm tra lượng tiền AM, chi tiết sản phẩm PD, số nonce và nhãn thời gian trùng khớp với giá trị ban đầu để chắc chắn rằng đã trả đúng tiền cho đúng sản phẩm.

**Use case: mua vé xe lửa**

Ví dụ như có thể sử dụng giao thức để mua vé xe lửa công cộng. Vé xe đôi khi được xem như giá trị tiền tệ. Đồng thời, việc duy trì một phòng bán vé cũng rất tốn chi phí. Việc mua một vé xe diễn ra như sau:

Bước 1: khách hàng tìm hành trình phù hợp và gửi tin SMS đến tổng đài viên xe lửa. Thông điệp này gồm điểm khởi đầu, điểm kết thúc, ngày giờ và có thể có thời gian xấp xỉ của hành trình.

Bước 2: tổng đài viên phản hồi với tất cả kết nối phù hợp câu truy vấn cùng với thông tin giá.

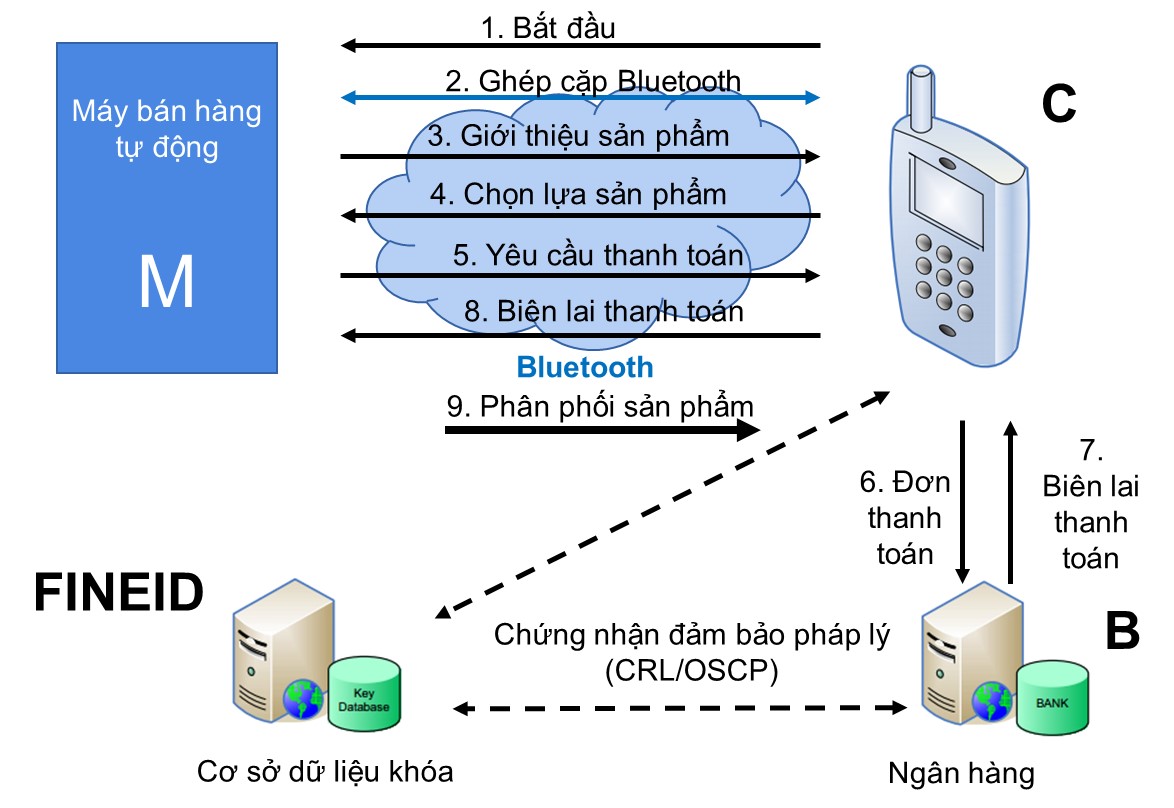
Bước 3: khách hàng chọn lựa hành trình phù hợp và gửi yêu cầu đến công ty xe lửa. Yêu cầu bao gồm định danh của kết nối đã chọn và chi tiết thẻ tín dụng của khách hàng. Chi tiết thẻ được mã hóa bằng khóa công khai của công ty tín dụng nên công ty xe lửa không để đọc được. Đơn hàng được ký bởi khách hàng.

Bước 4: công ty xe lửa gửi cho công ty tín dụng thông tin số tiền cần thanh toán và chi tiết được ký và mã hóa bằng khóa công khai của công ty tín dụng, đồng thời đính kèm tài khoản tín dụng và chi tiết đơn thanh toán của khách hàng.

Bước 5: sau khi nhận thông điệp từ bước 4, công ty tín dụng sẽ kiểm tra chữ ký của khách hàng và công ty xe lửa, trừ vào tài khoản của khách hàng, gửi phản hồi cho công ty xe lửa. Phản hồi này gồm có biên lai thanh toán ký bởi công ty tín dụng.

Bước 6: công ty xe lửa phát thành một thẻ điện tử đã ký. Vé được gửi đến khách hàng cùng với biên lai thanh toán. Trong xe lửa, người soát vé có thể kiểm tra thẻ điện tử nếu cần thiết bằng một đoạn mã lưu trong hệ thống thông tin của công ty xe lửa.

1. Thanh toán POS thực (máy bán hàng tự động)



**Hình 7:** tổng quan về giao thức thanh toán thực

**Bắt đầu.** Ở bước 1, người dùng *C* khởi tạo giao thức với thương gia *M* bằng việc chọn sản phẩm. Trong trường hợp máy bán hàng tự động chấp nhận nhiều cách thanh toán, người dùng cần phải chỉ rõ phương pháp thanh toán. Hoặc cũng có thể máy sẽ tự động khởi tạo giao thức, phát hiện thiết bị khi nó đến gần bán kính liên lạc Bluetooth. Không có thông điệp nào được gửi đi.

**Ghép cặp Bluetooth.** Để trao đổi thông điệp, máy bán hàng sẽ kết nối Bluetooth với điện thoại di động. Trong trường có nhiều thiết bị trong bán kính, máy bán hàng sẽ sinh ngẫu nhiên số PIN để ghép cặp và hiển thị số này ra màn hình. Người dùng phải nhập số PIN vào điện thoại.

**Giới thiệu sản phẩm.** Nếu người dùng chưa chọn sản phẩm, máy bán hàng sẽ gửi thông điệp với thông tin về các sản phẩm và giá tương ứng. Trong trường hợp bước 1 đã được khách hàng bắt đầu thì danh sách sản phẩm chỉ chứa sản phẩm đã được chọn từ ban đầu. Ngoài ra nó còn gửi chứng nhận và số nonce .

Sau khi nhận thông điệp, *C* sẽ lấy ra chứng nhận của *M* và kiểm tra tính hợp lệ.

**Chọn lựa sản phẩm.** Người dùng phải chọn sản phẩm, trừ khi nó đã được chọn. Thông tin chọn lựa của người dùng được gửi đến máy. Đồng thời chứng nhận giữ khóa công khai của người dùng được gửi đến máy bán hàng.

Điện thoại phải lưu lại giá *AM* của sản phẩm được chọn, sau này dùng để thanh toán.

Thông điệp trong bước này chứa ba phần. Phần đầu là chọn lựa của người dùng *S*, và số nonce do điện thoại tạo. Phần thông điệp này được mã hóa với khóa công khai của máy bán hàng. Sau đó chứng nhận của người dùng được gắn vào thông điệp. Phần cuối là chữ ký.

Sau khi nhận thông điệp, *M* lấy chứng nhận của C, kiểm tra, giải mã chữ ký SIG để nhận được . Sau khi giải mã thông điệp, *M* nhận được S và . Để kết luận, *M* tính hàm băm và kiểm tra . Máy bán hàng cũng có thể kiểm tra danh sách hủy bỏ chứng nhận để biết chứng nhận người dùng chưa bị thu hồi, nhưng việc kiểm tra cũng có thể là trách nhiệm của ngân hàng.

**Yêu cầu thanh toán.** Trong bước 5, máy bán hàng sẽ gửi yêu cầu thanh toán cho thiết bị di động. Yêu cầu này được ký bằng khóa bí mật của máy bán hàng.

Chi tiết thanh toán bao gồm số tài khoản và định danh tham chiếu của máy bán hàng. Lưu ý rằng giá của sản phẩm không được gửi trong chi tiết thanh toán vì *C* đã biết. Tuy nhiên nó cũng được gắn vào trong phần hai của thông điệp. Chứng nhận của *C*, giá sản phẩm *AM*, hai số nonce và được ghép lại, băm và ký bằng khóa bí mật của máy bán hàng, sau đó gắn vào thông điệp *MSG*. Phần cuối là chữ ký.

*C* sau đó sẽ gửi giá trị băm đã được ký của chứng nhận của *C*, giá và hai số nonce đến ngân hàng *B*. Ngân hàng sử dụng nó như là bằng chứng cho việc giao dịch. Bằng cách này, *C* không thể đưa một chứng nhận cho *M* và một cái khác cho *B*, hoặc đổi số lượng tiền cần trả. *C* có thể lưu giá trị băm đã ký như là biên lai cho máy bàn hàng, kết hợp với biên lai từ ngân hàng (ở bước 7) trở thành bằng chứng mua hàng nếu có tranh chấp xảy ra.

Sau khi nhận được thông điệp *MSG*, *C* kiểm tra chữ ký *SIG* sử dụng khóa công khai của *M*.

**Tạo hóa đơn thanh toán.** Trong bước 6, người dùng di động *C* sẽ liên lạc với ngân hàng *B*. Ngoài thông tin nhận được từ *M* ở bước trước thì cần gửi thêm số tài khoản và nhãn thời gian để giao dịch. Hóa đơn thanh toán gửi đến ngân hàng, mã hóa bằng khóa công khai của ngân hàng và ký bằng khóa bí mật của *C*.

Ở đây giả sử rằng người dùng đã có khóa công khai của ngân hàng.

**Xử lý thanh toán.** Sau khi nhận và giải mã hóa đơn thanh toán, ngân hàng kiểm tra chữ ký của *C* đính kèm. Ngân hàng nhận chứng nhận của *C* từ thư mục FINEID LDAP (Lightweight Directory Access Protocol); được dùng như khóa để tìm. Cùng lúc đó ngân hàng lấy chứng nhận của *M* để kiểm tra . Điều này để đảm bảo rằng cùng một chứng nhận và số nonce được dùng khi liên lạc giữa *C* và *M*. Ngoài ra ngân hàng còn kiểm tra rằng không chứng nhận nào bị hủy bỏ. Ngân hàng cũng so sánh nhãn thời gian *TS* với nhãn thời gian của đơn thanh toán trước đó nhận từ *C* để tránh tấn công lặp lại. Sau khi kiểm tra tất cả đều thỏa, ngân hàng sẽ chuyển lượng tiền từ tài khoản của *C* sang cho tài khoản của *M*. Trong trường hợp tài khoản của *M* là của một ngân hàng khác, một thủ tục bên trong ngân hàng sẽ được dùng để chuyển tiền cho *M*. Nếu giao dịch thành công, ngân hàng sẽ gửi thông báo xác nhận (biên lai) đã được mã hóa đến điện thoại di động.

Hóa đơn dùng để chứng minh thanh toán đã hoàn tất. Số tài khoản ngân hàng của máy bán hàng, lượng tiền, hai số nonce và được băm và ký bởi khóa bí mật của ngân hàng.

*C* có tất cả thông tin cần để tính toán cùng giá trị băm và kiểm tra chữ ký của ngân hàng.

**Bằng chứng thanh toán.** Ở bước 8, điện thoại chuyển tiếp biên lai của ngân hàng cho máy bán hàng. Để xác định được khóa công khai nào của ngân hàng được dùng để kiểm tra biên lai, định danh của ngân hàng được ghép vào thông điệp.

Ở đây giả sử rằng máy bán hàng đã có chứng nhận tham gia ngân hàng. Nhờ đó, máy có thể giải mã biên lai dùng khóa công khai của ngân hàng. Máy bán hàng sau đó tính hàm băm và kiểm tra rằng giá trị ra giống như trong biên lai.

Máy bán hàng phải có một danh sách các chứng nhận khóa công khai hợp lệ của các ngân hàng khác nhau. Máy bán hàng không cần có kết nối mạng, giao thức có thể mở rộng để kiểm tra tính hợp lệ của chứng thực ngân hàng bằng cách chuyển tiếp một yêu cầu giao thức trạng thái chứng nhận online (OCSP) qua điện thoại điện thoại di động đến một máy chủ OCSP đáng tin cậy.

# Chương trình ứng dụng

1. Giới thiệu
2. Mô tả chức năng ứng dụng

# Tài liệu tham khảo

Tiếng Anh:

1. Charlie Miller, Dion Blazakis, Dino DaiZovi, Stefan Esser, Vincenzo Iozzo, Ralf-Philipp Weinmann: “*iOS Hacker's Handbook*”, Wiley, ISBN 978-1118204122, 2012.
2. Collin Richard Mulliner: “*Security of Smart Phones*”, Department of Computer Science, University of California, 2006.
3. Jonathan Zdziarski: “*Hacking and Securing iOS Applications*”, O'Reilly Media, ISBN 978-1449318741, 2012.
4. Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski: “*Android Hacker's Handbook*”, Wiley, ISBN 978-1118608647, 2014.
5. Ken Dunham: “*Mobile Malware Attacks and Defense*”, Syngress, ISBN 978-1597492980, 2004.
6. Lawrence C. Miller: “*Securing Smartphones & Tablets For Dummies*”, John Wiley & Sons, Inc., 2012.
7. Marko Hassinen: “*Studies in Mobile Security*”, Department of Computer, Science, University of Kuopio, 2007.
8. Neil Bergman, Mike Stanfield, Jason Rouse, Joel Scambray: “*Hacking Exposed Mobile”*, McGraw-Hill Osborne Media, ISBN 978-0071817011, 2013.

Website:

1. <http://blogs.cisco.com/security/securing-mobile-data-in-the-event-of-device-loss-or-theft>
2. <http://en.wikipedia.org/wiki/Mobile_operating_system>