**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 điện thoại thông minh**

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** |
| PDA | Personal digital assistant | Máy trợ giúp cá nhân kỹ thuật số |
| WLAN | Wireless local area networks | Mạng cục bộ không dây |
| PIM | Personal information management | Quản lý thông tin cá nhân |
|  |  |  |
|  |  |  |
|  |  |  |

Mục lục

[Thông tin nhóm 1](#_Toc397711085)

[Danh mục các kí hiệu, chữ viết tắt và ý nghĩa 1](#_Toc397711086)

[I. Giới thiệu 3](#_Toc397711087)

[II. Thiết bị di động 3](#_Toc397711088)

[1) Tổng quan 3](#_Toc397711089)

[2) Công nghệ không dây 4](#_Toc397711090)

[3) Hệ điều hành di động 4](#_Toc397711091)

[4) Phần mềm thiết bị di động 4](#_Toc397711092)

[III. Mô hình nguy cơ 5](#_Toc397711093)

[1) Loss or Theft of Devices 5](#_Toc397711094)

[2) Denial-of-Service Attacks 5](#_Toc397711095)

[3) Wireless Attacks 5](#_Toc397711096)

[4) Break-In Attacks 5](#_Toc397711097)

[5) Viruses and Worms 5](#_Toc397711098)

[6) Infrastructure-based Attacks 5](#_Toc397711099)

[7) Overcharging Attacks 5](#_Toc397711100)

[IV. Cross-Service Attacks 5](#_Toc397711101)

[1) Giới thiệu 5](#_Toc397711102)

[2) Tấn công Cross-Service 5](#_Toc397711103)

[3) Ngăn ngừa Cross-Service Attacks bằng gán nhãn 5](#_Toc397711104)

[4) Cài đặt 5](#_Toc397711105)

[5) Đánh giá 5](#_Toc397711106)

[V. Giao thức và chi trả di động 5](#_Toc397711107)

[1) Payment protocols 5](#_Toc397711108)

[2) Virtual POS Payment 5](#_Toc397711109)

[3) Real POS (Vending Machine) Payment 5](#_Toc397711110)

[4) Traffic analysis 5](#_Toc397711111)

[VI. Chương trình ứng dụng 5](#_Toc397711112)

[VII. Tài liệu tham khảo 5](#_Toc397711113)

# 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 giao diện 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.

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.

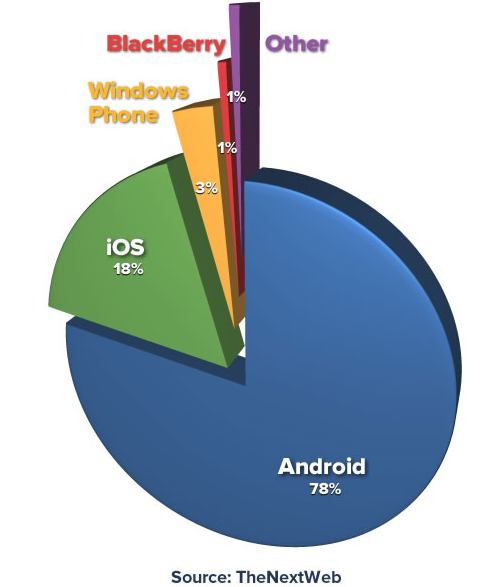
Máy nghe nhạc di động thường dùng để truy cập nội dung đa phương tiện. Hầu hết được gọi là máy nghe nhạc và chúng không thể cài đặt phần mềm thêm vào. Đa số đều cài một hệ điều hành đã được tùy chỉnh.

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 tin 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.



**Hình 1:** thị phần hệ điều hành di động trong quý 4 2013

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
2. Hệ điều hành di động
3. Phần mềm thiết bị di động

# Mô hình nguy cơ

1. Loss or Theft of Devices:

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 vừa qua. 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.. 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 sự đánh cắp thiết bị di động là sự tăng trưởng không ngừng các thiết bị di động, kết hợp với sự mạnh mẽ của các dịch vụ đám mây, đã làm thay đổi 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 giẫu thông tin vị trí ngườ dùng, thì những vấn đề về bảo mật thiết bị di động 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, chải sẻ file, kiểm tra e mail 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 viêc 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 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 thiết bị đánh mất (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 nhân 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 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

http://blogs.cisco.com/security/securing-mobile-data-in-the-event-of-device-loss-or-theft/

1. Denial-of-Service Attacks
2. Wireless Attacks
3. Break-In Attacks
4. Viruses and Worms
5. Infrastructure-based Attacks
6. Overcharging Attacks

# Cross-Service Attacks

1. Giới thiệu
2. Tấn công Cross-Service
3. Ngăn ngừa Cross-Service Attacks bằng gán nhãn
4. Cài đặt
5. Đánh giá

# Giao thức và chi trả di động

1. Payment protocols
2. Virtual POS Payment
3. Real POS (Vending Machine) Payment
4. Traffic analysis

# Chương trình ứng dụng

# Tài liệu tham khảo

Tiếng Anh:

1. Marko Hassinen, *Studies in Mobile Security*, 2007
2. Neil Bergman, Mike Stanfield, Jason Rouse, Joel Scambray, *Hacking Exposed Mobile*, 2013
3. Santa Barbara, *Security of Smart Phones*, 2006

Website: