**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



Học phần: **Quản lý an toàn thông tin**

Bài báo cáo:

**Phân tích đánh giá rủi ro ứng dụng Bluezone sử dụng NIST SP 800-30**

**Giảng viên hướng dẫn**: TS. Phạm Hoàng Duy

**Sinh viên thực hiện:** Nhóm 1

Nguyễn Tuấn Anh B17DCAT008

Nguyễn Hải Đăng B17DCAT032

Nguyễn Công Cháng B17DCAT024

Phạm Ngọc Khánh B17DCAT105

Hà Nội 2020

MỤC LỤC

[Chương 1. Giới thiệu về NIST 3](#_Toc56979222)

[I.Giới thiệu về NIST 3](#_Toc56979223)

[II.Giới thiệu NIST SP 800-30 4](#_Toc56979224)

[Chương 2. Đánh giá rủi ro của Bluezone sử dụng NIST SP800-30 5](#_Toc56979225)

[A.NGUYỄN TUẤN ANH – B17DCAT008 5](#_Toc56979226)

[I. Mô tả đặc trưng hệ thống 5](#_Toc56979227)

[1. Mô tả đặc trưng hệ thống 5](#_Toc56979228)

[2. Tổng quan về hệ thống Bluezone 5](#_Toc56979229)

[II.Xác định đe dọa 8](#_Toc56979230)

[1.Thiết bị người dùng bị xâm hại phần cứng bởi các tác nhân bên ngoài 8](#_Toc56979231)

[2.Dữ liệu người dùng bị xâm hại bởi phầm các nguyên nhân chủ quan 9](#_Toc56979232)

[3.Thiết bị không được hỗ trợ từ chính sách của Google, từ công nghệ BLE 9](#_Toc56979233)

[4.Cơ hội khai thác dữ liệu người dùng từ bên thứ ba 10](#_Toc56979234)

[III.Xác định lỗ hổng 12](#_Toc56979235)

[Lỗ hổng 1: Dữ liệu lưu trữ trên máy người dùng không được mã hóa và không được tìm thấy trên máy người dùng. 12](#_Toc56979236)

[Lỗ hổng 2: Khả năng giả mạo người dùng thông qua đăng ký tên và địa chỉ lỏng lẻo 12](#_Toc56979237)

[Lỗ hổng 3: Cấp quyền không cần thiết (vị trí, máy ảnh,danh bạ) 13](#_Toc56979238)

[IV.Phân tích kiểm soát 14](#_Toc56979239)

[1.Biện pháp hiện thời 14](#_Toc56979240)

[2. Biện pháp sắp tới 14](#_Toc56979241)

[V.Xác định mức độ chắc chắn 14](#_Toc56979242)

[VI.Phân tích tác động 15](#_Toc56979243)

[VII.Xác định rủi ro 15](#_Toc56979244)

[VIII.Khuyến nghị các biện pháp kiểm soát 16](#_Toc56979245)

[IX.Lập báo cáo kết quả 16](#_Toc56979246)

[**B. NGUYỄN HẢI ĐĂNG – B17DCAT032** 16](#_Toc56979247)

[1.Mô tả đặc trưng hệ thống 16](#_Toc56979248)

[2.Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool. 17](#_Toc56979249)

[2.1.Phân tích bằng virustotal và AndroPyTool: 17](#_Toc56979250)

[C. NGUYỄN CÔNG CHÁNG – B17DCAT024 23](#_Toc56979251)

[I. Mô tả đặc trưng của hệ thống: 23](#_Toc56979252)

[1. Bên phía nhà cung cấp: 23](#_Toc56979253)

[2. Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool: 24](#_Toc56979254)

[II. Xác định mối đe dọa. 25](#_Toc56979255)

[III.Xác định lỗ hổng: 26](#_Toc56979256)

[IV. Phân tích các biện pháp kiểm soát: 27](#_Toc56979257)

[V. Xác định mức độ chắc chắn: 28](#_Toc56979258)

[VI. Phân tích tác động: 28](#_Toc56979259)

[VII. Xác định rủi ro: 29](#_Toc56979260)

[VIII. Khuyến nghị các biện pháp kiểm soát: 29](#_Toc56979261)

[D. PHẠM NGỌC KHÁNH- B17DCAT105 29](#_Toc56979262)

[I. Mô tả đặc trưng của hệ thống: 29](#_Toc56979263)

[1. Bên phía nhà cung cấp: 29](#_Toc56979264)

[2. Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool: 30](#_Toc56979265)

[II. Xác định mối đe dọa. 31](#_Toc56979266)

[III. Xác định lỗ hổng: 32](#_Toc56979267)

[1.Nguy cơ khai báo giả mạo. 33](#_Toc56979268)

[2. Khi máy người dùng bị root (giải pháp: mã hóa dữ liệu, chống root/jailbreak) 33](#_Toc56979269)

[3. Mất thiết bị cài Bluezone (giải pháp : mã hóa dữ liệu) 33](#_Toc56979270)

[4.Máy điện thoại bị root/jailbreak 33](#_Toc56979271)

[IV. Phân tích các biện pháp kiểm soát: 33](#_Toc56979272)

[V. Xác định mức độ chắc chắn: 34](#_Toc56979273)

[VI. Phân tích tác động: 34](#_Toc56979274)

[VII. Xác định rủi ro: 34](#_Toc56979275)

[VIII. Khuyến nghị các biện pháp kiểm soát: 34](#_Toc56979276)

[IX. Lập báo cáo: 34](#_Toc56979277)

Chương 1. Giới thiệu về NIST

I.Giới thiệu về NIST

Năm 1901, do một dự luật của Nghị sĩ James H. Southard (đại diện Bang Ohio) đề xuất, Cục Tiêu chuẩn Quốc gia (National Bureau of Standards) của Mỹ được thành lập với nhiệm vụ cung cấp các đo lường tiêu chuẩn và hoạt động như một phòng thí nghiệm vật lý quốc gia.

Cục Tiêu chuẩn được hình thành với vai trò là một cơ quan đo lường, được chỉ đạo thành lập các bộ phận nhằm phát triển các tiêu chuẩn thương mại về vật liệu và sản phẩm. Trong thế chiến thứ Nhất, Cục Tiêu chuẩn đã nghiên cứu nhiều vấn đề phục vụ sản xuất cho chiến tranh. Trong chiến tranh thế giới thứ Hai, các nghiên cứu và phát triển trong lĩnh vực quân sự được thực hiện.

Năm 1948, với sự tài trợ của Không quân Mỹ, Cục Tiêu chuẩn bắt đầu thiết kế và xây dựng máy tính SEAC (Máy tính tự động phía Đông tiêu chuẩn - Standards Eastern Automatic Computer). Máy tính đã đi vào hoạt động từ tháng 5/1950. Cùng thời điểm, SWAC (Máy tính tự động phía Tây tiêu chuẩn - Standards Western Automatic Computer) cũng được xây dựng tại văn phòng Los Angeles của Cục Tiêu chuẩn và được sử dụng để nghiên cứu.

Do nhiệm vụ thay đổi, vào năm 1988, Cục Tiêu chuẩn đã trở thành Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). NIST có trụ sở chính tại thành phố Gaithersburg, bang Maryland và điều hành một cơ sở tại thành phố Boulder, bang Colorado.

Hiện nay, NIST có các phòng thí nghiệm:

- Công nghệ truyền thông (Communications Technology Laboratory);

- Kỹ nghệ (Engineering Laboratory);

- Công nghệ thông tin (Information Technology Laboratory);

- Đo lường vật liệu (Material Measurement Laboratory);

- Đo lường vật lý (Physical Measurement Laboratory).

NIST có 07 ủy ban thường trực để hỗ trợ ngành công nghiệp Mỹ, các Viện nghiên cứu và các phòng thí nghiệm khác của chính phủ Mỹ. Ngoài ra, NIST còn điều hành 02 cơ sở thí nghiệm đặc biệt: Trung tâm Nghiên cứu Neutron (NIST Center for Neutron Research) và Trung tâm Khoa học và Công nghệ Giới hạn nano (Center for Nanoscale Science and Technology).

II.Giới thiệu NIST SP 800-30

Mục đích của NIST 800-30 là cung cấp hướng dẫn để tiến hành đánh giá rủi ro của các tổ chức và hệ thống thông tin liên bang. Đánh giá rủi ro, được thực hiện ở cả ba cấp trong hệ thống phân cấp quản lý rủi ro, là một phần của quy trình quản lý rủi ro tổng thể. Cung cấp cho các nhà lãnh đạo / giám đốc điều hành cấp cao thông tin cần thiết để xác định các hành động thích hợp nhằm ứng phó với các rủi ro đã xác định.

Chương 2. Đánh giá rủi ro của Bluezone sử dụng NIST SP800-30

A.NGUYỄN TUẤN ANH – B17DCAT008

I. Mô tả đặc trưng hệ thống

1. Mô tả đặc trưng hệ thống

Bluezone là ứng dụng sử dụng công nghệ Bluetooth năng lượng thấp, giúp bảo vệ cộng đồng trong việc phòng, chống dịch COVID-19.

Bluezone cảnh báo nếu người dùng đã tiếp xúc gần với người nhiễm COVID-19, giảm thiểu các nguy cơ lây lan trong cộng đồng, giúp cho quá trình truy vết tìm ra F0 hoặc những đối tượng phơi nhiễm thứ cấp F1, F2 …, Fn.

2. Tổng quan về hệ thống Bluezone

2.1. Mô tả hệ thống

Các smartphone cài ứng dụng Bluezone có thể giao tiếp với nhau trong khoảng cách 2m, ghi nhận sự tiếp xúc gần vào lúc nào và trong bao lâu. Khi có một ca nhiễm SARS-CoV-2 mới, cơ quan y tế nhập dữ liệu F0 này lên hệ thống. Hệ thống sau đó gửi dữ liệu F0 đến các smartphone khác cài ứng dụng Bluezone. Lịch sử tiếp xúc với F0 trong 14 ngày trước đó sẽ được phân tích, đối chiếu và nếu trùng khớp, ứng dụng Bluezone sẽ cảnh báo cho người dùng có nguy cơ lây nhiễm, đồng thời hướng dẫn họ liên hệ với cơ quan Y tế để nhận trợ giúp.



Hình 1. Mô hình hoạt động của Bluezone

2.2. Nguyên tắc của Bluezone

Sự ra đời của Bluezone dựa trên triết lý Bảo vệ mình, Bảo vệ cộng đồng: Ứng dụng cảnh báo cho bạn nếu bạn tiếp xúc gần với người nhiễm SARS-CoV-2, khi tham gia cộng đồng là bạn đã kết nối và bảo vệ cộng đồng, bảo vệ Thế giới. Hoạt động của Bluezone dựa trên nguyên tắc: Bảo mật dữ liệu: Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19. Không thu thập vị trí: Ứng dụng không thu thập dữ liệu về vị trí của bạn.

Ẩn danh: Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm SARS-CoV-2. Minh bạch: Mã nguồn của dự án được phân phối theo giấy phép GNU GPL v3. Người dùng các nước trên Thế giới được tự do tìm hiểu hoạt động hệ thống ở mức mã nguồn, được tự do sử dụng, nghiên cứu, sửa đổi và chia sẻ.

2.3. Thuật toán truy vết tiếp xúc Bluetooth

2.3.1. Mô tả công nghệ bluetooth

Mỗi Bluezone Smartphone sẽ đóng 2 vai trò hoạt động (role), vừa là Thiết bị Peripheral (Thiết bị Phát) và vừa là Thiết bị Central (Thiết bị Thu). Thiết bị phát sẽ phát các mã Bluezone Id (BLID) ngẫu nhiên, thay đổi sau mỗi khoảng thời gian (tại Việt Nam hiện đang sử dụng cấu hình là 15 phút đổi 1 lần). Mỗi BLID có độ dài 12 byte (sẽ giải thích ở phía dưới). BLID của thiết bị phát này sẽ được các thiết bị thu khác ghi nhận, lưu trữ để tính toán về việc tiếp xúc gần khi có phát sinh F0 sau này. Thuật toán sinh BLID thay đổi theo thời gian như sau:

2.3.2. Giải thích các khái niệm

- BluezoneBaseID: Khóa ngẫu nhiên cho mỗi người dùng có độ dài 256 bits, không chia sẻ với bất kỳ ai.

- D0: Ngày bắt đầu cái Bluezone

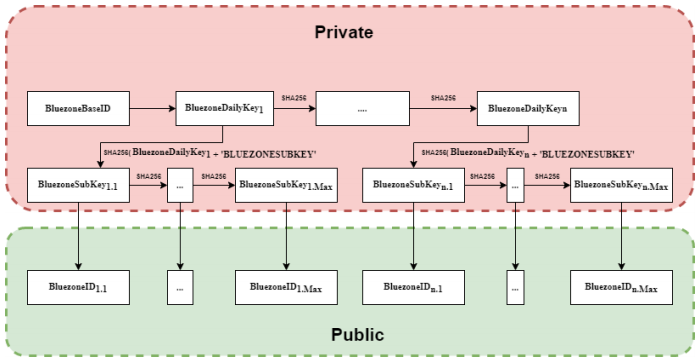
- BluezoneDailyKeyn: Khóa thay đổi hàng ngày, được sinh ra từ BluezoneBaseID. Khóa này sẽ được sử dụng trong trường hợp phát hiện F0

- Max: Tổng số ID được sinh trong 01 ngày, mặc định là 96 – tương đương với 15 phút đổi ID 1 lần

- Mỗi ngày sẽ sinh BluezoneID (BLID) theo các mốc thời gian trong ngày, sao cho tổng số BluezoneID trong ngày đạt mức Max

- Dk: Là ngày bắt đầu điều tra dịch tễ với 1 F0 khi phát hiện - Te: Là thời điểm nhân viên Y tế công nhận F0 và đưa thông tin F0 vào hệ thống để quảng bá tìm F1.

2.3.3. Thuật toán sinh BLID chi tiết



Hình 2. Mô hình sinh khóa của Bluezone

**Bước 0**: Sinh mã BluezoneBaseID khi người dùng cài Bluezone.

**Bước 1**: Hàng ngày sinh tiếp BluezoneDailyKey theo công thức: BluezoneDailyKeyn = SHA256(BluezoneDailyKeyn-1)

**Bước 2**: Tùy vào số lượng ID muốn thay đổi trong ngày (được cấu hình từ server), thực hiện sinh số Key phụ tương ứng (ví dụ 15 phút đổi ID một lần thì sẽ sinh ra 96 Key phụ). Công thức sinh Key phụ như sau: BluezoneSubKeyn.1 = SHA256(BluezoneDailyKeyn+ ‘BLUEZONESUBKEY’) BluezoneSubKeyn.i = SHA256 (BluezoneSubKeyn.i-1)

**Bước 3**: Sinh BLID để phát, thu và lưu trữ dưới dạng mảng byte có độ dài là 12 byte theo nguyên tắc: Lấy các byte ở vị trí thứ 0, 4, 8, 12, 16, 18, 20, 22, 24, 26, 28, 30 trong mảng 32 byte của BluezoneSubKey để làm giá trị cho 12 byte của BLID.

2.3.4 Truy vết tiếp xúc

Khi phát hiện F0, Cơ quan Y tế cập nhật (BluezoneDailyKeyk, Dk, Max,Te) lên hệ thống. Trong đó Dk là ngày bắt đầu điều tra dịch tễ (ví dụ cách thời điểm phát hiện F0 14 ngày), BluezoneDailyKeyk là Key tương ứng của F0 tại thời điểm ngày Dk , Te là thời điểm chốt thông 6 tin F0, nếu các lịch sử tiếp xúc với F0 sau thời điểm này sẽ không có giá trị vì F0 sẽ được đổi 1 BluezoneBaseID khác kể từ thời điểm Te. Max là số BluezoneID sinh trong 1 ngày.

Hệ thống sau đó sẽ phát quảng bá bộ số (BluezoneDailyKeyk, Dk, Max, Te) xuống cho toàn bộ Bluezoner. Các Bluezoner sẽ dựa vào (BluezoneDailyKeyk, Dk, Max, Te) để sinh tiếp lần lượt DailyKey => SubKey => BluezoneID với số lượng Max BluezoneID cho 1 ngày theo thuật toán ở mục 4.1.2.

Mỗi BLID của F0 sẽ chỉ có giá trị trong 1 khoảng thời gian xác định trong ngày, thời gian này được xác định như sau:

- Khoảng thời gian giữa 2 lần sinh BLID liên tiếp trong ngày là: ∆t = 24∗3600∗1000 Max−1

- BluezoneIDi (lần sinh thứ i trong ngày) chỉ có giá trị ghi nhận tiếp xúc trong khoảng từ (i – 1)\* ∆t đến i \*∆t

- Nếu phát hiện lịch sử tiếp xúc trên máy của người dùng có ghi nhận BluezoneIDi của F0, thời gian tiếp xúc ghi nhận là t. Người dùng chỉ được xác định là tiếp xúc với F0 khi và chỉ khi: (i – 1)\*∆t ≤ t < i\*∆t và t < Te

II.Xác định đe dọa

***“Tất cả dữ liệu về lịch sử tiếp xúc chỉ lưu trữ trên smartphone của người dùng, không chuyển lên hệ thống lưu trữ tập trung. Ứng dụng cũng không thu thập về dữ liệu vị trí của người dùng. Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm COVID-19.”*** trích Bluezone White paper.

Dựa trên cơ chế này có thể thấy được sẽ phát sinh rất nhiều rủi ro xoay quanh việc lưu trữ và bảo mật dữ liệu khi chúng ở trên thiết bị của người dùng. Sau đây là các mối đe dọa có thể xảy ra đối với ứng dụng Bluezone.

1.Thiết bị người dùng bị xâm hại phần cứng bởi các tác nhân bên ngoài

1.1.Tác nhân môi trường

Mức độ ảnh hưởng của các lỗi phần cứng lên điện thoại là khác nhau. Có lỗi nặng, có lỗi nhẹ. Nhìn chung thì lỗi phần cứng được đánh giá nghiêm trọng hơn so với những lỗi phần mềm trên smartphone. Các lỗi phần cứng do môi trường như độ ẩm, nhiệt độ, áp suất, sử dụng thiết bị trong môi trường khắc nghiệt…

Có rất nhiều lỗi phần cứng có thể gặp phải do các nguyên nhân trên, như trường hợp phần cứng bao gồm chip và vi mạch hoạt động không ổn định trong môi trường nhiệt độ cao . . . dẫn đến việc tiếp nhận và lưu trữ thông tin bị ảnh hưởng

1.2.Tác nhân con người

Khi sử dụng thiết bị di động khó tránh khỏi trường hợp kẻ xấu tiếp cận và cài thêm một số module nhằm xâm hại thiết bị. Đơn cử như trường hợp chủ nhân thiết bị di động cần sửa chữa thay màn hình …thì người thợ sửa hoàn toàn có khả năng can thiệp vào các phần không phải sửa chữa trên thiết bị dẫn đến nguy cơ mất an toàn. Trường hợp khác có thể xảy ra là người dùng xâm hại chính thiết bị của mình dẫn tới các chức năng không còn được đảm bảo bảo hoạt động đúng như yêu cầu của ứng dụng.

  Tin tặc(hacker) sẽ chiếm quyền truy cập vào điện thoại và mã hóa toàn bộ dữ liệu cá nhân tìm được. Dữ liệu bị mã hóa có thể bao gồm các danh sách thiết bị tiếp xúc được Bluezone ghi lại xảy ra nguy cơ mất mát dữ liệu không thể truy xuất lịch sử tiếp xúc khi cần. Do khi cần truy xuất dữ liệu này sẽ được gửi về server. Một khi dữ liệu đã bị mã hóa thì chỉ có một chìa khóa đặc biệt bí mật mới có thể giải mã được. Trong rất nhiều trường hợp người dùng sẽ không chấp nhận thỏa hiệp và dẫn tới mất vĩnh viễn dữ liệu. Vấn đề càng trở nên nghiêm trong khi cuộc tấn công mở rộng trên hiều thiết bị thì khối lượng thông tin mất mát là vô cùng lớn.

2.Dữ liệu người dùng bị xâm hại bởi phầm các nguyên nhân chủ quan

Người dùng quản lí thiết bị không tốt, chủ quan với các đường dẫn, ứng dụng độc hại dẫn đến dễ bị hack, chiếm quyền điều khiển, đọc ghi dữ liệu. Một khi thiết bị bị khai thác bởi các tác nhân độc hại trên thì hầu như mọi nguồn tài nguyên bị phơi nhiễm gần như hoàn toàn, thiệt hại sẽ rất lớn đối với thông tin dữ liệu của chính người dùng đó. Trong trường hợp người dùng cố tình xóa, phá hủy dữ liệu dữ liệu vì mục đích nào đó mà ứng dụng không có cơ chế cảnh báo hữu hiệu thì hậu quả không thể tránh khỏi là mọi dữ liệu có được trong qua trình thu thập tiếp xúc sẽ bị hủy.

3.Thiết bị không được hỗ trợ từ chính sách của Google, từ công nghệ BLE

3.1.Giới hạn từ công nghệ BLE

Bluetooth Low Energy (BLE), hay còn được biết đến là “Bluetooth Smart”, công nghệ này được giới thiệu khi BLE 4.0 chính thức được ra mắt. Bluetooth Low Energy còn được gọi là Bluetooth năng lượng thấp, Bluetooth công suất thấp, là công nghệ mạng cá nhân.  Sử dụng phổ biến cho các nền tảng mobile như (iOS, Android,Windows Phone,...).

BLE không hoạt động trên các phiên bản IOS cũ hơn IOS 7 . Đối với Android các phiên bản thấp hơn 4.2 còn khuyến cáo của bluezone là Android 6.0.

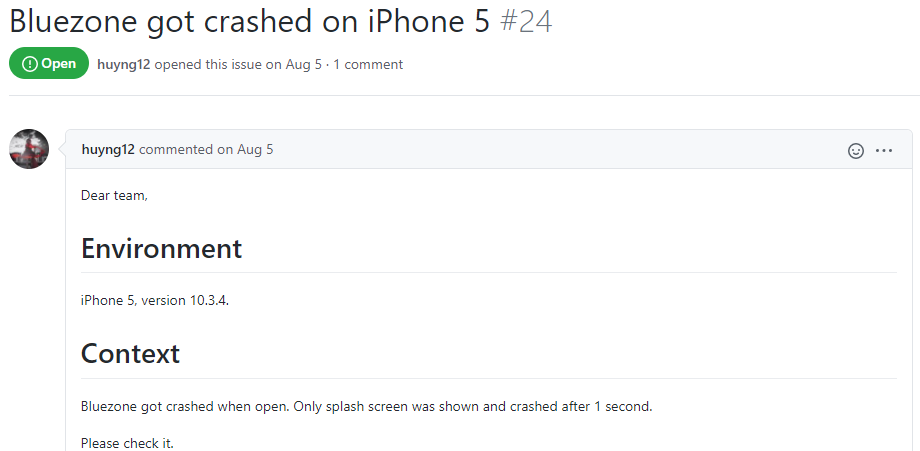
Công nghệ sử dụng để ghi lại tiếp xúc giữa các thiết bị được bluezone sử dụng chính là BLE(Bluetooth Low Energy). Các thiết bị từ IOS 10.\* và Android 6.0 được Bluezone giới hạn là phiên bản hệ điều hành thấp nhất có thể tiếp cận và sử dụng hiệu quả Bluezone. Tuy nhiên các thiết bị có hệ điều hành phiên bản thấp hơn đề xuất vẫn có thể sử dụng được, dẫn đến nhiều trường hợp bị lỗi khi sử dụng

Đối với thiết bị Android.



Hình 3. Lỗi phát sinh với Bluezone trên thiết bị Android 5.\*

Đối với thiết bị chạy hệ điều hành IOS.



Hình 4. Lỗi phát sinh với Bluezone trên thiết bị IOS Iphone 5.

3.2.Không hỗ trợ từ chính sách của Google

Thị phần điện thoại Huawei tại Viêt Nam trong năm 2019 được thống kê là 4% một con số không lớn so với thị phần các hãng như Xiaomi hay Samsung nhưng xét về số lượng người dùng được tính là đáng kể. Tuy nhiên số lượng thiết bị này không được hỗ trợ dịch vụ từ Google. Suy ra nếu các thiết bị này cài đặt Bluezone thì phải cài đặt từ các nguồn không đáng tin cậy dẫn đến nguy cơ được đề cập dưới đây.

Phân phối phần cài đặt của ứng dụng Bluezone chỉ có hai nguồn chính thống và đáng tin cậy đó là kho ứng dụng CH play và Appstore. Tức là mọi nguồn khác ngoài hai nguồn trên là không đáng tin cậy chưa tính đến việc mã nguồn của Bluezone được public trên github sẽ dẫn đến nguy cơ giả mạo ứng dụng hoặc ứng dụng bị cài mã độc rồi người dùng sẽ tải nó về mà không nghi ngại cài vào thiết bị. Từ đó gây ra nguy cơ dữ liệu bị xâm hại . . .

4.Cơ hội khai thác dữ liệu người dùng từ bên thứ ba

Các quyền mà ứng dụng yêu cầu :

* Máy ảnh
* Vị trí
* Bộ nhớ
* Chạy dịch vụ nền
* Truy cập cài đặt Bluetooth
* Kiểm tra giấy phép Google
* Xem kết nối mạng
* android.permission.ACCESS\_COARSE\_LOCATION
* android.permission.ACCESS\_FINE\_LOCATION
* android.permission.BLUETOOTH
* android.permission.BLUETOOTH\_ADMIN
* android.permission.INTERNET
* android.permission.READ\_PHONE\_STATE
* android.permission.WRITE\_EXTERNAL\_STORAGE
* com.mic.bluezone.permission.C2D\_MESSAGE



Hình 5. Các quyền xin cấp bởi Bluezone.

Trong các quyền trên thì một số quyền được cấp nhưng không phục vụ mục đích hoạt động của ứng dụng như :

* + Quyền truy cập danh bạ
  + Quyền về vị trí người dùng

Trong khi quyền về vị trí người dùng trên thiết bị Android là bắt buộc khi ứng dụng khai báo sử dụng và khai thác chức năng về Bluetooth. Đối với thiết bị IOS khi sử dụng tính năng quét xác định tiếp xúc thì nó chỉ cần sử dụng CoreBluetooth nên quyền về vị trí là không cần thiết phải được cấp cho ứng dụng. Tuy nhiên ngay khi muốn sử dụng ứng dụng này hài quyền bắt buộc phải cho phép đó là Location và Bluetooth nếu không ứng dụng sẽ không làm được gì.

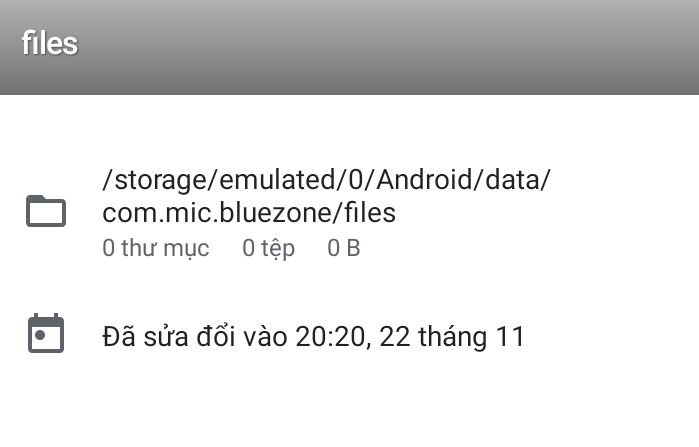
Về quyền truy cập danh bạn thì đối với một thiết bị xác định người tiếp xác và lưu và danh sách ẩn danh lại đi cần truy cập thông tin danh bạ người dùng thì đây là một quyền yêu cầu rất khó hiểu đến từ nhà phát triển Bluezone. Gây nên nguy cơ rò rỉ thông tin cá nhân ra bên ngoài cho một đơn vị thứ 3 mà người dùng không thể biết.

III.Xác định lỗ hổng

Những mối đe dọa được xác định ở mục số II rất rõ ràng từ đó xác định được các lỗ hổng tương ứng sau đây:

Lỗ hổng 1: Dữ liệu lưu trữ trên máy người dùng không được mã hóa và không được tìm thấy trên máy người dùng.

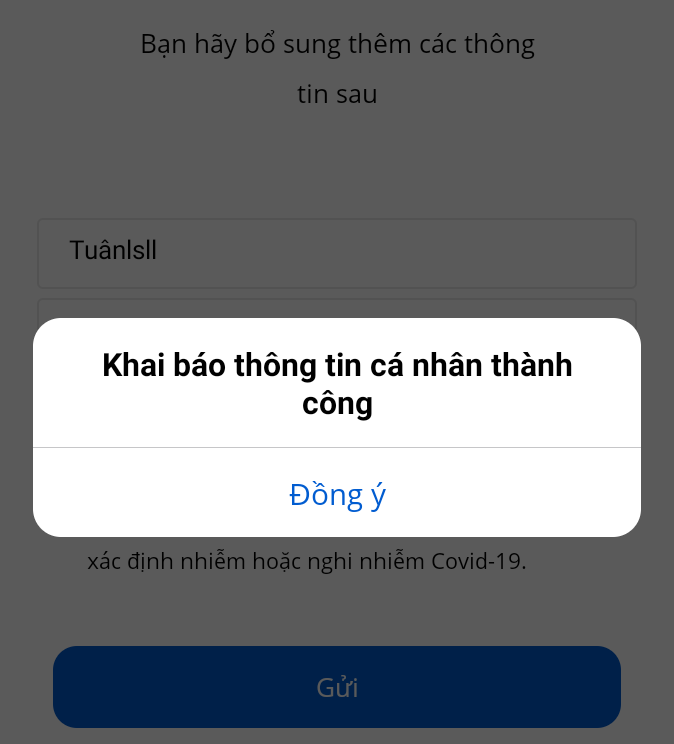
Sau khi cài đặt và sử dụng Bluezone thì theo mô tả của nhà phát triển thì dữ liệu được lưu trữ ngay trên ổ nhớ thiết bị mà không lưu trữ tập trung trên Server cụ thể là Google Filebase. Tuy nhiên khi tìm đến thư mục lưu trữ của Bluezone hoàn toàn không phát hiện được dữ liệu lưu trữ ở đâu cũng như hình thức mã hóa cho dữ liệu thu thập được.



Hình 6. Lưu trữ thông tin của Bluezone

Lỗ hổng 2: Khả năng giả mạo người dùng thông qua đăng ký tên và địa chỉ lỏng lẻo

Muốn sử dụng ứng dụng Bluezone cần phải khai báo số điện thoại và nhận mã OTP xác thực. Sau xác thực thì nhâp tên và địa chỉ vào form tuy nhiên việc nhập này được đánh giá là hoàn toàn không có tác dụng thu thập dữ liệu vì có thể thực hiện việc này vô hạn lần mà không bị ứng dụng đưa ra thông báo cảnh cáo . . .Đặt ra vấn đề là nhập tên và địa chỉ để làm gì ? khi người dùng còn chẳng xem lại được tên và địa chỉ của mình đã khai báo. Trong khi Sim điện thoại đăng ký đã có thông tin đầy đủ về nhân thân của người sử dụng thì việc nhập form này không hề có một mục đích gì phục vụ hoạt động của ứng dụng như kiểm tra giả mạo, truy xuất địa chỉ lưu trú vì người dùng có thể nhập liệu bất kỳ thứ gì cũng cũng được ghi nhận là thành công.



Hình 7. Khai báo không chính xác thông tin cá nhân

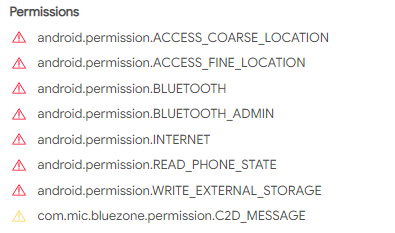
Lỗ hổng 3: Cấp quyền không cần thiết (vị trí, máy ảnh,danh bạ)

Các quyền nguy hiểm cho phép truy cập vào các thông tin cá nhân của người dùng. Hệ thống sẽ yêu cầu sự đồng ý của người dùng sau đó mới cấp quyền cho ứng dụng

Trong các quyền trên thì một số quyền được cấp nhưng không phục vụ mục đích hoạt động của ứng dụng như :

* Quyền truy cập danh bạ
* Quyền về vị trí người dùng
* Quyền truy về Camera

Trong khi quyền về vị trí người dùng trên thiết bị Android là bắt buộc khi ứng dụng khai báo sử dụng và khai thác chức năng về Bluetooth. Đối với thiết bị IOS khi sử dụng tính năng quét xác định tiếp xúc thì nó chỉ cần sử dụng CoreBluetooth nên quyền về vị trí là không cần thiết phải được cấp cho ứng dụng. Tuy nhiên ngay khi muốn sử dụng ứng dụng này hài quyền bắt buộc phải cho phép đó là Location và Bluetooth nếu không ứng dụng sẽ không hoạt động.



Hình 8. Các quyền được đánh giá nguy hiểm bởi Virus Total.

IV.Phân tích kiểm soát

1.Biện pháp hiện thời

- Tham khảo một số cách bảo vệ dữ liệu hợp lý bao gồm mã hóa và chống xâm phạm dữ liệu.

- Không cài đặt và sử dụng những chương trình độc hại để tránh việc làm giả dữ liệu

- Phát triển, nâng cấp ứng dụng để cấm các thiết bị có hệ điều hành không đảm bảo an toàn (lỗi thời) sử dụng ứng dụng tránh các phát sinh rủi ro.

- Không sử dụng các quyền nhằm thu thập thông tin cá nhân bao gồm vị trí, camera . . .

2. Biện pháp sắp tới

- Nâng cao nhận thức người dùng về phần mềm độc hại không rõ nguồn gốc. Nâng tầm cảnh báo nguy hại của các lại ứng dụng này lên mức cao nhất.

- Kiểm soát chặt chẽ mã nguồn ứng dụng tránh phát sinh rủi do vì phần mềm dựng, phầm mềm giả mạo, phần mềm chứa mã độc.

- Hạn chế những tác động kích hoạt quyền ko cần thiết của ứng dụng.

V.Xác định mức độ chắc chắn

**Lỗ hổng 1**: mức độ chắc chắn là CAO:

- Nguy cơ mất dữ liệu nếu không có cơ chế bảo vệ kĩ càng khỏi những phần mềm độc hại, phần mềm nghe trộm.

**Lỗ hổng 2**: mức độ chắc chắn là VỪA:

- Có nguy cơ vừa vì khả năng khai thác lỗ hổng là khó vì khả năng cao là hai thông tin về tên và địa chỉ còn không được đẩy về server để thu thập thông tin truy vết.

**Lỗ hổng 3**: mức độ chắc chắn CAO:

- Theo như tài liệu sách Trắng về Bluezone thì các quyền này không phục vụ cho các chức năng của ứng dụng nhưng vẫn phải cấp vì yêu cầu bắt buộc của hệ điều hành . . .Đặt ra nhiều rủi ro về thu thập thông tin cá nhân của các bên khác có thể là Google cũng có thể được hacker lợi dụng để khai thác với mục đích xấu.

VI.Phân tích tác động

**Lỗ hổng 1**: Tác động VỪA: Đa số người dùng chưa có ý thức về những phần mềm an toàn cũng như bảo vệ thông tin cá nhân trong trường hợp thông tin vị rò rỉ, bị khai thác và bị phá hoại

**Lỗ hổng 2**: Tác động CAO: trong trường hợp các thông tin được khai báo không đúng xảy ra giải mạo thì hậu quả sẽ rất nghiêm trọng.

**Lỗ hổng 3**: Tác động CAO: Quyền riêng tư cá nhân trên không gian mạng đòi hỏi những ứng dụng này cần có một cơ chế cấp quyền minh bạch và những lời giải thích rõ ràng. Nếu không sẽ gây ảnh hưởng đến tâm lý người dân cũng như ảnh hưởng đến công tác phòng dịch chung.

VII.Xác định rủi ro

Rủi ro = Tác động x Độ chắc chắn.

|  |  |  |  |
| --- | --- | --- | --- |
| Tác động Độ chắc chắn | Thấp(10) | Vừa(50) | Cao(100) |
| Cao(1.0) |  | Lỗ hổng 1 | Lỗ hổng 3 |
| Vừa(0.5) |  |  | Lỗ hổng 2 |
| Thấp(0.1) |  |  |  |

Lỗ hổng 1: Độ chắc chắn là cao nhưng tác động lại vừa, đề ra bài toán quản lý dữ liệu cho mỗi cá nhân sử dụng ứng dụng.

Lo hổng 2: Độ chắc chắn cao và tác động lớn: Đây là một vấn đềớn đối với tổ chức sản xuất ứng dụng. Đặt ra nhiều bài toán khác nhau để đối phó với các mối đe dọa

Lỗ hổng 3: Độ chắc chắn cao và tác động cao, điều này chỉ ra trách nhiệm lớn thuộc về đội ngũ phát triển. Đề ra bài toán phân quyền ứng dụng sao cho không tồn tại những nghi ngờ tác động đến dữ liệu nhạy cảm.

VIII.Khuyến nghị các biện pháp kiểm soát

Câu chuyện của truy vết sử dụng Bluetooth BLE không chỉ ở các thuật toán đảm bảo tính riêng tư, vấn đề lớn nhất đó là việc đảm bảo tính hiệu quả trong thực tế. Vấn đề dữ liệu đang đặt ra rất nhiều vấn đề

+ Những yếu tố tác động đến vấn đề an toàn của ứng dụng gồm có:

+ Người dùng.

+ Nhà phát triển ứng dụng bao gồm đội thiết kế và đội quản lý thông tin

+ Hacker đen.

Xây dựng khung pháp lý để sẵn sàng phản ứng:

Luật an ninh mạng quy định về hoạt động bảo vệ an ning quốc gia và bảo đảm trặt tự, an toàn xã hội trên không gian mạng; trách nhiện của cơ quan, tổ chức, cá nhân có liên quan. Luật chỉ ra những phạm vi mà luật bảo vệ, hành vi bị cấm, các hệ thống vật chất phần mềm; chính sách Nhà nước; Nguyên tắc bảo vê; Biện pháp bảo vệ để bám sắt vào từng khâu của quy trình phát triển ứng dụng BLUEZONE. Để từ đó quy kết trách nhiệm một cách rõ ràng và cụ thể. Tóm lại: nhấn mạnh về tấn công mạng và các giải pháp phòng chống

Luật an toàn thông tin được đưa ra để giải quyết vấn đề phát tán, rao bán thông tin cá nhân trên môi trường mạng: quy trách nhiệm về cơ quan, tổ chức, cá nhân. Đưa ra những quy định đối với các sản phẩn dịch vụ trong việc quản lý thông tin. Tóm lại: nhấn mạnh về quản lý an toàn thông tin.

Nâng cao ý thức của mỗi người để kiểm soát dữ lệu tốt, từ đó nâng cao hiệu quả của ứng dụng và xa hơn là công tác chống dịch toàn dân.

IX.Lập báo cáo kết quả

# **B. NGUYỄN HẢI ĐĂNG – B17DCAT032**

**Phân tích dựa trên NIST SP800-30**

1.Mô tả đặc trưng hệ thống

Các smartphone cài ứng dụng Bluezone có thể giao tiếp với nhau trong khoảng cách 2m, ghi nhận sự tiếp xúc gần vào lúc nào và trong bao lâu. Khi có một ca nhiễm SARS-CoV-2 mới, cơ quan y tế nhập dữ liệu F0 này lên hệ thống. Hệ thống sau đó gửi dữ liệu F0 đến các smartphone khác cài ứng dụng Bluezone. Lịch sử tiếp xúc với F0 trong 14 ngày trước đó sẽ được phân tích, đối chiếu và nếu trùng khớp, ứng dụng Bluezone sẽ cảnh báo cho người dùng có nguy cơ lây nhiễm, đồng thời hướng dẫn họ liên hệ với cơ quan Y tế để nhận trợ giúp.

Phạm vi áp dụng của Bluezone: trên các thiết bị có cài đặt ứng dụng, ứng dụng được cấp phép bởi Cục tin hóa Việt Nam và Bộ Thông tin và truyền thông.

Phạm vi phân tích là toàn bộ các phiên bản hiện có của Bluezone, nhóm sẽ tập trung đánh giá, phân tích ở một số phiên bản 3.0.6.

Sử dụng tài liệu Bluezone White Paper

Phần mền phân tích phân tích : AndroPytool

Dữ liệu & thông tin:(Bluezone thông cáo báo chí về nguyên tắc hoạt động của ứng dụng)

- **Bảo mật dữ liệu:** Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19.

- **Không thu thập vị trí:** Ứng dụng không thu thập dữ liệu về vị trí của bạn.

- **Ẩn danh:** Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm SARS-CoV-2.

- **Minh bạch:** Mã nguồn của dự án được phân phối theo giấy phép GNU GPL v3. Người dùng các nước trên Thế giới được tự do tìm hiểu hoạt động hệ thống ở mức mã nguồn, được tự do sử dụng, nghiên cứu, sửa đổi và chia sẻ.

2.Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool.

2.1.Phân tích bằng virustotal và AndroPyTool:

“permalink” : <https://www.virustotal.com/gui/file/af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c>

Mã op-code được sử dụng nhiều nhất: "invoke-virtual": 92429

Mã op-code được sử dụng ít nhất: "rem-double": 1

Tổng op-code quan sát được: 208

API được sử dụng nhiều nhất: "java.lang.StringBuilder": 17173

API được sử dụng ít nhất: "android.widget.TextView.getCompoundPaddingTop": 1 Tổng số API quan sát được: 5291

Các quyền cần thiết cho hoạt động của chương trình: android.permission.ACCESS\_FINE\_LOCATION android.permission.BLUETOOTH android.permission.BLUETOOTH\_ADMIN android.permission.INTERNET com.mic.bluezone.permission.C2D\_MESSAGE android.permission.ACCESS\_BACKGROUND\_LOCATION android.permission.ACCESS\_NETWORK\_STATE android.permission.ACCESS\_WIFI\_STATE 7 android.permission.FOREGROUND\_SERVICE android.permission.READ\_APP\_BADGE android.permission.RECEIVE\_BOOT\_COMPLETED android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZ

android.permission.REQUEST\_INSTALL\_PACKAGES android.permission.VIBRATE android.permission.WAKE\_LOCK com.anddoes.launcher.permission.UPDATE\_COUNT com.android.vending.CHECK\_LICENSE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND\_GET\_INSTALL\_R EFE RRER\_SERVICE com.htc.launcher.permission.READ\_SETTINGS com.htc.launcher.permission.UPDATE\_SHORTCUT com.huawei.android.launcher.permission.CHANGE\_BADGE com.huawei.android.launcher.permission.READ\_SETTINGS com.huawei.android.launcher.permission.WRITE\_SETTINGS com.majeur.launcher.permission.UPDATE\_BADGE com.oppo.launcher.permission.READ\_SETTINGS com.oppo.launcher.permission.WRITE\_SETTINGS com.sec.android.provider.badge.permission.READ com.sec.android.provider.badge.permission.WRITE com.sonyericsson.home.permission.BROADCAST\_BADGE 8 com.sonymobile.home.permission.PROVIDER\_INSERT\_BADG E

me.everything.badger.permission.BADGE\_COUNT\_READ me.everything.badger.permission.BADGE\_COUNT\_WRITE

Khi phân tích ta còn thu được một số thứ khác về các dịch vụ thư viện lập trình, dịch vụ liên kết với bên thứ 3 như Google, Huawei. Cơ sở dữ liệu Firebase

Những quyền càn chú ý:

+ android.permission.ACCESS\_FINE\_LOCATION

+ android.permission.BLUETOOTH

+ android.permission.BLUETOOTH\_ADMIN

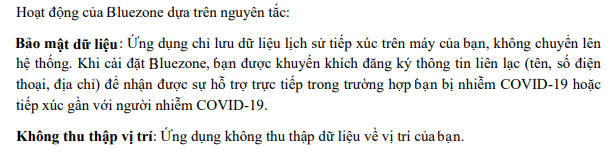
+ android.permission.INTERNET

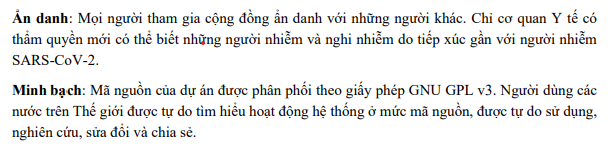
+ com.mic.bluezone.permission.C2D\_MESSAGE

1. **Xác định mối đe dọa.**

Đối với ứng dụng sẽ có rất nhiều mối nguy cơ đe dọa đến ứng dụng đó, mối đe dọa có thể nhắm đến các thông tin mà ứng dụng chứa hay các thông tin quan trọng có tính liên quan khác. Ứng dụng Bluezone không phải là ngoại lệ, ứng dụng này vẫn có rất nhiều mối đe dọa đến từ phía người dùng ứng dụng và bên phát triển ứng dụng.

- Về phía nhà phát triển ứng dụng thì ta có thể thấy sự không nhất quán giữa đội thiết kế và đội thực hiện code hay có thể nói là giữa các ban , nhóm trong việc phát triển và vận hành ứng dụng. Điều này ta có thể thấy trong tài liệu Bluezone của Bluezone White Paper:





Ở đây ta có thể thấy sự đối lập trong phát biểu của đội ngũ phát triển Bluezone khi ở bên phần “Nguyên tắc hoạt động” của Bluezone ta thấy họ phát biểu ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc ở máy của bạn, không chuyển lên hệ thống nhưng ở trong chính sách bảo mật họ lại phát biểu là cung cấp dữ liệu lịch sử tiếp xúc lên server.

Đây có thể là sự đối lập gây nên các mối đe dọa đến thông tin dữ liệu của người dùng Bluezone vì có thể vào một ngày đẹp trời họ có thể bị gửi dữ liệu tiếp xúc lên bởi một lỗi của hệ thống hay chủ đích của những người có ý định xấu.

Về phía người quản lý ứng dụng như các cơ quan ý tế hay các cơ quan có thẩm quyền thì mối đe dọa chính là việc những người quản lý sử dụng có sử dụng vào đúng mục đích mà ứng dụng được thiết kế hay không hay có thể vì một nguyên nhân nào đó có thể gây tác động đến hệ thống sửa đổi dữ liệu làm mất tính toàn vẹn hay làm lộ các thông tin khi chưa có sự cho phép ảnh hưởng tính bí mật hay việc chậm cập nhật các thông tin trên ứng dụng gây ảnh hưởng về tính sẵn dùng.

Về phía những người sử dụng ứng dụng đây cũng là đối tượng người dùng có mức độ đe dọa rất lớn khi với một số phiên bản bluezone ban đầu thì họ còn khai báo các thông tin sai lệch dẫn đến cho ứng dụng có những hoạt động sai lệch. Trong nhóm người dùng này cũng có những thành phần thích sự khám phá (nghiêm trọng có các thành phần phá phách) việc họ sử dụng ứng dụng có thể kèm theo một số các tác vụ mà nhà phát triển không mong muốn như hack,… vào ứng dụng Bluezone.

1. **Xác định lỗ hổng.**

Đối với ứng dụng Bluezone thì một vấn đề ta có thể đoán được là sự không nhất quán giữa đội code và đội thiết kế ứng dụng ta có thể gọi là “thiết kế ứng dụng một đằng và code một nẻo” đây là vấn đề rất nghiêm trọng có thể sinh ra rất nhiều lỗ hổng đối với ứng dụng Bluezone.

1. **Mối nguy mã ID Bluezone quá ngắn, dễ dẫn đến trùng mã. (Mối nguy hại xuất phát từ vấn đề của phần mềm )**
   1. **Phân tích**

Mã ID Bluezone quá ngắn, dễ dẫn đến trùng mã. Tổng số lượng mã ngẫu nhiên là ở khoảng 36^6, tức lớn hơn 2^31 một chút. Theo nghịch lý ngày sinh, chỉ cần 2^16 người đăng ký sử dụng, tức là khoảng 65 ngàn người, thì sẽ có hai người có mã ID Bluezone trùng nhau với xác suất cao. Khi đó, nếu một trong hai người bị nhiễm (phơi nhiễm), người kia cũng sẽ bị tính là nhiễm (phơi nhiễm).Vì vậy cần gia tăng độ dài của mã ID lên để cho mối nguy về việc trùng mã ID nó sẽ không còn xảy ra được.

* 1. . **Đánh giá**

Khả năng xảy ra: Thấp

Mức độ thiệt hại: Trung Bình

Đánh giá mối nguy: Thấp

1. **Mối nguy hiểm khi người dùng có khả năng bị đọc dữ liệu từ các ứng dụng khác trên di động khi Bluezone lưu dữ liệu thu thập được vào external storage. (Mối nguy hại xuất phát từ vấn đề của phần mềm)** 
   1. **Phân tích **

Vấn đề bảo mật dữ liệu rất tốt nhưng lại xảy ra nguy cơ mất an toàn mới khi Bluezone Storage Permission. Trong đó Store vẫn chạy khi thư mục Bluezone bị xóa đi, thực tế thư mục đó lưu database backup và file log txt

Trích dẫn bảo mật dữ liệu từ tài liệu Bluezone:

“ Bảo mật dữ liệu: Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19.”

Bluezone ghi xuống external storage những ID Bluezone và địa chỉ các thiết bị mà nó đã thấy. Tất cả các ứng dụng khác trên điện thoại có thể đọc được dữ liệu và qua đó có thể biết được người dùng đã gặp ai, ở đâu , vào lúc nào. Ứng dụng này có thể xóa hay ngụy tạo bằng cách nhét vào đó ID của người bệnh khiến người dùng nào bị false postitive ( không bị phơi nhiễm nhưng bị quy là có ) và false negative ( bị phơi nhiễm nhưng tưởng là không ).

* 1. **Đánh giá**

Khả năng xảy ra: Cao

Mức độ thiệt hại: Cao

Đánh giá mối nguy: Cao

1. **Lỗ hổng ở thiết bị của cơ quan y tế có chứa malware**
   1. **Phân thích**

Lỗ hổng này tồn tại khi ở các thiết bị của cơ quan y tế khi các thiết bị đã bị tấn công từ trước và có chứa các malware có khả năng tấn công kiểm soát các thiết bị, khiến cho việc cập nhật thông tin của các cơ quan y tế có sai sót dẫn đến sự hoạt động sai của Bluezone. Khi bị hoạt động sai thì sẽ khiến cho ứng dụng có thể bị nhận yêu cầu sai từ phía các cơ quan y tế dẫn đến yêu cầu gửi các thông tin của người dùng không chính xác lên server ảnh hưởng đến tính riêng tư, bí mật của người dùng.

* 1. **Đánh giá**

Khả năng xay ra: Trung bình

Mức độ thiệt hại: Cao

Đánh giá mối nguy: Cao

1. **Nhận xét**

Bluezone - ứng dụng truy vết tiếp xúc gần đã phát huy rất tốt khả năng cảnh báo sớm cho người dùng khi những người họ từng tiếp xúc bị xác định nhiễm Covid-19.

Ứng dụng Bluezone ra đời đã phát huy hiệu quả tối ưu được Việt Nam phát triển nhằm đưa cuộc sống thời đại dịch Covid-19 sớm trở lại như bình thường.

Với việc không thu thập thông tin người dùng khiến Bluezone có thêm sự tin tưởng từ người dùng và sự đánh giá tích cực từ quốc tế. Bluezone sẽ phát huy tối đa tác dụng nếu đông đảo người dùng cùng cài đặt

Tuy nhiên có mặt lợi thì bên cạnh đó ứng dụng cũng tồn tại những lỗ hổng không an toàn như khi cam kết vấn đề an toàn thông tin cá nhân đối với người dùng. Những giải pháp đưa ra để cải thiện phần mềm phần nào cỉ là mức tương đối. Nếu chung ta tin tưởng vào phần mềm và Chính phủ Việt Nam thì nên cài đặt Bluezone, số lượng người cài đặt ảnh hưởng trực tiếp tới hiệu quả của công nghệ này.

Đội phát triển Bluezone và Chính phủ Việt Nam nên đưa ra cam kết xóa bỏ dữ liệu mà máy chủ Bluezone thu thập được ngay sau khi dịch bệnh không còn nữa để đem lại sự tin tưởng đối với người dùng.

Đội phát triển Bluezone nên công bố phương án bảo vệ dữ liệu mà máy chủ thu thập được, đảm bảo chỉ người có thẩm quyền mới có thể đọc hoặc ghi dữ liệu. Đảm bảo an ninh cho máy chủ cũng là một vấn đề cần được quan tâm. Chính phủ Việt Nam nên thuê một bên thứ ba đánh giá độc lập cách làm của Bluezone.

Đội phát triển Bluezone nên cập nhật mã nguồn và whitepaper đã công bố trên GitHub cho đúng với phiên bản mới nhất. Nếu được thì cũng nên công bố mã nguồn của máy chủ. Làm vậy sẽ giúp những ai quan tâm có thể đóng góp dễ dàng hơn

1. **Tài liệu**

[Phân tích các vấn đề liên quan đến Bluezone | WhiteHat.vn](https://whitehat.vn/threads/phan-tich-cac-van-de-lien-quan-den-bluezone.13534/)

[Phần mềm chống Covid-19 của VN công khai mã nguồn, khẳng định an toàn - Vietnam ICTComm - Triển lãm quốc tế về công nghệ thông tin và truyền thông](https://ictcomm.vn/post/99-phan-mem-chong-covid-19-cua-vn-cong-khai-ma-nguon-khang-dinh-an-toan)

[Bluezone\_White\_paper.pdf](https://bluezone.gov.vn/Bluezone_White_paper.pdf)

C. NGUYỄN CÔNG CHÁNG – B17DCAT024

I. Mô tả đặc trưng của hệ thống:

Phạm vi áp dụng của Bluezone: trên toàn Đất nước Việt Nam, ứng dụng được cấp phép bởi Cục tin hóa Việt Nam và Bộ Thông tin và truyền thông.

Dựa theo tài liệu mà Bluezone White Paper cung cấp và sử dụng AndroPytool để phân tích phiên bản Bluezone 3.0.3 ta có được một số phát biểu, đánh giá, cách nhìn nhận về ứng dụng Bluezone như sau:

1. Bên phía nhà cung cấp:

Bluezone là ứng dụng sử dụng công nghệ Bluetooth năng lượng thấp, giúp bảo vệ cộng đồng trong việc phòng, chống dịch COVID-19.

Mô tả hệ thống Bluezone:

Các smartphone cài ứng dụng Bluezone có thể giao tiếp với nhau trong khoảng cách 2m, ghi nhận sự tiếp xúc gần vào lúc nào và trong bao lâu. Khi có một ca nhiễm SARS-CoV-2 mới, cơ quan y tế nhập dữ liệu F0 này lên hệ thống. Hệ thống sau đó gửi dữ liệu F0 đến các smartphone khác cài ứng dụng Bluezone. Lịch sử tiếp xúc với F0 trong 14 ngày trước đó sẽ được phân tích, đối chiếu và nếu trùng khớp, ứng dụng Bluezone sẽ cảnh báo cho người dùng có nguy cơ lây nhiễm, đồng thời hướng dẫn họ liên hệ với cơ quan Y tế để nhận trợ giúp.

Ta có sơ đồ cách thức hoạt động của Bluezone được bên phía nhà phát hành cung cấp:

      Bên nhà cung cấp còn thông báo cho truyền thông về nguyên tắc hoạt động của ứng dụng Bluezone:

**Bảo mật dữ liệu**: Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19.

**Không thu thập vị trí**: Ứng dụng không thu thập dữ liệu về vị trí của bạn.

**Ẩn danh**: Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm SARS-CoV-2.

**Minh bạch**: Mã nguồn của dự án được phân phối theo giấy phép GNU GPL v3. Người dùng các nước trên Thế giới được tự do tìm hiểu hoạt động hệ thống ở mức mã nguồn, được tự do sử dụng, nghiên cứu, sửa đổi và chia sẻ.

2. Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool:

Thông qua ứng dụng phân tích AndroPyTool ta nhận được rất nhiều thông số, dữ liệu trong đó:

Phiên bản bluezone:

Bluezone 3.0.3

Đường dẫn phân tích "permalink" của Virus total :

https://www.virustotal.com/gui/file/af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c/detection/f-af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c-1600873331

Mã op-code được sử dụng nhiều nhất: "invoke-virtual": 92429

Mã op-code được sử dụng ít nhất: "rem-double": 1

Tổng op-code quan sát được: 208

API được sử dụng nhiều nhất: "java.lang.StringBuilder": 17173

API được sử dụng ít nhất: "android.widget.TextView.getCompoundPaddingTop": 1

Tổng số API quan sát được:5291

Các quyền cần thiết cho hoạt động của chương trình:

android.permission.ACCESS\_FINE\_LOCATION

android.permission.BLUETOOTH

android.permission.BLUETOOTH\_ADMIN

android.permission.INTERNET

com.mic.bluezone.permission.C2D\_MESSAGE

android.permission.ACCESS\_BACKGROUND\_LOCATION

android.permission.ACCESS\_NETWORK\_STATE

android.permission.ACCESS\_WIFI\_STATE

android.permission.FOREGROUND\_SERVICE

android.permission.READ\_APP\_BADGE

android.permission.RECEIVE\_BOOT\_COMPLETED

android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS

android.permission.REQUEST\_INSTALL\_PACKAGES

android.permission.VIBRATE

android.permission.WAKE\_LOCK

com.anddoes.launcher.permission.UPDATE\_COUNT

com.android.vending.CHECK\_LICENSE

com.google.android.c2dm.permission.RECEIVE

com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE

com.htc.launcher.permission.READ\_SETTINGS

com.htc.launcher.permission.UPDATE\_SHORTCUT

com.huawei.android.launcher.permission.CHANGE\_BADGE

com.huawei.android.launcher.permission.READ\_SETTINGS

com.huawei.android.launcher.permission.WRITE\_SETTINGS

com.majeur.launcher.permission.UPDATE\_BADGE

com.oppo.launcher.permission.READ\_SETTINGS

com.oppo.launcher.permission.WRITE\_SETTINGS

com.sec.android.provider.badge.permission.READ

com.sec.android.provider.badge.permission.WRITE

com.sonyericsson.home.permission.BROADCAST\_BADGE

com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE

me.everything.badger.permission.BADGE\_COUNT\_READ

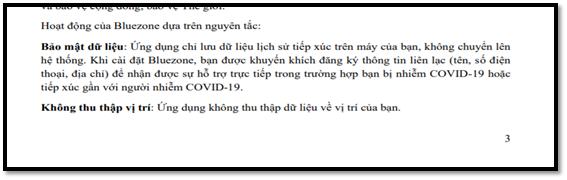
me.everything.badger.permission.BADGE\_COUNT\_WRITE

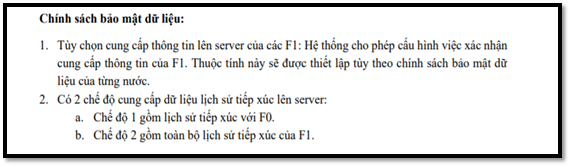
Cùng với rất nhiều các thông số khác như về các dịch vụ, thư viện lập trình, … được nhà phát hành sử dụng trong quá trình phát triển ứng dụng Bluezone. Trong đó ta thấy rất nhiều dịch vụ, thư viện,… của các bên thứ ba như google, huawei,… có thể kể đến như cơ sở dữ liệu Fire base,…

II. Xác định mối đe dọa.

Đối với  ứng dụng sẽ có rất nhiều mối nguy cơ đe dọa đến ứng dụng đó, mối đe dọa có thể nhắm đến các thông tin mà ứng dụng chứa hay các thông tin quan trọng có tính liên quan khác.Ứng dụng Bluezone không phải là ngoại lệ, ứng dụng này vẫn có rất nhiều mối đe dọa đến từ phía người dùng ứng dụng và bên phát triển ứng dụng.

1. Về phía nhà phát triển ứng dụng thì ta có thể thấy sự không nhất quán giữa đội thiết kế và đội thực hiện code hay có thể nói là giữa các ban , nhóm trong việc phát triển và vận hành ứng dụng. Điều này ta có thể thấy trong tài liệu Bluezone của Bluezone White Paper:





Ở đây ta có thể thấy sự đối lập trong phát biểu của đội ngũ phát triển Bluezone khi ở bên phần “Nguyên tắc hoạt động” của Bluezone ta thấy họ phát biểu ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc ở máy của bạn, **không chuyển lên hệ thống** nhưng ở trong chính sách bảo mật họ lại phát biểu là **cung cấp dữ liệu lịch sử tiếp xúc lên server**. Đây có thể là sự đối lập  gây nên các mối đe dọa đến thông tin dữ liệu của người dùng Bluezone vì có thể vào một ngày đẹp trời họ có thể bị gửi dữ liệu tiếp xúc lên bởi một lỗi của hệ thống hay chủ đích của những người có ý định xấu.

2.Về phía người quản lý ứng dụng như các cơ quan ý tế hay các cơ quan có thẩm quyền thì mối đe dọa chính là việc những người quản lý sử dụng có sử dụng vào đúng mục đích mà ứng dụng được thiết kế hay không hay có thể vì một nguyên nhân nào đó  có thể gây tác động đến hệ thống sửa đổi dữ liệu làm mất tính toàn vẹn hay làm lộ các thông tin khi chưa có sự cho phép ảnh hưởng tính bí mật hay việc chậm cập nhật các thông tin trên ứng dụng gây ảnh hưởng về tính sẵn dùng.

3. Về phía những người sử dụng ứng dụngđây cũng là đối tượng người dùng có mức độ đe dọa rất lớn khi với một số phiên bản bluezone ban đầu thì họ còn khai báo các thông tin sai lệch dẫn đến cho ứng dụng có những hoạt động sai lệch. Trong nhóm người dùng này cũng có những thành phần thích sự khám phá (nghiêm trọng có các thành phần phá phách) việc họ sử dụng ứng dụng có thể kèm theo một số các tác vụ mà nhà phát triển không mong muốn như hack,… vào ứng dụng Bluezone.

III.Xác định lỗ hổng:

Đối với ứng dụng Bluezone thì một vấn đề ta có thể đoán được là sự không nhất quán giữa đội code và đội thiết kế ứng dụng ta có thể gọi là “thiết kế ứng dụng một đằng và code một nẻo” đây là vấn đề rất nghiêm trọng có thể sinh ra rất nhiều lỗ hổng đối với ứng dụng Bluezone.

1. Khi chạy phần mềm AndroPyTool ta thu được các quyền mà ứng dụng Bluezone phiên bản 3.0.3 này sử dụng trong đó có một số quyền được cảnh bảo của VirusTotal:

android.permission.ACCESS\_FINE\_LOCATION

android.permission.BLUETOOTH

android.permission.BLUETOOTH\_ADMIN

android.permission.INTERNET

com.mic.bluezone.permission.C2D\_MESSAGE

Đây là những quyền nhìn thì ta có thể thấy là cần thiết cho việc xác định và truy vết của Bluezone nhưng có một số quyền như truy cập thông tin vị trí của thiết bị đây là quyền mà các bên có ý đồ xấu có thể sử dụng để biết truy cập và theo dõi lịch trình di chuyển của người sử dụng. Đây là những quyền được cảnh báo bởi Virus Total vì những quyền này có thể bị tin tặc, những bên có ý đồ xấu dựa vào đó để khai thác thông tin của người dùng.

2. Vấn đề sử dụng các thư viện hay các quyền của các bên thứ 3 cung cấp cũng có thể mang đến rất nhiều lỗ hổng hay các cửa sập “Trap door” mà các thư viện của các bên này cung cấp có thể kể đến như quyền mà bên Huawei cung cấp:

com.huawei.android.launcher.permission.CHANGE\_BADGE

com.huawei.android.launcher.permission.READ\_SETTINGS

com.huawei.android.launcher.permission.WRITE\_SETTINGS

Huawei là một công ty công nghệ của Trung Quốc đã bị Mỹ cảnh báo có những ứng dụng có chứa rất nhiều lỗ hổng có thể rò rỉ các thông tin về cho các server đặt tại Trung Quốc phục vụ cho các mục đích không minh bạch.

3. Một lỗ hổng khác từng xuất hiện trong các phiên bản cũ mà đến bây giờ vẫn còn tồn tại là vấn đề sinh ID của Bluezone. khi trong các phiên bản đầu tiên đây là vấn đề lớn khi thuật toán sinh ID dễ đoán và thiếu tính bảo mật. Còn trong các phiên bản hiện tại thì vấn đề vẫn chưa được giải quyết triệt để vì họ chỉ đơn giản là đổi từ thuật toán mã hóa này sang thuật toán mã hóa khác.

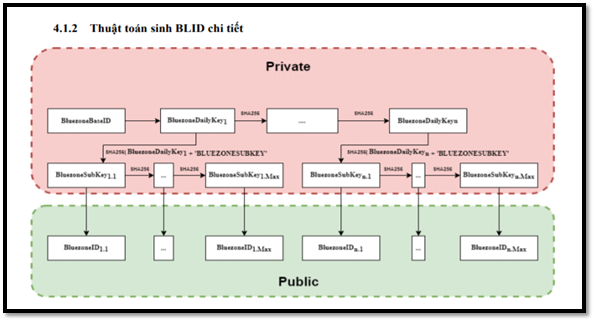
Ngoài ra bên phía nhà cung cấp đã chỉ ra cho người xem các lỗ hổng an ninh mà bên phía nhà phát triển thông báo:

4. **Nguy cơ chơi xấu.** Một lo ngại được các nhóm làm về truy vết tiếp xúc đặt ra nhưng chưa xử lý được như sau: nếu kẻ xấu thực hiện ghi nhận tất cả các Bluezone ID của tất cả các bệnh nhân đến khám tại 1 cơ sở y tế, ví dụ đặt 1 thiết bị thu tín hiệu BLE tại cơ sở này. Sau đó hắn sử dụng 1 thiết bị phát Bluetooth đặt tại nơi công cộng hoặc nơi làm việc của một đối thủ. Thiết bị phát này sẽ phát đi tín hiệu Bluezone giả mạo các Bluezone ID đã thu thập được trước đó. Nếu không may, 1 trong những Bluezone ID từ cơ sở y tế kia là F0, tất cả những người vô tình thu nhận được Bluezone ID này sẽ bị cảnh báo là F1, gây rắc rối và lo lắng cho họ.

IV. Phân tích các biện pháp kiểm soát:

Trong số các lỗ hổng của ứng dụng Bluezone thì về phía nhà cung cấp đã có những biện pháp nhằm khắc phục các lỗ hổng được phát hiện.

Lỗ hổng 3: Trong việc kiểm soát ID Bluezone thì bên phía nhà phát triển đã thay thế thuật toán sinh ID cũ bằng một thuật toán mới có mức độ bảo mật và an toàn cao hơn.



Đây có thể thấy là một thuật toán tiên tiến hơn sử dụng cơ chế sinh ID ngẫu nhiên dựa trên Hàm Băm SHA256. Những vấn đề trùng ID vẫn chưa được giải quyết.

Lỗ hổng 4: Về **Nguy cơ chơi xấu** bên phía Bluezone đưa ra giải pháp: “cho phép khi 1 Bluezone giả định có phát hiện tiếp xúc F0 (nhận được thông tin qua broadcast), Bluezone này sẽ có tùy chọn xác minh F0 mình đã tiếp xúc có đúng là F0 thật hay không, bằng cách gửi lịch sử tiếp xúc F0 của mình lên hệ thống để so sánh với lịch sử tiếp xúc của F0 đã được cơ quan Y tế cập nhật. Nếu không có sự tương đồng, Bluezone không phải là F1.” Đây có thể là cách giải quyết mà bên phía nhà phát triển Bluezone thấy hợp lý nhưng họ cũng đã đi ngược lại nguyên tắc phát triển ứng dụng mà chính họ đã nói ra: “Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, **không chuyển lên hệ thống**” Và vấn đề so khớp sẽ gặp vấn đề khi quá trình bắt và gửi ID có vấn đề như nói ở trên.

V. Xác định mức độ chắc chắn:

Với lỗ hổng 1: sử dụng các quyền vượt qua yêu cầu của ứng dụng thì mức độ chắc chắn: Thấp

Với lỗ hổng 2: sử dụng các thư viện của bên thứ 3 không được tin tưởng thì mức độ chắc chắn ở mức thấp

Lỗ hổng 3: vừa

Lỗ hổng 4: thấp

VI. Phân tích tác động:

Sự nhạy cảm và mức độ quan trọng của dữ liệu (toàn vẹn, bí mật, sẵn dùng. Các tác động tiêu cực lên uy tín của Bkav và bộ thông tin và truyền thông)

VII. Xác định rủi ro:

Rủi ro (*Rủi ro = Tác động x Độ chắc chắn*) của ứng dụng Bluezone: 100x0.5 = 50

VIII. Khuyến nghị các biện pháp kiểm soát:

Lỗ hổng 1 : Hạn chế quyền truy cập, cấp quyền vừa đủ dùng, giám sát ứng dụng

Lỗ hổng 2: Sử dụng các thư viện an toàn

D. PHẠM NGỌC KHÁNH- B17DCAT105

I. Mô tả đặc trưng của hệ thống:

Phạm vi áp dụng của Bluezone: trên toàn Đất nước Việt Nam, ứng dụng được cấp phép bởi Cục tin hóa Việt Nam và Bộ Thông tin và truyền thông.

Dựa theo tài liệu mà Bluezone White Paper cung cấp và sử dụng AndroPytool để phân tích phiên bản Bluezone 3.0.3 ta có được một số phát biểu, đánh giá, cách nhìn nhận về ứng dụng Bluezone như sau:

1. Bên phía nhà cung cấp:

Bluezone là ứng dụng sử dụng công nghệ Bluetooth năng lượng thấp, giúp bảo vệ cộng đồng trong việc phòng, chống dịch COVID-19.

Mô tả hệ thống Bluezone:

Các smartphone cài ứng dụng Bluezone có thể giao tiếp với nhau trong khoảng cách 2m, ghi nhận sự tiếp xúc gần vào lúc nào và trong bao lâu. Khi có một ca nhiễm SARS-CoV-2 mới, cơ quan y tế nhập dữ liệu F0 này lên hệ thống. Hệ thống sau đó gửi dữ liệu F0 đến các smartphone khác cài ứng dụng Bluezone. Lịch sử tiếp xúc với F0 trong 14 ngày trước đó sẽ được phân tích, đối chiếu và nếu trùng khớp, ứng dụng Bluezone sẽ cảnh báo cho người dùng có nguy cơ lây nhiễm, đồng thời hướng dẫn họ liên hệ với cơ quan Y tế để nhận trợ giúp.

Ta có sơ đồ cách thức hoạt động của Bluezone được bên phía nhà phát hành cung cấp:

Bên nhà cung cấp còn thông báo cho truyền thông về nguyên tắc hoạt động của ứng dụng Bluezone:

**Bảo mật dữ liệu**: Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19.

**Không thu thập vị trí**: Ứng dụng không thu thập dữ liệu về vị trí của bạn.

**Ẩn danh**: Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm SARS-CoV-2.

**Minh bạch**: Mã nguồn của dự án được phân phối theo giấy phép GNU GPL v3. Người dùng các nước trên Thế giới được tự do tìm hiểu hoạt động hệ thống ở mức mã nguồn, được tự do sử dụng, nghiên cứu, sửa đổi và chia sẻ.

2. Phân tích phiên bản Bluezone 3.0.3 bằng AndroPyTool:

Thông qua ứng dụng phân tích AndroPyTool ta nhận được rất nhiều thông số, dữ liệu trong đó:

Phiên bản bluezone:

Bluezone 3.0.3

Đường dẫn phân tích "permalink" của Virus total :

https://www.virustotal.com/gui/file/af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c/detection/f-af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c-1600873331

Mã op-code được sử dụng nhiều nhất: "invoke-virtual": 92429

Mã op-code được sử dụng ít nhất: "rem-double": 1

Tổng op-code quan sát được: 208

API được sử dụng nhiều nhất: "java.lang.StringBuilder": 17173

API được sử dụng ít nhất: "android.widget.TextView.getCompoundPaddingTop": 1

Tổng số API quan sát được:5291

Các quyền cần thiết cho hoạt động của chương trình:

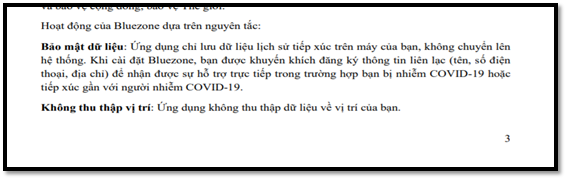
* android.permission.ACCESS\_FINE\_LOCATION
* android.permission.BLUETOOTH
* android.permission.BLUETOOTH\_ADMIN
* android.permission.INTERNET
* com.mic.bluezone.permission.C2D\_MESSAGE
* android.permission.ACCESS\_BACKGROUND\_LOCATION
* android.permission.ACCESS\_NETWORK\_STATE
* android.permission.ACCESS\_WIFI\_STATE
* android.permission.FOREGROUND\_SERVICE
* android.permission.READ\_APP\_BADGE
* android.permission.RECEIVE\_BOOT\_COMPLETED
* android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS
* android.permission.REQUEST\_INSTALL\_PACKAGES
* android.permission.VIBRATE
* android.permission.WAKE\_LOCK
* com.anddoes.launcher.permission.UPDATE\_COUNT
* com.android.vending.CHECK\_LICENSE
* com.google.android.c2dm.permission.RECEIVE
* com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE
* com.htc.launcher.permission.READ\_SETTINGS
* com.htc.launcher.permission.UPDATE\_SHORTCUT
* com.huawei.android.launcher.permission.CHANGE\_BADGE
* com.huawei.android.launcher.permission.READ\_SETTINGS
* com.huawei.android.launcher.permission.WRITE\_SETTINGS
* com.majeur.launcher.permission.UPDATE\_BADGE
* com.oppo.launcher.permission.READ\_SETTINGS
* com.oppo.launcher.permission.WRITE\_SETTINGS
* com.sec.android.provider.badge.permission.READ
* com.sec.android.provider.badge.permission.WRITE
* com.sonyericsson.home.permission.BROADCAST\_BADGE
* com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE
* me.everything.badger.permission.BADGE\_COUNT\_READ
* me.everything.badger.permission.BADGE\_COUNT\_WRITE

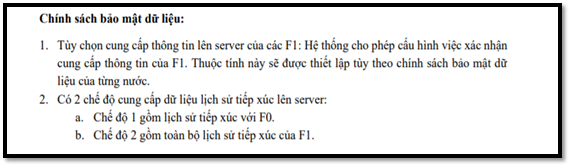
Cùng với rất nhiều các thông số khác như về các dịch vụ, thư viện lập trình, … được nhà phát hành sử dụng trong quá trình phát triển ứng dụng Bluezone. Trong đó ta thấy rất nhiều dịch vụ, thư viện,… của các bên thứ ba như google, huawei,… có thể kể đến như cơ sở dữ liệu Fire base,…

II. Xác định mối đe dọa.

Đối với ứng dụng sẽ có rất nhiều mối nguy cơ đe dọa đến ứng dụng đó, mối đe dọa có thể nhắm đến các thông tin mà ứng dụng chứa hay các thông tin quan trọng có tính liên quan khác. Ứng dụng Bluezone không phải là ngoại lệ, ứng dụng này vẫn có rất nhiều mối đe dọa đến từ phía người dùng ứng dụng và bên phát triển ứng dụng.

1. Về phía nhà phát triển ứng dụng thì ta có thể thấy sự không nhất quán giữa đội thiết kế và đội thực hiện code hay có thể nói là giữa các ban , nhóm trong việc phát triển và vận hành ứng dụng. Điều này ta có thể thấy trong tài liệu Bluezone của Bluezone White Paper:





Ở đây ta có thể thấy sự đối lập trong phát biểu của đội ngũ phát triển Bluezone khi ở bên phần “Nguyên tắc hoạt động” của Bluezone ta thấy họ phát biểu ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc ở máy của bạn, **không chuyển lên hệ thống** nhưng ở trong chính sách bảo mật họ lại phát biểu là **cung cấp dữ liệu lịch sử tiếp xúc lên server**. Đây có thể là sự đối lập gây nên các mối đe dọa đến thông tin dữ liệu của người dùng Bluezone vì có thể vào một ngày đẹp trời họ có thể bị gửi dữ liệu tiếp xúc lên bởi một lỗi của hệ thống hay chủ đích của những người có ý định xấu.

2. Về phía người quản lý ứng dụng như các cơ quan ý tế hay các cơ quan có thẩm quyền thì mối đe dọa chính là việc những người quản lý sử dụng có sử dụng vào đúng mục đích mà ứng dụng được thiết kế hay không hay có thể vì một nguyên nhân nào đó có thể gây tác động đến hệ thống sửa đổi dữ liệu làm mất tính toàn vẹn hay làm lộ các thông tin khi chưa có sự cho phép ảnh hưởng tính bí mật hay việc chậm cập nhật các thông tin trên ứng dụng gây ảnh hưởng về tính sẵn dùng.

3. Về phía những người sử dụng ứng dụngđây cũng là đối tượng người dùng có mức độ đe dọa rất lớn khi với một số phiên bản bluezone ban đầu thì họ còn khai báo các thông tin sai lệch dẫn đến cho ứng dụng có những hoạt động sai lệch. Trong nhóm người dùng này cũng có những thành phần thích sự khám phá (nghiêm trọng có các thành phần phá phách) việc họ sử dụng ứng dụng có thể kèm theo một số các tác vụ mà nhà phát triển không mong muốn như hack,… vào ứng dụng Bluezone.

III. Xác định lỗ hổng:

Đối với ứng dụng Bluezone thì một vấn đề ta có thể đoán được là sự không nhất quán giữa đội code và đội thiết kế ứng dụng ta có thể gọi là “thiết kế ứng dụng một đằng và code một nẻo” đây là vấn đề rất nghiêm trọng có thể sinh ra rất nhiều lỗ hổng đối với ứng dụng Bluezone.

**1.**Nguy cơ khai báo giả mạo.

Nếu 1 người A vì lý do nào đó cố tình khai báo mình bị nhiễm COVID-19 và gửi dữ liệu giả mạo về cho trung tâm. Các dữ liệu giả mạo này có thể gây rác và sinh ra các cảnh báo giả cho những người đã tiếp xúc với A trước đó.

2. Khi máy người dùng bị root (giải pháp: mã hóa dữ liệu, chống root/jailbreak)

Có hàng trăm ngàn ứng dụng độc hại không rõ nguồn gốc ngoài thị trường mạng nhưng không phải tất cả chúng đều có thể cài được trên Android hoặc dễ dàng xâm nhập thiết bị của bạn bởi hệ thống bảo mật của Android khá là an toàn, nhiều ứng dụng bạn phải root hoặc jailbreak máy mới có thể cài đặt được. Khi bạn root/ jailbreak đồng nghĩa với việc bỏ qua tất cả các hàng rào bảo mật cho phép các Worm , Virus, Spyware, Trojans lây nhiễm vào thiết bị của bạn. Chúng có thể tấn công các ứng dụng khác gây mất mát, đánh cắp dữ liệu. Trong trường hợp này là với thiết bị được cài đặt Bluezone.

3. Mất thiết bị cài Bluezone (giải pháp : mã hóa dữ liệu)

Khi thiết bị cài bị mất, kẻ xấu nếu đủ khả năng có thể xâm nhập vào thiết bị và có toàn quyền truy cập vào ứng dụng Bluezone. Từ đó thực hiện thay đổi dữ liệu của người dùng hợp pháp. Có thể từ việc mất thiết bị dẫn đến việc truy vết sai sót.

4.Máy điện thoại bị root/jailbreak

Thêm một vấn đề với thiết bị đã bị Root/Jailbreak, người dùng hoàn toàn có thể dùng quyền root để truy cập và chỉnh sửa dữ liệu của BlueZone bởi vì BlueZone lưu trữ tại trên thiết bị. Điều này sẽ gây ra tính không toàn vẹn của dữ liệu, dẫn đến các sai sót trong việc truy vết.

IV. Phân tích các biện pháp kiểm soát:

Trong số các lỗ hổng của ứng dụng Bluezone thì về phía nhà cung cấp đã có những biện pháp nhằm khắc phục các lỗ hổng được phát hiện.

**Lỗ hổng** 1: Về **Nguy cơ khai báo giả mạo** bên phía Bluezone: “Để giải quyết vấn đề này, các dữ liệu về F0 sẽ chỉ được cập nhật bởi cơ quan Y tế, không một ai có thể tự đưa dữ liệu của mình về trung tâm nếu cơ quan Y tế chưa xác nhận thông qua một kết quả xét nghiệm tiêu chuẩn.” Vấn đề này lại dẫn đến một mối đe dọa về đạo đức của người cập nhật dữ liệu hay có thể do một số tác động khiến bên cơ quan y tế đưa các thông tin bị sai lệch.

**Lỗ hổng 2**: Đây là lỗ hổng mà đến từ phía người dùng khi họ không hiểu rõ về thiết bị mà mình đang sử dụng hay có thể bị người khác chơi xấu dẫn đến những hệ quả xấu ảnh hưởng đến Bluezone. Đội ngũ phát triển ứng dụng đã sử dụng các thư viện an toàn sử dụng để mã hóa dữ liệu, ta có thể thấy và dự đoán khi nhìn vào các thư viện mà ứng dụng Bluezone này sử dụng thông qua quá trình phân tích AndroPyTool:

*java.security*

*java.security.cert*

**Lỗ hổng 4**:Xử lý phân tán dữ liệu tại Thiết bị đầu cuối. Trong lỗ hổng này thì ta có thể thấy Bluezone áp dụng cách xử lý giống với “lỗ hổng 10”

V. Xác định mức độ chắc chắn:

* Lỗ hổng 1: thấp
* Lỗ hổng 2: thấp
* Lỗ hổng 3: vừa
* Lỗ hổng 4: thấp

VI. Phân tích tác động:

Sự nhạy cảm và mức độ quan trọng của dữ liệu (toàn vẹn, bí mật, sẵn dùng. Các tác động tiêu cực lên uy tín của Bkav và bộ thông tin và truyền thông)

VII. Xác định rủi ro:

Rủi ro (*Rủi ro = Tác động x Độ chắc chắn*) của ứng dụng Bluezone: 100x0.5 = 50

VIII. Khuyến nghị các biện pháp kiểm soát:

**Lỗ hổng 3**: mã hóa dữ liệu

**Lỗ hổng 4**: Sử dụng thư viện phát hiện máy đã bị root/Jaibreak

IX. Lập báo cáo: