

Tiếp tục các chủ đề nghiên cứu liên quan đến thiết bị thông minh, mục tiêu lần này của nhóm IOT là sản phẩm của hãng Akuvox được triển khai với quy mô rộng trong các thành phố thông minh, tòa nhà thông minh. Quá trình đánh giá mình đã phát hiện nhiều lỗ hổng nghiêm trọng như command injection, android credential login Hardcode, certificated default webbase configure, Unauthenticate RTSP Camera. Các lỗ hổng này hoàn toàn có thể giúp attacker chiếm quyền các thiết bị, thực hiện các hành vi trái phép. Các lỗ hổng trong blog đã được report cho hãng Akuvox và đã có bản vá cho các lỗ hổng.

Về Akuvox



Thiết bị của hãng Akuvox được triển khai trong các căn hộ, tòa nhà, thành phố thông minh. Akuvox có giải pháp toàn diện cho một thành phố thông minh, hiện đang được triển khai tại nhiều nơi. Giải pháp của Akuvox gồm 2 lĩnh vực chính:

- Giải pháp cho tòa nhà (Building entrance **R29C**):

Kiểm soát truy cập vào tòa nhà, thang máy và các thiết bị trong thành phố. Ví dụ khách muốn đến chơi nhà bạn bạn không cần xuống đón, anh khách sử dụng thiết bị ở trước tòa nhà (**R29C**) đăng ký lên nhà B, sau đó anh B chấp thuận (**IT83** or **smartphone**) từ đó hệ thống mở cửa cho anh A, cấp quyền sử dụng thang máy và mở cửa căn hộ.

- Giải pháp cho căn hộ (Apartment door **R26C**):

Anh khách muốn vào căn hộ anh B sử dụng thiết bị **R26C** ngoài căn hộ bấm chuông thực hiện call video vào thiết bị được gắn trong nhà **IT83**. Anh B ở trong căn hộ hoặc từ xa xác minh danh tính anh khách qua màn hình (**IT83**) hoặc điện thoại mở cửa căn hộ cho khách hoặc người nhà.

- Ngoài ra còn một số giải pháp khác như đậu xe, SIP-base phone từ các cửa hàng, khu công cộng.

Một số lỗ hổng phát hiện được

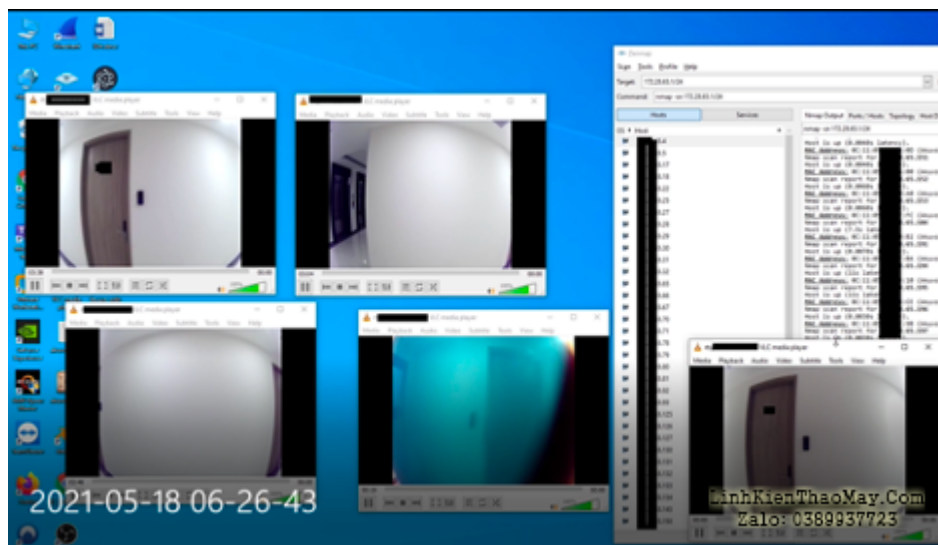
Tương tự như các giải pháp IOT khác, các thiết bị trong hệ thống thành phố thông minh được triển khai phân tán tại các node là các điểm công cộng hoặc người dùng cuối. Điều này dẫn tới rủi ro lớn cho hệ thống, đặc biệt trường hợp này các thiết bị được join chung vào cùng 1 mạng nội bộ.

Attack vector

- Hướng kiểm tra để attacker khai thác các lỗ hổng tương đối đơn giản, attacker cần thuê một căn hộ tại thành phố để tiếp cận với hệ thống mạng và thiết bị.
- Phân tích Thiết bị R315 được lắp đặt bên trong căn hộ và hệ thống mạng.
- Truy cập và thu thập thông tin hệ thống mạng toà nhà.
- Các attack surface thông qua các thiết bị : App android, Service web, Services và thực hiện khai thác các lỗ hổng.

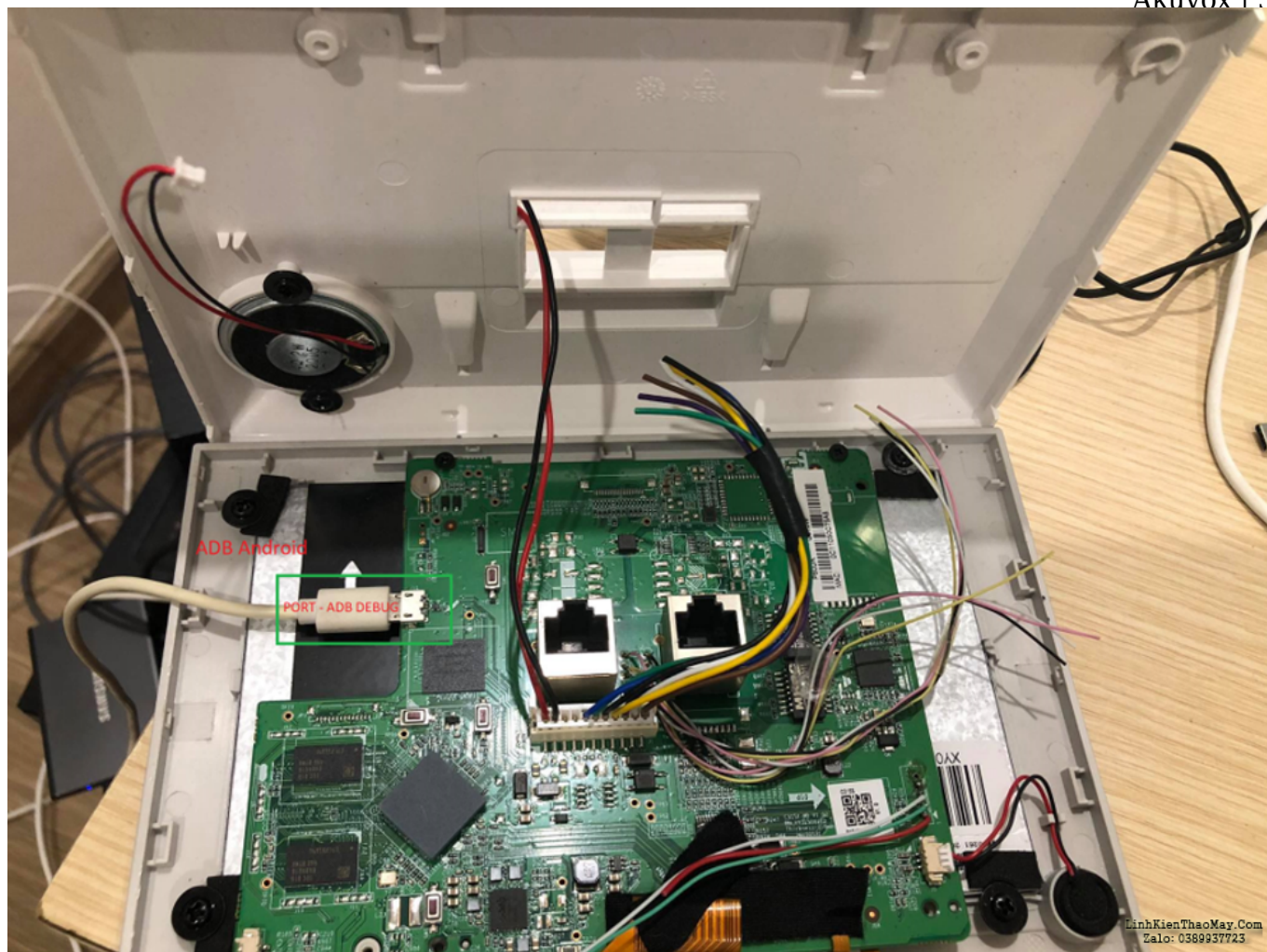
1. Truy Cập Camera tại các Hàng Lang Căn Hộ (Door bell)

Trong trường hợp giả định, quá trình triển khai thi công lắp đặt các thiết bị lỏng lẻo và các thông tin thu thập được thiết bị phía ngoài căn hộ hoàn toàn có thể dễ dàng bị thu thập thông qua scan mạng nội bộ. Điều này dẫn tới nếu không có các biện pháp xác thực như các dịch vụ RTSP. Lợi dụng lỗ hổng này, attacker có thể thực hiện streaming video thông qua giao thức mà không cần xác thực cho phép theo dõi nghe lén phía bên ngoài căn hộ.



2. Các Lỗ hổng Intercom R315C

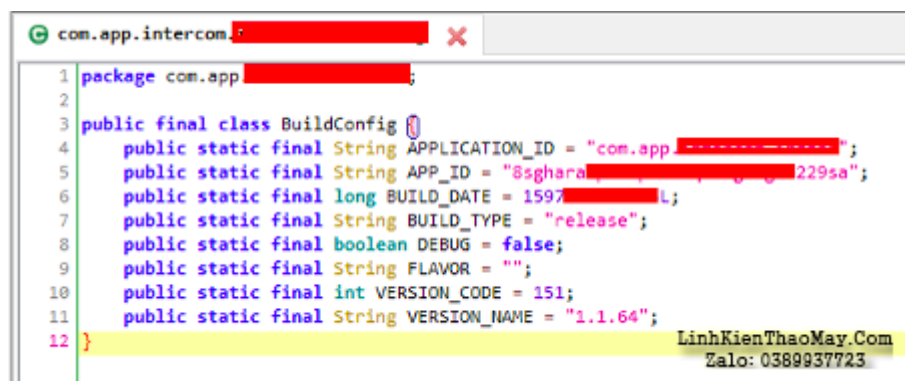
Thiết bị sử dụng hệ điều hành android cho phép attacker dễ dàng lấy được các thông tin nhạy cảm trong thiết bị.

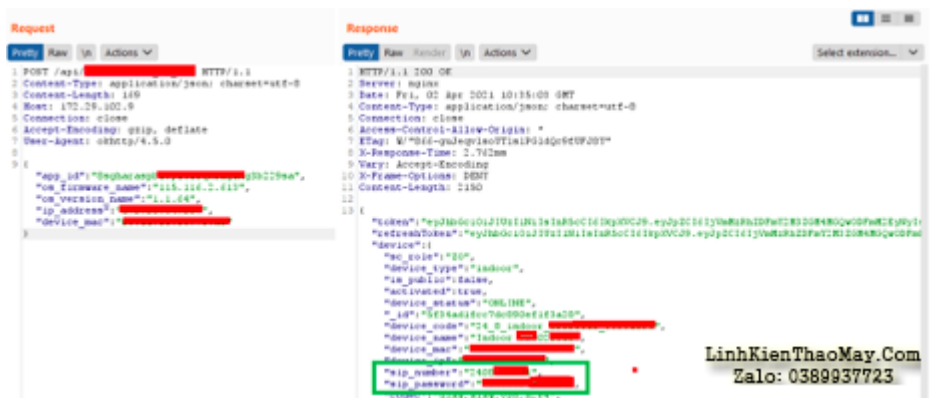


3. Truy cập thiết bị INTERCOM ở các Căn Hộ

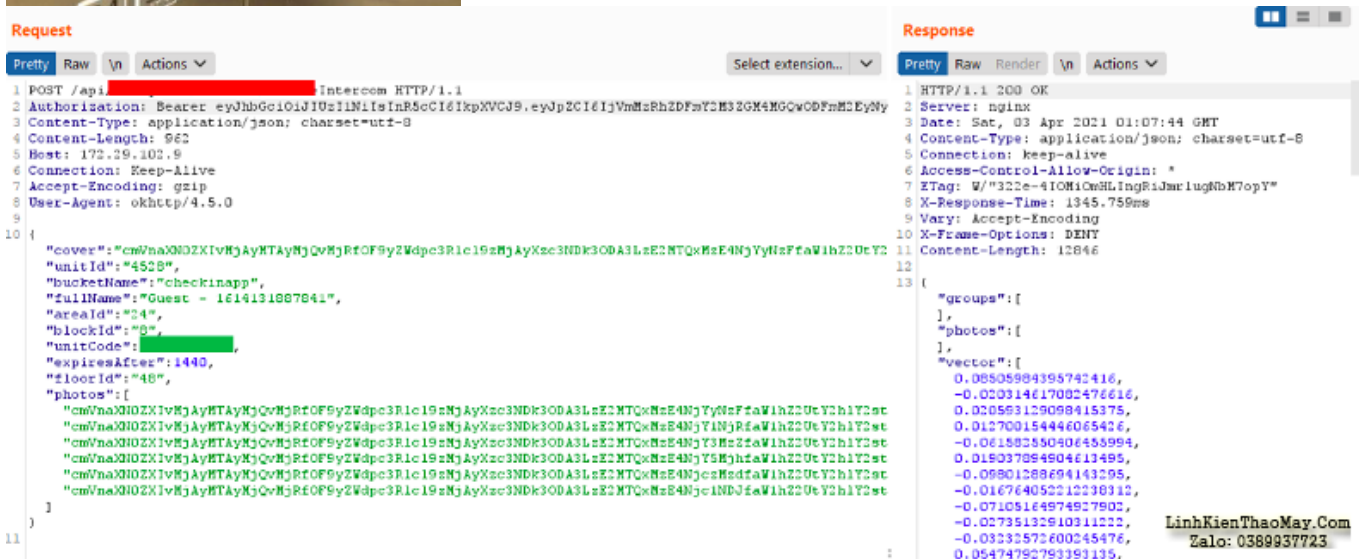
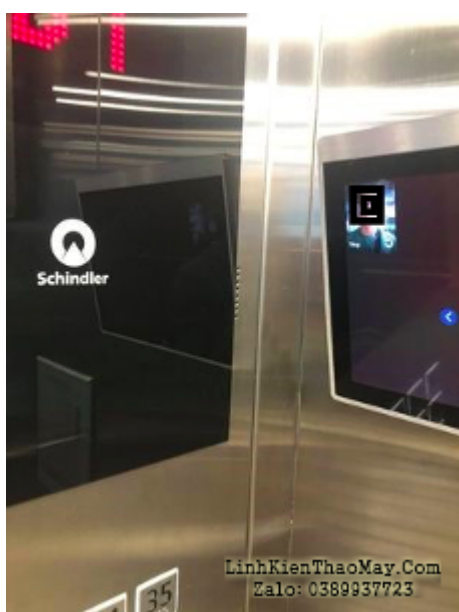
Sử dụng được các thông tin thu thập được như:

- Địa chỉ IP và địa chỉ MAC của thiết bị có được bằng cách scan các dải mạng
- Các thông tin **APP_ID** và **version firmware** có thể Reverse app *INDOOR.APK* có chứa trong thiết bị.





Để thực hiện đăng nhập hệ thống cloud và cho phép sử dụng tất cả các tính năng trên thiết bị. Trong đó có tính năng nguy hiểm như cho phép tin tặc đăng ký người các lên căn hộ bằng việc thỏa hiệp cơ chế phân tầng của thang máy và để lộ các account của các hệ thống khác.



4. Lỗ hổng Command Injection trong dịch vụ UDP

Tiếp tục thu thập thêm các thông tin các trong thiết bị. Liệt kê các các dịch vụ đang listen.

```
root@rk312x:/ # busybox netstat -pnltu
netstat: showing only processes with your user ID
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      907/lighttpd
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN      919/fcgi_server.fcgi
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      907/lighttpd
udp        0      0 0.0.0.0:50967           0.0.0.0:*               *          1913/com.akuvox.fac
udp        0      0 0.0.0.0:50492           0.0.0.0:*               *          1913/com.akuvox.fac
udp        0      0 0.0.0.0:189             0.0.0.0:*               *          2099/cfgd_server
root@rk312x:/ # pm path com.akuvox.fac
1|root@rk312x:/ #
```

Trong đó có dịch vụ cfgd_server port 189(UDP) cho phép thiết lập và lấy địa chỉ mac cho card mạng và một số tham số biến khác thông qua công cụ info_tool.

```
65     }
66   }
67   else
68   {
69     snprintf(comand, 0x200u, "info_tool set_mac_addr eth0 \"%s\" ", v8);
70   }
71   _android_log_print(4, "cfgd_server", "\nshellcmd:%s\n", comand);
72   v10 = system(comand);
73   v10 = sub_B6F99588(v10);
```

Dịch vụ cfgd_server nhận gói tin có dạng như sau:

RINS	checksum	length	SET_ENV; GET_ENV	Key Value;
				MinhKienThaoMay.Com Zalo: 0389937723

Thiết bị có chứa micro cho phép hacker tận dụng lỗ hổng tải liên thiết bị các mã độc cho phép nghe lén các hội thoại trong các căn hộ.

Demo thực hiện lệnh reboot thiết bị từ xa.

https://youtube.com/watch?v=b_FOXqPeXso%3Ffeature%3Doembed

Timeline:

04/04/2021: Thông báo các lỗ hổng và kèm PoC.

18/05/2021: thấy phải hồi đầu tiên và yêu cầu chi tiết lỗi command injection.

05/07/2021: Cập nhật tình trạng Fix bug và thông báo công bố lỗ hổng.

TRUNG TÂM SỬA CHỮA ĐIỆN TỬ QUẢNG BÌNH

MR. XÔ - 0901.679.359 - 80 Võ Thị Sáu, Phường Quảng Thuận, tx Ba Đồn, tỉnh Quảng Bình

GIÁ RẺ

NHANH CHÓNG

LINH KIỆN CHÍNH HÃNG

SANYO ELEC MSUNG
Panasonic TOSHIBA BISHI



TRUNG TÂM SỬA CHỮA ĐIỆN TỬ XÔ NGUYỄN

- Dịch vụ sửa chữa điện tử tại nhà
- Cung cấp linh kiện điện tử
- Tư vấn lắp đặt nhà thông minh

Đc: Quảng Thuận, tx Ba Đồn,
tỉnh Quảng Bình - 0901.679.359

22/07/2021: Nhận phản hồi đã fix các lỗi đã thông báo.

Tác giả: Hà Toàn

Các bài viết tương tự:

- [cần giúp đỡ âm ly 8 sò 2 ngày vẫn chưa tìm ra bệnh áp đối xứng +17vol qua 2 ổn áp 7912 7812 cấp cho rơ le mạch music master mic,,+52 cho công suất - ban đầu hỏng công suất chết câu chì,,thay thế và kiểm tra các điện áp chân b công suất =nhau 52 vol,các tầng khuếch đại thúc, đệm, trở tụ tốt,\(bo nguồn ,ổn áp và công suất đi liền\),,,tháo đường 52 vol thì rơ le lại đóng cấp vào lại ko đóng ,bỏ 1 câu chì 1 về lại đóng\(về đã bị nổ câu chì lúc đầu\),,,,kiểm tra ko thấy bị sao? 2 trở cân bằng về rơ le bảo vệ loa em đo 1 đường về 52vol còn 1 đường vài mili vol,,,ko hiểu là sao lại chênh lệch thế,,,](#)
- [chao cac ban. - dan am thanh KENWOOD rat mong cac ban gop y giúp mình chuyên la the nay minh moi nhan dc cua khách nho sua chua cho dan am thanh kenwood chay radio va doc dia CD nhungmay khách mang toi trong tình trạng chapphan cong suat .DIA va RADIO van hoat dong binh thuong nhung bi chap CONG SUAT nen kep loa vao dinh u neu de lau loa se bi chay .hien gio minh van chua dam lam gi ca moikiem tra so bo thi thay chay con STK4150 minh nhìn ma da thay chuoiroi vi hang xach tay ma lai thay con STK4150 minh chua thay gap con nay bao gio vi vay nho cac ban gop y va giúp mình xem tren thi truong co con nay khong vay?tro gioi lieu co ko cac ban nhi?ban nao da tung lam qua ban nay xin giúp do minh mot tay.thank cac ban nhieu.](#)
- [DAU DVD ARIRANG AR-36K - lúc đầu máy đã qua 1tay thợ không sửa được khách mang đến thấy cơ bị vỡ và tháo mất khách bảo ngta bảo hư cơ mình bật nên không thấy hiện tượng gì mình đã tách kiểm tra nguồn ok và nạp lại ROM máy đã hiển thị và load các phím bị liệt mình đã hàn lại ic mặt đã chạy an phím có tác dụng. Nhưng giờ cho đĩa vào mắt có sáng và moto quay đĩa chỉ nhích nhẹ một cái rồi thôi . Mình đã kiểm tra nguồn 3.3v và các nguồn đầy đủ](#)
- [Main PC-g31 b - Mong tất cả các đồng nghiệp giúp đỡ mình.hiện em nó khởi động không lên màn hình.led báo cây đang hoạt động kg sáng.quạt cpu vẫn quay.cpu và chip bắc,nam vẫn nóng.ram bình thường.các bạn cho mình hướng để sửa chữa em nó](#)

nhé.cây này của mình.nên mình muốn tự sửa và đi sâu vào main.mình chuyên tivi.

5. máy giặt sanyo (aqua) ASW 80VT - Máy bấm nút nguồn không lên . mình đã kiểm tra nút ấn vẫn tốt nguồn 5v vẫn có. mình đã thay thạch anh chạy ok được khoảng 3 ngày . nay nó lại bị lại mặc dù mình đã thay lạ thạch anh và mình kiểm tra 2 chân thạch anh 4M 1 chân là 5v chân còn lại là gân 1V . mình đang tập tẹ tự học sửa bo mạch mong anh em giúp đỡ
6. máy lạnh daikin,samsung,lg.... - mình vệ sinh đầu lạnh có cần giữ cánh quạt lại không các bạn. khi mình đi học thầy kiu không cần giữ. mà giờ đi làm người ta kiu giữ không giữ sẽ bị cháy. ai có kinh nghiệm chỉ mình với. mình không dám thử lửa cháy thiệt chắc hư
7. Thử chiếm quyền điều khiển các thiết bị SmartHome Lumi
8. Tivi LG model 21FU6LR - Chạy ic màn hình STV 9326, nửa màn hình dưới bình thường, trên giữa màn hình có vết sáng hơn và hình bị gấp, phía trên thì hình bị dẫn, kiểm tra nguồn 26v đủ, đường ra chân số 5 cao 22v, thay ic màn hình và các tụ hóa nhưng vẫn chưa ra bệnh
9. toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhưng khong ket noi dc voi may in va may tinh khong tim dc thiet bi - toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhưng khong ket noi dc voi may in va may tinh khong tim dc thiet bi
10. tủ lạnh Daewoo 160L - - ngăn trên làm đá bình thường . quạt chạy , đường gió xuống ngăn mát thông không bị tắc,đã để chắn gió xuống ngăn bảo quản lbes nhất .đã tháo kiểm tra đường hút gió xuống ngăn bảo quản không bị chắn hoặc tắc . vậy mà không có gió lạnh xuống , quạt thổi ra nói chung là tất cả các điều kiện ddeuf tốt vậy mà ngăn mát không lạnh gì
11. tủ lạnh đông tuyết. (tủ bảo ôn) - bực giàn. hết ga, mình đã lén giàn nóng riêng. và đã biết giàn nóng bị thủng. giờ mình muốn kiểm tra nguyên giàn lạnh xem có bị thủng ko mà mình ko nghĩ ra cách nào. vì mình mới vào nghề chưa am hiểu và chưa có kinh nghiệm j cả. vì cos một thợ trước đến nhà khách kiểm tra cái tủ này. ong thợ kia phán với chủ nhà là thủng giàn lạnh. giờ mình mới kiểm tra đc mỗi giàn nóng.
12. tu lanh_ sanyo - tu cua minh dong tiet wa trui` minh da thai cam~ bien am.cau tri` nhiet wa` dien tro nhiet khong bi dut.minh dakiem tra dong ho thoi gian con rat tot.minh k pit no bi j nua~ ai bet thi chi cho minh voi