HỆ THỐNG BẢO MẬT CỦA GIẢI PHÁP EASYCONTROL

Bước 1: Xác Thực tài khoản

Tài khoản được chia làm 2 cấp: Tài khoản sở hữu (master) và tài khoản điều khiển (user). Khách hàng sở hữu tài khoản Master có quyền chỉnh sửa, thay đổi hoặc xóa bỏ tài khoản user. Thông số đăng nhập trên phần mềm gồm: Tên tài khoản Master, tên user và mật khẩu user. (Không nhập mật khẩu master). Việc không yêu cầu nhập mật khẩu master trên phần mềm giúp gia tăng tính bảo mật cho mật khẩu master, nếu thiết bị smartphone nhiễm virus theo dõi cũng không thể theo dõi được mật khẩu master.

Tại trang login của phầm mềm Esmart, thiết bị smartphone kết nối với Data center để xác thực thông số đăng nhập. Nếu thông số đăng nhập đúng thì hệ thống Data Center sẽ trả về phầm mềm Esmart 1 key xác thực để Emsart chuyển sang đăng nhập vào hệ thống cloud, Dater Center cũng đồng thời gửi 1 Key báo sang hệ thống Cloud

Bước 2: Esmart kết nối với Cloud

- Esmart sử dụng Key được trả về của Data Center và chuyển kết nối đến Cloud. Kết nối Cloud được thiết kế trên Port riêng (không sử dụng Port 8080).

- Sau khi Esmart kết nối đến Cloud, hệ thống Cloud sẽ lần lượt gửi 3 yêu cầu để xác thực và Esmart phải trả về đúng 3 định dạng bảo mật: Gói 1: Nhận dạng sản phẩm ACIS, Gói 2: Nhận dạng thông tin người dùng, Gói 3: Nhận dạng MCE muốn kết nối.

- Sau khi xác nhận yêu cầu kết nối của Esmart, Hệ thống Cloud sẽ gửi về 1 Key sử dụng để đăng nhập vào room đồng thời khởi tạo 1 Room với ID key kết nối với MCE.

Bước 3: Giao tiếp với Room

Toàn bộ dữ liệu giao tiếp qua lại trong room: bao gồm dữ liệu điều khiển gửi từ Esmart xuống và dữ liệu phản hồi trạng thái thiết bị từ MCE về đều được mã hóa theo Form riêng của ACIS. Căn cứ vào thuật toán đã lập trình cứng trong thiết bị cũng như phần mềm, chỉ có phần mềm ACIS mới có thể giải mã và hiểu được form này.

Bước 4: Room giao tiếp với MCE

- MCE được thiết lập cứng giao tiếp “Điểm-Điểm” chỉ lắng nghe và giao tiếp với 1 IP duy nhất của hệ thống ACIS và không thể nhận cũng như không xử lý dữ liệu từ bất kỳ nguồn nào có IP khác.

- MCE được lập trình định kỳ 10 phút 1 lần gửi thông số key Random về hệ thống cloud để xác thực tình trạng kết nối cũng như thông báo về trạng thái thiết bị.

- Các dữ liệu MCE giao tiếp lên và trả về từ cloud đều theo form mã hóa riêng của ACIS. Trường hợp sai form truyền thì hệ thống cloud tự động kích out room và tái lập quy trình login từ đầu.

Bước 5: Giao tiếp không dây từ MCE đến các Device

- Trong thao tác Link phần cứng (khởi tạo kết nối từ MCE đến Device), MCE đã thực hiện 1 bước quan trọng là cung cấp Key giao tiếp cho các device. Các Device trong quá trình hoạt động truyền tín hiệu sau này đều sử dụng Key này trong form truyền để MCE có thể nhận dạng được device trong hệ thống của mình.

- Phần cứng giao tiếp sử dụng công nghệ RF- FSK với mã hóa 64 bit phân giải tầng số. Cho nên ngay cả sử dụng phần cứng giống ACIS cũng không thể bắt được dữ liệu truyền.

- Dữ liệu giao tiếp giữa MCE và device sử dụng công nghệ mã hóa AES hai chiều với việc đồng bộ và phát sinh key random liên tục từ hệ thống cho nên ngay cả nhân viên kỹ thuật ACIS dù có nhận dạng được dữ liệu truyền thì cũng không thể tương tác vào hệ thống.