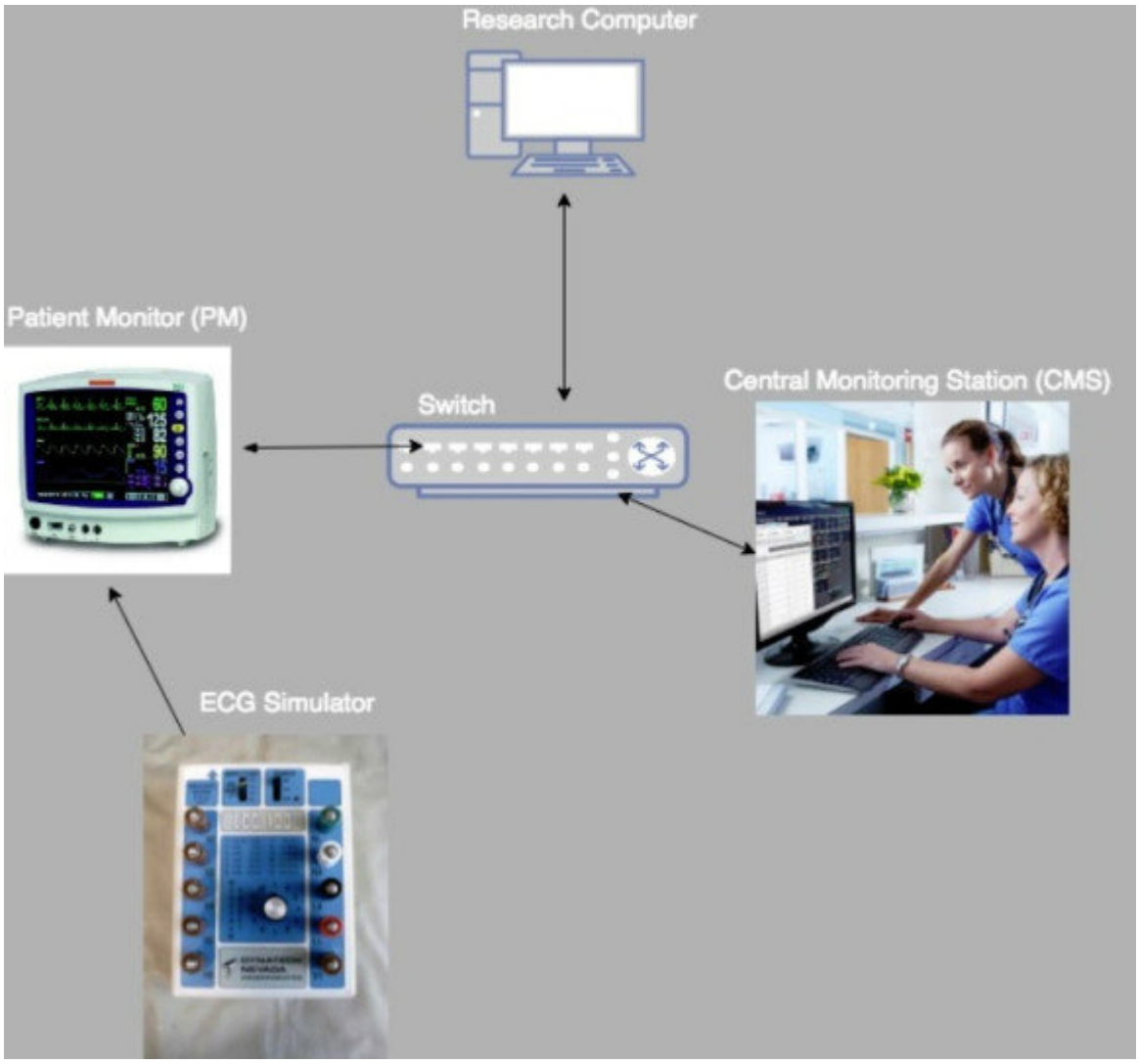
نفوذ به دستگاه های پایش علائم حیاتی بیمار، تهدید امنیتی جدید بیمارستان ها - دیجیاتو

علی باقرزاده | یکشنبه، ۲۱ مرداد ۱۳۹۷

در دفکان که یکی از بزرگترین رویدادهای گردهمایی هکرها در آمریکا است، محققان شرکت امنیتی مک آفی روشی برای هک سیستم های پایش علائم حیاتی بیمار را به نمایش گذاشته اند.

دستگاه های پایش علائم حیاتی بیماری امکان مشاهده اطلاعاتی از جمله ضربان قلب بیماران را در مراکز پرستاری بیمارستان فراهم می کنند. این دستگاه ها به طور معمول از حداقل دو بخش اصلی تشکیل شده اند: یکی از آنها در کنار بیمار قرار دارد و دارای حسگرهای مختلف است، قسمت دیگر ایستگاه مرکزی است که در مرکز پرستاری نصب می شود.

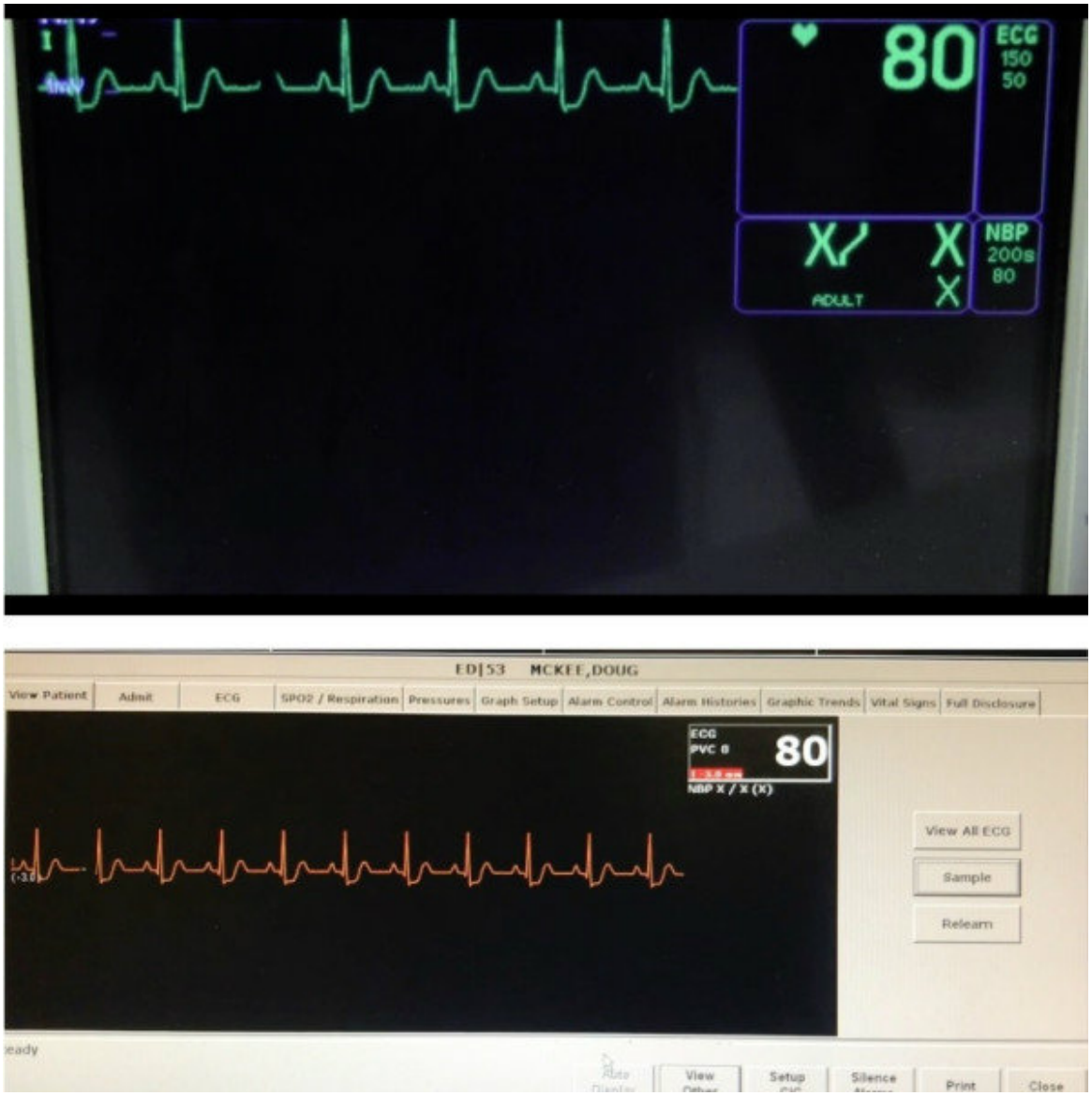
اطلاعات مرتبط با علائم بیماران از طریق شبکه و به واسطه پروتکل های نامعمول به ایستگاه مرکزی انتقال پیدا می کند. در صورتی که تغییر بحرانی در شرایط بیمار پیش آید، ایستگاه مرکزی به پرستاران هشدار می دهد.



این موضوع که هکرها موفق به یافتن روشی برای نفوذ به سیستم هایی که با جان انسان ها در ارتباط است شده اند ترسناک به نظر می رسد. به گفته «داگلاس مک کی»، محقق مک آفی، پروتکل شبکه ای که در این دستگاه ها به کار می رود RWHAT نام دارد و توسط بیشتر سیستم های بیمارستانی مورد استفاده قرار می گیرد. همین موضوع موجب نگرانی بیشتر شده است.

محققان موفق شده اند اطلاعات حیاتی که در لحظه ارسال می شوند را دستکاری کرده و آنها را با اطلاعات غلط جایگزین کنند. هکرها توانسته اند برای مدت 5 ثانیه میزان ضربان قلب را از 80 بار در دقیقه به صفر برسانند. البته باید اشاره کرد که هدف این هکرها هشدارهایی برای بهبود امنیت چنین دستگاه هایی بوده است.

به گفته مک کی فقدان هویت سنجی موجب می شود دستگاه های مخرب در میانه راه قرار گرفته و اطلاعات پایش علائم حیاتی بیمار را شبیه سازی کنند. در این صورت در حالی که ممکن است پرستار به اشتباه تصور کند که شرایط بیمار طبیعی است، ولی بیمار در شرایط ایست قلبی باشد.



اطلاعات نمایش داده شده در دستگاه سمت بیمار (تصویر بالا)، در کنار اطلاعات نمایش داده شده در بخش پرستاری (تصویر پایین)

در آزمایش انجام شده تعدادی دستگاه خریداری شد که به ویندوز XP مجهز بودند. برخی از این دستگاه های قدیمی همچنان در بسیاری از مراکز درمانی در حال استفاده هستند. نرم افزارهای قدیمی این دستگاه ها از چندین آسیب پذیری رنج می برند، البته گفته شده که به فرم ویرهای دستگاه های پایش به سختی می توان نفوذ کرد.

به گفته محققان امنیتی با استفاده از ابزار پایش شبکه وایرشراک اطلاعات بیماران به صورت متن ساده دریافت شده است. به عبارتی این اطلاعات به هیچ وجه رمزنگاری نشده بودند. پس از این مرحله و در بررسی فرایند دست دهی محققان موفق شدند اطلاعات تقلبی را برای ایستگاه مرکزی نمایش دهنده اطلاعات ارسال کنند.

به گفته مک کی تولید کنندگان دستگاه ها می توانند با رمزنگاری داده های رد و بدل شده در شبکه بین دستگاه ها و نیز افزودن فرایندهای هویت سنجی، فرایند حمله به این دستگاه ها را به

شدت مشکل تر کنند.

[دیجیاتو]