

Đứng ngoài cửa nhà cũng đánh cắp được tài khoản ngân hàng của người ngồi bên trong: Kẻ gian làm kiểu gì?

20:25 31/07/2024

Tác giả: Đang cập nhật

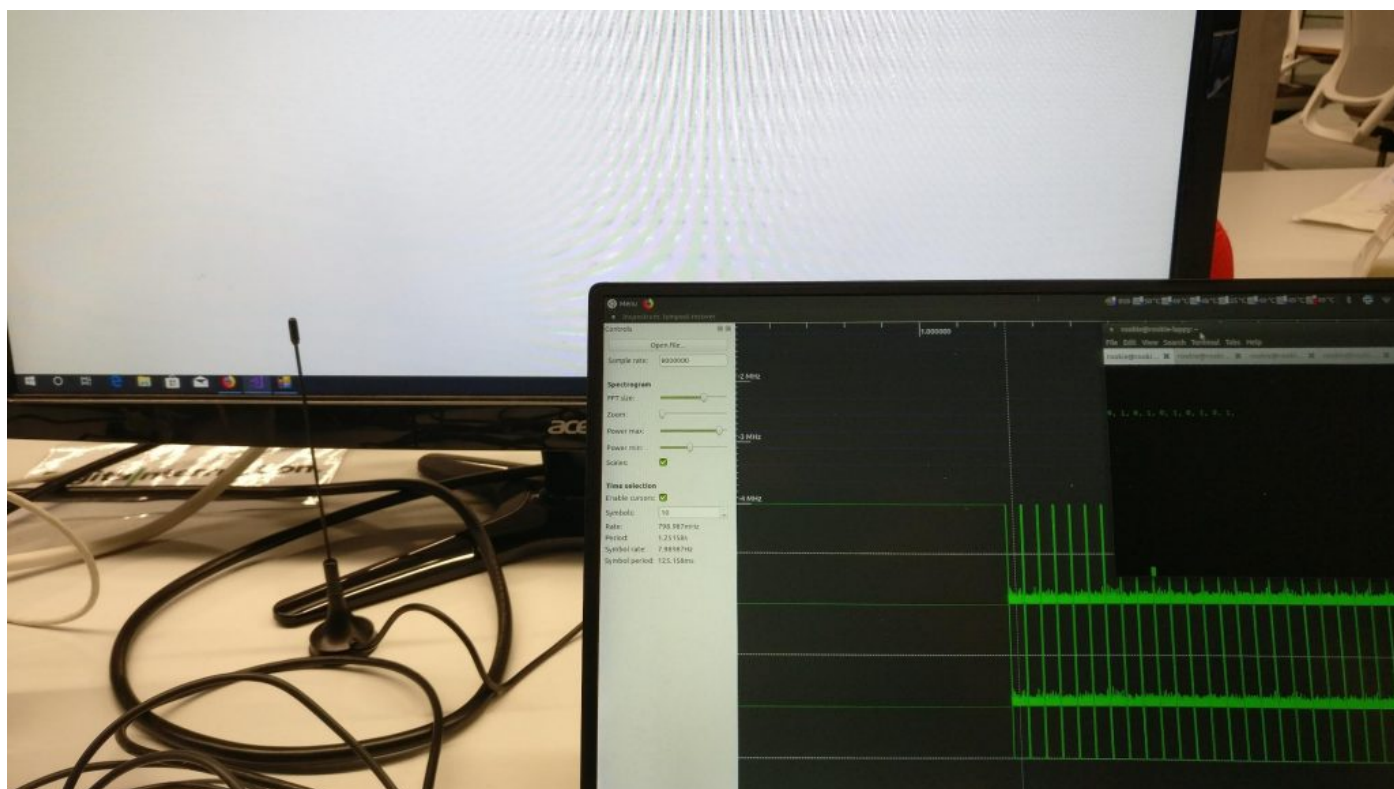
AI có khả năng xem trộm toàn bộ những gì màn hình bạn hiển thị bằng cách sử dụng tín hiệu rò rỉ từ cáp HDMI.

Các nhà nghiên cứu tại Uruguay đã lật tẩy cách hacker sử dụng trí tuệ nhân tạo (AI) để theo dõi những gì hiển thị trên màn hình của bạn bằng cách sử dụng tia bức xạ điện từ rò rỉ từ cáp kết nối giữa màn hình và máy tính. Nhưng người dùng máy tính tại nhà không cần quá lo lắng. Các cuộc tấn công có thể được thực hiện bằng nhiều phương pháp, bao gồm sử dụng ăng-ten đặt bên ngoài tòa nhà để hứng tín hiệu từ cáp HDMI. Ở thời điểm hiện tại khi công nghệ truyền video kỹ thuật số phức tạp thì vẫn luôn có lỗ hổng để hacker có thể khai thác.

Theo Federico Larroca tại Đại học Cộng hòa Uruguay, anh và đội ngũ của mình đã phát triển một mô hình AI có thể tái tạo tín hiệu số từ tín hiệu rò rỉ cách xa vài mét.

Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) và NATO gọi những cuộc tấn công này là các cuộc tấn công TEMPEST. Tiêu chuẩn TEMPEST tại NSA yêu cầu các biện pháp bảo vệ để ngăn chặn bức xạ điện từ mà hacker có thể lấy cắp và giải mã.

Sử dụng phương pháp tương tự như Larroca và đội ngũ của anh đã phát triển, hacker có thể theo dõi màn hình khi người dùng nhập tin nhắn mã hóa, đăng nhập ngân hàng hoặc nhập thông tin cá nhân khác. Đội ngũ cho biết hacker có thể lấy được tín hiệu ngay cả khi đứng bên ngoài tòa nhà chỉ bằng ăng-ten. Họ cũng có thể cài đặt một thiết bị nhỏ để thu tín hiệu và hoặc truyền dữ liệu hoặc ai đó thu lại dữ liệu đó theo cách thủ công.



Các nhà nghiên cứu đã huấn luyện mô hình AI bằng cách sử dụng một tập hợp tín hiệu gốc và tín hiệu thu lại khớp nhau. Sau đó, họ sử dụng phần mềm nhận dạng văn bản trên hình ảnh thu hồi và so sánh nó với hình ảnh màn hình gốc. Trong quá trình thử nghiệm, quá trình thu lén đã giải mã sai khoảng 30% ký tự. Đội ngũ cho biết tỷ lệ lỗi này đủ thấp để con người vẫn có thể đọc chính xác hầu hết văn bản.

Điều đáng lo ngại là tỷ lệ thành công của các cuộc tấn công này ngày càng cao. Phương pháp tấn công trước đây có tỷ lệ lỗi cao hơn khoảng 60% so với phương pháp mà đội ngũ của Larroca đã phát triển. Một điểm sáng là Larroca đánh giá rằng người dùng máy tính gia đình hoặc doanh nghiệp nhỏ không cần lo lắng về việc này.

Larroca tin rằng các cuộc tấn công như vậy đã diễn ra nhưng chỉ trong môi trường công nghiệp hoặc chính phủ có độ nhạy cảm cao. Trong những trường hợp này, toàn bộ tòa nhà thường được che chắn khỏi tín hiệu điện từ để ngăn chặn các vi phạm an ninh như vậy.

Link bài viết: <http://www.tinthat.vn/dung-ngoai-cua-nha-cung-danh-cap-duoc-tai-khoan-ngan-hang-cua-nguoi-ngoai-ben-trong-ke-gian-lam-kieu-gi>