ANH: HỘ CHIẾU ĐIỆN TỬ BỊ PHÁ MÃ

Một ch

Một chuyên gia bảo mật vừa phá mã thành công một trong những loại hộ chiếu sinh trắc mới của Anh mà trước đó chính phủ nước này hy vọng sẽ giúp giảm được nạn tội phạm biên giới và tình trạng nhập cư trái phép.

Phương thức tấn công trên chỉ sử dụng bộ đọc RFID thông dụng và các mã cá nhân hoá để lấy dữ liệu ra khỏi con chip RFID từ một chiếc hộ chiếu được bọc trong phong bì kín - tiết lộ của Adam Laurie, chuyên gia tư vấn về bảo mật RFID và Bluetooth. Với kiểu tấn công này, người mang hộ chiếu không hề biết thông tin của mình đã bị đánh cắp.

Cách đây một năm, chính phủ Anh quốc đã bắt đầu ban hành loại hộ chiếu điện tử RFID, kết hợp với dấu vân tay và dữ liệu sinh trắc trên chip cho dù có nhiều lo ngại về cách thức lưu trữ và xử lý những dạng dữ liệu này. Con chip RFID này chứa nhiều thông tin cá nhân của ngời mang hộ chiếu, kể cả ảnh, và công nghệ bảo mật nhằm phát hiện những thay đổi trái phép.

Laurie cho biết cuộc tấn công trên được thực hiện đối với chiếc hộ chiếu vẫn còn nằm trong phong bì gốc khi nó được chuyển đi từ bộ phận cấp hộ chiếu. Laurie đã đặt thiết bị đọc dữ liệu gần hộ chiếu để lấy thông tin từ con chip RFID bên trong.

Cũng theo Laurie, dữ liệu trên chip của hộ chiếu bị khoá cho tới khi bộ đọc RFID cung cấp khoá mã hoá. Khoá mã hoã được tính toán trên cơ sở kết hợp giữa dữ liệu cá nhân của người mang hộ chiếu (chẳng hạn như ngày sinh) với một vùng gọi là MZR (machine-readable zone) bao gồm chuỗi ký tự và con số được in ở cuối trang đầu tiên của hộ chiếu.

Để quét con chip RFID, Laurie đã sử dụng thiết bị đọc RFID của hãng ACG ID. Những dữ liệu thu được cho phép Laurie tạo ra một bản copy chính xác của hộ chiếu.