CÁC CUỘC GỌI DI ĐỘNG CÓ THỂ KHÔNG CÒN RIÊNG TƯ

Một nhà khoa học máy tính người Đức đã cho công bố các chi tiết về việc phá đoạn mã bí mật được dùng để bảo vệ các cuộc đàm thoại của hơn 4 tỷ người sử dụng điện thoại di động.

Karsten Nohl cùng với các chuyên gia khác, đã d&agra

Một nhà khoa học máy tính người Đức đã cho công bố các chi tiết về việc phá đoạn mã bí mật được dùng để bảo vệ các cuộc đàm thoại của hơn 4 tỷ người sử dụng điện thoại di động.

Karsten Nohl cùng với các chuyên gia khác, đã dành ra 5 tháng để tìm cách phá vỡ thuật toán được sử dụng để mã hóa các cuộc gọi sử dụng công nghệ GSM, chuẩn phổ biến nhất cho các mạng điện thoại di động trên khắp thế giới.

Nohl phát biểu tại một hội thảo về truyền thông ở Berlin rằng công trình của ông cho thấy tính an toàn của GSM còn nhiều thiếu sót.

Ông cho biết: "Chúng tôi đang cố gắng để cảnh báo cho mọi người điểm yếu phổ biến này. Cùng với những đòi hỏi từ phía người tiêu dùng, chúng tôi hy vọng cũng tạo ra được một vài sức ép để việc mã hóa được tốt hơn".

Hiệp hội GSM (GSMA) nơi tạo ra thuật toán và giám sát sự phát triển của tiêu chuẩn này cho rằng công trình của Nohl mang tính bất hợp pháp cao ở Anh và nhiều quốc gia khác.

Nhưng Nohl cho rằng ông đã tham khảo ý kiến các luật sự trước khi công bố và tin rằng công trình này là hợp pháp.

Mã hóa GSM lần đầu tiên được giới thiệu vào năm 1987 và đã trở thành công cụ chính để mã hóa các cuộc đàm thoại di động.

30.000 USD có thể nghe lén mọi cuộc đàm thoại di động

Karsten Nohl cùng với vài chục người khác tuyên bố tài liệu do họ công bố sẽ phá vỡ thuật toán A5/1, một đoạn mã 22 năm tuổi được nhiều nhà sản xuất sử dụng. Vào năm 1994 một loạt các

điểm yếu của hệ thống này từng được công bố.

Karsten Nohl, người tự nhận là một "nhà nghiên cứu bảo mật trước các cuộc tấn công" cũng từng công bố ý định sẽ phá vỡ đoạn mã tại hội nghị Hacking at Random (HAR) tại Hà Lan vào tháng 8/2009.

Ông cho biết: "Bất kỳ chức năng mật mã nào cũng là một chìa khóa để mở. Bạn không thể giải mã nếu không có khóa bí mật". Để làm được điều này, Nohl cùng các cộng sự sử dụng mạng máy tính để phá mã qua "mọi đầu mối" mà họ có được về đầu vào và đầu ra của đoạn mã.

Tất cả các đầu mối được liệt ra trong một bảng kê mà theo mô tả của Nohl: "Nó giống như một danh bạ điện thoại, nếu một ai đó nói cho bạn một cái tên, bạn có thể tra bảng ra số của họ".

Ông cho biết chỉ cần sử dụng cẩm nang mã này cùng một máy tính khỏe và một thiết bị vô tuyến trị giá 30.000 USD sẽ cho phép bất kỳ ai giải mã các tín hiệu từ hàng tỷ người sử dụng GSM trên thế giới.

Bất kỳ ai, bao gồm cả bọn tội phạm cũng chỉ cần 30.000 USD để hóa giải thuật toán A5/1.

GSM không còn an toàn

Nhiều chuyên gia cho biết, trước đây đã có thể giải mã các tín hiệu GSM để nghe lén các cuộc đàm thoại, nhưng đầu tư cho thiết bị phải lên đến hàng trăm nghìn USD.

Theo Ian Meakin ở công ty mã hóa điện thoại di động Cellcrypt thì "chỉ có các cơ quan chính phủ và các tổ chức tội phạm được tài trợ vốn lớn mới có khả năng tiếp cận đến công nghệ cần thiết".

Ông cho rằng công trình của Nohl là một "sự lo ngại lớn" vì nó làm giảm chi phí để giải mã các cuộc gọi GSM. Một cách vô tình, nó có thể đặt các công cụ và công nghệ này vào tay bọn tội phạm.

Tuy nhiên, GSMA lại bác bỏ các lo lắng. Họ cho rằng từ trước đến nay đã có nhiều phác thảo về cách thức làm thế nào để xâm phạm đến A5/1 nhưng cho đến bây giờ vẫn chưa có được một

cuộc tấn công trên thực tế.

Hiệp hội cũng cho biết họ cũng đang đề nghị nâng cấp A5/1 lên một tiêu chuẩn mới bảo mật hơn gọi là A5/3 mà hiện tại đang được xây dựng.