# NGƯỜI DÙNG WI-FI KHÔNG NÊN SỬ DỤNG TÍNH NĂNG BẢO MẬT WEP

Ba chu

Ba chuyên gia bảo mật cao cấp của Đức vừa cảnh báo người dùng không nên sử dụng chuẩn WEP (giao thức bảo mật) của Wi-Fi để bảo vệ các thông tin nhạy cảm trên hệ thống bởi chúng có thể "gãy gục" trước một phương thức tấn công mới.

Một cuộc tấn công "demo" vào giao thức bảo mật WEP (Wired Equivalent Privacy) sẽ được ba chuyên gia trên trình diễn tại một hội nghị bảo mật trong tuần này ở Hamburg, Đức.

Các đây 6 năm, các nhà toán học đã chỉ ra rằng khoá thuật toán RC4 (nền tảng của giao thức WEP) bị hổng, nhưng nếu muốn phá được thuật toán này thì các cuộc tấn công phải cần sự can thiệp của ít nhất 4 triệu gói dữ liệu để tính toán đầy đủ mã bảo mật của WEP. Tuy nhiên, một số sai sót bảo mật WEP được phát hiện tiếp sau đó đã giúp rút ngắn khoảng cách phá mã thuật toán này xuống còn từng phút. Thế nhưng thời gian này vẫn chưa đủ để đột nhập vào hệ thống bởi các khoá bảo mật WEP cứ mỗi 5 phút lại thay đổi mật lần.

Nghiên cứu mới nhất của ba chuyên gia bảo mật trên chỉ ra rằng chỉ cần ... 3 giây là có thể phá mã được WEP. Thời gian này đủ để giải mã khoá WEP 104-bit nếu sử dụng bộ xử lý Pentium M 1.7GHz. So với các phương thức giải mã WEP trước đây, phương pháp mới tốn ít thời gian và sức mạnh máy tính hơn.

Các chuyên gia này cảnh báo nếu người dùng Wi-Fi muốn truyền dữ liệu mang tính riêng tư và nhạy cảm như tài khoản ngân hàng, họ cần phải chuyển sang một giao thức bảo mật an toàn hơn thay cho WEP, chẳng hạn như tính năng mã hoá WPA (nếu được mạng hỗ trợ).