

BẢO MẬT BẰNG HÌNH ẢNH

Là người sử dụng máy tính, chắc hẳn bạn hiểu tầm quan trọng của việc bảo mật thông tin và mật khẩu vốn là đối tượng hay bị dòm ngó, dễ bị đánh cắp, nhất là khi nó quá đơn giản.

Bức ảnh ph

Là người sử dụng máy tính, chắc hẳn bạn hiểu tầm quan trọng của việc bảo mật thông tin và mật khẩu vốn là đối tượng hay bị dòm ngó, dễ bị đánh cắp, nhất là khi nó quá đơn giản.

Bức ảnh phong cảnh Trường đại học Rutgers - Camden

Một phương pháp bảo mật mới vừa được công bố đang thu hút sự chú ý: mật khẩu bằng hình ảnh đồ họa. Đây là công trình nghiên cứu mới của các chuyên gia máy tính từ Đại học Rutgers - Camden (Mỹ)... Một trong những giải pháp là "bắt lại từ một vị trí click chuột" trên một hình đã được chọn lựa trước của người dùng (mật khẩu được tạo và máy nhận diện bằng cách vị trí nhấp chuột). Một phương án khác là ngăn chặn "shoulder surfing" (một cách ăn cắp mật khẩu bằng cách từ phía sau nhìn lén qua vai của người đang gõ mật khẩu) bằng cách chọn vùng ngẫu nhiên trong tập hợp những biểu tượng được người dùng dự trù trước giữa một khu vực hình ảnh. Nếu các giải pháp này có thể hoàn hảo cho hệ thống chính, nó sẽ giúp không phải tốn công tạo ra mật khẩu mới cho các ứng dụng trực tuyến. Giáo sư máy tính Jean - Camille Birget và đội nghiên cứu của ông đã có ý tưởng "mật khẩu đồ họa" độc đáo này. Giáo sư Jean cho biết theo lệ thường, mật khẩu được tạo bằng các con số và các ký tự, với giải pháp về hình thì người dùng sẽ chọn những khu vực trong một hình cho trước, gọi là "điểm chọn" (click point), các vị trí này rất dễ nhớ với chủ nhân nhưng lại trở nên khó đoán cho người khác. Trong chương trình bảo mật máy tính bằng hình ảnh, Jean - Camille Birget hướng dẫn: "Bạn có thể yêu cầu người dùng chọn bức tranh, điều này giúp người dùng nhớ những điểm nhấn chuột ban đầu trên hình. Hình chọn phải đủ phức tạp ví như hình một thành phố, để có thể bảo mật, người dùng cần phải chọn nhiều vị trí trên hình. Bức ảnh phong cảnh Trường đại học Rutgers - Camden là một ví dụ. Đây là hình thật mô tả một cách đơn giản mật khẩu hình ảnh phù hợp với lối dùng mật khẩu cũ (số và chữ). Để đăng nhập, người

dùng được yêu cầu chọn đồng thời bốn vị trí có vòng tròn trên hình. Những vị trí này đã được chọn khi tạo ra mật khẩu, bốn vị trí chọn này tùy ý thích của người dùng, quan trọng nhất là họ phải chọn vị trí sao cho dễ nhớ. Người dùng cũng có thể dùng hình riêng của mình để tạo mật khẩu, càng nhiều điểm được chọn độ bảo mật càng cao. Phương pháp thứ hai được phát triển để ngăn chặn "shoulder surfing", một kiểu đánh cắp mật khẩu do người dùng không biết đang bị kẻ xấu theo dõi từ phía sau. Theo phương pháp này, người dùng phải chọn 10 biểu tượng, được trộn lẫn trong gần 200 biểu tượng khác. Theo thứ tự để truy cập vào hệ thống, người dùng phải tìm các hình, cụ thể ở đây là hình tam giác, và các biểu tượng họ chọn đặt tại các góc và nhấp chuột vào bên trong khu vực hình (tam giác) đã chọn ấy. Leonardo Sobrado, một thành viên của nhóm nghiên cứu, nói rằng: " Ý tưởng chính của mô hình là cho phép người dùng chứng tỏ khả năng hiểu biết về các điều bí mật mà không tiết lộ các bí mật này ra ngoài một cách vô tình cho người khác. Câu hỏi hay các yêu cầu bị thay đổi theo thời gian khi thực hiện trả lời, nhưng các bí mật (mật khẩu) thì chẳng thay đổi. Nếu muốn thử nghiệm công nghệ này, bạn có thể tải chương trình ở: <http://clam.rutgers.edu/~lsobrado/graphicalpassword/>. Các thông tin chi tiết bạn có thể tìm thấy ở trang The Graphical Passwords Project (<http://clam.rutgers.edu/~birget/grPssw>). TAM TRUNG