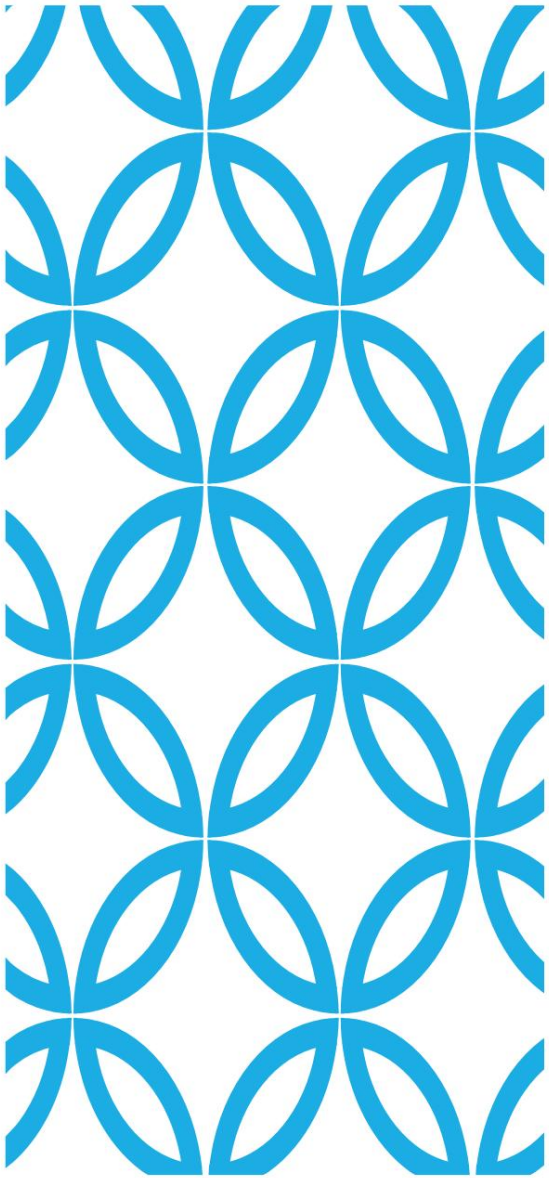


# XÁC THỰC CỦA MỌI NGƯỜI

Tiến sĩ Nguyễn Tuấn Nam

nam.nguyen@brumob.com

# XÁC THỰC

Việc xác thực được thực hiện khác nhau tùy thuộc vào khả năng của đối tượng được xác thực

Hai khả năng quan trọng nhất Khả năng
lưu trữ khóa mật mã chất lượng cao
Khả năng thực hiện các hoạt động mật mã

"Khóa chất lượng cao" = bí mật được chọn từ một không gian rất lớn sao cho không thể tính toán được bí mật bằng cách tìm kiếm toàn diện

Máy tính có cả hai khả năng

Người không có

# XÁC THỰC NGƯỜI DÙNG

3 kỹ thuật chính để xác minh rằng bạn là người mà bạn tuyên bố

- Những gì bạn biết: mật khẩu
- Những gì bạn có: Thẻ ATM, chìa khóa vật lý
- Bạn là ai: thiết bị sinh trắc học (hệ thống nhận dạng giọng nói, máy phân tích dấu vân tay)

# MẬT KHẨU

Máy tính tiền nhiệm

Lời chào đặc biệt

Nhiều vấn đề khi sử dụng mật khẩu để xác thực Kẻ nghe trộm có thể thấy mật khẩu Kẻ xâm nhập có thể đọc tệp thông tin mật khẩu Đoán mật khẩu bằng cách đăng nhập trực tiếp Có thể bị bẻ khóa bằng tìm kiếm máy tính ngoại tuyến Thuận tiện và bảo mật

Người dùng được ủy quyền sẽ trở thành kẻ thù nếu cơ chế bảo mật trở nên quá bất tiện đối phó với

# DỰ ĐOÁN MẬT KHẨU TRỰC TUYẾN

Người ta có thể mạo danh bạn nếu họ đoán được mật khẩu của bạn

Nhiều mật khẩu được chọn rõ ràng

- Tên
- DOB

Đoán đủ, mật khẩu nào cũng đoán được

- Việc đó có khả thi hay không phụ thuộc vào số lần dự đoán và mật khẩu có thể được kiểm tra nhanh như thế nào
- Sử dụng trong quân sự: sai mật khẩu  bị bắn

# CÁCH NGĂN NGỪA MẬT KHẨU TRỰC TUYẾN ĐOÁN

Làm việc theo nhóm

# NGĂN NGỪA MẬT KHẨU TRỰC TUYẾN ĐOÁN

Máy tính nhanh hơn và kiên nhẫn hơn nhiều so với con người trong việc đưa ra dự đoán thiết kế hệ thống sao cho con người phải gõ các dự đoán

Theo dõi số lần mật khẩu sai liên tiếp của một tài khoản

Khi số lượng vượt quá ngưỡng khóa tài khoản

Ví dụ: mã PIN trên thẻ ATM

# NGĂN NGỪA MẬT KHẨU TRỰC TUYẾN ĐOÁN

## Làm chậm một người đoán

Số lần đoán tài khoản/mật khẩu bị giới hạn cho mỗi lần kết nối Mật khẩu sai khiến quá trình xử lý chậm

## Bắt một người đoán

Theo dõi kết nối

Thực hiện hành động khắc phục

Báo cáo người dùng về thời điểm đăng nhập lần trước và số lần nhập mật khẩu không thành công

# NGĂN NGỪA MẬT KHẨU TRỰC TUYẾN ĐOÁN

Thời gian dự kiến đoán mật khẩu = số lần đoán dự kiến/tỷ lệ đoán

Bên cạnh việc giới hạn tỷ lệ đoán, chúng ta có thể đảm bảo không gian tìm kiếm đủ lớn

Mật khẩu được chọn ngẫu nhiên bất tiện

Cho phép người dùng chọn mật khẩu của riêng mình nhưng cảnh báo họ chọn mật khẩu tốt và thực thi lựa chọn đó nếu có thể

# DỰ ĐOÁN MẬT KHẨU NGOẠI TUYẾN

## Đoán mật khẩu trực tuyến

Việc đoán có thể được làm chậm lại và được kiểm tra

## Đoán mật khẩu ngoại tuyến

Kẻ tấn công có thể lấy được hàm băm mật mã của mật khẩu hoặc số lượng được mã hóa bằng mật khẩu

Kẻ tấn công đoán mật khẩu, thực hiện phép băm tương tự và so sánh với số lượng

Không ai biết và ở tốc độ chỉ bị giới hạn bởi tính toán có thể mua được quyền lực

# ĐOÁN MẬT KHẨU NGOẠI TUYẾN

Tệp mật khẩu UNIX có thể đọc công khai Cách đoán mật khẩu chưa được kiểm tra và hiệu suất khá cao

Không tra cứu được nếu quên mật khẩu

## Muối

Lưu trữ cả muối và hàm băm của sự kết hợp giữa muối và mật khẩu

# BÍ MẬT NÊN LỚN NHƯ THẾ NÀO?

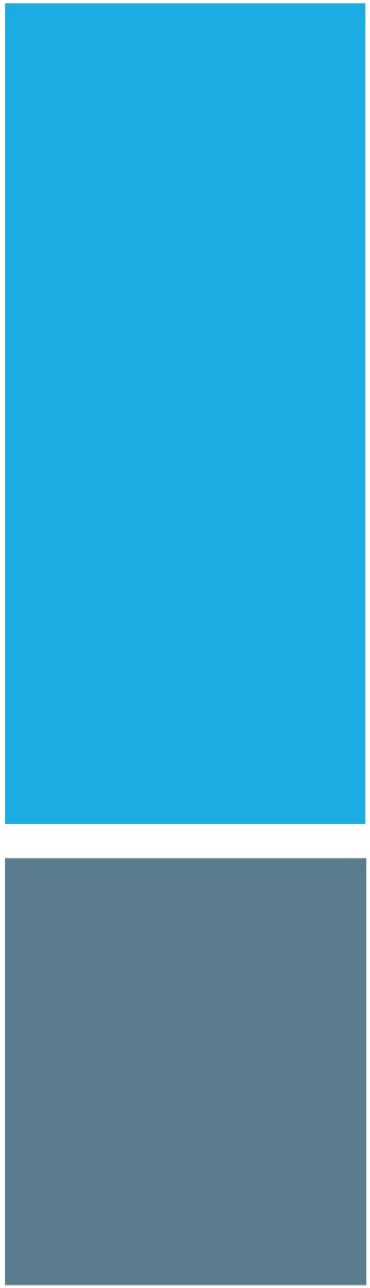
Để ngăn chặn một cuộc tấn công trực tuyến, bí mật không cần phải chọn từ một không gian rộng lớn  Hệ thống ATM có 4 đến 6 chữ số thập phân

Tấn công ngoại tuyến

Bí mật phải được chọn từ một không gian rất lớn  64 bit

# NGHE TRỘM

Rủi ro và cách phòng ngừa?



# NGHE TRỘM

## Phải nói mật khẩu mới được sử dụng luôn có khả năng bị nghe lén

Xem khi ai đó nhập mật khẩu

Wiretap để xem tất cả mật khẩu (máy ảnh, thiết bị ghi nhật ký)

## Phòng ngừa

Khoảng cách

Mật khẩu phức tạp (cần nhiều ngón tay hơn khi gõ)

Che giấu mật khẩu

Mật khẩu một lần (danh sách)

Danh sách mật khẩu được sử dụng lại (danh sách có thể ngắn hơn và sử dụng lâu hơn)

# MẬT KHẨU VÀ CẨU THẢ NGƯỜI DÙNG

Mật khẩu được đăng trên bảng điều khiển

Bao gồm mật khẩu trực tuyến ở những nơi có thể truy cập được

Bao gồm mật khẩu trong tập lệnh

Tự động truy cập vào các hệ thống khác

Đưa mật khẩu vào tin nhắn gửi qua email, SMS

# SỬ DỤNG MẬT KHẨU Ở NHIỀU NƠI

BẠN NGHĨ SAO?

BẠN CÓ THÍCH NÓ KHÔNG?

# YÊU CẦU MẬT KHẨU THƯỜNG XUYÊN THAY ĐỔI

Quản trị viên: mật khẩu được thay đổi 90 ngày một lần

Người dùng đặt lại mật khẩu cho cùng một thứ

Admin: mật khẩu mới phải khác mật khẩu cũ

Người dùng: đặt thành cái mới, sau đó đặt lại cái cũ

Quản trị viên: theo dõi n mật khẩu trước đó

Người dùng: n+1 lần và đặt lại về cũ

Admin: không cho phép đổi mật khẩu quá sớm

Người dùng: mật khẩu mới giống với mật khẩu cũ

Ad: cấm cái đó đi

Người dùng: chấp nhận mật khẩu khó nhớ và đăng chúng lên thiết bị đầu cuối của họ


# ĐĂNG NHẬP NGỰA Trojan VÀO CHỤP MẬT KHẨU

# PHÂN PHỐI MẬT KHẨU BAN ĐẦU

Người dùng xuất hiện tại terminal của quản trị hệ thống

Tạo tài khoản và mật khẩu mạnh ban đầu và cung cấp cho người dùng (trao tay, gửi qua đường bưu điện)

# MÃ XÁC THỰC

Thiết bị vật lý mà người đó mang theo và sử dụng để xác thực những gì bạn có

Phải kết hợp với 1 trong 2 cơ chế còn lại để được bảo mật (bạn biết gì, bạn là ai)

Một số hình thức

- Chìa khóa
- Thẻ tín dụng

Điều bất lợi

- Yêu cầu phần cứng tùy chỉnh (khe cắm chìa khóa hoặc đầu đọc thẻ) trên mỗi lần truy cập thiết bị
- Token có thể bị mất hoặc bị đánh cắp được bổ sung mã PIN hoặc mật khẩu
- Để quên token ở nhà?

# THẺ THÔNG MINH

Kích thước của thẻ tín dụng nhưng có CPU và bộ nhớ nhúng

Nhiều mẫu khác nhau

- Thẻ nhớ được bảo vệ bằng mã PIN
- Thẻ thách thức/phản hồi bằng mật mã
- Máy tính mật mã
- Thẻ thông minh không có đầu đọc
- Không cần kết nối điện với thiết bị đầu cuối
- Có màn hình và bàn phím

# TRUY CẬP VẬT LÝ


# sinh trắc học

Máy quét võng mạc

Kiểm tra các mạch máu nhỏ ở phía sau mắt cu a ba n

Đắt tiền và đe dọa tâm lý người dùng giao diện

Đầu đọc dấu vân tay

# THIẾT BỊ SINH TRẮC

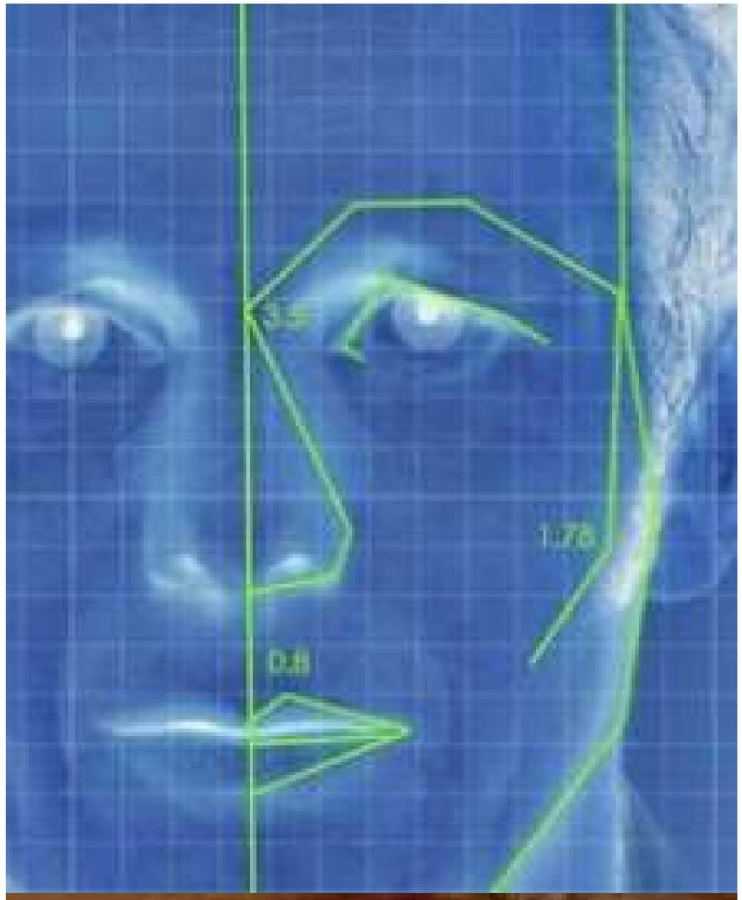
Nhận dạng khuôn mặt

Đo kích thước khuôn mặt

Đừng đến nơi làm việc với mắt thâm đen và quai hàm sưng tấy

Máy quét mống mắt

Lập bản đồ bố cục đặc biệt của mống mắt của bạn



# sinh trắc học

Đầu đọc dấu tay

Dấu giọng

Thời gian gõ phím

Chữ ký