BỘ CÔNG THƯƠNG

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

HỒ PHÚC LÂM

ĐỀ TÀI: TÌM HIỂU VỀ HÀM BĂM VÀ CÁCH THỨC TẤN CÔNG MẬT KHẨU

Học phần: Nhập môn An toàn thông tin

Mã học phần: 420300100404

Lớp học phần: DHKHMT17B

GVHD: TS Ngô Hữu Dũng

TP. HỒ CHÍ MINH, THÁNG 04 NĂM 2024

LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn chân thành đến TS Ngô Hữu Dũng đã hướng dẫn và hỗ trợ tôi suốt quá trình thực hiện bài báo cáo về "Tìm hiểu về Hàm Băm và Cách thức Tấn công Mật khẩu". Thầy đã dành thời gian quý báu để chia sẻ kiến thức chuyên sâu và cung cấp những hướng dẫn cần thiết, giúp tôi hiểu rõ hơn về nội dung dự án và phát triển kỹ năng trong lĩnh vực An toàn thông tin.

Sự động viên và những lời chỉ bảo từ Thầy Ngô Hữu Dũng đã truyền động lực lớn để tôi hoàn thành dự án này một cách thành công. Tôi rất biết ơn về sự nhiệt tình và tận tâm của Thầy trong việc hướng dẫn và định hướng cho tương lai nghề nghiệp của tôi.

Xin chân thành cảm ơn Thầy Ngô Hữu Dũng một lần nữa!

Trân trọng,

Hồ Phúc Lâm

Nhận xét của Giáo viên hướng dẫn

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

MỤC LỤC

CHƯƠNG I. HÀM BĂM

1.1. Giới thiệu hàm băm

Hàm băm là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán h một chiều nào đó, rồi đưa ra một bản băm - văn bản đại diện - có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.Giá trị của hàm băm là duy nhất, và không thể suy ngược lại được nội dung thông điệp từ giá trị băm này.

Trong ngành mật mã học, một hàm băm mật mã học (tiếng Anh: Cryptographic hash function) là một hàm băm với một số tính chất bảo mật nhất định để phù hợp việc sử dụng trong nhiều ứng dụng bảo mật thông tin đa dạng, chẳng hạn như chứng thực (authentication) và kiểm tra tính nguyên vẹn của thông điệp (message integrity). Một hàm băm nhận đầu vào là một xâu ký tự dài (hay thông điệp) có độ dài tùy ý và tạo ra kết quả là một xâu ký tự có độ dài cố định, đôi khi được gọi là tóm tắt thông điệp (message digest) hoặc chữ ký số (digital fingerprint).

1.2. Hàm băm MD5 (Message Digest Algorithm 5)

- MD5 là một thuật toán băm được phát triển bởi Ronald Rivest vào năm 1991.
- MD5 tạo ra một băm có độ dài 128 bit (16 byte), thường được biểu diễn dưới dạng chuỗi hexa 32 ký tự.
- Thuật toán này nhanh chóng và đơn giản, nhưng đã bị thay thế trong các ứng dụng an ninh bởi những lỗ hổng bảo mật đã được phát hiện.
- MD5 không nên được sử dụng cho mục đích bảo mật nhạy cảm vì hiện nay đã có khả năng tìm ra hai đầu vào khác nhau cho cùng một giá trị băm.

1.3. SHA-1 (Secure Hash Algorithm 1)

- SHA-1 là một thuật toán băm được phát triển bởi NSA vào năm 1993 và được công bố năm 1995.
- SHA-1 tạo ra một băm có độ dài 160 bit (20 byte), thường được biểu diễn dưới dạng chuỗi hexa 40 ký tự.
- Trong thời gian gần đây, SHA-1 cũng đã bị coi là không an toàn do các vấn đề liên quan đến va chạm (collision attacks) và nên được thay thế bởi các thuật toán băm mạnh hơn như SHA-256.

1.4. SHA-256 (Secure Hash Algorithm 256-bit)

- SHA-256 là một thuật toán băm trong họ các thuật toán SHA-2, được phát triển bởi NSA.
- SHA-256 tạo ra một băm có độ dài 256 bit (32 byte), thường được biểu diễn dưới dạng chuỗi hexa 64 ký tự.
- SHA-256 hiện được coi là một trong những thuật toán băm mạnh và an toàn nhất được sử dụng rộng rãi trong các ứng dụng bảo mật, bao gồm mã hóa mật khẩu, chữ ký số, và xác thực dữ liệu.

1.5. SHA-3 (Secure Hash Algorithm 3)

- SHA-3 là một thuật toán băm thuộc họ các thuật toán SHA, được thiết kế bởi Keccak Team.
- NIST đã tiêu chuẩn hóa SHA-3 và công bố nó là một tiêu chuẩn Federal Information Processing Standard (FIPS) vào năm 2015.
- SHA-3 được coi là một trong những thuật toán băm mạnh và an toàn nhất hiện nay.
- SHA-3 được sử dụng rộng rãi trong các ứng dụng bảo mật, bao gồm mã hóa mật khẩu, chữ ký số, xác thực dữ liệu, và các ứng dụng an ninh mạng.

CHƯƠNG 2. MẬT KHẨU

2.1. Độ mạnh mật khẩu

1. **Độ dài của mật khẩu:** Độ dài của mật khẩu là yếu tố quan trọng nhất trong việc xác định độ mạnh của nó. Mật khẩu càng dài thì càng khó để bị dò ra bằng các phương pháp tấn công dò mật khẩu.
2. **Đa dạng hóa ký tự:** Mật khẩu nên bao gồm các loại ký tự khác nhau như chữ cái (in hoa và thường), chữ số và ký tự đặc biệt. Việc sử dụng các loại ký tự đa dạng sẽ làm tăng độ khó cho việc đoán đúng mật khẩu.
3. **Không sử dụng các thông tin dễ đoán:** Tránh sử dụng các mật khẩu dễ đoán như tên người dùng, ngày sinh, dòng chữ liên tục trên bàn phím, hoặc các từ xuất hiện trong từ điển.
4. **Không sử dụng các mật khẩu trùng lặp:** Không sử dụng cùng một mật khẩu cho nhiều tài khoản. Nếu mật khẩu của một tài khoản bị phơi bày, hacker có thể sử dụng nó để truy cập vào các tài khoản khác của bạn.
5. **Các yêu cầu bảo mật của hệ thống:** Ngoài các yếu tố trên, các hệ thống có thể yêu cầu các tiêu chí bảo mật khác như sử dụng mật khẩu có ít nhất một chữ số, một ký tự đặc biệt, hoặc một ký tự in hoa.

2.2. Các dạng tấn công mật khẩu phổ biến

- **Brute Force Attack** (tấn công dò mật khẩu)
    - Kẻ tấn công sử dụng một công cụ mạnh mẽ, có khả năng thử nhiều username và password cùng lúc (từ dễ đến khó) cho tới khi đăng nhập thành công
    - VD: đặt mật khẩu đơn giản như 123456, password123, daylamatkhau,…rất dễ bị tấn công brute force.

- **Dictionary Attack** (tấn công từ điển)
    - Là một biến thể của Brute Force Attack
    - Tuy nhiên kẻ tấn công nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng
    - Nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản và có ngữ nghĩa. VD: motconvit, iloveyou,… Đây là lý do khiến Dictionary Attack có tỉ lệ thành công cao hơn
- **Key Logger Attack** (tấn công Key Logger)
    - Kẻ tấn công lưu lại lịch sử các phím mà nạn nhân gõ, bao gồm cả ID, password hay nhiều nội dung khác
    - Kẻ tấn công cần phải sử dụng một phần mềm độc hại (malware) đính kèm vào máy tính (hoặc điện thoại) nạn nhân, phần mềm đó sẽ ghi lại tất cả những ký tự mà nạn nhân nhập vào máy tính và gửi về cho kẻ tấn công. Phần mềm này được gọi là Key Logger
    - Nguy hiểm hơn 2 cách tấn công trên, do việc đặt mật khẩu phức tạp không giúp ích gì trong trường hợp này

CHƯƠNG 3. KẾT LUẬN

Trong bài báo cáo này, chúng ta đã tìm hiểu về hai khái niệm quan trọng trong lĩnh vực An toàn thông tin là hàm băm và cách thức tấn công mật khẩu.

Về hàm băm, chúng ta đã nắm được rằng đây là các thuật toán không sử dụng khóa để mã hóa thông điệp, mà thay vào đó, chúng biến đổi thông điệp thành một văn bản đại diện (bản băm) có kích thước cố định. Các hàm băm như MD5, SHA-1, SHA-256 và SHA-3 đều là những thuật toán phổ biến được sử dụng để đảm bảo tính toàn vẹn thông điệp và cung cấp chứng thực trong các ứng dụng bảo mật.

Đối với mật khẩu, chúng ta đã tìm hiểu về các yếu tố quan trọng để tạo ra mật khẩu mạnh và tránh các dạng tấn công phổ biến như Brute Force Attack, Dictionary Attack và Key Logger Attack. Việc sử dụng mật khẩu dài, đa dạng hóa ký tự, không sử dụng các thông tin dễ đoán và không tái sử dụng mật khẩu là những thủ thuật quan trọng giúp tăng cường độ bảo mật của hệ thống.

TÀI LIỆU THAM KHẢO

- https://hplamit1302.github.io/AnToanThongTin/
- Giáo trình: Chương 6. Hàm Băm và chữ ký số
- https://vi.wikipedia.org/wiki/Cryptographic-hash-function
- https://fptshop.com.vn/tin-tuc/danh-gia/hash-la-gi-175056
- https://locker.io/vi/passwords/password-health-checker