HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ
MÃ HỌC PHẦN: INT1344

LAB : hash_extender

Sinh viên thực hiện: Lê Ngọc Đức

Mã sinh viên: B22DCAT092

Tên lớp: 04

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HÀ NỘI 2025

LAB : Hash_extender

1. Mục đích

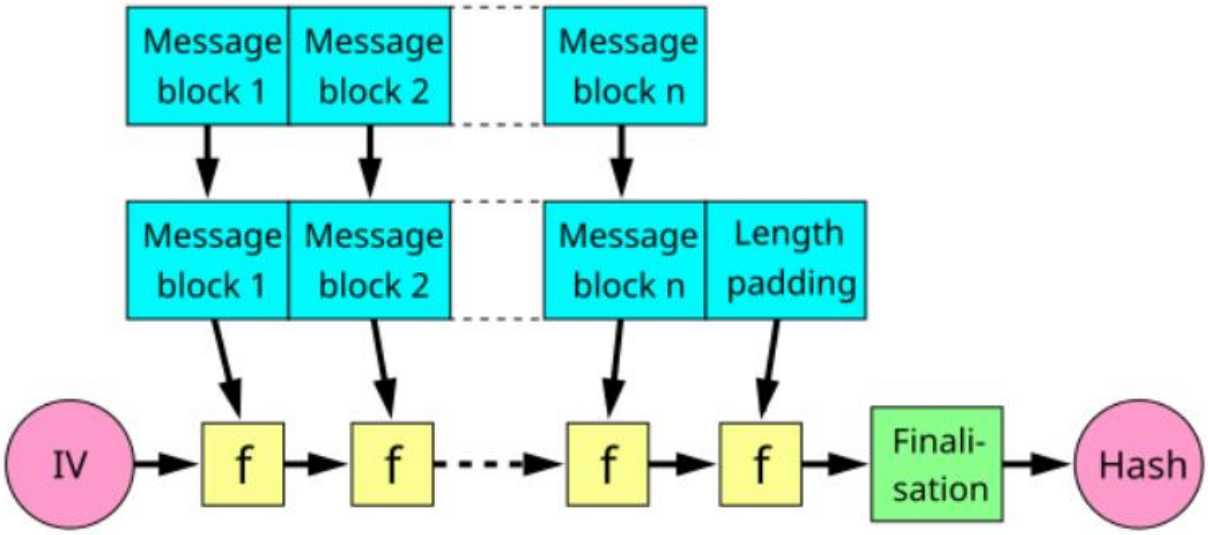
Giúp sinh viên hiểu và thực hành tấn công mở rộng độ dài (Length Extension Attack – LEA) với những hàm băm sử dụng kiến trúc Merkle–Damgård và MAC sử dụng dạng hash(secret||message)

2. Yêu cầu đối với sinh viên

Sử dụng thuần thục hệ điều hành Linux và có kiến thức về mật mã học

3. Nội dung lý thuyết

Lý thuyết về kiến trúc Merkle–Damgård



Lý thuyết về Length Extension Attack:

Giả sử attacker biết giá trị hash H(m) và độ dài của m, nhưng không biết m:

- Attacker tính toán padding của m (vì padding chỉ phụ thuộc vào độ dài m).
- Attacker tạo chuỗi giả mạo m' = m || p || z, với z là dữ liệu thêm tùy ý.
- Attacker khởi tạo lại trạng thái nội bộ của hàm băm từ H(m).
- Sau đó tiếp tục băm tiếp phần z (cộng với padding mới) để tính ra H(m') — mà không cần biết m.

Kết quả: Attacker có thể tính được hash hợp lệ của m' và giả mạo thông điệp có vẻ hợp lệ với hash ban đầu.

4. Nội dung thực hành

Add module file lab:

imodule https://github.com/ptit-wibu/labtainer/raw/refs/heads/main/hash_extender.tar

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r hash_extender

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người

thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Nhiệm vụ 1: Chạy server

Thực hiện xem ip của server và attacker bằng câu lệnh

ifconfig

Thực hiện chạy server bằng câu lệnh

python3 server.py

Nhiệm vụ 2: Thực hiện lấy MAC

- Sau khi hoàn thành bước trên, tiến hành lấy MAC bằng cách

curl "http://<server_IP>:5000/mac?message=user=client"

- Tiến hành mở tool và đưa MAC vào trong file

Nano attack.py

Nhiệm vụ 3: Thực hiện tấn công LEA

- Chạy file attack bằng câu lệnh

python3 attack.py

- Quan sát xem có trả về hello admin với successful hay không

Nhiệm vụ 4: Thực hiện lại nội dung trên bằng cách thay đổi secretkey thành tên + MSV

- Thực hiện lại các nhiệm vụ trên bằng cách thay tên + MSV vào trong trường secret key của file server.py

Kết thúc bài lab:

o Kiểm tra checkwork:

checkwork

o Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab

Khởi động lại bài lab:

labtainer -r hash_extender