Bài Thực Hành: Giấu Tin Trong Metadata của File Âm Thanh WAV

1. Mục tiêu

- Nắm bắt cơ bản về định dạng file âm thanh WAV và cấu trúc metadata.
- Tìm hiểu kỹ thuật giấu tin (steganography) trong metadata của file WAV.
- Thực hiện nhúng thông điệp bí mật vào file WAV bằng FFmpeg.
- Trích xuất thông tin ẩn từ file WAV đã được nhúng tin.

2. Yêu cầu thực hành

Giấu tin trong metadata của file WAV là một phương pháp steganography đơn giản, cho phép nhúng dữ liệu bí mật vào phần thông tin phụ của file mà không ảnh hưởng đến chất lượng âm thanh. Bài lab này sử dụng FFmpeg để thực hiện các thao tác giấu tin và trích xuất tin.

Kịch bản

- **Kẻ tấn công**: Sử dụng file âm thanh để giấu mã độc hoặc thông điệp bí mật và truyền đi mà không bị phát hiện.
- **Nhà nghiên cứu bảo mật**: Phân tích và trích xuất dữ liệu ẩn từ file âm thanh để phát hiện thông tin nguy hiểm.

Yêu cầu

- Kiến thức cơ bản về steganography.
- Hiểu cấu trúc file WAV và vai trò của metadata.
- Công cụ cần thiết: **FFmpeg**

3. Thực hành

Khởi động bài lab: *labtainer stego_tool_audio_metadata*

Bước 1: Chuẩn bị âm thanh WAV

Giả sử đang làm việc trên cửa sổ của Alice

Chuẩn bị một file âm thanh WAV để thực hành. Nếu bạn chỉ có file ở định dạng khác (ví dụ: MP3), chuyển đổi sang WAV bằng lệnh:

ffmpeg -i sample.mp3 input.wav

Bước 2: Nhúng dữ liệu vào metadata của file WAV

Trên cửa sổ của Alice giấu thông điệp bí mật vào metadata sử dụng lệnh:

ffmpeg -i input.wav -metadata comment="Secret message: Attack at dawn" -codec copy stego_audio.wav

Giải thích lệnh:

- -i input.wav: File âm thanh đầu vào.
- -metadata comment="Secret message: Attack at dawn": Nhúng thông điệp vào trường comment trong metadata.
- -codec copy: Giữ nguyên dữ liệu âm thanh, không mã hóa lại để đảm bảo chất lượng không đổi.
- stego_audio.wav: File đầu ra chứa thông điệp ẩn.

So sánh dữ liệu trước và sau khi giấu để xem sự khác biệt về nội dung và dung lượng bằng các lệnh sau:

ls -l input.wav stego_audio.wav

cmp input.wav stego_audio.wav

Sau đó thực hiện chuyển video chứa thông điệp đã giấu sang cho Bob

scp *stego_audio.wav* bob:/home/ubuntu/

Password: password123

Bước 3: Trích xuất dữ liệu từ file wav

Phía Bob thực hiện giải mã

ffmpeg -i stego_audio.wav

Kết quả hiển thị sẽ bao gồm trường comment với nội dung: Secret message: Attack at dawn.

Xem cụ thể trường comment

Để chỉ xem nội dung của trường comment, sử dụng lệnh:

ffprobe -v error -show_entries format_tags=comment -of default=noprint_wrappers=1:nokey=1 stego_audio.wav

Giải thích lệnh:

- ffprobe: Công cụ phân tích file đa phương tiện
- -v error: Chỉ hiển thị thông báo lỗi
- -show_entries format_tags=comment: Trích xuất giá trị của trường comment trong metadata
- -of default=noprint_wrappers=1:nokey=1: Định dạng đầu ra gọn gàng, chỉ hiển thị giá trị
- Ý nghĩa: Tùy chọn -of (output format) xác định cách định dạng kết quả. Cụ thể:
    - default: Sử dụng định dạng mặc định của ffprobe.
    - noprint_wrappers=1: Loại bỏ các "wrapper" như [FORMAT] và [/FORMAT] thường xuất hiện trong đầu ra, giúp kết quả sạch hơn.
    - nokey=1: Chỉ hiển thị giá trị của trường comment (ví dụ: "Secret message: Attack at dawn") mà không hiển thị tên trường (comment=). Điều này làm cho đầu ra chỉ chứa nội dung thông điệp.
- stego_audio.wav: File âm thanh cần kiểm tra

Bước 4: Xóa thông điệp ẩn trong metadata

Nếu muốn xóa metadata để tạo file sạch, chạy lệnh:

ffmpeg -i stego_audio.wav -map_metadata -1 -codec copy clean_audio.wav

Giải thích:

- -map_metadata -1: Xóa toàn bộ metadata.
- -codec copy: Giữ nguyên dữ liệu âm thanh.
- clean_audio.wav: File đầu ra không chứa metadata.

Kiểm tra file đã làm sạch:

ffprobe -v error -show_entries format_tags=comment -of default=noprint_wrappers=1:nokey=1 clean_audio.wav

Kết quả: Không hiển thị nội dung (trường comment đã bị xóa).

4. Kết quả cần đạt được

• Hoàn thành các bước: Chuẩn bị file, nhúng tin, chuyển file, trích xuất tin, và xóa metadata.

• Cần nộp 1 file: trong thư mục: /home/student/labtainer_xfer/TÊN_BÀI_LAB (tên tài khoản.*TÊN_BÀI_LAB.lab)*

• Kết thúc bài lab:

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

stoplab stego_tool_audio_metadata

• Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

• Sinh viên cần nộp file *.lab* để chấm điểm.

• Để kiểm tra kết quả khi trong khi làm bài thực hành sử dụng lệnh:

checkwork <tên bài thực hành>

• Khởi động lại bài lab: Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer –r stego_tool_audio_metadata