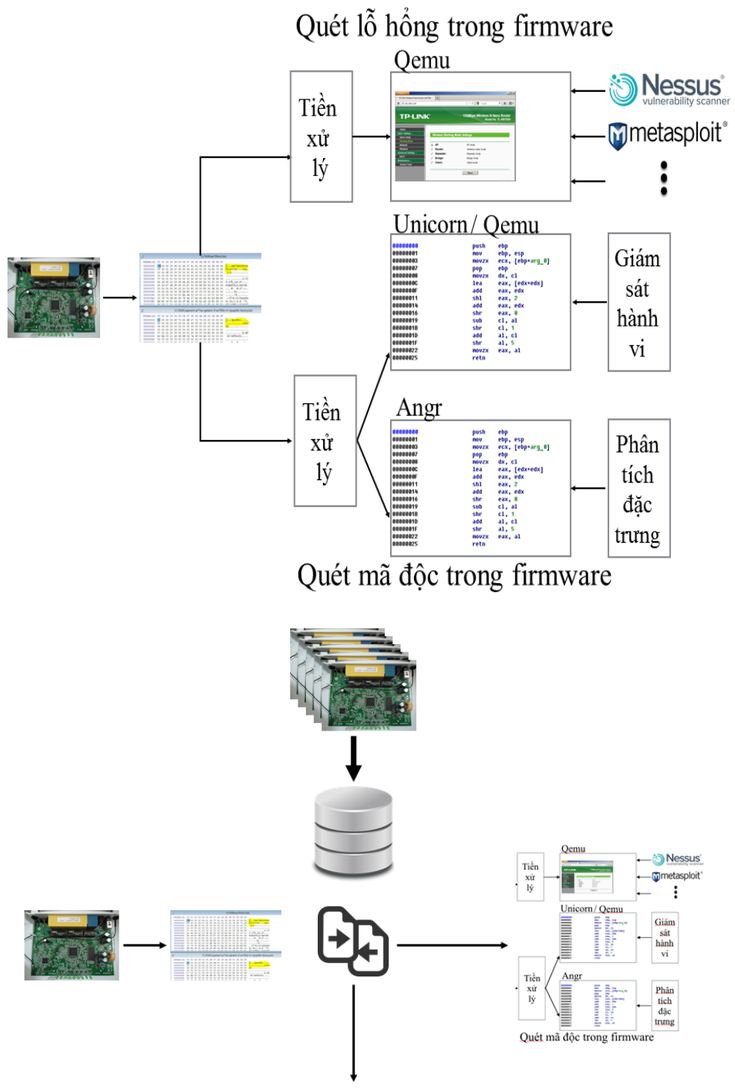
Phân tích và phát hiện lỗ hổng bảo mật trong firmware của các thiết bị mạng

PGS TS Nguyễn Ngọc Bình, Viện Quốc tế Pháp ngữ - ĐH QGHN
ThS Trần Nghi Phú, Học viện An ninh nhân dân

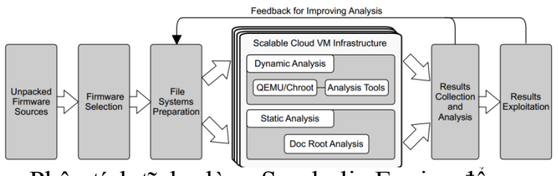
Công nghệ ngày càng phát triển mãnh mẽ, đi sâu vào mọi khía cạnh của cuộc sống, do đó vấn đề an ninh an toàn trở thành một trong những vấn đề được quan tâm nhất trong thế giới ngày nay. Nguy cơ về mất an ninh thông tin không chỉ dừng lại mức ứng dụng phần mềm mà đặt ra cả ở mức phần cứng thiết bị và ngày nay một lĩnh vực đang dấy lên nhiều lo ngại là nguy cơ từ các hệ thống nhúng tích hợp, firmware của các thiết bị, đặc biệt các thiết bị đóng vai trò trung tâm trong kết nối, truyền dẫn thông tin như các thiết bị mạng. Các nghiên cứu từ trước tập trung cho các ứng dụng mức cao trên kiến trúc i386, hệ điều hành Windows, các phương pháp và công cụ hỗ trợ cho việc phân tích firmware còn rất hạn chế và gặp nhiều khó khăn do tiếp cận mức thấp, kiến trúc đa dạng, thiếu tài liệu đặc tả đầy đủ. Nghiên cứu của chúng tôi tập trung vào việc tìm hiểu kiến trúc của các thiết bị mạng, từ đó tìm cách trích xuất firmware từ các thiết bị này, sau đó phân tích nhằm phát hiện có hay không các lỗ hổng bảo mật hay malware cài cắm trong firmware. Việc phân tích và phát hiện dựa trên 2 phương pháp tĩnh và động. Các firmware được tiến hành phân tách, thu thập lấy phần thực thi chính của firmware thường là các Embeded Web trên nền Linux 2.6, phần lõi này được tiến hành phân tích tĩnh tìm ra backdoor hoặc chạy trong môi trường mô phỏng để quét phát hiện lỗ hổng bảo mật.

- Phương pháp trích xuất firmware từ thiết bị mạng thực tế
- Cơ chế hoạt động và phương pháp phát hiện Backdoor
- Các loại lỗ hổng bảo mật và kỹ thuật phát hiện
- Lỗ hổng bảo mật trong firmware của các thiết bị mạng, có 2 loại Blob firmware và UserSpace firmware
- Backdoor trong các thiết bị mạng

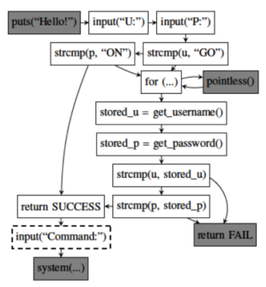
- Xây dựng mô hình và thiết bị trích xuất phần cứng trích xuất firmware từ thiết bị mạng.
- Phân tích các firmware để thu được các thông tin cần thiết, trích xuất phần lõi firmware như Embeded Web.
- Ảo hóa firmware trên QEMU, cài đặc các Embeded Web lên QEMU.
- Xây dựng hệ thống quét lỗ hổng bảo mật từ ngoài và chạy các Embeded Web trong các Sandbox
- Thu thập bộ mẫu 23.000 firmware phục vụ nghiên cứu, đánh giá
- Chạy một số mẫu trên các hệ thống phân tích, phát hiện nguồn mở

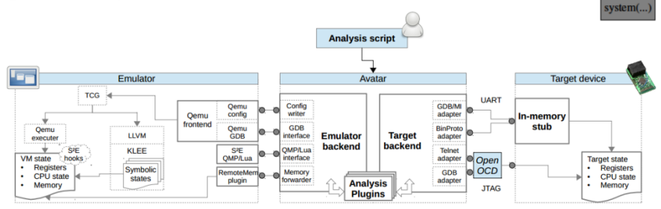


- Phân tích động: trích xuất phần Embeded Web trong firmware đưa lên chạy trên môi trường hệ điều hành Linux 2.6 để tiến hành rà quét lỗ hổng bảo mật từ ngoài bằng các công cụ quyét lỗ hổng bảo mật hoặc chạy trong Sanbox để phát hiện lỗi, phát hiện mã độc



- Phân tích tĩnh: dùng Symbolic Engine để phát hiện Backdoor
- Phân tích động phần lõi trên cơ sở sử dụng phần cứng của thiết bị như theo mô hình Avatar





- http://owasp.org/index.php/Top 10 2013-A1-Injection
- F. B. et al. QEMU – Quick EMUlator. http://www.qemu.org
- J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti. Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares. In ISOC Network and Distributed System Security Symposium (NDSS), 2014.
- Y. Shoshitaishvili, R. Wang, C. Hauser, C. Kruegel, and G. Vigna. Fir-malice: Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware. In ISOC Network and Distributed System Security Symposium (NDSS), 2015
- "Binwalk." [Online]. Available: http://binwalk.org/
- A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in Proceedings of the 23rd USENIX Security Symposium. USENIX, 2014, pp. 95–110. [Online]. Available: https://www.usenix.org/conference/ usenixsecurity14/technical-sessions/presentation/costin