

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**



HOÀNG XUÂN DẬU

**GIÁO TRÌNH
CƠ SỞ AN TOÀN THÔNG TIN**

HÀ NỘI - 2020

MỤC LỤC

DANH MỤC CÁC HÌNH	5
DANH MỤC CÁC THUẬT NGỮ TIẾNG ANH VÀ VIỆT TẮT	8
MỎ ĐẦU.....	10
CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN	12
1.1. Khái quát về an toàn thông tin	12
1.1.1. Một số khái niệm cơ bản	12
1.1.2. Sự cần thiết của an toàn thông tin	15
1.2. Các yêu cầu đảm bảo an toàn thông tin.....	16
1.2.1. Bí mật	16
1.2.2. Toàn vẹn	17
1.2.3. Sẵn sàng.....	18
1.3. Các thành phần của an toàn thông tin	18
1.3.1. An toàn máy tính và dữ liệu	18
1.3.2. An ninh mạng	19
1.3.3. Quản lý an toàn thông tin	19
1.3.4. Chính sách an toàn thông tin	20
1.4. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT	21
1.4.1. Bảy vùng trong cơ sở hạ tầng CNTT	21
1.4.2. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT	22
1.5. Mô hình tổng quát đảm bảo ATTT VÀ HTTT	23
1.5.1. Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng	23
1.5.2. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin.....	24
1.6. Kết chương	25
1.7. Câu hỏi ôn tập	25
CHƯƠNG 2. LỖ HỒNG BẢO MẬT VÀ ĐIỂM YẾU HỆ THỐNG	27
2.1. Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống.....	27
2.1.1. Khái quát	27
2.1.2. Một số thống kê về lỗ hổng bảo mật	29
2.2. Các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng	31
2.2.1. Lỗi tràn bộ đệm	32
2.2.2. Lỗi không kiểm tra đầu vào.....	38
2.2.3. Các vấn đề với kiểm soát truy cập	40

2.2.4. Các điểm yếu trong xác thực, trao quyền.....	41
2.2.5. Các điểm yếu trong các hệ mật mã	41
2.2.6. Các lỗ hổng bảo mật khác	41
2.3. Quản lý, khắc phục lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống	42
2.3.1. Nguyên tắc chung.....	42
2.3.2. Các biện pháp cụ thể	42
2.4. Giới thiệu một số công cụ rà quét điểm yếu và lỗ hổng bảo mật.....	43
2.4.1. Công cụ rà quét lỗ hổng bảo mật hệ thống.....	43
2.4.2. Công cụ rà quét lỗ hổng ứng dụng web	45
2.5. Kết chương.....	46
2.6. Câu hỏi ôn tập	46
CHƯƠNG 3. CÁC DẠNG TẤN CÔNG VÀ CÁC PHẦN MỀM ĐỘC HẠI	48
3.1. Khái quát về mối đe dọa và tấn công	48
3.1.1. Mối đe dọa.....	48
3.1.2. Tấn công	48
3.2. Các công cụ hỗ trợ tấn công.....	49
3.2.1. Công cụ quét cổng dịch vụ	50
3.2.2. Công cụ nghe lén	51
3.2.3. Công cụ ghi phím gõ	51
3.3. Các dạng tấn công thường gặp	52
3.3.1. Tấn công vào mật khẩu	52
3.3.2. Tấn công bằng mã độc	53
3.3.3. Tấn công từ chối dịch vụ	59
3.3.4. Tấn công từ chối dịch vụ phân tán	62
3.3.5. Tấn công giả mạo địa chỉ	64
3.3.6. Tấn công nghe lén	65
3.3.7. Tấn công kiểu người đứng giữa	66
3.3.8. Tấn công bằng bom thư và thư rác	67
3.3.9. Tấn công sử dụng các kỹ thuật xã hội	68
3.3.10. Tấn công pharming.....	70
3.3.11. Tấn công APT	72
3.4. Các dạng phần mềm độc hại	73
3.4.1. Phân loại	73
3.4.2. Mô tả các dạng phần mềm độc hại	74
3.4.3. Phòng chống phần mềm độc hại	81

3.5. Kết chương	82
3.6. Câu hỏi ôn tập	83
CHƯƠNG 4. ĐÁM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA	85
4.1. Khái quát về mã hóa thông tin và ứng dụng	85
4.1.1. Các khái niệm cơ bản	85
4.1.2. Các thành phần của một hệ mã hóa	88
4.1.3. Mã hóa dòng và mã hóa khối	88
4.1.4. Sơ lược lịch sử mật mã	89
4.1.5. Ứng dụng của mã hóa	90
4.2. Các phương pháp mã hóa	90
4.2.1. Phương pháp thay thế	91
4.2.2. Phương pháp hoán vị	91
4.2.3. Phương pháp XOR	92
4.2.4. Phương pháp Vernam	92
4.2.5. Phương pháp sách hoặc khóa chạy	93
4.2.6. Phương pháp hàm băm	93
4.3. Các giải thuật mã hóa	93
4.3.1. Các giải thuật mã hóa khóa đối xứng	94
4.3.2. Các giải thuật mã hóa khóa bất đối xứng	102
4.4. Các hàm băm	105
4.4.1. Khái quát về hàm băm	105
4.4.2. Một số hàm băm thông dụng	108
4.5. Kết chương	112
4.6. Câu hỏi ôn tập	112
CHƯƠNG 5. CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐÁM BẢO AN TOÀN THÔNG TIN ...	114
5.1. Kiểm soát truy cập	114
5.1.1. Khái quát về kiểm soát truy cập	114
5.1.2. Các biện pháp kiểm soát truy cập	115
5.1.3. Một số công nghệ kiểm soát truy cập	121
5.2. Tường lửa	125
5.2.1. Khái quát	125
5.2.2. Các loại tường lửa	127
5.2.3. Các kỹ thuật kiểm soát truy cập	129
5.2.4. Các hạn chế của tường lửa	130
5.3. Các hệ thống phát hiện và ngăn chặn xâm nhập	130

5.3.1. Khái quát	130
5.3.2. Phân loại.....	131
5.3.3. Các kỹ thuật phát hiện xâm nhập	134
5.4. Kết chương	136
5.5. Câu hỏi ôn tập	136
CHƯƠNG 6. QUẢN LÝ, CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN	138
6.1 Quản lý an toàn thông tin	138
6.1.1. Khái quát	138
6.1.2. Đánh giá rủi ro an toàn thông tin.....	139
6.1.3. Phân tích chi tiết rủi ro an toàn thông tin	142
6.1.4. Thực thi quản lý an toàn thông tin	144
6.2. Các chuẩn quản lý an toàn thông tin	147
6.2.1. Giới thiệu.....	147
6.2.2. Chu trình Plan-Do-Check-Act.....	148
6.3. Pháp luật và chính sách an toàn thông tin	149
6.3.1. Khái quát	149
6.3.2. Luật quốc tế về an toàn thông tin	150
6.3.3. Luật Việt Nam về an toàn thông tin	152
6.4. Vấn đề đạo đức an toàn thông tin.....	154
6.4.1. Một số bộ quy tắc ứng xử trong CNTT và ATTT	155
6.4.2. Một số vấn đề khác.....	155
6.5. Kết chương	156
6.6. Câu hỏi ôn tập	156
TÀI LIỆU THAM KHẢO	158

DANH MỤC CÁC HÌNH

Hình 1.1. Tam giác CIA (Confidentiality - Integrity - Availability) [1].....	12
Hình 1.2. Mô hình hệ thống thông tin của cơ quan, tổ chức	13
Hình 1.3. Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin.....	14
Hình 1.4. Số lượng các thiết bị IoT kết nối Internet từ 2015 đến 2025	15
Hình 1.5. Số lượng sự cố mất ATTT báo cáo bởi các cơ quan chính phủ Hoa Kỳ giai đoạn 2006-2018 [3]	16
Hình 1.6. Một văn bản được đóng dấu Confidential (Mật).....	17
Hình 1.7. Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa	17
Hình 1.8. Minh họa tính sẵn sàng: (a) không đảm bảo và (b) đảm bảo tính sẵn sàng	18
Hình 1.9. Các thành phần chính của an toàn thông tin [1]	19
Hình 1.10. Chu trình quản lý an toàn thông tin [2]	20
Hình 1.11. Chính sách an toàn thông tin và các thành phần của nó [2]	20
Hình 1.12. Bảy vùng trong hạ tầng CNTT theo mức kết nối mạng [2]	21
Hình 1.13. Đảm bảo ATTT cần cân bằng giữa mức An toàn, Chi phí và tính Hữu dụng	23
Hình 1.14. Mô hình đảm bảo an toàn thông tin với bảy lớp [28].....	24
Hình 1.15. Mô hình đảm bảo an toàn thông tin với ba lớp chính và các lớp con [29].....	24
Hình 2.1. Mô hình hệ điều hành Unix/Linux kèm theo các dịch vụ và ứng dụng	28
Hình 2.2. Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống năm 2014 [7].....	29
Hình 2.3. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng năm 2014 [7]	30
Hình 2.4. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng giai đoạn 2005-2019 [7].....	30
Hình 2.5. Top 20 hệ điều hành có lỗ hổng bảo mật phát hiện từ 2015 đến 2019 [7].....	31
Hình 2.6. Top 20 ứng dụng có lỗ hổng bảo mật phát hiện từ 2015 đến 2019 [7]	31
Hình 2.7. Các vùng bộ nhớ cấp cho chương trình.....	33
Hình 2.8. Một đoạn chương trình viết bằng C gồm một hàm chính và một hàm con.....	33
Hình 2.9. Các thành phần được lưu trong vùng bộ nhớ ngăn xếp.....	34
Hình 2.10. Cấp phát bộ nhớ cho các biến trong vùng bộ nhớ ngăn xếp	34
Hình 2.11. Đoạn chương trình C minh họa gây tràn bộ nhớ đệm trong ngăn xếp	35
Hình 2.12. Minh họa hiện tượng tràn bộ nhớ đệm (buffer) trong ngăn xếp.....	35
Hình 2.13. Một shellcode viết bằng hợp ngữ và chuyển thành chuỗi tấn công	36
Hình 2.14. Chèn và thực hiện shellcode khai thác lỗ tràn bộ đệm	36
Hình 2.15. Chèn shellcode với phần đệm bằng lệnh NOP (N)	36
Hình 2.16. Bản đồ lây nhiễm sâu Slammer (màu xanh đậm) theo trang www.caida.org vào ngày 25/1/2003 lúc 6g00 (giờ UTC) với 74.855 máy chủ bị nhiễm.....	37
Hình 2.17. Cung cấp dữ liệu có kích thước quá lớn gây lỗi cho ứng dụng.....	39
Hình 2.18. Báo cáo kết quả quét của Microsoft Baseline Security Analyzer	44
Hình 2.19. Màn hình tổng hợp kết quả quét lỗ hổng của Nessus Vulnerability Scanner	44
Hình 2.20. Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner	45
Hình 3.1. Giao diện của công cụ quét cổng Zenmap	50
Hình 3.2. Sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm.....	51
Hình 3.3. Mô đun Keylogger phần cứng và cài đặt trên máy tính để bàn.....	52
Hình 3.4. Form đăng nhập và đoạn mã xử lý xác thực người dùng	55
Hình 3.5. Form tìm kiếm sản phẩm và đoạn mã xử lý tìm sản phẩm	56
Hình 3.6. (a) Thủ tục bắt tay 3 bước của giao thức TCP và (b) Tấn công SYN Flood.....	60

Hình 3.7. Mô hình tấn công Smurf.....	61
Hình 3.8. Kiến trúc tấn công DDoS trực tiếp.....	63
Hình 3.9. Kiến trúc tấn công DDoS gián tiếp hay phản xạ	64
Hình 3.10. Minh họa quá trình tấn công giả mạo địa chỉ IP	65
Hình 3.11. Một mô hình tấn công nghe lén.....	66
Hình 3.12. Mô hình chung của tấn công kiểu người đứng giữa.....	66
Hình 3.13. Một kịch bản tấn công kiểu người đứng giữa	67
Hình 3.14. Một email phishing gửi cho khách hàng của mạng đấu giá eBay	69
Hình 3.15. Một email phishing gửi cho khách hàng của ngân hàng Royal Bank	70
Hình 3.16. Tấn công pharming “cướp” trình duyệt.....	71
Hình 3.17. Tấn công pharming thông qua tấn công vào máy chủ DNS.....	71
Hình 3.18. Phân loại các dạng phần mềm độc hại dựa trên phương pháp lây nhiễm	74
Hình 3.19. Chèn và gọi thực hiện mã vi rút trong chương trình	76
Hình 3.20. Một email do vi rút gửi đến người dùng	77
Hình 3.21. Một mô hình lây lan của sâu mạng	78
Hình 3.22. Bản đồ lây nhiễm sâu Code Red trên toàn thế giới.....	79
Hình 3.23. Mô hình mô hình giao tiếp giữa các thành phần trong botnet.....	79
Hình 3.24. Mô hình Hacker sử dụng các máy tính Zombie/Bot để gửi thư rác	80
Hình 3.25. Màn hình chính của Microsoft Windows Defender	82
Hình 4.1. Các khâu Mã hóa và Giải mã của một hệ mã hóa	86
Hình 4.2. Mã hóa khóa đối xứng sử dụng 1 khóa bí mật chia sẻ để mã hóa và giải mã	86
Hình 4.3. Mã hóa khóa bất đối xứng sử dụng một cặp khóa để mã hóa và giải mã	87
Hình 4.4. Minh họa thông điệp đầu vào và chuỗi băm đầu ra của hàm băm	87
Hình 4.5. Các thành phần của một hệ mã hóa đơn giản.....	88
Hình 4.6. Mô hình phương pháp mã hóa dòng	89
Hình 4.7. Mô hình phương pháp mã hóa khối	89
Hình 4.8. Mã hóa bằng hệ mã hóa Caesar.....	91
Hình 4.9. Phương pháp thay thế với 4 bộ mã thay thế	91
Hình 4.10. Phương pháp hoán vị thực hiện đổi chỗ các bit	92
Hình 4.11. Phương pháp hoán vị thực hiện đổi chỗ các ký tự	92
Hình 4.12. Ví dụ mã hóa bằng phương pháp XOR	92
Hình 4.13. Ví dụ mã hóa bằng phương pháp Vernam	93
Hình 4.14. Mô hình DES: các khâu mã hóa và giải mã	94
Hình 4.15. Thủ tục sinh các khóa phụ từ khóa chính của DES.....	95
Hình 4.16. Các bước xử lý chuyển khối rõ 64 bit thành khối mã 64 bit của DES	96
Hình 4.17. Các bước xử lý của hàm Feistel (F)	97
Hình 4.18. Mã hóa và giải mã với giải thuật 3-DES	98
Hình 4.19. Các bước xử lý mã hóa dữ liệu của AES	99
Hình 4.20. Thủ tục sinh khóa Rijndael.....	100
Hình 4.21. Hàm SubBytes sử dụng Rijndael S-box	101
Hình 4.22. Hàm ShiftRows	101
Hình 4.23. Hàm MixColumns	101
Hình 4.24. Hàm AddRoundKey	101
Hình 4.25. Quá trình mã hóa và giải mã trong AES	102
Hình 4.26. Mô hình nén dữ liệu của hàm băm	106
Hình 4.27. Phân loại các hàm băm theo khóa sử dụng	106

Hình 4.28. Mô hình tổng quát xử lý dữ liệu của hàm băm	107
Hình 4.29. Mô hình chi tiết xử lý dữ liệu của hàm băm	108
Hình 4.30. Lưu đồ xử lý một thao tác trong MD5	110
Hình 4.31. Lưu đồ một vòng xử lý của SHA1	111
Hình 5.1. Một hệ thống kiểm soát truy cập cửa hố trợ xác thực bằng vân tay.....	114
Hình 5.2. Ví dụ ma trận kiểm soát truy cập	116
Hình 5.3. Mô hình danh sách kiểm soát truy cập	117
Hình 5.4. Mô hình kiểm soát truy cập Bell-LaPadula.....	118
Hình 5.5. Một mô hình kiểm soát truy cập RBAC.....	120
Hình 5.6. Một số luật của tường lửa lọc gói tin	120
Hình 5.7. Giao diện kiểm tra thông tin của một chứng chỉ số khóa công khai	122
Hình 5.8. Thẻ thông minh tiếp xúc (a) và thẻ không tiếp xúc (b)	122
Hình 5.9. Một số thẻ bài (Token) của hãng RSA Security.....	123
Hình 5.10. Ví điện tử (một dạng thẻ bài) của cổng thanh toán trực tuyến Paypal	123
Hình 5.11. Hệ thống ApplePay tích hợp vào điện thoại di động	124
Hình 5.12. Xác thực dựa trên đặc điểm sinh trắc: (a) Khóa vân tay, (b) Khe xác thực vân tay trên máy tính xách tay và (c) Xác thực vân tay trên điện thoại Samsung	125
Hình 5.13. Quét võng mạc nhận dạng tròng mắt	125
Hình 5.14. Một tường lửa phần cứng chuyên dụng của hãng Cisco Systems.....	126
Hình 5.15. Các tường lửa bảo vệ mạng gia đình hoặc văn phòng nhỏ	126
Hình 5.16. Tường lửa bảo vệ các máy chủ dịch vụ.....	127
Hình 5.17. Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm	127
Hình 5.18. Các mô hình tường lửa: (a) Tường lửa lọc gói, (b) Cổng ứng dụng và (c) Cổng chuyển mạch.....	128
Hình 5.19. Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động.....	129
Hình 5.20. Vị trí các hệ thống IDS và IPS trong sơ đồ mạng	130
Hình 5.21. Mô hình các NIDS được triển khai để giám sát, phát hiện xâm nhập.....	132
Hình 5.22. Kiến trúc của Snort NIDS	132
Hình 5.23. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các máy	133
Hình 5.24. Các thành phần chính của OSSEC	133
Hình 5.25. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký.....	134
Hình 5.26. Giá trị entropy của IP nguồn của các gói tin từ lưu lượng hợp pháp (phần giá trị cao, đều) và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS (phần giá trị thấp)	135
Hình 6.1. Mô hình hệ thống quản lý an toàn thông tin theo chuẩn ISO 27001.....	139
Hình 6.2. Mô hình đánh giá rủi ro an toàn thông tin.....	139
Hình 6.3. Chu trình Plan-Do-Check-Act của ISO/IEC 27001:2005	148

DANH MỤC CÁC THUẬT NGỮ TIẾNG ANH VÀ VIỆT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
AES	Advanced Encryption Standard	Chuẩn mã hóa tiên tiến
APT	Advanced Persistent Threat	Tấn công có chủ đích
ATTT	Information Security	An toàn thông tin
CMND		Chứng minh nhân dân
CNTT	Information Technology	Công nghệ thông tin
ATM	Automatic Teller Machine	Máy giao dịch ngân hàng tự động
CD/DVD	Compact Disk/Digital Video Disk	Đĩa CD, DVD
CRC	Cyclic redundancy checks	Kiểm tra dư thừa vòng
CSDL	Database	Cơ sở dữ liệu
CSRF	Cross-Site Request Forgery	Tấn công giả mạo yêu cầu liên miề
DAC	Discretionary Access Control	Kiểm soát truy cập tùy chọn
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DNS	Domain Name System	Hệ thống tên miền
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DoS	Denial of Service	Tấn công từ chối dịch vụ
FTP	File Transfer Protocol	Giao thức truyền file
HTTP	HyperText Transfer Protocol	Giao thức truyền siêu văn bản
HTTT	Information System	Hệ thống thông tin
IDEA	International Data Encryption Algorithm	Giải thuật mã hóa dữ liệu quốc tế
ICMP	Internet Control Message Protocol	Giao thức điều khiển truyền thông điệp
IP	Internet Protocol	Giao thức Internet
IoT	Internet of Things	Internet vạn vật
IPSec	Internet Protocol Security	An toàn giao thức Internet
IRC	Internet Relay Chat	Giao thức IRC
ISS	Information systems security	An toàn hệ thống thông tin
LAN	Local Area Network	Mạng cục bộ
MAC	Mandatory Access Control	Kiểm soát truy cập bắt buộc
MAC	Message Authentication Code	Mã xác thực thông điệp (sử dụng hàm băm có khóa)
MD	Message Digest	Chuỗi đại diện thông điệp
MDC	Modification Detection Code	Mã phát hiện sự đổi (sử dụng hàm băm không khóa)
NSA	National Security Agency	Cơ quan mật vụ liên bang Hoa Kỳ
PGP	Pretty Good Privacy	Chuẩn bảo mật PGP
PIN	Personal Identification Number	Số nhận dạng cá nhân
PKI	Public Key Infrastructure	Hệ tầng khóa công khai

RBAC	Role-Based Access Control	Kiểm soát truy cập dựa trên vai trò
RSA	RSA Public Key Cryptosystem	Hệ mật khóa công khai RSA
SET	Secure Electronic Transactions	Các giao dịch điện tử an toàn
SHA	Secure Hash Algorithm	Giải thuật băm an toàn
SMTP	Simple Mail Transfer Protocol	Giao thức truyền thư điện tử đơn giản
SQL	Structured Query Language	Ngôn ngữ truy vấn có cấu trúc
SSH	Secure Shell	Vỏ an toàn
SSL/TLS	Secure Socket Layer/Transport Layer Security	Bộ giao thức bảo mật SSL / TLS
SSO	Single Sign On	Đăng nhập một lần
TCP	Transmission Control Protocol	Giao thức điều khiển truyền
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng
USB	Universal Serial Bus	Chuẩn phôi ghép USB
VPN	Virtual Private Network	Mạng riêng ảo
XSS	Cross-Site Scripting	Tấn công script liên miên
WAN	Wide Area Network	Mạng diện rộng
WLAN	Wireless Local Area Network	Mạng cục bộ không dây
	Computer & Data Security	An toàn máy tính và dữ liệu
	Computer-based Information System	HTTT dựa trên máy tính
	Computer Security	An toàn máy tính
	Cyber Security	An ninh không gian mạng
	Information Assurance	Đảm bảo thông tin
	Information Security Policy	Chính sách an toàn thông tin
	Information Technology Security	An toàn công nghệ thông tin
	Management of Information Security	Quản lý an toàn thông tin
	Network Security	An ninh mạng
	Risk Assessment	Đánh giá rủi ro
	Risk Management	Quản lý rủi ro
	Security Vulnerability	Lỗ hổng bảo mật
	System Weakness	Các điểm yếu hệ thống

MỞ ĐẦU

An toàn thông tin (Information security) là một lĩnh vực tương đối mới và được quan tâm trong vài thập kỷ gần đây và phát triển mạnh trong khoảng hơn một thập kỷ qua nhờ sự phát triển mạnh mẽ của mạng Internet và các dịch vụ mạng trên nền Internet. Tuy nhiên, do Internet ngày càng mở rộng và gần như không còn khái niệm biên giới quốc gia trong không gian mạng, các sự cố mất an toàn thông tin liên tục xảy ra. Đặc biệt, các dạng tấn công, xâm nhập vào các hệ thống máy tính và mạng xuất hiện ngày càng phổ biến với mức độ phá hoại ngày càng nghiêm trọng. Vấn đề đảm bảo an toàn cho thông tin, các hệ thống và mạng trở nên cấp thiết và là mối quan tâm của mỗi quốc gia, cơ quan, tổ chức và mỗi người dùng.

An toàn thông tin được định nghĩa là việc bảo vệ chống truy cập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép. Dưới một góc nhìn khác, an toàn thông tin là việc bảo vệ các thuộc tính, bao gồm tính bí mật, tính toàn vẹn và tính sẵn sàng của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải. An toàn thông tin có thể được chia thành ba phần chính: An toàn máy tính và dữ liệu, An ninh mạng và Quản lý an toàn thông tin.

Môn học Cơ sở an toàn thông tin là môn học cơ sở chuyên ngành trong chương trình đào tạo đại học các ngành An toàn thông tin và ngành Công nghệ thông tin (chuyên ngành An toàn thông tin mạng) của Học viện Công nghệ Bưu chính Viễn thông. Mục tiêu của môn học cung cấp cho sinh viên các khái niệm và nguyên tắc cơ bản về đảm bảo an toàn thông tin, an toàn máy tính, an toàn hệ thống thông tin và mạng; các nguy cơ và các lỗ hổng gây mất an toàn; các dạng tấn công, xâm nhập thường gặp; các dạng phần mềm độc hại; các kỹ thuật, giải pháp và công cụ phòng chống, đảm bảo an toàn thông tin, hệ thống và mạng; vấn đề quản lý an toàn thông tin, chính sách, pháp luật và đạo đức an toàn thông tin.

Với phạm vi là môn học cơ sở đầu tiên về an toàn thông tin, tác giả cố gắng trình bày những vấn đề cơ bản nhất phục vụ mục tiêu môn học. Nội dung của giáo trình này được biên soạn thành 6 chương với tóm tắt nội dung như sau:

Chương 1- Tổng quan về an toàn thông tin giới thiệu các khái niệm về an toàn thông tin, an toàn hệ thống thông tin và các yêu cầu đảm bảo an toàn thông tin, an toàn hệ thống thông tin. Chương 1 cũng đề cập các nguy cơ, rủi ro trong các vùng của hạ tầng công nghệ thông tin theo mức kết nối mạng. Phần cuối của chương giới thiệu mô hình tổng quát đảm bảo an toàn thông tin và an toàn hệ thống thông tin.

Chương 2- Các lỗ hổng bảo mật và các điểm yếu hệ thống trình bày các khái niệm về các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống, các dạng lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng. Chương này đi sâu phân tích cơ chế xuất hiện và khai thác các lỗ hổng tràn bộ đệm và lỗ hổng không kiểm tra đầu vào. Phần cuối của

chương đề cập vấn đề quản lý, khắc phục các lỗ hổng bảo mật, tăng cường khả năng đề kháng cho hệ thống và giới thiệu một số công cụ rà quét lỗ hổng bảo mật.

Chương 3- Các dạng tấn công và các phần mềm độc hại mô tả các dạng tấn công điển hình vào các hệ thống máy tính và mạng, bao gồm tấn công vào mật khẩu, tấn công nghe lén, người đứng giữa, tấn công DoS, DDoS, tấn công sử dụng các kỹ thuật xã hội, tấn công APT... Nửa cuối của chương đề cập đến các dạng phần mềm độc hại, gồm cơ chế lây nhiễm và tác hại của chúng. Kèm theo phần mô tả mỗi dạng tấn công, hoặc phần mềm độc hại, chương cung cấp các biện pháp, kỹ thuật phòng chống.

Chương 4 – Đảm bảo an toàn thông tin dựa trên mã hóa giới thiệu các khái niệm cơ bản về mật mã, hệ mã hóa, các phương pháp mã hóa. Phần tiếp theo của chương 4 trình bày một số giải thuật cơ bản của mã hóa khóa đối xứng (DES, 3-DES và AES), mã hóa khóa bất đối xứng (RSA) và các hàm băm (MD5 và SHA1).

Chương 5- Các kỹ thuật và công nghệ đảm bảo an toàn thông tin trình bày khái quát về kiểm soát truy cập, các cơ chế (mô hình) kiểm soát truy cập và một số công nghệ kiểm soát truy cập được sử dụng trên thực tế. Phần tiếp theo của chương 5 giới thiệu về tường lửa – một trong các kỹ thuật được sử dụng rất phổ biến trong đảm bảo an toàn cho hệ thống máy tính và mạng. Phần cuối của chương giới thiệu về các hệ thống phát hiện, ngăn chặn xâm nhập.

Chương 6 – Quản lý, chính sách và pháp luật an toàn thông tin giới thiệu một số khái niệm cơ bản trong quản lý an toàn thông tin, vấn đề đánh giá rủi ro an toàn thông tin và thực thi quản lý an toàn thông tin. Nội dung tiếp theo được đề cập trong chương là các chuẩn quản lý an toàn thông tin, trong đó giới thiệu một số chuẩn quan trọng của bộ chuẩn ISO/IEC 27000. Phần cuối của chương giới thiệu khái quát về các vấn đề chính sách, pháp luật và đạo đức an toàn thông tin.

Tài liệu được biên soạn dựa trên kinh nghiệm giảng dạy môn học Cơ sở an toàn thông tin trong nhiều năm của tác giả tại Học viện Công nghệ Bưu chính Viễn thông, kết hợp tiếp thu các đóng góp của đồng nghiệp và phản hồi từ sinh viên. Tài liệu có thể được sử dụng làm tài liệu học tập cho sinh viên hệ đại học các ngành An toàn thông tin và ngành Công nghệ thông tin (chuyên ngành An toàn thông tin mạng). Trong quá trình biên soạn, mặc dù tác giả đã rất cố gắng song không thể tránh khỏi có những thiếu sót. Tác giả rất mong muốn nhận được ý kiến phản hồi và các góp ý cho các thiếu sót, cũng như ý kiến về việc cập nhật, hoàn thiện nội dung của tài liệu.

Hà Nội, Tháng 3 năm 2020

Tác giả

TS. Hoàng Xuân Dậu

CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Chương 1 giới thiệu các khái niệm về an toàn thông tin, an toàn hệ thống thông tin và các yếu cầu đảm bảo an toàn thông tin, an toàn hệ thống thông tin. Chương này cũng đề cập các nguy cơ, rủi ro trong các vùng của hạ tầng công nghệ thông tin theo mức kết nối mạng. Phần cuối của chương 1 giới thiệu mô hình tổng quát đảm bảo an toàn thông tin và an toàn hệ thống thông tin.

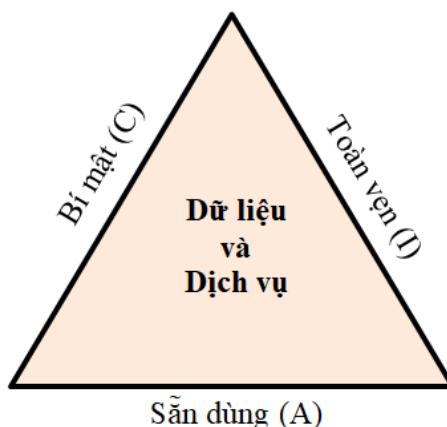
1.1. Khái quát về an toàn thông tin

An toàn thông tin là một lĩnh vực còn tương đối mới và phát triển mạnh trong những năm gần đây cùng với sự phát triển mạnh mẽ của mạng Internet và các thiết bị kết nối Internet, nhất là sự bùng nổ của các thiết bị di động như điện thoại thông minh. Mục này trước hết trình bày một số khái niệm cơ bản trong an toàn thông tin, bao gồm khái niệm an toàn thông tin, hệ thống thông tin, an toàn hệ thống thông tin và một số khái niệm cơ bản khác. Tiếp theo, mục phân tích các lý do của sự cần thiết của an toàn thông tin.

1.1.1. Một số khái niệm cơ bản

1.1.1.1. An toàn thông tin

An toàn thông tin là việc bảo vệ chống truy cập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép, theo cách hiểu trực tiếp¹. Định nghĩa một cách hình thức, an toàn thông tin là việc bảo vệ các thuộc tính *bí mật* (confidentiality), *toàn vẹn* (integrity) và *sẵn sàng* (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải [1][19]. Hình 1.1 biểu diễn *Tam giác CIA* với ba cạnh là ba thuộc tính cần bảo vệ nói trên của các tài sản thông tin, bao gồm Dữ liệu và Dịch vụ. Như vậy, có thể thấy bộ ba thuộc tính CIA là trái tim của an toàn thông tin. Tuy nhiên, một số ý kiến cho rằng, bộ ba CIA là chưa thực sự đầy đủ và cần bổ sung thêm các thuộc tính, như *xác thực* (authenticity) và *không chối bỏ* (non-repudiation)²; hoặc *xác thực* (authenticity), *hữu dụng* (utility) và *sở hữu* (possession)³.



Hình 1.1. *Tam giác CIA* (Confidentiality - Integrity - Availability) [1]

¹ Theo Viện SAN, Hoa Kỳ tại <https://www.sans.org/information-security/>

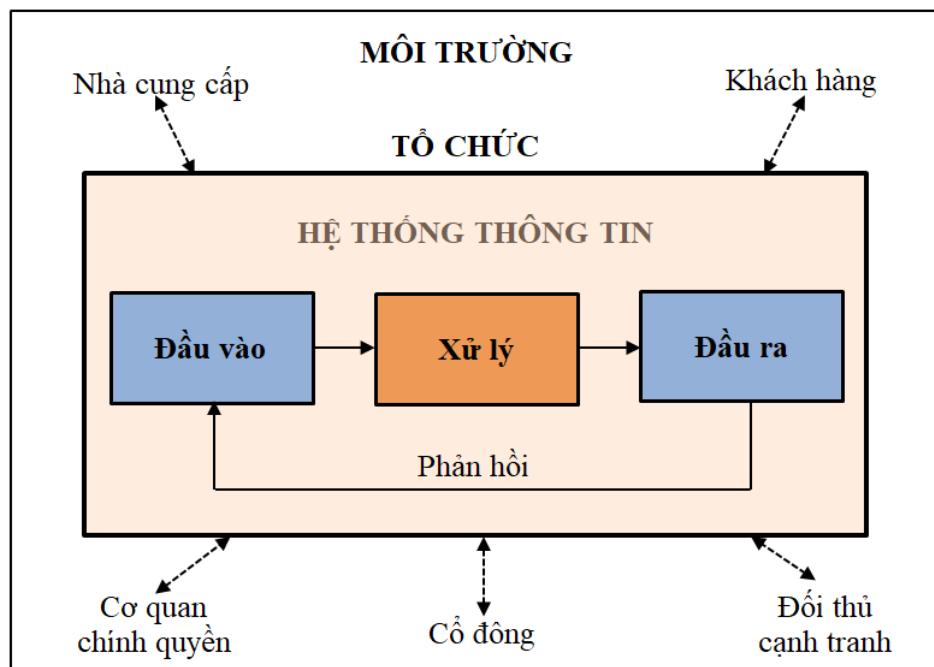
² Theo <http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

³ Theo <https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad>

An toàn thông tin gồm hai lĩnh vực chính là *An toàn công nghệ thông tin* và *Đảm bảo thông tin*. An toàn công nghệ thông tin, hay còn gọi là An toàn máy tính là việc đảm bảo an toàn cho các hệ thống công nghệ thông tin, bao gồm các hệ thống máy tính và mạng, chống lại các cuộc tấn công phá hoại. Theo một nhánh khác, đảm bảo thông tin là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố, như thiên tai, hỏng hóc, trộm cắp, phá hoại,... Đảm bảo thông tin thường được thực hiện sử dụng các kỹ thuật *sao lưu ngoại vi* (offsite backup), trong đó dữ liệu thông tin từ hệ thống gốc được sao lưu ra các hệ thống lưu trữ đặt ở một vị trí khác.

1.1.1.2. Hệ thống thông tin và an toàn hệ thống thông tin

Hệ thống thông tin là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, và chuyển giao thông tin, tri thức và các sản phẩm số [2] [19]. Trong nền kinh tế số, hệ thống thông tin đóng vai trò rất quan trọng trong hoạt động của các tổ chức, cơ quan và doanh nghiệp (gọi chung là tổ chức). Có thể nói, hầu hết các tổ chức đều sử dụng các hệ thống thông tin với các quy mô khác nhau để quản lý các hoạt động của mình. Hình 1.2 minh họa mô hình hệ thống thông tin của một tổ chức trong môi trường tương tác với các đối tượng có liên quan khác nhau. Trong mô hình này, mỗi hệ thống thông tin gồm ba thành phần chính: (i) Đầu vào là thành phần thu thập thông tin, (ii) Xử lý là thành phần xử lý thông tin và (iii) Đầu ra là thành phần kết xuất thông tin. Hệ thống thông tin được sử dụng để tương tác với khách hàng, với nhà cung cấp, với cơ quan chính quyền, với cổ đông và với đối thủ cạnh tranh. Có thể nêu ra một số hệ thống thông tin điển hình, như các hệ lập kế hoạch nguồn lực doanh nghiệp, các máy tìm kiếm và các hệ thống thông tin địa lý.

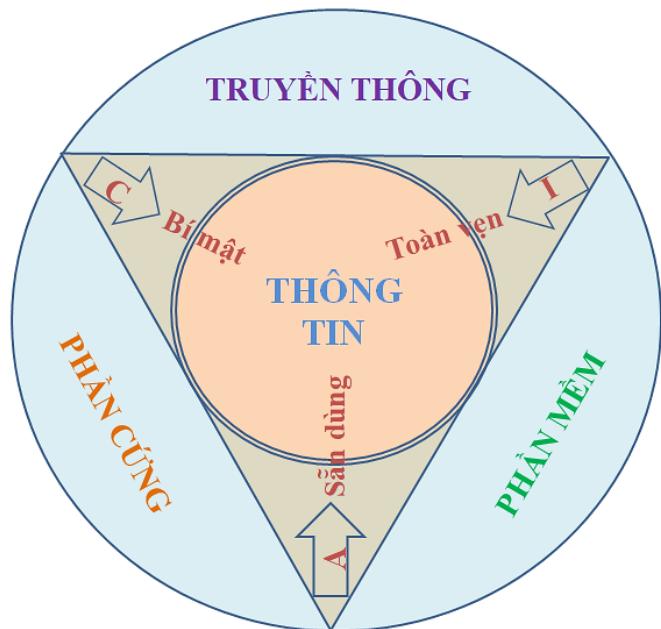


Hình 1.2. Mô hình hệ thống thông tin của cơ quan, tổ chức

Trong lớp các hệ thống thông tin, hệ thống thông tin dựa trên máy tính, hay sử dụng công nghệ máy tính để thực thi các nhiệm vụ là lớp hệ thống thông tin được sử dụng rộng rãi nhất. Hệ thống thông tin dựa trên máy tính thường gồm các thành phần

chính: (1) *phần cứng* để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu; (2) *phần mềm* chạy trên phần cứng để xử lý dữ liệu; và (3) *mạng/truyền thông* là hệ thống truyền dẫn thông tin/dữ liệu. Ngoài các thành phần trên, hệ thống thông tin dựa trên máy tính còn có thể gồm: *cơ sở dữ liệu* để lưu trữ dữ liệu và các *thủ tục* là tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.

An toàn hệ thống thông tin là việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin, bao gồm tính *bí mật*, tính *toàn vẹn* và tính *sẵn sàng* [1]. Hình 1.3 minh họa các thành phần cơ bản của Hệ thống thông tin dựa trên máy tính và An toàn hệ thống thông tin.



Hình 1.3. Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin

1.1.1.3. Một số khái niệm khác

Truy cập (Access)¹ là việc một chủ thể, người dùng hoặc một đối tượng có khả năng sử dụng, xử lý, sửa đổi, hoặc gây ảnh hưởng đến một chủ thể, người dùng hoặc một đối tượng khác. Trong khi người dùng hợp pháp có quyền truy cập hợp pháp đến một hệ thống thì kẻ tấn công truy cập bất hợp pháp đến hệ thống.

Tài sản (Asset) là tài nguyên của các tổ chức, cá nhân được bảo vệ. Tài sản có thể là tài sản lô gíc, như một trang web, thông tin, hoặc dữ liệu. Tài sản cũng có thể là tài sản vật lý, như hệ thống máy tính, thiết bị mạng, hoặc các tài sản khác.

Mối đe dọa (Threat)² là bất kỳ một hành động nào có thể gây hư hại đến một tài sản, bao gồm cả các tài sản lô gíc và các tài sản vật lý.

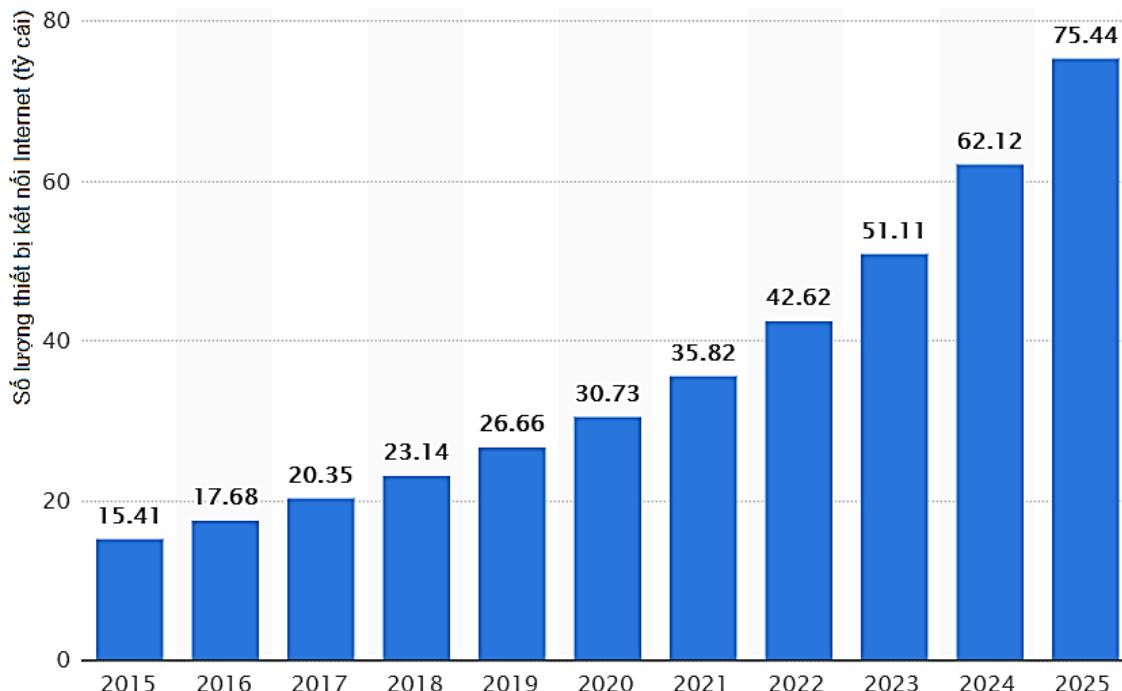
Tấn công (Attack) theo nghĩa tổng quát là một hành động có chủ ý hoặc không có chủ ý có khả năng gây hại, hoặc làm thỏa hiệp các thông tin, hệ thống và các tài sản được bảo vệ. Tấn công có thể thuộc dạng chủ động hoặc thụ động và có thể được thực hiện trực tiếp hoặc gián tiếp.

¹ Một số tài liệu sử dụng thuật ngữ Truy nhập.

² Một số tài liệu sử dụng thuật ngữ Hiểm họa.

1.1.2. Sự cần thiết của an toàn thông tin

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của các thiết bị di động, và đặc biệt là các thiết bị IoT, số lượng người dùng mạng Internet và số lượng thiết bị kết nối vào mạng Internet tăng trưởng nhanh chóng. Theo thống kê và dự báo của trang Statista [3] cho trên Hình 1.4, số lượng các thiết bị có kết nối Internet là khoảng 15 tỷ trong năm 2015, tăng lên hơn 26 tỷ vào năm 2019 và dự báo sẽ rất tăng mạnh lên trên 75 tỷ vào năm 2025. Các thiết bị IoT kết nối thông minh là nền tảng cho phát triển nhiều ứng dụng quan trọng trong các lĩnh vực của đời sống xã hội, như thành phố thông minh, cộng đồng thông minh, ngôi nhà thông minh, các ứng dụng giám sát và chăm sóc sức khỏe,...

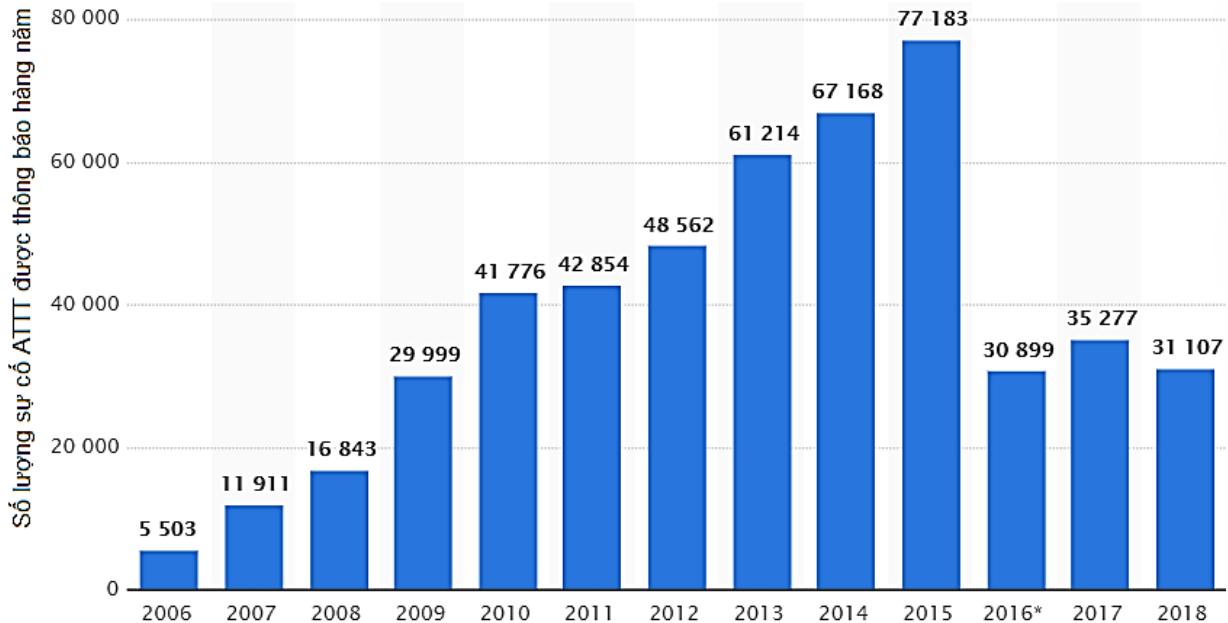


Hình 1.4. Số lượng các thiết bị IoT kết nối Internet từ 2015 đến 2025

Cùng với những lợi ích to lớn mà các thiết bị kết nối Internet mang lại, các sự cố mất an toàn thông tin đối với các hệ thống máy tính, điện thoại di động thông minh, các thiết bị IoT và người dùng cũng tăng vọt. Cũng theo số liệu thống kê của trang Statista cho trên Hình 1.5, số lượng các sự cố mất an toàn thông tin được thông báo bởi các cơ quan chính phủ Hoa Kỳ giai đoạn 2006-2015 tăng rất mạnh, từ 5.503 vụ vào năm 2006 lên đến 77.183 vụ vào năm 2015 [3]. Tuy nhiên, trong các năm 2016-2018, số lượng các sự cố mất an toàn thông tin đã giảm đáng kể và chỉ còn 31.107 vụ vào năm 2018.

Ở Việt Nam, trong báo cáo “*Tổng kết an ninh mạng năm 2019 và dự báo xu hướng 2020*” [5], Tập đoàn công nghệ Bkav cho biết 20.892 tỷ đồng (tương đương khoảng 902 triệu USD) là tổng thiệt hại ước tính do vi rút máy tính và các dạng mã độc khác gây ra đối với người dùng Việt Nam trong năm 2019, vượt xa mốc 14.900 tỷ đồng thiệt hại do vi rút máy tính và các dạng mã độc khác trong năm 2018. Dự báo trong năm 2020 và các năm tiếp theo, số lượng sự cố và thiệt hại do mất an toàn thông tin gây ra còn có thể lớn hơn nữa, do số lượng thiết bị kết nối tăng trưởng nhanh chóng và nguy cơ từ sự bùng phát mạnh của các phần mềm độc hại (mã độc tấn công APT sẽ tinh vi hơn, mã độc

không file (Fileless) sẽ là xu hướng chính, các loại mã độc botnet, các loại mã độc mã hóa tống tiền (ransomware), mã độc đào tiền ảo...) và các kỹ thuật tấn công, phá hoại ngày càng tinh vi.



Hình 1.5. Số lượng sự cố ATTT báo cáo bởi các cơ quan chính phủ Hoa Kỳ
giai đoạn 2006-2018 [3]

Từ các số liệu nêu trên có thể khẳng định, việc đảm bảo an toàn cho thông tin, máy tính, hệ thống mạng và các thiết bị kết nối khác là rất cần thiết bởi 2 lý do: (1) số lượng các thiết bị có kết nối Internet tăng nhanh chóng, đặc biệt là các thiết bị thông minh, IoT và (2) sự bùng phát của các dạng phần mềm độc hại, các dạng tấn công mạng trên diện rộng và các nguy cơ gây mất an toàn thông tin. Việc đảm bảo an toàn thông tin không chỉ cần thiết đối với các cá nhân, tổ chức, cơ quan, doanh nghiệp mà còn là vấn đề cấp thiết đối với an ninh quốc gia. Hơn nữa, việc xây dựng các giải pháp an toàn thông tin chỉ thực sự hiệu quả khi được thực hiện bài bản, đồng bộ, đảm bảo cân bằng giữa tính an toàn, tính hữu dụng của hệ thống và chi phí đầu tư cho các biện pháp đảm bảo an toàn.

1.2. Các yêu cầu đảm bảo an toàn thông tin

Như đã trình bày trong Mục 1.1, việc đảm bảo an toàn thông tin, hoặc hệ thống thông tin là việc đảm bảo ba thuộc tính an ninh, an toàn của thông tin, hoặc hệ thống, bao gồm tính bí mật, tính toàn vẹn và tính sẵn sàng. Đây cũng là ba yêu cầu cơ bản trong đảm bảo an toàn thông tin và hệ thống thông tin [1][2] [19]. Phần tiếp theo mô tả chi tiết về các yêu cầu kể trên.

1.2.1. Bí mật

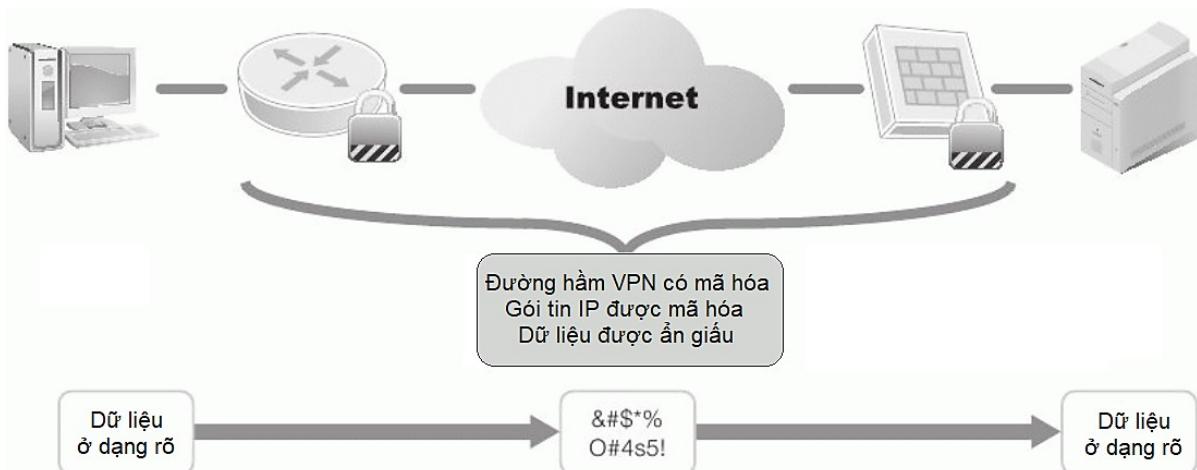
Tính bí mật đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy cập thông tin, hệ thống. Các thông tin bí mật có thể bao gồm: (i) dữ liệu riêng của cá nhân, (ii) các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan, tổ chức và (iii) các thông tin có liên quan đến an ninh của các quốc gia và các chính phủ. Hình 1.6

minh họa một văn bản được đóng dấu *Confidential* (Mật), theo đó chỉ những người có thẩm quyền mới được đọc và phổ biến văn bản.

Thông tin bí mật lưu trữ hoặc trong quá trình truyền tải cần được bảo vệ bằng các biện pháp phù hợp, tránh bị lộ lọt hoặc bị đánh cắp. Các biện pháp có thể sử dụng để đảm bảo tính bí mật của thông tin như bảo vệ vật lý, hoặc sử dụng mật mã. Hình 1.7 minh họa việc đảm bảo tính bí mật của thông tin truyền trên Internet bằng cách sử dụng đường hầm VPN dựa trên mã hóa.



Hình 1.6. Một văn bản được đóng dấu Confidential (Mật)



Hình 1.7. Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa

1.2.2. Toàn vẹn

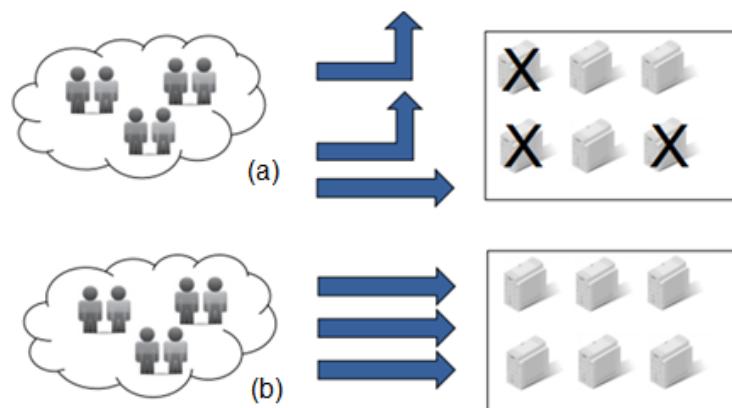
Tính toàn vẹn đảm bảo rằng thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ và chính xác của dữ liệu. Trong nhiều tổ chức, thông tin và dữ liệu có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế. Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin. Thông tin hoặc dữ liệu là toàn vẹn nếu nó đồng thời thỏa mãn ba điều kiện: (1) không bị thay đổi, (2) hợp lệ và (3) chính xác. Có nhiều biện pháp có thể sử dụng để đảm bảo, hoặc xác minh tính toàn vẹn của thông tin, hoặc dữ liệu, như sử dụng chữ ký số, hoặc các hàm băm mật mã.

1.2.3. Sẵn sàng

Tính sẵn sàng, hay sẵn dùng hoặc khả dụng đảm bảo rằng thông tin, hoặc hệ thống có thể truy cập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn sàng có thể được đo thông qua các yếu tố:

- Thời gian cung cấp dịch vụ (Uptime);
- Thời gian ngừng cung cấp dịch vụ (Downtime);
- Tỷ lệ phục vụ: $A = (\text{Uptime}) / (\text{Uptime} + \text{Downtime})$;
- Thời gian trung bình giữa các sự cố;
- Thời gian trung bình ngừng để sửa chữa;
- Thời gian khôi phục sau sự cố.

Hình 1.8 minh họa tính sẵn sàng của một hệ thống trong 2 trường hợp: (a) hệ thống không đảm bảo tính sẵn sàng khi có một số thành phần gặp sự cố (biểu diễn bằng biểu tượng có dấu X) do đó không có khả năng phục vụ tất cả các yêu cầu của người dùng (người dùng truy cập được dịch vụ biểu diễn bằng mũi tên thẳng “ \rightarrow ” người dùng không truy cập được dịch vụ biểu diễn bằng mũi tên đi ra “ \uparrow ”), và (b) hệ thống đảm bảo tính sẵn sàng khi tất cả các thành phần của nó hoạt động bình thường. Các biện pháp đảm bảo hoặc tăng cường tính sẵn sàng cho hệ thống có thể kể đến như: xây dựng hệ thống cung cấp dịch vụ dựa trên chuỗi cân bằng tải¹, hoặc nền tảng điện toán đám mây.



Hình 1.8. Minh họa tính sẵn sàng: (a) không đảm bảo và (b) đảm bảo tính sẵn sàng

1.3. Các thành phần của an toàn thông tin

An toàn thông tin có thể được chia thành ba thành phần chính: *An toàn máy tính và dữ liệu*, *An ninh mạng* và *Quản lý an toàn thông tin* [1]. Ba thành phần trên của an toàn thông tin có quan hệ mật thiết và giao thoa với nhau, trong đó phần chung của cả ba thành phần trên là *Chính sách an toàn thông tin*² như minh họa trên Hình 1.9. Phần tiếp theo mô tả chi tiết về các thành phần trên.

1.3.1. An toàn máy tính và dữ liệu

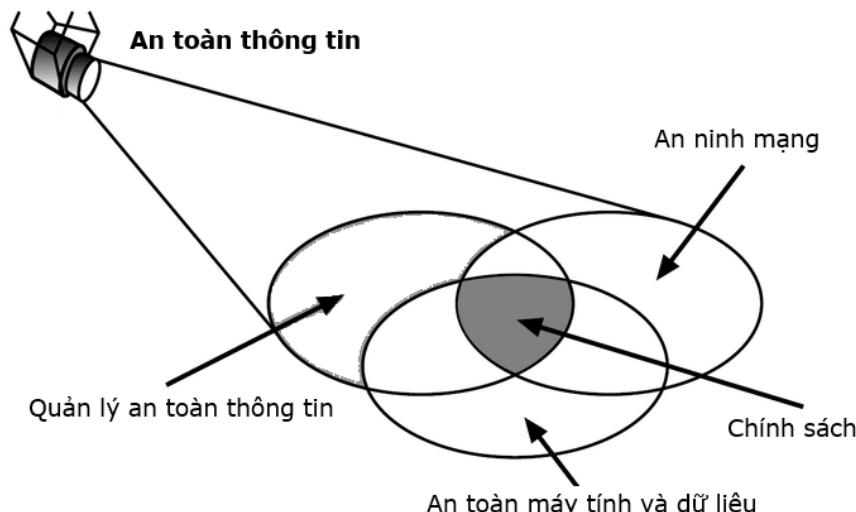
An toàn máy tính và dữ liệu (Computer and data security) là việc đảm bảo an toàn cho hệ thống phần cứng, phần mềm và dữ liệu trên máy tính; đảm bảo cho máy tính có thể

¹ Đọc thêm tại <https://docs.microsoft.com/en-us/windows-server/networking/technologies/network-load-balancing>

² Chính sách an toàn thông tin là phần chung do nó tồn tại trong cả 3 thành phần chính của an toàn thông tin.

vận hành an toàn, đáp ứng các yêu cầu của người sử dụng. An toàn máy tính và dữ liệu bao gồm các nội dung sau:

- Đảm bảo an toàn cho hệ điều hành, ứng dụng và dịch vụ;
- Vấn đề kiểm soát truy cập;
- Vấn đề mã hóa và bảo mật dữ liệu;
- Vấn đề phòng chống phần mềm độc hại;
- Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.



Hình 1.9. Các thành phần chính của an toàn thông tin [1]

1.3.2. An ninh mạng

An ninh mạng (Network security) là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các dạng tấn công, xâm nhập trái phép. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:

- Các tường lửa, proxy cho lọc gói tin và kiểm soát truy cập;
- Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- Vấn đề giám sát hoạt động của hệ thống mạng.

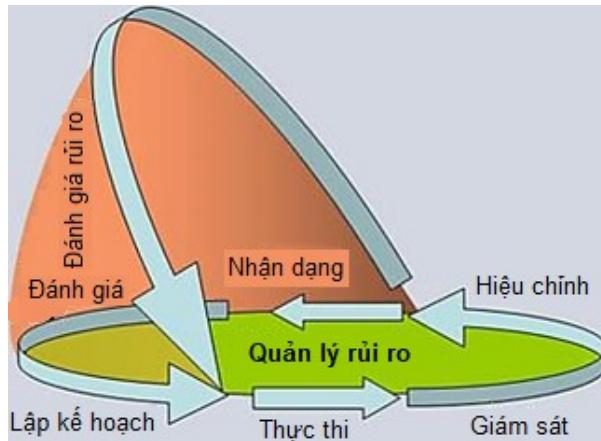
Trong bối cảnh mạng Internet toàn cầu phát triển mạnh mẽ và được sử dụng rộng rãi như hiện nay, thuật ngữ *An ninh không gian mạng* (Cyber security hoặc Cyberspace security) thường được sử dụng thay cho An ninh mạng. An ninh không gian mạng là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên không gian mở của mạng Internet, không bị giới hạn bởi biên giới quốc gia về mặt vật lý.

1.3.3. Quản lý an toàn thông tin

Quản lý an toàn thông tin (Information security management) là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Một trong các nội dung cốt lõi của quản lý an toàn thông tin là việc quản lý các rủi ro (Risk management), trong đó việc nhận dạng và đánh giá rủi ro (Risk identification

and assessment) đóng vai trò then chốt. Các nội dung khác của quản lý an toàn thông tin, bao gồm các chuẩn quản lý an toàn thông tin, chính sách an toàn thông tin và vấn đề đào tạo, nâng cao ý thức an toàn thông tin cho người dùng.

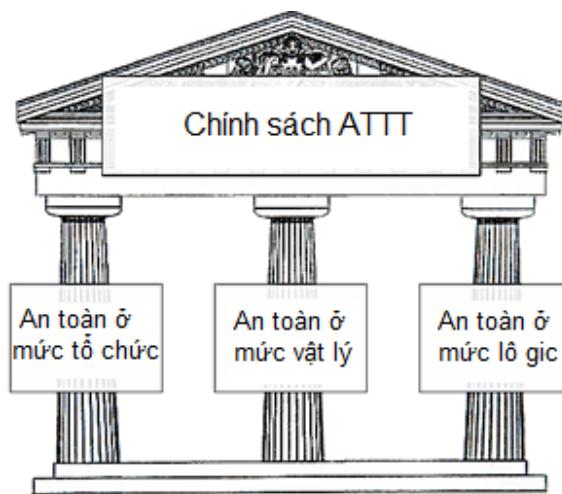
Việc thực thi quản lý an toàn thông tin cần được thực hiện theo chu trình lặp lại, từ khâu lập kế hoạch, thực thi kế hoạch, giám sát kết quả thực hiện và hiệu chỉnh các kiểm soát như minh họa trên Hình 1.10, do các điều kiện bên trong và bên ngoài hệ thống luôn thay đổi theo thời gian [2].



Hình 1.10. Chu trình quản lý an toàn thông tin [2]

1.3.4. Chính sách an toàn thông tin

Chính sách an toàn thông tin (Information security policy) là các nội quy, quy định của cơ quan, tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ đầy đủ [2]. Chính sách an toàn thông tin, như minh họa trên Hình 1.11 gồm 3 thành phần: (1) chính sách an toàn ở mức vật lý, (2) chính sách an toàn ở mức tổ chức và (3) chính sách an toàn ở mức lô gic.



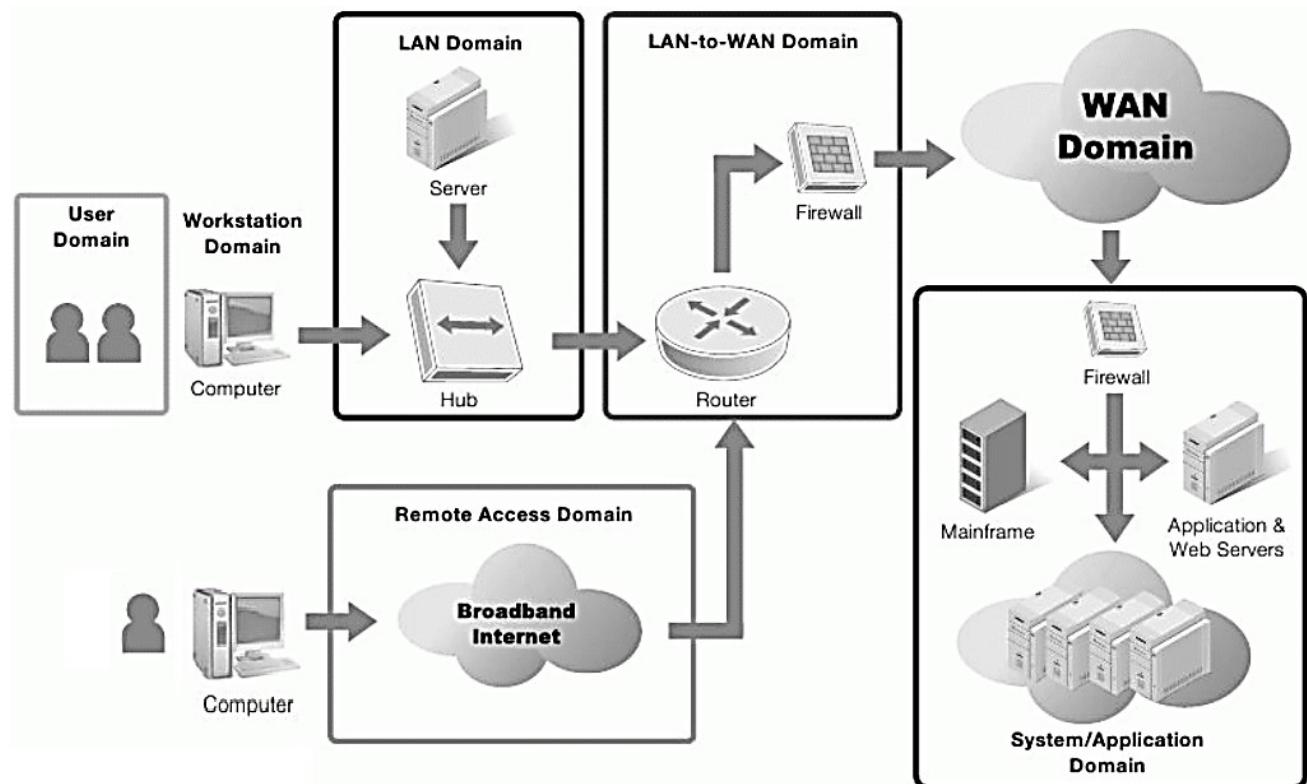
Hình 1.11. Chính sách an toàn thông tin và các thành phần của nó [2]

Một ví dụ về chính sách an toàn thông tin: để tăng cường an toàn cho hệ thống công nghệ thông tin, một tổ chức có thể áp dụng chính sách xác thực ‘mạnh’, trong đó sử dụng các đặc điểm sinh trắc, như xác thực sử dụng vân tay thay cho mật khẩu truyền thống cho hệ thống cửa ra vào trung tâm dữ liệu, hoặc đăng nhập vào hệ thống máy tính.

1.4. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

1.4.1. Bảy vùng trong cơ sở hạ tầng CNTT

Hạ tầng công nghệ thông tin của các tổ chức, cơ quan, doanh nghiệp có thể có quy mô lớn hay nhỏ khác nhau, nhưng thường gồm bảy vùng theo mức kết nối mạng như biểu diễn trên Hình 1.12 [2].



Hình 1.12. Bảy vùng trong hạ tầng CNTT theo mức kết nối mạng [2]

Theo đó, các vùng cụ thể gồm:

- Vùng người dùng (User domain) gồm người dùng hệ thống, bao gồm nhân viên và khách viếng thăm được cấp tài khoản truy cập vào hệ thống;
- Vùng máy trạm (Workstation domain) gồm các máy tính và các thiết bị tính toán được kết nối mạng LAN/WLAN;
- Vùng mạng LAN (LAN domain) gồm hệ thống kết nối mạng LAN/WLAN và các máy chủ nội bộ;
- Vùng LAN-to-WAN (LAN-to-WAN domain) gồm hệ thống kết nối mạng LAN/WLAN đến mạng WAN;
- Vùng mạng WAN (WAN domain) là vùng mạng điện rộng, hay mạng Internet toàn cầu;
- Vùng truy cập từ xa (Remote Access domain) gồm các công cụ hỗ trợ người dùng kết nối từ xa đến hệ thống CNTT của cơ quan, tổ chức thông qua mạng Internet; và
- Vùng hệ thống/ứng dụng (Systems/Application domain) gồm hệ thống máy chủ cung cấp các dịch vụ mạng, như máy chủ web, DNS, email và dịch vụ điện toán đám mây.

Do mỗi vùng nêu trên có đặc điểm khác nhau nên chúng có các mối đe dọa và nguy cơ mất an toàn thông tin khác nhau. Mục tiếp theo trình bày các mối đe dọa và nguy cơ đối với từng vùng.

1.4.2. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

Vùng người dùng

Có thể nói vùng người dùng là vùng có nhiều mối đe dọa và nguy cơ nhất do người dùng có bản chất khó đoán định và khó kiểm soát hành vi [2]. Các vấn đề thường gặp trong vùng người dùng bao gồm: thiếu ý thức, coi nhẹ vấn đề an ninh an toàn, vi phạm các chính sách an ninh an toàn; đura đĩa CD/DVD, thẻ nhớ USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép; phá hoại dữ liệu, ứng dụng và hệ thống; ngoài ra, các nhân viên bất mãn có thể tấn công hệ thống từ bên trong, hoặc nhân viên có thể tống tiền hoặc chiếm đoạt thông tin nhạy cảm, thông tin quan trọng.

Vùng máy trạm

Vùng máy trạm cũng có nhiều mối đe dọa và nguy cơ do vùng này tiếp xúc trực tiếp với vùng người dùng. Các mối đe dọa và nguy cơ thường gặp trong vùng máy trạm bao gồm: truy cập trái phép vào máy trạm, hệ thống, ứng dụng và dữ liệu; các lỗ hổng an ninh trong hệ điều hành, trong các phần mềm ứng dụng máy trạm; các hiểm họa từ vi rút, mã độc và các phần mềm độc hại khác. Ngoài ra, vùng máy trạm cũng chịu các nguy cơ do người dùng thực hiện các hành vi bị cấm, như đura đĩa CD/DVD, thẻ nhớ USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép.

Vùng mạng LAN

Các mối đe dọa và nguy cơ có thể có đối với vùng mạng LAN bao gồm: truy cập trái phép vào mạng LAN vật lý, truy cập trái phép vào hệ thống, ứng dụng và dữ liệu; các lỗ hổng an ninh trong hệ điều hành và các phần mềm ứng dụng máy chủ; nguy cơ từ người dùng giả mạo trong mạng WLAN; tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa do sóng mang thông tin của WLAN truyền trong không gian có thể bị nghe lén. Ngoài ra, các hướng dẫn và cấu hình chuẩn cho máy chủ trong mạng LAN nếu không được tuân thủ nghiêm ngặt sẽ dẫn đến những lỗ hổng an ninh mà kẻ tấn công có thể khai thác.

Vùng mạng LAN-to-WAN

Vùng mạng LAN-to-WAN là vùng chuyển tiếp từ mạng nội bộ ra mạng diện rộng, nên mối đe dọa và nguy cơ lớn nhất là kẻ tấn công từ mạng WAN có thể thăm dò và rà quét trái phép các cổng dịch vụ có thể dẫn đến nguy cơ truy cập trái phép. Ngoài ra, một nguy cơ khác cần phải xem xét là lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác.

Vùng mạng WAN

Vùng mạng WAN, hay mạng Internet là vùng mạng mở, trong đó hầu hết dữ liệu được truyền dưới dạng rõ, nên các mối đe dọa và nguy cơ lớn nhất là dễ bị nghe lén và dễ bị tấn công phá hoại, tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS).

Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm vi rút, sâu và các phần mềm độc hại đến người dùng tại các hệ thống đích.

Vùng truy cập từ xa

Trong vùng truy cập từ xa, các mối đe dọa và nguy cơ điển hình bao gồm: tấn công kiểu vét cạn vào tên người dùng và mật khẩu, tấn công vào hệ thống đăng nhập và kiểm soát truy cập; truy cập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu; các thông tin bí mật có thể bị đánh cắp từ xa; và vấn đề rò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.

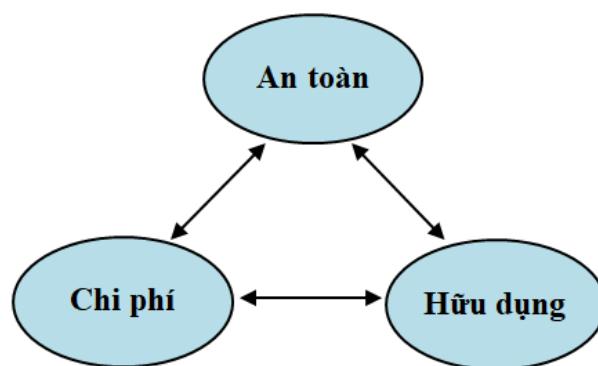
Vùng hệ thống và ứng dụng

Trong vùng hệ thống và ứng dụng, các mối đe dọa và nguy cơ có thể bao gồm: truy cập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp; các khó khăn trong quản lý các máy chủ với yêu cầu tính sẵn sàng cao; các lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ; các vấn đề an ninh trong các môi trường ảo của điện toán đám mây; và vấn đề hỏng hóc hoặc mất dữ liệu.

1.5. Mô hình tổng quát đảm bảo ATTT VÀ HTTT

1.5.1. Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng

Nguyên tắc chủ đạo xuyên suốt trong đảm bảo an toàn thông tin, hệ thống và mạng là *Phòng vệ nhiều lớp có chiều sâu* (Defense in depth)¹. Theo nguyên tắc này, ta cần tạo ra nhiều lớp bảo vệ, kết hợp tính năng, tác dụng của mỗi lớp để đảm bảo an toàn tối đa cho thông tin, hệ thống và mạng. Một lớp, một công cụ phòng vệ riêng rẽ dù có hiện đại, nhưng vẫn không thể đảm bảo an toàn. Do vậy, việc tạo ra nhiều lớp bảo vệ có khả năng bổ sung cho nhau là cách làm hiệu quả. Một điểm quan trọng khác cần lưu ý khi thiết kế và triển khai hệ thống đảm bảo an toàn cho thông tin, hệ thống và mạng là cần cân bằng giữa mức an toàn, chi phí và tính hữu dụng, như minh họa trên Hình 1.13. Hệ thống đảm bảo an toàn thông tin chỉ thực sự phù hợp và hiệu quả khi hệ thống được bảo vệ đạt mức an toàn phù hợp mà vẫn có khả năng cung cấp các tính năng hữu ích cho người dùng với chi phí cho đảm bảo an toàn phù hợp với giá trị của tài sản được bảo vệ.

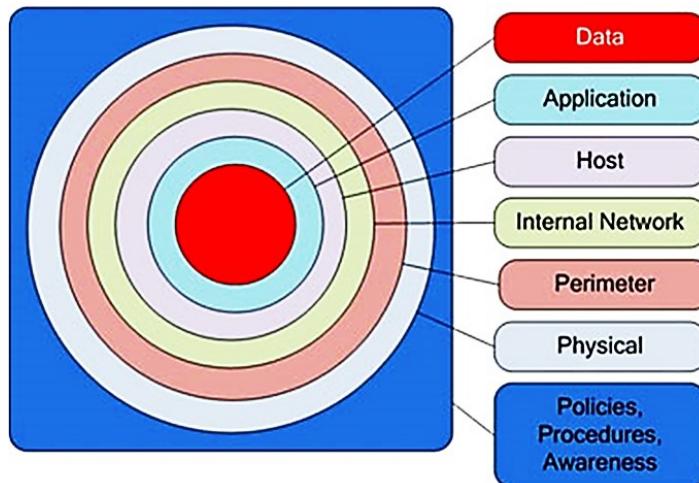


Hình 1.13. Đảm bảo ATTT cần cân bằng giữa mức An toàn, Chi phí và tính Hữu dụng

¹ Ngoài nguyên tắc phòng vệ nhiều lớp có chiều sâu được thừa nhận rộng rãi, một số nguyên tắc khác cũng được nghiên cứu ứng dụng như nguyên tắc bảo vệ tổng thể, nguyên tắc bảo vệ liên tục, nguyên tắc công khai thuật toán và cơ chế bảo vệ và nguyên tắc đơn giản trong sử dụng.

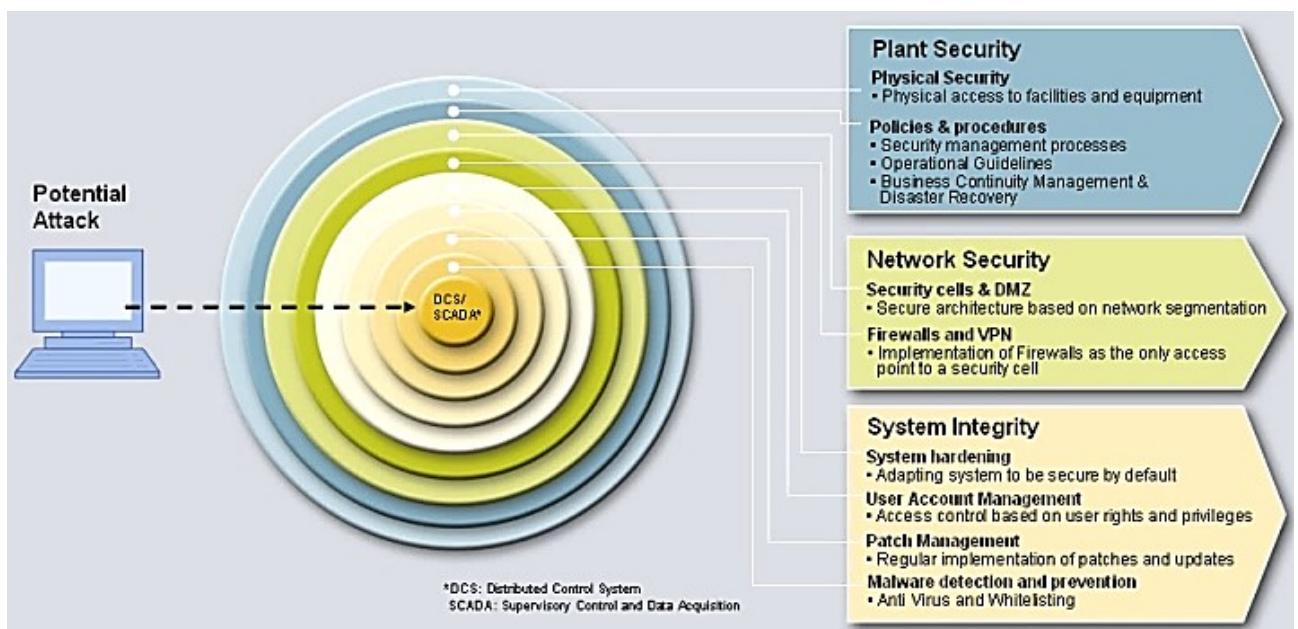
1.5.2. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

Hình 1.14 minh họa mô hình đảm bảo an toàn thông tin theo mức truy cập với 7 lớp bảo vệ, bao gồm lớp chính sách, thủ tục, ý thức (Policies, procedures, awareness); lớp vật lý (Physical); lớp ngoại vi (Perimeter); lớp mạng nội bộ (Internal network); lớp máy tính (Host); lớp ứng dụng (Application) và lớp dữ liệu (Data). Trong mô hình này, để truy cập được đến đối tượng đích là dữ liệu, kẻ tấn công cần phải vượt qua cả 7 lớp bảo vệ [28].



Hình 1.14. Mô hình đảm bảo an toàn thông tin với bảy lớp [28]

Cụ thể hơn, Hình 1.15 minh họa mô hình phòng vệ được triển khai gồm 3 lớp chính: lớp an ninh cơ quan/tổ chức (Plant Security), lớp an ninh mạng (Network Security) và lớp an ninh hệ thống (System Integrity) [29].



Hình 1.15. Mô hình đảm bảo an toàn thông tin với ba lớp chính và các lớp con [29]

Mỗi lớp chính trong mô hình này lại gồm một số lớp con như sau:

- Lớp an ninh cơ quan/tổ chức gồm 2 lớp con:
 - + Lớp bảo vệ vật lý (Physical Security) có nhiệm vụ kiểm soát các truy cập vật lý đến các trang thiết bị hệ thống và mạng.

- + Lớp chính sách & thủ tục (Policies & procedures) bao gồm các quy trình quản lý an toàn thông tin, các hướng dẫn vận hành, quản lý hoạt động liên tục và phục hồi sau sự cố.
- Lớp an ninh mạng gồm 2 lớp con:
 - + Lớp bảo vệ vùng hạn chế truy cập (Security cells and DMZ) cung cấp các biện pháp bảo vệ cho từng phân đoạn mạng.
 - + Lớp các tường lửa, mạng riêng ảo (Firewalls and VPN) được triển khai như điểm truy cập duy nhất đến một phân đoạn mạng.
- Lớp an ninh hệ thống gồm 4 lớp con:
 - + Lớp tăng cường an ninh hệ thống (System hardening) đảm bảo việc cài đặt và cấu hình các thành phần trong hệ thống đảm bảo các yêu cầu an toàn.
 - + Lớp quản trị tài khoản người dùng (User Account Management) thực hiện kiểm soát truy cập dựa trên quyền truy cập và các đặc quyền của người dùng.
 - + Lớp quản lý các bản vá (Patch Management) có nhiệm vụ định kỳ cài đặt các bản vá an ninh và các bản cập nhật cho hệ thống.
 - + Lớp phát hiện và ngăn chặn phần mềm độc hại (Malware detection and prevention) có nhiệm vụ bảo vệ hệ thống, chống vi rút, sâu và các phần mềm độc hại khác.

1.6. Kết chương

Chương này đã trình bày khái quát về an toàn thông tin và an toàn hệ thống thông tin. Cụ thể, chương đã đề cập các vấn đề sau:

- Nêu các khái niệm cơ bản về an toàn thông tin, hệ thống thông tin, an toàn hệ thống thông tin và một số khái niệm khác trong an toàn thông tin như truy cập, tài sản, mối đe dọa...
- Phân tích 2 lý do dẫn đến sự cần thiết của an toàn thông tin.
- Trình bày chi tiết 3 yêu cầu cơ bản trong đảm bảo an toàn thông tin và hệ thống thông tin.
- Mô tả các thành phần chính của an toàn thông tin.
- Mô tả các vùng trong hạ tầng công nghệ thông tin và các mối đe dọa, nguy cơ trong từng vùng.
- Trình bày mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin.

1.7. Câu hỏi ôn tập

- 1) An toàn thông tin là gì?
- 2) Tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống?
- 3) Đảm bảo thông tin thường được thực hiện bằng cách nào? Cho ví dụ minh họa.
- 4) Hệ thống thông tin là gì? Nêu vai trò của các thành phần trong một hệ thống thông tin điển hình.

- 5) An toàn hệ thống thông tin là gì? Vẽ mô hình hệ thống thông tin kết hợp với an toàn hệ thống thông tin.
- 6) Nêu 3 yêu cầu cơ bản đảm bảo an toàn thông tin và hệ thống thông tin. Liệt kê các biện pháp, kỹ thuật cơ bản có thể được sử dụng để đảm bảo mỗi yêu cầu.
- 7) Ngoài 3 yêu cầu cơ bản đảm bảo an toàn thông tin và hệ thống thông tin, hãy khảo sát tài liệu bổ sung và mô tả các yêu cầu khác, hoặc bổ sung trong đảm bảo an toàn thông tin và hệ thống thông tin.
- 8) An toàn thông tin gồm những thành phần cơ bản nào? Mô tả văn tắt chức năng của mỗi thành phần.
- 9) An ninh không gian mạng (Cyber security) có điểm gì khác biệt so với An ninh mạng (Network security)? Khảo sát tài liệu và mô tả các thành phần của an ninh không gian mạng.
- 10) Nêu các mối đe dọa và nguy cơ trong vùng người dùng và vùng máy trạm trong hạ tầng CNTT. Tại sao nói vùng người dùng là vùng có nhiều mối đe dọa và nguy cơ nhất?
- 11) Nêu các mối đe dọa và nguy cơ trong vùng mạng LAN, LAN-to-WAN và vùng mạng WAN trong hạ tầng CNTT. Tại sao vùng mạng WAN thường có nguy cơ bị tấn công phá hoại cao?
- 12) Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là gì? Tại sao cần phải cân bằng giữa tính hữu dụng, chi phí và mức an toàn khi thiết kế và triển khai hệ thống đảm bảo an toàn thông tin?
- 13) Mô tả một mô hình nhiều lớp cho đảm bảo an toàn thông tin và hệ thống thông tin.
- 14) So sánh 2 mô hình đảm bảo an toàn thông tin đa lớp trên các Hình 1.14 và Hình 1.15. Lập một bảng ánh xạ tương đương về chức năng giữa các lớp bảo vệ trong 2 mô hình.

CHƯƠNG 2. LỖ HỒNG BẢO MẬT VÀ ĐIỂM YẾU HỆ THỐNG

Chương 2 giới thiệu các khái niệm về lỗ hổng bảo mật và điểm yếu tồn tại trong hệ thống, các dạng lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng. Chương đi sâu phân tích cơ chế xuất hiện và khai thác các lỗ hổng tràn bộ đệm và lỗ hổng không kiểm tra đầu vào. Phần cuối của chương đề cập vấn đề quản lý, khắc phục các lỗ hổng bảo mật, tăng cường khả năng đề kháng cho hệ thống và giới thiệu một số công cụ rà quét phát hiện các lỗ hổng bảo mật.

2.1. Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Các lỗ hổng bảo mật và điểm yếu tồn tại trong hệ thống máy tính nói riêng và hệ thống mạng nói chung là vấn đề đã và đang được quan tâm, đặc biệt trong môi liên hệ mật thiết với vấn đề nóng hiện nay là đảm bảo an toàn cho thông tin, hệ thống và mạng. Mục này trước hết mô tả khái quát các thành phần của một hệ thống máy tính làm cơ sở cho phân tích về điểm yếu và lỗ hổng. Tiếp theo là phần trình bày về các khái niệm như điểm yếu hệ thống và lỗ hổng bảo mật và một số thông kê về lỗ hổng bảo mật.

2.1.1. Khái quát

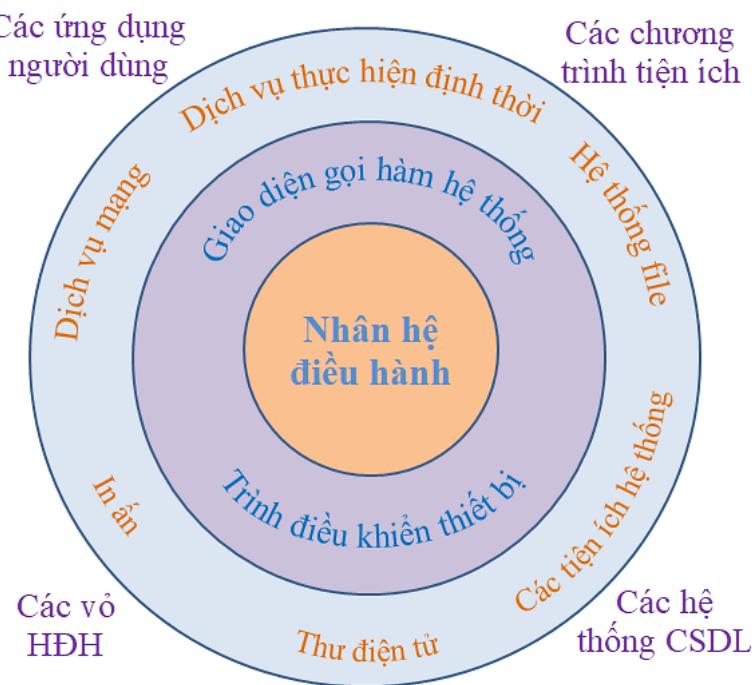
2.1.1.1. Các thành phần của hệ thống

Một hệ thống máy tính gồm 2 thành phần cơ bản là hệ thống phần cứng và hệ thống phần mềm. Hệ thống phần cứng bao gồm các mô đun phần cứng tạo nên máy tính vật lý, bao gồm CPU, ROM, RAM, Bus,...; các giao diện ghép nối và các thiết bị ngoại vi, như bàn phím, màn hình, ổ đĩa,... và các giao diện ghép nối mạng LAN, WLAN,...

Hệ thống phần mềm bao gồm hệ điều hành và các phần mềm ứng dụng. Hệ điều hành cung cấp môi trường làm việc cho các ứng dụng và giao diện người dùng. Hệ điều hành được cấu thành từ nhân hệ điều hành, các trình điều khiển thiết bị, các trình quản lý tiến trình, quản lý file, cung cấp dịch vụ, tiện ích,... Các phần mềm ứng dụng là các chương trình cung cấp các tính năng hữu ích cho người dùng, bao gồm các dịch vụ (máy chủ web, cơ sở dữ liệu...), trình duyệt web, các ứng dụng giao tiếp, các bộ ứng dụng văn phòng, các công cụ lập trình, phát triển phần mềm... Hình 2.1 minh họa mô hình hệ điều hành Unix/Linux, các dịch vụ, ứng dụng. Theo đó, lớp trong cùng là nhân hệ điều hành, tiếp theo là lớp giao diện lời gọi hàm hệ thống và các trình điều khiển thiết bị, kế tiếp là lớp các dịch vụ và tiện ích hệ thống và ngoài cùng là lớp các ứng dụng người dùng.

2.1.1.2. Điểm yếu hệ thống và lỗ hổng bảo mật

Trên thực tế, gần như không có hệ thống nào là hoàn hảo, không có điểm yếu, hoặc khiếm khuyết. Các hệ thống máy tính, hoặc hệ thống thông tin là các hệ thống rất phức tạp, được cấu thành từ nhiều thành phần phần cứng, phần mềm, do vậy chúng luôn tồn tại các lỗi, các khiếm khuyết, hay các điểm yếu. Các điểm yếu có thể tồn tại trong các mô đun phần cứng cũng như trong các mô đun phần mềm. Nhìn chung, các hệ thống càng phức tạp, có nhiều thành phần với nhiều tính năng thì khả năng xuất hiện các lỗi và điểm yếu càng tăng.



Hình 2.1. Mô hình hệ điều hành Unix/Linux kèm theo các dịch vụ và ứng dụng

Các điểm yếu hệ thống là các lỗi hay các khuyết khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, lỗi cấu hình hoạt động. Các điểm yếu có thể tồn tại trong cả các mô đun phần cứng và các mô đun phần mềm. Một số điểm yếu được phát hiện và đã được khắc phục. Tuy nhiên, cũng có những điểm yếu được phát hiện nhưng chưa được khắc phục, hoặc các điểm yếu chưa được phát hiện, hoặc chỉ tồn tại trong một điều kiện đặc biệt nào đó.

Lỗ hổng bảo mật là một điểm yếu tồn tại trong hệ thống cho phép kẻ tấn công khai thác gây tổn hại đến các thuộc tính an toàn, an ninh của hệ thống đó, bao gồm tính bí mật, tính toàn vẹn và tính sẵn sàng. Phụ thuộc vào khả năng bị khai thác, các lỗ hổng bảo mật có mức độ nghiêm trọng khác nhau. Theo Microsoft, có 4 mức độ nghiêm trọng của các lỗ hổng bảo mật: *nguy hiểm* (critical), *quan trọng* (important), *trung bình* (moderate) và *thấp* (low). Tuy nhiên, một số tổ chức khác chỉ phân loại các lỗ hổng bảo mật theo 3 mức độ nghiêm trọng: *cao* (high), *trung bình* (medium) và *thấp* (low).

Lỗ hổng bảo mật thuộc *cấp độ nguy hiểm* là lỗ hổng cho phép kẻ tấn công thực hiện mã khai thác mà không cần tương tác người dùng. Các thông tin khai thác lỗ hổng, như mã mẫu¹ khai thác tồn tại phổ biến trên mạng Internet. Ngoài ra, việc khai thác lỗ hổng có thể được thực hiện dễ dàng mà không yêu cầu có tài khoản trong hệ thống hoặc các điều kiện phức tạp. Ví dụ như một số lỗ hổng tràn bộ đệm thuộc cấp độ nguy hiểm do có thể bị khai thác bởi sâu mạng hoặc email chứa vi rút, mã độc. Các lỗ hổng loại nguy hiểm cần được khắc phục ngay hoặc càng sớm càng tốt.

Lỗ hổng bảo mật thuộc *cấp độ quan trọng* là lỗ hổng khi bị khai thác có thể dẫn đến vi phạm các yêu cầu an toàn thông tin như bí mật, toàn vẹn và sẵn sàng của dữ liệu, tài nguyên tính toán, hoặc cả hệ thống. Khác với lỗ hổng loại nguy hiểm, lỗ hổng loại quan

¹ Mã mẫu là các đoạn mã ví dụ dùng để hướng dẫn khai thác các lỗ hổng bảo mật đã biết tồn tại trong hệ thống.

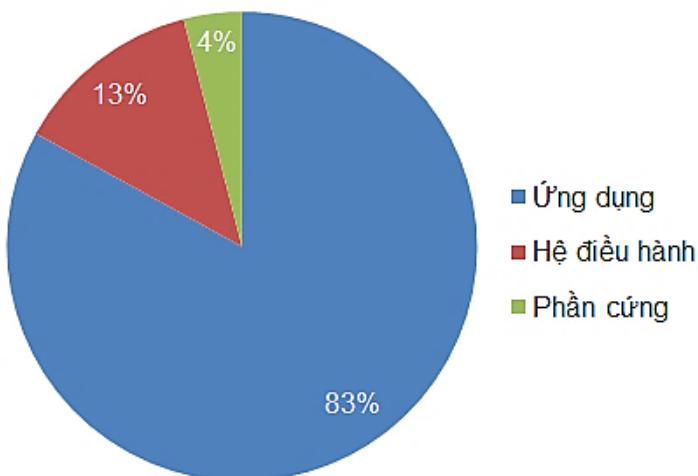
trọng cho phép kẻ tấn công thực hiện mã khai thác, nhưng cần có tương tác người dùng. Ví dụ vi rút hoặc các phần mềm độc hại cần tương tác người dùng để lây lan, như sao chép các file qua thẻ nhớ USB, mở email đính kèm, thực thi mã độc,... Các lỗ hổng loại quan trọng cũng cần được khắc phục càng sớm càng tốt.

Lỗ hổng bảo mật thuộc *cấp độ trung bình* là các lỗ hổng mà khi khai thác, kẻ tấn công phải ở trong cùng mạng cục bộ với hệ thống nạn nhân. Một ngữ cảnh khai thác lỗ hổng loại này là kẻ tấn công thực hiện việc bẫy nạn nhân sử dụng các kỹ thuật xã hội, như khai thác sự cẩn thận, tò mò và lòng tham của người dùng. Ngoài ra, việc khai thác lỗ hổng loại trung bình cũng chỉ cho phép kẻ tấn công có quyền truy cập rất hạn chế vào hệ thống. Với lỗ hổng loại trung bình, cần xem xét khắc phục sớm nhất hoặc định kỳ để hạn chế ảnh hưởng.

Loại cuối cùng là các lỗ hổng bảo mật thuộc *cấp độ thấp*. Các lỗ hổng loại này ít có ảnh hưởng đến hoạt động của tổ chức và chúng chỉ có thể bị khai thác khi kẻ tấn công có truy cập cục bộ hoặc truy cập vật lý trực tiếp vào hệ thống. Mặc dù mức rủi ro thấp, các lỗ hổng loại này vẫn cần được xem xét khắc phục định kỳ để hạn chế ảnh hưởng.

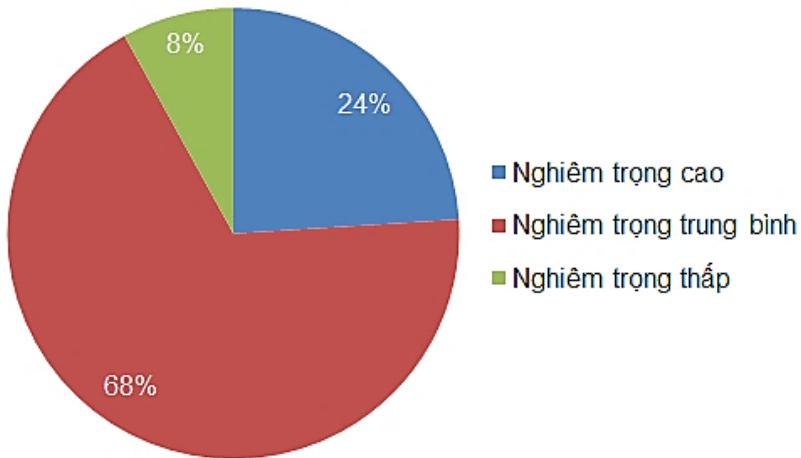
2.1.2. Một số thống kê về lỗ hổng bảo mật

Theo số liệu thống kê từ Cơ sở dữ liệu lỗ hổng quốc gia Hoa Kỳ [7], trong năm 2014, phân bố lỗ hổng bảo mật được phát hiện trên các thành phần của hệ thống lần lượt là phần cứng – 4%, hệ điều hành – 13% và phần mềm ứng dụng – 83%, như minh họa trên Hình 2.2. Như vậy, có thể thấy các lỗ hổng bảo mật chủ yếu xuất hiện trong hệ thống phần mềm và phần lớn tồn tại trong các phần mềm ứng dụng.

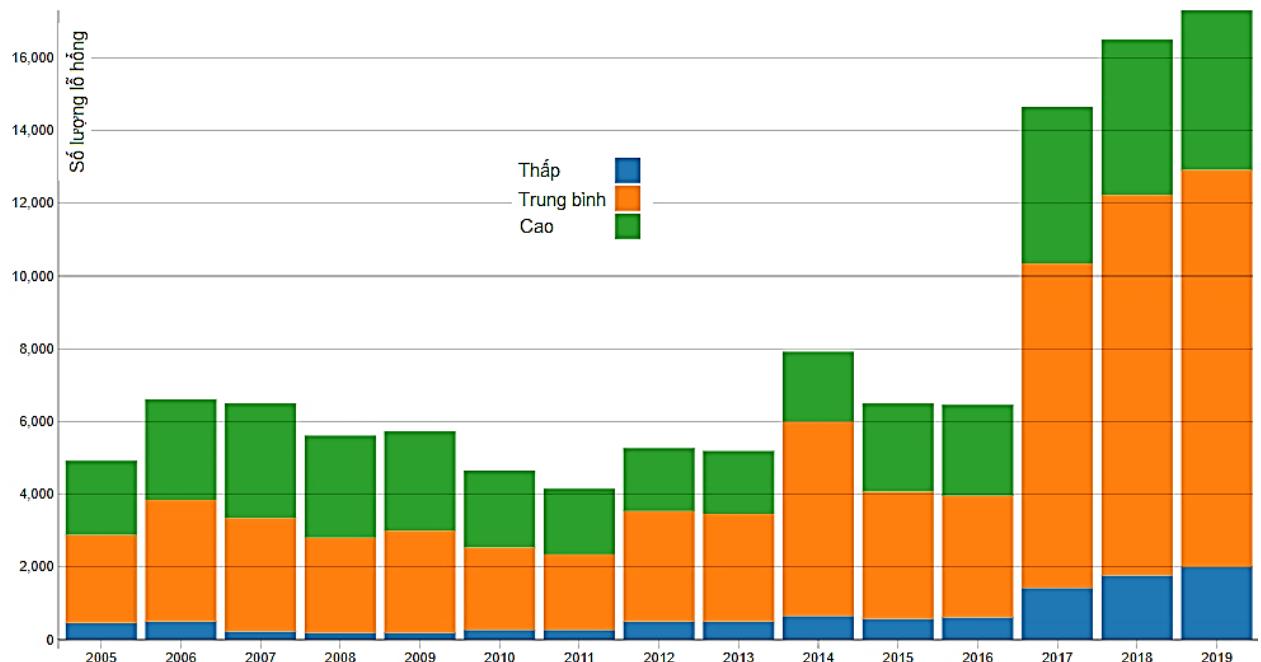


Hình 2.2. Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống năm 2014 [7]

Theo mức độ nghiêm trọng của các lỗ hổng bảo mật hệ thống minh họa trên Hình 2.3, trong năm 2014 các lỗ hổng có mức độ nghiêm trọng cao chiếm 24%, các lỗ hổng có mức độ nghiêm trọng trung bình chiếm 68% và các lỗ hổng có mức độ nghiêm trọng thấp chỉ chiếm 8%. Theo thống kê rộng hơn trong giai đoạn 2005-2019 cho trên Hình 2.4 [7], các lỗ hổng có mức độ nghiêm trọng cao và mức độ nghiêm trọng trung bình luôn chiếm đa số. Như vậy, ta có thể thấy, đa số các lỗ hổng bảo mật có mức độ nghiêm trọng từ trung bình trở lên và cần được xem xét khắc phục càng sớm càng tốt.



Hình 2.3. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng năm 2014 [7]

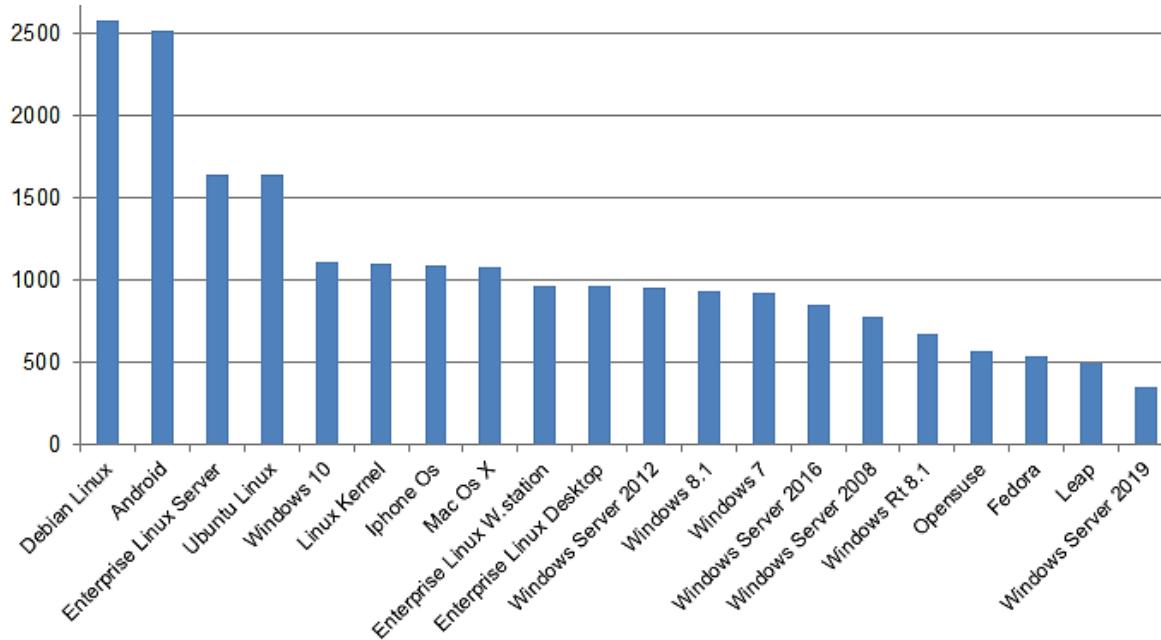


Hình 2.4. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng giai đoạn 2005-2019 [7]

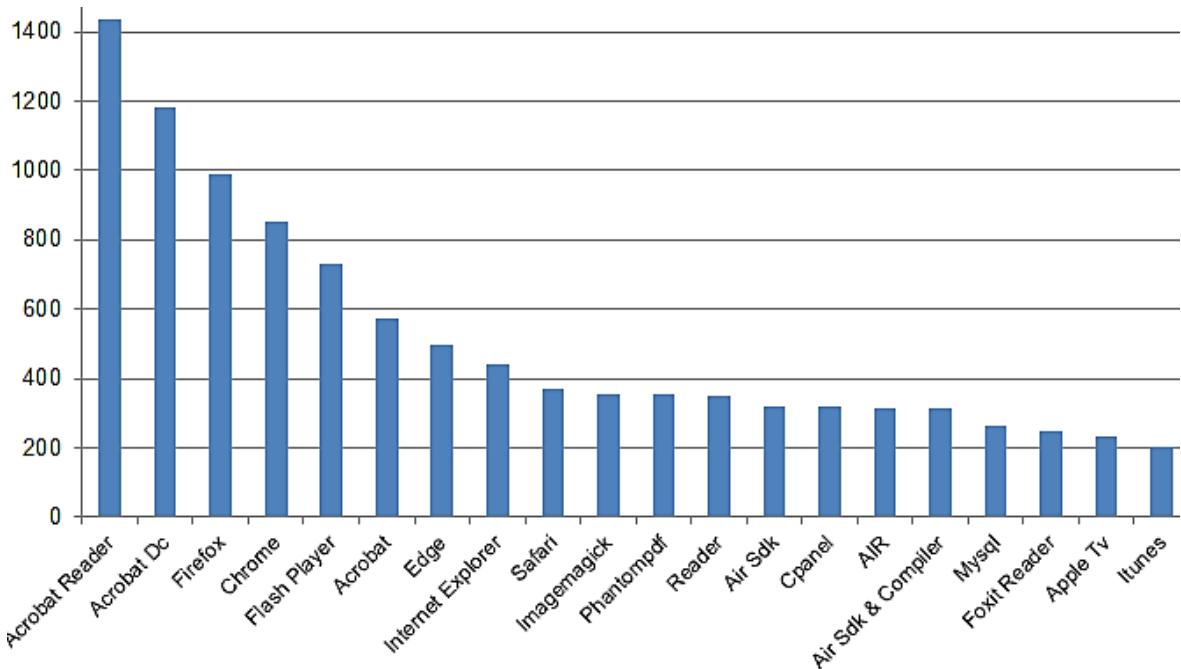
Hình 2.5 cung cấp số liệu thống kê về top 20 hệ điều hành có các loại lỗ hổng bảo mật được phát hiện trong 5 năm từ 2015 đến 2019 [7]. Theo đó, các hệ điều hành thuộc dòng Debian Linux và Google Android cho các thiết bị di động và IoT có số lỗ hổng được phát hiện cao nhất với trên 2500 trường hợp. Sở dĩ có điều này là do số lượng các thiết bị di động và IoT chạy hệ điều hành gốc Linux đã và đang tăng trưởng rất mạnh trong những năm gần đây. Xếp sau Debian Linux và Google Android là các hệ điều hành khác gốc Linux gồm Enterprise Linux Server và Ubuntu Linux với trên 1600 lỗ hổng được phát hiện do các bản Linux và đặc biệt là Ubuntu Linux được sử dụng ngày càng rộng rãi. Hệ điều hành phổ biến cho máy tính để bàn và máy tính xách tay - Microsoft Windows 10 đứng thứ 5 với trên 1000 lỗ hổng được phát hiện.

Tương tự, Hình 2.6 cung cấp số liệu thống kê về top 20 ứng dụng có các loại lỗ hổng bảo mật được phát hiện trong 5 năm từ 2015 đến 2019 [7]. Theo đó, các sản phẩm của hãng Adobe chiếm 3 vị trí trong top 5 ứng dụng có số lượng lỗ hổng được phát hiện cao

nhất, bao gồm Acrobat Reader, Acrobat Dc và Flash Player với lần lượt 1434, 1181 và 728 lỗ hổng. Có thể thấy các trình duyệt web, gồm Firefox, Chrome, Edge, Internet Explorer và Safari là những ứng dụng có số lượng lỗ hổng bảo mật được phát hiện rất cao khi có chiếm 5 vị trí trong top 10 ứng dụng có số lượng lỗ hổng bảo mật được phát hiện cao nhất.



Hình 2.5. Top 20 hệ điều hành có lỗ hổng bảo mật phát hiện từ 2015 đến 2019 [7]



Hình 2.6. Top 20 ứng dụng có lỗ hổng bảo mật phát hiện từ 2015 đến 2019 [7]

2.2. Các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng

Nhu đã đề cập trong mục 2.1, trên thực tế các lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng chiếm hơn 95% số lượng lỗ hổng bảo mật được phát hiện cho thấy mức độ phổ biến của các lỗ hổng bảo mật trong hệ thống phần mềm. Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng bao gồm:

- Lỗi tràn bộ đệm (Buffer overflow);
- Lỗi không kiểm tra đầu vào (Unvalidated input);
- Các vấn đề với kiểm soát truy cập (Access-control problems);
- Các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (Weaknesses in authentication, authorization, or cryptographic practices); và
- Các lỗ hổng bảo mật khác.

Phần tiếp theo của mục này trình bày chi tiết về từng dạng điểm yếu, lỗi và lỗ hổng bảo mật kể trên.

2.2.1. Lỗi tràn bộ đệm

2.2.1.1. Giới thiệu

Lỗi tràn bộ đệm là một trong các lỗi thường gặp trong hệ điều hành và đặc biệt xuất hiện nhiều ở các phần mềm ứng dụng, như đã nêu ở mục 2.1. Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi của bộ nhớ đệm, là giới hạn cuối hoặc cả giới hạn đầu của bộ nhớ đệm. Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí cho phép kẻ tấn công chèn và thực hiện mã độc để kiểm soát hệ thống. Lỗi tràn bộ đệm chiếm một tỷ lệ lớn trong số các lỗi dẫn đến lỗ hổng bảo mật [7]. Tuy nhiên, trên thực tế không phải tất cả các lỗi tràn bộ đệm đều có thể bị khai thác.

Lỗi tràn bộ đệm xuất hiện trong khâu lập trình phần mềm trong quá trình phát triển phần mềm. Nguyên nhân của lỗi tràn bộ đệm là người lập trình không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào được nạp vào bộ nhớ đệm. Khi dữ liệu có kích thước quá lớn hoặc có định dạng sai được ghi vào bộ nhớ đệm, nó sẽ gây tràn và có thể ghi đè lên các tham số thực hiện chương trình. Điều này có thể khiến chương trình bị lỗi và ngừng hoạt động. Một nguyên nhân bổ sung khác là việc sử dụng các thư viện không an toàn trong các ngôn ngữ lập trình, như Hợp ngữ, ngôn ngữ C và C++.

2.2.1.2. Cơ chế gây tràn và khai thác

a. Cơ chế gây tràn

Trên hầu hết các nền tảng, khi một chương trình ứng dụng được nạp vào bộ nhớ, hệ điều hành cấp phát các vùng nhớ để tải mã và lưu dữ liệu của chương trình. Hình 2.7 minh họa các vùng bộ nhớ cấp cho chương trình, bao gồm vùng lưu mã thực hiện (Executable code), vùng lưu dữ liệu toàn cục (Data), vùng bộ nhớ cấp phát động (Heap) và vùng bộ nhớ ngăn xếp (Stack). Vùng bộ nhớ ngăn xếp là vùng nhớ lưu các tham số gọi hàm, thủ tục, phương thức (gọi chung là hàm hay chương trình con) và lưu dữ liệu cục bộ của hàm. Vùng nhớ cấp phát động là vùng nhớ chung lưu dữ liệu cho chương trình, được cấp phát hay giải phóng trong quá trình hoạt động của chương trình.

Chúng ta sử dụng vùng bộ nhớ ngăn xếp để giải thích cơ chế gây tràn và khai thác lỗi tràn bộ đệm. Bộ nhớ ngăn xếp được cấp phát cho chương trình dùng để lưu các biến cục bộ của hàm, trong đó có các biến nhớ được gọi là bộ đệm, các tham số hình thức của hàm, các tham số quản lý ngăn xếp, và địa chỉ trả về (Return address). Địa chỉ trả về là địa chỉ của lệnh nằm kế tiếp lời gọi hàm ở chương trình gọi được tự động lưu vào ngăn

xếp khi hàm được gọi thực hiện. Khi việc thực hiện hàm kết thúc, hệ thống nạp địa chỉ trả về đã lưu trong ngăn xếp vào thanh ghi con trả lệnh (Instruction pointer), kích hoạt việc quay trở lại thực hiện lệnh kế tiếp lời gọi hàm ở chương trình gọi.



Hình 2.7. Các vùng bộ nhớ cấp cho chương trình

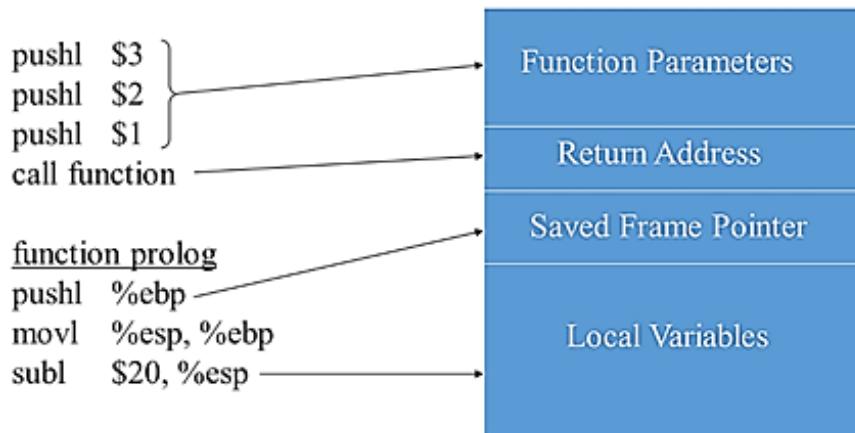
Hình 2.8 là một đoạn chương trình viết bằng C gồm một hàm con (*function()*) và hàm chính (*main()*) minh họa cho việc hàm chính triệu hồi thực hiện hàm con. Hàm *function()* có 3 tham số hình thức kiểu nguyên và khai báo 2 biến cục bộ *buffer1* và *buffer2* kiểu xâu ký tự. Hàm chính *main()* chỉ chứa lời gọi đến hàm *function()* với 3 tham số thực.

```
// định nghĩa một hàm
void function(int a, int b, int c) {
    char buffer1[8];
    char buffer2[12];
}

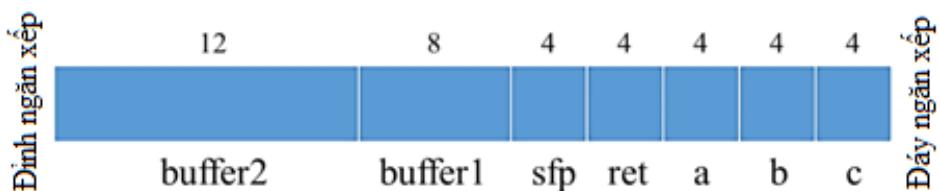
// chương trình chính
int main(){
    function(1,2,3); // gọi hàm
}
```

Hình 2.8. Một đoạn chương trình viết bằng C gồm một hàm chính và một hàm con

Hình 2.9 biểu diễn vị trí các thành phần trong ngăn xếp: các tham số gọi hàm được lưu vào thành phần Function Parameters, địa chỉ trả về được lưu vào ô Return Address, giá trị con trả khung ngăn xếp được lưu vào ô Save Frame Pointer và các biến cục bộ trong hàm được lưu vào thành phần Local Variables. Hình 2.10 minh họa chi tiết việc cấp phát bộ nhớ cho các biến trong ngăn xếp: ngoài ô địa chỉ trả về (ret) và con trả khung (sfp) được cấp cố định ở giữa, các tham số gọi hàm được cấp các ô nhớ bên phải (phía đáy ngăn xếp) và các biến cục bộ được cấp các ô nhớ bên trái (phía đỉnh ngăn xếp).



Hình 2.9. Các thành phần được lưu trong vùng bộ nhớ ngăn xếp



Hình 2.10. Cấp phát bộ nhớ cho các biến trong vùng bộ nhớ ngăn xếp

Hình 2.11 là một đoạn chương trình minh họa việc gây tràn bộ nhớ đệm trong ngăn xếp. Đoạn chương trình này gồm hàm con `function()` và hàm chính `main()`, trong đó hàm `function()` nhận một con trỏ xâu ký tự `str` làm đầu vào. Hàm này khai báo biến `buffer` kiểu xâu ký tự với độ dài 16 byte. Hàm này sử dụng hàm thư viện `strcpy()` để sao chép xâu ký tự từ con trỏ `str` sang biến cục bộ `buffer`. Hàm chính `main()` kê khai xâu ký tự `large_string` với độ dài 256 byte và sử dụng một vòng lặp để điền đầy xâu `large_string` bằng ký tự ‘A’. Sau đó `main()` gọi hàm `function()` với tham số đầu vào là `large_string`.

Có thể thấy đoạn chương trình biểu diễn trên Hình 2.11 khi được thực hiện sẽ gây tràn trong biến nhớ `buffer` của hàm `function()` do tham số truyền vào `large_string` có kích thước 256 byte lớn hơn nhiều so với `buffer` có kích thước 16 byte và hàm `strcpy()` không hề thực hiện việc kiểm tra kích thước dữ liệu vào khi sao chép vào biến `buffer`. Như minh họa trên Hình 2.12, chỉ 16 byte đầu tiên của `large_string` được lưu vào `buffer`, phần còn lại được ghi đè lên các ô nhớ khác trong ngăn xếp, bao gồm `sfp`, `ret` và cả con trỏ xâu tham số đầu vào `str`. Ô nhớ chứa địa chỉ trả về `ret` bị ghi đè và giá trị địa chỉ trả về mới là ‘AAAA’ (0x41414141). Khi kết thúc thực hiện hàm con `function()`, chương trình tiếp tục thực hiện lệnh tại địa chỉ 0x41414141. Đây không phải là địa chỉ của lệnh chương trình phải thực hiện theo lôgic đã định ra từ trước.

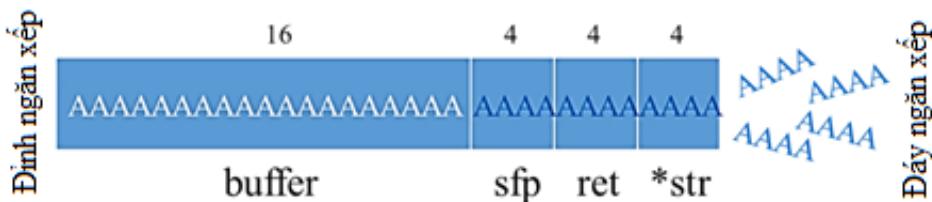
```

// định nghĩa một hàm
void function(char *str) {
    char buffer[16];
    strcpy(buffer, str);
}

```

```
// chương trình chính
int main(){
    char large_string[256];
    int i;
    for (i = 0; i < 255; i++) {
        large_string[i] = 'A';
    }
    function(large_string);
}
```

Hình 2.11. Đoạn chương trình C minh họa gây tràn bộ nhớ đệm trong ngăn xếp



Hình 2.12. Minh họa hiện tượng tràn bộ nhớ đệm (buffer) trong ngăn xếp

Như vậy, lỗi tràn bộ đệm xảy ra khi dữ liệu nạp vào biến nhớ (gọi chung là bộ đệm) có kích thước lớn hơn so với khả năng lưu trữ của bộ đệm và chương trình thiếu các bước kiểm tra kích thước và định dạng dữ liệu nạp vào. Phần dữ liệu tràn sẽ được ghi đè lên các ô nhớ liền kề với bộ đệm trong ngăn xếp, như các biến cục bộ khác, con trỏ khung ngăn xếp, địa chỉ trả về của lời gọi hàm, các biến tham số đầu vào của hàm....

b. Khai thác lỗi tràn bộ đệm

Khi một ứng dụng chứa lỗ hổng tràn bộ đệm, kẻ tấn công có thể khai thác bằng cách gửi mã độc dưới dạng dữ liệu đến chương trình ứng dụng nhằm ghi đè, thay thế địa chỉ trả về của lời gọi hàm với mục đích tái định hướng chương trình đến thực hiện đoạn mã độc mà kẻ tấn công gửi đến. Đoạn mã độc mà kẻ tấn công xây dựng là mã máy có thể thực hiện được và thường được gọi là *shellcode*. Như vậy, để có thể khai thác lỗi tràn bộ đệm, kẻ tấn công thường phải thực hiện việc gỡ rối (debug) chương trình, hoặc có thông tin chi tiết về chương trình từ các nguồn khác và nắm chắc cơ chế gây lỗi cũng như phương pháp quản lý, cấp phát vùng nhớ ngăn xếp của chương trình ứng dụng.

Mã *shellcode* có thể được viết bằng hợp ngữ, C, hoặc các ngôn ngữ lập trình khác, sau đó được dịch thành mã máy, rồi chuyển định dạng thành một chuỗi dữ liệu và cuối cùng được gửi đến chương trình ứng dụng. Hình 2.13 minh họa một đoạn mã *shellcode* viết bằng hợp ngữ và được chuyển đổi thành một chuỗi dưới dạng hexa làm dữ liệu đầu vào gây tràn bộ đệm và gọi thực hiện vỏ *sh* trong các hệ thống Linux hoặc Unix thông qua lệnh /bin/sh.

Hình 2.14 minh họa việc chèn *shellcode*, ghi đè lên ô nhớ địa chỉ trả về *ret*, tái định hướng việc trả về từ chương trình con và chuyển đến thực hiện mã *shellcode* được chèn vào. Các lệnh của *shellcode* chèn vào minh họa sử dụng ký tự S. Trên thực tế, để

tăng khả năng đoạn mã *shellcode* được thực hiện, người ta thường chèn một số lệnh NOP (ký hiệu N) vào phần đầu *shellcode* để phòng khả năng địa chỉ ret mới không trỏ chính xác đến địa chỉ bắt đầu *shellcode*, như minh họa trên Hình 2.15. Lệnh NOP (No OPeration) là lệnh không thực hiện tác vụ nào cả, chỉ tiêu tốn một số chu kỳ đồng hồ của bộ vi xử lý.

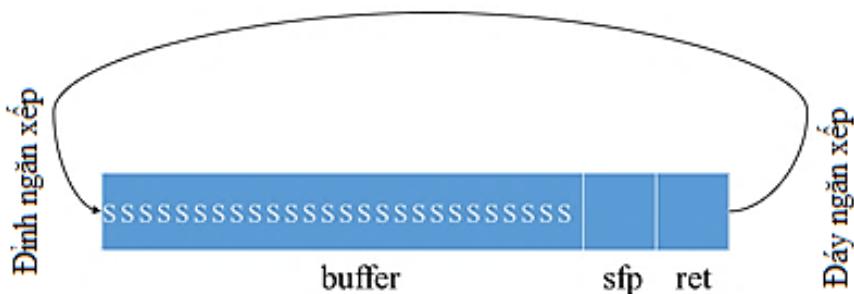
```

jmp    0x1F
popl   %esi
movl   %esi, 0x8(%esi)
xorl   %eax, %eax
movb   %eax, 0x7(%esi)
movl   %eax, 0xC(%esi)
movb   $0xB, %al
movl   %esi, %ebx
leal   0x8(%esi), %ecx
leal   0xC(%esi), %edx
int    $0x80
xorl   %ebx, %ebx
movl   %ebx, %eax
inc    %eax
int    $0x80
call   -0x24
.string "/bin/sh"
}

char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";

```

Hình 2.13. Một shellcode viết bằng hợp ngữ và chuyển thành chuỗi tấn công



Hình 2.14. Chèn và thực hiện shellcode khai thác lỗ tràn bộ đệm

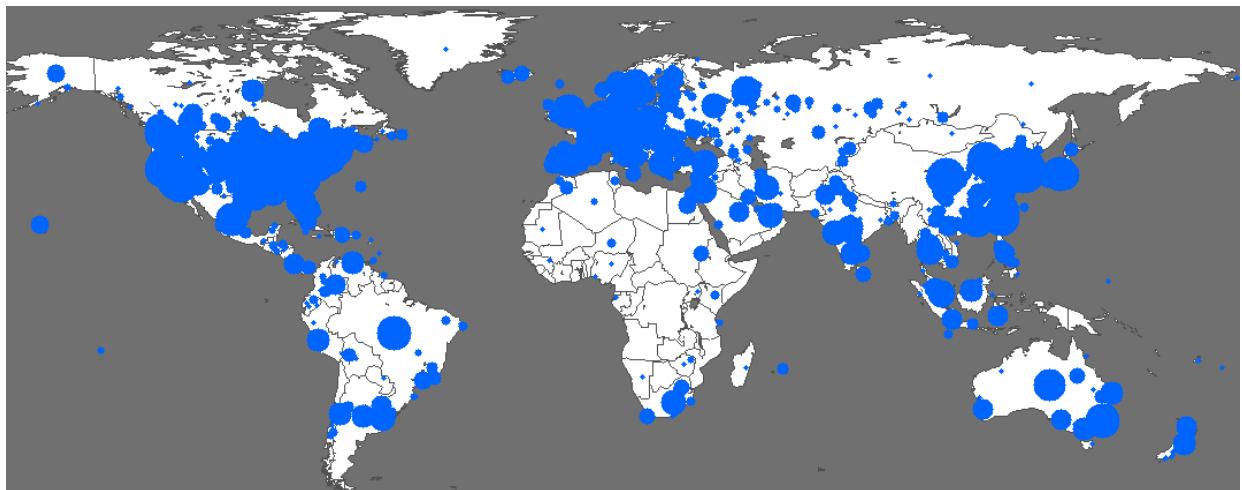


Hình 2.15. Chèn shellcode với phần đệm bằng lệnh NOP (N)

c. Ví dụ về khai thác lối tràn bô đêm

Sâu SQL Slammer (một số tài liệu gọi là sâu Sapphire) được phát hiện ngày 25/1/2003 vào lúc 5g30 (UTC) là sâu có tốc độ lây lan nhanh nhất vào thời điểm đó: Sâu đã lây nhiễm đến gần 75.000 máy chủ tại nhiều nước trên toàn cầu chỉ trong khoảng 30

phút sau khi xuất hiện, phân bố như minh họa trên Hình 2.16. Sâu Slammer khai thác lỗ tràn bộ đệm trong thành phần Microsoft SQL Server Resolution Service của hệ quản trị cơ sở dữ liệu Microsoft SQL Server 2000.



Hình 2.16. Bản đồ lây nhiễm sâu Slammer (màu xanh đậm) theo trang www.caida.org vào ngày 25/1/2003 lúc 6g00 (giờ UTC) với 74.855 máy chủ bị nhiễm

Lỗ tràn bộ đệm này trong SQL Server 2000 đã được phát hiện và Microsoft đã phát hành bản vá từ 6 tháng trước đó, nhưng vẫn còn rất nhiều máy chủ chạy hệ quản trị cơ sở dữ liệu SQL Server 2000 chưa được cập nhật. SQL Slammer sử dụng giao thức UDP với kích thước gói tin 376 byte và vòng lặp chính của sâu chỉ gồm 22 lệnh hợp ngữ. Chu trình hoạt động của SQL Slammer gồm:

- Sinh tự động địa chỉ IP;
- Quét tìm các máy có lỗ với IP tự sinh trên cổng dịch vụ 1434;
- Nếu tìm được, gửi một bản sao của sâu đến máy có lỗ;
- Mã của sâu gây tràn bộ đệm, thực thi mã của sâu và quá trình lặp lại.

SQL Slammer là sâu “lành tính” vì nó không can thiệp vào hệ thống file, không thực hiện việc phá hoại hay đánh cắp thông tin trên hệ thống bị lây nhiễm. Tuy nhiên, sâu tạo ra lưu lượng mạng khổng lồ trong quá trình lây nhiễm, gây tê liệt đường truyền mạng Internet trên nhiều vùng của thế giới. Do mã của SQL Slammer chỉ được lưu trong bộ nhớ nó gây tràn mà không được lưu vào hệ thống file, nên chỉ cần khởi động lại máy là có thể tạm thời xóa được sâu khỏi hệ thống. Tuy nhiên, hệ thống chứa lỗ hỏng có thể bị lây nhiễm lại nếu nó ở gần một máy khác bị nhiễm sâu. Các biện pháp phòng chống triệt để khác là cập nhật bản vá cho bộ phần mềm Microsoft SQL Server 2000. Thông tin chi tiết về sâu SQL Slammer có thể tìm ở các trang:

- <https://technet.microsoft.com/library/security/ms02-039>, hoặc
- <https://www.caida.org/publications/papers/2003/sapphire/sapphire.html>.

2.2.1.3. Phòng chống

Để phòng chống lỗ tràn bộ đệm một cách hiệu quả, cần kết hợp nhiều biện pháp. Các biện pháp có thể thực hiện bao gồm:

- Kiểm tra thủ công hay sử dụng các công cụ phân tích tự động mã nguồn của chương trình ứng dụng để tìm và khắc phục các điểm có khả năng xảy ra lỗi tràn bộ đệm, đặc biệt lưu ý đến các hàm xử lý xâu ký tự.
- Sử dụng cơ chế không cho phép thực hiện mã trong dữ liệu DEP (Data execution prevention). Cơ chế DEP được hỗ trợ bởi hầu hết các hệ điều hành (từ Microsoft Windows XP trở lên và các hệ điều hành họ Linux, Unix,...) không cho phép thực hiện mã chương trình chứa trong vùng nhớ dành cho dữ liệu. Như vậy, nếu kẻ tấn công khai thác lỗi tràn bộ đệm, chèn được mã độc vào bộ đệm trong ngăn xếp, mã độc cũng không thể thực hiện.
- Ngẫu nhiên hóa sơ đồ địa chỉ cấp phát các ô nhớ trong ngăn xếp khi thực hiện chương trình, nhằm gây khó khăn cho việc gỡ rối và phát hiện vị trí các ô nhớ quan trọng như ô nhớ chứa địa chỉ trả về.
- Sử dụng các cơ chế bảo vệ ngăn xếp, theo đó thêm một số ngẫu nhiên (canary) vào vị trí phía trước địa chỉ trả về và kiểm tra lại số ngẫu nhiên này trước khi trả về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trả về.
- Sử dụng các ngôn ngữ, thư viện và công cụ lập trình an toàn. Trong các trường hợp có thể, sử dụng các ngôn ngữ không gây tràn, như Java, các ngôn ngữ lập trình trên nền tảng Microsoft .Net. Với các ngôn ngữ có thể gây tràn như C, C++, nên sử dụng các thư viện an toàn để thay thế các thư viện chuẩn có thể gây tràn.

2.2.2. Lỗi không kiểm tra đầu vào

2.2.2.1. Giới thiệu

Lỗi không kiểm tra đầu vào là một trong các dạng lỗ hổng bảo mật phổ biến, trong đó chương trình ứng dụng không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào, nhờ đó kẻ tấn công có thể khai thác lỗi để tấn công ứng dụng và hệ thống. Dữ liệu đầu vào cho ứng dụng rất đa dạng, có thể đến từ nhiều nguồn với nhiều định dạng khác nhau. Các dạng dữ liệu đầu vào điển hình cho ứng dụng có thể bao gồm:

- Các trường dữ liệu văn bản;
- Các lệnh được truyền qua địa chỉ URL để kích hoạt chương trình;
- Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng, hoặc các tiến trình khác cung cấp;
- Các đối số đầu vào trong dòng lệnh;
- Các dữ liệu từ mạng hoặc từ các nguồn không tin cậy.

Trên thực tế, kẻ tấn công có thể sử dụng phương pháp thủ công, hoặc tự động để kiểm tra các dữ liệu đầu vào và thử tất cả các khả năng có thể để khai thác lỗi không kiểm tra đầu vào. Theo thống kê của trang web OWASP¹, một trang web chuyên về thống kê các lỗi bảo mật ứng dụng web, lỗi không kiểm tra đầu vào luôn có mặt ở nhóm dẫn đầu trong các lỗi bảo mật web trong khoảng 5 năm trở lại đây.

¹ Dự án OWASP có địa chỉ tại <http://www.owasp.org>

2.2.2.2. Tán công khai thác

Có hai dạng chính tấn công khai thác lỗ khống kiểm tra đầu vào: (1) cung cấp dữ liệu quá lớn hoặc sai định dạng để gây lỗi cho ứng dụng và (2) chèn mã khai thác vào dữ liệu đầu vào để thực hiện trên hệ thống của nạn nhân nhằm đánh cắp dữ liệu nhạy cảm hoặc thực hiện các hành vi phá hoại. Hình 2.17 minh họa tấn công khai thác lỗ khống kiểm tra đầu vào dạng (1) thông qua việc nhập dữ liệu quá lớn, gây lỗi thực hiện cho trang web.



Hình 2.17. Cung cấp dữ liệu có kích thước quá lớn gây lỗi cho ứng dụng

Chúng ta minh họa tấn công khai thác lỗi không kiểm tra đầu vào dạng (2) bằng việc chèn mã tấn công SQL vào dữ liệu đầu vào, tiếp theo mã tấn công SQL được thực hiện trên hệ quản trị cơ sở dữ liệu đích nhằm đánh cắp, hoặc phá hủy dữ liệu trong cơ sở dữ liệu. Giả thiết một trang web sử dụng câu lệnh SQL sau để tìm kiếm các sản phẩm:

```
"SELECT * FROM tbl_products WHERE product_name like "%\" + keyword + "%\"
```

trong đó *tbl_products* là bảng lưu thông tin các sản phẩm, *product_name* là trường tên sản phẩm và *keyword* là từ khóa cung cấp bởi người dùng thông qua form tìm kiếm. Nếu người dùng nhập từ khóa là "iPhone X", khi đó câu lệnh SQL trở thành:

"SELECT * FROM tbl_products WHERE product_name like '%iPhone X%'"

Nếu trong bảng có sản phẩm thỏa mãn điều kiện tìm kiếm, câu lệnh SQL sẽ trả về tập bản ghi kết quả. Nếu không có sản phẩm nào thỏa mãn điều kiện tìm kiếm, câu lệnh SQL sẽ trả về tập bản ghi rỗng. Tuy nhiên, nếu người dùng nhập từ khóa "iPhone X"; ***DELETE FROM tbl_products:--***, khi đó câu lệnh SQL trở thành:

"SELECT * FROM tbl_products WHERE product_name like '%iPhone X'; ***DELETE*** FROM ***tbl_products***:--%"

Như vậy, câu lệnh SQL được thực hiện trên cơ sở dữ liệu gồm 2 câu lệnh: câu lệnh chọn SELECT ban đầu và câu lệnh xóa DELETE do kẻ tấn công chèn thêm. Câu lệnh “*DELETE FROM tbl_products*” sẽ xóa tất cả các bản ghi trong bảng *tbl_products*. Sở dĩ

kẻ tấn công có thể thực hiện điều này là do hầu hết các hệ quản trị cơ sở dữ liệu quan hệ cho phép thực hiện nhiều câu lệnh SQL theo *mảng* (batch) trong một chuỗi lệnh, trong đó các câu lệnh được ngăn cách bởi dấu (;). Ngoài ra, dấu “--” ở cuối dữ liệu nhập để loại bỏ hiệu lực của phần lệnh còn lại do “--” là ký hiệu bắt đầu phần chú thích của dòng lệnh SQL. Ngoài lệnh DELETE, kẻ tấn công có thể chèn thêm các lệnh SQL khác, như INSERT, hoặc UPDATE để thực hiện việc chèn thêm bản ghi, hoặc sửa đổi dữ liệu theo ý đồ tấn công của mình.

2.2.2.3. Phòng chống

Biện pháp chủ yếu cho phòng chống tấn công khai thác lỗi không kiểm tra đầu vào là thực hiện lọc dữ liệu đầu vào. Tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy cần được kiểm tra kỹ lưỡng. Các biện pháp cụ thể bao gồm:

- Kiểm tra kích thước và định dạng dữ liệu đầu vào;
- Kiểm tra sự hợp lý của nội dung dữ liệu;
- Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng. Chẳng hạn, với dạng tấn công chèn mã SQL, cần lọc bỏ:
 - + Các ký tự đặc biệt: *, ', =, --
 - + Các từ khóa ngôn ngữ: SELECT, INSERT, UPDATE, DELETE, DROP...

2.2.3. Các vấn đề với kiểm soát truy cập

Kiểm soát truy cập¹ là một lớp bảo vệ đặc biệt quan trọng trong hệ thống các lớp bảo vệ hệ thống và dữ liệu. Kiểm soát truy cập liên quan đến việc kiểm soát *ai* (chủ thẻ) được truy cập đến *cái gì* (đối tượng). Kiểm soát truy cập có thể được thực hiện bởi hệ điều hành, hoặc từng ứng dụng. Kiểm soát truy cập thường gồm 2 khâu: xác thực và trao quyền. Xác thực là việc xác minh tính chân thực của thông tin nhận dạng của chủ thẻ, còn trao quyền (còn gọi là ủy quyền) là việc cấp quyền truy cập cho chủ thẻ sau khi thông tin nhận dạng đã được xác thực. Các chủ thẻ được cấp quyền truy cập vào hệ thống theo các cấp độ khác nhau dựa trên chính sách an ninh của cơ quan, tổ chức.

Các vấn đề thường gặp với kiểm soát truy cập là hệ thống xác thực, hoặc trao quyền yếu hoặc có lỗi. Nếu kiểm soát truy cập có lỗi, một người dùng bình thường có thể chiếm đoạt quyền của người quản trị và toàn quyền truy cập vào hệ thống. Hoặc, kẻ tấn công có thể lợi dụng lỗ hổng bảo mật của hệ thống kiểm soát truy cập để truy cập trái phép vào các file trong hệ thống. Một dạng khai thác hệ thống kiểm soát truy cập điển hình là một ứng dụng được thực thi sử dụng tài khoản quản trị sẽ có toàn quyền truy cập vào hệ thống, và nếu một kẻ tấn công chiếm được quyền điều khiển ứng dụng đó, hắn sẽ có toàn quyền truy cập vào hệ thống.

Để đảm bảo an toàn cho hệ thống kiểm soát truy cập, các biện pháp sau cần được xem xét áp dụng:

¹ Một số tài liệu sử dụng thuật ngữ “Điều khiển truy cập”. Từ tiếng Anh gốc là Access control.

- Không sử dụng tài khoản quản trị (root hoặc administrator) để thực thi các chương trình ứng dụng.
- Luôn thực thi các chương trình ứng dụng với quyền tối thiểu, vừa đủ để chúng thực thi các tác vụ.
- Kiểm soát chặt chẽ người dùng, xóa bỏ hoặc cấm truy cập với những người dùng ngầm định, kiểu *everyone*.
- Thực thi chính sách mật khẩu an toàn.
- Chỉ cấp quyền vừa đủ cho người dùng thực thi nhiệm vụ.

2.2.4. Các điểm yếu trong xác thực, trao quyền

Do các khâu xác thực và trao quyền là hai thành phần cốt lõi của một hệ thống kiểm soát truy cập, nên các điểm yếu trong xác thực và trao quyền ảnh hưởng trực tiếp đến độ an toàn của hệ thống kiểm soát truy cập. Một điểm yếu điển hình trong khâu xác thực là mật khẩu được sử dụng dưới dạng rõ, dẫn đến nguy cơ bị lộ mật khẩu rất cao trong quá truyền thông tin xác thực. Ngoài ra, việc sử dụng mật khẩu đơn giản, dễ đoán, hoặc dùng mật khẩu trong thời gian dài cũng là điểm yếu dễ bị khai thác. Việc sử dụng cơ chế xác thực không đủ mạnh, như các cơ chế xác thực đơn giản cung cấp bởi giao thức HTTP cũng tiềm ẩn các nguy cơ bị tấn công khai thác.

Khâu trao quyền cũng tồn tại một số điểm yếu, như sử dụng cơ chế trao quyền không đủ mạnh, dễ bị vượt qua. Chẳng hạn, một trang web chỉ thực hiện ẩn các liên kết đến các trang web mà người dùng không được quyền truy cập mà không thực sự kiểm tra quyền truy cập trên từng trang, nếu người dùng tự gõ URL của trang thì vẫn có thể truy cập.

2.2.5. Các điểm yếu trong các hệ mật mã

Các vấn đề với các hệ mật mã bao gồm việc sử dụng các giải thuật mã hóa, giải mã, hàm băm yêu, lạc hậu, hoặc có lỗ hổng đã biết không thể khắc phục (như các giải thuật DES, MD4, MD5,...), hoặc sử dụng khóa mã hóa, giải mã yêu, như các khóa có chiều dài ngắn, hoặc dễ đoán. Các hệ mật mã khóa bí mật có độ an toàn cao, tốc độ cao, nhưng gặp phải khó khăn trong vấn đề trao đổi, chia sẻ các khóa bí mật. Các khóa bí mật trao đổi trong môi trường không an toàn như mạng Internet có thể bị lộ, bị đánh cắp. Một số vấn đề khác có thể gặp phải với các hệ mã hóa, bao gồm vấn đề xác thực người gửi, người nhận, vấn đề sử dụng các khóa, các chứng chỉ hết hạn hoặc bị thu hồi, hoặc chi phí tính toán quá lớn, đặc biệt đối với các hệ mật mã khóa công khai.

2.2.6. Các lỗ hổng bảo mật khác

Các thao tác không an toàn với các file cũng có thể là một lỗ hổng bảo mật nghiêm trọng. Chẳng hạn, một người dùng thực hiện đọc/ghi một file chứa thông tin nhạy cảm được lưu ở những nơi mà những người dùng khác cũng có thể ghi file đó. Các lỗi bảo mật điển hình khác có thể gồm:

- Không kiểm tra chính xác loại file, định danh thiết bị, các liên kết hoặc các thuộc tính khác của file trước khi sử dụng;

- Cho phép tải file tài liệu, hình ảnh lên máy chủ nhưng không kiểm tra định dạng file và không cấm quyền thực hiện, và do vậy kẻ tấn công có thể tải lên và thực hiện các file chứa mã độc;
- Không kiểm tra mã trả về sau mỗi thao tác với file;
- Giả thiết một file có đường dẫn cục bộ là file cục bộ và bỏ qua các thủ tục kiểm tra cần thiết. Kẻ tấn công có thể khai thác lỗi này bằng cách ánh xạ file ở xa vào hệ thống file cục bộ, tức là có đường dẫn cục bộ và có thể được thực thi trên hệ thống cục bộ.

Một dạng điểm yếu bảo mật khác xảy ra khi xuất hiện các điều kiện đua tranh (Race condition). Một điều kiện đua tranh tồn tại khi có sự thay đổi trật tự của 2 hay một số sự kiện gây ra sự thay đổi hành vi của hệ thống. Đây là một dạng lỗi nếu chương trình chỉ có thể thực hiện đúng chức năng nếu các sự kiện phải xảy ra theo đúng trật tự. Kẻ tấn công có thể lợi dụng khoảng thời gian giữa 2 sự kiện để chèn mã độc, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống.

2.3. Quản lý, khắc phục lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống

2.3.1. Nguyên tắc chung

Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần được thực hiện theo nguyên tắc chung là cân bằng giữa *mức An toàn*, *Chi phí* và *tính Hữu dụng*, như minh họa trên Hình 1.13, trang 23. Ý nghĩa cụ thể của nguyên tắc này là đảm bảo an toàn cho hệ thống ở mức phù hợp với chi phí hợp lý và hệ thống vẫn phải hữu dụng, hay có khả năng cung cấp đầy đủ các tính năng hữu ích cho người dùng.

2.3.2. Các biện pháp cụ thể

Trên cơ sở nguyên tắc chung của việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống, các biện pháp cụ thể cần được xem xét áp dụng với từng trường hợp cụ thể, đảm bảo hiệu quả. Biện pháp thiết yếu đầu tiên cần được thực hiện cho mọi trường hợp là thường xuyên cập nhật thông tin về các điểm yếu, lỗ hổng bảo mật từ các trang web cung cấp thông tin chính thức sau:

- CVE - Common Vulnerabilities and Exposures: <http://cve.mitre.org>
- CVE Details: <http://www.cvedetails.com>
- US National Vulnerability Database: <http://web.nvd.nist.gov>
- OWASP: <https://www.owasp.org/index.php/Category:Vulnerability>

Biện pháp hiệu quả tiếp theo là định kỳ cập nhật các bản vá, bản nâng cấp hệ điều hành và các phần mềm ứng dụng, nhằm khắc phục các lỗ hổng đã biết, cũng như tăng cường khả năng đề kháng cho hệ thống bằng các phiên bản mới an toàn hơn. Để thực hiện công việc này có thể sử dụng các hệ thống quản lý các bản vá và tự động cập nhật định kỳ, như Microsoft Windows Updates, các tiện ích cập nhật tự động trên Linux/Unix, và tính năng tự động cập nhật của các ứng dụng, như Google Update Service. Căn cứ vào mức độ nghiêm trọng của các lỗ hổng bảo mật, tần suất cập nhật các bản vá cần được

tuân thủ. Với các lỗ hổng nghiêm trọng, cần cập nhật tức thời các bản vá, còn với các lỗ hổng ít nghiêm trọng hơn, cần có kế hoạch cập nhật, hoặc khắc phục định kỳ.

Một biện pháp hiệu quả khác là sử dụng các phần mềm, hoặc công cụ rà quét các điểm yếu, lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng, để chủ động tìm và khắc phục các điểm yếu và lỗ hổng bảo mật của hệ thống. Nhờ vậy có thể giảm thiểu nguy cơ bị lợi dụng, khai thác các lỗ hổng bảo mật đã biết.

Một biện pháp bổ sung là cần có chính sách quản trị người dùng, mật khẩu và quyền truy cập chặt chẽ ở cả mức hệ điều hành và mức ứng dụng, trong đó người dùng chỉ được cấp quyền truy cập vừa đủ vào hệ thống để thực hiện công việc được giao. Nếu người dùng được cấp nhiều quyền truy cập hơn mức cần thiết, họ có khuynh hướng lạm dụng quyền để truy cập vào các dữ liệu nhạy cảm, hoặc có thể bị kẻ tấn công khai thác.

Việc sử dụng các biện pháp phòng vệ ở lớp ngoài như tường lửa, proxy cũng đem lại hiệu quả do chúng giúp làm giảm bề mặt tiếp xúc với hệ thống, qua đó giảm thiểu khả năng bị tấn công. Tường lửa và proxy có thể chặn các dịch vụ, hoặc cổng không sử dụng, hoặc không thực sự cần thiết, đồng thời ghi log các hoạt động truy cập mạng phục vụ cho việc phân tích, điều tra khi cần thiết.

Với các nhà phát triển phần mềm thì phát triển phần mềm an toàn là một trong các biện pháp cho phép giải quyết tận gốc vấn đề lỗ hổng bảo mật. Cần bổ sung các yêu cầu đảm bảo an ninh, an toàn vào quy trình phát triển phần mềm. Ngoài ra, cần kiểm tra, kiểm thử tất cả các khâu, như thiết kế, cài đặt để tìm các điểm yếu, lỗ hổng bảo mật, và có biện pháp khắc phục phù hợp với các điểm yếu, lỗ hổng được phát hiện.

2.4. Giới thiệu một số công cụ rà quét điểm yếu và lỗ hổng bảo mật

Các công cụ rà quét các điểm yếu và lỗ hổng bảo mật có thể được người quản trị sử dụng để chủ động rà quét các hệ thống, nhằm tìm ra các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống. Trên cơ sở kết quả rà quét, người quản trị có thể phân tích và đề xuất áp dụng các biện pháp khắc phục phù hợp. Các công cụ bao gồm: công cụ rà quét cổng dịch vụ, các công cụ rà quét lỗ hổng bảo mật hệ thống, và các công cụ rà quét lỗ hổng ứng dụng web, hay các trang web.

2.4.1. Công cụ rà quét lỗ hổng bảo mật hệ thống

Các công cụ rà quét lỗ hổng bảo mật hệ thống cho phép rà quét hệ thống, tìm các điểm yếu và lỗ hổng bảo mật. Đồng thời, chúng cũng phân tích chi tiết từng điểm yếu, lỗ hổng, kèm theo là hướng dẫn khắc phục, sửa chữa. Các công cụ được sử dụng rộng rãi là Microsoft Baseline Security Analyzer¹ cho rà quét các hệ thống chạy hệ điều hành Microsoft Windows và Nessus Vulnerability Scanner² cho rà quét các hệ thống chạy nhiều loại hệ điều hành khác nhau.

Microsoft Baseline Security Analyzer cho phép quét các thành phần của hệ điều hành Microsoft Windows (vẫn đe cài đặt, cấu hình hệ thống, quản trị người dùng), các dịch vụ, tiện ích chạy trên Windows (máy chủ web IIS, máy chủ cơ sở dữ liệu SQL server, trình

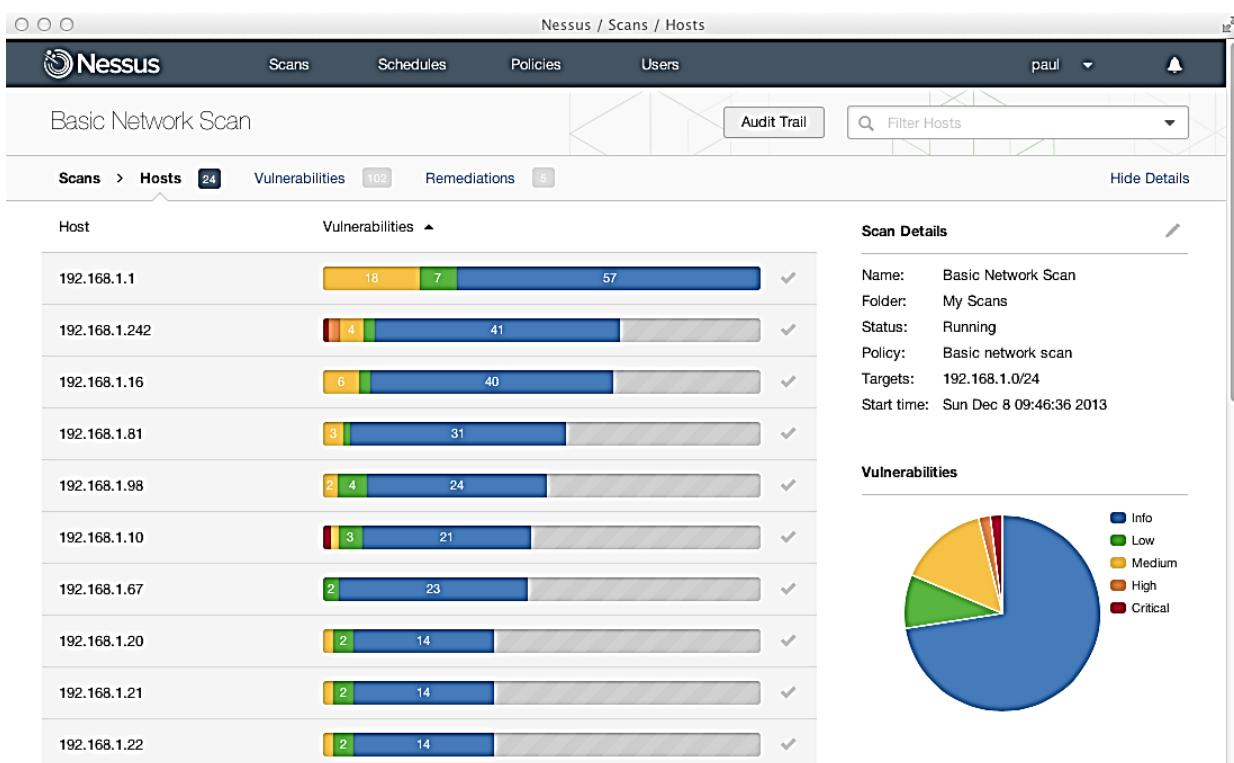
¹ Tham khảo tại: <https://www.microsoft.com/en-us/download/details.aspx?id=15623>

² Tham khảo tại: <https://www.tenable.com/products/nessus/nessus-professional>

cập nhật Windows Updates,...) và các chương trình ứng dụng (Microsoft Office, trình duyệt Internet Explorer,...) trên một máy tính hoặc một nhóm các máy tính. Hình 2.18 là màn hình báo cáo kết quả rà quét điểm yếu và lỗ hổng bảo mật của Microsoft Baseline Security Analyzer. Ưu điểm của Microsoft Baseline Security Analyzer là tốc độ rà quét nhanh, miễn phí và dễ sử dụng. Hạn chế của công cụ này là chỉ có khả năng rà quét hệ điều hành Microsoft Windows và các ứng dụng do Microsoft phát triển.

The screenshot shows the Microsoft Baseline Security Analyzer interface. At the top, there's a toolbar with icons for back, forward, search, and help, followed by the title "Microsoft Baseline Security Analyzer". Below the title is a logo of a shield with a checkmark. The main content area is titled "Administrative Vulnerabilities". It contains a table with three columns: "Score", "Issue", and "Result". The "Score" column uses icons: a yellow exclamation mark for updates, a yellow exclamation mark for password expiration, blue information icons for incomplete updates and windows firewall, green checkmarks for local account password test and file system, and a green checkmark for file system. The "Issue" column lists the specific vulnerability types. The "Result" column provides details and links for each issue. At the bottom of the interface are buttons for "Print this report", "Copy to clipboard", "Previous security report", and "Next security report".

Hình 2.18. Báo cáo kết quả quét của Microsoft Baseline Security Analyzer

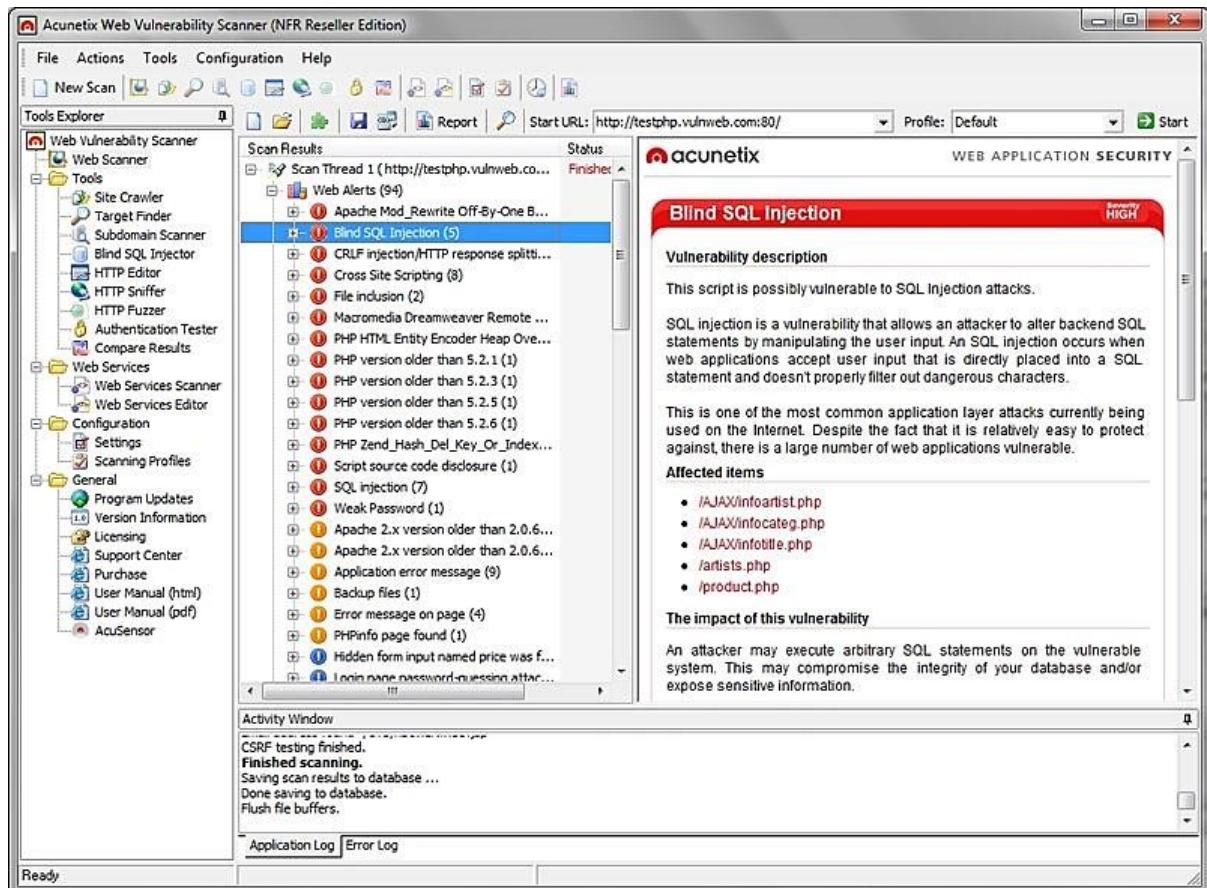


Hình 2.19. Màn hình tổng hợp kết quả quét lỗ hổng của Nessus Vulnerability Scanner

Ngược lại, Nessus Vulnerability Scanner có khả năng rà quét hầu hết các hệ điều hành và các ứng dụng khác nhau. Tương tự Microsoft Baseline Security Analyzer, công cụ này cũng hỗ trợ quét từng máy cụ thể, hoặc quét mạng theo địa chỉ IP. Hình 2.19 là màn hình tổng hợp kết quả quét lỗ hổng cho một tập các host của Nessus Vulnerability Scanner. Ưu điểm của bộ công cụ này là có khả năng rà quét tìm điểm yếu, lỗ hổng trên nhiều hệ điều hành và ứng dụng. Tuy nhiên, hạn chế của nó là ván đề phí bản quyền cao và tương đối chậm do hệ thống hoạt động dưới dạng một máy chủ web.

2.4.2. Công cụ rà quét lỗ hổng ứng dụng web

Các công cụ rà quét lỗ hổng ứng dụng web cho phép rà quét, phân tích các trang web, tìm các lỗ và lỗ hổng bảo mật. Chúng cũng hỗ trợ phân tích tình trạng các lỗ tìm được, như các lỗ XSS, lỗ chèn mã SQL, lỗ CSRF, lỗ bảo mật phiên,... Các công cụ được sử dụng phổ biến bao gồm Acunetix Web Vulnerability Scanner¹, IBM AppScan², Beyond Security AVDS³ và SQLmap⁴. Trong số các công cụ trên, Acunetix Web Vulnerability Scanner là một trong các bộ công cụ quét các điểm yếu, lỗ hổng cho các website, ứng dụng web được sử dụng phổ biến nhất.



Hình 2.20. Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner

Hình 2.20 biểu diễn giao diện kết quả rà quét một trang web mẫu của Acunetix Web Vulnerability Scanner. Công cụ này có khả năng tải toàn bộ website để phân tích, đánh

¹ Tham khảo tại: <https://www.acunetix.com/vulnerability-scanner>

² Tham khảo tại: <https://www.ibm.com/security/application-security/appscan>

³ Tham khảo tại: <https://www.beyondsecurity.com/avds.html>

⁴ Tham khảo tại: <http://sqlmap.org>

giá kiều kiểm thử hộp trắng, hoặc kết hợp giữa kiểm thử hộp trắng và kiểm thử hộp đen sử dụng một cơ sở dữ liệu gồm hàng ngàn các mẫu tấn công website được xây dựng sẵn. Acunetix Web Vulnerability Scanner cung cấp mô tả chi tiết cho từng lỗ hổng tìm được và kèm theo là hướng dẫn khắc phục, sửa chữa. Ưu điểm của bộ công cụ là tốc độ quét nhanh và giao diện trực quan, dễ sử dụng. Hạn chế duy nhất của bộ công cụ này là vấn đề phí bản quyền.

2.5. Kết chương

Chương này đã trình bày chi tiết về các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống, một số kỹ thuật khai thác để tấn công và các biện pháp khắc phục. Cụ thể các vấn đề sau đã được đề cập:

- Mô tả các khái niệm điểm yếu và lỗ hổng bảo mật tồn tại trong các hệ thống máy tính, hệ thống thông tin và các phương pháp phân loại các lỗ hổng bảo mật.
- Trình bày một số số liệu thống kê về các lỗ hổng bảo mật tồn tại trong hệ thống và trong hệ điều hành và các phần mềm ứng dụng. Theo đó, số lượng các lỗ hổng bảo mật có cấp độ nghiêm trọng trung bình và cao tồn tại trong các dịch vụ mạng và các phần mềm ứng dụng chiếm tỷ lệ lớn nhất.
- Mô tả 5 dạng lỗ lỗ hổng bảo mật phổ biến tồn tại trong hệ điều hành và các phần mềm ứng dụng. Trong đó đi sâu phân tích nguyên nhân xuất hiện và cơ chế khai thác tấn công 2 dạng lỗ hổng có số lượng lớn nhất và mức độ nghiêm trọng cao nhất là lỗ hổng tràn bộ đệm và lỗ hổng không kiểm tra đầu vào.
- Trình bày nguyên tắc và các biện pháp cụ thể cho việc quản lý, khắc phục lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống.
- Giới thiệu một số công cụ ra quét các điểm yếu và lỗ hổng bảo mật.

2.6. Câu hỏi ôn tập

- 1) Điểm yếu hệ thống là gì? Nếu các nguyên nhân của sự tồn tại các điểm yếu trong hệ thống. Tại sao có thể nói “Hệ thống càng phức tạp, càng có nhiều thành phần và nhiều tính năng thì khả năng tồn tại các điểm yếu càng tăng”?
- 2) Lỗ hổng bảo mật là gì? Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống? Tại sao?
- 3) Nếu các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng. Tại sao các trình duyệt web thường tồn tại nhiều lỗ hổng bảo mật và bị tấn công khai thác nhiều nhất?
- 4) Lỗi tràn bộ đệm là lỗi trong khâu nào của quá trình phát triển phần mềm? Giải thích lý do tại sao?
- 5) Các vùng bộ nhớ nào của chương trình thường bị gây tràn trong tấn công khai thác lỗi tràn bộ đệm?
- 6) Mô tả cơ chế gây tràn bộ đệm và khai thác lỗi tràn bộ đệm trong ngắn xếp.

- 7) Khảo sát tài liệu và mô tả cơ chế gây tràn bộ đệm và khai thác lỗi tràn bộ đệm trong vùng nhớ Heap.
- 8) Giải thích tại sao một chuỗi các lệnh NOP thường được sử dụng ở phần đầu đoạn mã shellcode trong tấn công khai thác lỗi tràn bộ đệm trong ngăn xếp?
- 9) Khảo sát và mô tả cơ chế của ít nhất 2 trường hợp tấn công khai thác lỗi tràn bộ đệm đã xảy ra trên thực tế.
- 10) Nêu các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm. Trong số các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm, theo bạn biện pháp nào cho hiệu quả cao nhất? Giải thích lý do cho sự lựa chọn của mình.
- 11) Mô tả cơ chế tấn công khai thác lỗi không kiểm tra đầu vào.
- 12) Nêu các biện pháp phòng chống tấn công khai thác lỗi không kiểm tra đầu vào.
- 13) Mô tả các vấn đề với hệ thống kiểm soát truy cập và khả năng bị khai thác.
- 14) Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần được thực hiện theo nguyên tắc chung nào?
- 15) Mô tả vắn tắt các biện pháp cụ thể trong việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống.

CHƯƠNG 3. CÁC DẠNG TẤN CÔNG VÀ CÁC PHẦN MỀM ĐỘC HẠI

Chương 3 giới thiệu về các dạng tấn công điển hình vào các hệ thống máy tính và mạng, bao gồm tấn công vào mật khẩu, tấn công bằng mã độc, tấn công giả mạo, nghe lén, người đứng giữa, tấn công DoS/DDoS, tấn công sử dụng các kỹ thuật xã hội, tấn công APT. Nửa sau của chương đề cập đến các dạng phần mềm độc hại, gồm phân loại, cơ chế lây nhiễm và tác hại của chúng. Kèm theo phần mô tả mỗi tấn công, hoặc phần mềm độc hại, chương đề cập các biện pháp, kỹ thuật phòng chống tương ứng.

3.1. Khái quát về mối đe dọa và tấn công

Mối đe dọa và tấn công vào các hệ thống máy tính và mạng là các yếu tố có tính chất khách quan nhưng lại có quan hệ mật thiết với lỗ hổng bảo mật là yếu tố chủ quan tồn tại trong hệ thống. Mục này giới thiệu khái quát về mối đe dọa, tấn công, quan hệ giữa mối đe dọa, tấn công với lỗ hổng bảo mật và các dạng tấn công, hình thức tấn công.

3.1.1. Mối đe dọa

Theo định nghĩa tại mục 1.1.1.3, *Mối đe dọa* là bất kỳ hành động nào có thể gây hư hại đến các tài sản, hay các tài nguyên hệ thống. Các tài nguyên hệ thống bao gồm phần cứng, phần mềm, cơ sở dữ liệu, các file, dữ liệu, hoặc hạ tầng mạng vật lý,... Mối đe dọa và lỗ hổng bảo mật luôn có quan hệ hữu cơ với nhau: Các mối đe dọa thường khai thác một hoặc một số lỗ hổng bảo mật đã biết để thực hiện các cuộc tấn công. Điều này có nghĩa là nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực. Nói chung, không thể triệt tiêu được hết các mối đe dọa do đó là yếu tố khách quan, nhưng có thể giảm thiểu các lỗ hổng bảo mật tồn tại trong hệ thống, qua đó giảm thiểu khả năng bị khai thác để thực hiện tấn công.

Trên thực tế, không phải tất cả các mối đe dọa đều là ác tính hay độc hại. Một số mối đe dọa là chủ động, cố ý, nhưng một số khác chỉ là ngẫu nhiên, hoặc vô tình. Các mối đe dọa thường gặp đối với thông tin, hệ thống và mạng có thể gồm:

- Phần mềm độc hại, hoặc các dạng mã độc
- Kẻ tấn công ở bên trong
- Kẻ tấn công ở bên ngoài
- Hu hỏng phần cứng hoặc phần mềm
- Mất trộm, mất cắp các thiết bị
- Tai họa thiên nhiên
- Gián điệp công nghiệp
- Khủng bố phá hoại.

3.1.2. Tấn công

Mục 1.1.1.3 đã đề cập khái niệm tấn công theo nghĩa tổng quát. Tấn công theo nghĩa chi tiết là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh, an toàn

của tổ chức, cơ quan, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn sàng của thông tin, hệ thống và mạng. Một cuộc tấn công vào hệ thống máy tính hoặc các tài nguyên mạng thường được thực hiện bằng cách khai thác các lỗ hổng bảo mật tồn tại trong hệ thống. Như vậy, tấn công chỉ có thể trở thành hiện thực¹ nếu có sự tồn tại đồng thời của mối đe dọa và lỗ hổng bảo mật, hay có thể nói:

$$\text{Tấn công} = \text{Mối đe dọa} + \text{Lỗ hổng bảo mật}$$

Có thể chia các dạng tấn công theo mục đích thực hiện thành 4 loại chính như sau:

- Giả mạo (Fabrication) là dạng tấn công thực hiện việc giả mạo thông tin (email, địa chỉ IP...) và thường được sử dụng để đánh lừa người dùng thông thường;
- Chặn bắt (Interception) là dạng tấn công thường liên quan đến việc nghe lén thông tin trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
- Gây ngắt quãng (Interruption) dạng tấn công làm ngắt, hoặc chậm kênh truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy cập dịch vụ của người dùng hợp pháp;
- Sửa đổi (Modification) dạng tấn công thực hiện việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

Theo hình thức thực hiện, có thể chia các dạng tấn công thành 2 kiểu chính như sau:

- Tấn công chủ động (Active attack) là một đột nhập, xâm nhập về mặt vật lý vào hệ thống, hoặc mạng. Các tấn công chủ động thực hiện sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong file, hoặc giành quyền truy cập trái phép vào hệ thống máy tính hoặc hệ thống mạng.
- Tấn công thụ động (Passive attack) là kiểu tấn công thường không gây ra thay đổi trên hệ thống. Các tấn công thụ động điển hình là nghe lén và giám sát lưu lượng trên đường truyền.

Trên thực tế, tấn công thụ động thường là giai đoạn đầu của một cuộc tấn công chủ động, trong đó kẻ tấn công sử dụng các kỹ thuật tấn công thụ động để thu thập các thông tin về hệ thống, mạng. Trên cơ sở các thông tin có được từ giai đoạn tấn công thụ động, kẻ tấn công sẽ lựa chọn kỹ thuật tấn công chủ động có xác suất thành công cao nhất.

3.2. Các công cụ hỗ trợ tấn công

Các công cụ hỗ trợ tấn công là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ kẻ tấn công thu thập các thông tin về hệ thống máy tính, hoặc mạng. Trên cơ sở các thông tin thu được, kẻ tấn công sẽ lựa chọn công cụ, kỹ thuật tấn công có khả năng thành công cao nhất. Các công cụ hỗ trợ tấn công bao gồm 4 nhóm chính:

- Công cụ quét điểm yếu, lỗ hổng bảo mật
- Công cụ quét cổng dịch vụ
- Công cụ nghe lén
- Công cụ ghi phím gõ.

¹ Mặc dù quan hệ giữa tấn công với mối đe dọa và lỗ hổng bảo mật không hoàn toàn là quan hệ 1:1, nhưng sự xuất hiện đồng thời của mối đe dọa và lỗ hổng bảo mật có thể xem như là điều kiện cần của tấn công.

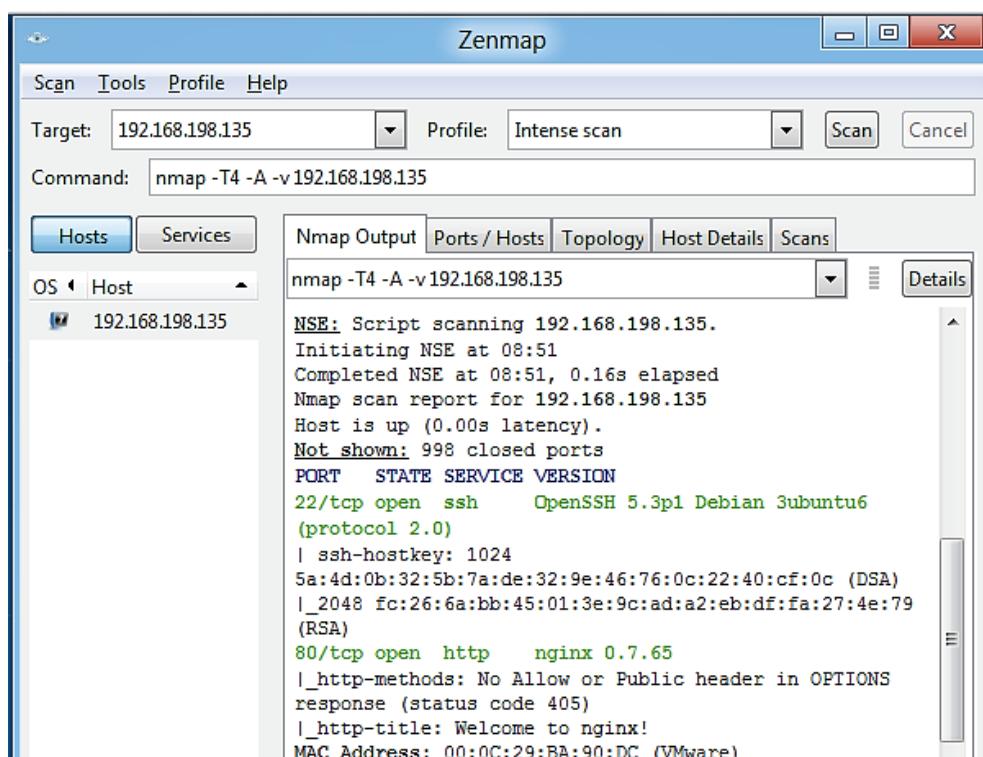
Các công cụ quét điểm yếu, lỗ hổng bảo mật đã được trình bày ở mục 2.4. Mục này giới thiệu 3 nhóm công cụ còn lại, bao gồm các công cụ quét cổng dịch vụ, công cụ nghe lén và công cụ ghi phím gõ.

3.2.1. Công cụ quét cổng dịch vụ

Các công cụ quét cổng dịch vụ (Port scanner) cho phép quét các cổng, tìm các cổng đang mở, đang hoạt động, đồng thời tìm các thông tin về ứng dụng, dịch vụ và hệ điều hành đang hoạt động trên hệ thống. Dựa trên thông tin quét cổng dịch vụ, có thể xác định được dịch vụ, ứng dụng nào đang chạy trên hệ thống. Có thể nêu một số ví dụ về liên kết giữa cổng và dịch vụ, ứng dụng hoạt động trong hệ thống như sau:

- Cổng 80/443 kết nối thành công có nghĩa là dịch vụ/máy chủ web đang hoạt động;
- Cổng 25 kết nối thành công có nghĩa là dịch vụ gửi/nhận email SMTP đang hoạt động;
- Cổng 1433 kết nối thành công có nghĩa là máy chủ Microsoft SQL Server đang hoạt động;
- Cổng 53 kết nối thành công có nghĩa là dịch vụ tên miền DNS đang hoạt động.

Các công cụ quét cổng dịch vụ được sử dụng phổ biến bao gồm: Nmap, Zenmap¹, Portsweep, Advanced Port Scanner, Angry IP Scanner, SuperScan và NetScanTools. Hình 3.1 là giao diện của công cụ quét cổng dịch vụ Nmap/ Zenmap – một trong các công cụ quét cổng dịch vụ được sử dụng rộng rãi. Nmap cung cấp tập lệnh rà quét rất mạnh. Tuy nhiên, Nmap tương đối khó sử dụng do chỉ hỗ trợ giao diện dòng lệnh với rất nhiều tham số khác nhau.



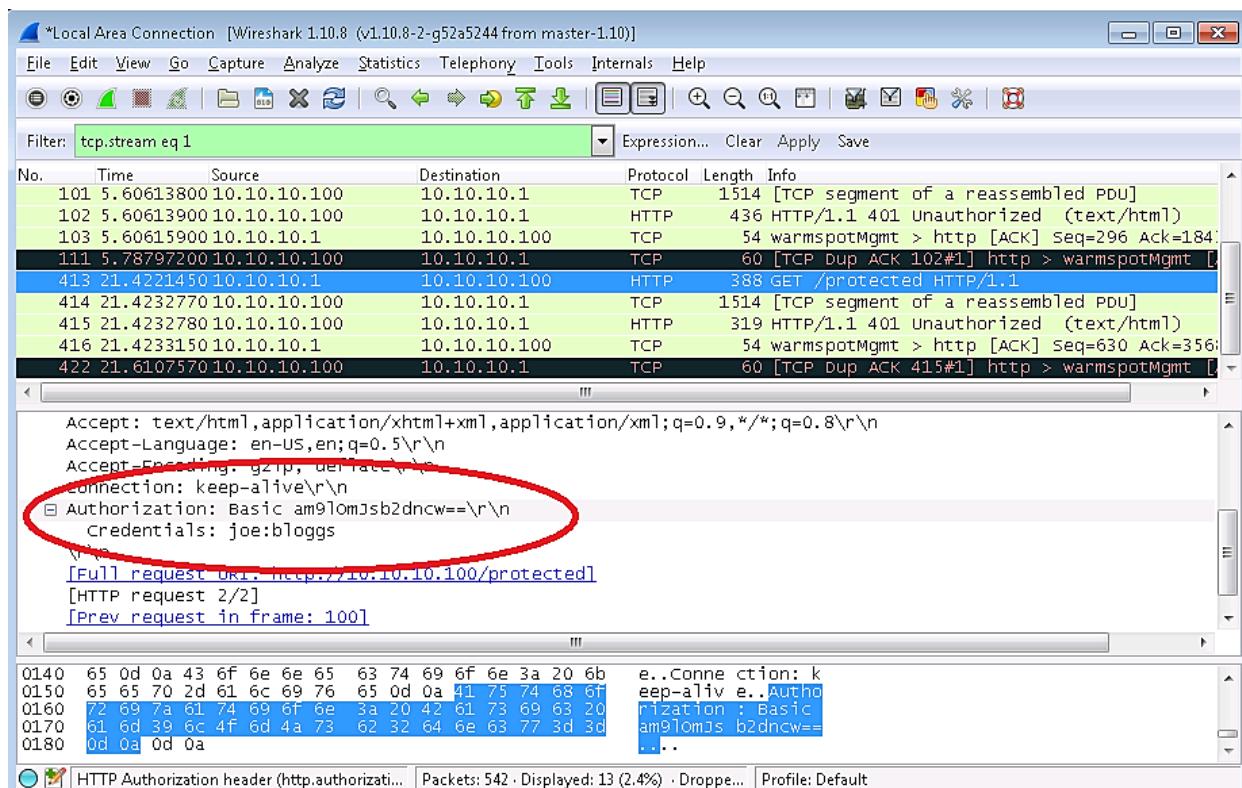
Hình 3.1. Giao diện của công cụ quét cổng Zenmap

¹ Tham khảo tại: <https://nmap.org/zenmap>

3.2.2. Công cụ nghe lén

Công cụ nghe lén (Sniffer) cho phép bắt các gói tin khi chúng được truyền trên mạng. Công cụ nghe lén có thể là mô đun phần cứng, phần mềm hoặc kết hợp. Các thông tin nhạy cảm như thông tin tài khoản, thẻ tín dụng, hoặc mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe lén khi được truyền từ máy trạm đến máy chủ và bị lạm dụng. Một số công cụ phần mềm cho phép bắt gói tin truyền trên mạng được sử dụng phổ biến bao gồm:

- Tcpdump¹
- Wireshark² (minh họa trên Hình 3.2)
- Pcap³ / Winpcap⁴ / Libpcap⁵ (Packet capture – các thư viện hỗ trợ bắt gói tin)
- Network-Tools/IP Tools⁶.



Hình 3.2. Sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm

3.2.3. Công cụ ghi phím gõ

Công cụ ghi phím gõ (Keylogger) là một dạng công cụ giám sát bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào một file. File đã ghi sau đó có thể được gửi cho kẻ tấn công theo địa chỉ email chỉ định trước, hoặc kẻ tấn công có thể sao chép trực tiếp từ hệ thống bị giám sát. Ngoài kẻ tấn công, người quản lý cũng có thể cài đặt keylogger vào máy tính của nhân viên để theo dõi hoạt động của họ.

¹ Tham khảo tại: <http://www.tcpdump.org>

² Tham khảo tại: <https://www.wireshark.org>

³ Tham khảo tại: <http://www.tcpdump.org>

⁴ Tham khảo tại: <https://www.winpcap.org>

⁵ Tham khảo tại: <http://www.tcpdump.org>

⁶ Tham khảo tại: <https://www.softpedia.com/get/Network-Tools/IP-Tools>

Việc cài đặt keylogger có thể được thực hiện tương đối đơn giản: Hình 3.3 minh họa một keylogger dưới dạng một khớp nối phần cứng kết nối cổng bàn phím với đầu nối bàn phím, hỗ trợ cả giao diện cổng bàn phím PS/2 và USB. Với keylogger phần mềm, kẻ tấn công có thể tích hợp keylogger vào một phần mềm ứng dụng thông thường và lừa người dùng tải và cài đặt vào máy tính của mình.



Hình 3.3. Mô đun Keylogger phần cứng và cài đặt trên máy tính để bàn

3.3. Các dạng tấn công thường gặp

Các dạng tấn công thường gặp là những dạng tấn công điển hình, xảy ra thường xuyên nhắm vào thông tin, hệ thống máy tính, hệ thống mạng và người dùng. Các dạng tấn công thường gặp bao gồm:

- Tấn công vào mật khẩu
- Tấn công bằng mã độc
- Tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán
- Tấn công giả mạo địa chỉ
- Tấn công nghe lén
- Tấn công kiểu người đứng giữa
- Tấn công bằng bom thư và thư rác
- Tấn công sử dụng các kỹ thuật xã hội
- Tấn công pharming
- Tấn công APT.

Phản tiếp theo của mục này trình bày chi tiết về các dạng tấn công thường gặp nêu trên và các biện pháp phòng chống tương ứng.

3.3.1. Tấn công vào mật khẩu

3.3.1.1. Giới thiệu

Tấn công vào mật khẩu (Password attack) là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản của người dùng để lạm dụng. Tên người dùng và mật khẩu không được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách chuyển đến máy chủ. Các thông tin này cũng có thể bị đánh cắp thông qua các dạng tấn công XSS, hoặc lừa đảo, bẫy người dùng cung cấp thông tin. Đây là một trong các dạng tấn công phổ biến nhất do hầu hết các ứng dụng sử cơ chế xác thực người dùng dựa trên tên người dùng,

hoặc địa chỉ email và mật khẩu. Nếu kẻ tấn công có tên người dùng và mật khẩu thì hắn có thể đăng nhập vào tài khoản và thực hiện các thao tác như người dùng hợp pháp.

Có thể chia tấn công vào mật khẩu thành 2 dạng:

- **Tấn công dựa trên từ điển** (Dictionary attack): Dạng tấn công này khai thác vấn đề người dùng có xu hướng chọn mật khẩu là các từ đơn giản cho dễ nhớ. Kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu, nhờ vậy có thể giảm số lần thử và tăng khả năng thành công. Danh sách các từ có tần suất sử dụng cao làm mật khẩu thường được biên soạn sẵn gọi là từ điển được dùng trong dạng tấn công này.
- **Tấn công vét cạn** (Brute force attack): Tấn công vét cạn sử dụng phương pháp sinh các tổ hợp các ký tự, số và tính toán để tìm mật khẩu một cách tự động. Phương pháp này thường được sử dụng với các mật khẩu đã được mã hóa. Kẻ tấn công sinh tổ hợp ký tự, sau đó mã hóa với cùng thuật toán mà hệ thống sử dụng, tiếp theo so sánh chuỗi mã hóa tạo từ tổ hợp ký tự với chuỗi mật khẩu mã hóa thu thập được. Nếu hai chuỗi mã hóa trùng nhau thì tổ hợp ký tự là mật khẩu đúng.

3.3.1.2. Phòng chống

Để đảm bảo an toàn cho mật khẩu, cần thực hiện kết hợp các biện pháp sau:

- Chọn mật khẩu đủ mạnh: Mật khẩu mạnh cho người dùng thông thường hiện nay cần có độ dài lớn hơn hoặc bằng 8 ký tự, gồm tổ hợp của 4 loại ký tự: chữ cái hoa, chữ cái thường, chữ số và ký tự đặc biệt (thuộc nhóm “?#\$*...”). Mật khẩu cho người quản trị hệ thống cần có độ dài lớn hơn hoặc bằng 10 ký tự cũng với tổ hợp các loại ký tự như mật khẩu cho người dùng thông thường.
- Định kỳ thay đổi mật khẩu: Thời hạn đổi mật khẩu tùy thuộc vào chính sách an ninh của cơ quan, tổ chức, có thể là 3 tháng, hoặc 6 tháng. Với yêu cầu này, hệ thống cần hỗ trợ cơ chế nhắc đổi mật khẩu khi đến hạn cho người dùng.
- Mật khẩu không nên lưu ở dạng rõ: Nên lưu mật khẩu ở dạng đã mã hóa sử dụng hàm băm một chiều.
- Hạn chế trao đổi tên người dùng và mật khẩu trên kênh truyền không được mã hóa.
- Nên hạn chế số lần đăng nhập lỗi, chẳng hạn nếu người dùng cố gắng đăng nhập với thông tin sai 3 lần liên tục sẽ bị khóa tài khoản trong một khoảng thời gian.

3.3.2. Tấn công bằng mã độc

3.3.2.1. Giới thiệu

Tấn công bằng mã độc (Malicious code attack) là dạng tấn công sử dụng các mã độc làm công cụ để tấn công hệ thống nạn nhân. Tấn công bằng mã độc có thể được chia thành 2 loại:

- Khai thác các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân. Loại tấn công này lại gồm 2 dạng con:
 - + Tấn công khai thác lỗ tràn bộ đệm
 - + Tấn công khai thác lỗ kiểm tra đầu vào, gồm tấn công chèn mã SQL (SQL injection) và tấn công sử dụng mã script, kiểu XSS, CSRF.

- Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại, như:
 - + Các phần mềm quảng cáo (Adware), gián điệp (Spyware)
 - + Các dạng mã độc như vi rút, zombie/bot, hay trojan.

Tấn công khai thác lỗ tràn bộ đệm đã được đề cập ở mục 2.2.1. Các dạng tấn công sử dụng mã script, kiểu XSS¹ và CSRF² đặc thù với các ứng dụng web sẽ được đề cập chi tiết trong môn học *An toàn ứng dụng web và cơ sở dữ liệu* của chương trình đào tạo đại học ngành An toàn thông tin, Học viện Công nghệ Bưu chính Viễn thông. Dạng tấn công lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại sẽ được đề cập ở mục 3.4. Phần tiếp theo của mục này đề cập về tấn công chèn mã SQL.

3.3.2.2. Tấn công chèn mã SQL

a. Khái quát

Tấn công chèn mã SQL (SQL injection hay SQLi) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và cuối cùng được thực hiện trên máy chủ cơ sở dữ liệu của hệ thống nạn nhân. Tấn công chèn mã SQL là dạng tấn công có thể thực hiện trên nhiều ứng dụng, nhưng rất phổ biến ở các ứng dụng web và các trang web có kết nối đến cơ sở dữ liệu. Hai nguyên nhân chính của lỗ hổng bảo mật trong ứng dụng cho phép thực hiện tấn công chèn mã SQL gồm:

- Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra, hoặc kiểm tra không đầy đủ;
- Các câu lệnh SQL động được sử dụng trong ứng dụng, trong đó có thao tác ghép nối dữ liệu đầu vào từ người dùng với mã lệnh SQL gốc.

Tùy vào mức độ tinh vi, tấn công chèn mã SQL có thể cho phép kẻ tấn công thực hiện các hành vi sau trên hệ thống nạn nhân:

- (1) Vượt qua các khâu xác thực người dùng;
- (2) Chèn, sửa đổi, hoặc xóa dữ liệu;
- (3) Đánh cắp các thông tin trong cơ sở dữ liệu; và
- (4) Chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu.

Các mục tiếp theo sẽ phân tích chi tiết cơ chế tấn công chèn mã SQL để thực hiện từng hành vi nêu trên.

b. Vượt qua các khâu xác thực người dùng

Xem xét một form đăng nhập và đoạn mã xử lý xác thực người dùng lưu trong bảng cơ sở dữ liệu tbl_accounts(username, password) cho như trên Hình 3.4.

```
<!-- Form đăng nhập -->
<form method="post" action="/log_in.asp">
  Tên đăng nhập: <input type="text" name="username"><br \>
  Mật khẩu: <input type="password" name="password"><br \>
```

¹ Đọc thêm về tấn công XSS tại <https://owasp.org/www-community/attacks/xss/>

² Đọc thêm về tấn công CSRF tại <https://owasp.org/www-community/attacks/csrf/>

```

<input type=submit name="login" value="Log In">
</form>

<%
' Mã xử lý đăng nhập trong file log_in.asp viết bằng ASP/VB:
' giả thiết đã kết nối với CSDL SQL servé qua đồi tượng
' conn và bảng tbl_accounts lưu thông tin người dùng
Dim username, password, sqlString, rsLogin
' lấy dữ liệu từ form
username = Request.Form("username")
password = Request.Form("password")
' tạo và thực hiện câu truy vấn sql
sqlString = "SELECT * FROM tbl_accounts WHERE username=''" &
username & "' AND password = '" & password & "'"
set rsLogin = conn.execute(sqlString)
if (NOT rsLogin.eof()) then
    ' cho phép đăng nhập, bắt đầu phiên làm việc
else
    ' từ chối đăng nhập, báo lỗi
end if
%>

```

Hình 3.4. Form đăng nhập và đoạn mã xử lý xác thực người dùng

Nếu người dùng nhập 'admin' vào trường *username* và 'abc123' vào trường *password* của form, mã xử lý hoạt động đúng: Nếu tồn tại người dùng với *username* và *password* kể trên, hệ thống sẽ cho phép đăng nhập với thông báo đăng nhập thành công; Ngược lại, nếu không tồn tại người dùng với *username* và *password* đã cung cấp, hệ thống sẽ từ chối đăng nhập và trả lại thông báo lỗi. Tuy nhiên, nếu người dùng nhập *aaaa' OR 1=1--* vào trường *username* và một chuỗi bất kỳ, chẳng hạn 'aaaa' vào trường *password* của form, mã xử lý hoạt động sai và chuỗi chứa câu truy vấn SQL trở thành:

```
SELECT * FROM tbl_accounts WHERE username='aaaa' OR 1=1--' AND password='aaaa'
```

Câu truy vấn sẽ trả về mọi bản ghi trong bảng do phần OR 1=1 làm cho điều kiện trong mệnh đề WHERE trở lên luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bởi ký hiệu (--). Phần lệnh SQL sau ký hiệu (--) được coi là chú thích và không được thực hiện. Nếu trong bảng *tbl_accounts* có chứa ít nhất một bản ghi, kẻ tấn công sẽ luôn đăng nhập thành công vào hệ thống.

c. Chèn, sửa đổi, hoặc xóa dữ liệu

Xem xét một form tìm kiếm sản phẩm và đoạn mã xử lý tìm sản phẩm lưu trong bảng cơ sở dữ liệu *tbl_products*(*product_id*, *product_name*, *product_desc*, *product_cost*) cho như trên Hình 3.5.

```

<!-- Form tìm kiếm sản phẩm -->
<form method="post" action="/search.asp">
    Từ khóa tìm sản phẩm: <input type="text" name="keyword">
    <input type="submit" name="search" value="Search">
</form>
<%
' Mã xử lý tìm sản phẩm trong file search.asp viết bằng ASP/VB:
' giả thiết đã kết nối với CSDL SQL server qua đối tượng
' conn và bảng tbl_products lưu thông tin sản phẩm
Dim keyword, sqlString, rsSearch
' lấy dữ liệu từ form
keyword = Request.Form("keyword")
' tạo và thực hiện câu truy vấn SQL
sqlString = "SELECT * FROM tbl_products WHERE product_name like
'%" & keyword & "%'"
set rsSearch = conn.execute(sqlString)
if (NOT rsSearch.eof()) then
    ' hiển thị danh sách các sản phẩm
else
    ' thông báo không tìm thấy sản phẩm
end if
%>

```

Hình 3.5. Form tìm kiếm sản phẩm và đoạn mã xử lý tìm sản phẩm

Nếu người dùng nhập chuỗi "**Samsung Galaxy S20**" vào trường *keyword* của form, mã xử lý hoạt động đúng: Nếu tìm thấy các sản phẩm có tên chứa từ khóa, hệ thống sẽ hiển thị danh sách các sản phẩm tìm thấy; Ngược lại, nếu không tìm thấy sản phẩm nào có tên chứa từ khóa, hệ thống thông báo không tìm thấy sản phẩm. Tuy nhiên, nếu người dùng nhập chuỗi "**Samsung Galaxy S20';DELETE FROM tbl_products;--**" vào trường *keyword* của form, mã xử lý sẽ hoạt động sai và chuỗi chứa câu truy vấn SQL trở thành:

SELECT * FROM tbl_products WHERE keyword like '%**Samsung Galaxy S20';DELETE FROM tbl_products;--%**'

Chuỗi lệnh SQL mới gồm 2 câu lệnh SQL: câu lệnh SELECT tìm kiếm các sản phẩm có tên chứa từ khóa "**Samsung Galaxy S20**" trong bảng *tbl_products* và câu lệnh DELETE xóa tất cả các sản phẩm lưu trong bảng *tbl_products*. Sở dĩ điều này có thể thực hiện được là do hệ quản trị cơ sở dữ liệu Microsoft SQL server nói riêng và hầu hết các hệ quản trị cơ sở dữ liệu quan hệ nói chung cho phép thực hiện nhiều lệnh SQL theo lô và dùng dấu (;) để ngăn cách các lệnh trong chuỗi lệnh. Ký hiệu "**--**" dùng để hủy tác dụng của phần lệnh còn lại nếu có.

Bằng thủ thuật tương tự, kẻ tấn công có thể thay lệnh **DELETE** bằng lệnh **UPDATE** hoặc **INSERT** để chỉnh sửa, hoặc chèn thêm các bản ghi vào bảng cơ sở dữ liệu. Chẳng hạn, kẻ tấn công chèn thêm lệnh **UPDATE** để cập nhật mật khẩu của người quản trị bằng

cách nhập chuỗi sau làm từ khóa tìm kiếm (giả thiết bảng tbl_administrators chưa thông tin tài khoản người quản trị):

```
Galaxy S20';UPDATE tbl_administrators SET password='abc123'  
WHERE username = 'admin';--
```

Hoặc kẻ tấn công có thể chèn thêm bản ghi vào bảng tbl_administrators bằng cách nhập chuỗi sau làm từ khóa tìm kiếm:

```
Galaxy S20';INSERT INTO tbl_administrators (username, password)  
VALUES ('attacker', 'abc12345');--
```

d. Đánh cắp các thông tin trong cơ sở dữ liệu

Lỗ hổng chèn mã SQL có thể cho phép kẻ tấn công đánh cắp dữ liệu trong cơ sở dữ liệu thông qua một số bước như sau:

- (1) Tìm lỗ hổng chèn mã SQL và thăm dò các thông tin về hệ quản trị cơ sở dữ liệu:
 - + Nhập một số dữ liệu mẫu vào các trường nhập liệu hoặc URL để kiểm tra một trang web có chứa lỗ hổng chèn mã SQL, như các dấu nháy đơn, dấu --, ...
 - + Tìm phiên bản máy chủ cơ sở dữ liệu: nhập các câu lệnh lỗi và kiểm tra thông báo lỗi, hoặc sử dụng biến @@version với Microsoft SQL Server, hoặc hàm version() với MySQL trong câu lệnh ghép sử dụng UNION SELECT.
- (2) Tìm thông tin về số lượng và kiểu dữ liệu các trường của câu truy vấn hiện tại của trang web.
 - + Sử dụng mệnh đề ORDER BY <số thứ tự của trường>, hoặc
 - + Sử dụng UNION SELECT 1, 2, 3, ...
- (3) Trích xuất thông tin về các bảng, các trường của cơ sở dữ liệu thông qua các bảng hệ thống (metadata). Chẳng hạn, với hệ quản trị cơ sở dữ liệu Microsoft SQL Server, các bảng “sys.objects”, “sys.tables” và “sys.columns” được sử dụng tương ứng để lưu thông tin quản lý các đối tượng, các bảng dữ liệu người dùng và các trường của các bảng.
- (4) Sử dụng UNION SELECT để ghép các thông tin định trích xuất vào câu truy vấn hiện tại của ứng dụng.

e. Chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu

Khả năng máy chủ cơ sở dữ liệu bị chiếm quyền điều khiển xảy ra khi trang web tồn tại đồng thời 2 lỗ hổng bảo mật, bao gồm: (1) lỗ hổng cho phép tấn công chèn mã SQL và (2) lỗ hổng thiết lập quyền truy cập cơ sở dữ liệu. Lỗ hổng (2) liên quan đến việc sử dụng người dùng có quyền quản trị để truy cập và thao tác dữ liệu của trang web. Khai thác 2 lỗ hổng này, kẻ tấn công có thể triệu gọi thực hiện các lệnh hệ thống của máy chủ cơ sở dữ liệu cho phép can thiệp sâu vào cơ sở dữ liệu, hệ quản trị cơ sở dữ liệu và cả hệ điều hành nền. Chẳng hạn, hệ quản trị cơ sở dữ liệu Microsoft SQL Server cung cấp thủ tục *sp_send_dbmail* cho phép gửi email từ máy chủ cơ sở dữ liệu và thủ tục *xp_cmdshell* cho phép chạy các lệnh và chương trình cài đặt trên hệ điều hành Microsoft Windows.

Sau đây là một số ví dụ chạy các lệnh của Microsoft Windows thông qua thủ tục `xp_cmdshell`:

EXEC `xp_cmdshell 'dir *.exe'` : liệt kê nội dung thư mục hiện thời

EXEC `xp_cmdshell 'shutdown /s /t 00'` : tắt máy chủ nền chạy hệ quản trị CSDL

EXEC `xp_cmdshell 'net stop W3SVC'` : dừng hoạt động máy chủ web Microsoft IIS chạy trên cùng hệ thống

EXEC `xp_cmdshell 'net stop MSSQLSERVER'` : dừng hoạt động máy chủ CSDL Microsoft SQL server chạy trên hệ thống.

Ngoài ra, kẻ tấn công có thể thực hiện các thao tác nguy hiểm đến cơ sở dữ liệu nếu có quyền của người quản trị cơ sở dữ liệu, hoặc quản trị hệ thống, như:

Xóa cả bảng (gồm cả cấu trúc): `DROP TABLE <tên bảng>`

Xóa cả cơ sở dữ liệu: `DROP DATABASE <tên CSDL>`

Tạo 1 tài khoản mới truy cập CSDL: `sp_addlogin <username> <password>`

Đổi mật khẩu tài khoản truy cập CSDL: `sp_password <password>`

f. Phòng chống

Do tính chất nguy hiểm của tấn công chèn mã SQL, nhiều giải pháp đã được đề xuất nhằm hạn chế tác hại và ngăn chặn triệt để dạng tấn công này. Nhìn chung, cần áp dụng kết hợp các biện pháp phòng chống tấn công chèn mã SQL để đảm bảo an toàn cho hệ thống. Các biện pháp, kỹ thuật cụ thể có thể áp dụng bao gồm:

- Kiểm tra và lọc dữ liệu đầu vào:
 - + Kiểm tra kích thước và định dạng của tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
 - + Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt (như *, ‘, =, --) và các từ khóa của ngôn ngữ SQL (SELECT, INSERT, UPDATE, DELETE, DROP,...) mà kẻ tấn công có thể sử dụng.
- Sử dụng thủ tục cơ sở dữ liệu (stored procedure) nếu hệ quản trị cơ sở dữ liệu hỗ trợ thủ tục, hoặc cơ chế tham số hóa dữ liệu:
 - + Đưa tất cả các câu lệnh truy vấn (SELECT) và câu lệnh cập nhật, sửa, xóa dữ liệu (INSERT, UPDATE, DELETE) vào các thủ tục. Dữ liệu truyền vào thủ tục thông qua các tham số, giúp tách dữ liệu khỏi mã lệnh SQL, nhờ đó ngăn chặn hiệu quả tấn công chèn mã SQL;
 - + Hạn chế thực hiện các câu lệnh SQL động trong thủ tục;
 - + Sử dụng cơ chế tham số hóa dữ liệu được hỗ trợ bởi nhiều ngôn ngữ lập trình web như ASP.NET, PHP và JSP.
- Thiết lập quyền truy cập phù hợp cho người dùng cơ sở dữ liệu:
 - + Không sử dụng người dùng có quyền quản trị hệ thống hoặc quản trị cơ sở dữ liệu làm người dùng truy cập dữ liệu. Ví dụ: không sử dụng người dùng `sa` trong Microsoft SQL server hoặc `root` trong MySQL làm người dùng truy cập dữ liệu.

Chỉ sử dụng những người dùng này cho mục đích quản trị hệ thống và quản trị cơ sở dữ liệu.

- + Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện các câu lệnh SQL và thực thi các thủ tục.
- + Trường hợp tốt nhất, không cấp quyền thực thi các câu lệnh truy vấn, cập nhật, sửa, xóa trực tiếp trên các bảng dữ liệu. Thủ tục hóa tất cả các câu lệnh SQL và chỉ cấp quyền thực thi thủ tục.
- + Cấm hoặc vô hiệu hóa việc thực thi các thủ tục hệ thống cho phép can thiệp vào hệ quản trị cơ sở dữ liệu và hệ điều hành nền.
- Sử dụng các công cụ rà quét lỗ hổng chèn mã SQL, như SQLMap, hoặc Acunetix Vulnerability Scanner để chủ động rà quét, tìm các lỗ hổng chèn mã SQL và có biện pháp khắc phục phù hợp.

3.3.3. Tấn công từ chối dịch vụ

3.3.3.1. Giới thiệu

Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy cập các tài nguyên mạng. Tấn công DoS có thể được chia thành 2 loại: (1) tấn công lô gíc và (2) tấn công gây ngập lụt. Tấn công lô gíc là dạng tấn công khai thác các lỗi phần mềm làm dịch vụ ngừng hoạt động, hoặc làm giảm hiệu năng hệ thống. Tấn công DoS sử dụng sâu SQL Slammer đề cập ở mục 2.2.1.2.c là dạng tấn công lô gíc khai thác lỗi tràn bộ đệm trong phần mềm. Ngược lại, trong tấn công gây ngập lụt, kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

Có nhiều kỹ thuật tấn công DoS đã được phát hiện trên thực tế. Các kỹ thuật tấn công DoS thường gặp bao gồm: SYN Flood, Smurf, Teardrop, Ping of Death, Land Attack, ICMP Flood, HTTP Flood, UDP Flood,... Trong phạm vi của tài liệu này, chúng ta tập trung đề cập đến 2 kỹ thuật tấn công DoS phổ biến nhất là SYN Flood và Smurf.

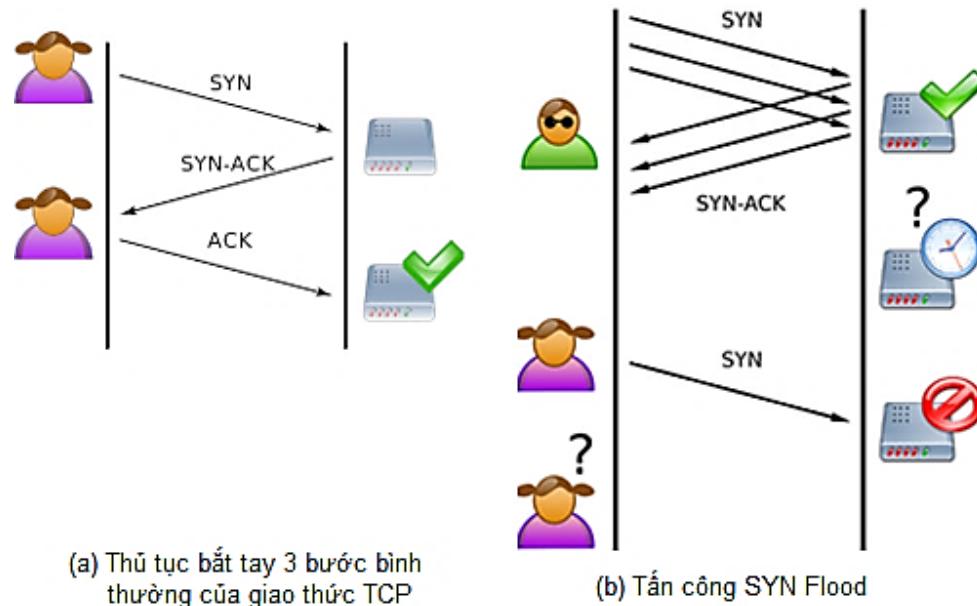
3.3.3.2. Tấn công SYN Flood

a. Giới thiệu

Tấn công SYN Flood là kỹ thuật tấn công DoS khai thác điểm yếu trong thủ tục bắt tay 3 bước (3-way handshake) khi hai bên tham gia truyền thông thiết lập kết nối TCP để bắt đầu phiên trao đổi dữ liệu. SYN là bit cờ điều khiển của giao thức TCP dùng để đồng bộ số trình tự gói tin. Thủ tục bắt tay khi một người dùng hợp pháp thiết lập một kết nối TCP đến máy chủ, như minh họa trên hình Hình 3.6 (a) gồm 3 bước như sau:

- (1) Người dùng thông qua máy khách gửi yêu cầu mở kết nối (SYN hay SYN-REQ) đến máy chủ;
- (2) Máy chủ nhận được yêu cầu kết nối, lưu vào Bảng kết nối (gọi là Backlog) và gửi lại xác nhận kết nối SYN-ACK cho máy khách;
- (3) Khi nhận được SYN-ACK từ máy chủ, máy khách gửi lại xác nhận kết nối ACK đến máy chủ. Khi máy chủ nhận được xác nhận kết nối ACK từ máy khách, nó xác

nhận kết nối mở thành công, máy chủ và máy khách bắt đầu phiên truyền thông TCP. Bản ghi mở kết nối được xóa khỏi Bảng kết nối.



Hình 3.6. (a) Thủ tục bắt tay 3 bước của giao thức TCP và (b) Tấn công SYN Flood

b. Kịch bản tấn công

Kịch bản tấn công SYN Flood, như minh họa trên Hình 3.6 (b) gồm các bước sau:

- (1) Kẻ tấn công gửi một lượng lớn yêu cầu mở kết nối (SYN-REQ) đến máy nạn nhân;
- (2) Nhận được yêu cầu mở kết nối, máy nạn nhân lưu yêu cầu kết nối vào Bảng kết nối trong bộ nhớ;
- (3) Máy nạn nhân sau đó gửi xác nhận kết nối (SYN-ACK) đến kẻ tấn công;
- (4) Do kẻ tấn công không gửi lại xác nhận kết nối ACK, nên máy nạn nhân vẫn phải lưu tất cả các yêu cầu mở kết nối chưa được xác nhận trong Bảng kết nối. Khi Bảng kết nối bị điền đầy thì các yêu cầu mở kết nối mới của người dùng hợp pháp sẽ bị từ chối;
- (5) Máy nạn nhân chỉ có thể xóa một yêu cầu mở kết nối chưa được xác nhận khi nó hết hạn (timed-out).

Do kẻ tấn công sử dụng địa chỉ giả mạo, hoặc địa chỉ không có thực làm địa chỉ nguồn (Source IP) trong gói tin IP của yêu cầu mở kết nối, nên xác nhận kết nối SYN-ACK gửi từ máy nạn nhân không thể đến đích. Đồng thời, kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu mở kết nối dở dang để chúng điền đầy Bảng kết nối. Hậu quả là máy nạn nhân không thể chấp nhận yêu cầu mở kết nối của những người dùng khác. Tấn công SYN Flood làm cạn kiệt tài nguyên bộ nhớ Bảng kết nối của máy nạn nhân, đồng thời có thể làm máy nạn nhân ngừng hoạt động và gây nghẽn đường truyền mạng.

c. Phòng chống

Nhiều biện pháp phòng chống tấn công SYN Flood được đề xuất, nhưng cho đến hiện nay chưa có giải pháp nào có khả năng ngăn chặn triệt để dạng tấn công này. Do vậy, để phòng chống tấn công SYN Flood hiệu quả, cần kết hợp các biện pháp sau:

- Sử dụng kỹ thuật lọc địa chỉ giả mạo (Spoofed IP Filtering): Kỹ thuật này đòi hỏi chỉnh sửa giao thức TCP/IP nhằm không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước Bảng kết nối: Tăng kích thước Bảng kết nối cho phép tăng khả năng chấp nhận các yêu cầu mở kết nối;
- Giảm thời gian chờ (SYN-RECEIVED Timer): Các yêu cầu mở kết nối chưa được xác nhận sẽ bị xóa sớm hơn khi thời gian chờ ngắn hơn;
- Sử dụng SYN cache: SYN cache thay mặt máy chủ tiếp nhận yêu cầu mở kết nối và yêu cầu này chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng tường lửa và Proxy: Tường lửa và proxy có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực, đồng thời chúng có khả năng tiếp nhận yêu cầu mở kết nối, chờ đến khi có xác nhận mới chuyển cho máy chủ đích.

3.3.3.3. Tấn công Smurf

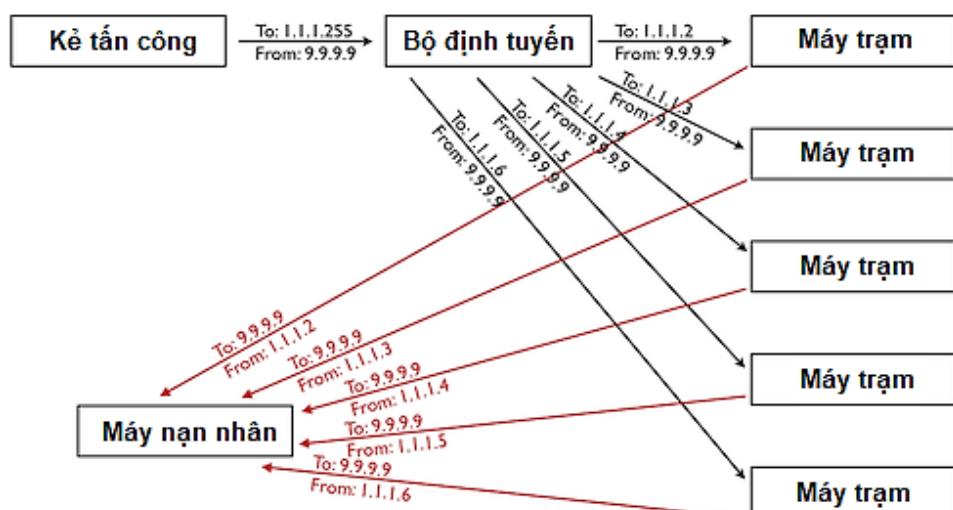
a. Giới thiệu

Tấn công Smurf là dạng tấn công DoS sử dụng giao thức ICMP và kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân. Trên mỗi phân vùng mạng IP thường có 1 địa chỉ quảng bá, theo đó khi có một gói tin gửi tới địa chỉ này, nó sẽ được bộ định tuyến của mạng chuyển đến tất cả các máy trong mạng đó.

b. Kịch bản tấn công

Hình 3.7 minh họa mô hình tấn công Smurf, với kịch bản gồm các bước như sau:

- (1) Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP với địa chỉ IP nguồn là địa chỉ của máy nạn nhân (From: 9.9.9.9) đến một địa chỉ quảng bá của một mạng (To: 1.1.1.255);
- (2) Bộ định tuyến của mạng nhận được yêu cầu ICMP gửi đến địa chỉ quảng bá sẽ tự động chuyển yêu cầu này đến tất cả các máy trong mạng (To: 1.1.1.2,...);
- (3) Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời đến máy có địa chỉ IP là địa nguồn trong yêu cầu ICMP (To: 9.9.9.9). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền, hoặc ngừng hoạt động.



Hình 3.7. Mô hình tấn công Smurf

c. Phòng chống

Có thể sử dụng các biện pháp sau để phòng chống tấn công Smurf:

- Cấu hình các máy trong mạng và router không trả lời các yêu cầu ICMP, hoặc các yêu cầu phát quảng bá;
- Cấu hình các router không chuyển tiếp yêu cầu ICMP gửi đến các địa chỉ quảng bá của mạng;
- Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.

Việc cấu hình các bộ định tuyến không chuyển tiếp yêu cầu ICMP, hoặc các máy trong mạng không trả lời các yêu cầu ICMP có thể gây khó khăn cho các ứng dụng dựa trên phát quảng bá và giao thức ICMP, như ứng dụng giám sát trạng thái hoạt động của các máy trong mạng dựa trên giao thức ICMP.

3.3.4. Tấn công từ chối dịch vụ phân tán

3.3.4.1. Giới thiệu

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) là một loại tấn công DoS đặc biệt, liên quan đến việc gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo. Điểm khác biệt chính giữa DDoS và DoS là phạm vi tấn công: trong khi số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm, thì số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc hàng trăm ngàn máy. Đồng thời, các máy tham gia tấn công DDoS có thể đến từ rất nhiều vị trí địa lý khác nhau, phân tán trên toàn cầu. Do vậy, việc phòng chống tấn công DDoS gấp nhiều khó khăn hơn so với việc phòng chống tấn công DoS.

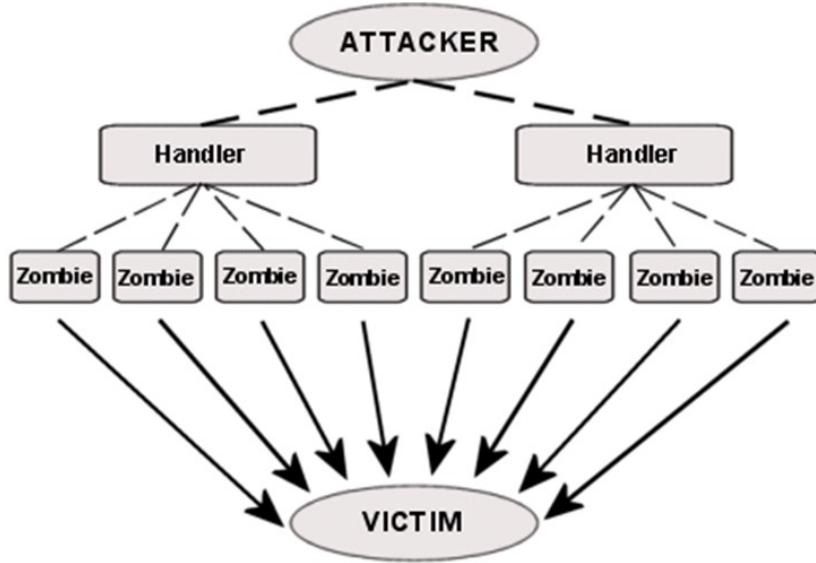
Có thể chia tấn công DDoS thành 2 dạng chính theo mô hình kiến trúc: tấn công DDoS trực tiếp (Direct DDoS) và tấn công DDoS gián tiếp, hay phản xạ (Indirect/Reflective DDoS). Trong tấn công DDoS trực tiếp, các yêu cầu tấn công được các máy tấn công gửi trực tiếp đến hệ thống nạn nhân. Ngược lại, trong tấn công DDoS gián tiếp, các yêu cầu tấn công được gửi đến các máy phản xạ (Reflector) và sau đó gián tiếp chuyển đến hệ thống nạn nhân. Các mục tiếp theo sẽ trình bày chi tiết về hai dạng tấn công DDoS nêu trên.

3.3.4.2. Tấn công DDoS trực tiếp

Hình 3.8 minh họa kiến trúc điển hình của dạng tấn công DDoS trực tiếp. Theo đó, tấn công DDoS trực tiếp được thực hiện theo nhiều giai đoạn với kịch bản như sau:

- (1) Kẻ tấn công (Attacker) chiếm quyền điều khiển hàng ngàn, thậm chí hàng chục ngàn máy tính, hoặc thiết bị tính toán (gọi chung là máy tính) có kết nối Internet, sau đó bí mật cài đặt các agent tự động lên các máy này. Các agent tự động cho phép kẻ tấn công điều khiển các máy này từ xa. Các máy tính được cài đặt agent tự động và bị điều khiển từ xa được gọi là các máy tính ma;
- (2) Các máy tính ma (gọi chung là bot) hình thành mạng máy tính ma, được gọi là botnet hay zombie network (gọi chung là botnet). Các botnet không bị giới hạn bởi chủng loại thiết bị và tô pô mạng vật lý;

- (3) Kẻ tấn công có thể giao tiếp với các bot thông qua một mạng lưới các máy trung gian (gọi là Handler) gồm nhiều tầng. Phương thức giao tiếp có thể là các giao thức truyền thông, như IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP,...
- (4) Tiếp theo, kẻ tấn công ra lệnh cho các bot trong botnet mà mình quản lý đồng loạt tạo các yêu cầu giả mạo gửi đến các hệ thống nạn nhân (Victim) tạo thành một cuộc tấn công DDoS;
- (5) Lượng yêu cầu giả mạo có thể rất lớn, đến từ rất nhiều máy trong botnet với vị trí địa lý khác nhau phân tán trên toàn cầu nên việc đối phó và lẩn vét để tìm ra kẻ tấn công thực sự là rất khó khăn.



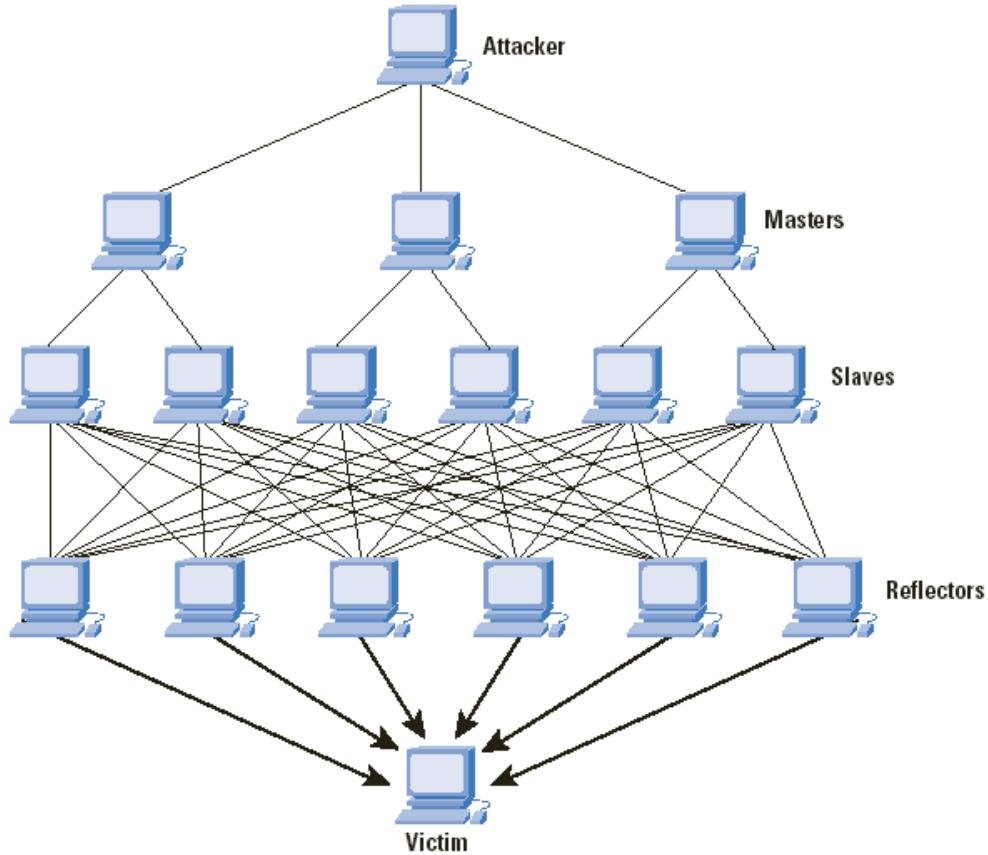
Hình 3.8. Kiến trúc tấn công DDoS trực tiếp

3.3.4.3. Tấn công DDoS gián tiếp

Hình 3.9 minh họa kiến trúc tấn công DDoS gián tiếp, hay phản xạ. Theo đó, tấn công DDoS gián tiếp cũng được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- (1) Kẻ tấn công chiếm quyền điều khiển của một lượng lớn máy tính, hoặc thiết bị tính toán trên mạng Internet, sau đó cài đặt agent tự động và biến chúng thành các bot, hay zombie (gọi là slave). Các bot hình thành nên mạng botnet.
- (2) Kẻ tấn công giao tiếp với các bot thông qua một mạng lưới các máy trung gian (Masters) gồm nhiều tầng sử dụng các giao thức truyền thông, như IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP,...
- (3) Theo lệnh của kẻ tấn công, các Bot/Slave trong botnet gửi một lượng lớn yêu cầu (Request) giả mạo với địa chỉ nguồn là địa chỉ hệ thống nạn nhân đến một số lớn các máy khác (Reflectors – máy phản xạ) trên mạng Internet;
- (4) Các Reflector gửi các phản hồi (Reply) đến hệ thống nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;
- (5) Khi các yêu cầu giả mạo gửi đến các Reflector có số lượng rất lớn, số lượng phản hồi cũng sẽ rất lớn gây ngập lụt đường truyền mạng, hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người

dùng. Các Reflector bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất và băng thông đường truyền lớn trên Internet và không chịu sự điều khiển của kẻ tấn công.



Hình 3.9. Kiến trúc tấn công DDoS gián tiếp hay phản xạ

3.3.4.4. Phòng chống tấn công DDoS

Nhìn chung, để phòng chống tấn công DDoS hiệu quả, cần kết hợp nhiều biện pháp và sự phối hợp của nhiều bên do tấn công DDoS có tính phân tán cao và hệ thống mạng máy tính ma được hình thành và điều khiển theo nhiều tầng, nhiều lớp. Sau đây là một số biện pháp có thể xem xét áp dụng:

- Sử dụng các phần mềm rà quét vi rút và các phần mềm độc hại nhằm loại bỏ các loại bot, zombie, slave khỏi các hệ thống máy tính, hoặc các thiết bị tính toán có kết nối Internet của người dùng;
- Sử dụng các hệ thống lọc đặt trên các bộ định tuyến, tường lửa của các nhà cung cấp dịch vụ Internet (ISP) để lọc các yêu cầu điều khiển (C&C – Command and Control) gửi từ kẻ tấn công đến các bot;
- Sử dụng các hệ thống giám sát, phát hiện bất thường, nhằm phát hiện sớm các dấu hiệu của tấn công DDoS.
- Sử dụng tường lửa để chặn tạm thời các cổng dịch vụ, hoặc các địa chỉ bị tấn công.

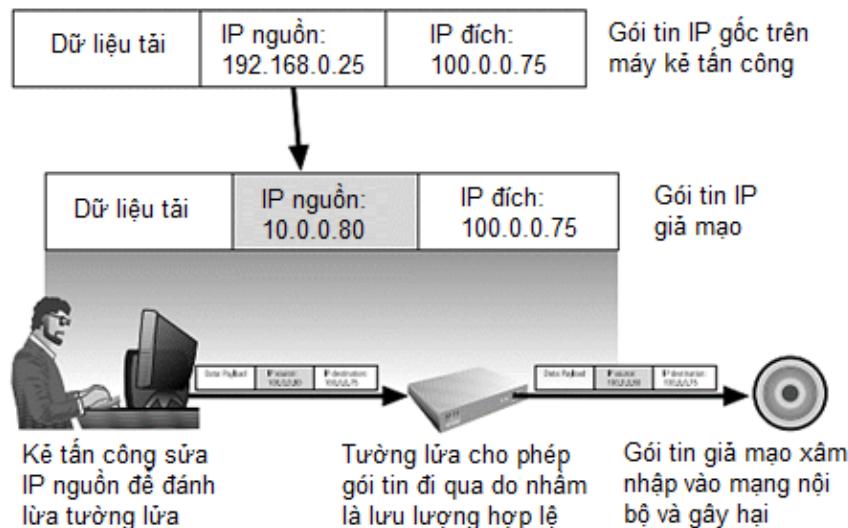
3.3.5. Tấn công giả mạo địa chỉ

Tấn công giả mạo địa chỉ (Address spoofing attack) là dạng tấn công sử dụng địa chỉ giả, hoặc địa chỉ không có thực để đánh lừa nạn nhân. Trên mạng Internet, thông tin địa

chỉ thường hay bị giả mạo là địa chỉ IP và địa chỉ email. Mục này chỉ đề cập đến tấn công giả mạo địa chỉ IP, trong đó kẻ tấn công sử dụng địa chỉ IP giả làm địa chỉ IP nguồn của các gói tin IP gửi đi, thường để đánh lừa máy nạn nhân nhằm vượt qua hàng rào kiểm soát an ninh thông thường. Chẳng hạn, nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của một máy trong mạng LAN, hắn có thể có nhiều cơ hội xâm nhập vào các máy khác trong mạng LAN đó do chính sách kiểm soát an ninh đối với các máy trong cùng mạng LAN thường được giảm nhẹ.

Hình 3.10 minh họa một cuộc tấn công giả mạo địa chỉ IP vào một máy nạn nhân trong mạng cục bộ. Các bước thực hiện như sau:

- (1) Giả sử máy tính của kẻ tấn công có địa chỉ IP là 192.168.0.25 và hắn muốn gửi gói tin tấn công đến máy nạn nhân có địa chỉ IP là 100.0.0.75;
- (2) Kẻ tấn công tạo và gửi yêu cầu giả mạo với địa chỉ IP nguồn của các gói tin IP của yêu cầu là 100.0.0.80 và gửi đến máy nạn nhân. Địa chỉ IP 100.0.0.80 là địa chỉ cùng mạng LAN với máy nạn nhân có địa chỉ IP là 100.0.0.75;
- (3) Nếu tường lửa của mạng LAN không lọc được các gói tin với địa chỉ nguồn giả mạo, yêu cầu giả mạo của kẻ tấn công có thể đến được mạng cục bộ và gây tác hại cho máy nạn nhân.



Hình 3.10. Minh họa quá trình tấn công giả mạo địa chỉ IP

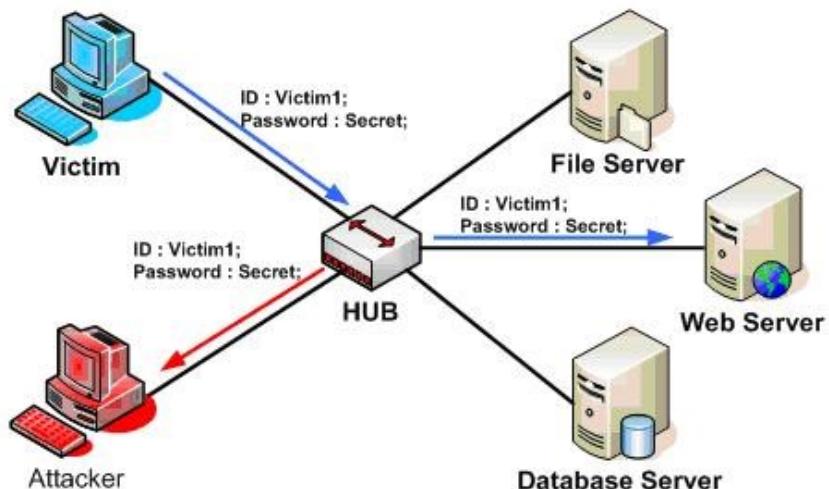
Biện pháp phòng chống tấn công giả mạo địa chỉ IP hiệu quả nhất là sử dụng kỹ thuật lọc trên tường lửa, hoặc các bộ định tuyến với nguyên tắc lọc như sau: các gói tin từ mạng ngoài đi vào mạng LAN mà có địa chỉ IP nguồn là địa chỉ nội bộ của mạng LAN đó thì chúng là các gói tin giả mạo và phải bị chặn.

3.3.6. Tấn công nghe lén

Tấn công nghe lén (Sniffing/Eavesdropping) là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub, switch, router, hoặc môi trường truyền dẫn để bắt các gói tin dùng cho phân tích, hoặc lạm dụng về sau. Đây là kiểu tấn công thụ động nhằm thu thập các thông tin nhạy cảm, hoặc giám sát lưu lượng mạng. Các thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin thanh toán nếu không được

mã hóa có thể bị nghe lén và lạm dụng. Các thông tin truyền trong mạng WiFi, hoặc các mạng không dây khác cũng có thể bị nghe lén dễ dàng do môi trường truyền dẫn vô tuyến và nếu không sử dụng các cơ chế bảo mật đủ mạnh.

Hình 3.11 minh họa một mô hình tấn công nghe lén, trong đó kẻ tấn công (Attacker) cài đặt công cụ lắng nghe trên thiết bị mạng HUB nhằm bắt toàn bộ lưu lượng mạng trao đổi giữa máy nạn nhân (Victim) và máy chủ web (Web Server). Nếu lưu lượng mạng giữa máy nạn nhân và máy chủ web không được mã hóa đủ mạnh, kẻ tấn công có thể trích xuất các thông tin nhạy cảm, như tên người dùng (ID) và mật khẩu (Password) gửi từ máy nạn nhân đến máy chủ web.



Hình 3.11. Một mô hình tấn công nghe lén

Để phòng chống tấn công nghe lén, có thể áp dụng các biện pháp sau:

- Có cơ chế bảo vệ các thiết bị mạng và hệ thống truyền dẫn ở mức vật lý;
- Sử dụng các biện pháp, cơ chế xác thực người dùng đủ mạnh;
- Sử dụng các biện pháp bảo mật thông tin truyền dựa trên các kỹ thuật mã hóa.

3.3.7. Tấn công kiểu người đứng giữa

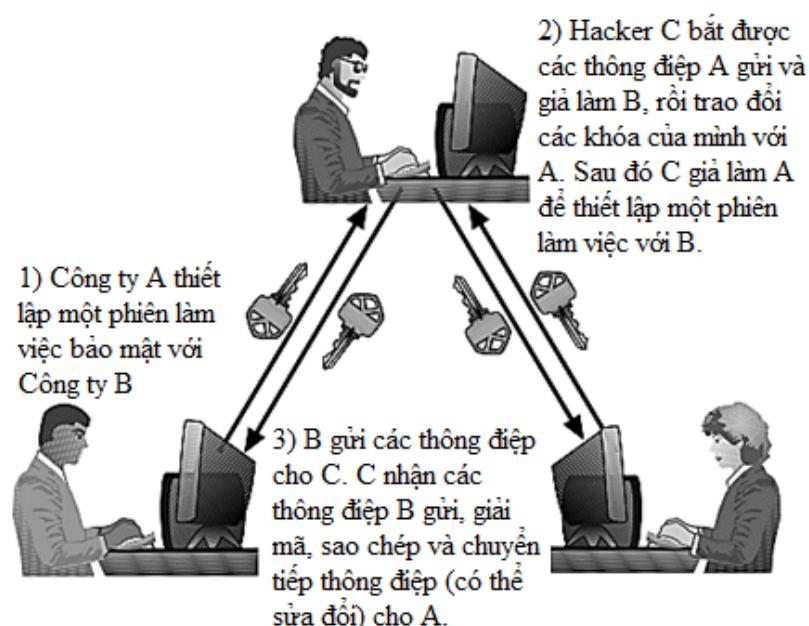
Tấn công kiểu người đứng giữa (Man in the middle attack - MITM) là dạng tấn công khai thác quá trình chuyển gói tin đi qua nhiều trạm thuộc các mạng khác nhau, trong đó kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông và chuyển thông điệp lại cho bên kia. Mục đích chính của dạng tấn công này là đánh cắp thông tin. Hình 3.12 minh họa mô hình chung của tấn công kiểu người đứng giữa trong một phiên truyền file ở dạng rõ sử dụng giao thức FTP giữa máy khách (Client) và máy chủ (Server).



Hình 3.12. Mô hình chung của tấn công kiểu người đứng giữa

Hình 3.13 biểu diễn một kịch bản tấn công kiểu người đứng giữa, trong đó hai bên A và B (Công ty A và Công ty B) trao đổi các thông điệp bí mật và kẻ tấn công C (Hacker) chặn bắt và có thể sửa đổi, lạm dụng các thông điệp trao đổi giữa A và B. Các bước tấn công cụ thể như sau:

- (1) A gửi các thông điệp để thiết lập một phiên làm việc bảo mật với B;
- (2) C bắt được các thông điệp A gửi. C giả làm B và trao đổi các khóa của mình với A. Sau đó C giả làm A để thiết lập một phiên làm việc có trao đổi khóa với B;
- (3) B gửi các thông điệp cho C mà vẫn tưởng như đang liên lạc với A. C nhận các thông điệp B gửi, giải mã bằng khóa của mình (và có thể sửa đổi), sau đó chuyển tiếp thông điệp cho A. A nhận các thông điệp mà không biết là chúng đã bị C bắt và lạm dụng.



Hình 3.13. Một kịch bản tấn công kiểu người đứng giữa

Một trong các biện pháp hiệu quả để phòng chống tấn công kiểu người đứng giữa là hai bên tham gia truyền thông phải có cơ chế xác thực thông tin nhận dạng của nhau và xác thực tính toàn vẹn của các thông điệp trao đổi. Chẳng hạn, các bên có thể sử dụng chứng thư số khóa công khai để xác thực thông tin nhận dạng của nhau và sử dụng chữ ký số để đảm bảo tính toàn vẹn của các thông điệp trao đổi. Ngoài ra, các bên có thể sử dụng kỹ thuật mã hóa dữ liệu để đảm bảo tính bí mật của các thông điệp trao đổi có chứa thông tin cá nhân, hoặc nhạy cảm.

3.3.8. Tấn công bằng bom thư và thư rác

Tấn công bằng bom thư (Mail bombing attack) là một dạng tấn công DoS khi kẻ tấn công gửi một lượng rất lớn email đến hộp thư của nạn nhân. Khi đó hộp thư và cả máy chủ nạn nhân có thể bị tê liệt và không thể hoạt động bình thường. Tấn công bằng bom thư có thể được thực hiện bằng một số thủ thuật như sau:

- Gửi bom thư bằng cách sử dụng các kỹ thuật xã hội, lừa nhiều người dùng phát tán một số lượng lớn email;

- Khai thác lỗi trong hệ thống gửi/nhận email sử dụng giao thức SMTP;
- Lợi dụng các máy chủ email không được cấu hình an toàn để gửi email cho chúng.

Tấn công bằng thư rác (Email spamming attack) là dạng tấn công gửi các email không mong muốn, như email quảng cáo, email chứa các phần mềm độc hại. Theo một số thống kê, khoảng 70-80% lượng email gửi trên mạng Internet là email rác [5][6]. Kẻ tấn công thường sử dụng các máy tính bị điều khiển (bot/zombie) để gửi email cho chúng. Spam email gây lãng phí tài nguyên tính toán và thời gian của người dùng.

Có thể hạn chế, hoặc giảm thiểu tác hại của hình thức tấn công bằng bom thư và thư rác sử dụng các biện pháp sau:

- Cấu hình máy chủ email SMTP hỗ trợ các giải pháp bảo mật email, như xác thực người gửi, hoặc xác thực máy chủ gửi email (SPF, DKIM, S/MIME...);
- Sử dụng các bộ lọc thư rác tập trung trên máy chủ email cũng như phân tán trên các máy khách email.

3.3.9. Tấn công sử dụng các kỹ thuật xã hội

3.3.9.1. Giới thiệu

Tấn công sử dụng các kỹ thuật xã hội (Social engineering attack) là dạng tấn công phi kỹ thuật nhằm vào người dùng. Dạng tấn công này khai thác các điểm yếu cố hữu của người dùng, như cả tin, ngây thơ, tò mò và lòng tham. Dạng thường gặp của kiểu tấn công này là thuyết phục người dùng tiết lộ thông tin truy cập hoặc các thông tin có giá trị cho kẻ tấn công. Một số kỹ thuật xã hội mà kẻ tấn công thường sử dụng gồm:

- Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng, từ đó thuyết phục hoặc đánh lừa nạn nhân cung cấp thông tin;
- Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân, hoặc tổ chức;
- Kẻ tấn công có thể lập trang web giả các trang web của các tổ chức để đánh lừa người dùng cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,...

3.3.9.2. Trò lừa đảo Nigeria 4-1-9

Trò lừa đảo Nigeria 4-1-9 là một trong các dạng tấn công sử dụng các kỹ thuật xã hội nổi tiếng nhất khởi phát ở Nigeria, sau đó đã lan ra nhiều nước khác, trong đó đã có hàng chục nghìn người ở Hoa Kỳ, Canada và Châu Âu đã sập bẫy của những kẻ lừa đảo. Kẻ lừa đảo lợi dụng sự ngây thơ và lòng tham của một số người để thực hiện tấn công với kịch bản tóm tắt như sau:

- (1) Kẻ lừa đảo gửi thư tay, hoặc email đến nhiều người nhận, mô tả về việc có 1 khoản tiền lớn (tù thừa kế, hoặc lợi tức,...) cần chuyển ra nước ngoài, nhờ người nhận giúp đỡ để hoàn thành giao dịch. Khoản tiền có thể lên đến hàng chục, hoặc trăm triệu USD. Kẻ lừa đảo hứa sẽ trả cho người hỗ trợ một phần số tiền, có thể lên đến 20-30% khoản tiền;
- (2) Nếu người nhận có phản hồi và đồng ý tham gia hỗ trợ, kẻ lừa đảo sẽ gửi tiếp thư, hoặc email khác, yêu cầu chuyển trước cho hắn 1 khoản phí giao dịch chuyển tiền

(từ vài ngàn đến hàng chục ngàn USD) với lý do hắn không có đủ tiền và khoản tiền trên không thể rút ra ở trong nước;

- (3) Nếu người nhận gửi tiền phí giao dịch theo yêu cầu thì người đó sẽ mất tiền, do giao dịch mà kẻ lừa đảo hứa hẹn là giả mạo.

Nhiều biến thể của trò lừa đảo Nigeria 4-1-9 đã xuất hiện trong những năm gần đây trên thế giới cũng như ở Việt Nam [5], chẳng hạn như thông báo lừa trúng thưởng các tài sản có giá trị lớn (như điện thoại thông minh, xe máy,...) để chiếm đoạt khoản “phí trả thưởng” thông qua thẻ cào điện thoại, thẻ game,..; lừa đầu tư vào tài khoản vàng ảo, lừa mua gian hàng ảo với hứa hẹn lợi suất cao...

3.3.9.3. Phishing

Phishing là một dạng đặc biệt phát triển rất mạnh và tinh vi của tấn công sử dụng các kỹ thuật xã hội, trong đó kẻ tấn công bẫy người dùng để đánh cắp thông tin cá nhân, thông tin tài khoản, thông tin thẻ tín dụng,... Kẻ tấn công thường lập các trang web giả mạo có giao diện giống hệt các trang web của các tổ chức tài chính, ngân hàng, sau đó chúng gửi email cho người dùng yêu cầu xác thực thông tin. Địa chỉ email của người dùng có thể được thu thập trên Internet, hoặc đánh cắp từ các cơ sở dữ liệu của các cơ quan, tổ chức. Hình 3.14 và Hình 3.15 minh họa 2 email lừa đảo gửi cho khách hàng tương ứng của mạng đấu giá trực tuyến eBay và ngân hàng Royal Bank yêu cầu người dùng cập nhật thông tin thanh toán đã hết hạn, hoặc xác nhận thông tin tài khoản đã lâu không sử dụng. Nếu người dùng làm theo hướng dẫn thì sẽ vô tình cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng cho kẻ tấn công.



Hình 3.14. Một email phishing gửi cho khách hàng của mạng đấu giá eBay

3.3.9.4. Phòng chống

Do tấn công sử dụng các kỹ thuật xã hội nhằm đến người dùng nên biện pháp phòng chống hiệu quả là giáo dục, đào tạo nâng cao ý thức cảnh giác cho người dùng. Một số khuyến nghị giúp người dùng phòng tránh dạng tấn công này:

- Cảnh giác với các lời mời, hoặc thông báo trúng thưởng bằng email, tin nhắn điện thoại, tin nhắn chat, hoặc quảng cáo trên các trang web, diễn đàn mà không có lý do, nguồn gốc trúng thưởng rõ ràng;

- Cảnh giác với các yêu cầu cung cấp thông tin, xác nhận tài khoản, thông tin thanh toán, thông tin thẻ tín dụng,..;
- Kiểm tra kỹ địa chỉ (URL) các trang web, đảm bảo truy cập đúng trang web của cơ quan, tổ chức.

From: CustomerSecurity@royalbank.com¹
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder²

Royal Bank

Dear valued Royal Bank customer,³

It has come to our attention that you have not logged into your online banking account for some time⁴ now and, as a security measure, we must suspend your online account.⁵ If you would like to continue to use the online banking facility offered by Royal Bank, please click the link below and renew your security details⁶ immediately. Failure to do so will result in your online account being suspended.⁸

Renew your security details immediately and continue to use our online banking facility:
<https://customerbankingrenewal.royalbank.com/>⁹

We are sorry for any inconvenience¹⁰ caused and hope you continue to use our online banking facility.

The Royal Bank Online Security Team¹¹

Link: <http://customerbankingrenewal.royalbank.com/>

Hình 3.15. Một email phishing gửi cho khách hàng của ngân hàng Royal Bank

3.3.10. Tấn công pharming

Pharming là kiểu tấn công vào trình duyệt của người dùng, trong đó người dùng nhập địa chỉ 1 trang web, trình duyệt gửi yêu cầu truy cập, tải và nạp 1 trang web khác, thường là trang web độc hại. Có 2 dạng tấn công pharming:

- (1) Kẻ tấn công thường sử dụng sâu, vi rút hoặc các phần mềm độc hại cài đặt vào hệ thống nạn nhân để kiểm soát trình duyệt của người dùng; và
- (2) Kẻ tấn công cũng có thể tấn công vào hệ thống phân giải tên miền để thay đổi kết quả truy vấn: thay thế địa chỉ IP của website hợp pháp thành địa chỉ IP của website độc hại.

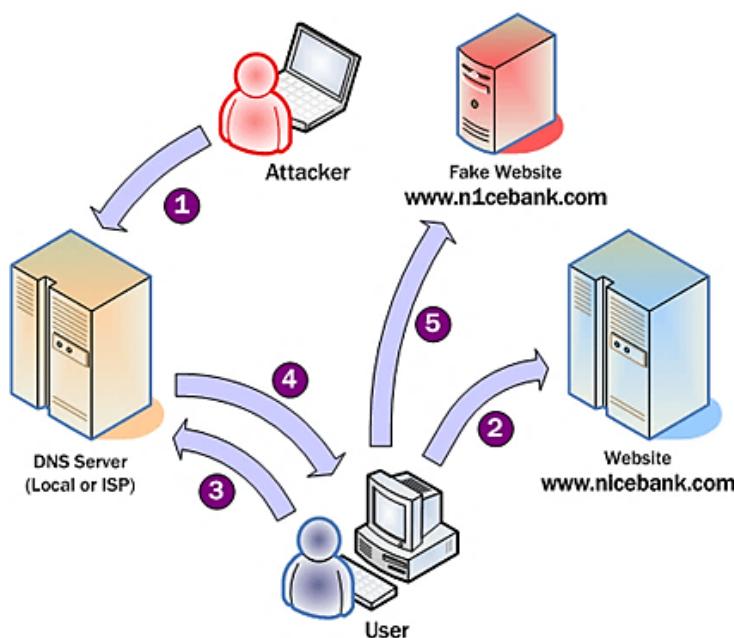
Hình 3.16 minh họa cửa sổ trình duyệt của người dùng bị tấn công pharming ở dạng (1), hay còn gọi là *tấn công cướp trình duyệt* (Browser hijacking), trong đó người dùng nhập địa chỉ trang google.com thì trình duyệt lại tải và nạp trang adventureinsecurity.com. Trong trường hợp này, trình duyệt của nạn nhân đã bị cài đặt trình cắm (plug-in, hoặc add-on) độc hại có khả năng kiểm soát trình duyệt. Hình 3.17 minh họa các bước của tấn công pharming dạng (2), trong đó kẻ tấn công xâm nhập vào máy chủ DNS chỉnh sửa địa chỉ IP của website hợp pháp thành địa chỉ IP của máy chủ web của chúng. Kết quả là trình duyệt người dùng bị chuyển hướng yêu cầu nạp website của kẻ tấn công. Các bước cụ thể của tấn công pharming dạng này như sau:

- (1) Kẻ tấn công (Attacker) xâm nhập vào máy chủ DNS của người dùng thực hiện chỉnh sửa địa chỉ IP của website hợp pháp thành IP của máy chủ web của chúng;

- (2) Người dùng (User) sử dụng trình duyệt để gửi yêu cầu truy cập website hợp pháp, chẳng hạn trang (Website - www.nicebank.com);
- (3) Trình duyệt của người dùng gửi yêu cầu phân giải địa chỉ IP của trang website hợp pháp lên máy chủ DNS (DNS Server);
- (4) Máy chủ DNS thực hiện yêu cầu phân giải địa chỉ IP và trả về kết quả. Tuy nhiên, do máy chủ DNS đã bị kiểm soát nên địa chỉ IP nó trả về là địa chỉ IP của máy chủ web của kẻ tấn công;
- (5) Trình duyệt của người dùng gửi yêu cầu, tải và nạp trang web giả mạo từ máy chủ web của kẻ tấn công (Fake website – www.n1cebank.com).



Hình 3.16. Tấn công pharming “cướp” trình duyệt



Hình 3.17. Tấn công pharming thông qua tấn công vào máy chủ DNS

Để phòng chống tấn công pharming dạng (1) cần sử dụng các công cụ rà quét và diệt các phần mềm độc hại hoạt động ở chế độ thời gian thực như đề cập tại mục 3.4.3 để đảm

bảo các dạng phần mềm độc hại không xâm nhập vào hệ thống và kiểm soát trình duyệt. Để phòng chống tấn công pharming dạng (1) cần sự hỗ trợ của nhân viên quản trị mạng, đảm bảo hệ thống máy chủ DNS được an toàn, tránh bị xâm nhập và chỉnh sửa các bản ghi phân giải tên miền do máy chủ DNS quản lý.

3.3.11. Tấn công APT

Tấn công APT (Advanced Persistent Threat), hay còn được gọi là tấn công có chủ đích là hình thức tấn công tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, từng đối tượng cụ thể nhằm mục đích tìm kiếm các thông tin giá trị và gửi ra bên ngoài [23]. Hai thuộc tính quan trọng của tấn công APT là tiên tiến, hay cao cấp (Advanced) và Kiên trì, dai dẳng (Persistent). Thuộc tính “tiên tiến” có nghĩa là các kỹ thuật tiên tiến được sử dụng để tấn công vào hệ thống mục tiêu một cách bài bản. Bên cạnh đó các cuộc tấn công APT thường kết hợp nhiều kỹ thuật khác nhau một cách khoa học. Tính “tiên tiến” còn thể hiện ở khả năng ẩn mình, thay đổi liên tục khiến cho việc phát hiện tấn công APT trở nên rất khó khăn. Phần lớn các cuộc tấn công được ghi nhận trên thế giới đều có những đặc điểm và cách thức tấn công, khai thác khác nhau.

Thuộc tính “kiên trì” có nghĩa là mục tiêu được xác định rất cụ thể để thực hiện tấn công, ẩn mình và khai thác theo từng giai đoạn. Nhiều kỹ thuật, phương pháp tấn công khác nhau vào mục tiêu được sử dụng cho đến khi thành công. Bên cạnh đó sự kiên trì của kẻ tấn công còn thể hiện ở chỗ, chúng có thể sử dụng hàng tháng, thậm chí hàng năm chỉ để thu thập thông tin của nạn nhân làm tiền đề cho cuộc tấn công. Ví dụ, để tấn công vào người dùng chúng kiên trì tìm hiểu thông tin về người dùng đó như sở thích, tính cách hay cách đặt tên file, mối quan hệ của nạn nhân trên thế giới ảo. Đồng thời, tấn công APT dai dẳng ở chỗ khi chúng đã xâm nhập được vào hệ thống và đã đánh cắp được dữ liệu và gửi ra ngoài, chúng không bao giờ dừng việc đánh cắp dữ liệu mà mục đích của chúng là cài cắm mã độc vào hệ thống để lấy được càng nhiều dữ liệu càng tốt. Một cuộc tấn công APT điển hình thường được thực hiện theo các giai đoạn sau:

- Truy cập ban đầu: Mục tiêu của giai đoạn này là lây nhiễm mã độc vào hệ thống mục tiêu thông qua bẫy người dùng tải và cài đặt mã độc, hoặc tấn công khai thác các lỗ hổng của hệ điều hành hoặc các ứng dụng;
- Thâm nhập lần đầu và triển khai mã độc: Sau khi có quyền truy cập, kẻ tấn công cài đặt mã độc thường trú lâu dài trong hệ thống mục tiêu và duy trì kết nối với hệ thống điều khiển của kẻ tấn công. Các kỹ thuật tiên tiến như mã hóa, xáo trộn mã, đa hình được sử dụng giúp mã độc có thể tồn tại lâu dài trong hệ thống mục tiêu;
- Mở rộng truy cập và di chuyển ngang: Các xâm nhập sâu hơn vào các hệ thống được thực hiện để có thể đánh cắp nhiều dữ liệu nhạy cảm hơn. Các cửa hậu và các đường hầm cũng có thể được cài đặt để thuận tiện cho việc vận chuyển dữ liệu đánh cắp được sau này;
- Giai đoạn tấn công: Kẻ tấn công thực hiện quá trình giám sát các đối tượng, hoặc hệ thống nhằm trích xuất và vận chuyển dữ liệu nhạy cảm đến nơi an toàn trong hệ thống. Các dữ liệu trích xuất được thường được nén và mã hóa trước khi được vận chuyển ra ngoài;

- Gây thiệt hại: Thực hiện việc vận chuyển dữ liệu đánh cắp được ra ngoài. Kẻ tấn công có thể thực hiện một số dạng tấn công khác, như tấn công DDoS vào hệ thống mục tiêu để đánh lạc hướng người quản trị và xóa các dấu vết việc sao chép và truyền dữ liệu ra ngoài;
- Tấn công tiếp theo: Thông thường cuộc tấn công APT không kết thúc sau khi đã lấy được dữ liệu mong muốn. Kẻ tấn công vẫn giám sát hệ thống thông qua các cửa hậu đã mở hoặc các mã độc thường trú nhằm chờ cơ hội xâm nhập sâu hơn, hoặc thực hiện các cuộc tấn công trong tương lai.

Do tấn công APT là dạng tấn công phức tạp, kết hợp của việc sử dụng mã độc cao cấp với các kỹ thuật tấn công tinh vi nên cần có một chiến lược thích hợp để phòng chống dạng tấn công này. Chiến lược tổng quát là kết hợp nhiều biện pháp, hoặc lớp phòng vệ, kết hợp với việc đào tạo nâng cao ý thức người dùng về an toàn thông tin. Trong đó, các lớp phòng vệ cần thiết bao gồm: tường lửa, kiểm soát truy cập, các hệ thống phát hiện và diệt mã độc, các hệ thống giám sát phát hiện xâm nhập có tích hợp khả năng phân tích tương quan các dạng nguy cơ, kết hợp với hệ thống quản lý và chính sách an toàn thông tin đầy đủ và được giám sát thực hiện nghiêm ngặt.

3.4. Các dạng phần mềm độc hại

Các phần mềm độc hại, còn gọi là phần mềm mã độc (Malware hay Malicious software), hay ngắn gọn là mã độc là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống. Khi mới được phát hiện vào những năm 1970-1980, các phần mềm độc hại còn tương đối ít chủng loại và được gọi chung là vi rút (virus)¹. Tuy nhiên, theo thời gian vi rút đã phát triển rất mạnh thành nhiều dạng khác nhau, đặc biệt với sự bùng nổ của mạng Internet toàn cầu và thuật ngữ “phần mềm độc hại” hay “mã độc” (malware)² được sử dụng chỉ các dạng mã độc thay thế cho thuật ngữ “vi rút”.

3.4.1. Phân loại

Có nhiều phương pháp phân loại các phần mềm độc hại dựa trên các tiêu chí khác nhau, như dựa trên phương pháp lây nhiễm, hoặc khả năng lẩn tránh bị rà quét. Các hãng bảo mật cũng sử dụng các phương pháp khác nhau để phân loại các phần mềm độc hại, chẳng hạn Kaspersky Lab sử dụng “classification tree”³, hay Microsoft sử dụng CARO (Computer Antivirus Research Organization)⁴ để đặt tên các phần mềm độc hại và họ các phần mềm độc hại. Một trong các phương pháp phân loại được thừa nhận rộng rãi biểu diễn như trên Hình 3.18. Theo đó, các phần mềm độc hại được chia thành 2 nhóm chính dựa trên phương pháp lây nhiễm như sau:

- (1) *Các phần mềm độc hại cần chương trình chủ, vật chủ* (host – gọi chung là vật chủ) để ký sinh và lây nhiễm. Các phần mềm độc hại thuộc nhóm này cần có vật chủ, hoặc hành động của người dùng hỗ trợ cho quá trình ký sinh và lây nhiễm. Các

¹ Đọc thêm tại http://www.worldlibrary.in/articles/eng/Timeline_of_notable_computer_viruses_and_worms

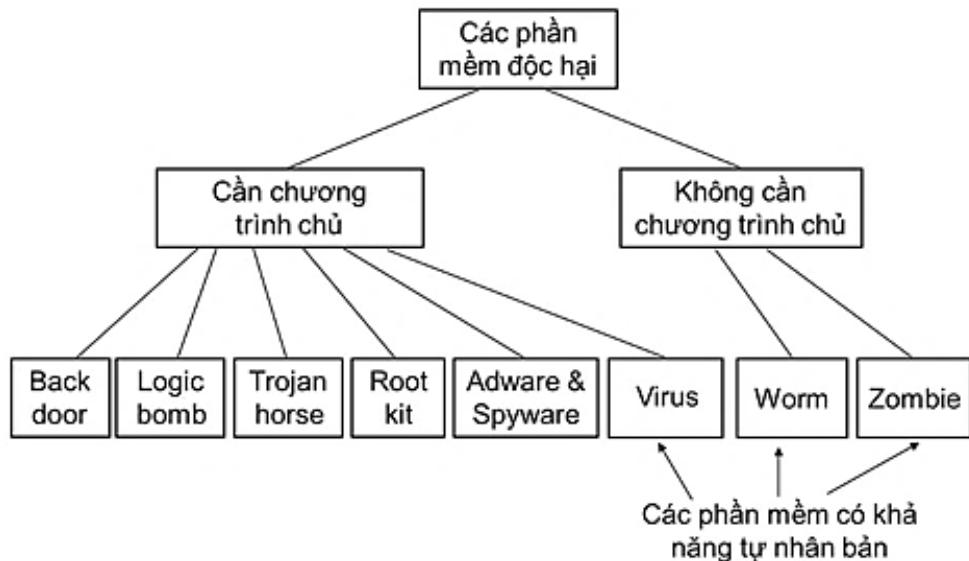
² Đọc thêm tại <https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/>

³ Đọc thêm tại <https://www.kaspersky.com/resource-center/threats/malware-classifications>

⁴ Đọc thêm tại <https://www.microsoft.com/en-us/wdsi/help/malware-naming>

thành viên của nhóm này gồm Logic bomb (Bom lô gic), Backdoor (Cửa hậu), Trojan horse (Con ngựa thành Tơ roa), Virus (Vi rút), Rootkit (Các bộ công cụ giành quyền truy cập mức root), Adware (Phần mềm quảng cáo) và Spyware (Phần mềm gián điệp);

- (2) Các phần mềm độc hại không cần vật chủ để lây nhiễm. Các phần mềm độc hại thuộc nhóm này có khả năng lây lan tự động mà không cần có vật chủ, hoặc hành động của người dùng hỗ trợ cho quá trình lây nhiễm. Các thành viên của nhóm này gồm Worm (Sâu) và Zombie hay Bot (Phần mềm máy tính ma).



Hình 3.18. Phân loại các dạng phần mềm độc hại dựa trên phương pháp lây nhiễm

Trong số các phần mềm độc hại như mô tả trên Hình 3.18, các phần mềm độc hại có khả năng tự lây nhiễm (self-infection), hay tự nhân bản (self-replicate) gồm vi rút, sâu và phần mềm máy tính ma. Các dạng phần mềm độc hại còn lại không có khả năng tự lây nhiễm. Việc phân loại các phần mềm độc hại kể trên mang tính chất tương đối do hiện nay, các dạng phần mềm độc hại và các biến thể của chúng phát triển rất nhanh và nhiều dạng mã độc mới được phát hiện trong thời gian gần đây. Chẳng hạn, các dạng mã độc mã hóa dữ liệu nhằm tống tiền (Ransomware), mã độc đào tiền ảo và mã độc chuyên dụng cho tấn công APT đang phát triển rất mạnh. Ngoài ra, có một số phần mềm độc hại có các đặc tính kết hợp của nhiều dạng phần mềm độc hại kể trên, chẳng hạn một phần mềm độc hại có các đặc tính của cả vi rút, sâu và phần mềm gián điệp. Mục tiếp theo trình bày chi tiết từng dạng phần mềm độc hại đã nêu trên Hình 3.18.

3.4.2. Mô tả các dạng phần mềm độc hại

3.4.2.1. Bom lô gic

Bom lô gic (Logic bomb) là các đoạn mã độc thường được “nhúng” vào các chương trình ứng dụng bình thường và thường được cài đặt hẹn giờ để “phát nổ” trong một số điều kiện cụ thể. Điều kiện để bom “phát nổ” có thể là sự xuất hiện hoặc biến mất của các file cụ thể, một thời điểm cụ thể trong ngày, hoặc một ngày trong tuần. Khi “phát nổ”, bom lô gic có thể xoá dữ liệu, xóa các file, tắt cả hệ thống...

Thực tế đã ghi nhận quả bom lô gic do Timothy A. Lloyd¹ - cựu nhân viên quản trị mạng cài lại đã “phát nổ” tại công ty Omega Engineering, Hoa Kỳ vào ngày 30/7/1996, 20 ngày sau khi ông bị sa thải. Quả bom lô gic của Timothy A. Lloyd đã xoá sạch các bản thiết kế và các phần mềm quan trọng, gây thiệt hại về doanh thu và hợp đồng gần 10 triệu USD cho công ty. Ông Timothy A. Lloyd đã bị toà án liên bang Hoa Kỳ tuyên 41 tháng tù giam và nộp phạt 2 triệu USD².

3.4.2.2. Trojan horse

Trojan horse, hay thường gọi tắt là trojan lấy tên theo tích “Con ngựa thành Tơ roa”, là chương trình chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng. Trojan thường được sử dụng để thực thi gián tiếp các tác vụ, trong đó tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy cập. Chẳng hạn, trong một hệ thống nhiều người dùng, một người dùng ác tính có thể tạo ra một trojan đeo lốt một chương trình hữu ích đặt ở thư mục chung, nơi mọi người dùng đều có quyền truy cập. Khi trojan này được thực thi bởi một người dùng khác, nó sẽ thay đổi quyền truy cập các file riêng của người dùng đó, cho phép tất cả người dùng (bao gồm cả người dùng ác tính) truy cập vào các file riêng của người dùng đó.

3.4.2.3. Cửa hậu

Cửa hậu (Backdoor) thường được các lập trình viên tạo ra, dùng để gỡ rối và kiểm thử trong quá trình phát triển chương trình. Cửa hậu thường cho phép truy cập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường. Khi các cửa hậu được lập trình viên tạo ra để truy cập bất hợp pháp vào hệ thống, chúng trở thành một mối đe dọa đến an ninh hệ thống. Các cửa hậu thường được thiết kế và cài đặt khéo léo và chỉ được kích hoạt trong một ngữ cảnh nào đó, do vậy chúng rất khó bị phát hiện.

Thực tế đã phát hiện nhiều cửa hậu được bí mật cài đặt trên các hệ thống máy tính, như mã độc cửa hậu được bí mật cài đặt trong BIOS của một loạt máy tính của hãng Lenovo, Trung quốc. Do mã độc được tích hợp vào BIOS của máy nên người dùng không thể loại bỏ được chúng bằng cách cài đặt lại hệ điều hành, hoặc sử dụng các công cụ rà quét phần mềm độc hại. Mã độc này tự động được kích hoạt khi hệ thống khởi động và âm thầm thu thập dữ liệu người dùng và gửi về máy chủ đặt tại Trung quốc³.

3.4.2.4. Vi rút

a. Giới thiệu

Vi rút (Virus) là một chương trình có khả năng “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút cũng được kích hoạt và sẽ tiếp tục “lây nhiễm” sang các chương trình khác đang hoạt động. Tương tự như vi rút sinh học, vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép các file, gọi thực thi các ứng dụng và dịch vụ qua mạng, gửi nhận email...

¹ Đọc thêm <http://edition.cnn.com/2000/TECH/computing/06/27/omega.files.idg/>

² Đọc thêm <http://edition.cnn.com/2002/TECH/industry/02/28/hacker.jail.sentence.idg/index.html>

³ Đọc thêm <https://www.techworm.net/2015/08/lenovo-pcs-and-laptops-seem-to-have-a-bios-level-backdoor.html>

Do vi rút là một chương trình nên nó có thể thực hiện được mọi tác vụ mà một chương trình ứng dụng thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, vi rút tự động được thực hiện khi chương trình này được kích hoạt. Hình 3.19 minh họa việc chèn mã vi rút vào cuối một chương trình và chỉnh sửa chương trình để khi chương trình được kích hoạt, mã vi rút luôn được thực hiện trước, sau đó mới thực hiện mã chương trình. Dạng vi rút lây nhiễm vào chương trình được gọi là *file vi rút* và được đề cập chi tiết trong mục tiếp theo.



Hình 3.19. Chèn và gọi thực hiện mã vi rút trong chương trình

b. Các loại vi rút

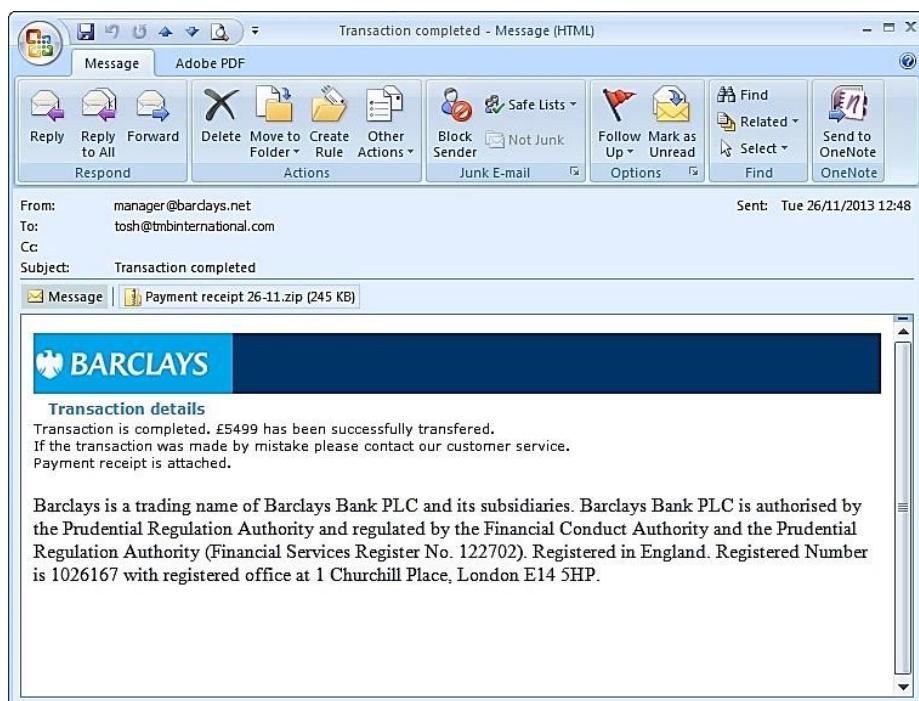
Dạng vi rút đầu tiên được phát hiện là vi rút lây nhiễm vào các file chương trình. Theo thời gian, có nhiều loại vi rút xuất hiện khai thác nhiều phương thức lây nhiễm khác nhau và được tích hợp các kỹ thuật ẩn tinh vi mình nhằm tránh bị rà quét. Hiện nay, các loại vi rút thường gặp bao gồm boot vi rút, file vi rút, macro vi rút và email vi rút. *Boot vi rút* là dạng vi rút lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần quản lý hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record). Do boot vi rút lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động. Boot vi rút có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy cập được.

File vi rút là dạng vi rút phổ biến nhất, đối tượng lây nhiễm của chúng là các file chương trình và các file dữ liệu. File vi rút thường sử dụng phương pháp sửa đổi các file đích để tích hợp mã của mình như mô tả trong mục a. Mỗi khi chương trình được kích hoạt hoặc file dữ liệu được mở, vi rút được kích hoạt và thường trú trong bộ nhớ. Các chương trình được kích hoạt trong hệ thống đều có khả năng bị lây nhiễm vi rút đang hoạt động. Ngoài ra, cũng tồn tại một số loại file vi rút hoạt động độc lập, lây nhiễm bằng cách khai thác các tính năng thực thi tự động (như Auto-run, auto-exec, auto-play), hoặc giả danh các chương trình hợp pháp nhằm bẫy người dùng kích hoạt chúng. Nhìn chung, file vi rút có thể gây các trục trặc, hoặc lỗi cho chương trình, gây hỏng hoặc phá hủy các file dữ liệu, hoặc đánh cắp các dữ liệu nhạy cảm,...

Macro vi rút là một loại file vi rút đặc biệt do chúng chỉ lây nhiễm vào các tài liệu của bộ phần mềm Microsoft Office. Macro vi rút hoạt động được nhờ tính năng cho phép tạo

và thực hiện các đoạn mã macro trong các tài liệu của Microsoft Office, gồm trình soạn thảo văn bản Word, bảng tính Excel, trình email Outlook.... Các đoạn mã macro thường được dùng để tự động hóa một số tác vụ và được viết bằng ngôn ngữ Visual Basic for Applications (VBA). Macro vi rút thường lây nhiễm vào các file định dạng chuẩn (các template như normal.dot và normal.dotx) và từ đó lây nhiễm vào tất cả các file tài liệu được mở. Macro vi rút cũng có thể được tự động kích hoạt nhờ các macro được hệ thống chạy tự động, như AutoExecute, Automacro và Command macro. Theo thống kê, macro vi rút chiếm khoảng 2/3 tổng lượng vi rút đã được phát hiện. Tuy nhiên, lượng tài liệu bị lây nhiễm macro vi rút đã giảm đáng kể từ khi Microsoft Office phiên bản 2010 và các phiên bản mới hơn có thiết lập ngầm định không cho phép tự động chạy các macro.

Email vi rút là loại vi rút sử dụng email làm phương tiện lây lan. Email vi rút lây nhiễm bằng cách tự động gửi một bản copy của nó như 1 file đính kèm đến tất cả các địa chỉ email trong sổ địa chỉ của người dùng trên máy bị lây nhiễm. Nếu người dùng mở email hoặc file đính kèm, vi rút được kích hoạt. Email vi rút có thể lây nhiễm rất nhanh chóng, lan tràn trên khắp thế giới trong một thời gian ngắn. Hình 3.20 là một email do vi rút gửi đến người dùng, theo đó email có đính kèm một file giả dạng một giấy biên nhận chứa mã vi rút lừa người dùng mở và kích hoạt.

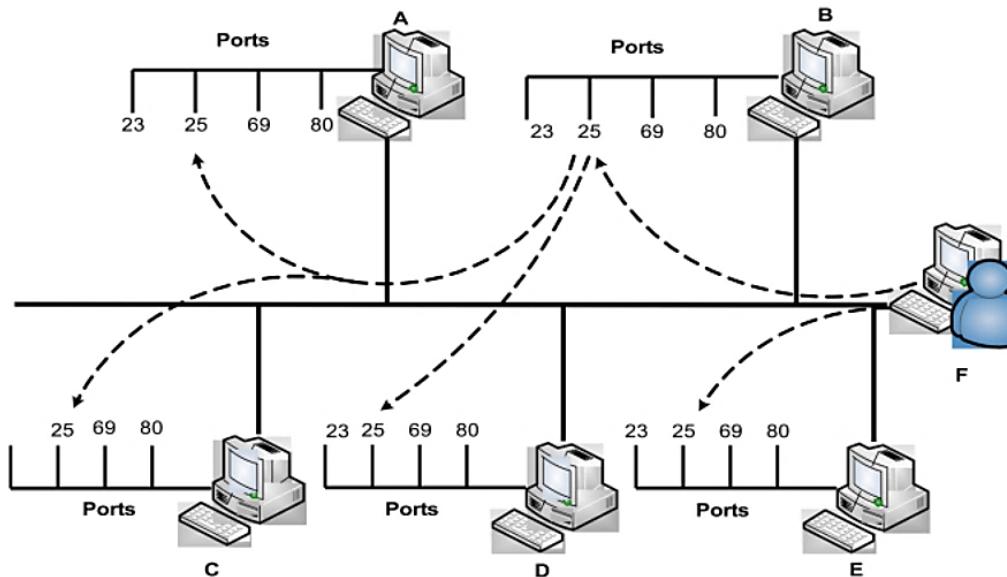


Hình 3.20. Một email do vi rút gửi đến người dùng

3.4.2.5. Sâu

Sâu (Worm) là một loại phần mềm độc hại có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần chương trình chủ, vật chủ, hoặc sự trợ giúp của người dùng. Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm “bàn đạp” để tiếp tục rà quét, tấn công các máy khác. Một trong các dạng sâu phổ biến nhất là sâu mạng (network worm) sử dụng kết nối mạng để lây lan từ máy này sang máy khác. Hình 3.21 minh họa một mô hình lây lan của sâu mạng: Bắt đầu từ máy F, sâu quét các máy B và E trên cổng 25

(SMTP) để lây nhiễm. Khi sâu lây nhiễm thành công lên máy B, nó lại tiếp tục rà quét các máy A, C và D trên cổng 25 để tìm đích lây nhiễm tiếp theo. Mặc dù sử dụng phương thức lây lan khác vi rút, nhưng khi hoạt động, sâu tương tự vi rút.



Hình 3.21. Một mô hình lây lan của sâu mạng

Hiện nay, sâu có thể lây lan sử dụng nhiều phương pháp khác nhau. Một số sâu chỉ sử dụng một phương pháp lây lan, nhưng một số sâu khác có khả năng lây lan theo nhiều phương pháp. Các phương pháp lây lan chính của sâu gồm:

- Lây lan qua thư điện tử: Sâu sử dụng email để gửi bản sao của mình đến các máy khác. Dạng sâu này tương tự email vi rút, nhưng có khả năng tự kích hoạt mà không cần người dùng mở email hay thực hiện file đính kèm.
- Lây lan thông qua khả năng thực thi từ xa: Sâu gửi và thực thi một bản sao của nó trên một máy khác thông qua việc khai thác các lỗ hổng an ninh của hệ điều hành, các dịch vụ, hoặc phần mềm ứng dụng.
- Lây lan thông qua khả năng log-in (đăng nhập) từ xa: Sâu đăng nhập vào hệ thống ở xa như một người dùng và sử dụng lệnh để sao chép bản thân nó từ máy này sang máy khác.

Sâu Code Red¹ được phát hiện vào tháng 7/2001 lây nhiễm thông qua việc khai thác lỗ tràn bộ đệm khi xử lý các file .ida trong máy chủ web Microsoft IIS (Internet Information Service). Code Red quét các địa chỉ IP ngẫu nhiên để tìm các hệ thống có lỗi và lây nhiễm vào 360.000 máy chủ trong vòng 14 giờ, như biểu diễn trên bản đồ lây nhiễm Code Red trên Hình 3.22.

Tiếp theo sâu Code Red, sâu Nimda² được phát hiện vào tháng 9/2001 là sâu có khả năng lây lan theo nhiều con đường:

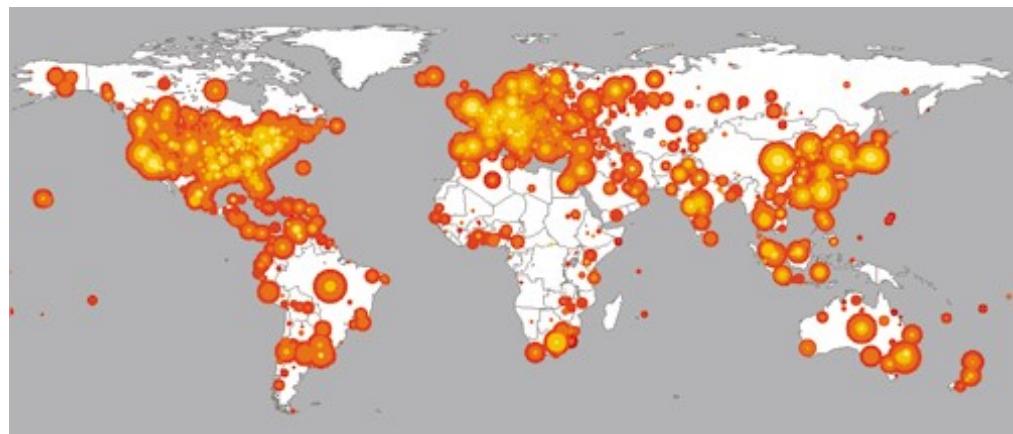
- Qua email từ máy client sang client.
- Qua các thư mục chia sẻ trên mạng.

¹ Đọc thêm tại <https://www.caida.org/research/security/code-red/>

² Đọc thêm tại <https://www.f-secure.com/v-descs/nimda.shtml>

- Từ máy chủ web sang trình duyệt.
- Từ máy khách đến máy chủ nhờ khai thác các lỗi máy chủ.

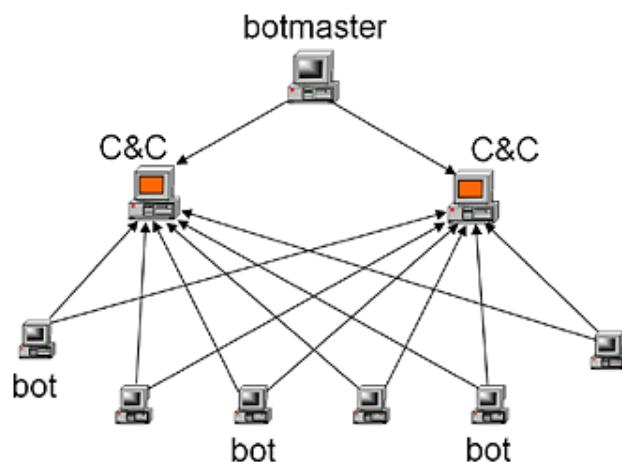
Nhờ khả năng hỗ trợ nhiều phương pháp lây lan, chỉ 22 phút sau khi ra đời, Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet vào thời điểm đó.



Hình 3.22. Bản đồ lây nhiễm sâu Code Red trên toàn thế giới

3.4.2.6. Zombie/Bot

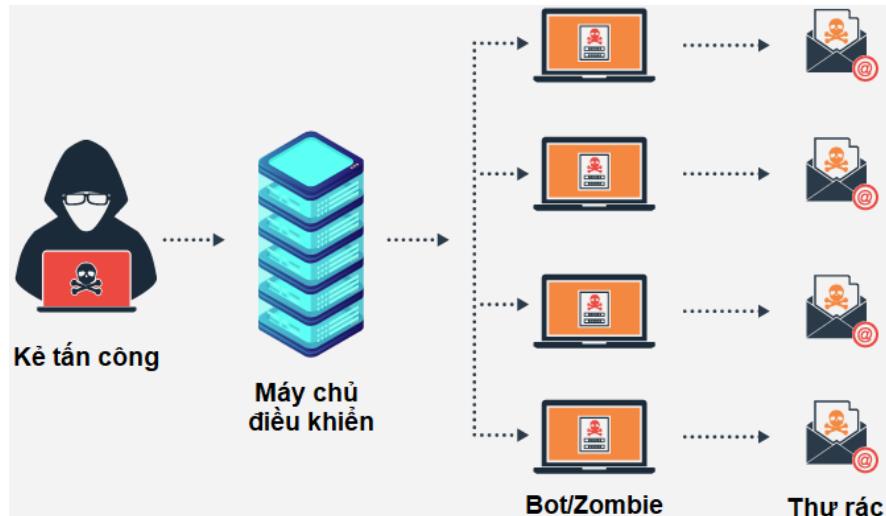
Zombie/Bot (còn gọi là *Automated agent* – từ đây thông nhất gọi là Bot) là một chương trình được thiết kế để giành quyền kiểm soát một máy tính, hoặc thiết bị tính toán có kết nối Internet và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác, hoặc gửi thư rác. Tương tự như sâu, bot có khả năng tự lây nhiễm sang các hệ thống khác mà không cần chương trình chủ, vật chủ, hoặc hỗ trợ từ người dùng. Một tập hợp các máy tính bot dưới sự kiểm soát của một, hoặc một nhóm kẻ tấn công được gọi là mạng máy tính ma, hay botnet. Kẻ tấn công kiểm soát và điều khiển các bot trong botnet thông qua một hệ thống các máy chủ lệnh và điều khiển trung gian (Command and control – C&C) sử dụng các giao thức truyền thông thông dụng như HTTP, hoặc IRC. Hình 3.23 minh họa mô hình giao tiếp giữa các thành phần trong botnet: kẻ tấn công/chủ của botnet (botmaster) gửi lệnh cho các bot thông qua các máy chủ C&C.



Hình 3.23. Mô hình mô hình giao tiếp giữa các thành phần trong botnet

Khác với các phần mềm độc hại khác, các bot có khả năng tự tải mã cập nhật và nâng cấp phiên bản từ các máy chủ C&C nhằm tăng khả năng sống sót. Các bot định kỳ truy

cập đến các máy chủ C&C để tải lệnh và mã cập nhật. Các bot thường được điều phối và sử dụng để thực hiện các cuộc tấn công DDoS các máy chủ, các website của các công ty, hoặc các tổ chức chính phủ, như đã minh họa trên Hình 3.8 và Hình 3.9 trong mục 3.3.4. Các máy tính bot/zombie cũng có thể được sử dụng để gửi thư rác tạo ra khoản tiền không nhỏ cho các nhóm tin tặc/kẻ tấn công, như minh họa trên Hình 3.24.



Hình 3.24. Mô hình Hacker sử dụng các máy tính Zombie/Bot để gửi thư rác

3.4.2.7. Rootkit

Rootkit là một dạng phần mềm độc hại gồm một tập các công cụ có mục đích giành quyền truy cập vào hệ thống máy tính mà người dùng không có thẩm quyền không thể truy cập. Rootkit thường che giấu mình bằng cách đội lốt một phần mềm khác. Rootkit có thể được cài đặt tự động, hoặc kẻ tấn công cài đặt rootkit khi chiếm được quyền quản trị hệ thống. Do rootkit có quyền truy cập hệ thống ở mức quản trị nên nó có toàn quyền truy cập vào các thành phần trong hệ thống và rất khó bị phát hiện.

3.4.2.8. Adware và Spyware

Adware (tên đầy đủ là advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm. Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm đó hoặc một dịch vụ miễn phí. Adware cũng có thể được cài đặt như một trình cắm chạy trong trình duyệt web của người dùng nhằm hiển thị các pop-up quảng cáo. Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được cài đặt và kích hoạt tự động mà không được sự đồng ý của người dùng.

Spyware (Spy software) là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân. Có 4 loại spyware thường gặp, gồm system monitor (công cụ giám sát hệ thống), trojan, adware và tracking cookie (các cookie theo dõi người dùng). Spyware có thể được cài đặt vào hệ thống nạn nhân thông qua nhiều phương pháp, như tích hợp, đóng gói vào các phần mềm khác, bẫy nạn nhân tự tải và cài đặt, hoặc kẻ tấn công có thể sử dụng vi rút, sâu để tải và cài đặt. Spyware thường được trang bị khả năng ẩn mình nên rất khó có thể phát hiện bằng các phương pháp thông thường.

3.4.3. Phòng chống phần mềm độc hại

3.4.3.1. Nguyên tắc chung

Có thể thấy các phần mềm độc hại là một trong các nguy cơ gây mất an toàn lớn nhất và thường trực nhất đối với thông tin, hệ thống và người dùng do sự bùng nổ về số lượng, mức độ tinh vi ngày càng cao và khả năng phá hoại ngày càng lớn của chúng. Nguyên tắc chung trong phòng chống phần mềm độc hại vẫn là *phòng vệ theo chiều sâu*, trong đó nhiều nhóm biện pháp đảm bảo an toàn cần được áp dụng để phòng ngừa và ngăn chặn việc lây nhiễm các phần mềm độc hại vào hệ thống. Có thể liệt kê các biện pháp phòng chống các phần mềm độc hại theo thứ tự ưu tiên từ cao đến thấp như sau:

- (1) Sử dụng các biện pháp kiểm soát truy cập cung cấp bởi tường lửa và hệ điều hành để hạn chế giao diện tiếp xúc của hệ thống với mạng ngoài. Chẳng hạn, tường lửa có thể chặn các kết nối trái phép từ Internet đến hệ thống máy tính để khai thác các lỗ hổng, hoặc tải các phần mềm độc hại;
- (2) Sử dụng công cụ rà quét và diệt trừ các phần mềm độc hại. Với mỗi hệ thống máy tính, nhất là các máy trạm và máy tính cá nhân, cần cài đặt **một bộ công cụ** (và chỉ nên một tại mỗi thời điểm) rà quét phần mềm độc hại có khả năng bảo vệ hệ thống theo thời gian thực. Bộ công cụ này cần được cập nhật thường xuyên để đảm bảo khả năng phát hiện và diệt trừ các phần mềm độc hại mới nhất;
- (3) Đào tạo và nâng cao ý thức cảnh giác của người dùng về mã độc, phần mềm độc hại, các chương trình ứng dụng trên máy tính, trên mạng Internet không rõ nguồn gốc. Việc nâng cao ý thức người dùng đóng vai trò quan trọng trong việc phòng ngừa việc lây lan của các dạng phần mềm độc hại;
- (4) Sử dụng các phần mềm có bản quyền. Sử dụng các phần mềm có bản quyền là cách hiệu quả để hạn chế các loại phần mềm độc hại, như trojan, adware và spyware thường được tích hợp vào các công cụ phá khoá (cracker) hệ điều hành và các phần mềm ứng dụng;
- (5) Thường xuyên cập nhật hệ điều hành và các phần mềm ứng dụng. Việc cập nhật thường xuyên, nhất là các bản vá an ninh nhằm giảm thiểu các lỗ hổng bảo mật đã biết trên hệ thống và nhờ vậy giảm thiểu khả năng bị khai thác bởi các dạng phần mềm độc hại;
- (6) Phân quyền người dùng phù hợp giúp hạn chế khả năng tự động cài đặt các dạng phần mềm độc hại lên hệ thống. Không sử dụng người dùng có quyền quản trị (root, hoặc administrator) để thực thi các ứng dụng. Người dùng thông thường chỉ nên được cấp quyền truy cập vừa đủ để thực thi nhiệm vụ.

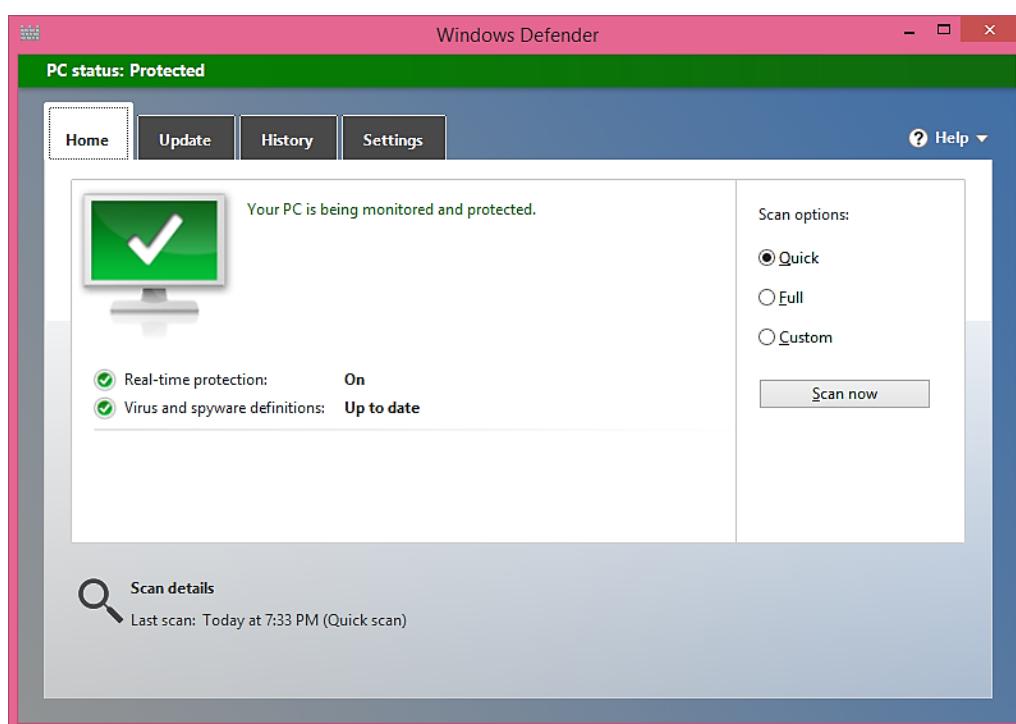
3.4.3.2. Các công cụ rà quét phần mềm độc hại

Các công cụ rà quét vi rút và các phần mềm độc hại (Antivirus software) là các phần mềm có khả năng rà quét, bảo vệ hệ thống khỏi vi rút và các phần mềm độc hại khác theo thời gian thực. Hầu hết các công cụ này đều cho phép thực hiện 2 chế độ quét: (i) quét định kỳ từng phần, hoặc toàn bộ hệ thống các file và (ii) bảo vệ hệ thống theo thời gian thực (Realtime protection). Chúng cho phép giám sát tất cả các thao tác đọc/ghi hệ thống

file để phát hiện các phần mềm độc hại. Đa số công cụ rà quét vi rút và các phần mềm độc hại hoạt động dựa trên một cơ sở dữ liệu các mẫu, hoặc chữ ký của các phần mềm độc hại đã biết. Do vậy, để đảm bảo hiệu quả rà quét, cơ sở dữ liệu này phải được cập nhật thường xuyên. Một số bộ công cụ cho phép quét theo hành vi hoặc heuristics.

Có thể liệt kê một số công cụ rà quét vi rút và các phần mềm độc hại thông dụng, như:

- Microsoft Security Essentials (Microsoft Windows 7 trở lên)
- Microsoft Windows Defender (Microsoft Windows 8 trở lên) – Hình 3.25
- Semantec Norton Antivirus
- Kaspersky Antivirus
- BitDefender Antivirus
- AVG Antivirus
- McAfee VirusScan
- Trend Micro Antivirus
- F-secure Antivirus và
- BKAV Antivirus.



Hình 3.25. Màn hình chính của Microsoft Windows Defender

3.5. Kết chương

Chương này đã trình bày về các dạng tấn công điển hình vào các hệ thống máy tính và mạng, và các phần mềm độc hại thường gặp. Cụ thể chương đã đề cập các vấn đề sau:

- Trình bài khái quát về mối đe dọa, tấn công và quan hệ giữa mối đe dọa, lỗ hổng bảo mật và tấn công.
- Mô tả vắn tắt một số công cụ hỗ trợ tấn công.

- Mô tả chi tiết các dạng tấn công điển hình vào các hệ thống máy tính và mạng, kèm theo các biện pháp phòng chống với mỗi dạng tấn công.
- Mô tả chi tiết các dạng phần mềm độc hại thường gặp, bao gồm phân loại, phương thức lây nhiễm, hoạt động và phương pháp rà quét, phòng chống các phần mềm độc hại.

3.6. Câu hỏi ôn tập

- 1) Mối đe dọa (threat) là gì? Tại sao nói “Tấn công = Mối đe dọa + Lỗ hổng bảo mật”?
- 2) Mô tả văn tắt 4 loại tấn công chính và 2 kiểu tấn công chủ động và thụ động. Tại sao nói tấn công thụ động thường là giai đoạn đầu của một cuộc tấn công chủ động?
- 3) Nêu mục đích và các dạng tấn công vào mật khẩu.
- 4) Tấn công chèn mã SQL là gì? Nêu các nguyên nhân của lỗ hổng chèn mã SQL. Tấn công chèn mã SQL có khả năng cho phép kẻ tấn công thực hiện những hành vi gì trên hệ thống nạn nhân?
- 5) Mô tả cơ chế tấn công chèn mã SQL trong từng trường hợp khai thác sau: vượt qua xác thực người dùng; chèn, sửa xoá dữ liệu; và đánh cắp dữ liệu.
- 6) Nêu các biện pháp phòng chống tấn công chèn mã SQL. Có thể ngăn chặn triệt để tấn công chèn mã SQL được không? Tại sao?
- 7) Vẽ sơ đồ, mô tả cơ chế tấn công SYN Flood và các biện pháp phòng chống.
- 8) Vẽ sơ đồ, mô tả cơ chế tấn công Smurf và các biện pháp phòng chống.
- 9) Vẽ sơ đồ và mô tả kịch bản tấn công DDoS trực tiếp và tấn công DDoS gián tiếp.
- 10) Mô tả cơ chế và các biện pháp phòng chống tấn công người đứng giữa.
- 11) Đối tượng của tấn công sử dụng các kỹ thuật xã hội là gì? Mô tả kịch bản của Trò lừa đảo Nigeria 4-1-9. Khảo sát tài liệu và mô tả văn tắt 3 biến thể của Trò lừa đảo Nigeria 4-1-9 trong thời điểm hiện nay.
- 12) Tấn công Phishing là gì? Mô tả kịch bản tấn công phishing thường gặp và mô tả tối thiểu 1 kịch bản tấn công Phishing thực tế xảy ra hiện nay.
- 13) Tấn công pharming là gì? Mô tả các dạng tấn công pharming.
- 14) Tấn công APT là gì? Mô tả các thuộc tính Advanced và Persistent của tấn công APT. Khảo sát tài liệu và mô tả văn tắt về cuộc tấn công APT vào hệ thống mạng của Vietnam Airlines vào tháng 7 năm 2016.
- 15) Phần mềm độc hại là gì? Mô tả một phương pháp phân loại các phần mềm độc hại.
- 16) Vi rút là gì? Nêu các phương pháp lây nhiễm và các loại vi rút.
- 17) Trojan là gì? Mô tả cơ chế hoạt động của trojan. Trojan thường khai thác biện pháp kiểm soát truy nhập nào để giành quyền truy cập vào các file của nạn nhân?
- 18) Sâu máy tính là gì? Nêu điểm khác biệt cơ bản của sâu và vi rút. Nêu các phương pháp lây lan của sâu.

- 19) Zombie, hay bot là gì? Zombie/Bot có đặt điểm gì khác biệt so với các loại phần mềm độc hại khác? Nếu 2 trường hợp điển hình kẻ tấn công sử dụng Zombie, hay bot để lạm dụng, hoặc tấn công các hệ thống.
- 20) Nêu nguyên tắc chung và các biện pháp phòng chống các phần mềm độc hại.
- 21) Giải thích tại sao trong một hệ thống máy tính cá nhân chỉ nên sử dụng một bộ công cụ rà quét các phần mềm độc hại hoạt động ở chế độ “bảo vệ theo thời gian thực”?
- 22) Có nên sử dụng công cụ rà quét các phần mềm độc hại hoạt động ở chế độ “bảo vệ theo thời gian thực” trên các máy chủ hay không? Tại sao?
- 23) Tìm hiểu một phiên bản của bộ công cụ rà quét các phần mềm độc hại Kaspersky Antivirus và Bkav Antivirus. So sánh các tính năng của 2 bộ công cụ này.

CHƯƠNG 4. ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

Chương 4 trình bày vấn đề đảm bảo an toàn thông tin dựa trên các kỹ thuật mã hóa - mật mã, bao gồm các khái niệm cơ bản về mật mã, hệ mã hóa, vai trò và ứng dụng của mã hóa trong đảm bảo an toàn thông tin trong phần đầu. Phần tiếp theo của chương mô tả các phương pháp mã hóa, một số giải thuật cơ bản của mã hóa khóa đối xứng, mã hóa khóa bất đối xứng và các hàm băm. Đây là các giải thuật đã và đang được sử dụng rộng rãi trong đảm bảo an toàn cho thông tin lưu trữ và thông tin truyền trên mạng.

4.1. Khái quát về mã hóa thông tin và ứng dụng

Mục này trình bày một số khái niệm, thuật ngữ cơ bản trong mật mã học, các thành phần chính của một hệ mã hóa, phương pháp mã hóa dòng và mã hóa khối, sơ lược lịch sử mật mã, vai trò và các ứng dụng của mã hóa – mật mã.

4.1.1. Các khái niệm cơ bản

Mật mã

Theo từ điển Webster's Revised Unabridged Dictionary¹: “*mật mã (cryptography) là một hành động hoặc nghệ thuật viết các ký tự bí mật*”. Còn theo từ điển Free Online Dictionary of Computing²: “*mật mã là việc mã hóa dữ liệu mà nó chỉ có thể được giải mã bởi một số người chỉ định*”.

Bản rõ, Bản mã, Mã hóa và Giải mã

Bản rõ (Plaintext), hay thông tin chưa mã hóa là thông tin ở dạng có thể hiểu được.

Bản mã (Ciphertext), hay thông tin đã được mã hóa là thông tin ở dạng đã bị xáo trộn, không thể hiểu được.

Mã hóa (Encryption) là hành động xáo trộn bản rõ để chuyển thành bản mã.

Giải mã (Decryption) là hành động giải xáo trộn bản mã để chuyển thành bản rõ.

Hình 4.1 mô tả 2 khâu chính của một hệ mã hóa, trong đó khâu *Mã hóa* chuyển Bản rõ thành Bản mã sử dụng khoá mã hóa K1 được thực hiện ở phía người gửi và khâu *Giải mã* chuyển Bản mã thành Bản rõ sử dụng khoá giải mã K2 được thực hiện ở phía người nhận. Các khoá K1 và K2 có thể giống nhau hoặc khác nhau. Nếu K1 khác K2 thì chúng có quan hệ về mặt toán học với nhau.

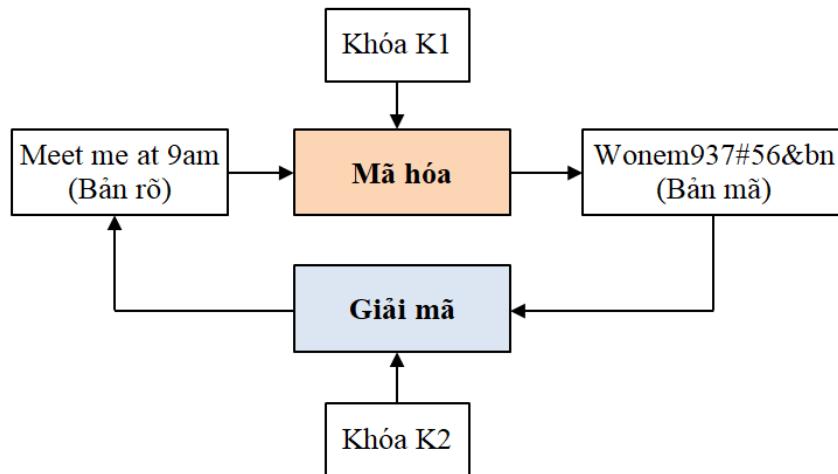
Giải thuật mã hóa & giải mã, Bộ mã hóa, Khóa/Chìa, Không gian khóa

Giải thuật mã hóa (Encryption algorithm) là giải thuật dùng để mã hóa thông tin và *Giải thuật giải mã* (Decryption algorithm) dùng để giải mã thông tin.

Bộ mã hóa (Cipher) gồm một giải thuật để mã hóa và một giải thuật để giải mã thông tin. Giải thuật mã hóa và giải thuật giải mã có thể giống nhau hoặc khác nhau phụ thuộc vào mỗi hệ mã hóa cụ thể.

¹ Tham khảo tại: <http://www.dict.org/bin/Dict?Form=Dict3&Database=web1913>

² Tham khảo tại: <http://foldoc.org/cryptography>



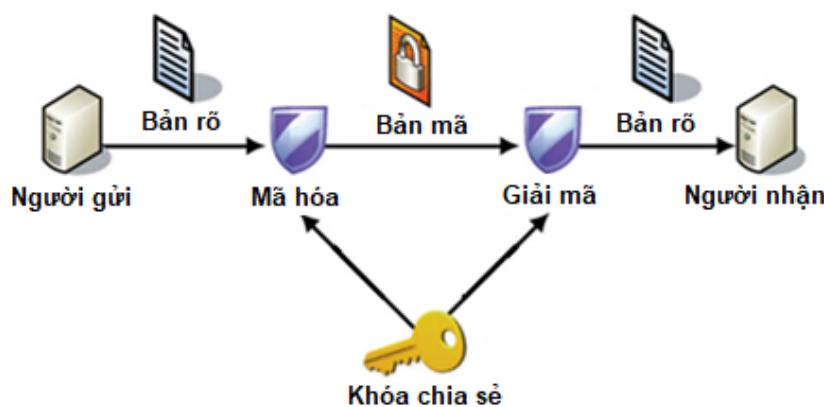
Hình 4.1. Các khâu Mã hóa và Giải mã của một hệ mã hóa

Khóa, hay *Chìa* (Key) là một chuỗi dữ liệu được sử dụng trong giải thuật mã hóa và giải thuật giải mã. Khóa để mã hóa và khóa để giải mã có thể giống nhau hoặc khác nhau phụ thuộc vào mỗi hệ mã hóa cụ thể.

Không gian khóa (Keyspace) là tập hợp tất cả các khóa có thể có của một hệ mã hóa. Ví dụ, nếu sử dụng khóa kích thước 64 bit thì không gian khóa là 2^{64} . Nhìn chung, không gian khóa càng lớn thì độ an toàn của hệ mã hóa càng cao do giảm thiểu được khả năng bị tấn công vét cạn tìm khóa.

Mã hóa khóa đối xứng, Mã hóa khóa bất đối xứng, Hàm băm, Thám mã

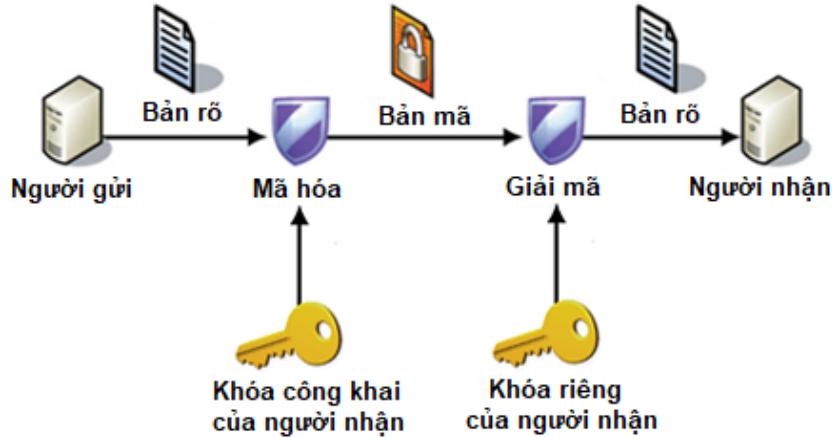
Mã hóa khóa đối xứng (Symmetric key cryptography) là dạng mã hóa trong đó một khóa được sử dụng cho cả khâu mã hóa và khâu giải mã. Do khóa sử dụng chung cần phải được giữ bí mật nên mã hóa khóa đối xứng còn được gọi là mã hóa khóa bí mật (Secret key cryptography). Hình 4.2 minh họa hoạt động của một hệ mã hóa khóa đối xứng, trong đó một khóa bí mật duy nhất, hay khóa chia sẻ được sử dụng cho cả hai khâu mã hóa bản rõ ở bên người gửi và giải mã khôi phục bản rõ từ bản mã ở bên người nhận.



Hình 4.2. Mã hóa khóa đối xứng sử dụng 1 khóa bí mật chia sẻ để mã hóa và giải mã

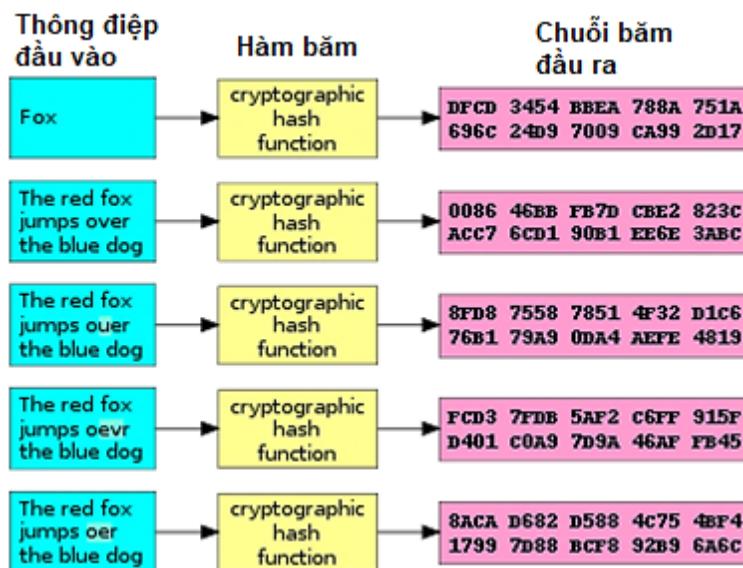
Mã hóa khóa bất đối xứng (Asymmetric key cryptography) là dạng mã hóa trong đó một cặp khóa được sử dụng: khóa công khai (public key) dùng để mã hóa, khóa riêng (private key) dùng để giải mã. Chỉ có khóa riêng cần phải giữ bí mật, còn khóa công khai có thể phổ biến rộng rãi. Do khóa để mã hóa có thể công khai nên mã hóa khóa bất đối

xứng còn thường được gọi là mã hóa khóa công khai (Public key cryptography). Hình 4.3 mô tả hoạt động của một hệ mã hóa khóa bát đối xứng, trong đó người gửi sử dụng khóa công khai của người nhận để mã hóa bản rõ và người nhận sử dụng khóa riêng của mình để giải mã khôi phục bản rõ từ bản mã.



Hình 4.3. Mã hóa khóa bát đối xứng sử dụng một cặp khóa để mã hóa và giải mã

Hàm băm (Hash function) là một ánh xạ chuyen đổi dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định. Hình 4.4 minh họa các thông điệp đầu vào và chuỗi băm đầu ra của hàm băm mật mã (Cryptographic hash function). Chuỗi đầu ra của hàm băm thường được sử dụng rộng rãi trong lưu trữ một số loại dữ liệu bí mật, như mật khẩu, hoặc trong kiểm tra tính toàn vẹn của các thông điệp truyền đưa.

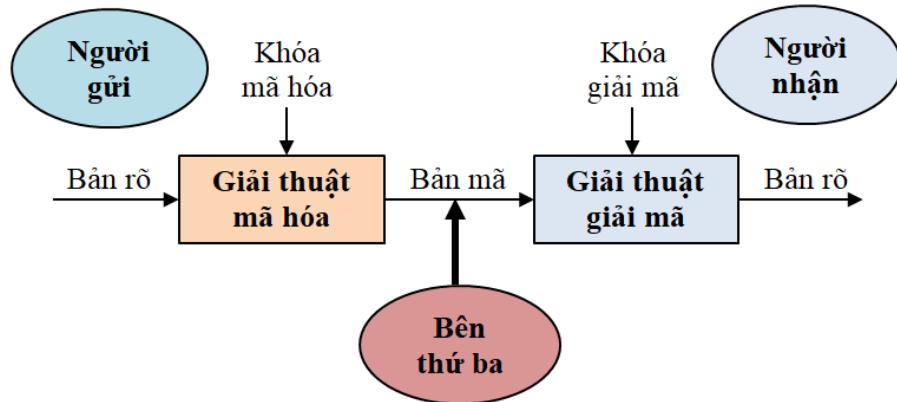


Hình 4.4. Minh họa thông điệp đầu vào và chuỗi băm đầu ra của hàm băm

Thám mã (Cryptanalysis), hay phá mã là quá trình giải mã thông điệp đã bị mã hóa mà không cần có trước thông tin về giải thuật mã hóa và khóa mã. Thám mã ra đời, phát triển song hành với mật mã và là công việc đòi hỏi khối lượng tính toán rất lớn, cũng như kinh nghiệm, tri thức chuyên gia. Nhìn chung, thám mã liên quan đến việc phân tích toán học các giải thuật mật mã, khai thác các điểm yếu trong giải thuật và cài đặt các hệ mã hóa nhằm khôi phục thông điệp gốc và/hoặc khóa mã.

4.1.2. Các thành phần của một hệ mã hóa

Một hệ mã hóa hay hệ mật mã (Cryptosystem) là một bản cài đặt của các kỹ thuật mật mã và các thành phần có liên quan để cung cấp dịch vụ bảo mật thông tin. Hình 4.5 mô tả các thành phần của một hệ mã hóa đơn giản được sử dụng để đảm bảo tính bí mật của thông tin bản rõ từ người gửi truyền đến người nhận mà không bị một bên thứ ba nghe lén. Các thành phần của một hệ mã hóa đơn giản gồm Bản rõ, Giải thuật mã hóa, Bản mã, Giải thuật giải mã, Khóa mã hóa và Khóa giải mã. Ngoài các thành phần trên, một thành phần quan trọng khác của một hệ mã hóa là Không gian khóa đã được đề cập trong mục 4.1.1.



Hình 4.5. Các thành phần của một hệ mã hóa đơn giản

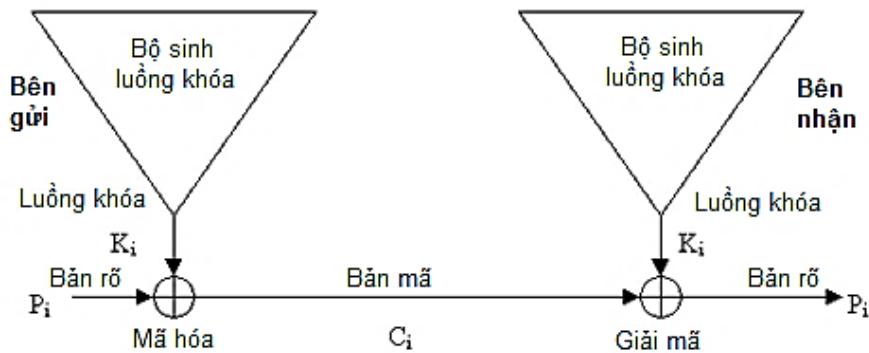
4.1.3. Mã hóa dòng và mã hóa khối

Với các thông điệp có kích thước lớn và để tăng cường độ an toàn, thông điệp thường được chia ra thành các phần có kích thước bằng nhau, sau đó áp dụng thuật toán mã hóa trên từng phần này và ghép các phần đã mã hóa để tạo bản mã ở bên người gửi. Ở bên người nhận, bản mã cũng được chia thành các phần có kích thước bằng nhau, sau đó thực hiện giải mã từng phần và ghép các phần đã giải mã để tạo bản rõ. Mã hóa dòng và mã hóa khối là hai phương pháp mã hóa, trong đó mỗi phương pháp thực hiện việc chia dữ liệu để mã hóa theo cách khác nhau.

4.1.3.1. Mã hóa dòng

Mã hóa dòng (Stream cipher) là kiểu mã hóa mà từng bit, hoặc ký tự của bản rõ được kết hợp với từng bit, hoặc ký tự tương ứng của khóa để tạo thành bản mã. Hình 4.6 biểu diễn một mô hình mã hóa dòng với quá trình mã hóa ở bên gửi và quá trình giải mã ở bên nhận. Theo đó, ở bên gửi các bit P_i của bản rõ được liên tục đưa vào kết hợp với bit tương ứng K_i của khóa để tạo thành bit mã C_i ; Ở bên nhận, bit mã C_i được kết hợp với bit khóa K_i để khôi phục bit rõ P_i . Một bộ sinh luồng khóa (Keystream generator) được sử dụng ở cả bên gửi và bên nhận để liên tục sinh các bit khóa K_i từ khóa gốc K . Các giải thuật mã hóa dòng tiêu biểu như A5/1, A5/2 và RC4 đã và đang được sử dụng rộng rãi trong viễn thông. Ngoài ra, một số giải thuật mã hóa dòng mới, như SALSA, SOSEMANUK, PANAMA¹ đã được đề xuất trong thời gian gần đây.

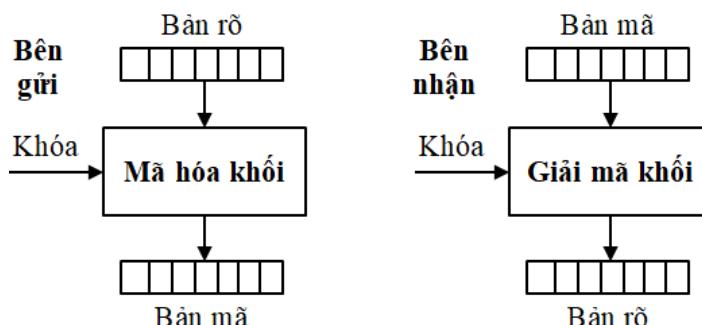
¹ Đọc thêm tại <https://www.jscape.com/blog/stream-cipher-vs-block-cipher>.



Hình 4.6. Mô hình phương pháp mã hóa dòng

4.1.3.2. Mã hóa khối

Mã hóa khối (Block cipher) là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa và giải mã. Hình 4.7 biểu diễn một mô hình mã hóa khối với quá trình mã hóa ở bên gửi và quá trình giải mã ở bên nhận. Theo đó, ở bên gửi bản rõ được chia thành các khối (block) có kích thước cố định, sau đó từng khối được mã hóa để chuyển thành khối mã. Các khối mã được ghép lại thành bản mã. Ở bên nhận, bản mã cũng được chia thành các khối và từng khối được giải mã để chuyển thành khối rõ. Cuối cùng ghép các khối rõ để có bản rõ hoàn chỉnh. Các giải thuật mã hóa khối tiêu biểu như DES, 3-DES, IDEA, AES, Blowfish và Twofish¹ đã và đang được sử dụng rất rộng rãi trong mã hóa dữ liệu với kích thước khối 64, hoặc 128 bit.



Hình 4.7. Mô hình phương pháp mã hóa khối

4.1.4. Sơ lược lịch sử mật mã

Có thể nói mật mã là con đẻ của toán học nên sự phát triển của mật mã đi liền với sự phát triển của toán học. Tuy nhiên, do nhiều giải thuật mật mã đòi hỏi khối lượng tính toán lớn nên mật mã chỉ thực sự phát triển mạnh cùng với sự ra đời và phát triển của máy tính điện tử. Sau đây là một số mốc trong sự phát triển của mật mã và các ứng dụng thực tế của mật mã:

- Các kỹ thuật mã hóa thô sơ đã được người cỗ Ai cập sử dụng cách đây 4000 năm.
- Người cỗ Hy lạp, Ấn độ cũng đã sử dụng mã hóa cách đây hàng ngàn năm.
- Các kỹ thuật mã hóa chỉ thực sự phát triển mạnh từ thế kỷ 1800 nhờ công cụ toán học và phát triển vượt bậc trong thế kỷ 20 nhờ sự phát triển của máy tính và ngành công nghệ thông tin.

¹ Đọc thêm tại <https://www.jscrape.com/blog/stream-cipher-vs-block-cipher>.

- Trong chiến tranh thế giới thứ I và II, các kỹ thuật mã hóa được sử dụng rộng rãi trong liên lạc quân sự sử dụng sóng vô tuyến. Quân đội các nước đã sử dụng các công cụ phá mã, thám mã để giải mã các thông điệp của quân địch.
- Năm 1976 chuẩn mã hóa DES (Data Encryption Standard) được Cơ quan mật vụ Hoa Kỳ (NSA – National Security Agency) chấp nhận và sử dụng rộng rãi.
- Năm 1976, hai nhà khoa học Whitman Diffie và Martin Hellman đã đưa ra khái niệm mã hóa khóa bắt đổi xứng, hay mã hóa khóa công khai. Điều này đã đem đến những thay đổi lớn trong kỹ thuật mật mã. Theo đó, các hệ mã hóa khóa công khai bắt đầu được sử dụng rộng rãi nhờ khả năng hỗ trợ trao đổi khóa dễ dàng hơn trong khi các hệ mã hóa khóa bí mật gặp khó khăn trong quản lý và trao đổi khóa, đặc biệt khi số lượng người dùng lớn.
- Năm 1977, ba nhà khoa học Hoa Kỳ, gồm Ronald Rivest, Adi Shamir, và Leonard Adleman giới thiệu giải thuật mã hóa khóa công khai RSA. Từ đó, RSA trở thành giải thuật mã hóa khóa công khai được sử dụng rộng rãi nhất do RSA có thể vừa được sử dụng để mã hóa thông tin và sử dụng để tạo và kiểm tra chữ ký số.
- Năm 1991, phiên bản đầu tiên của chuẩn PGP (Pretty Good Privacy) ra đời.
- Năm 2001, chuẩn mã hóa AES (Advanced Encryption Standard) được thừa nhận và ứng dụng rộng rãi.

4.1.5. Ứng dụng của mã hóa

Mã hóa thông tin có thể được sử dụng để đảm bảo an toàn thông tin với các thuộc tính: bí mật, toàn vẹn, xác thực (authentication), không thể chối bỏ (non-repudiation). Cụ thể, các kỹ thuật mã hóa được ứng dụng rộng rãi trong các hệ thống, công cụ và dịch vụ bảo mật như:

- Dịch vụ xác thực (Kerberos, SSO, RADIUS,...)
- Các hệ thống kiểm soát truy cập trong hệ điều hành, ứng dụng
- Các công cụ cho đảm bảo an toàn cho truyền thông không dây (như các chuẩn bảo mật cho mạng WIFI, gồm WEP, WPA, WPA2,...)
- Các nền tảng và công cụ bảo mật, như PKI, PGP
- Các dịch vụ, ứng dụng dựa trên chứng thư số, chữ ký số, như các hệ thống thanh toán trực tuyến, dịch vụ công trực tuyến, ngân hàng trực tuyến, ngân hàng số, ví điện tử,...
- Các giao thức bảo mật, như SSL/TLS, SSH, SET, IPSec
- Các hệ thống bảo mật kênh truyền, như VPN
- Các công nghệ và ứng dụng dựa trên mã, như công nghệ khôi chuỗi (Blockchain), tiền kỹ thuật số (Bitcoin, Ethereum,...).

4.2. Các phương pháp mã hóa

Phương pháp mã hóa là phương pháp xáo trộn dữ liệu để tạo bản mã từ bản rõ. Các phương pháp mã hóa cổ điển thường phải giữ bí mật phương pháp xáo trộn dữ liệu.

Ngược lại, các phương pháp mã hóa hiện đại thường không giữ bí mật phương pháp xáo trộn dữ liệu, nhưng giữ bí mật khóa mã. Mục này mô tả một số phương pháp mã hóa cổ điển và hiện đại đã và đang được sử dụng, bao gồm phương pháp thay thế, phương pháp hoán vị, phương pháp XOR, phương pháp Vernam, phương pháp sách hoặc khóa chạy và phương pháp hàm băm. Phần tiếp theo của mục này trình bày chi tiết các phương pháp mã hóa kê trên.

4.2.1. Phương pháp thay thế

Phương pháp thay thế (Substitution) là phương pháp thay thế một giá trị này bằng một giá trị khác, như thay một ký tự bằng một ký tự khác, hoặc thay một bit bằng một bit khác. Hình 4.8 biểu diễn bộ chữ gốc, bộ chữ mã và ví dụ mã hóa sử dụng hệ mã hóa nổi tiếng thời La Mã là Caesar cipher. Nguyên tắc của Caesar cipher là dịch 3 chữ trong bộ ký tự tiếng Anh sang bên phải ($A \rightarrow D$, $B \rightarrow E$, $C \rightarrow F, \dots$). Bản rõ “LOVE” được mã hóa thành “ORYH” theo Caesar cipher.

Bộ chữ gốc	ABCDEFGHIJKLMNPQRSTUVWXYZ
Bộ chữ mã	DEFGHIJKLMNOPQRSTUVWXYZABC
LOVE --> ORYH	

Hình 4.8. Mã hóa bằng hệ mã hóa Caesar

Bản rõ =	ABCDEFGHIJKLMNPQRSTUVWXYZ
Bộ mã thay thế 1 =	DEFGHIJKLMNOPQRSTUVWXYZABC
Bộ mã thay thế 2 =	GHIJKLMNOPQRSTUVWXYZABCDE
Bộ mã thay thế 3 =	JKLMNOPQRSTUVWXYZABCDEFGHI
Bộ mã thay thế 4 =	MNOPQRSTUVWXYZABCDEFGHIJKLMNOP
TEXT --> WKGF	

Hình 4.9. Phương pháp thay thế với 4 bộ mã thay thế

Để tăng độ an toàn của phương pháp thay thế với một bộ chữ mã, người ta có thể sử dụng nhiều bộ mã thay thế, như minh họa trên Hình 4.9 với 4 bộ mã thay thế với nguyên tắc: ký tự số 1 ở bản rõ thay thế sử dụng bộ mã thay thế 1, ký tự số 2 sử dụng bộ mã thay thế 2,..., ký tự số 5 sử dụng bộ mã thay thế 1, ký tự số 6 sử dụng bộ mã thay thế 2,... Nếu các bộ mã thay thế được sắp đặt ngẫu nhiên thì cùng một ký tự xuất hiện ở các vị trí khác nhau trong bản rõ sẽ được chuyển đổi thành các ký tự khác nhau trong bản mã. Điều này giúp tăng độ an toàn do làm tăng độ khó trong việc phân tích đoán bản rõ từ bản mã.

4.2.2. Phương pháp hoán vị

Phương pháp hoán vị, hoặc đổi chỗ (Permutation) thực hiện sắp xếp lại các phần tử trong khối bản rõ để tạo bản mã. Thao tác hoán vị có thể thực hiện với từng bit, hoặc từng byte, ký tự trong bản rõ. Hình 4.10 minh họa ví dụ mã hóa bằng phương pháp hoán vị thực hiện đổi chỗ các bit, trong đó việc đổi chỗ được thực hiện theo Khóa trong khối 8 bit, tính từ bên phải.

Hình 4.11 biểu diễn ví dụ mã hóa bằng phương pháp hoán vị thực hiện đổi chỗ các ký tự, trong đó việc đổi chỗ được thực hiện theo khóa trong khối 8 ký tự, tính từ bên phải. Với bản rõ “SACKGAULSPARENOONE” ta có 3 khối rõ, 2 khối đầu có đủ 8 ký tự, còn khối cuối chỉ có 2 ký tự “NE” nên phải chèn thêm dấu trắng cho đủ khối 8 ký tự để thực hiện mã hóa hoán vị.

Khóa	$1 \rightarrow 4, 2 \rightarrow 8, 3 \rightarrow 1, 4 \rightarrow 5, 5 \rightarrow 7, 6 \rightarrow 2, 7 \rightarrow 6, 8 \rightarrow 3$
Vị trí bit	8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1
Các khối bản rõ 8-bit	0 0 1 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 0
Bản mã	0 0 0 0 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 1 0 1 1 0 0 0 0 1

Hình 4.10. Phương pháp hoán vị thực hiện đổi chỗ các bit

Vị trí ký tự:	8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1
Bản rõ:	SACKGAUL SPARENNO NE
Khóa:	1 → 4, 2 → 8, 3 → 1, 4 → 5, 5 → 7, 6 → 2, 7 → 6, 8 → 3
Bản mã:	UKAGLSCA ORPEOSAN E N

Hình 4.11. Phương pháp hoán vị thực hiện đổi chỗ các ký tự

4.2.3. Phương pháp XOR

Phương pháp mã hóa XOR sử dụng phép toán lô gíc XOR (eXclusive OR – hoặc loại trừ) để tạo bản mã, trong đó từng bit của bản rõ được XOR với bit tương ứng của khóa. Để giải mã, ta thực hiện XOR từng bit của bản mã với bit tương ứng của khóa.

Hình 4.12 minh họa quá trình mã hóa bản rõ “CAT” với khóa “VVV”. Theo đó, các ký tự của bản rõ và khóa trước hết được chuyển thành mã ASCII và biểu diễn dưới dạng nhị phân. Sau đó, thực hiện phép toán XOR trên các bit tương ứng của bản rõ và khóa để tạo bản mã.

Giá trị text	Giá trị nhị phân
CAT dưới dạng bit	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 0
VVV là khóa	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Bản mã	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 1 0

Hình 4.12. Ví dụ mã hóa bằng phương pháp XOR

4.2.4. Phương pháp Vernam

Phương pháp Vernam sử dụng một chuỗi ký tự để nối vào các ký tự của bản rõ để tạo bản mã. Chuỗi ký tự này được gọi là *one-time pad* và mỗi ký tự trong chuỗi chỉ dùng 1 lần trong một tiến trình mã hóa. Với bộ chữ tiếng Anh có 26 chữ cái, quá trình mã hóa bằng phương pháp Vernam được thực hiện như sau:

- Các ký tự của bản rõ và chuỗi nối thêm được chuyển thành số trong khoảng 1-26;
- Cộng giá trị của ký tự trong bản rõ với giá trị tương ứng trong chuỗi nối thêm;
- Nếu giá trị cộng lớn hơn 26 thì đem trừ cho 26 (phép modulo – lấy phần dư);
- Chuyển giá trị số thành ký tự để tạo bản mã.

Hình 4.13 minh họa quá trình mã hóa bản rõ “SACKGAULSPARENOONE” bằng phương pháp Vernam với chuỗi nối thêm “FPQRNSBIEHTZLACDGJ”.

Bản rõ:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Giá trị bản rõ:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
Chuỗi nối thêm:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
Giá trị chuỗi nối thêm:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Tổng bản mã+chuỗi nối:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
Sau khi trừ đi modulo:																18		
Bản mã:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

Hình 4.13. Ví dụ mã hóa bằng phương pháp Vernam

4.2.5. Phương pháp sách hoặc khóa chạy

Phương pháp sách, hoặc khóa chạy thực hiện việc mã hóa và giải mã sử dụng các khóa mã chứa trong các cuốn sách. Hiện nay phương pháp mã hóa này thường được dùng trong các bộ phim trinh thám do tính chất kỳ bí của nó. Ví dụ như, với bản mã “259,19,8; 22,3,8; 375,7,4; 394,17,2” và cuốn sách được dùng chứa khóa là “A Fire Up on the Deep”, ta có thể giải mã như sau:

- Trang 259, dòng 19, từ thứ 8 là *sack*
- Trang 22, dòng 3, từ thứ 8 là *island*
- Trang 375, dòng 7, từ thứ 4 là *sharp*
- Trang 394, dòng 17, từ thứ 2 là *path*

Như vậy, bản rõ tương ứng của bản mã “259,19,8;22,3,8;375,7,4;394,17,2” là “sack island sharp path”.

4.2.6. Phương pháp hàm băm

Theo định nghĩa trong mục 4.1.1, hàm băm là một ánh xạ chuyển đổi dữ liệu đầu vào có kích thước thay đổi thành dữ liệu đầu ra có kích thước cố định. Độ dài của thông điệp đầu vào là bất kỳ¹, nhưng chuỗi băm đầu ra thường có độ dài cố định. Hình 4.4, trang 87 đã minh họa một số thông điệp đầu vào với độ dài khác nhau, nhưng chuỗi băm đầu ra luôn có kích thước cố định và một thay đổi dù rất nhỏ ở thông điệp đầu vào cũng dẫn đến thay đổi ở chuỗi băm đầu ra. Nói theo một cách khác, các hàm băm là các giải thuật để tạo các chuỗi đại diện, hay bản tóm lược của thông điệp, thường được sử dụng để đảm bảo tính toàn vẹn của thông điệp. Chi tiết về các hàm băm được trình bày ở mục 4.4.

4.3. Các giải thuật mã hóa

Các giải thuật mã hóa là các giải thuật cho phép đảm bảo tính bí mật của thông tin lưu trữ, hoặc thông điệp truyền đưa bằng cách chuyển đổi thông điệp bản rõ thành bản mã ở bên người gửi và khôi phục bản rõ ban đầu từ bản mã ở bên người nhận. Mục này tập trung trình bày hai nhóm giải thuật mã hóa được sử dụng phổ biến, bao gồm:

- Các giải thuật mã hóa khóa đối xứng với các đại diện là DES, 3-DES và AES, và

¹ Thực tế, độ dài thông điệp đầu vào của các hàm băm là giới hạn, nhưng thường rất lớn (cỡ 2^{64} bit và có thể đến 2^{128} bit) nên có thể coi độ dài thông điệp đầu vào của các hàm băm là bất kỳ.

- Các giải thuật mã hóa khóa bất đối xứng với đại diện tiêu biểu là RSA.

4.3.1. Các giải thuật mã hóa khóa đối xứng

4.3.1.1. Khái quát

Mã hóa khóa đối xứng hay thường gọi là mã hóa khóa bí mật sử dụng một khóa bí mật duy nhất cho cả quá trình mã hóa và giải mã. Khóa bí mật được sử dụng trong quá trình mã hóa và giải mã còn được gọi là *khóa chung*, hay *khóa chia sẻ* (Shared key). Khóa bí mật dùng chung cần được bên gửi và bên nhận chia sẻ một cách an toàn trước khi có thể thực hiện việc mã hóa và giải mã các thông điệp. Hình 4.2, trang 86 đã mô tả hoạt động của một hệ mã hóa bất đối xứng, trong đó một khóa bí mật chia sẻ được sử dụng cho cả quá trình mã hóa và giải mã.

Các hệ mã hóa khóa đối xứng thường sử dụng khóa với kích thước tương đối ngắn. Một số kích thước khóa được sử dụng phổ biến là 64, 128, 192 và 256 bit. Do sự phát triển nhanh về tốc độ tính toán của máy tính, nên hiện nay các khóa có kích thước nhỏ hơn 128 bit được xem là không an toàn và hầu hết các hệ mã hóa khóa đối xứng đảm bảo an toàn hiện tại sử dụng khóa có kích thước từ 128 bit trở lên.

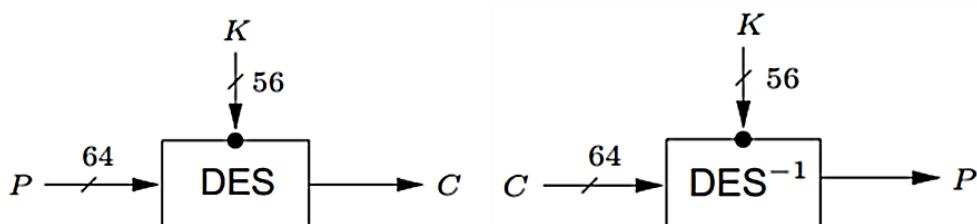
Ưu điểm nổi bật của các hệ mã hóa khóa đối xứng là độ an toàn cao (với kích thước khóa đủ lớn) và tốc độ thực thi nhanh so với các hệ mã hóa khóa bất đối xứng có độ an toàn tương đương. Tuy nhiên, nhược điểm lớn nhất của chúng là việc quản lý và phân phối khóa rất khó khăn, đặc biệt là trong các môi trường mở như mạng Internet do các bên tham gia phiên truyền thông cần thực hiện việc trao đổi các khóa bí mật một cách an toàn trước khi có thể sử dụng chúng để mã hóa và giải mã các thông điệp trao đổi.

Một số hệ mã hóa khóa đối xứng tiêu biểu, gồm DES (Data Encryption Standard), 3-DES (Triple-DES), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish và Twofish. Phần tiếp theo của mục này là mô tả các giải thuật mã hóa DES, 3-DES và AES do chúng là các giải thuật đã và đang được sử dụng rộng rãi nhất trên thực tế.

4.3.1.2. Giải thuật mã hóa DES

a. Giới thiệu

DES được phát triển tại công ty IBM vào đầu những năm 1970 và được chấp nhận là chuẩn mã hóa ở Hoa Kỳ vào năm 1977. DES được sử dụng rộng rãi trong những năm 1970 và 1980. DES là dạng mã hóa khối với kích thước khối 64 bit và khóa 64 bit. Mặc dù DES sử dụng khóa 64 bit, chỉ có 56 bit được thực sự sử dụng, 8 bit còn lại dùng cho kiểm tra chẵn lẻ. Vì vậy, 56 bit cũng được gọi là kích thước hiệu dụng của khóa DES.

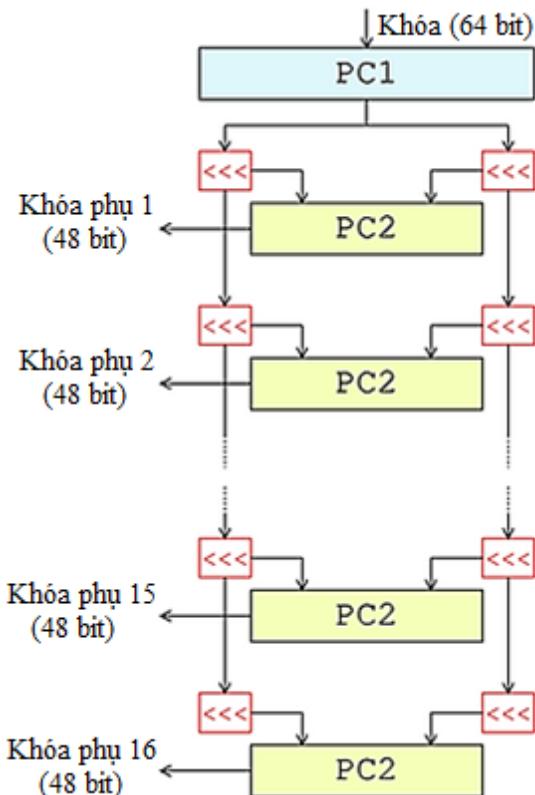


Hình 4.14. Mô hình DES: các khâu mã hóa và giải mã

Một ưu điểm của DES là sử dụng chung một giải thuật cho cả khâu mã hóa và khâu giải mã, như minh họa trên Hình 4.14, trong đó P là khối bản rõ 64 bit, K là khóa với kích thước hiệu dụng 56 bit, C là khối bản mã 64 bit, DES biểu diễn khâu mã hóa và DES' biểu diễn khâu giải mã. Hiện nay, DES được coi là không an toàn do có không gian khóa nhỏ, dễ bị vét cạn và một lý do khác là tốc độ tính toán của các hệ thống máy tính ngày càng nhanh trong những năm gần đây.

b. Thủ tục sinh khoá phụ

DES sử dụng một thủ tục sinh 16 khóa phụ (Subkey) từ khóa chính để sử dụng trong 16 vòng lặp hàm Feistel – là hàm xử lý khối dữ liệu của DES. Hình 4.15 mô tả thủ tục sinh 16 khóa phụ từ khóa chính của DES.



Hình 4.15. Thủ tục sinh các khóa phụ từ khóa chính của DES

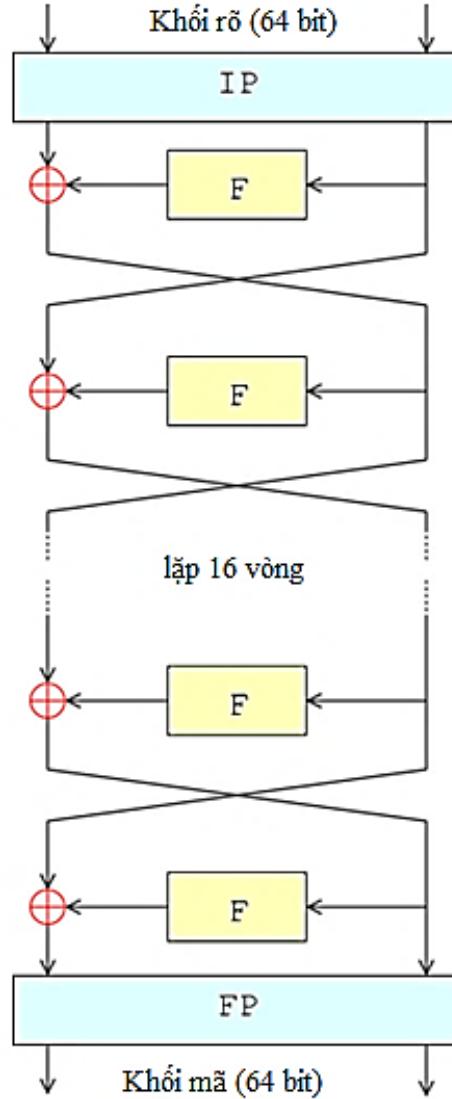
Thủ tục sinh khóa phụ DES gồm các bước xử lý chính như sau:

- Bước 1: 56 bit khóa được chọn từ khóa gốc 64 bit bởi khâu PC1 (Permuted Choice 1-Hoán vị lựa chọn 1). 8 bit còn lại được hủy hoặc dùng để kiểm tra chẵn lẻ;
- Bước 2: 56 bit được chia thành 2 phần 28 bit, mỗi phần được xử lý riêng;
- Bước 3: Mỗi phần được quay trái 1 hoặc 2 bit;
- Bước 4: Hai phần 28 bit được ghép lại và 48 bit được chọn làm Khóa phụ 1 bởi khâu PC2;
- Bước 5: Lặp lại các bước 3 và 4 để tạo 15 khóa phụ còn lại.

c. Mã hoá khối bản rõ

Với mỗi khối bản rõ 64 bit, DES thực hiện 3 bước xử lý như minh họa trên Hình 4.16 để chuyển khối bản rõ thành khối bản mã 64 bit tương ứng. Các bước cụ thể gồm:

- Bước 1: Hoán vị khởi tạo (IP – Initial Permutation);
- Bước 2: 16 vòng lặp chính thực hiện xáo trộn dữ liệu sử dụng hàm Feistel (F). Trong mỗi vòng lặp, một khóa phụ (được tạo theo thủ tục ở trên) được sử dụng. Sau mỗi vòng lặp, các kết quả trung gian được kết hợp lại sử dụng phép \oplus (XOR).
- Bước 3: Hoán vị kết thúc (FP – Final Permutation) để tạo khối bản mã đầu ra.



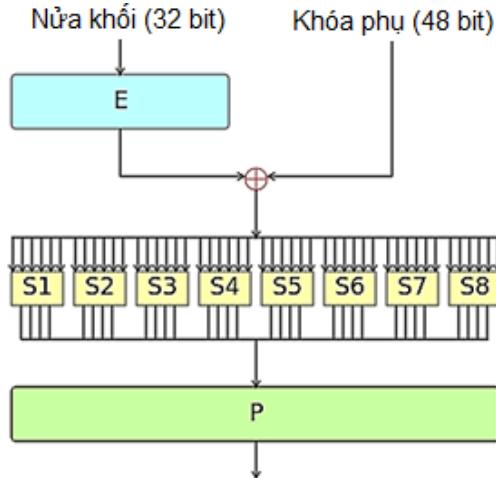
Hình 4.16. Các bước xử lý chuyển đổi khối rõ 64 bit thành khối mã 64 bit của DES

Hàm Feistel là hạt nhân trong các vòng lặp xử lý dữ liệu của DES. Trước hết, mỗi khối dữ liệu 64 bit được chia thành 2 khối con 32 bit và được xử lý lần lượt. Hàm Feistel được thực hiện trên mỗi khối dữ liệu 32 bit như biểu diễn trên Hình 4.17 gồm 4 bước xử lý như sau:

- Bước E (Expansion – Mở rộng) thực hiện mở rộng 32 bit khối đầu vào thành 48 bit bằng cách nhân đôi một nửa số bit.
- Bước \oplus trộn khối 48 bit kết quả ở bước E với khóa phụ 48 bit.
- Bước Si (Substitution – Thay thế) chia khối dữ liệu 48 bit thành 8 khối 6 bit và được chuyển vào các bộ thay thế (S1-S8). Mỗi bộ thay thế Si sử dụng phép chuyển

đổi phi tuyến tính để chuyển 6 bit đầu vào thành 4 bit đầu ra theo bảng tham chiếu. Các bộ thay thế là thành phần nhân an ninh của DES.

- Bước P (Permutation – Hoán vị) sắp xếp khối 32 bit đầu ra từ các bộ thay thế bằng phép hoán vị cố định cho ra đầu ra 32 bit.



Hình 4.17. Các bước xử lý của hàm Feistel (F)

d. Giải mã khối bản mã

Như đã đề cập, giải thuật DES có thể được sử dụng cho cả khâu mã hóa và khâu giải mã. Trong khâu giải mã các bước xử lý tương tự khâu mã hóa. Tuy nhiên, các khóa phụ dùng cho các vòng lặp được sử dụng theo trật tự ngược lại: khóa phụ số 16, 15,..., 2, 1 tương ứng được sử dụng cho các vòng lặp số 1, 2,..., 15, 16.

4.3.1.3. Giải thuật mã hóa 3-DES

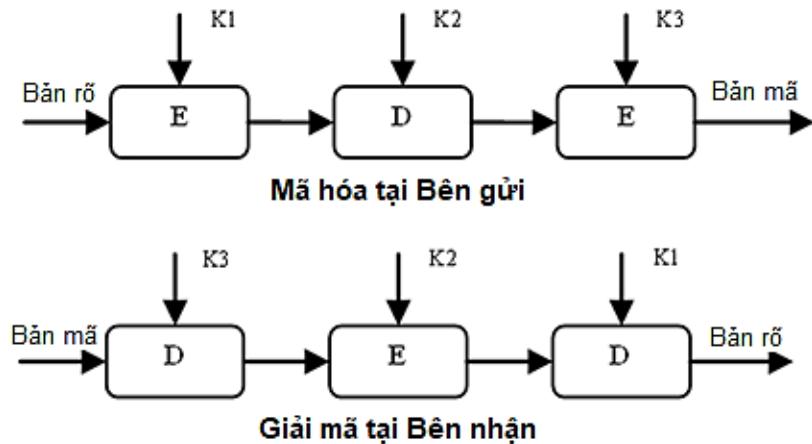
3-DES hay Triple DES có tên đầy đủ là Triple Data Encryption Algorithm (TDEA). 3-DES ra đời nhằm khắc phục vấn đề không gian khóa nhỏ của DES. Giải thuật 3-DES được phát triển từ giải thuật DES bằng cách áp dụng DES 3 lần cho mỗi khối dữ liệu đầu vào 64 bit. 3-DES sử dụng một bộ gồm 3 khóa DES: K1, K2, K3, trong đó mỗi khóa kích thước hiệu dụng là 56 bit. 3-DES cho phép lựa chọn các bộ khóa như sau:

- Lựa chọn 1: Cả 3 khóa độc lập và tổng kích thước bộ khóa là 168 bit;
- Lựa chọn 2: Các khóa K1 và K2 độc lập, còn K3 = K1 và tổng kích thước bộ khóa là 112 bit;
- Lựa chọn 3: 3 khóa giống nhau, K1 = K2 = K3 và tổng kích thước bộ khóa giữ nguyên là 56 bit.

Hình 4.18 biểu diễn quá trình mã hóa và giải mã với giải thuật 3-DES, trong đó khâu mã hóa được ký hiệu là E và khâu giải mã được ký hiệu là D. Theo đó, ở bên gửi Bản rõ được mã hóa bằng khóa K1, giải mã bằng khóa K2 và mã hóa bằng khóa K3 để cho ra Bản mã. Ở bên nhận, quá trình giải mã bắt đầu bằng việc giải mã bằng khóa K3, sau đó mã hóa bằng khóa K2 và cuối cùng giải mã bằng khóa K1 để khôi phục bản rõ.

Ưu điểm của 3-DES là nâng cao được độ an toàn so với DES nhờ tăng kích thước khóa. Ngoài ra, do thành phần chính của 3-DES là DES nên có thể tái sử dụng các mô đun cài đặt DES trong quá trình triển khai ứng dụng 3-DES. Tuy nhiên, nhược điểm

chính của 3-DES là tốc độ thực thi chậm do phải thực hiện DES lặp 3 lần cho mỗi khâu mã hóa và giải mã.



Hình 4.18. Mã hóa và giải mã với giải thuật 3-DES

4.3.1.4. Giải thuật mã hóa AES

a. Giới thiệu

AES (Advanced Encryption Standard) là một chuẩn mã hóa dữ liệu được Viện Tiêu chuẩn và Công nghệ Hoa Kỳ công nhận năm 2001. AES được xây dựng dựa trên hệ mã hóa Rijndael được phát triển và công bố năm 1998 bởi 2 nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen. AES là dạng mã hóa khóa, với khối dữ liệu có kích thước 128 bit và khóa bí mật với kích thước có thể là 128, 192, hoặc 256 bit. AES được thiết kế dựa trên mạng hoán vị-thay thế (Substitution-permutation network) và nó có thể cho tốc độ thực thi cao khi cài đặt trên cả phần cứng và phần mềm. Đặc biệt, giải thuật AES đã được tích hợp vào các bộ vi xử lý gần đây của hãng Intel dưới dạng tập lệnh AES-NI, giúp tăng đáng kể tốc độ thực thi các thao tác mã hóa và giải mã dựa trên AES.

AES vận hành dựa trên một ma trận vuông 4×4 , được gọi là *state* (trạng thái). Ma trận này gồm 16 phần tử, mỗi phần tử là 1 byte dữ liệu. State được khởi trị là khối 128 bit bản rõ và qua quá trình biến đổi sẽ chứa khối 128 bit bản mã ở đầu ra. Như đã đề cập, AES hỗ trợ 3 kích thước khóa và kích thước của khóa quyết định số vòng lặp cần thực hiện để chuyển đổi bản rõ thành bản mã. Số vòng lặp AES cần thực hiện theo kích thước khóa như sau:

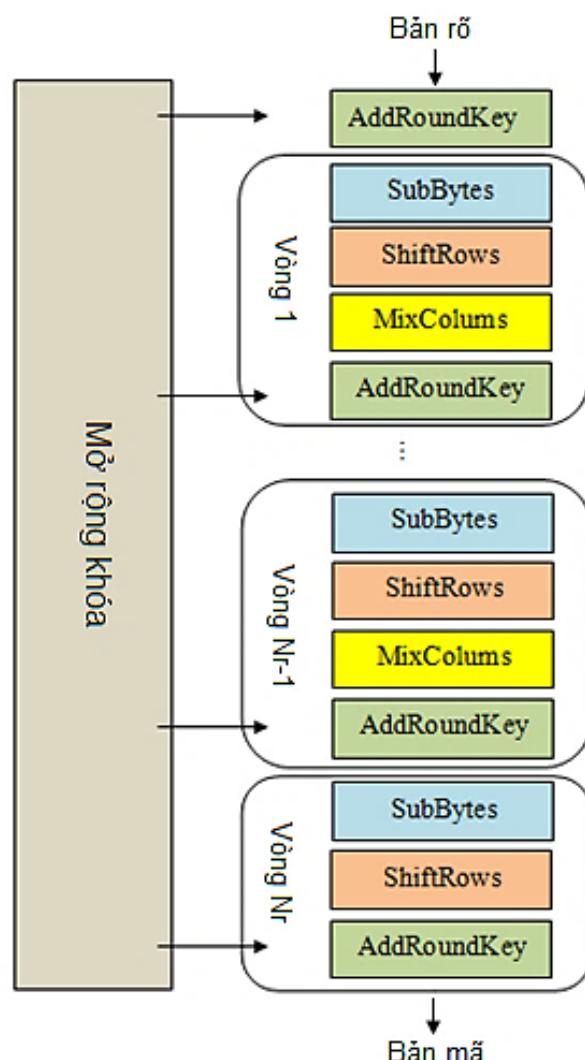
- 10 vòng lặp với khóa 128 bit;
- 12 vòng lặp với khóa 192 bit;
- 14 vòng lặp với khóa 256 bit.

b. Quá trình mã hóa

Giải thuật AES thực hiện mã hóa khối dữ liệu bản rõ, như minh họa trên Hình 4.19 gồm các bước xử lý chính như sau:

- Bước 1: Mở rộng khóa thực hiện việc sinh các khóa vòng (Round key) dùng trong các vòng lặp từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.

- Bước 2: Vòng khởi tạo thực hiện hàm AddRoundKey, trong đó mỗi byte trong *state* được kết hợp với khóa vòng sử dụng phép XOR.
- Bước 3: Các vòng lặp chính, trong đó mỗi vòng thực hiện 4 hàm biến đổi dữ liệu như sau:
 - + SubBytes là hàm thay thế phi tuyến tính, trong đó mỗi byte trong *state* được thay thế bằng một byte khác sử dụng bảng tham chiếu S-box;
 - + ShiftRows là hàm dịch dòng, trong đó mỗi dòng trong *state* được dịch một số bước theo chu kỳ;
 - + MixColumns là làm trộn các cột trong *state*, kết hợp 4 bytes trong mỗi cột.
 - + AddRoundKey là hàm kết hợp *state* với khóa vòng sử dụng phép XOR.
- Bước 4: Vòng lặp cuối tương tự các vòng lặp chính, nhưng chỉ thực hiện 3 hàm biến đổi dữ liệu, bao gồm SubBytes, ShiftRows và AddRoundKey.



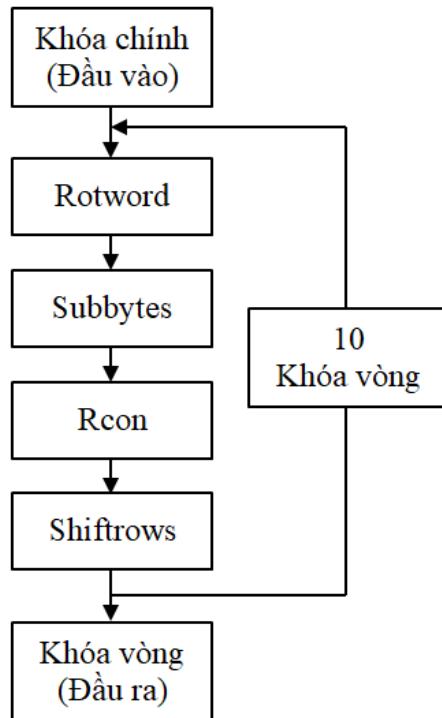
Hình 4.19. Các bước xử lý mã hóa dữ liệu của AES

c. Mở rộng khóa

Bước mở rộng khóa AES sinh các khóa vòng cho các vòng lặp xử lý dữ liệu sử dụng thủ tục sinh khóa Rijndael như biểu diễn trên Hình 4.20. Thủ tục sinh khóa Rijndael nhận

đầu vào là khóa chính AES và xuất ra một khóa vòng sau mỗi vòng lặp. Một vòng lặp của thủ tục sinh khóa Rijndael gồm các khâu sau:

- Rotword thực hiện quay trái 8 bit từng từ 32 bit lấy từ khóa chính;
- SubBytes là hàm thay thế phi tuyến tính các byte trong khóa tương tự hàm SubBytes của quá trình mã hóa AES.
- Rcon thực hiện việc tính toán giá trị $Rcon(i) = x^{(i-1)} \bmod (x^8 + x^4 + x^3 + x + 1)$.
- ShiftRows là hàm dịch dòng tương tự hàm ShiftRows của quá trình mã hóa AES.



Hình 4.20. Thủ tục sinh khóa Rijndael

d. Các hàm xử lý dữ liệu

Như đã đề cập, AES sử dụng 4 hàm xử lý để biến đổi dữ liệu, bao gồm SubBytes, ShiftRows, MixColumns và AddRoundKey. Mục này trình bày chi tiết về các hàm này.

Hàm SubBytes thay thế mỗi byte trong ma trận *state* bởi 1 byte trong Rijndael S-box, hay $b_{ij} = S(a_{ij})$ như minh họa trên Hình 4.21. S-box là một bảng tham chiếu phi tuyến tính, được tạo ra bằng phép nhân nghịch đảo một số cho trước trong trường $GF(2^8)$ ¹.

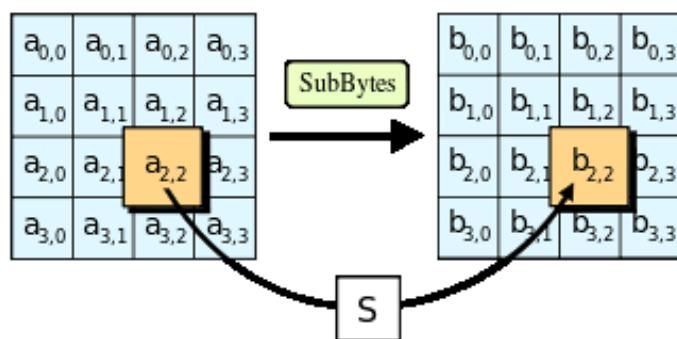
Hàm ShiftRows dịch các dòng của ma trận *state* theo chu kỳ sang trái theo nguyên tắc: hàng số 0 giữ nguyên, hàng số 1 dịch 1 byte sang trái, hàng số 2 dịch 2 byte sang trái và hàng số 3 dịch 3 byte sang trái, như minh họa trên Hình 4.22.

*Hàm MixColumns*² nhân mỗi cột của ma trận *state* với một đa thức $c(x)$, như minh họa trên Hình 4.23. Đa thức này được tính theo công thức: $c(x) = 3x^3 + x^2 + x + 2$.

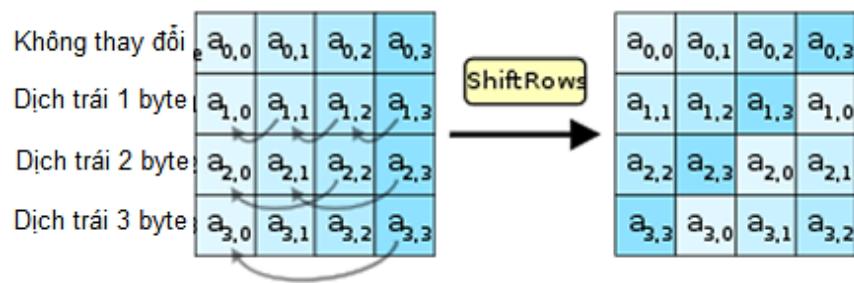
Hàm AddRoundKey kết hợp mỗi byte của ma trận *state* với một byte tương ứng của khóa vòng sử dụng phép \oplus (XOR), như minh họa trên Hình 4.24.

¹ Đọc thêm về bảng S-box tại https://cryptography.fandom.com/wiki/Rijndael_S-box

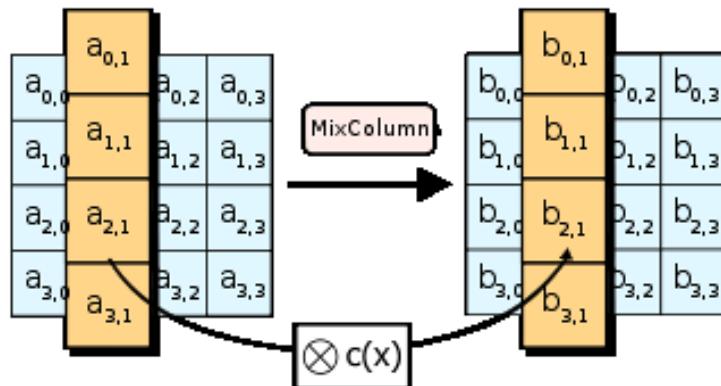
² Đọc thêm về hàm MixColumns và $c(x)$ https://cryptography.fandom.com/wiki/Rijndael_mix_columns



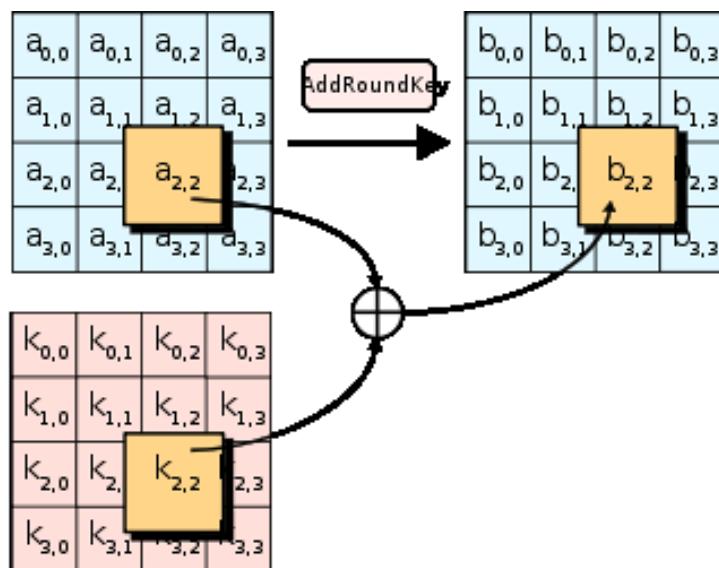
Hình 4.21. Hàm SubBytes sử dụng Rijndael S-box



Hình 4.22. Hàm ShiftRows



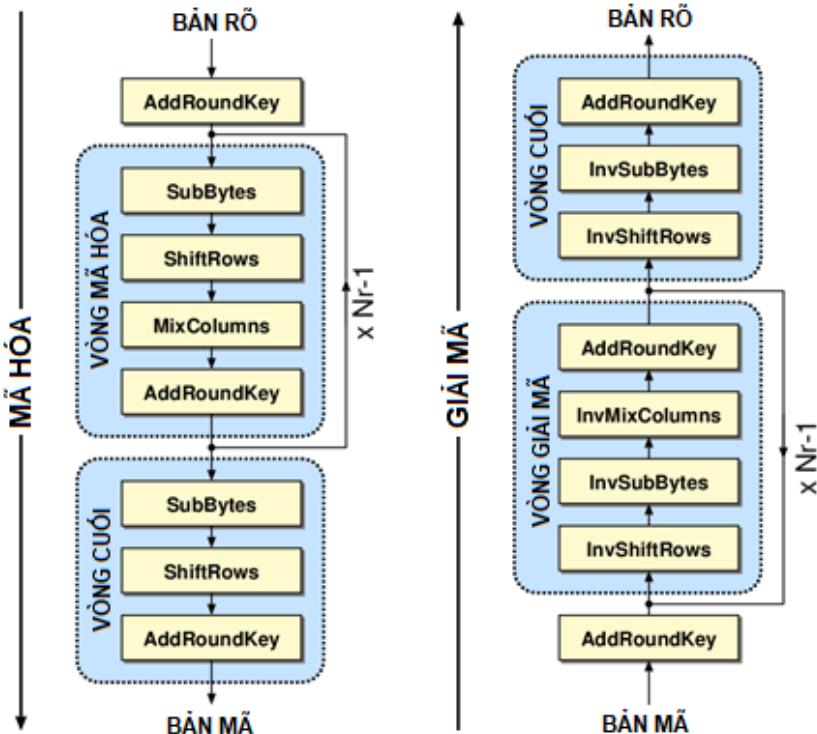
Hình 4.23. Hàm MixColumns



Hình 4.24. Hàm AddRoundKey

e. Quá trình giải mã

Quá trình giải mã trong AES cũng gồm các bước xử lý tương tự như quá trình mã hóa. Hình 4.25 biểu diễn quá trình giải mã đối sánh với quá trình mã hóa trong AES. Theo đó, ngoài bước Mở rộng khóa, quá trình giải mã gồm Vòng khởi tạo thực thi hàm AddRoundKey, Các vòng giải mã và Vòng cuối để chuyển đổi khối mã thành khối rõ.



Hình 4.25. Quá trình mã hóa và giải mã trong AES

Điểm khác biệt chính của quá trình giải mã so với quá trình mã hóa là các *hàm đảo* được sử dụng, bao gồm InvSubBytes, InvShiftRows và InvMixColumns tương ứng thay cho các hàm SubBytes, ShiftRows và MixColumns. Hàm InvSubBytes thay thế phi tuyến tính các byte của ma trận *state* sử dụng bảng *S-box đảo*¹, hàm InvShiftRows dịch các byte của từng dòng trong ma trận *state* sang phải theo cùng nguyên tắc với ShiftRows và hàm InvMixColumns nhân các cột của ma trận *state* với đa thức $c(x)$ *đảo*².

4.3.2. Các giải thuật mã hóa khóa bất đối xứng

4.3.2.1. Khái quát

Mã hóa khóa bất đối xứng, thường được gọi là mã hóa khóa công khai sử dụng một cặp khóa cho quá trình mã hóa và giải mã. Trong cặp khóa, khóa công khai được sử dụng cho khâu mã hóa và khóa riêng được sử dụng cho khâu giải mã. Chỉ khóa riêng cần giữ bí mật, còn khóa công khai có thể phổ biến rộng rãi, nhưng phải đảm bảo tính toàn vẹn và xác thực chủ thể³. Hình 4.3, trang 87 đã mô tả hoạt động của một hệ mã hóa khóa bất đối xứng, trong đó một cặp khóa, gồm khóa công khai và khóa riêng tương ứng được sử dụng cho quá trình mã hóa và giải mã.

¹ Đọc thêm về bảng S-box đảo tại https://cryptography.fandom.com/wiki/Rijndael_S-box

² Đọc thêm về hàm InvMixColumns và $c(x)$ đảo tại https://cryptography.fandom.com/wiki/Rijndael_mix_columns

³ Đảm bảo tính toàn vẹn là khóa không bị sửa đổi và xác thực chủ thể là xác minh được chủ sở hữu của khóa.

Đặc điểm nổi bật của các hệ mã hóa khóa bất đối xứng là kích thước khóa rất lớn, có thể lên đến hàng ngàn bit. Do vậy, các hệ mã hóa dạng này thường có tốc độ thực thi chậm hơn nhiều lần so với các hệ mã hóa khóa đối xứng có độ an toàn tương đương. Mặc dù vậy, các hệ mã hóa khóa bất đối xứng có khả năng đạt độ an toàn cao và ưu điểm nổi bật nhất là việc quản lý và phân phối khóa đơn giản hơn do chỉ khóa riêng trong cặp khóa cần giữ bí mật, còn khóa công khai có thể phân phối rộng rãi trong môi trường mở như mạng Internet.

Các giải thuật mã hóa khóa bất đối xứng điển hình bao gồm: RSA, Rabin, ElGamal, McEliece, Knapsack,... [14][15]. Mục tiếp theo trình bày về giải thuật RSA là một trong các giải thuật mã hóa khóa bất đối xứng được sử dụng rộng rãi nhất trên thực tế.

4.3.2.2. Giải thuật mã hóa RSA

a. Giới thiệu

Giải thuật mã hóa RSA được 3 nhà khoa học người Mỹ là R. Rivest, A. Shamir và L. Adleman phát minh năm 1977 và tên giải thuật RSA được đặt theo chữ cái đầu của tên 3 đồng tác giả. Độ an toàn của RSA dựa trên tính khó của việc phân tích số nguyên rất lớn, với độ lớn cỡ hàng trăm chữ số thập phân. RSA sử dụng một cặp khóa, trong đó khóa công khai dùng để mã hóa và khóa riêng dùng để giải mã. Chỉ khóa riêng RSA cần giữ bí mật, còn khóa công khai có thể công bố rộng rãi.

Hiện nay, các khóa RSA có kích thước nhỏ hơn 1024 bit được coi là không an toàn do tốc độ các hệ thống máy tính tăng nhanh. Để đảm bảo an toàn, khuyến nghị sử dụng khóa 2048¹ bit trong giai đoạn 2010-2020. Trong tương lai, cần sử dụng khóa RSA có kích thước lớn hơn, chẳng hạn 3072 bit.

RSA hiện là một trong các giải thuật mã hóa khóa bất đối xứng được sử dụng rộng rãi nhất trên thực tế: RSA có thể được sử dụng để mã hóa thông điệp, và để tạo và kiểm tra chữ ký số. Phản tiếp theo mô tả vấn đề sinh khóa, mã hóa – giải mã và một số yêu cầu tăng cường độ an toàn trong quá trình sinh khóa RSA.

b. Sinh khóa

RSA cung cấp một thủ tục sinh cặp khóa, gồm khóa công khai và khóa riêng tương đối đơn giản. Cụ thể, thủ tục sinh khóa gồm các bước như sau:

- Tạo 2 số nguyên tố p và q ;
- Tính modulo $n = p \times q$
- Tính $\Phi(n) = (p-1) \times (q-1)$
- Chọn số nguyên tố e sao cho $0 < e < \Phi(n)$ và $\gcd(e, \Phi(n)) = 1$, trong đó hàm $\gcd()$ tính ước số chung lớn nhất của 2 số nguyên. Do $\gcd(e, \Phi(n)) = 1$ nên e và $\Phi(n)$ là 2 số nguyên tố cùng nhau.
- Chọn số nguyên d sao cho $d \equiv e^{-1} \pmod{\Phi(n)}$,
hoặc $(d \times e) \pmod{\Phi(n)} = 1$

¹ Đọc thêm về khuyến nghị kích thước khóa tại <https://paragonie.com/blog/2019/03/definitive-2019-guide-cryptographic-key-sizes-and-algorithm-recommendations>.

hay d là modulo nghịch đảo của e .

- Ta có (n, e) là khóa công khai, (n, d) là khóa riêng và n còn được gọi là modulo.

c. Mã hóa và giải mã

- Mã hóa:

- + Thông điệp bản rõ m đã được chuyển thành số, với $m < n$. Nếu thông điệp bản rõ m có kích thước lớn thì được chia thành các khối m_i , với $m_i < n$.
 - + Bản mã $c = m^e \text{ mod } n$
- Giải mã:
- + Bản mã c , với $c < n$
 - + Bản rõ $m = c^d \text{ mod } n$

d. Ví dụ

- Sinh khóa:

- + Chọn 2 số nguyên tố $p = 3$ và $q = 11$
- + Tính $n = p \times q = 3 \times 11 = 33$
- + Tính $\Phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$
- + Chọn số e sao cho $0 < e < 20$, và $\gcd(e, \Phi(n)) = 1$. Chọn $e = 7$.
- + Tính $(d \times e) \text{ mod } \Phi(n) \rightarrow (d \times 7) \text{ mod } 20 = 1$

$$d = (20 \times k + 1)/7 \rightarrow d = 3 \quad (k=1)$$

- + Ta có: khóa công khai là $(33, 7)$ và khóa riêng là $(33, 3)$

- Mã hóa:

- + Với bản rõ $m = 6$,
- + $c = m^e \text{ mod } n = 6^7 \text{ mod } 33 = 279936 \text{ mod } 33 = 30$
- + Vậy bản mã $c = 30$

- Giải mã:

- + Với bản mã $c = 30$
- + $m = c^d \text{ mod } n = 30^3 \text{ mod } 33 = 27000 \text{ mod } 33 = 6$
- + Vậy bản rõ $m = 6$.

e. Một số yêu cầu với quá trình sinh khóa

Dưới đây liệt kê một số yêu cầu cơ bản đặt ra với các tham số sinh khóa và khóa để đảm bảo độ an toàn cho cặp khóa RSA. Các yêu cầu cụ thể gồm [14]:

- Yêu cầu với các tham số sinh khóa p và q :

- + Các số nguyên tố p và q phải được chọn sao cho việc phân tích n ($n = p \times q$) là không khả thi về mặt tính toán. p và q nên có cùng độ lớn (tính bằng bit) và phải là các số đủ lớn. Nếu n có kích thước 2048 bit thì p và q nên có kích thước khoảng 1024 bit.

- + Hiệu số $p - q$ không nên quá nhỏ, do nếu $p - q$ quá nhỏ, tức $p \approx q$ và $p \approx \sqrt{n}$. Như vậy, có thể chọn các số nguyên tố ở gần \sqrt{n} và thử lần lượt. Khi có được p , có thể tính q và tìm ra d là khóa bí mật từ khóa công khai e và $\Phi(n) = (p - 1)(q - 1)$. Nếu p và q được chọn ngẫu nhiên và $p - q$ đủ lớn, khả năng hai số này bị phân tích từ n giảm đi.
- + Các số nguyên tố p và q nên là *số nguyên tố mạnh* (Strong prime). Số nguyên tố p được xem là số nguyên tố mạnh nếu nó thỏa mãn 3 điều kiện: (i) $p - 1$ có một thừa số nguyên tố lớn, giả thiết là r ; (ii) $p + 1$ có một thừa số nguyên tố lớn và (iii) $r - 1$ có một thừa số nguyên tố lớn.
- Vấn đề sử dụng số mũ mã hóa (e) nhỏ: Khi sử dụng số mũ mã hóa (e) nhỏ, chẳng hạn $e = 3$ có thể tăng tốc độ mã hóa. Kẻ tấn công có thể nghe lén và lấy được bản mã, từ đó phân tích bản mã để khôi phục bản rõ. Do số mũ mã hóa nhỏ nên chi phí cho phân tích, hoặc vét cạn không quá lớn. Do vậy, nên sử dụng số mũ mã hóa e đủ lớn và thêm chuỗi ngẫu nhiên vào khôi rõ trước khi mã hóa để giảm khả năng bị vét cạn hoặc phân tích bản mã.
- Vấn đề sử dụng số mũ giải mã (d) nhỏ: Khi sử dụng số mũ giải mã (d) nhỏ, có thể tăng tốc độ giải mã. Nếu d nhỏ và $\gcd(p-1, q-1)$ cũng nhỏ thì d có thể tính được tương đối dễ dàng từ khóa công khai (n, e) . Do vậy, để đảm bảo an toàn, nên sử dụng số mũ giải mã d đủ lớn.

Do giới hạn phạm vi môn học, chi tiết về các yêu cầu trên và các yêu cầu bổ sung khác, độc giả có thể tìm thấy trong mục 8.2.3, trang 290-291, tài liệu tham khảo [14].

4.4. Các hàm băm

Theo định nghĩa trong mục 4.1.1, trang 87, hàm băm là một ánh xạ chuyển đổi dữ liệu đầu vào có kích thước thay đổi sang dữ liệu đầu ra có kích thước cố định. Hầu hết các hàm băm đều hỗ trợ độ dài thông điệp đầu vào rất lớn, đến 2^{64} bit, hoặc thậm chí đến 2^{128} bit, nên có thể coi độ dài thông điệp đầu vào của hàm băm là *bất kỳ*. Do chuỗi băm đầu ra thường có kích thước cố định và nhỏ hơn nhiều lần so với thông điệp đầu vào, nó thường được gọi là *chuỗi đại diện*, hay *bản tóm lược* (digest) của thông điệp. Mục này giới thiệu các tính chất cơ bản của hàm băm, phân loại các hàm băm, mô hình xử lý dữ liệu và mô tả một số hàm băm thông dụng gồm MD5 và SHA1.

4.4.1. Khái quát về hàm băm

4.4.1.1. Giới thiệu

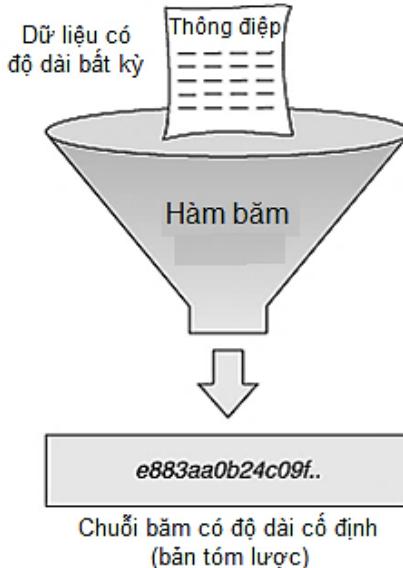
Hàm băm là một hàm toán học h có tối thiểu 2 thuộc tính cơ bản [14]:

- Nén: với h là một ánh xạ từ chuỗi đầu vào x có chiều dài bất kỳ sang một chuỗi đầu ra $h(x)$ có chiều dài cố định n bit;
- Dễ tính toán: cho trước hàm h và đầu vào x , việc tính toán $h(x)$ là dễ dàng.

Đây là 2 thuộc tính cơ bản nhất mà mọi hàm băm đều có. Ngoài ra, hàm băm còn có một số thuộc tính cơ bản khác, gồm kháng tiền ảnh (preimage resistance), kháng tiền ảnh thứ 2 (2nd-preimage resistance) và kháng va chạm (collision resistance). Chi tiết về các

thuộc tính của hàm băm, độc giả có thể tìm thấy trong các mục 9.2.1 và 9.2.2, trang 322-324, tài liệu tham khảo [14].

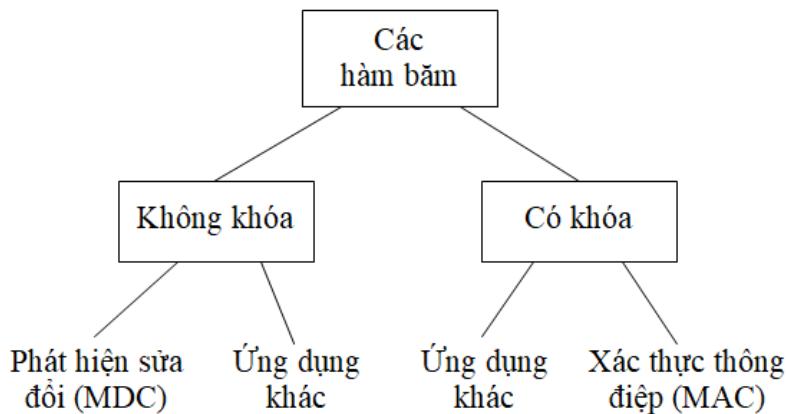
Hình 4.26 minh họa mô hình nén dữ liệu của hàm băm, theo đó thông điệp dữ liệu đầu vào với chiều dài bất kỳ đi qua nhiều vòng xử lý của hàm băm để tạo chuỗi đại diện, hay bản tóm lược có kích thước cố định ở đầu ra.



Hình 4.26. Mô hình nén dữ liệu của hàm băm

4.4.1.2. Phân loại

Có thể phân loại các hàm băm theo khóa sử dụng, hoặc theo chức năng. Theo khóa sử dụng, các hàm băm gồm 2 loại: hàm băm không khóa (unkeyed) và hàm băm có khóa (keyed), như biểu diễn trên Hình 4.27. Trong khi hàm băm không khóa nhận đầu vào chỉ là thông điệp (theo dạng $h(x)$, với hàm băm h và thông điệp x), hàm băm có khóa nhận đầu vào gồm thông điệp và khóa bí mật (theo dạng $h(x, K)$, với hàm băm h và thông điệp x và khóa bí mật K). Trong nhóm các hàm băm không khóa, các mã phát hiện sửa đổi (MDC – Modification Detection Code) được sử dụng rộng rãi nhất, bên cạnh một số hàm băm không khóa cho các ứng dụng khác. Tương tự, trong nhóm các hàm băm có khóa, các mã xác thực thông điệp (MAC - Message Authentication Code) được sử dụng rộng rãi nhất, bên cạnh một số hàm băm có khóa cho các ứng dụng khác.



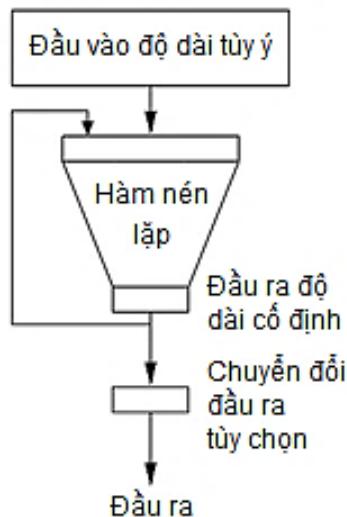
Hình 4.27. Phân loại các hàm băm theo khóa sử dụng

Theo chức năng, có thể chia các hàm băm thành 2 loại chính:

- Mã phát hiện sửa đổi (MDC) thường được dùng để tạo chuỗi đại diện, hay bản tóm lược cho thông điệp và được sử dụng kết hợp với các kỹ thuật khác¹ để đảm bảo tính toàn vẹn của thông điệp. MDC thuộc loại hàm băm không khóa. MDC lại được chia thành 2 loại con:
 - + Hàm băm một chiều (OWHF - One-way hash function) là dạng hàm băm, theo đó việc tính toán giá trị băm của thông điệp là tương đối dễ dàng với chi phí tính toán thấp, nhưng việc khôi phục thông điệp từ giá trị băm là rất khó khăn, hoặc không khả thi về mặt tính toán;
 - + Hàm băm kháng va chạm (CRHF - Collision resistant hash function) là dạng hàm băm, theo đó sẽ rất khó để tìm được 2 thông điệp khác nhau nhưng có cùng giá trị băm đầu ra².
- Mã xác thực thông điệp (MAC) cũng được dùng để đảm bảo tính toàn vẹn của thông điệp mà không cần một kỹ thuật bổ sung nào khác. MAC là loại hàm băm có khóa, với đầu vào là thông điệp và một khóa bí mật. Các hàm băm MAC được sử dụng rộng rãi để đảm bảo tính toàn vẹn khỏi dữ liệu truyền trong các giao thức bảo mật, như SSL/TLS và IPsec.

4.4.1.3. Mô hình xử lý dữ liệu

Hình 4.28 biểu diễn mô hình tổng quát xử lý dữ liệu của các hàm băm. Theo đó, thông điệp đầu vào với độ dài tùy ý đi qua hàm nén lặp nhiều vòng để tạo chuỗi đầu ra có kích thước cố định. Chuỗi đầu ra đi qua một khâu chuyển đổi định dạng tùy chọn để tạo ra chuỗi băm đầu ra.

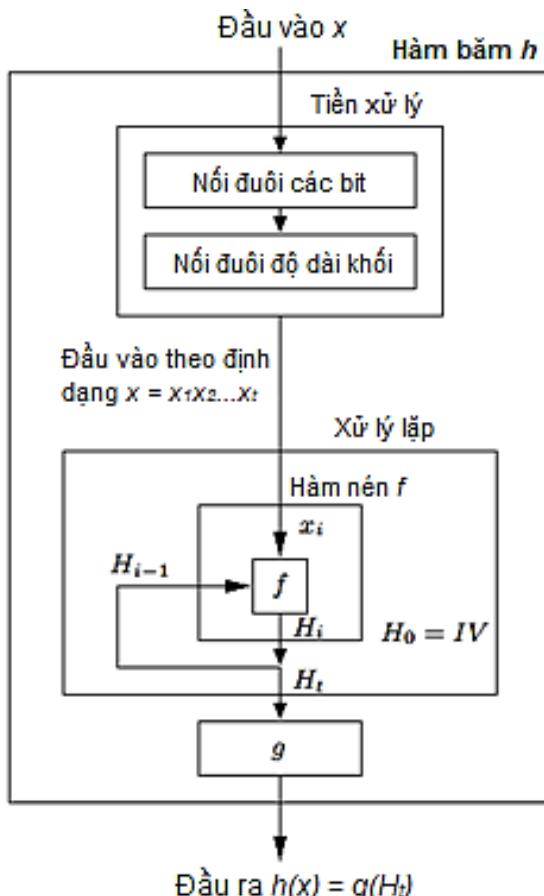


Hình 4.28. Mô hình tổng quát xử lý dữ liệu của hàm băm

¹ MDC thường được sử dụng với chữ ký số để đảm bảo tính toàn vẹn của thông điệp truyền đưa. Đọc thêm tại <https://www.us-cert.gov/ncas/tips/ST04-018>.

² Về lý thuyết, tồn tại 2 chuỗi đầu vào khác nhau nhưng có cùng chuỗi băm đầu ra do không gian đầu vào lớn hơn rất nhiều lần không gian đầu ra. Tuy nhiên, việc tìm được 2 chuỗi đầu vào như vậy với hàm băm CRHF có độ khó tính toán rất cao.

Hình 4.29 mô tả chi tiết quá trình xử lý dữ liệu của các hàm băm. Theo đó, quá trình xử lý gồm 3 bước chính: (1) tiền xử lý, (2) xử lý lặp và (3) chuyển đổi định dạng đầu ra. Trong bước (1) tiền xử lý, thông điệp đầu vào x trước hết được nối đuôi thêm một số bit và kích thước khối, sau đó chia thành các khối có kích thước xác định. Kết quả của bước này là thông điệp đầu vào được chia thành t khối dữ liệu có cùng kích thước có dạng $x = x_1x_2\dots x_t$ làm đầu vào cho bước xử lý lặp. Trong bước (2) xử lý lặp, từng khối dữ liệu x_i được xử lý thông qua hàm nén f để tạo đầu ra là H_i , trong đó giá trị khởi tạo $H_0 = IV^1$. Kết quả của bước xử lý lặp là chuỗi đầu ra H_t và trong bước (3), H_t được chuyển đổi định dạng bởi hàm g để tạo chuỗi giá trị băm kết quả $h(x) = g(H_t)$.



Hình 4.29. Mô hình chi tiết xử lý dữ liệu của hàm băm

4.4.2. Một số hàm băm thông dụng

4.4.2.1. Khái quát

Các hàm băm thông dụng giới thiệu trong mục này đều là các hàm băm không khóa, gồm một số hàm băm và họ hàm băm thông dụng như sau:

- Hàm băm CRC-32 với chuỗi đầu ra 32 bit là mã phát hiện lỗi (error-detecting code) được sử dụng trong mạng truyền thông số và các thiết bị lưu trữ;
- Họ hàm băm MD (Message Digest):
 - + Các hàm băm MD2, MD4, MD5 với độ dài chuỗi băm đầu ra 128 bit đều do R. Rivest (đồng tác giả giải thuật RSA) thiết kế. Các hàm băm này hiện nay

¹ IV (Initializing Value) là giá trị khởi tạo, hoặc giá trị được đặt trước. IV được chọn theo từng hàm băm cụ thể.

được coi là không còn an toàn do tồn tại nhiều lỗi bảo mật không thể khắc phục và khuyến nghị không nên tiếp tục sử dụng;

- + Hàm băm MD6 cho chuỗi đầu băm ra có độ dài trong khoảng 0 đến 512 bit được giới thiệu lần đầu vào năm 2008. MD6 được thiết kế để cạnh tranh với các hàm băm SHA2, SHA3. Tuy nhiên, sau nhiều lần chỉnh sửa, MD6 vẫn chưa được viện NIST, Hoa Kỳ công nhận và dự án tạm dừng từ năm 2011¹.
- Họ hàm băm SHA (Secure Hash Algorithm):
 - + Hàm băm SHA0 lần đầu được giới thiệu vào năm 1993 và chỉ được sử dụng trong một thời gian ngắn và bị thay thế bởi SHA1 ra đời vào năm 1995 do gặp phải một số vấn đề về độ an toàn². Cả hai hàm băm đều có độ dài chuỗi đầu ra 160 bit. Đến năm 2011, viện NIST khuyến nghị không nên tiếp tục sử dụng SHA1 do hàm băm này cũng không còn thực sự an toàn. Mặc dù vậy, SHA1 vẫn đang được sử dụng trong nhiều ứng dụng quản lý mật khẩu và đảm bảo tính toàn vẹn dữ liệu truyền thông;
 - + Các hàm băm SHA2, gồm nhóm 6 hàm băm³: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 tương ứng với các chuỗi băm đầu ra 224, 256, 384 và 512 bit. Trong đó, hai hàm băm SHA-256 và SHA-512 hiện nay được sử dụng rộng rãi trong các ứng dụng chữ ký số;
 - + Hàm băm SHA3 cho chuỗi đầu ra có độ dài trong khoảng 0 đến 512 bit được viện NIST công bố vào năm 2015. SHA3 được thiết kế với cấu trúc bên trong hoàn toàn mới và khác biệt với cấu trúc của các hàm băm thế hệ trước, như MD5, SHA1 và SHA2. Mặc dù được đánh giá có độ an toàn cao hơn so với SHA2, nhưng SHA3 vẫn chưa được sử dụng rộng rãi trên thực tế⁴.

Các mục con tiếp theo của mục này mô tả chi tiết về MD5 và SHA1 - 2 hàm băm đã và đang được sử dụng rộng rãi. Mặc dù các hàm băm này được cho là không còn thực sự an toàn trong thời gian hiện nay, nhưng cấu trúc của chúng vẫn được sử dụng trong phát triển các hàm băm mới hơn, như SHA-224, SHA-256, SHA-384 và SHA-512.

4.4.2.2. Hàm băm MD5

a. Giới thiệu

MD5 là hàm băm không khóa được Ronald Rivest thiết kế năm 1991 để thay thế phiên bản trước đó là MD4. Chuỗi giá trị băm đầu ra của MD5 là 128 bit và thường được biểu diễn thành 32 số hexa. MD5 được sử dụng khá rộng rãi trong nhiều ứng dụng, như tạo chuỗi đảm bảo tính toàn vẹn thông điệp trao đổi, tạo chuỗi phát hiện lỗi (Checksum) và mã hóa mật khẩu trong các hệ điều hành và các ứng dụng. MD5 hiện nay được khuyến nghị không nên sử dụng do không còn đủ an toàn. Nhiều điểm yếu của MD5 đã bị khai thác, như trường hợp MD5 bị khai thác bởi mã độc Flame vào năm 2012⁵.

¹ Đọc thêm về MD6 tại <https://groups.csail.mit.edu/cis/md6/>.

² Đọc thêm về các vấn đề an toàn của SHA0 và SHA1 tại <https://tools.ietf.org/html/rfc6194>

³ Đọc thêm về SHA2 tại <https://tools.ietf.org/html/rfc6234>.

⁴ Đọc thêm tại <https://www.csoonline.com/article/3256088/why-arent-we-using-sha3.html>.

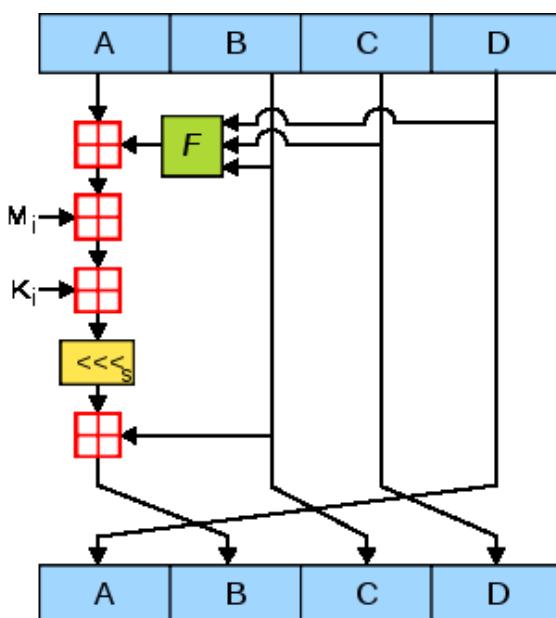
⁵ Đọc thêm tại <https://threatpost.com/microsoft-details-flame-hash-collision-attack-060612/76658/>

b. Quá trình xử lý thông điệp

Quá trình xử lý thông điệp của MD5 gồm 2 khâu là *tiền xử lý* và *các vòng lặp xử lý*. Chi tiết về các khâu này như sau:

- **Tiền xử lý:** Thông điệp được chia thành các khối 512 bit (tương đương 16 từ, mỗi từ 32 bit). Việc nối đuôi các bit và độ dài thông điệp sao cho kích thước thông điệp sau nối đuôi chia hết cho 512.
- **Các vòng lặp xử lý:** Phần xử lý chính của MD5 làm việc trên *state* 128 bit, chia thành 4 từ (A, B, C, D), mỗi từ 32 bit. Cụ thể các bước được thực hiện như sau:
 - + Các từ A, B, C, D được khởi trị bằng một hằng cố định;
 - + Từng phần 32 bit của khối đầu vào 512 bit được đưa dần vào để thay đổi *state*;
 - + Quá trình xử lý gồm 4 vòng, mỗi vòng gồm 16 thao tác tương tự nhau. Mỗi thao tác gồm: Xử lý bởi hàm F (có 4 dạng hàm khác nhau cho mỗi vòng), phép cộng modulo và phép quay trái.

Hình 4.30 biểu diễn lưu đồ xử lý của một thao tác trong MD5, trong đó A, B, C, D là các từ 32 bit của *state*; Mi: khối 32 bit thông điệp đầu vào; Ki là 32 bit hằng khác nhau cho mỗi thao tác; $\lll s$ là thao tác dịch trái s bit; \boxplus biểu diễn phép cộng modulo 32 bit và F là hàm phi tuyến tính.



Hình 4.30. Lưu đồ xử lý một thao tác trong MD5

Hàm phi tuyến tính F gồm 4 dạng được dùng cho 4 vòng lặp như sau:

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$

$$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$$

$$H(B, C, D) = B \oplus C \oplus D$$

$$I(B, C, D) = C \oplus (B \vee \neg D)$$

trong đó, các ký hiệu \oplus , \wedge , \vee , \neg tương ứng biểu diễn các phép toán lô gíc XOR, AND, OR và NOT.

4.4.2.3. Hàm băm SHA1

a. Giới thiệu

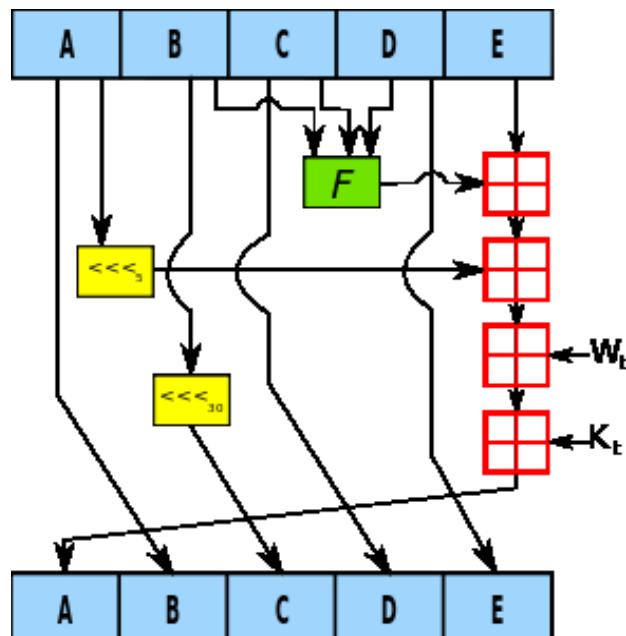
SHA1 được Cơ quan mật vụ Hoa Kỳ thiết kế năm 1995 để thay thế cho hàm băm SHA0. Chuỗi giá trị băm đầu ra của SHA1 có kích thước 160 bit và thường được biểu diễn thành 40 số hexa. Tương tự MD5, SHA1 được sử dụng rộng rãi để đảm bảo tính xác thực và toàn vẹn thông điệp. Theo khuyến nghị của viện NIST, Hoa Kỳ, SHA1 không thực sự an toàn trong thời gian hiện nay và nên được thay thế bằng SHA2 và SHA3.

b. Quá trình xử lý thông điệp

SHA1 sử dụng thủ tục xử lý thông điệp tương tự MD5, cũng gồm 2 khâu là *tiền xử lý* và *các vòng lặp xử lý*. Chi tiết các khâu này như sau:

- Tiền xử lý: Thông điệp được chia thành các khối 512 bit (tương đương 16 từ, mỗi từ 32 bit). Việc nối đuôi các bit và độ dài thông điệp sao cho kích thước thông điệp sau nối đuôi chia hết cho 512.
- Các vòng lặp xử lý: Phần xử lý chính của SHA1 làm việc trên *state* 160 bit, chia thành 5 từ (A, B, C, D, E), mỗi từ 32 bit. Cụ thể các bước được thực hiện như sau:
 - + Các từ A, B, C, D, E được khởi trị bằng một hằng cố định;
 - + Từng phần 32 bit của khối đầu vào 512 bit được đưa dần vào để thay đổi *state*;
 - + Quá trình xử lý gồm 80 vòng, mỗi vòng gồm các thao tác: add, and, or, xor, rotate, mod. Mỗi vòng xử lý gồm: Xử lý bởi hàm phi tuyến tính F, phép cộng modulo và phép quay trái.

Hình 4.31 biếu diễn lưu đồ một vòng xử lý của SHA1, trong đó A, B, C, D, E là các từ 32 bit của *state*; W_t : khối 32 bit thông điệp đầu vào; K_t là 32 bit hằng khác nhau cho mỗi vòng; $<<<n$ là thao tác dịch trái n bit; \oplus biếu diễn phép cộng modulo 32 bit và F là hàm phi tuyến tính.



Hình 4.31. Lưu đồ một vòng xử lý của SHA1

Hàm phi tuyến tính F phụ thuộc vào số vòng lặp t như sau:

$$F_t(B, C, D) = \begin{cases} (B \wedge C) \vee ((\neg B \wedge D) & \text{nếu } 0 \leq t \leq 19 \\ B \oplus C \oplus D & \text{nếu } 20 \leq t \leq 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & \text{nếu } 40 \leq t \leq 59 \\ B \oplus C \oplus D & \text{nếu } 60 \leq t \leq 79 \end{cases}$$

trong đó, các ký hiệu \oplus , \wedge , \vee , \neg tương ứng biểu diễn các phép toán lô gic XOR, AND, OR và NOT.

4.5. Kết chương

Chương này trình bày vấn đề đảm bảo an toàn thông tin dựa trên các kỹ thuật mật mã, trong đó bao gồm các phương pháp và giải thuật mật mã cho đảm bảo tính bí mật, toàn vẹn, xác thực và không chối bỏ của thông tin lưu trữ hoặc truyền đưa. Cụ thể các vấn đề sau được đề cập:

- Nếu một số khái niệm cơ bản của mã hóa, mật mã và ứng dụng của mã hóa, mật mã trong đảm bảo an toàn thông tin.
- Trình bày 6 phương pháp mã hóa là các phương pháp cơ bản thực hiện việc xáo trộn thông tin.
- Mô tả hệ mã hóa khóa đối xứng/bí mật, bao gồm mô hình, các đặc điểm, ưu nhược điểm và trình bày chi tiết các giải thuật mã hóa khóa đối xứng DES, 3-DES và AES.
- Mô tả hệ mã hóa khóa bất đối xứng/công khai, bao gồm mô hình, các đặc điểm, ưu nhược điểm và trình bày chi tiết giải thuật mã hóa khóa bất đối xứng RSA.
- Trình bày khái quát về hàm băm, các thuộc tính cơ bản, mô hình xử lý dữ liệu của hàm băm, phân loại hàm băm và 2 giải thuật băm MD5 và SHA1.

Ngoài các vấn đề nêu trên trong phạm vi của môn học Cơ sở an toàn thông tin, các vấn đề khác liên quan đến mã hóa, mật mã sẽ được trình bày trong các môn học khác theo tiến trình học tập của ngành đào tạo đại học an toàn thông tin bao gồm:

- Hạ tầng khóa công khai PKI, chứng thư số và chữ ký số.
- Các giao thức, công cụ bảo mật thông tin dựa trên mật mã, bao gồm giao thức SSL/TLS, giao thức IP Security, chuẩn bảo mật PGP.
- Vấn đề quản lý và phân phối khóa bí mật và khóa công khai.
- Các giao thức xác thực dựa trên mật mã, như EAP (Extensible Authentication Protocol), CHAP (Challenge-handshake authentication protocol), Kerberos, SSO (Single Sign On), RADIUS và DIAMETER.

4.6. Câu hỏi ôn tập

- 1) Mã hóa thông tin là gì? Nếu các khái niệm bộ mã hóa, khóa và không gian khóa. Tại sao nói “Không gian khóa càng lớn thì độ an toàn của hệ mã hóa càng cao”?
- 2) Vẽ sơ đồ và mô tả các thành phần của một hệ mã hóa.

- 3) Mô tả các phương pháp mã hóa dòng và mã hóa khối. Liệt kê các giải thuật mã hóa dòng và mã hóa khối tiêu biểu.
- 4) Nêu các ứng dụng của mã hóa. Mô tả một ứng dụng của mã hóa/mật mã thường được sử dụng trong đời sống hàng ngày?
- 5) Mô tả phương pháp mã hóa thay thế (substitution). Mô tả phương pháp mã hóa hoán vị (permutation).
- 6) Mô tả phương pháp mã hóa XOR. Tại sao nói phương pháp mã hóa XOR ít được sử dụng riêng do kém an toàn?
- 7) Vẽ sơ đồ hoạt động và nêu các đặc điểm của hệ mã hóa khóa đối xứng.
- 8) Nêu các đặc điểm và mô tả các bước xử lý khối dữ liệu của giải thuật mã hóa DES. Tại sao DES được khuyến nghị không nên sử dụng trong thời gian hiện nay?
- 9) Mô tả nguyên tắc hoạt động của giải thuật mã hóa 3-DES. Nêu các ưu nhược điểm của giải thuật mã hóa 3-DES.
- 10) Nêu các đặc điểm và mô tả các bước xử lý khối dữ liệu của giải thuật mã hóa AES. Nêu các ưu điểm và nhược điểm của AES.
- 11) Vẽ sơ đồ hoạt động và nêu các đặc điểm hệ mã hóa khóa bất đối xứng. Tại sao kích thước khóa của mã hóa khóa bất đối xứng thường rất lớn so với khóa của mã hóa khóa đối xứng khi có độ an toàn tương đương?
- 12) Nêu các đặc điểm, thủ tục sinh khóa, mã hóa và giải mã của giải thuật mã hóa RSA. Độ an toàn của RSA dựa trên yếu tố nào?
- 13) Nêu các yêu cầu đảm bảo an toàn của quá trình sinh khóa RSA.
- 14) Nêu các ưu điểm và nhược điểm của RSA. Giải thích tại sao RSA thường ít được sử dụng để mã hóa các thông điệp có kích thước lớn?
- 15) Nêu 2 thuộc tính tối thiểu mà mọi hàm băm đều có. Ngoài 2 thuộc tính trên, các hàm băm còn có những thuộc tính cơ bản nào?
- 16) Mô tả phương pháp phân loại các hàm băm.
- 17) Mô tả mô hình xử lý dữ liệu tổng quát và chi tiết của các hàm băm.
- 18) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật băm MD5. Nêu các điểm yếu của MD5.
- 19) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật băm SHA1. Nêu các điểm yếu của SHA1.
- 20) Khảo sát tài liệu và nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật băm SHA-256 và SHA-512.

CHƯƠNG 5. CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐẢM BẢO AN TOÀN THÔNG TIN

Chương 5 giới thiệu khái quát về kiểm soát truy cập, các biện pháp kiểm soát truy cập và một số công nghệ kiểm soát truy cập được sử dụng trên thực tế. Phần tiếp theo của chương trình bày về tường lửa – một trong các kỹ thuật được sử dụng rất phổ biến trong đảm bảo an toàn cho hệ thống máy tính và mạng. Phần cuối của chương giới thiệu khái quát về các hệ thống phát hiện và ngăn chặn tấn công, xâm nhập.

5.1. Kiểm soát truy cập

5.1.1. Khái quát về kiểm soát truy cập

Kiểm soát truy cập (Access control)¹ được sử dụng rất rộng rãi như là lớp bảo vệ đầu tiên trong đảm bảo an toàn cho thông tin, hệ thống và mạng trên thực tế. Một hệ thống kiểm soát cửa ra vào như minh họa trên Hình 5.1 có khả năng kiểm soát người đi vào, đi ra một căn nhà, hoặc một tòa nhà theo một quy định cho trước là một ví dụ về hệ thống kiểm soát truy cập. Định nghĩa một cách hình thức, *kiểm soát truy cập* là quá trình mà trong đó người dùng được *nhận dạng* và *trao quyền* truy cập đến các thông tin, các hệ thống và tài nguyên. Một hệ thống kiểm soát truy cập thường được cấu thành từ 3 dịch vụ: Xác thực (Authentication), Trao quyền, hoặc cấp quyền (Authorization) và Quản trị (Administration).



Hình 5.1. Một hệ thống kiểm soát truy cập cửa hổ trợ xác thực bằng vân tay

Xác thực là quá trình xác minh tính chân thực, hay tính đúng của các thông tin nhận dạng mà người dùng cung cấp. Đây là khâu đầu tiên cần thực hiện trong một hệ thống kiểm soát truy cập. Cần nhớ rằng, xác thực chỉ có khả năng khẳng định các thông tin nhận dạng mà người dùng cung cấp tồn tại trong hệ thống mà thường không thể xác minh chủ thể thực sự của thông tin đó². Chẳng hạn, khi người dùng gửi yêu cầu đăng nhập vào hệ thống gồm tên người dùng (username) và mật khẩu (password), hệ thống chỉ có thể

¹ Một số tài liệu dịch “access control” là “điều khiển truy cập”.

² Xác thực chỉ kiểm tra thông tin nhận dạng của người dùng có tồn tại trong hệ thống hay không. Việc xác thực chủ thể thực sự cần có thông tin hoặc kỹ thuật bổ sung, chẳng hạn xác thực sử dụng các đặc điểm sinh trắc có khả năng xác thực chủ thể thực sự.

kiểm tra có tồn tại một tài khoản người dùng trong cơ sở dữ liệu có tên người dùng và mật khẩu trùng khớp với thông tin trong yêu cầu đăng nhập hay không, mà không thể xác minh người gửi yêu cầu có phải là chủ sở hữu thực sự của thông tin cung cấp. Sau khi người dùng đã được xác thực, *trao quyền* xác định các tài nguyên mà người dùng được phép truy cập dựa trên chính sách quản trị tài nguyên của cơ quan, tổ chức và vai trò của người dùng trong hệ thống.

Trong khi Xác thực và Trao quyền là các dịch vụ chính của một hệ thống kiểm soát truy cập, *Quản trị* là dịch vụ cung cấp khả năng thêm, bớt và sửa đổi các thông tin nhận dạng của người dùng, cũng như quyền truy cập của người dùng trong hệ thống. Chẳng hạn, các thông tin định danh tài khoản người dùng như tên người dùng và mật khẩu có thể được thay đổi nhờ dịch vụ quản trị. Mặc dù không trực tiếp tham gia vào quá trình xác thực và trao quyền cho người dùng, quản trị là dịch vụ không thể thiếu trong một hệ thống kiểm soát truy cập.

Do kiểm soát truy cập cũng là một thành phần trong lớp các biện pháp đảm bảo an toàn thông tin, mục đích chính của kiểm soát truy cập cũng là đảm bảo tính bí mật, toàn vẹn và sẵn sàng của thông tin, hệ thống và các tài nguyên. Đây cũng chính là các yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin đã đề cập trong mục 1.2, CHƯƠNG 1.

5.1.2. Các biện pháp kiểm soát truy cập

Các biện pháp, mô hình hay cơ chế kiểm soát truy cập là các phương pháp thực hiện kiểm soát truy cập, gồm 4 loại chính:

- Kiểm soát truy cập tùy chọn – Discretionary Access Control (DAC)
- Kiểm soát truy cập bắt buộc – Mandatory Access Control (MAC)
- Kiểm soát truy cập dựa trên vai trò – Role-Based Access Control (RBAC); và
- Kiểm soát truy cập dựa trên luật – Rule-Based Access Control.

Phân tiếp theo trình bày chi tiết từng biện pháp kiểm soát truy cập kể trên.

5.1.2.1. Kiểm soát truy cập tùy chọn

Kiểm soát truy cập tùy chọn, hay tùy quyền được định nghĩa là cơ chế hạn chế truy cập đến các đối tượng dựa trên thông tin nhận dạng của các chủ thể, hoặc nhóm của các chủ thể. Các thông tin nhận dạng chủ thể được gọi là các *nhân tố* (factor) có thể gồm:

- Bạn là ai? (CMND, bằng lái xe, vân tay,...)
- Những cái bạn biết (tên truy cập, mật khẩu, số PIN...)
- Bạn có gì? (Thẻ ATM, thẻ tín dụng, ...).

Đặc điểm nổi bật của kiểm soát truy cập tùy chọn là cơ chế này cho phép người dùng có thể cấp hoặc huỷ quyền truy cập cho các người dùng khác đến các đối tượng thuộc quyền điều khiển của họ. Điều này cũng có nghĩa là chủ sở hữu của các đối tượng là người có toàn quyền điều khiển các đối tượng này. Chẳng hạn, trong một hệ thống nhiều người dùng, mỗi người dùng được cấp 1 thư mục riêng và là chủ sở hữu của thư mục này. Người dùng có quyền tạo, sửa đổi và xoá các file trong thư mục của riêng mình. Người

dùng cũng có khả năng cấp hoặc huỷ quyền truy cập vào các file của mình cho những người dùng khác.

Có nhiều kỹ thuật thực hiện cơ chế kiểm soát truy cập tuỳ chọn trên thực tế, trong đó 2 kỹ thuật được sử dụng rộng rãi nhất là *Ma trận kiểm soát truy cập* (Access Control Matrix - ACM) và *Danh sách kiểm soát truy cập* (Access Control List - ACL). Ma trận kiểm soát truy cập là một phương pháp thực hiện kiểm soát truy cập thông qua 1 ma trận 2 chiều gồm chủ thể, đối tượng và các quyền truy cập, như biểu diễn trên Hình 5.2. Các đối tượng, hay khách thể là các thực thể cần bảo vệ, được ký hiệu là O₁, O₂, O₃,.... Các đối tượng có thể là các file, các thư mục hay các tiến trình. Các chủ thể là người dùng, hoặc các tiến trình tác động lên các đối tượng, được ký hiệu là S₁, S₂, S₃,.... Quyền truy cập là hành động mà chủ thể thực hiện trên đối tượng. Các quyền bao gồm r (read – đọc), w (write - ghi), x (execute – thực hiện) và o (own – chủ sở hữu).

Đối tượng Chủ thể \	O1	O2	O3	O4
S1	rw	rwxo	r	rwxo
S2	rw	rx	rw	rwx
S3	r	rw	rwo	rw

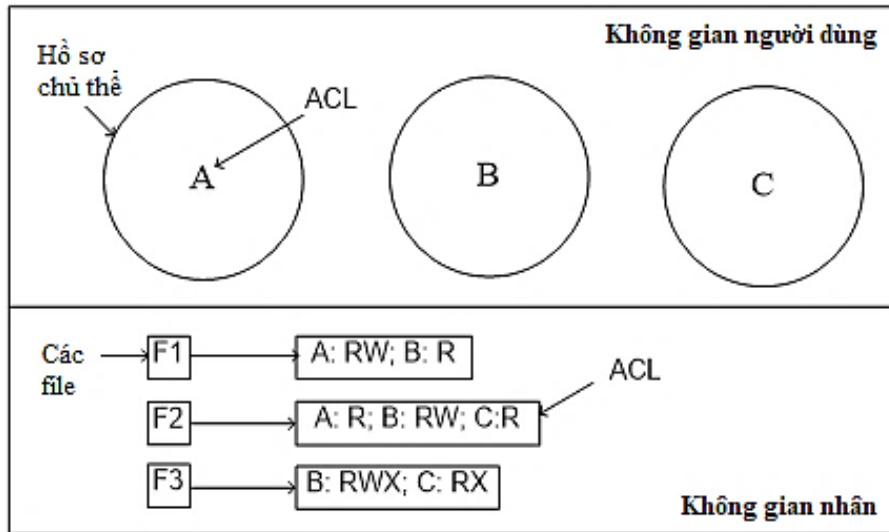
Hình 5.2. Ví dụ ma trận kiểm soát truy cập

Ưu điểm của ma trận kiểm soát truy cập là đơn giản và dễ sử dụng. Tuy nhiên, khi số lượng các đối tượng và số lượng các chủ thể lớn, kích thước của ma trận sẽ rất lớn. Hơn nữa, quyền truy cập của các chủ thể đến các đối tượng là khác nhau, trong đó một số chủ thể không có quyền truy cập vào một số đối tượng, và như vậy ô nhớ chứa quyền truy cập của chủ thể đến các đối tượng này là *rỗng*. Trong ma trận kiểm soát truy cập có thể tồn tại rất nhiều ô *rỗng* và điều này làm giảm hiệu quả sử dụng bộ nhớ của phương pháp này. Do vậy, ma trận kiểm soát truy cập ít được sử dụng hiện nay trên thực tế.

Danh sách kiểm soát truy cập là một danh sách các quyền truy cập của một chủ thể đối với một đối tượng. Một danh sách kiểm soát truy cập chỉ ra những người dùng hoặc tiến trình được truy cập vào đối tượng nào và các thao tác cụ thể, hay quyền được thực hiện trên đối tượng đó. Một bản ghi điển hình của ACL có dạng (chủ thể, thao tác). Ví dụ bản ghi (Alice, write) của 1 file có nghĩa là Alice có quyền ghi vào file đó. Khi chủ thể yêu cầu truy cập, hệ điều hành sẽ kiểm tra ACL xem yêu cầu đó có được phép hay không. ACL có thể được áp dụng cho một hoặc 1 nhóm đối tượng.

Hình 5.3 biểu diễn mô hình danh sách kiểm soát truy cập trong không gian người dùng và không gian nhân được tổ chức bởi hệ điều hành. Mỗi file (F1, F2, F3,...) có một danh sách kiểm soát truy cập của riêng mình lưu trong hồ sơ của file. Quyền truy cập vào file được tổ chức thành một chuỗi gồm nhiều cặp (chủ thể, thao tác), với A, B, C là ký hiệu biểu diễn chủ thể và các thao tác hay quyền gồm R (Read - đọc), W (Write - ghi), và X (eXecute - thực hiện). Chẳng hạn, trong danh sách kiểm soát truy cập file F1 là (A: RW; B: R) thì chủ thể A được quyền đọc (R) và ghi (W) đối với F1, còn chủ thể B

chỉ có quyền đọc (R). Tương tự, danh sách kiểm soát truy cập (A: R; B: RW; C: R) của file F2 có nghĩa là A chỉ có quyền đọc (R), B được quyền đọc (R) và ghi (W), còn chủ thẻ C chỉ cũng có quyền đọc (R) đối với F2.



Hình 5.3. Mô hình danh sách kiểm soát truy cập

5.1.2.2. Kiểm soát truy cập bắt buộc

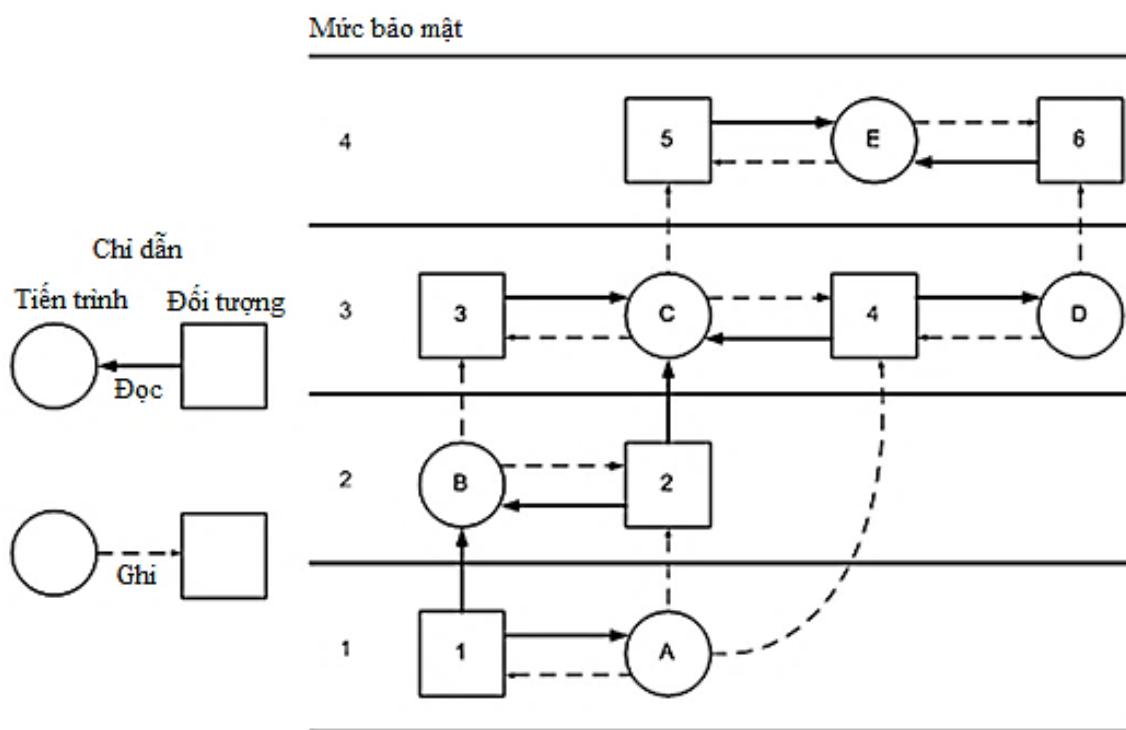
Kiểm soát truy cập bắt buộc được định nghĩa là các cơ chế hạn chế truy cập đến các đối tượng dựa trên hai yếu tố chính: (1) Tính nhạy cảm của thông tin chứa trong các đối tượng và (2) Sự trao quyền chính thức cho các chủ thẻ truy cập các thông tin nhạy cảm này. Các thông tin nhạy cảm thường được gán nhãn với các mức nhạy cảm. Có nhiều phương pháp phân chia các mức nhạy cảm của các thông tin tùy thuộc vào chính sách an toàn thông tin của các cơ quan, tổ chức. Các mức nhạy cảm thường được sử dụng gồm:

- Tối mật (Top Secret - T): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến những thiệt hại trầm trọng đối với an ninh quốc gia.
- Tuyệt mật (Secret - S): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến một loạt thiệt hại đối với an ninh quốc gia.
- Mật (Confidential - C): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến thiệt hại đối với an ninh quốc gia.
- Không phân loại (Unclassified - U): Những thông tin không gây thiệt hại đối với an ninh quốc gia nếu bị tiết lộ.

Đặc điểm nổi bật của cơ chế kiểm soát truy cập bắt buộc là nó không cho phép người tạo ra các đối tượng (thông tin, hoặc tài nguyên) có toàn quyền truy cập các đối tượng này. Quyền truy cập đến các đối tượng do người quản trị hệ thống định ra trước trên cơ sở chính sách an toàn thông tin của tổ chức đó. Đây cũng là điểm khác biệt cơ bản với cơ chế kiểm soát truy cập tùy chọn, trong đó người tạo ra các đối tượng là chủ sở hữu và có toàn quyền đối với các đối tượng họ tạo ra. Ví dụ, với cơ chế kiểm soát truy cập bắt buộc, một tài liệu được tạo ra và được đóng dấu “Mật” thì chỉ những người có trách nhiệm trong cơ quan, tổ chức mới được quyền xem và phổ biến cho người khác, còn bản thân tác giả của tài liệu không được quyền phổ biến đến người khác. Cơ chế kiểm soát truy

cập bắt buộc thường được sử dụng phổ biến trong các cơ quan an ninh, quân đội và ngân hàng, nơi thường có nhiều dữ liệu nhạy cảm.

Có nhiều kỹ thuật thực hiện cơ chế kiểm soát truy cập bắt buộc, trong đó mô hình kiểm soát truy cập Bell-LaPadula¹ là một trong các kỹ thuật được sử dụng rộng rãi nhất. Mô hình Bell-LaPadula, như biểu diễn trên Hình 5.4 là mô hình bảo mật đa cấp thường được sử dụng trong quân sự, nhưng nó cũng có thể áp dụng cho các lĩnh vực khác. Theo mô hình này trong quân sự, các tài liệu được gán một mức độ bảo mật, chẳng hạn như không phân loại, mật, tuyệt mật và tối mật. Người dùng cũng được xác định các cấp độ bảo mật, tùy thuộc vào những tài liệu mà họ được phép xem. Chẳng hạn, một vị tướng quân đội có thể được phép xem tất cả các tài liệu, trong khi một trung úy có thể bị hạn chế chỉ được xem các tài liệu mật và thấp hơn. Đồng thời, một tiến trình được thực thi nhân danh một người dùng cũng có mức độ bảo mật của người dùng đó.



Hình 5.4. Mô hình kiểm soát truy cập Bell-LaPadula

Mô hình Bell-LaPadula sử dụng nguyên tắc “đọc xuống” (read down) và nguyên tắc “ghi lên” (write up) trong việc cấp quyền truy cập cho người dùng đến các đối tượng để đảm bảo thông tin, dữ liệu không bị rò rỉ. Với nguyên tắc đọc xuống, một người dùng ở mức độ bảo mật k chỉ có thể đọc các đối tượng ở cùng mức bảo mật hoặc thấp hơn. Ví dụ, một vị tướng có thể đọc các tài liệu của một trung úy, nhưng trung úy đó không thể đọc các tài liệu của vị tướng đó do trung úy có mức độ bảo mật thấp hơn vị tướng. Ngược lại, nguyên tắc ghi lên quy định, một người dùng ở mức độ bảo mật k chỉ có thể ghi các đối tượng ở cùng mức bảo mật hoặc cao hơn. Ví dụ, một trung úy có thể nối thêm một tin nhắn vào hộp thư của chung của đơn vị về tất cả mọi thứ ông ấy biết, nhưng một vị tướng không thể ghi thêm một tin nhắn vào hộp thư của trung úy với tất cả mọi thứ ông ấy biết.

¹ Đọc thêm tại <https://www.sciencedirect.com/topics/computer-science/lapadula-model>

vì vị tướng có thể đã nhìn thấy các tài liệu có mức bảo mật cao mà không thể được tiết lộ cho một trung úy.

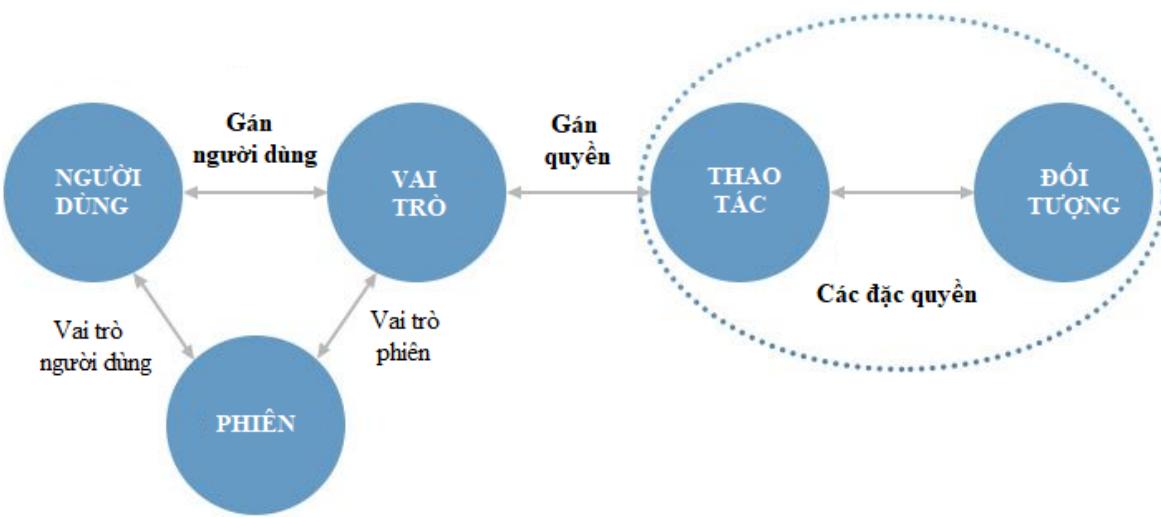
Hình 5.4 minh họa việc thực hiện các nguyên tắc đọc xuống và ghi lên trong mô hình Bell-LaPadula. Trong đó, người dùng, hoặc tiến trình thực thi bởi người dùng được ký hiệu là A, B, C, D, E và được biểu diễn bởi các hình tròn. Các đối tượng được đánh số 1, 2, 3, 4, 5, 6 và được biểu diễn bởi các hình vuông. Mũi tên liền nét biểu diễn quyền đọc, mũi tên đứt nét biểu diễn quyền ghi. Các mức bảo mật cho cả tiến trình và đối tượng được đánh số 1, 2, 3, 4, với 1 tương đương mức bảo mật thấp nhất và 4 tương đương mức bảo mật cao nhất. Theo mô hình này, tiến trình B có mức bảo mật là 2 chỉ được phép đọc các đối tượng số 1 và 2 – là các đối tượng có cùng mức bảo mật và thấp hơn mức bảo mật của B. B không được phép đọc đối tượng số 3, hoặc số 4 do các đối tượng này có mức bảo mật cao hơn. Ngược lại, B có quyền ghi các đối tượng số 2 và 3 – là các đối tượng có cùng mức bảo mật và cao hơn. Tuy nhiên, B không được phép ghi đối tượng số 1 do đối tượng này có mức bảo mật thấp hơn. Tương tự, tiến trình A chỉ có thể đọc đối tượng số 1 (cùng mức bảo mật) và ghi các đối tượng số 1 và 4 (cùng mức bảo mật và cao hơn).

5.1.2.3. Kiểm soát truy cập dựa trên vai trò

Kiểm soát truy cập dựa trên vai trò cho phép người dùng truy cập vào hệ thống và thông tin dựa trên vai trò (role) của họ trong cơ quan, tổ chức đó. Kiểm soát truy cập dựa trên vai trò có thể được áp dụng cho một nhóm người dùng hoặc từng người dùng riêng lẻ. Quyền truy cập vào các đối tượng trong hệ thống được tập hợp thành các nhóm “vai trò” với các mức quyền truy cập khác nhau. Các vai trò được tổ chức thành một cây theo mô hình phân cấp tự nhiên của các cơ quan, tổ chức. Ví dụ như, hệ thống thông tin trong một trường học chia người dùng thành các nhóm và gán sẵn quyền truy cập vào các phần trong hệ thống như sau:

- Nhóm Quản lý được quyền truy cập vào tất cả các thông tin trong hệ thống;
- Nhóm Giáo viên được truy cập vào cơ sở dữ liệu các môn học, bài báo khoa học, cập nhật điểm các lớp do mỗi giáo viên phụ trách;
- Nhóm Sinh viên chỉ được quyền xem nội dung các môn học, tải tài liệu học tập và xem điểm của mình.

Việc liên kết giữa người dùng và nhóm vai trò có thể được tạo lập và huỷ bỏ dễ dàng và được thực hiện theo nguyên tắc: Người dùng được cấp “thẻ thành viên” của các nhóm “vai trò” trên cơ sở năng lực và vai trò, cũng như trách nhiệm của họ trong một tổ chức. Trong nhóm “vai trò”, người dùng được cấp vừa đủ quyền để thực hiện các thao tác cần thiết cho công việc được giao. Hình 5.5 minh họa một mô hình RBAC, trong đó quyền truy cập vào các đối tượng, hay các thao tác trên đối tượng được tập hợp thành các nhóm vai trò và việc cấp quyền truy cập các đối tượng cho người dùng được thực hiện thông qua thao tác gán hay kết nạp người dùng vào nhóm vai trò. Việc cấp quyền truy cập các đối tượng cho người dùng có thể có hiệu lực trong dài hạn, hoặc cũng có thể có hiệu lực trong ngắn hạn, như theo phiên làm việc (Session).



Hình 5.5. Một mô hình kiểm soát truy cập RBAC

5.1.2.4. Kiểm soát truy cập dựa trên luật

Kiểm soát truy cập dựa trên luật là cơ chế cho phép người dùng truy cập vào hệ thống và thông tin dựa trên các luật đã được định nghĩa trước. Các luật có thể được thiết lập để hệ thống cho phép truy cập đến các tài nguyên của mình cho người dùng thuộc một tên miền, một mạng hay một dải địa chỉ IP. Tường lửa, hoặc proxy là ví dụ điển hình về việc thực hiện cơ chế kiểm soát truy cập dựa trên luật. Các luật trong tường lửa thực hiện kiểm soát truy cập sử dụng các thông tin trích xuất từ các gói tin chuyển đến hoặc chuyển đi. Các thông tin thường được sử dụng trong các luật của tường lửa có thể bao gồm:

- Giao thức truyền thông sử dụng;
- Địa chỉ IP nguồn, IP đích của gói tin;
- Cổng nguồn, cổng đích;
- Địa chỉ IP hoặc các tên miền để lọc, hoặc chặn các website bị cấm;
- Tập các từ khoá để lọc các nội dung bị cấm.

Hình 5.6 minh họa một số luật của tường lửa lọc gói tin. Theo đó, các thông tin của gói tin được sử dụng để lọc bao gồm: giao thức (Protocol), địa chỉ IP nguồn (Source IP), địa chỉ IP đích (Destination IP) và cổng đích (Dest.Port). Khi luật thỏa mãn, một hành động (Action) được thực thi. Các hành động hỗ trợ bao gồm chấp nhận (Accept) và từ chối (Deny).

No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	20.1.1.1	80	Accept
2	TCP	10.1.1.2	20.1.1.1	80	Deny
3	TCP	10.1.1.0/24	20.1.1.1	80	Deny
4	TCP	10.1.1.3	20.1.1.1	80	Accept
5	TCP	10.2.2.0/24	20.2.2.5	80	Deny
6	TCP	10.2.2.5	20.2.2.0/24	80	Deny
7	TCP	10.3.3.0/24	20.3.3.9	80	Accept
8	TCP	10.3.3.9	20.3.3.0/24	80	Deny
9	IP	0.0.0.0/0	0.0.0.0/0	0-65535	Deny

Hình 5.6. Một số luật của tường lửa lọc gói tin

5.1.3. Một số công nghệ kiểm soát truy cập

Trên cơ sở các biện pháp, cơ chế kiểm soát truy cập đã trình bày, mục này mô tả một số công nghệ kiểm soát truy cập đã và đang được ứng dụng rộng rãi trên thực tế, trong đó nhấn mạnh đến các thông tin, hoặc các phương tiện mang thông tin xác thực người dùng được sử dụng. Các công nghệ kiểm soát truy cập được đề cập bao gồm:

- Kiểm soát truy cập dựa trên mật khẩu (password)
- Kiểm soát truy cập dựa trên các khoá mã (encrypted key)
- Kiểm soát truy cập dựa trên thẻ thông minh (smartcard)
- Kiểm soát truy cập dựa trên thẻ bài (token)
- Kiểm soát truy cập dựa trên các đặc điểm sinh trắc (biometric).

5.1.3.1. Kiểm soát truy cập dựa trên mật khẩu

Kiểm soát truy cập dựa trên mật khẩu là công nghệ kiểm soát truy cập được sử dụng từ lâu và vẫn đang được sử dụng rộng rãi do tính dễ dùng và chi phí thấp. Thông thường, mỗi người dùng được cấp 1 tài khoản để truy cập vào hệ thống. Mỗi tài khoản người dùng thường gồm 2 thành tố: tên người dùng và mật khẩu, trong đó mật khẩu cần được giữ bí mật. Trong một số hệ thống, tên người dùng có thể được thay thế bằng địa chỉ email, số điện thoại,... Mật khẩu có thể lưu trong cơ sở dữ liệu của hệ thống ở dạng rõ hoặc dạng mã hóa, thường dưới dạng giá trị băm.

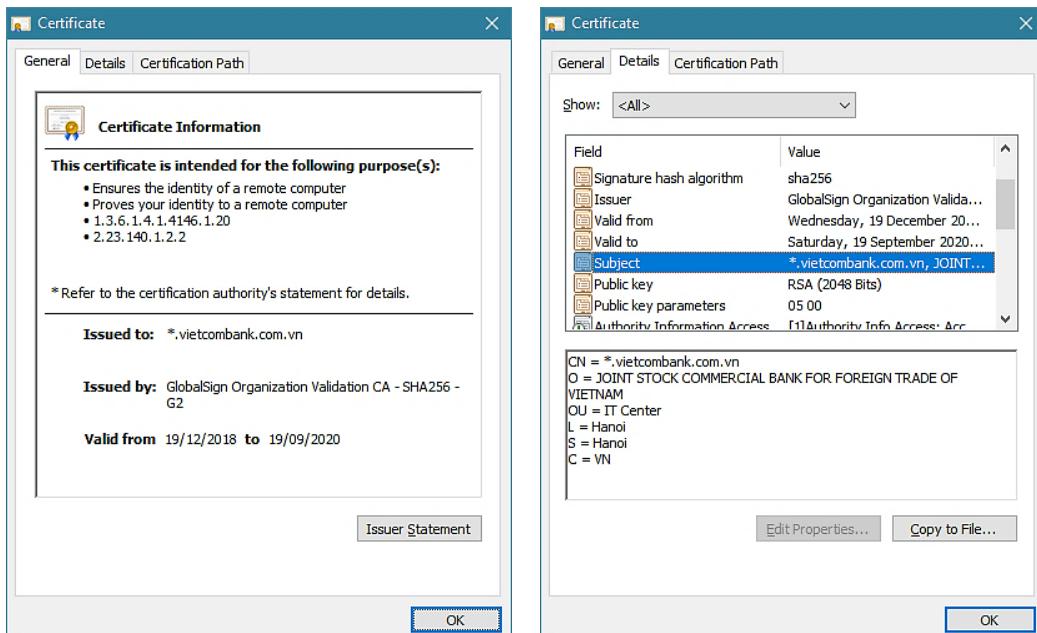
Độ an toàn của kiểm soát truy cập sử dụng mật khẩu dựa trên 2 yếu tố: (1) độ khó đoán của mật khẩu và (2) tuổi thọ của mật khẩu. Độ khó đoán của mật khẩu lại phụ thuộc vào số bộ ký tự sử dụng trong mật khẩu và độ dài của mật khẩu. Nhìn chung, mật khẩu càng an toàn nếu càng nhiều bộ ký tự được sử dụng và có độ dài đủ lớn. Với các tài khoản người dùng của ứng dụng thông thường, khuyến nghị nên sử dụng mật khẩu với độ dài từ 8 ký tự trở lên và gồm các ký tự thuộc cả 4 bộ ký tự phổ biến, gồm chữ cái in thường, chữ cái in hoa, chữ số và ký tự đặc biệt. Theo tuổi thọ, mật khẩu gồm 3 loại: không hết hạn, có thời hạn sử dụng và sử dụng 1 lần. Để đảm bảo an toàn, khuyến nghị định kỳ đổi mật khẩu. Khoảng thời gian sử dụng của mật khẩu có thể được thiết lập từ 3 tháng đến 6 tháng phụ thuộc chính sách an toàn thông tin của cơ quan, tổ chức.

Nhìn chung, kiểm soát truy cập dựa trên mật khẩu có độ an toàn thấp do người dùng có xu hướng chọn các từ đơn giản, dễ nhớ làm mật khẩu. Ngoài ra, mật khẩu có thể bị nghe lén khi được truyền trên môi trường mạng mở như Internet. Hơn nữa, việc nhiều ứng dụng cung cấp tính năng “nhớ tài khoản/mật khẩu” và tự động đăng nhập để tăng sự tiện lợi cho người dùng cũng tạo ra các nguy cơ tài khoản/mật khẩu bị rò rỉ, hoặc bị đánh cắp. Do vậy, để đảm bảo an toàn, cần có chính sách quản lý tài khoản và sử dụng mật khẩu phù hợp với từng hệ thống cụ thể.

5.1.3.2. Kiểm soát truy cập dựa trên các khoá mã

Kiểm soát truy cập dựa trên các khoá mã cho phép đảm bảo tính bí mật của thông tin, đồng thời cho phép kiểm tra thông tin nhận dạng của các bên tham gia giao dịch. Một trong các ứng dụng rộng rãi nhất của khóa mã là chứng thư số khóa công khai (Public

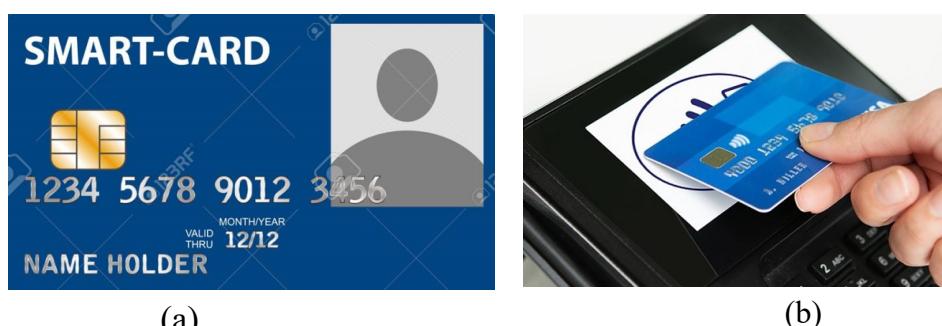
Key Digital Certificate)¹. Một chứng thư số khóa công khai gồm nhiều mục tin, nhưng có 3 mục thông tin quan trọng nhất: (1) Thông tin nhận dạng của chủ thẻ (Subject), (2) Khoá công khai của chủ thẻ (Public key) và (3) Chữ ký số của nhà cung cấp chứng thư số (Certificate Authority – CA). Hình 5.7 là giao diện của một chứng thư số khóa công khai cấp cho tên miền *.vietcombank.com.vn. Chứng thư số khóa công khai có thể được sử dụng để xác thực các thực thể tham gia phiên truyền thông, đồng thời hỗ trợ trao đổi khóa cho các khâu mã hóa – giải mã thông điệp nhằm đảm bảo tính bí mật thông điệp truyền, cũng như sử dụng trong quá trình tạo và kiểm tra chữ ký số đảm bảo tính toàn vẹn của thông điệp truyền.



Hình 5.7. Giao diện kiểm tra thông tin của một chứng chỉ số khóa công khai

5.1.3.3. Kiểm soát truy cập dựa trên thẻ thông minh

Thẻ thông minh là các thẻ nhựa gắn các chip điện tử có khả năng tính toán và lưu trữ bảo mật thông tin. Kiểm soát truy cập dựa trên thẻ thông minh là phương pháp có độ an toàn cao do thẻ thông minh sử dụng hai nhân tố để xác thực và nhận dạng chủ thẻ: (1) cái bạn có là thẻ thông minh và (2) cái bạn biết là số PIN, hay mã xác thực thẻ. Hình 5.8 là hình ảnh thẻ thông minh tiếp xúc (a) và thẻ thông minh không tiếp xúc (b).



Hình 5.8. Thẻ thông minh tiếp xúc (a) và thẻ không tiếp xúc (b)

¹ Đọc thêm về chứng thư số khóa công khai tại <https://tools.ietf.org/html/rfc5280>.

5.1.3.4. Kiểm soát truy cập dựa trên thẻ bài

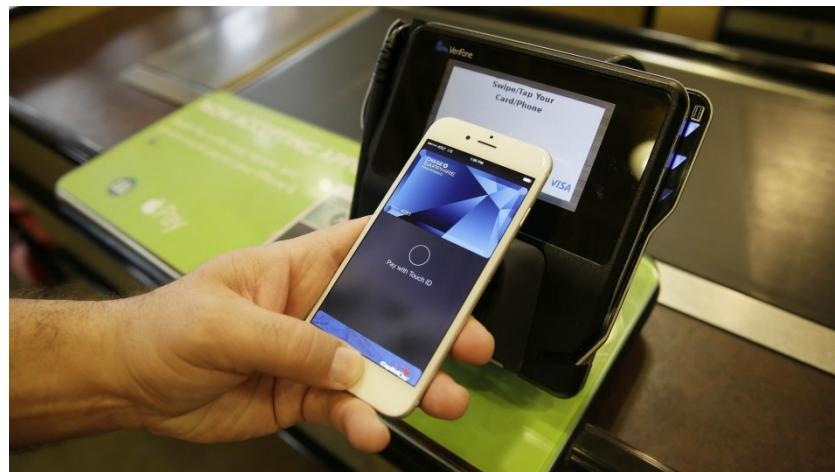
Các thẻ bài thường là các thiết bị cầm tay được thiết kế nhỏ gọn để có thể dễ dàng mang theo. Khác với thẻ thông minh, thẻ bài được tích hợp pin cung cấp nguồn nuôi. Thẻ bài có thể được sử dụng để lưu mật khẩu, các thông tin cá nhân và các thông tin quan trọng khác. Tương tự thẻ thông minh, thẻ bài thường được trang bị cơ chế xác thực 2 nhân tố, gồm thẻ bài và mật khẩu, hoặc PIN. Ưu điểm của thẻ bài là có cơ chế xác thực mạnh hơn thẻ thông minh do thẻ bài có CPU với năng lực xử lý cao hơn và bộ nhớ lưu trữ lớn hơn. Hình 5.9, Hình 5.10 và Hình 5.11 minh họa một số thẻ bài của hãng RSA Security, ví điện tử của công thanh toán trực tuyến Paypal và hệ thống ApplePay tích hợp vào điện thoại di động.



Hình 5.9. Một số thẻ bài (Token) của hãng RSA Security



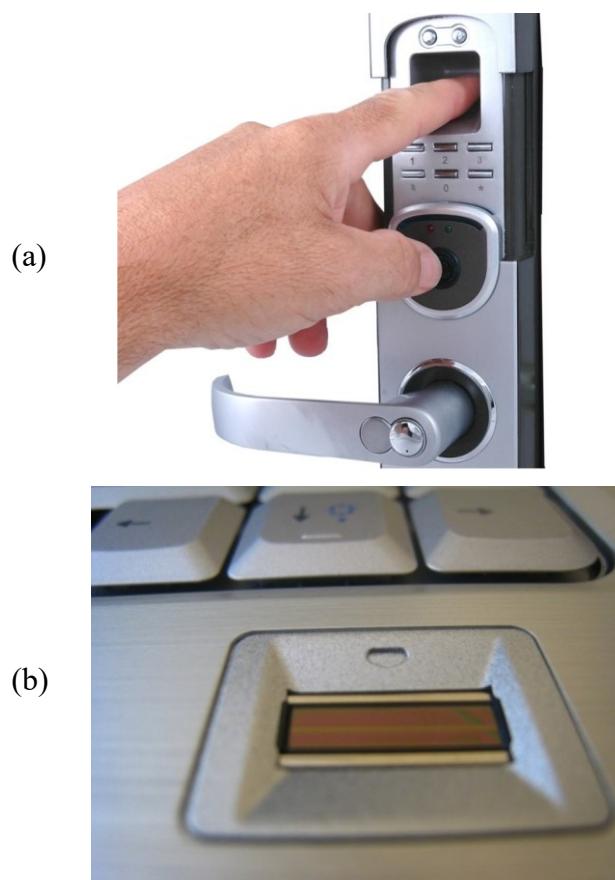
Hình 5.10. Ví điện tử (một dạng thẻ bài) của công thanh toán trực tuyến Paypal



Hình 5.11. Hệ thống ApplePay tích hợp vào điện thoại di động

5.1.3.5. Kiểm soát truy cập dựa trên các đặc điểm sinh trắc

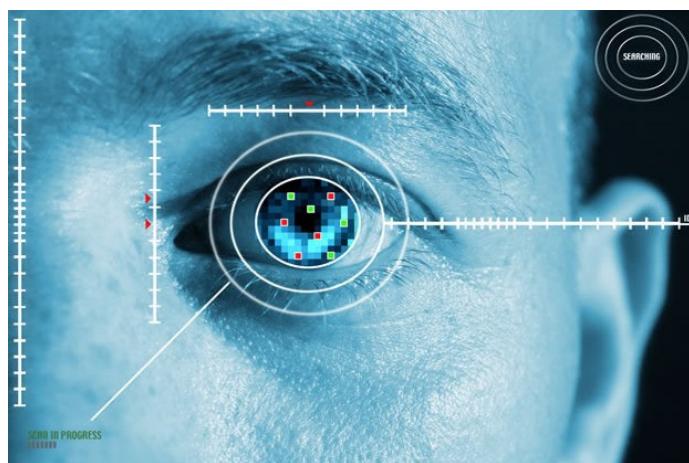
Các đặc điểm sinh trắc là các đặc điểm riêng có để nhận dạng người dùng, bao gồm dấu vân tay, tròng mắt, khuôn mặt, tiếng nói, chữ ký tay,... Kiểm soát truy cập sử dụng các đặc điểm sinh trắc để nhận dạng chủ thẻ là phương pháp có khả năng cung cấp độ an toàn cao nhất và cho phép xác thực chủ thẻ do các đặc điểm sinh trắc luôn đi cùng chủ thẻ và khó bị đánh cắp hoặc làm giả. Hiện nay, kiểm soát truy cập dựa trên các đặc điểm sinh trắc phát triển rất mạnh với nhiều ứng dụng phong phú do những tiến bộ vượt bậc trong công nghệ xử lý và nhận dạng hình ảnh. Hình 5.12 minh họa (a) Khóa vân tay, (b) Khe xác thực vân tay trên máy tính xách tay và (c) Xác thực vân tay trên điện thoại thông minh Samsung. Hình 5.13 minh họa việc quét võng mạc để nhận dạng tròng mắt.



(c)



Hình 5.12. Xác thực dựa trên đặc điểm sinh trắc: (a) Khóa vân tay, (b) Khe xác thực vân tay trên máy tính xách tay và (c) Xác thực vân tay trên điện thoại Samsung



Hình 5.13. Quét vân mạc nhận dạng trong mắt

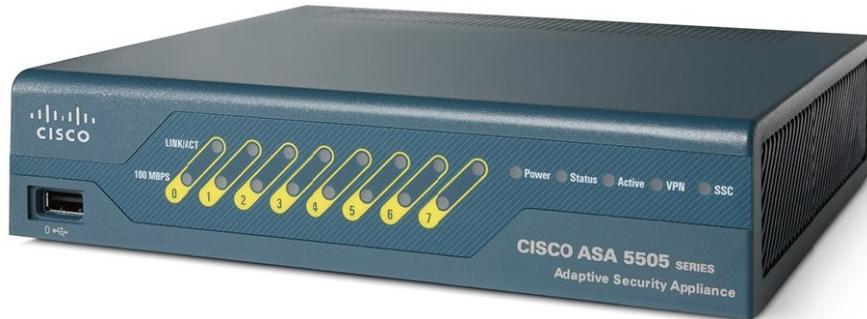
Nhược điểm chính của kiểm soát truy cập sử dụng các đặc điểm sinh trắc là phương pháp này yêu cầu chi phí đầu tư lớn cho các thiết bị quét, đọc và xử lý các đặc điểm sinh trắc. Ngoài ra, phương pháp này tương đối chậm do thường liên quan đến xử lý ảnh – công việc đòi hỏi khối lượng tính toán lớn. Một vấn đề khác cần quan tâm là tỷ lệ nhận dạng sai còn tương đối cao do có nhiều yếu tố nhiễu ảnh hưởng. Ngoài ra, cũng có một số lo ngại về tính riêng tư của người dùng khi một lượng lớn dữ liệu sinh trắc được thu thập có khả năng bị rò rỉ và lạm dụng.

5.2. Tường lửa

5.2.1. Khái quát

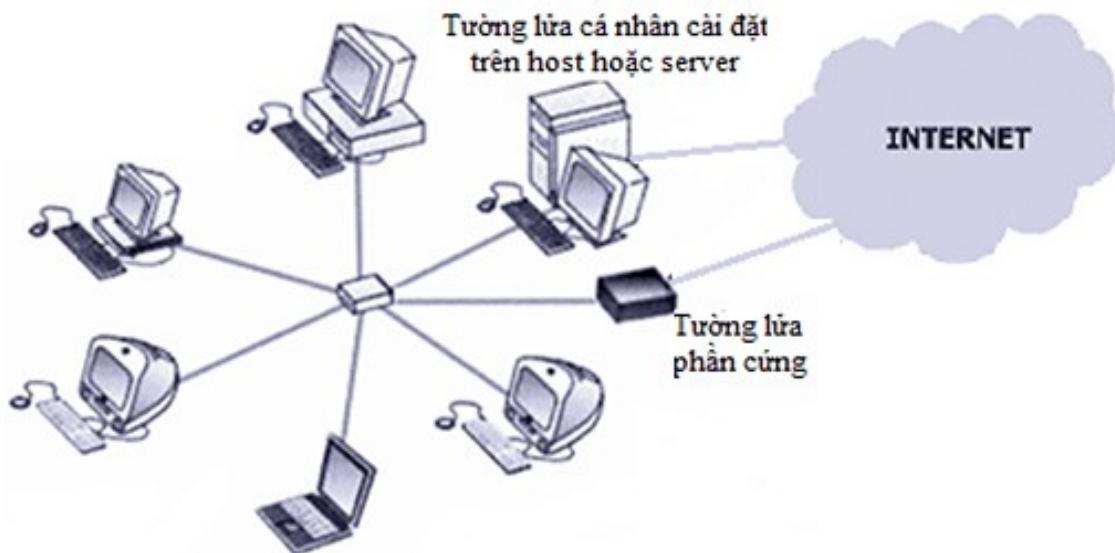
Tường lửa (Firewall) là một trong các kỹ thuật được sử dụng phổ biến nhất để bảo vệ hệ thống và mạng cục bộ tránh các đe dọa từ bên ngoài. Tường lửa có thể là một thiết bị phần cứng chuyên dụng, hoặc mô đun phần mềm chạy trên máy tính. Tường lửa phần cứng thường có tốc độ xử lý cao thích hợp với các hệ thống mạng văn phòng, hoặc mạng các máy chủ dịch vụ có băng thông lớn. Hình 5.14 là hình ảnh một tường lửa phần cứng chuyên dụng của hãng Cisco Systems. Ngược lại, tường lửa phần mềm thường có khả năng xử lý hạn chế hơn, thích hợp với các văn phòng nhỏ, mạng gia đình, hoặc máy tính cá nhân. Tường lửa phần mềm tích hợp trong các hệ điều hành Microsoft Windows (trên

Windows 10 là Windows Defender Firewall) là một trong các tường lửa phần mềm được sử dụng rộng rãi trên các máy tính cá nhân chạy hệ điều hành này.



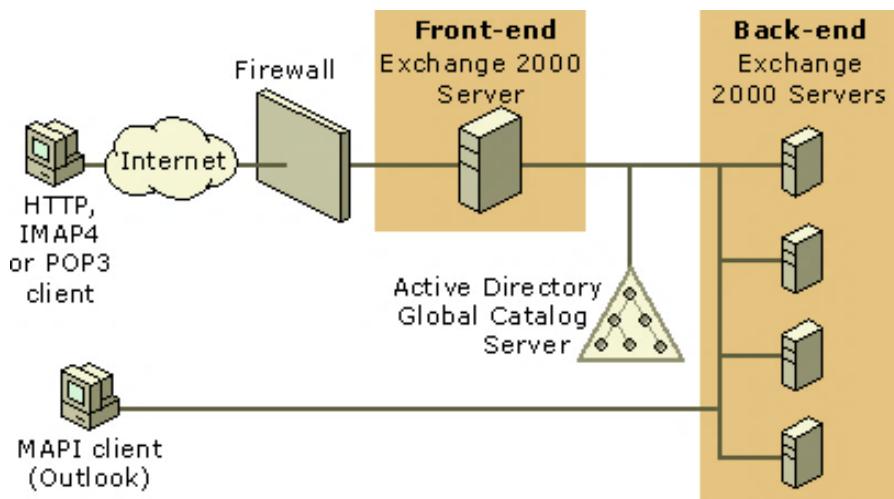
Hình 5.14. Một tường lửa phần cứng chuyên dụng của hãng Cisco Systems

Để đảm bảo hiệu quả bảo vệ, tường lửa phải miễn dịch với các loại tấn công, xâm nhập và thường được đặt ở vị trí cổng vào của mạng nội bộ cơ quan hoặc tổ chức, như minh họa trên Hình 5.15. Nhờ vị trí đặt ở cổng mạng, tất cả các gói tin từ trong ra và từ ngoài vào đều phải đi qua tường lửa và chỉ các gói tin hợp pháp được phép đi qua tường lửa. Việc xác định một gói tin là hợp pháp hay không được thực hiện bởi thao tác lọc dựa trên các luật. Tập các luật sử dụng cho việc lọc các gói tin được xây dựng dựa trên chính sách an ninh của cơ quan, tổ chức.

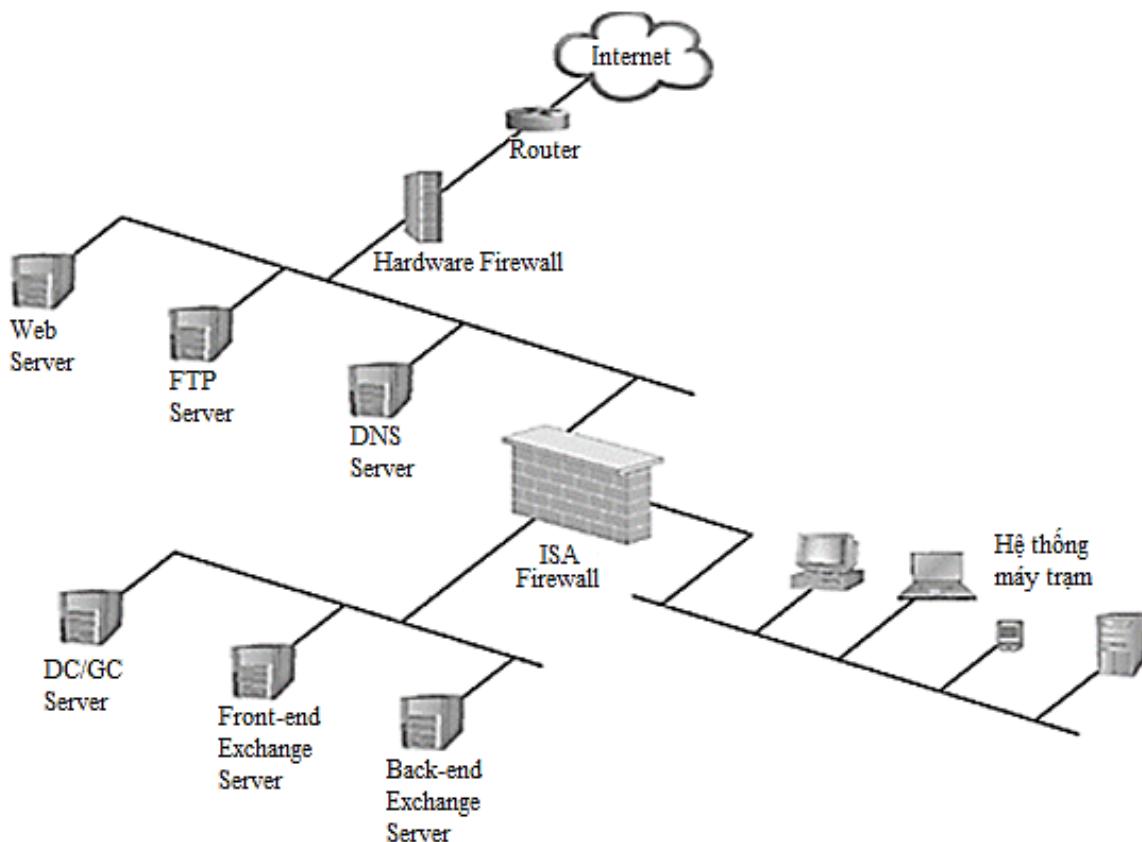


Hình 5.15. Các tường lửa bảo vệ mạng gia đình hoặc văn phòng nhỏ

Hình 5.16 biểu diễn sơ đồ mạng trong đó tường lửa được sử dụng để bảo vệ các máy chủ dịch vụ email Microsoft Exchange. Tất cả các kết nối đến hệ thống máy chủ email (Front-end) đều phải đi qua tường lửa. Hình 5.17 biểu diễn sơ đồ mạng sử dụng 2 tường lửa để bảo vệ, trong đó một tường lửa phần cứng (Hardware Firewall) được sử dụng tại cổng kết nối Internet để bảo vệ các máy chủ dịch vụ công cộng (dịch vụ web, dịch vụ FTP và dịch vụ DNS) và một tường lửa phần mềm (ISA Firewall) được sử dụng để bảo vệ các máy chủ nội bộ và các máy trạm trong mạng LAN của cơ quan, tổ chức. Hai tường lửa có chính sách kiểm soát truy cập và tập luật khác nhau phù hợp với các đối tượng được bảo vệ khác nhau.



Hình 5.16. Tường lửa bảo vệ các máy chủ dịch vụ

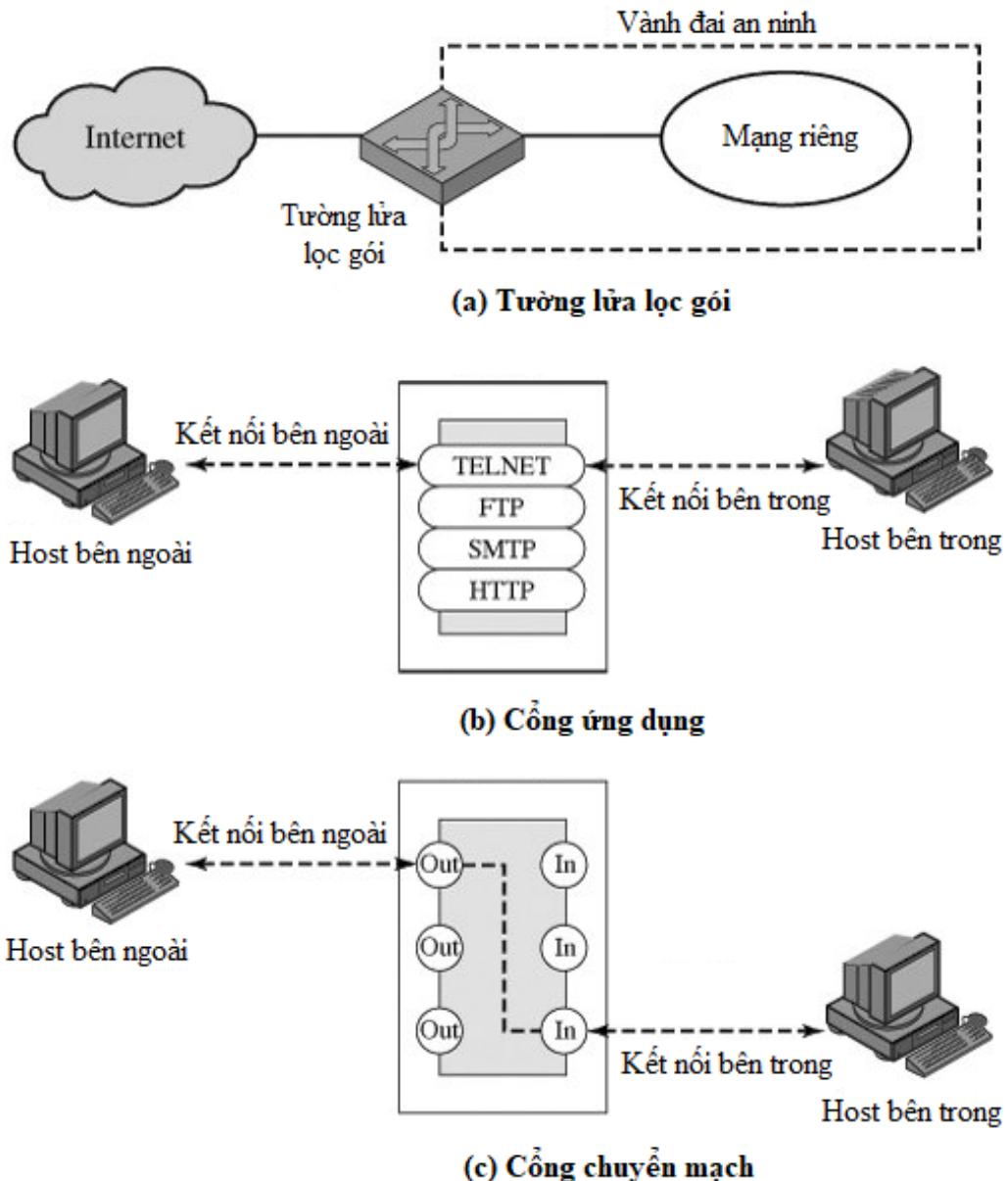


Hình 5.17. Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm

5.2.2. Các loại tường lửa

Có nhiều phương pháp phân loại các tường lửa, chẳng hạn như dựa trên vị trí các lớp giao thức mạng và khả năng lưu trạng thái của các kết nối mạng. Dựa trên vị trí các lớp giao thức mạng, có thể chia tường lửa thành 3 loại: tường lửa lọc gói (Packet-filtering firewall), cổng ứng dụng (Application-level gateway) và cổng chuyển mạch (Circuit-level gateway). Tường lửa lọc gói thường thực hiện việc lọc các gói tin IP, theo đó một tập, hoặc một nhóm các luật được áp dụng cho mỗi gói tin gửi đi, hoặc chuyển đến để quyết định chuyển tiếp các gói tin hợp pháp, hay loại bỏ gói tin bất hợp pháp. Cổng ứng dụng, còn gọi là máy chủ proxy thường được sử dụng để phát lại lưu lượng mạng ở mức

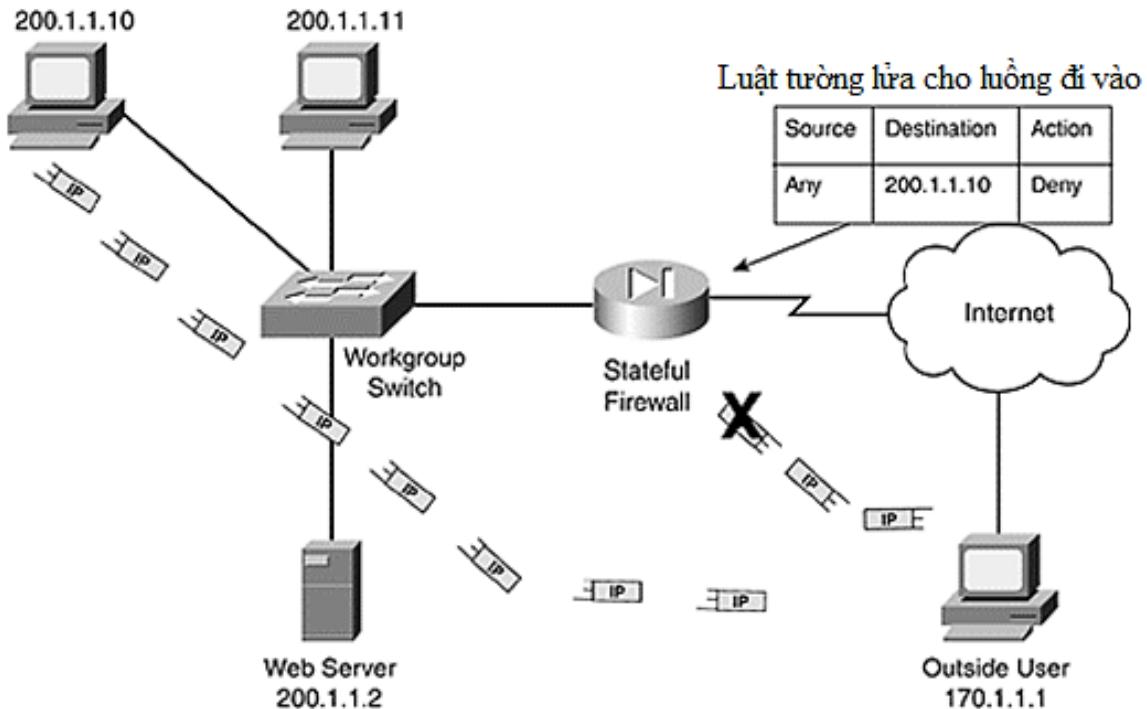
ứng dụng. Cổng ứng dụng thực hiện việc lọc các yêu cầu (request), hoặc hồi đáp (response) ở các giao thức ứng dụng phổ biến như HTTP, SMTP, FTP,... Cổng chuyển mạch hoạt động ở mức thấp nhất, với cơ chế tương tự như các bộ chuyển mạch (switch). Hình 5.18 minh họa các mô hình tường lửa, gồm (a) Tường lửa lọc gói, (b) Cổng ứng dụng và (c) Cổng chuyển mạch.



Hình 5.18. Các mô hình tường lửa: (a) Tường lửa lọc gói, (b) Cổng ứng dụng và (c) Cổng chuyển mạch

Dựa trên khả năng lưu trạng thái của các kết nối mạng, tường lửa được chia thành 2 loại: tường lửa có trạng thái (Stateful firewall) và tường lửa không trạng thái (Stateless firewall). Tường lửa có trạng thái có khả năng lưu trạng thái của các kết nối mạng đi qua và được lập trình để phân biệt các gói tin thuộc về các kết nối mạng khác nhau. Theo đó, chỉ những gói tin thuộc một kết nối mạng đang hoạt động mới được đi qua tường lửa, còn các gói tin khác không thuộc kết nối đang hoạt động sẽ bị chặn lại. Hình 5.19 minh họa một tường lửa có trạng thái chặn các gói tin IP gửi từ người dùng ngoài (Outside User)

đến địa chỉ IP 200.1.1.10 do chúng không thuộc kết nối đang hoạt động. Ngược lại, tường lửa không trạng thái thực hiện việc lọc các gói tin riêng rẽ mà không quan tâm mỗi gói tin thuộc về kết nối mạng nào. Tường lửa dạng này dễ bị tấn công bởi kỹ thuật giả mạo địa chỉ, giả mạo nội dung gói tin do tường lửa không có khả năng nhớ các gói tin đi trước thuộc cùng một kết nối mạng.



Hình 5.19. Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động

5.2.3. Các kỹ thuật kiểm soát truy cập

Hầu hết các tường lửa hỗ trợ nhiều kỹ thuật kiểm soát truy cập, gồm kiểm soát dịch vụ, kiểm soát hướng, kiểm soát người dùng và kiểm soát hành vi. Chi tiết về các kỹ thuật này như sau:

- Kiểm soát dịch vụ xác định dịch vụ nào có thể được truy cập và thường được thực hiện thông qua việc mở hoặc đóng một cổng dịch vụ nào đó. Chẳng hạn, để cung cấp dịch vụ web và cấm tất cả các dịch vụ khác, tường lửa mở cổng HTTP 80 và HTTPS 443, còn đóng tất cả các cổng dịch vụ khác.
- Kiểm soát hướng điều khiển hướng được phép đi của các gói tin của mỗi dịch vụ. Hướng có thể gồm luồng từ mạng nội bộ đi ra (outgoing) và luồng từ ngoài đi vào mạng nội bộ (incoming).
- Kiểm soát người dùng xác định người dùng nào được quyền truy cập và thường áp dụng cho người dùng mạng nội bộ.
- Kiểm soát hành vi thực hiện kiểm soát việc sử dụng các dịch vụ cụ thể. Ví dụ như, tường lửa có thể được cấu hình để lọc loại bỏ thư rác, hoặc hạn chế truy cập đến một bộ phận thông tin của máy chủ web.

5.2.4. Các hạn chế của tường lửa

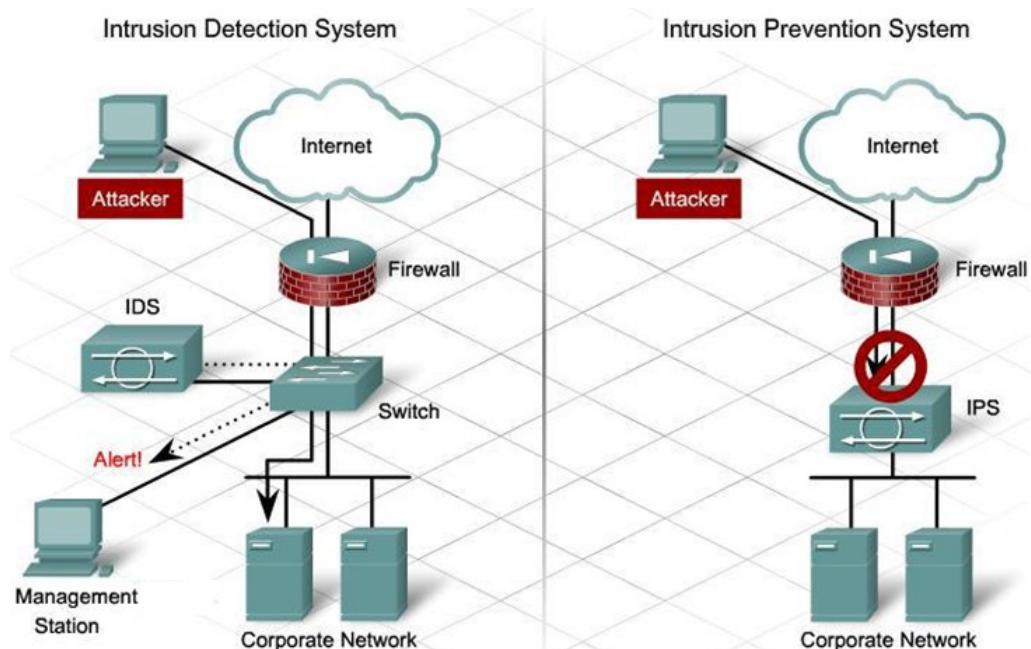
Mặc dù tường lửa được sử dụng rộng rãi để bảo vệ mạng nội bộ khỏi các cuộc tấn công, xâm nhập, nhưng cũng như hầu hết các kỹ thuật và công cụ đảm bảo an toàn khác, tường lửa cũng có những hạn chế. Các hạn chế của tường lửa gồm:

- Không thể chống lại các tấn công không đi qua tường lửa. Đó có thể là các dạng tấn công khai thác yếu tố con người, hoặc kẻ tấn công có thể xâm nhập trực tiếp vào hệ thống mạng nội bộ mà không đi qua tường lửa.
- Không thể chống lại các dạng tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng bảo mật của các phần mềm.
- Không thể chống lại các mối đe dọa từ bên trong, như tấn công từ người dùng trong mạng nội bộ.
- Không thể ngăn chặn việc vận chuyển các chương trình hoặc các file bị nhiễm vi rút hoặc các phần mềm độc hại do chúng thường ở dạng nén hoặc mã hóa.

5.3. Các hệ thống phát hiện và ngăn chặn xâm nhập

5.3.1. Khái quát

Các hệ thống phát hiện, ngăn chặn tấn công, xâm nhập (IDS/IPS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ nhiều lớp theo chiều sâu. IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập và IPS (Intrusion Prevention System) là hệ thống ngăn chặn tấn công, xâm nhập. Các hệ thống IDS/IPS có thể được triển khai ở trước hoặc sau tường lửa trong mô hình mạng tùy theo mục đích sử dụng. Hình 5.20 cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ chuyển mạch (Switch) phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa.



Hình 5.20. Vị trí các hệ thống IDS và IPS trong sơ đồ mạng

Nhiệm vụ chính của các hệ thống IDS/IPS bao gồm:

- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập;
- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi log các hành vi này cho phân tích bổ sung sau này;
- Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập (với IPS);
- Gửi thông báo, cảnh báo cho người quản trị về các hành vi tấn công, xâm nhập đã phát hiện được.

Về cơ bản IPS và IDS giống nhau về chức năng giám sát lưu lượng mạng hoặc các sự kiện trong hệ thống. Tuy nhiên, IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công, xâm nhập phát hiện được. Trong khi đó, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

5.3.2. Phân loại

5.3.2.1. Các phương pháp phân loại

Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu. Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS); và
- Hệ thống phát hiện xâm nhập cho máy (HIDS – Host-based IDS).

NIDS và HIDS hiện đều đang được sử dụng rộng rãi và mỗi loại có những ưu điểm, nhược điểm riêng. Ưu điểm của NIDS là có khả năng giám sát phát hiện các dạng xâm nhập cho cả mạng, hoặc phân đoạn mạng do nó thường được triển khai tại cổng mạng và sử dụng lưu lượng mạng gồm các gói tin đi/đến làm nguồn dữ liệu. Hạn chế của NIDS là gặp nhiều khó khăn khi phải giám sát cổng mạng có lưu lượng lớn, hoặc lưu lượng bị mã hóa và các dạng xâm nhập trên các máy không phát sinh lưu lượng qua cổng mạng. Ngược lại, các ưu điểm của HIDS là có khả năng phát hiện chính xác các xâm nhập và các hành vi lạm dụng trên từng máy cụ thể do HIDS được cài đặt trên từng máy để giám sát các sự kiện xảy ra trong hệ thống. Hạn chế của HIDS là phải triển khai trên từng máy và điều này có thể phát sinh chi phí lớn cho cài đặt và bảo trì với các hệ thống mạng lớn.

Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phát hiện được sử dụng, bao gồm:

- Phát hiện xâm nhập dựa trên chữ ký, dấu hiệu, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection); và
- Phát hiện xâm nhập dựa trên bất thường (Anomaly intrusion detection).

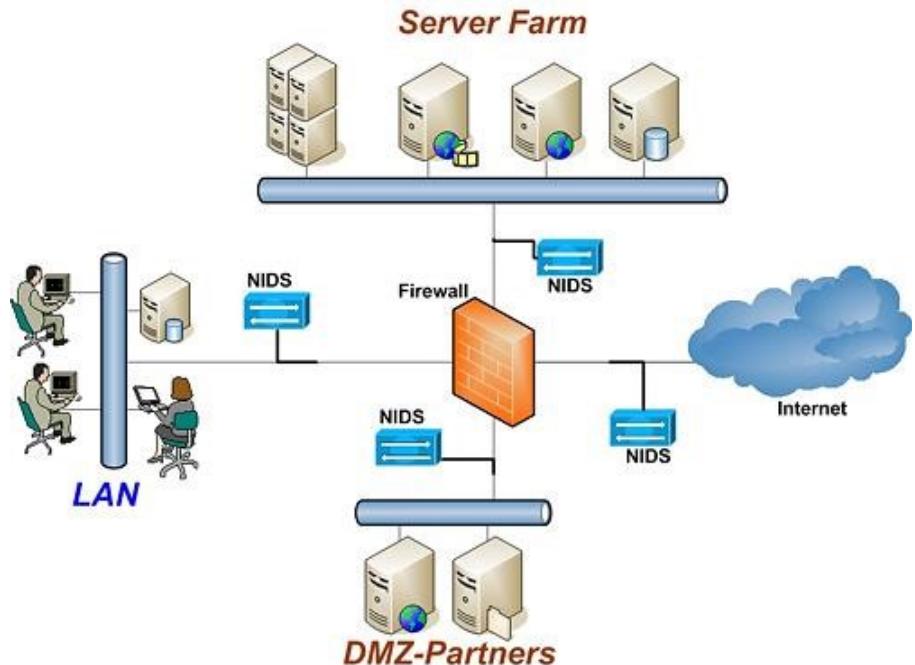
Chi tiết về hai kỹ thuật phát hiện này được đề cập trong mục 5.3.3.

5.3.2.2. NIDS và HIDS

a. NIDS

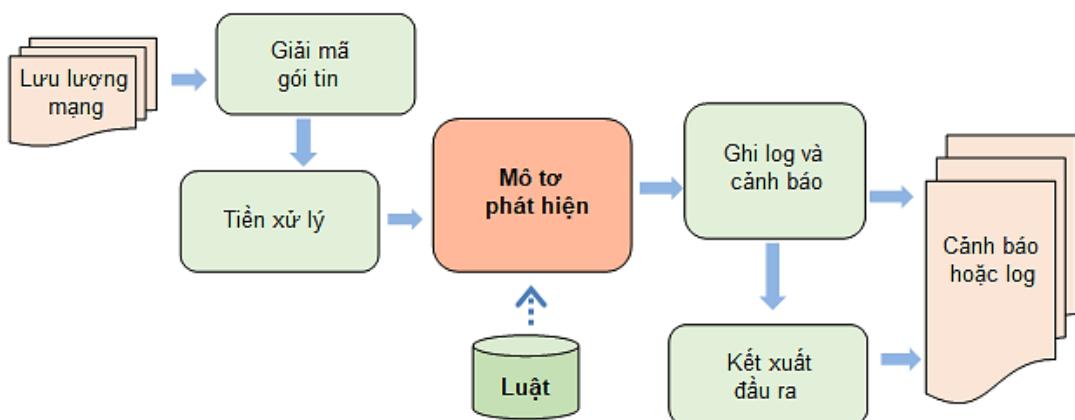
Hệ thống phát hiện xâm nhập mạng giám sát cổng mạng và thực hiện thu thập, phân tích lưu lượng mạng gồm các gói tin để phát hiện tấn công, xâm nhập cho cả mạng hoặc

một phân đoạn mạng. Hình 5.21 biểu diễn một sơ đồ mạng, trong đó một NIDS được triển khai để giám sát, phát hiện xâm nhập tại cổng vào hệ thống mạng từ Internet và một số NIDS được bố trí giám sát từng phân đoạn mạng.



Hình 5.21. Mô hình các NIDS được triển khai để giám sát, phát hiện xâm nhập

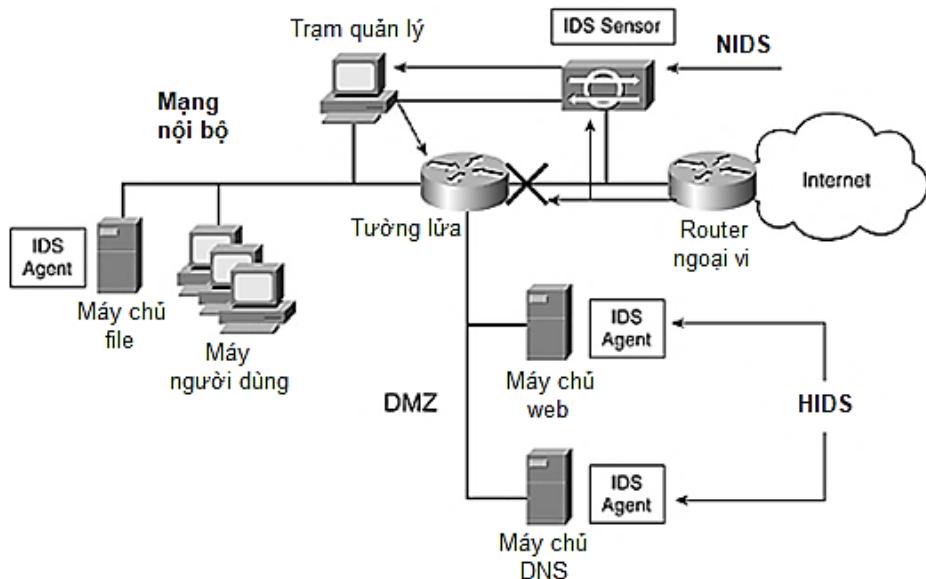
Có nhiều hệ thống NIDS dựa trên phần cứng và phần mềm, thương mại hoặc mã mở được phát triển và ứng dụng trên thực tế. Có thể kể đến một số hệ thống NIDS nổi tiếng như Check Point IPS, McAfee Network Security Platform, Snort, Bro và Suricata. Trong đó, Snort là một trong các hệ thống phát hiện xâm nhập mạng được sử dụng rộng rãi nhất. Snort là một NIDS đầy đủ dựa trên phần mềm, hỗ trợ nhiều nền tảng hệ điều hành, mã mở, miễn phí. Snort cung cấp một tập luật phát hiện dựng sẵn phong phú với khoảng 3000 luật cho phép giám sát, phát hiện hầu hết các dạng tấn công mạng đã biết. Ngoài ra, Snort cũng cho phép người dùng thêm, bớt hoặc chỉnh sửa tập luật. Hình 5.22 biểu diễn kiến trúc của Snort NIDS, trong đó thành phần quan trọng nhất của hệ thống là mô hình phát hiện thực hiện việc đối sánh dữ liệu gói tin với các luật để nhận dạng và cảnh báo các tấn công, xâm nhập.



Hình 5.22. Kiến trúc của Snort NIDS

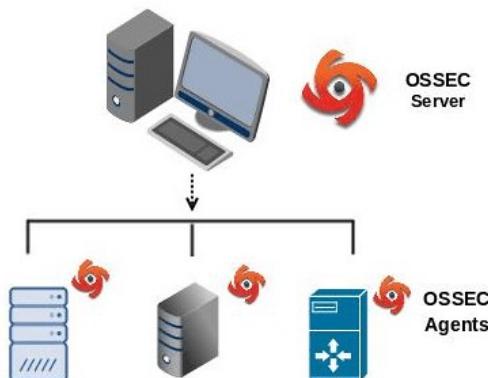
b. HIDS

Hệ thống phát hiện xâm nhập cho máy giám sát các hoạt động của một máy, thu thập và thực hiện phân tích các sự kiện xảy ra trong máy, hoặc dịch vụ chạy trên máy để phát hiện tấn công, xâm nhập, hoặc các hành vi lạm dụng. Hình 5.23 minh họa một sơ đồ mạng sử dụng kết hợp NIDS và HIDS, trong đó một NIDS được sử dụng để giám sát lưu lượng tại cổng mạng và hệ thống HIDS để giám sát các máy thông qua các IDS Agent. Các IDS Agent được cài đặt để giám sát hoạt động trên máy chủ file, máy chủ web và máy chủ DNS. Một trạm quản lý được thiết lập để thu nhận các thông tin từ các NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng.



Hình 5.23. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các máy

Cũng như NIDS, các HIDS cũng được phát triển và ứng dụng rộng rãi trên thực tế. Có thể kể đến các HIDS nổi tiếng như IMB QRadar, Tripwire, OSSEC, Security Onion và Wazuh. Trong đó, OSSEC là một trong các hệ thống phát hiện xâm nhập máy được sử dụng rộng rãi nhất. OSSEC là một HIDS đầy đủ dựa trên phần mềm, mã mở, miễn phí. Hình 5.24 biêt diễn các thành phần chính của OSSEC, theo đó một hệ thống OSSEC bao gồm một OSSEC Server và các OSSEC Agents. Các OSSEC Agents được cài đặt trên các host cần giám sát, có nhiệm vụ thu thập dữ liệu và gửi về OSSEC Server phân tích, xử lý. Kết quả phát hiện có thể được ghi log và sinh cảnh báo gửi người quản trị.



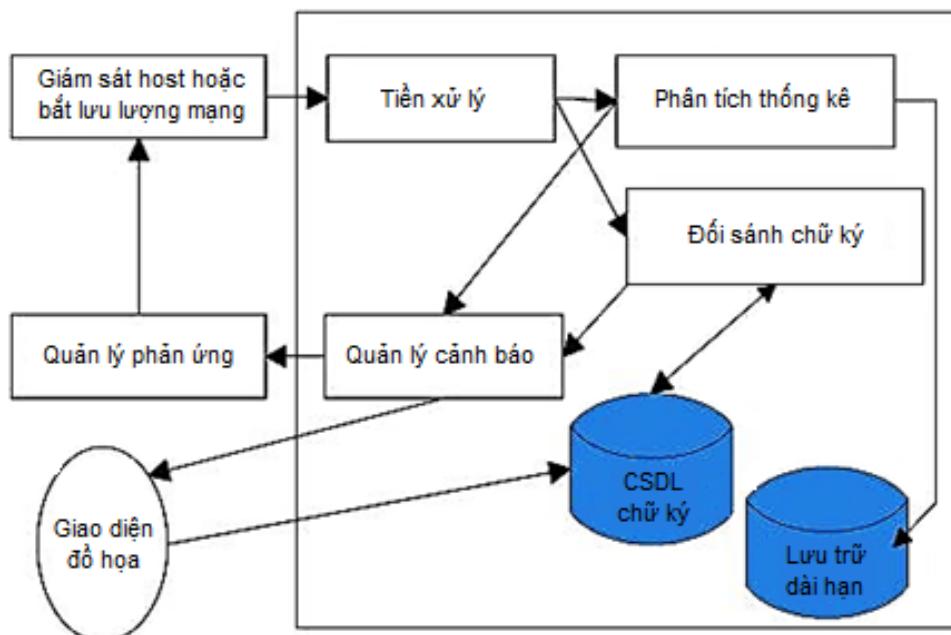
Hình 5.24. Các thành phần chính của OSSEC

5.3.3. Các kỹ thuật phát hiện xâm nhập

Bản chất của kỹ thuật phát hiện xâm nhập là việc giám sát thu thập và phân tích dữ liệu nhằm phát hiện các dấu hiệu xuất hiện tấn công, xâm nhập. Để có thể nhận dạng được các hành vi tấn công, xâm nhập, trước hết cần xây dựng cơ sở dữ liệu các dấu hiệu, hoặc chữ ký của các tấn công, xâm nhập đã biết, hoặc xây dựng hồ sơ mô tả tập các hành vi bình thường của đối tượng cần giám sát. Đây là các cơ sở của 2 kỹ thuật phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường.

5.3.3.1. Phát hiện xâm nhập dựa trên chữ ký

Như đã nêu, phát hiện xâm nhập dựa trên chữ ký trước hết cần xây dựng cơ sở dữ liệu các chữ ký, hoặc các dấu hiệu của các loại tấn công, xâm nhập đã biết. Hầu hết các chữ ký, dấu hiệu được nhận dạng và mã hóa thủ công và dạng biểu diễn thường gặp là các luật phát hiện. Bước tiếp theo là sử dụng cơ sở dữ liệu các chữ ký để giám sát các hành vi của hệ thống, hoặc mạng, và cảnh báo nếu phát hiện dấu hiệu, chữ ký của tấn công, xâm nhập. Hình 5.25 biểu diễn lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký điển hình, trong đó CSDL chữ ký là cơ sở dữ liệu lưu các dấu hiệu, chữ ký của các tấn công, xâm nhập đã biết.



Hình 5.25. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

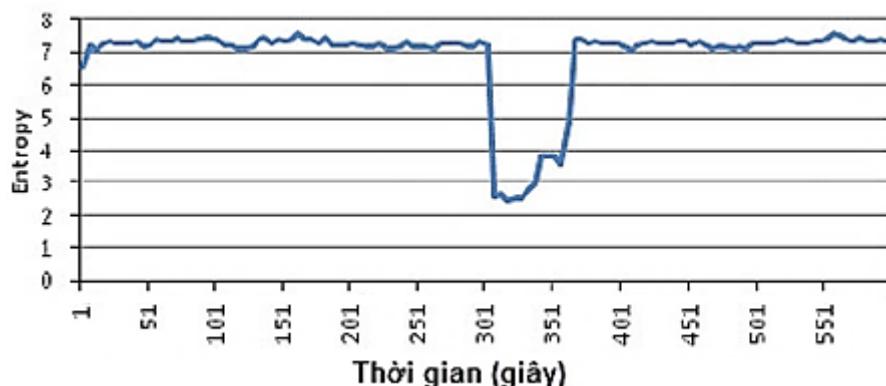
Ưu điểm lớn nhất của phát hiện xâm nhập dựa trên chữ ký là có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả. Ngoài ra, phương pháp này cho tốc độ xử lý cao, đồng thời yêu cầu tài nguyên tính toán tương đối thấp. Nhờ vậy, các hệ thống phát hiện xâm nhập dựa trên chữ ký đã và đang được ứng dụng rộng rãi trong thực tế. Tuy nhiên, nhược điểm chính của phương pháp này là không có khả năng phát hiện các tấn công, xâm nhập mới, hoặc các biến thể của xâm nhập đã biết, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu chữ ký. Hơn nữa, phương pháp này cũng đòi hỏi nhiều công sức chuyên gia cho xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.

5.3.3.2. Phát hiện xâm nhập dựa trên bất thường

Phát hiện xâm nhập dựa trên bất thường dựa trên giả thiết: *các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường*. Quá trình xây dựng và triển khai một hệ thống phát hiện xâm nhập dựa trên bất thường thường gồm 2 giai đoạn: (1) huấn luyện và (2) phát hiện. Trong giai đoạn huấn luyện, hồ sơ của đối tượng cần giám sát trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện, cần giám sát đối tượng trong một khoảng thời gian đủ dài để thu thập được đầy đủ dữ liệu mô tả các hành vi của đối tượng trong điều kiện bình thường làm dữ liệu huấn luyện. Tiếp theo, thực hiện huấn luyện dữ liệu để xây dựng mô hình phát hiện, hay hồ sơ của đối tượng. Trong giai đoạn phát hiện, thực hiện giám sát hành vi hiện tại của đối tượng và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và các hành vi lưu trong hồ sơ của đối tượng.

Có nhiều kỹ thuật xử lý, phân tích dữ liệu cho xây dựng hồ sơ của đối tượng cần giám sát đã được nghiên cứu, đề xuất cho phát hiện xâm nhập dựa trên bất thường. Mục tiêu của các kỹ thuật xử lý, phân tích dữ liệu là có thể xây dựng hồ sơ phát hiện tự động từ dữ liệu huấn luyện, cải thiện được hiệu quả phát hiện, bao gồm tăng tỷ lệ phát hiện đúng, giảm tỷ lệ phát hiện sai và giảm yêu cầu sử dụng tài nguyên tính toán. Một số kỹ thuật xử lý, phân tích dữ liệu cho phát hiện xâm nhập dựa trên bất thường có thể kể đến bao gồm: phân tích thống kê, khai phá dữ liệu, học máy và phân tích tương quan.

Hình 5.26 biểu diễn giá trị entropy IP nguồn (IP entropy) của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy IP nguồn của các gói tin từ lưu lượng tấn công DDoS theo quan sát thực nghiệm và dựa trên kỹ thuật phân tích thống kê¹. Có thể thấy sự khác biệt rõ nét giữa giá trị IP entropy của lưu lượng bình thường và lưu lượng tấn công và như vậy nếu một ngưỡng entropy được chọn phù hợp ta hoàn toàn có thể phát hiện sự xuất hiện của cuộc tấn công DDoS dựa trên sự thay đổi đột biến của giá trị entropy.



Hình 5.26. Giá trị entropy của IP nguồn của các gói tin từ lưu lượng hợp pháp (phản giá trị cao, đều) và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS (phản giá trị thấp)

Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên,

¹ Đọc thêm về phát hiện tấn công DDoS dựa trên IP entropy tại https://link.springer.com/chapter/10.1007/978-3-642-25141-2_9

phương pháp này thường có tỷ lệ cảnh báo sai tương đối cao so với phát hiện dựa trên chữ ký do một số hành vi xâm nhập không tạo ra bát thường và ngược lại một hành vi bát thường nhưng không phải là xâm nhập. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bát thường. Ngoài ra, phương pháp này cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại. Mặc dù vậy, đây vẫn là một hướng nghiên cứu phát hiện xâm nhập đang rất được quan tâm nhằm cải thiện tỷ lệ phát hiện, giảm tỷ lệ cảnh báo sai và giảm yêu cầu sử dụng tài nguyên tính toán, lưu trữ.

5.4. Kết chương

Chương này trình bày các kỹ thuật, công nghệ và công cụ đảm bảo an toàn cho thông tin, hệ thống và mạng. Cụ thể các vấn đề sau đã được đề cập:

- Trình bày khái quát về kiểm soát truy cập, các thành phần của một hệ thống kiểm soát truy cập, các biện pháp kiểm soát truy cập và một số công nghệ kiểm soát truy cập được sử dụng trên thực tế.
- Giới thiệu khái quát về tường lửa, các loại tường lửa, các kỹ thuật kiểm soát truy cập của tường lửa và các hạn chế của tường lửa.
- Mô tả khái quát về hệ thống phát hiện và ngăn chặn xâm nhập, các loại hệ thống phát hiện và ngăn chặn xâm nhập và các kỹ thuật phát hiện xâm nhập.

Ngoài các vấn đề nêu trên trong phạm vi của môn học Cơ sở an toàn thông tin, các vấn đề khác liên quan đến các kỹ thuật, công nghệ và công cụ đảm bảo an toàn cho thông tin, hệ thống và mạng sẽ được trình bày trong các môn học khác theo tiến trình học tập của ngành đào tạo đại học an toàn thông tin bao gồm:

- Công nghệ mạng riêng ảo (VPN – Virtual Private Network)
- Hệ thống Honeypot và Honeynet
- Các hệ thống và công cụ thu thập và phân tích mã độc
- Các giải pháp, công cụ giám sát phòng chống tấn công DDoS
- Công nghệ ảo hóa, điện toán đám mây và các vấn đề bảo mật liên quan
- Các công nghệ, công cụ giám sát, phát hiện tấn công, xâm nhập dựa trên nền tảng học máy, học sâu.

5.5. Câu hỏi ôn tập

- 1) Nêu khái niệm, các thành phần và mục đích của kiểm soát truy cập. Lấy 3 ví dụ về hệ thống kiểm soát truy cập trên thực tế.
- 2) Nêu cơ chế hoạt động của kiểm soát truy cập tùy chọn (DAC).
- 3) Nêu cơ chế hoạt động của kiểm soát truy cập bắt buộc (MAC).
- 4) Nêu cơ chế hoạt động của kiểm soát truy cập dựa trên vai trò (RBAC).
- 5) Nêu cơ chế hoạt động của kiểm soát truy cập dựa trên luật (Rule-based access control).

- 6) Tại sao khâu xác thực trong hệ thống kiểm soát truy cập thường không thể xác minh được chủ thể thực sự của thông tin cung cấp?
- 7) So sánh 2 kỹ thuật thực hiện kiểm soát truy cập tùy chọn: ma trận kiểm soát truy cập và danh sách kiểm soát truy cập.
- 8) Mô tả cơ chế hoạt động của mô hình bảo mật đa cấp Bell-LaPadula.
- 9) Giám đốc một công ty yêu cầu chuẩn bị một văn bản quan trọng để ông ký duyệt và nhân viên văn phòng đóng dấu công ty và dấu “Mật”. Vậy nhân viên văn phòng có được phép tiết lộ nội dung văn bản cho người khác hay không? Tại sao?
- 10) Mô tả công nghệ kiểm soát truy cập dựa trên mật khẩu.
- 11) Trong các công nghệ kiểm soát truy cập: dựa trên mật khẩu, khóa mã, thẻ thông minh, thẻ bài và các đặc điểm sinh trắc, công nghệ nào có khả năng cho độ bảo mật cao nhất? Tại sao?
- 12) Tường lửa là gì? Nêu vai trò của tường lửa và các phương pháp phân loại tường lửa.
- 13) Nêu các kỹ thuật kiểm soát truy cập và các hạn chế của tường lửa.
- 14) Các hệ thống IDS/IPS là gì? Nêu các nhiệm vụ chính của IDS/IPS. IDS và IPS giống và khác nhau ở những điểm nào?
- 15) Nêu các phương pháp phân loại IDS/IPS. Có thể sử dụng kết hợp NIDS và HIDS trong cùng một hệ thống mạng được không?
- 16) Mô tả phương pháp phát hiện xâm nhập dựa trên chữ ký. Nêu ưu nhược điểm của phương pháp này. Tại sao phát hiện xâm nhập dựa trên chữ ký không có khả năng phát hiện các tấn công xâm nhập mới?
- 17) Mô tả phương pháp phát hiện xâm nhập dựa trên bất thường. Nêu ưu nhược điểm của phương pháp này.
- 18) Tại sao phát hiện xâm nhập dựa trên bất thường có khả năng phát hiện các tấn công xâm nhập mới? Tại sao phát hiện xâm nhập dựa trên bất thường thường có tỷ lệ cảnh báo sai cao hơn phát hiện xâm nhập dựa trên chữ ký?
- 19) Tìm hiểu kiến trúc và hoạt động của Snort NIDS.
- 20) Tìm hiểu kiến trúc và hoạt động của OSSEC HIDS.

CHƯƠNG 6. QUẢN LÝ, CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN

Chương 6 giới thiệu một số khái niệm cơ bản trong quản lý an toàn thông tin, vấn đề đánh giá rủi ro an toàn thông tin và thực thi quản lý an toàn thông tin. Nội dung tiếp theo của chương đề cập đến các chuẩn quản lý an toàn thông tin, trong đó giới thiệu một số chuẩn của bộ chuẩn ISO/IEC 27000. Phần cuối của chương giới thiệu khái quát về các vấn đề chính sách, pháp luật và đạo đức an toàn thông tin.

6.1 Quản lý an toàn thông tin

Mục 1.3.3 đã giới thiệu khái quát quản lý an toàn thông tin là việc quản lý và giám sát việc thực thi các biện pháp, cơ chế đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Quản lý an toàn thông tin bao gồm nhiều nội dung, trong đó vấn đề quản lý rủi ro an toàn thông tin là một trong nội dung quan trọng nhất. Mục này trình bày một số khái niệm cơ bản trong quản lý an toàn thông tin, 2 khâu quan trọng của quản lý rủi ro an toàn thông tin, bao gồm đánh giá rủi ro an toàn thông tin và thực thi quản lý an toàn thông tin.

6.1.1. Khái quát

Chúng ta bắt đầu mục này với khái niệm *Tài sản* (Asset) trong lĩnh vực an toàn thông tin, gọi tắt là *Tài sản an toàn thông tin*. Tài sản an toàn thông tin là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin. Tài sản an toàn thông tin có thể gồm:

- Phân cứng (máy chủ, các thiết bị mạng,...);
- Phân mềm (hệ điều hành, các phần mềm máy chủ dịch vụ,...); và
- Thông tin (thông tin khách hàng, nhà cung cấp, hoạt động kinh doanh,...).

Khái niệm tiếp theo là *Quản lý an toàn thông tin*. Hiểu một cách đầy đủ, quản lý an toàn thông tin là một tiến trình nhằm đảm bảo các tài sản an toàn thông tin quan trọng của cơ quan, tổ chức, doanh nghiệp được *bảo vệ đầy đủ* với *chi phí phù hợp*.

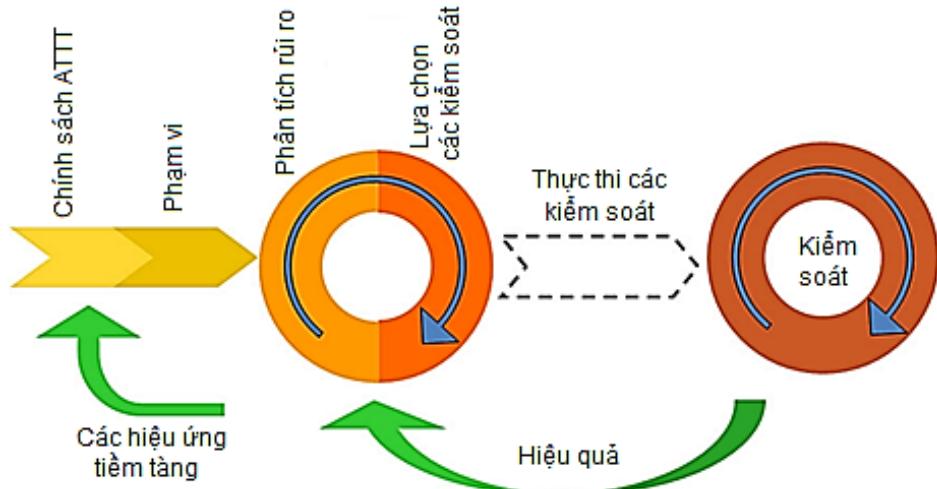
Có thể thấy quản lý an toàn thông tin là một thành phần rất quan trọng trong an toàn thông tin và nó phải trả lời được 3 câu hỏi:

1. Những tài sản nào cần được bảo vệ?
2. Những đe dọa nào có thể có đối với các tài sản này?
3. Những biện pháp có thể thực hiện để ứng phó với các đe dọa đó?

Theo [1][2], quản lý an toàn thông tin có thể được thực hiện theo 3 khâu chính sau:

- Khâu 1: Xác định rõ mục đích đảm bảo an toàn thông tin và xây dựng hồ sơ tổng hợp về các rủi ro;
- Khâu 2: Đánh giá rủi ro với từng tài sản an toàn thông tin cần bảo vệ; và
- Khâu 3: Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được.

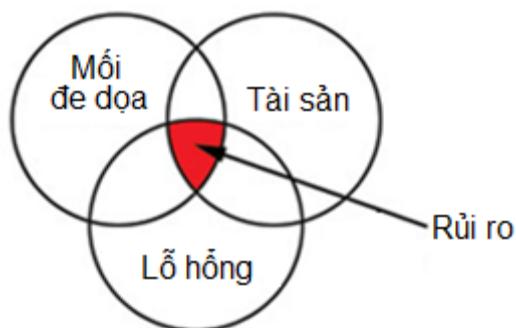
Một điểm quan trọng cần lưu ý là, quá trình quản lý an toàn thông tin cần được thực hiện liên tục theo chu trình do sự thay đổi nhanh chóng của công nghệ và môi trường xuất hiện rủi ro. Hình 6.1 mô tả mô hình hệ thống quản lý an toàn thông tin theo chuẩn ISO 27001. Theo đó, phần việc Phân tích rủi ro được thực hiện trong các Khâu 1 và Khâu 2, và các phần việc Lựa chọn các kiểm soát và Thực thi các kiểm soát được thực hiện trong Khâu 3. Khi các kiểm soát được triển khai sẽ có khả năng thay đổi mức rủi ro đối với các tài sản an toàn thông tin.



6.1.2. Đánh giá rủi ro an toàn thông tin

6.1.2.1. Giới thiệu

Đánh giá rủi ro an toàn thông tin (Security risk assessment) là một bộ phận quan trọng của quản lý rủi ro an toàn thông tin. Theo đó, mỗi tài sản của tổ chức cần được xem xét, nhận dạng các rủi ro có thể có và đánh giá mức rủi ro. Đánh giá rủi ro là một trong các cơ sở để xác định mức rủi ro chấp nhận được với từng loại tài sản. Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức chấp nhận được, với mức chi phí phù hợp.



Hình 6.2 minh họa mô hình đánh giá rủi ro an toàn thông tin, trong đó 3 nhân tố chính liên quan trực tiếp cần được xem xét gồm: (1) Tài sản an toàn thông tin (Asset) cần được bảo vệ, (2) Các mối đe dọa (Threat) đối với các tài sản an toàn thông tin và (3) Các lỗ hổng bảo mật (Vulnerability) tồn tại trong các tài sản an toàn thông tin. Như vậy, việc

đánh giá rủi ro an toàn thông tin cần phải xem xét toàn diện cả vấn đề bên trong của tài sản an toàn thông tin (lỗ hổng bảo mật) và vấn đề bên ngoài (mối đe doạ).

Có 4 phương pháp tiếp cận đánh giá rủi ro: Phương pháp đường cơ sở (Baseline approach), Phương pháp không chính thức (Informal approach), Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis) và Phương pháp kết hợp (Combined approach). Tùy theo quy mô của hệ thống thông tin của đơn vị và tài sản an toàn thông tin cần được bảo vệ, đơn vị có thể xem xét lựa chọn phương pháp đánh giá rủi ro cho phù hợp. Mục tiếp theo mô tả chi tiết về các phương pháp đánh giá rủi ro kể trên.

6.1.2.2. Các phương pháp đánh giá rủi ro

Phương pháp đánh giá rủi ro đường cơ sở là phương pháp đơn giản nhất. Mục đích của phương pháp này là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên các tài liệu cơ bản, các quy tắc thực hành và các thực tế tốt nhất của ngành đã được áp dụng. Phương pháp đường cơ sở có ưu điểm là không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức và cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống. Tuy nhiên, nhược điểm của nó là không xem xét kỹ đến các điều kiện này sinh các rủi ro ở các hệ thống của các tổ chức khác nhau. Một vấn đề khác của phương pháp này là mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể. Nếu chọn mức quá cao có thể gây tổn kém, nhưng nếu chọn mức quá thấp có thể gây mất an toàn. Nhìn chung, phương pháp đường cơ sở phù hợp với các tổ chức có hệ thống công nghệ thông tin quy mô nhỏ và nguồn lực hạn chế.

Phương pháp không chính thức là phương pháp tiếp cận đánh giá rủi ro tiếp theo. Phương pháp không chính thức liên quan đến việc thực hiện các nội dung sau:

- Thực hiện một số dạng phân tích rủi ro hệ thống công nghệ thông tin của tổ chức một cách không chính thức,
- Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các chuyên gia tư vấn từ bên ngoài, và
- Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản công nghệ thông tin của tổ chức.

Phương pháp này có ưu điểm là không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp. Đồng thời, việc có phân tích hệ thống công nghệ thông tin của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở. Phương pháp không chính thức có các nhược điểm:

- Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức, và
- Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân.

Trên thực tế phương pháp không chính thức phù hợp với các tổ chức có hệ thống công nghệ thông tin quy mô nhỏ và vừa và nguồn lực tương đối hạn chế.

Phương pháp phân tích chi tiết rủi ro là phương pháp đánh giá toàn diện, được thực hiện một cách chính thức và được chia thành nhiều giai đoạn, bao gồm:

- Nhận dạng các tài sản,
- Nhận dạng các mối đe dọa và lỗ hổng đối với các tài sản này,
- Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với cơ quan, tổ chức, và
- Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn nêu trên.

Ưu điểm của phương pháp này là cho phép xem xét chi tiết các rủi ro đối với hệ thống công nghệ thông tin của tổ chức và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi ro đề xuất. Đồng thời, nó cũng cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống công nghệ thông tin khi chúng được nâng cấp, sửa đổi. Tuy nhiên, phương pháp này có 2 nhược điểm:

- Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia có trình độ cao, và
- Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp.

Phương pháp phân tích chi tiết rủi ro phù hợp với các tổ chức chính phủ cung cấp các dịch vụ thiết yếu cho người dân và doanh nghiệp, hoặc các tổ chức có hệ thống công nghệ thông tin quy mô lớn, hoặc các tổ chức cung cấp nền tảng hạ tầng truyền thông cho quốc gia.

Phương pháp kết hợp là phương pháp tiếp cận đánh giá rủi ro cuối cùng. Phương pháp này kết hợp các thành phần của 3 phương pháp đường cơ sở, không chính thức và phân tích chi tiết, với mục tiêu là cung cấp mức bảo vệ hợp lý càng nhanh càng tốt và sau đó thực hiện kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian. Phương pháp kết hợp được thực hiện theo 3 bước:

- Thực hiện phương pháp đường cơ sở với tất cả các thành phần của hệ thống công nghệ thông tin của tổ chức;
- Tiếp theo, các thành phần có mức rủi ro cao, hoặc trọng yếu được xem xét đánh giá theo phương pháp không chính thức;
- Cuối cùng hệ thống được xem xét đánh giá toàn diện rủi ro ở mức chi tiết.

Các ưu điểm của phương pháp kết hợp là bắt đầu bằng việc đánh giá rủi ro ở mức cao để nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý an toàn thông tin, đồng thời có thể giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu, cũng như có thể giúp giảm chi phí với đa số các tổ chức. Tuy nhiên, phương pháp kết hợp có nhược điểm là nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp và hậu quả là hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết. Nói chung, phương pháp kết hợp phù hợp các cơ quan, tổ chức có hệ thống công nghệ thông tin quy mô vừa và lớn.

6.1.3. Phân tích chi tiết rủi ro an toàn thông tin

6.1.3.1. Giới thiệu

Phân tích chi tiết rủi ro an toàn thông tin là phương pháp xem xét, phân tích toàn diện các rủi ro của từng thành phần trong hệ thống công nghệ thông tin của cơ quan, tổ chức. Phân tích chi tiết rủi ro an toàn thông tin gồm nhiều hoạt động và được chia thành 9 bước như sau:

1. Mô tả đặc điểm hệ thống
2. Nhận dạng các mối đe dọa
3. Nhận dạng các lỗ hổng bảo mật
4. Phân tích các kiểm soát
5. Xác định xác suất rủi ro
6. Phân tích các ảnh hưởng
7. Xác định các rủi ro
8. Đề xuất các kiểm soát
9. Viết tài liệu kết quả phân tích.

Nội dung cụ thể từng bước của phân tích chi tiết rủi ro an toàn thông tin được trình bày trong mục tiếp theo.

6.1.3.2. Các bước phân tích chi tiết rủi ro

Bước 1: Mô tả đặc điểm hệ thống

- Đầu vào: Các thành phần của hệ thống:
 - + Phần cứng, phần mềm, giao diện
 - + Dữ liệu và thông tin
 - + Con người
 - + Sứ mệnh của hệ thống.
- Đầu ra:
 - + Ranh giới và chức năng hệ thống;
 - + Tính trọng yếu của dữ liệu và hệ thống;
 - + Tính nhạy cảm

Bước 2: Nhận dạng các mối đe dọa

- Đầu vào:
 - + Lịch sử tấn công vào hệ thống
 - + Dữ liệu từ các tổ chức chuyên về an toàn thông tin
 - + Dữ liệu từ các phương tiện thông tin đại chúng.
- Đầu ra:
 - + Báo cáo về các mối đe dọa đối với hệ thống

Bước 3: Nhận dạng các lỗ hổng bảo mật

- Đầu vào:
 - + Các báo cáo đánh giá rủi ro đã có
 - + Các nhận xét kiểm toán hệ thống
 - + Các yêu cầu an ninh, an toàn
 - + Các kết quả kiểm tra an ninh, an toàn
- Đầu ra:
 - + Danh sách các lỗ hổng bảo mật tiềm tàng.

Bước 4: Phân tích các kiểm soát

- Đầu vào:
 - + Các kiểm soát hiện có
 - + Các kiểm soát được lập kế hoạch
- Đầu ra:
 - + Danh sách các kiểm soát hiện có và được lập kế hoạch.

Bước 5: Xác định xác suất rủi ro

- Đầu vào:
 - + Động cơ của các nguồn đe dọa
 - + Khả năng của đe dọa
 - + Bản chất của lỗ hổng bảo mật
 - + Các kiểm soát hiện có
- Đầu ra:
 - + Đánh giá xác suất rủi ro.

Bước 6: Phân tích các ảnh hưởng (liên quan sự vi phạm tính toàn vẹn, sẵn sàng và bí mật của các tài sản hệ thống)

- Đầu vào:
 - + Phân tích ảnh hưởng sứ mệnh
 - + Đánh giá tầm quan trọng của tài sản
 - + Tầm quan trọng của dữ liệu
 - + Tính nhạy cảm của dữ liệu
- Đầu ra:
 - + Đánh giá các ảnh hưởng.

Bước 7: Xác định các rủi ro

- Đầu vào:
 - + Khả năng bị mối đe dọa khai thác
 - + Tầm quan trọng của ảnh hưởng
 - + Sự phù hợp của các kiểm soát theo kế hoạch, hoặc hiện có

- Đầu ra:
 - + Các rủi ro và các mức rủi ro có liên quan.

Bước 8: Đề xuất các kiểm soát

- Đầu vào: Không
- Đầu ra: Đề xuất các biện pháp xử lý, kiểm soát rủi ro

Bước 9: Viết tài liệu kết quả phân tích

- Đầu vào: Không
- Đầu ra: Báo cáo đánh giá rủi ro.

6.1.4. Thực thi quản lý an toàn thông tin

6.1.4.1. Giới thiệu

Thực thi quản lý an toàn thông tin là bước tiếp theo của khâu đánh giá rủi ro, nhằm triển khai, thực thi các kiểm soát nhằm đảm bảo an toàn cho hệ thống công nghệ thông tin của tổ chức. Các nội dung chính của thực thi quản lý an toàn thông tin gồm:

- Thực thi (Implementation) bao gồm việc thực thi các kiểm soát và đào tạo nâng cao ý thức người dùng và đào tạo chuyên môn an toàn thông tin.
- Thực thi tiếp tục (Implementation follow-up) bao gồm việc bảo trì, kiểm tra hợp chuẩn, quản lý thay đổi và xử lý sự cố.

Trong bước thực thi quản lý an toàn thông tin, các thuật ngữ kiểm soát (control), đảm bảo an toàn (safeguard), hoặc biện pháp đối phó (countermeasure) có thể được sử dụng tương đương, hoặc tráo đổi cho nhau. Kiểm soát là phương tiện để quản lý rủi ro, bao gồm các chính sách, thủ tục, các hướng dẫn, các thực tế, hoặc cấu trúc tổ chức. Kiểm soát có thể là vấn đề quản lý hành chính hoặc kỹ thuật, hoặc có bản chất luật pháp. Các kiểm soát được thực thi trong quản lý an toàn thông tin có thể gồm 6 loại:

- Kiểm soát quản lý (Management control)
- Kiểm soát vận hành (Operational control)
- Kiểm soát kỹ thuật (Technical control)
- Kiểm soát hỗ trợ (Supportive control)
- Kiểm soát ngăn ngừa (Preventive control)
- Kiểm soát phát hiện và phục hồi (Detection and recovery control).

Mục tiếp theo trình bày chi tiết về các loại kiểm soát nêu trên.

6.1.4.2. Các loại kiểm soát

Kiểm soát quản lý bao gồm các nội dung:

- Tập trung vào các chính sách, lập kế hoạch, hướng dẫn và chuẩn an toàn thông tin;
- Các kiểm soát có ảnh hưởng đến việc lựa chọn các kiểm soát vận hành và kiểm soát kỹ thuật nhằm giảm tổn thất do rủi ro và bảo vệ sứ mệnh của tổ chức;
- Các kiểm soát tham chiếu đến vấn đề được giải quyết thông qua lĩnh vực quản lý.

Kiểm soát vận hành bao gồm các nội dung:

- Giải quyết vấn đề thực thi chính xác và sử dụng các chính sách và chuẩn an toàn thông tin, đảm bảo tính nhất quán trong vận hành an toàn thông tin và khắc phục các khiếm khuyết vận hành đã được nhận dạng;
- Các kiểm soát này liên quan đến các cơ chế và thủ tục được thực thi chủ yếu bởi con người, hơn là bởi hệ thống;
- Được sử dụng để tăng cường an ninh cho một hệ thống, hoặc một nhóm các hệ thống.

Kiểm soát kỹ thuật bao gồm các nội dung:

- Các kiểm soát kỹ thuật thường liên quan đến việc sử dụng đúng đắn các biện pháp đảm bảo an ninh bằng phần cứng và phần mềm trong hệ thống;
- Bao gồm các biện pháp từ đơn giản đến phức tạp để đảm bảo an toàn cho các thông tin nhạy cảm và các chức năng trọng yếu của các hệ thống;
- Một số kiểm soát kỹ thuật như xác thực, trao quyền và thực thi kiểm soát truy cập,...

Kiểm soát hỗ trợ là các kiểm soát chung ở lớp dưới, có quan hệ và được sử dụng bởi nhiều kiểm soát khác.

Kiểm soát ngăn ngừa là kiểm soát tập trung vào việc ngăn ngừa việc xảy ra các vi phạm an ninh, bằng cách khắc chế các nỗ lực vi phạm chính sách an ninh, hoặc khai thác các lỗ hổng bảo mật.

Kiểm soát phát hiện và phục hồi là kiểm soát tập trung vào việc đáp trả vi phạm an ninh bằng cách đưa ra cảnh báo vi phạm, hoặc các nỗ lực vi phạm chính sách an ninh, hoặc khai thác các lỗ hổng bảo mật, đồng thời cung cấp các biện pháp phục hồi các tài nguyên tính toán bị ảnh hưởng do vi phạm an ninh.

6.1.4.3. Xây dựng kế hoạch đảm bảo an toàn

Kế hoạch đảm bảo an toàn là một tài liệu chỉ rõ các phần việc sẽ được thực hiện, các tài nguyên cần sử dụng và những người, hoặc nhân viên chịu trách nhiệm thực hiện. Mục đích của kế hoạch đảm bảo an toàn là cung cấp chi tiết về các hành động cần thiết để cải thiện các vấn đề đã được nhận dạng trong hồ sơ đánh giá rủi ro một cách nhanh chóng. Theo chuẩn hướng dẫn quản lý rủi ro năm 2002 của viện NIST, kế hoạch đảm bảo an toàn nên gồm các thông tin chi tiết sau:

- Các rủi ro (sự kết hợp của tài sản/mối đe dọa/lỗ hổng)
- Các kiểm soát được khuyến nghị (từ đánh giá rủi ro)
- Các hành động ưu tiên cho mỗi rủi ro
- Các kiểm soát được chọn (dựa trên phân tích lợi ích – chi phí)
- Các tài nguyên cần có cho thực thi các kiểm soát đã chọn
- Nhân sự chịu trách nhiệm
- Ngày bắt đầu và kết thúc việc thực thi

- Các yêu cầu bảo trì và các nhận xét khác.

6.1.4.4. Nội dung thực thi quản lý an toàn thông tin

Như đã đề cập trong mục 6.1.4.1, việc thực thi quản lý an toàn thông tin gồm 2 khâu là (1) *thực thi* và (2) *thực thi tiếp tục*. Khâu *thực thi* gồm 2 phần việc là (1) thực thi các kiểm soát, và (2) đào tạo nâng cao ý thức người dùng và đào tạo chuyên sâu về an toàn thông tin. Thực thi các kiểm soát là phần việc tiếp theo cần thực hiện trong kế hoạch đảm bảo an toàn của tiến trình quản lý an toàn thông tin. Thực thi các kiểm soát có liên hệ mật thiết với việc đào tạo nâng cao ý thức an toàn thông tin cho nhân viên nói chung và đào tạo chuyên sâu về an toàn thông tin cho nhân viên chuyên trách về an toàn thông tin, công nghệ thông tin trong tổ chức.

Khâu *thực thi tiếp tục* là việc cần lặp lại trong chu trình quản lý an toàn thông tin để đáp ứng sự thay đổi trong môi trường công nghệ thông tin và môi trường rủi ro. Trong đó, các kiểm soát đã được thực thi cần được giám sát để đảm bảo tính hiệu quả, và bất kỳ một sự thay đổi trên hệ thống cần được xem xét vấn đề an ninh và hồ sơ rủi ro của hệ thống bị ảnh hưởng. Giai đoạn thực thi tiếp tục bao gồm các khía cạnh: bảo trì các kiểm soát an ninh, kiểm tra hợp chuẩn an ninh, quản lý thay đổi và cấu hình và xử lý các sự cố.

Bảo trì các kiểm soát an ninh gồm các phần việc phải đảm bảo các yêu cầu sau:

- Các kiểm soát cần được xem xét định kỳ để đảm bảo chúng hoạt động như mong muốn;
- Các kiểm soát cần được nâng cấp khi các yêu cầu mới được phát hiện;
- Các thay đổi với hệ thống không được có các ảnh hưởng tiêu cực đến các kiểm soát;
- Các mối đe dọa mới, hoặc các lỗ hổng đã không trở thành được biết đến.

Kiểm tra hợp chuẩn an ninh là quá trình kiểm toán việc quản lý an toàn thông tin của tổ chức nhằm đảm bảo tính phù hợp với kế hoạch đảm bảo an ninh. Việc kiểm toán có thể được thực hiện bởi nhân sự bên trong hoặc bên ngoài tổ chức. Cần sử dụng danh sách kiểm tra (checklist) các vấn đề: các chính sách và kế hoạch an ninh được tạo ra, các kiểm soát phù hợp được lựa chọn và các kiểm soát được sử dụng và bảo trì phù hợp.

Quản lý thay đổi và cấu hình là quá trình xem xét các thay đổi được đề xuất cho hệ thống trong quá trình sử dụng. Các thay đổi với các hệ thống hiện có là cần thiết do nhiều lý do, như hệ thống có trực trặc, hoặc sự xuất hiện của các mối đe dọa hoặc lỗ hổng mới, sự xuất hiện của yêu cầu mới, nhiệm vụ mới,... Các thay đổi cần được xem xét kỹ lưỡng các vấn đề vận hành, tính năng và an toàn,... Quản lý cấu hình liên quan đến việc lưu vết cấu hình của mỗi hệ thống khi chúng được nâng cấp, thay đổi. Việc này bao gồm danh sách các phiên bản của phần cứng, phần mềm cài đặt trong mỗi hệ thống và thông tin quản lý cấu hình hữu ích để khôi phục hệ thống khi việc thay đổi hoặc nâng cấp thất bại.

Xử lý các sự cố bao gồm các thủ tục được sử dụng để phản ứng lại các sự cố an ninh. Xử lý sự cố có liên quan đến vấn đề đào tạo nâng cao ý thức an toàn thông tin cho người dùng và đào tạo chuyên sâu cho chuyên viên an toàn thông tin.

6.2. Các chuẩn quản lý an toàn thông tin

6.2.1. Giới thiệu

Trong các chuẩn quản lý an toàn thông tin, bộ chuẩn NIST SP 800 của Viện NIST, Hoa Kỳ và bộ chuẩn quốc tế ISO/IEC 27000 được tham chiếu và sử dụng rộng rãi nhất. Nhiều quốc gia, trong đó có Việt Nam đã dịch và chấp thuận nguyên vẹn một số chuẩn trong bộ chuẩn quốc tế ISO/IEC 27000 làm chuẩn quản lý an toàn thông tin quốc gia. Trong phạm vi của môn học, mục này giới thiệu khái quát về bộ chuẩn quản lý an toàn thông tin ISO/IEC 27000 và chuẩn con ISO/IEC 27001. Chi tiết về bộ chuẩn ISO/IEC 27000 và các bộ chuẩn quản lý an toàn thông tin khác được đề cập trong môn học Quản lý an toàn thông tin.

Chuẩn ISO/IEC 27000: 2009 giới thiệu khái quát về bộ chuẩn ISO/IEC 27000 và định nghĩa các thuật ngữ và từ vựng sử dụng cho toàn bộ các chuẩn con trong bộ chuẩn ISO/IEC 27000.

Chuẩn ISO/IEC 27001:2005 chuyên về hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS). Chuẩn này cung cấp các thông tin để thực thi các yêu cầu của ISO/IEC 27002 và vấn đề cài đặt một hệ thống quản lý an toàn thông tin. Trong việc xây dựng hệ thống ISMS, chuẩn này cung cấp các chi tiết cho thực hiện chu kỳ Plan-Do-Check-Act (Lập kế hoạch – Thực hiện – Giám sát – Hành động). Một điểm cần lưu ý là ISO/IEC 27001 chỉ tập trung vào các phần việc phải thực hiện mà không chỉ dẫn cách thức thực hiện.

Chuẩn ISO/IEC 17799 được soạn thảo năm 2000 bởi các tổ chức ISO (International Organization for Standardization) và IEC (International Electrotechnical Commission) là tiền thân của bộ chuẩn ISO 27000. Năm 2005, ISO 17799 được chỉnh sửa và trở thành ISO 17799:2005. Năm 2007, ISO 17799:2005 được đổi tên thành ISO 27002, song hành với ISO 27001.

Chuẩn ISO/IEC 27002 gồm 127 điều, cung cấp cái nhìn tổng quan về nhiều lĩnh vực trong an toàn thông tin. Nó đề ra các khuyến nghị về quản lý an toàn thông tin cho những người thực hiện việc khởi tạo, thực hiện và duy trì an ninh an toàn trong tổ chức của họ. Chuẩn này được thiết kế để cung cấp nền tảng cơ sở giúp đề ra các chuẩn an toàn thông tin cho tổ chức và các thực tế quản lý an toàn thông tin một cách hiệu quả.

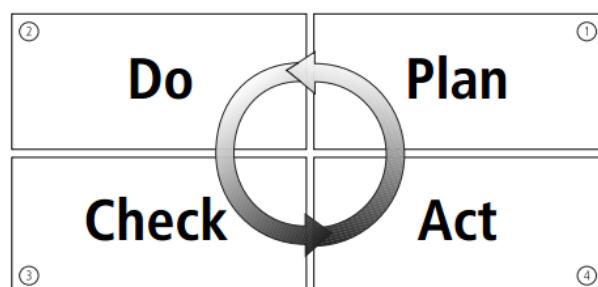
Bộ chuẩn ISO/IEC 27000:2014 được Việt Nam dịch và chấp thuận nguyên vẹn thành chuẩn TCVN 11238:2015. Cụ thể danh sách các chuẩn trong bộ chuẩn này như sau:

- TCVN 11238 (ISO/IEC 27000), Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng (*Information security management systems - Overview and vocabulary*).
- TCVN ISO/IEC 27001 (ISO/IEC 27001), Hệ thống quản lý an toàn thông tin - Các yêu cầu (*ISO/IEC 27001 Information security management systems - Requirements*)
- TCVN ISO/IEC 27002 (ISO/IEC 27002), Quy tắc thực hành cho hệ thống quản lý an toàn thông tin (*Code of practice for information security management*).
- TCVN 10541 (ISO/IEC 27003), Hướng dẫn triển khai hệ thống quản lý an toàn thông tin (*Information security management system implementation guidance*).

- TCVN 10542 (ISO/IEC 27004), Quản lý an toàn thông tin - Đo lường (*Information security management - Measurement*).
- TCVN 10295 (ISO/IEC 27005), Quản lý rủi ro an toàn thông tin (*Information security risk management*).
- ISO/IEC 27006, Các yêu cầu đối với cơ quan đánh giá và chứng nhận hệ thống quản lý an toàn thông tin (Requirements for bodies providing audit and certification of information security management systems).
- ISO/IEC 27007, Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin (*Guidelines for information security management systems auditing*).
- ISO/IEC TR 27008, Hướng dẫn cho đánh giá viên về biện pháp kiểm soát hệ thống quản lý an toàn thông tin (*Guidelines for auditors on information security management systems controls*).
- TCVN 10543 (ISO/IEC 27010), Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành (*Information security management guidelines for inter-sector and inter-organisational communications*).
- ISO/IEC 27011, Hướng dẫn quản lý an toàn thông tin cho các tổ chức viễn thông dựa theo ISO/IEC 27002 (*Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*).
- TCVN 9965 (ISO/IEC 27013), Hướng dẫn triển khai tích hợp TCVN ISO/IEC 27001 và ISO/IEC 20000-1 (*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*).
- ISO/IEC 27014, Quản trị an toàn thông tin (*Governance of information security*).
- ISO/IEC TR 27015, Hướng dẫn quản lý an toàn thông tin cho các dịch vụ tài chính (*Information security management guidelines for financial services*).
- ISO/IEC TR 27016, Quản lý an toàn thông tin - Kinh tế của tổ chức (*Information security management - Organisational economics*).

6.2.2. Chu trình Plan-Do-Check-Act

Chuẩn ISO/IEC 27001:2005 chuyên về hệ thống quản lý an toàn thông tin cung cấp các chi tiết cho thực hiện chu kỳ Plan-Do-Check-Act gồm 4 pha: Plan - Lập kế hoạch, Do – Thực hiện kế hoạch, Check – Giám sát việc thực hiện và Act – Thực hiện các cải tiến, hiệu chỉnh, như biểu diễn trên Hình 6.3.



Hình 6.3. Chu trình Plan-Do-Check-Act của ISO/IEC 27001:2005

Theo đó, chi tiết các pha trong chu trình này như sau:

Pha **Plan** gồm các nội dung:

- Đề ra phạm vi của ISMS;
- Đề ra chính sách của ISMS;
- Đề ra hướng tiếp cận đánh giá rủi ro;
- Nhận dạng các rủi ro;
- Đánh giá rủi ro;
- Nhận dạng và đánh giá các lựa chọn phương pháp xử lý rủi ro;
- Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát;
- Chuẩn bị tuyển bối, báo cáo áp dụng.

Pha **Do** gồm các nội dung:

- Xây dựng kế hoạch xử lý rủi ro;
- Thực thi kế hoạch xử lý rủi ro;
- Thực thi các kiểm soát;
- Thực thi các chương trình đào tạo chuyên môn và giáo dục ý thức;
- Quản lý các hoạt động;
- Quản lý các tài nguyên;
- Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh.

Pha **Check** gồm các nội dung:

- Thực thi các thủ tục giám sát;
- Thực thi việc đánh giá thường xuyên tính hiệu quả của ISMS;
- Thực hiện việc kiểm toán (audit) nội bộ với ISMS;
- Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý;
- Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS.

Pha **Act** gồm các nội dung:

- Thực hiện các cải tiến đã được nhận dạng;
- Thực hiện các hành động sửa chữa và ngăn chặn;
- Áp dụng các bài đã được học;
- Thảo luận kết quả với các bên quan tâm;
- Đảm bảo các cải tiến đạt được các mục tiêu.

6.3. Pháp luật và chính sách an toàn thông tin

6.3.1. Khái quát

Các chính sách và pháp luật an toàn thông tin có vai trò rất quan trọng trong việc đảm bảo an toàn cho thông tin, hệ thống và mạng. Trong đó, vai trò của nhân viên đảm bảo an toàn thông tin là quan trọng nhất trong việc giảm thiểu rủi ro, đảm bảo an toàn cho hệ thống và giảm thiệt hại nếu xảy ra sự cố. Các nhân viên đảm bảo an toàn thông tin phải

hiểu rõ những khía cạnh pháp lý và vấn đề đạo đức an toàn thông tin. Theo đó, họ phải luôn nắm vững môi trường pháp lý hiện tại (gồm các luật và các quy định luật pháp trong lĩnh vực an toàn thông tin và công nghệ thông tin) và luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp. Ngoài ra, cần thực hiện việc giáo dục ý thức về luật pháp và đạo đức an toàn thông tin cho cán bộ quản lý và nhân viên trong tổ chức, đảm bảo sử dụng đúng mục đích các công nghệ đảm bảo an toàn thông tin.

Chính sách, còn gọi là quy định, nội quy là các quy định về các hành vi chấp nhận được của các nhân viên trong tổ chức tại nơi làm việc. Chính sách là các “luật” của tổ chức có giá trị thực thi trong nội bộ, gồm một tập các quy định và các chế tài xử phạt bắt buộc phải thực hiện. Các chính sách, hoặc nội quy cần được nghiên cứu, soạn thảo kỹ lưỡng. Đồng thời, chính sách cần đầy đủ, đúng đắn và áp dụng công bằng với mọi nhân viên. Điểm khác biệt giữa luật và chính sách là luật luôn bắt buộc, còn với chính sách, việc thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được.

Cần có phân biệt rõ ràng giữa *luật* (law) và *đạo đức* (ethic). Luật gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể. Các điều luật thường được xây dựng từ các vấn đề đạo đức. Trong khi đó, đạo đức định nghĩa những hành vi xã hội chấp nhận được. Đạo đức thường dựa trên các đặc điểm văn hóa. Do đó, hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau có thể khác nhau. Một số hành vi vi phạm đạo đức được luật hóa trên toàn thế giới, như trộm, cướp, cưỡng dâm, bạo hành trẻ em,... Khác biệt giữa luật và đạo đức thể hiện ở chỗ luật được thực thi bởi các cơ quan chính quyền, còn đạo đức không được thực thi bởi các cơ quan chính quyền.

Để các chính sách nói chung và chính sách an toàn thông tin nói riêng có thể được áp dụng hiệu quả, chúng phải đạt được các yêu cầu sau:

- Có khả năng phổ biến rộng rãi, bằng tài liệu giấy hoặc điện tử;
- Nhân viên có thể xem, hiểu được. Chính sách cần được thực hiện trên nhiều ngôn ngữ, ví dụ bằng tiếng Anh và tiếng địa phương;
- Chính sách cần rõ ràng dễ hiểu. Tổ chức cần có các điều tra/khảo sát về mức độ hiểu biết/nắm bắt các chính sách của nhân viên;
- Cần có biện pháp để nhân viên cam kết thực hiện, có thể thực hiện thông qua ký văn bản cam kết hoặc tích vào ô xác nhận tuân thủ;
- Chính sách cần được thực hiện đồng đều, bình đẳng, nhất quán, không có ưu tiên với bất kỳ nhân viên nào, kể cả người quản lý.

6.3.2. Luật quốc tế về an toàn thông tin

Mục này đề cập đến một số luật và văn bản có liên quan đến an toàn thông tin của Hoa Kỳ và Châu Âu – là những nước và khu vực đã phát triển và có hệ thống luật pháp về an toàn thông tin tương đối hoàn thiện.

Có thể nói hệ thống luật pháp về an toàn thông tin của Hoa Kỳ khá đầy đủ và được chia thành các nhóm: các luật tội phạm máy tính, các luật về sự riêng tư, luật xuất khẩu và chống gián điệp, luật bản quyền và luật tự do thông tin. Các luật về tội phạm máy tính bao gồm:

- Computer Fraud and Abuse Act of 1986 (CFA Act) quy định về các tội phạm lừa đảo và lạm dụng máy tính;
- Computer Security Act, 1987 đề ra các nguyên tắc đảm bảo an toàn cho hệ thống máy tính;
- National Information Infrastructure Protection Act of 1996 là bản sửa đổi của CFA Act, tăng khung hình phạt một số tội phạm máy tính đến 20 năm tù;
- USA PATRIOT Act, 2001 cho phép các cơ quan nhà nước một số quyền theo dõi, giám sát các hoạt động trên mạng nhằm phòng chống khủng bố hiệu quả hơn;
- USA PATRIOT Improvement and Reauthorization Act là mở rộng của USA PATRIOT Act, 2001, cấp cho các cơ quan nhà nước nhiều quyền hạn hơn cho nhiệm vụ phòng chống khủng bố.

Các luật về sự riêng tư nhằm bảo vệ quyền riêng tư của người dùng, bảo vệ các thông tin cá nhân của người dùng, bao gồm:

- Federal Privacy Act, 1974 là luật Liên bang Hoa Kỳ bảo vệ quyền riêng tư của người dùng máy tính và mạng Internet;
- Electronic Communications Privacy Act , 1986 là luật bảo vệ quyền riêng tư trong các giao tiếp điện tử;
- Health Insurance Portability and Accountability Act, 1996 (HIPAA) là luật bảo vệ tính bí mật và an toàn của các dữ liệu y tế của người bệnh. Tổ chức, hoặc cá nhân vi phạm có thể bị phạt đến 250.000 USD hoặc 10 năm tù;
- Financial Services Modernization Act or Gramm-Leach-Bliley Act, 1999 là luật điều chỉnh các hoạt động liên quan đến nhà nước của các ngân hàng, bảo hiểm và các hằng dịch vụ an ninh.

Các luật xuất khẩu và chống gián điệp hạn chế việc xuất khẩu các công nghệ và hệ thống xử lý thông tin và phòng chống gián điệp kinh tế, bao gồm:

- Economic Espionage Act, 1996 có nhiệm vụ phòng chống việc thực hiện giao dịch có liên quan đến bí mật kinh tế và công nghệ;
- Security and Freedom through Encryption Act, 1999 quy định về các vấn đề có liên quan đến sử dụng mã hóa trong đảm bảo an toàn và tự do thông tin.

U.S. Copyright Law là Luật bản quyền của Hoa Kỳ, điều chỉnh các vấn đề có liên quan đến xuất bản, quyền tác giả của các tài liệu, phần mềm, bao gồm cả các tài liệu số. Freedom of Information Act, 1966 (FOIA) là Luật tự do thông tin nêu rõ các cá nhân được truy cập các thông tin không gây tổn hại đến an ninh quốc gia.

Các tổ chức và luật quốc tế có liên quan đến an toàn thông tin, gồm:

- Hội đồng Châu Âu về chống tội phạm mạng (Council of Europe Convention on Cybercrime);
- Hiệp ước về chống tội phạm mạng được Hội đồng châu Âu phê chuẩn vào năm 2001;

- Hiệp ước bảo vệ quyền sở hữu trí tuệ (Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)): là hiệp ước do Tổ chức Thương mại thế giới WTO chủ trì đàm phán trong giai đoạn 1986–1994;
- Digital Millennium Copyright Act (DMCA) là Luật bản quyền số Thiên niên kỷ.

6.3.3. Luật Việt Nam về an toàn thông tin

6.3.3.1. Khái quát

Luật an toàn thông tin mạng được Quốc hội thông qua vào tháng 11 năm 2015 và chính thức có hiệu lực từ ngày 01/7/2016 và Luật an ninh mạng mạng được Quốc hội thông qua vào tháng 6 năm 2018 và chính thức có hiệu lực từ ngày 01/01/2019. Đây là các cơ sở pháp lý quan trọng cho việc quản lý các hoạt động liên quan đến an toàn, an ninh thông tin ở Việt Nam. Ngoài Luật an toàn thông tin mạng và Luật an ninh mạng, đã có nhiều văn bản có liên quan đến công nghệ thông tin và an toàn thông tin được Quốc hội, Chính phủ và các cơ quan nhà nước ban hành như:

- Luật công nghệ thông tin số 67/2006/QH11 của Quốc hội, ngày 12/07/2006.
- Nghị định số 90/2008/NĐ-CP của Chính phủ “Về chống thư rác”, ngày 13/08/2008.
- Quyết định số 59/2008/QĐ-BTTTT của Bộ Thông tin và Truyền thông “Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số”, ngày 31/12/2008.
- Quyết định 63/QĐ-TTg của Thủ tướng Chính phủ “Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020”, ngày 13/01/2010.
- Chỉ thị số 897/CT-TTg của Thủ tướng Chính phủ “V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số”, 10/06/2011.
- Thông tư số 23/2011/TT-BTTTT của Bộ TT&TT “Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước”, ngày 11/08/2011.
- Nghị định số 77/2012/NĐ-CP của Chính phủ “Sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 của Chính phủ về chống thư rác”, ngày 05/10/2012.
- Nghị định 72/2013/NĐ-CP của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng; quy định về việc chia sẻ thông tin trên các trang mạng xã hội.

6.3.3.2. Luật an toàn thông tin mạng

Luật an toàn thông tin mạng là bộ luật đầy đủ đầu tiên của Việt Nam về an toàn thông tin được Quốc hội khóa XIII thông qua tại Phiên họp thứ 10 vào ngày 19/12/2015 và chính thức có hiệu lực từ ngày 01/7/2016 [17]. Luật quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an

toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng. Đối tượng áp dụng của luật là các cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin mạng tại Việt Nam.

Luật an toàn thông tin gồm 8 chương và 54 điều với nội dung chính như sau:

- Chương I – Những quy định chung gồm 8 điều quy định phạm vi điều chỉnh, đối tượng áp dụng của luật; giải thích các từ ngữ, thuật ngữ; nguyên tắc bảo đảm an toàn thông tin mạng, chính sách của Nhà nước và vấn đề hợp tác quốc tế về an toàn thông tin mạng.
- Chương II – Bảo đảm an toàn thông tin mạng gồm 21 điều quy định về các vấn đề bảo vệ thông tin mạng, bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin và ngăn chặn xung đột thông tin trên mạng.
- Chương III – Mật mã dân sự gồm 7 điều quy định về các vấn đề có liên quan đến mật mã dân sự, bao gồm kinh doanh, xin cấp giấy phép kinh doanh, xuất khẩu nhập khẩu, sử dụng sản phẩm, dịch vụ mật mã dân sự.
- Chương IV – Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng gồm 3 điều quy định quản lý tiêu chuẩn, quy chuẩn kỹ thuật, đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng.
- Chương V – Kinh doanh trong lực vực an toàn thông tin mạng gồm 7 điều quy định về việc cấp giấy phép kinh doanh sản phẩm dịch vụ và quản lý nhập khẩu sản phẩm an toàn thông tin mạng.
- Chương VI – Phát triển nguồn nhân lực an toàn thông tin mạng gồm 2 điều quy định về đào tạo, bồi dưỡng nghiệp vụ và văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng.
- Chương VII – Quản lý nhà nước về an toàn thông tin mạng gồm 2 điều quy định các nội dung và trách nhiệm quản lý nhà nước về an toàn thông tin mạng.
- Chương VIII – Điều khoản thi hành gồm 2 điều quy định ngày bắt đầu có hiệu lực của luật và giao chính phủ và các cơ quan nhà nước ban hành các văn bản hướng dẫn chi tiết việc thực hiện.

6.3.3.3. Luật an ninh mạng

Tiếp theo Luật an toàn thông tin mạng, Luật an ninh mạng được Quốc hội khóa XIV thông qua tại Phiên họp thứ 5 vào ngày 12/6/2018 và chính thức có hiệu lực từ ngày 01/01/2019 [18]. Luật gồm 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Nội dung tóm tắt của luật như sau:

- Chương I – Những quy định chung gồm 9 điều quy định phạm vi điều chỉnh, đối tượng áp dụng của luật; giải thích các từ ngữ, thuật ngữ; nguyên tắc, biện pháp bảo vệ an ninh mạng, chính sách của Nhà nước và vấn đề hợp tác quốc tế về an ninh mạng; quy định các hành vi bị nghiêm cấm và xử lý vi phạm pháp luật về an ninh mạng.

- Chương II – Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia gồm 6 điều quy định về các vấn đề thẩm định, đánh giá điều kiện, kiểm tra, giám sát và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.
- Chương III – Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng gồm 7 điều quy định các vấn đề phòng ngừa và xử lý các hành vi xâm phạm an ninh mạng, bao gồm phòng ngừa và xử lý các hành vi tuyên truyền chống nhà nước, kích động bạo loạn, gây rối...; phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, quyền riêng tư của cá nhân; phòng, chống tấn công, khủng bố và các tình huống nguy hiểm trên mạng; và vấn đề đấu tranh bảo vệ an ninh mạng.
- Chương IV – Hoạt động bảo vệ an ninh mạng gồm 7 điều quy định về vấn đề bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, hệ thống thông tin của các cơ quan tổ chức; bảo đảm an ninh thông tin trên không gian mạng; vấn đề nghiên cứu, phát triển và nâng cao năng lực tự chủ về an ninh mạng; và vấn đề bảo vệ trẻ em trên không gian mạng.
- Chương V – Bảo đảm hoạt động bảo vệ an ninh mạng gồm 6 điều quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng, tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; vấn đề giáo dục, bồi dưỡng kiến thức, nghiệp vụ và phổ biến kiến thức an ninh mạng; và vấn đề kinh phí bảo vệ an ninh mạng.
- Chương VI – Trách nhiệm của cơ quan, tổ chức, cá nhân quy định trách nhiệm của các chủ thể trong đảm bảo an ninh mạng, bao gồm trách nhiệm của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, chính quyền các tỉnh, thành phố, các tổ chức và cá nhân.
- Chương VII – Điều khoản thi hành gồm 1 điều quy định ngày bắt đầu có hiệu lực của luật và yêu cầu về điều kiện an ninh mạng đối với hệ thống thông tin đang vận hành, sử dụng được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

6.4. Vấn đề đạo đức an toàn thông tin

Vấn đề đạo đức nghề nghiệp (Professional ethic) hay quy tắc ứng xử (Code of conduct) được đề cập trong ngành công nghệ thông tin nói chung và an toàn thông tin nói riêng do các công việc trong lĩnh vực an toàn thông tin có thể liên quan đến các thông tin nhạy cảm, như thông tin, hệ thống bí mật quốc gia, hoặc thông tin bí mật của các cơ quan, tổ chức, hoặc bí mật công nghệ, bí mật kinh doanh của các công ty. Nếu các thông tin nhạy cảm bị rò rỉ, hoặc bị đánh cắp và lạm dụng, có thể ảnh hưởng nghiêm trọng đến an ninh quốc gia, hoặc ảnh hưởng xấu đến các cơ quan, tổ chức và người dùng. Do vậy, người làm việc trong lĩnh vực an toàn thông tin cần có hiểu biết về chính sách, pháp luật và có thái độ và hành động đúng đắn trong khi thực thi nhiệm vụ.

6.4.1. Một số bộ quy tắc ứng xử trong CNTT và ATTT

Nhiều tổ chức xã hội nghề nghiệp đã ban hành các quy tắc ứng xử bắt buộc tại nơi làm việc, như với nghề luật sư, bác sĩ và vận động viên thể thao. Nếu vi phạm nghiêm trọng các quy tắc ứng xử tại nơi làm việc có thể bị cấm hành nghề có thời hạn, hoặc vĩnh viễn. Trong lĩnh vực công nghệ thông tin và an toàn thông tin, hiện không có bộ quy tắc ứng xử bắt buộc. Một số tổ chức xã hội nghề nghiệp như ACM (Association for Computing Machinery) và ISSA (Information Systems Security Association) đã hợp tác để đề ra các quy tắc ứng xử trong an toàn thông tin. Tuy nhiên, các quy tắc ứng xử trong an toàn thông tin chỉ có tính khuyến nghị do các tổ chức trên không có thẩm quyền bắt buộc phải thực hiện.

Hiệp hội an toàn thông tin Việt Nam đã công bố Bộ Qui tắc ứng xử an toàn thông tin vào đầu năm 2015, trong đó đưa ra một số quy tắc và khuyến nghị về những việc không được làm cho các thành viên và nhân viên của các tổ chức hoạt động trong lĩnh vực an toàn thông tin. Viện đạo đức máy tính, Hoa Kỳ đưa ra Bộ Quy tắc ứng xử 10 điểm (Ten Commandments of Computer Ethics) như sau:

1. Không được sử dụng máy tính để gây hại cho người khác;
2. Không được can thiệp vào công việc của người khác trên máy tính;
3. Không trộm cắp các file trên máy tính của người khác;
4. Không được sử dụng máy tính để trộm cắp;
5. Không được sử dụng máy tính để tạo bằng chứng giả;
6. Không sao chép hoặc sử dụng phần mềm không có bản quyền;
7. Không sử dụng các tài nguyên máy tính của người khác khi không được phép hoặc không có bồi thường thỏa đáng;
8. Không chiếm đoạt tài sản trí tuệ của người khác;
9. Nên suy nghĩ về các hậu quả xã hội của chương trình mình đang xây dựng hoặc hệ thống đang thiết kế;
10. Nên sử dụng máy tính một cách có trách nhiệm, đảm bảo sự quan tâm và tôn trọng đến đồng bào của mình.

6.4.2. Một số vấn đề khác

Liên quan đến vấn đề đạo đức trong an toàn thông tin, có một số vấn đề khác cần lưu ý bao gồm: (1) sự khác biệt về vấn đề đạo đức giữa các nền văn hóa, (2) vấn đề vi phạm bản quyền phần mềm và nội dung số và (3) vấn đề lạm dụng các tài nguyên của cơ quan, tổ chức.

Trên thực tế, có sự khác biệt khá lớn về vấn đề đạo đức giữa các nền văn hóa. Trong đó, nhận thức về vấn đề đạo đức trong sử dụng các tài nguyên của cơ quan, tổ chức là rất khác biệt giữa các quốc gia có nền văn hóa khác nhau. Trong nhiều trường hợp, một hành vi được phép của một số cá nhân trong một quốc gia lại vi phạm quy tắc đạo đức của quốc gia khác. Chẳng hạn, hành vi tiết lộ thông tin cá nhân và đặc biệt là mức thu nhập của người khác được coi là bình thường ở Việt Nam, nhưng đây là hành vi vi phạm quyền riêng tư ở các nước phát triển như Hoa Kỳ và Châu Âu.

Vấn đề vi phạm bản quyền phần mềm và nội dung số là rất nghiêm trọng, đặc biệt là ở các nước đang phát triển ở châu Á và châu Phi. Đa số người dùng có hiểu biết về vấn đề bản quyền phần mềm và nội dung số, nhưng coi việc sử dụng phần mềm bất hợp pháp là bình thường vì nhiều nước chưa có quy định, hoặc không xử lý nghiêm vi phạm. Tỷ lệ vi phạm bản quyền phần mềm ở Việt Nam hiện rất cao, đến khoảng 90% do các chế tài xử lý vi phạm chưa đầy đủ, hoặc chế tài xử lý chưa được thực hiện nghiêm minh và chưa đủ sức răn đe.

Vấn đề lạm dụng các tài nguyên của công ty, tổ chức xảy ra tương đối phổ biến và cần có các quy định và chế tài để kiểm soát. Một số cơ quan, tổ chức chưa có các quy định cấm nhân viên sử dụng các tài nguyên của cơ quan, tổ chức vào việc riêng. Một số đơn vị khác có quy định nhưng chưa được thực thi chặt chẽ và chưa có chế tài xử phạt nghiêm minh. Các hành vi lạm dụng các tài nguyên của công ty, tổ chức thường gặp bao gồm:

- In ấn tài liệu riêng;
- Sử dụng email cá nhân cho việc riêng;
- Tải các tài liệu, file không được phép;
- Cài đặt và chạy các chương trình, phần mềm không được phép;
- Sử dụng máy tính công ty làm việc riêng;
- Sử dụng các phương tiện làm việc khác như điện thoại công ty quá mức vào việc riêng.

6.5. Kết chương

Chương này đã trình bày khái quát về quản lý, chính sách, pháp luật và đạo đức an toàn thông tin. Cụ thể các vấn đề sau đã được đề cập:

- Trình bày khái quát về quản lý an toàn thông tin, vấn đề quản lý rủi ro an toàn thông tin, bao gồm nhận dạng rủi ro và các hướng tiếp cận đánh giá rủi ro an toàn thông tin và vấn đề thực thi quản lý an toàn thông tin đảm bảo các kiểm soát được lựa chọn và thực thi nhằm đưa mức rủi ro đối với các tài sản an toàn thông tin về mức chấp nhận được với chi phí phù hợp.
- Mô tả khái quát về bộ chuẩn quản lý an toàn thông tin ISO 27000, một số chuẩn con và bộ tiêu chuẩn quản lý an toàn thông tin tương ứng của Việt Nam.
- Giới thiệu khái quát về vấn đề chính sách và pháp luật an toàn thông tin trên thế giới và ở Việt Nam.
- Giới thiệu khái quát về vấn đề đạo đức an toàn thông tin và các bộ quy tắc ứng xử trong công nghệ thông tin và an toàn thông tin.

6.6. Câu hỏi ôn tập

- 1) Nêu khái niệm tài sản an toàn thông tin, khái niệm quản lý an toàn thông tin. Nêu vai trò và các khâu cần thực hiện của quản lý an toàn thông tin.
- 2) Đánh giá rủi ro an toàn thông tin là gì? Mô tả các phương pháp tiếp cận đánh giá rủi ro an toàn thông tin.

- 3) Rủi ro an toàn thông tin có liên quan đến những nhũng yếu tố nào? Giải thích.
- 4) Mô tả các bước của phân tích chi tiết rủi ro an toàn thông tin.
- 5) Mô tả các loại kiểm soát trong thực thi quản lý an toàn thông tin.
- 6) Mô tả nội dung thực thi quản lý an toàn thông tin.
- 7) Mô tả văn tắt các chuẩn ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 và ISO/IEC 27005.
- 8) Mô tả chu trình Plan-Do-Check-Act của chuẩn ISO/IEC 27001.
- 9) Khảo sát tài liệu, tìm hiểu các nội dung chính của bộ chuẩn NIST SP 800.
- 10) Phân biệt pháp luật và chính sách. Nêu các yêu cầu của chính sách để có thể được áp dụng hiệu quả.
- 11) Mô tả văn tắt các văn bản luật có liên quan đến an toàn thông tin của Việt Nam.
- 12) Tìm hiểu và nêu các nội dung cơ bản của Luật an toàn thông tin mạng số 86/2015/QH13.
- 13) Tìm hiểu và nêu các nội dung cơ bản của Luật an ninh mạng số 24/2018/QH14.
- 14) Nêu sự cần thiết của vấn đề đạo đức an toàn thông tin. Nêu bộ qui tắc ứng xử của Viện đạo đức máy tính Hoa Kỳ.
- 15) Nhiều người dùng trên các mạng xã hội, hoặc các nhóm chat đăng, hoặc chia sẻ các thông tin sai sự thật, hoặc giật gân nhằm mục đích “câu” like, view, hoặc mục đích trực lợi khác. Nhũng người này đã vi phạm vào nội dung/điều khoản nào của văn bản luật pháp nào?

TÀI LIỆU THAM KHẢO

- [1] Michael E. Whitman, Herbert J. Mattord, *Principles of information security*, 4th edition, Course Technology, Cengage Learning, 2012.
- [2] David Kim, Michael G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlettlearning, 2012.
- [3] Statista.com, *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*, <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>, truy cập tháng 3.2020.
- [4] Statista.com, *Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2018*, <https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/>, truy cập tháng 3.2020.
- [5] Tập đoàn Bkav, Tổng kết an ninh mạng 2019 và dự báo xu hướng 2020, https://m.bkav.com.vn/tin_tuc_noi_bat/-/chi_tiet/669034/tong-ket-an-ninh-mang-nam-2019-va-du-bao-2020, truy cập tháng 3.2020.
- [6] Realtime Technologies, The Latest Cyber Security Trends, <https://realtimetech.net/latest-cyber-security-trends/>, truy cập tháng 2.2020.
- [7] US National Vulnerability Database, <https://nvd.nist.gov>, truy cập tháng 8.2018.
- [8] Boni, W. C., & Kovacich, G. L. *I-way robbery: crime on the Internet*, Boston MA: Butterworth, 1999.
- [9] Butler, J. G.. *Contingency planning and disaster recovery: protecting your organisation's resources*. New York: Computer Tech Research, 1998.
- [10] Denning D. E.. *Information warfare and security*, New York. Addison-Wesley, 1999.
- [11] Erbschloe, M. & Vacca, J. R.. *Information warfare*. New York: McGraw-Hill, 2001.
- [12] Ghosh, A.. *E-Commerce security – weak links, best defenses*. New York: Wiley Computer Publishing, 1998.
- [13] Hutchinson, W. & Warren, M.. *Information warfare: corporate attack and defence in the digital age*. Oxford: Butterworth-Heinneman, 2001.
- [14] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Fifth Printing, August 2001.
- [15] Bruce Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, 1996.
- [16] Schneier, B.. *Secrets and lies: digital security in a networked world*. New York: John Wiley and Sons, 2000.
- [17] Quốc hội, Luật an toàn thông tin mạng, Luật số: 86/2015/QH13, 2015.
- [18] Quốc hội, Luật an ninh mạng, Luật số: 24/2018/QH14, 2018.
- [19] TCVN 11238 (ISO/IEC 27000), Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng (Information security management systems - Overview and vocabulary).

- [20] TCVN ISO/IEC 27001 (ISO/IEC 27001), Hệ thống quản lý an toàn thông tin - Các yêu cầu (ISO/IEC 27001 Information security management systems - Requirements).
- [21] TCVN ISO/IEC 27002 (ISO/IEC 27002), Quy tắc thực hành cho hệ thống quản lý an toàn thông tin (Code of practice for information security management).
- [22] TCVN 10295 (ISO/IEC 27005), Quản lý rủi ro an toàn thông tin (Information security risk management).
- [23] Eric Cole, Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Elsevier, USA, 2013.
- [24] Nguyễn Khanh Văn, Giáo trình Cơ sở an toàn thông tin, Đại học Bách khoa Hà Nội, 2014.
- [25] Thái Thanh Tùng, Giáo trình Mật mã học và An toàn thông tin, NXB Thông tin và Truyền thông, 2011.
- [26] William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2016.
- [27] Peter Gregory, CISSP Guide to Security Essentials, 2nd Edition, Cengage Learning, 2014.
- [28] New Signature, E is for E5, <https://newsignature.com/articles/e-is-for-e5/>, truy cập tháng 3.2020.
- [29] Siemens, Operational Guidelines for Industrial Security, <https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf>, truy cập tháng 3.2020.