

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



HOÀNG XUÂN DẬU

**BÀI GIẢNG
AN TOÀN VÀ BẢO MẬT
HỆ THỐNG THÔNG TIN**

HÀ NỘI 2021

MỤC LỤC

DANH MỤC CÁC HÌNH	4
DANH MỤC CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT	7
MỞ ĐẦU	8
CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN	10
1.1. Khái quát về an toàn thông tin	10
1.1.1. An toàn thông tin là gì?	10
1.1.2. Sự cần thiết của an toàn thông tin	11
1.1.3. Các thành phần của an toàn thông tin	13
1.2. Khái quát về an toàn hệ thống thông tin	15
1.2.1. Các thành phần của hệ thống thông tin	15
1.2.2. An toàn hệ thống thông tin là gì?	16
1.3. Các yêu cầu đảm bảo an toàn hệ thống thông tin	16
1.3.1. Tính bí mật	16
1.3.2. Toàn vẹn	17
1.3.3. Sẵn dùng	17
1.4. Bảy vùng trong hạ tầng CNTT và các mối đe dọa	18
1.4.1. Bảy vùng trong cơ sở hạ tầng CNTT	18
1.4.2. Các mối đe dọa và nguy cơ	19
1.5. Mô hình tổng quát đảm bảo an toàn hệ thống thông tin	20
1.5.1. Giới thiệu	20
1.5.2. Một số mô hình đảm bảo an toàn hệ thống thông tin	21
1.6. Câu hỏi ôn tập	22
CHƯƠNG 2. CÁC DẠNG TẤN CÔNG VÀ PHẦN MỀM ĐỘC HẠI	23
2.1. Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công	23
2.1.1. Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công	23
2.1.2. Các dạng mối đe dọa thường gặp	24
2.1.3. Các loại tấn công	25
2.2. Các công cụ hỗ trợ tấn công	25
2.2.1. Công cụ rà quét lỗ hổng, điểm yếu hệ thống	26
2.2.2. Công cụ quét cổng dịch vụ	27
2.2.3. Công cụ nghe lén	27
2.2.4. Công cụ ghi phím gõ	28
2.3. Các dạng tấn công thường gặp	29
2.3.1. Tấn công vào mật khẩu	29
2.3.2. Tấn công bằng mã độc	30
2.3.3. Tấn công từ chối dịch vụ	44
2.3.4. Tấn công từ chối dịch vụ phân tán	47
2.3.5. Tấn công giả mạo địa chỉ	49
2.3.6. Tấn công nghe lén	50
2.3.7. Tấn công kiểu người đứng giữa	51

2.3.8. Tấn công bằng bom thư và thư rác.....	52
2.3.9. Tấn công sử dụng các kỹ thuật xã hội.....	52
2.3.10. Tấn công pharming.....	55
2.3.11. Tấn công APT	56
2.4. Các dạng phần mềm độc hại	57
2.4.1. Phân loại.....	58
2.4.2. Mô tả các dạng phần mềm độc hại.....	59
2.4.3. Phòng chống phần mềm độc hại	64
2.5. Câu hỏi ôn tập	66
CHƯƠNG 3. ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA	67
3.1. Khái quát về mã hóa thông tin và ứng dụng.....	67
3.1.1. Các khái niệm.....	67
3.1.2. Các thành phần của một hệ mã hóa.....	69
3.1.3. Lịch sử mã hóa	70
3.1.4. Mã hóa dòng và mã hóa khối	71
3.1.5. Ứng dụng của mã hóa.....	72
3.2. Các phương pháp mã hóa	72
3.2.1. Phương pháp thay thế.....	72
3.2.2. Phương pháp hoán vị.....	73
3.2.3. Phương pháp XOR	73
3.2.4. Phương pháp Vernam.....	74
3.2.5. Phương pháp sách hoặc khóa chạy.....	74
3.2.6. Phương pháp hàm băm.....	74
3.3. Các giải thuật mã hóa	75
3.3.1. Các giải thuật mã hóa khóa đối xứng	75
3.3.2. Các giải thuật mã hóa khóa bất đối xứng	83
3.3.3. Các hàm băm	86
3.4. Chữ ký số, chứng chỉ số và PKI.....	91
3.4.1. Chữ ký số	91
3.4.2. Chứng chỉ số.....	95
3.4.3. PKI	97
3.5. Quản lý khóa và phân phối khóa	98
3.5.1. Giới thiệu.....	98
3.5.2. Phân phối khóa bí mật.....	100
3.5.3. Phân phối khóa công khai	103
3.6. Một số giao thức đảm bảo ATTT dựa trên mã hóa	105
3.6.1. SSL/TLS.....	105
3.6.2. SET.....	108
3.6.3. PGP.....	109
3.7. Câu hỏi ôn tập	112
CHƯƠNG 4. CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐẢM BẢO AN TOÀN THÔNG TIN ...	114
4.1. Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT	114
4.2. Kiểm soát truy cập.....	115
4.2.1. Khái niệm kiểm soát truy cập.....	115

4.2.2. Các biện pháp kiểm soát truy cập.....	116
4.2.3. Một số công nghệ kiểm soát truy cập.....	121
4.3. Tường lửa	126
4.3.1. Giới thiệu tường lửa	126
4.3.2. Các loại tường lửa	128
4.3.3. Các kỹ thuật kiểm soát truy cập	129
4.3.4. Các hạn chế của tường lửa	130
4.4. Các hệ thống phát hiện và ngăn chặn xâm nhập	130
4.4.1. Giới thiệu.....	130
4.4.2. Phân loại.....	131
4.4.3. Các kỹ thuật phát hiện xâm nhập	132
4.5. Câu hỏi ôn tập	134
CHƯƠNG 5. QUẢN LÝ, CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN	136
5.1. Quản lý an toàn thông tin	136
5.1.1. Khái quát về quản lý an toàn thông tin.....	136
5.1.2. Đánh giá rủi ro an toàn thông tin	137
5.1.3. Phân tích chi tiết rủi ro an toàn thông tin	139
5.1.4. Thực thi quản lý an toàn thông tin	142
5.2. Các chuẩn quản lý an toàn thông tin	144
5.2.1. Giới thiệu.....	144
5.2.2. Chu trình Plan-Do-Check-Act.....	145
5.3. Pháp luật và chính sách an toàn thông tin	146
5.3.1. Giới thiệu về pháp luật và chính sách an toàn thông tin	146
5.3.2. Luật quốc tế về an toàn thông tin	147
5.3.3. Luật Việt Nam về an toàn thông tin	148
5.4. Vấn đề đạo đức an toàn thông tin.....	149
5.4.1. Sự cần thiết của đạo đức an toàn thông tin	149
5.4.2. Một số bộ quy tắc ứng xử trong CNTT và ATTT	149
5.4.3. Một số vấn đề khác.....	150
5.5. Câu hỏi ôn tập	151
TÀI LIỆU THAM KHẢO	152

DANH MỤC CÁC HÌNH

Hình 1.1. Các thuộc tính cần bảo vệ của tài sản thông tin: Bí mật (C), Toàn vẹn (I) và Sẵn dùng (A)	10
Hình 1.2. Thống kê và dự báo số lượng các thiết bị IoT kết nối Internet từ 2015 đến 2025	11
Hình 1.3. Số lượng sự cố mất ATTT báo cáo bởi các cơ quan chính phủ Hoa Kỳ giai đoạn 2006-2018 [3]	12
Hình 1.4. Các thành phần chính của An toàn thông tin	13
Hình 1.5. Chu trình quản lý an toàn thông tin	14
Hình 1.6. Chính sách an toàn thông tin	14
Hình 1.7. Mô hình hệ thống thông tin của cơ quan, tổ chức	15
Hình 1.8. Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin	16
Hình 1.9. Một văn bản được đóng dấu Confidential (Mật)	17
Hình 1.10. Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa	17
Hình 1.11. Minh họa tính sẵn dùng: (a) không đảm bảo và (b) đảm bảo tính sẵn dùng	18
Hình 1.12. Bảy vùng trong hạ tầng CNTT theo mức kết nối mạng	18
Hình 1.13. Đảm bảo ATTT cần cân bằng giữa mức An toàn, Chi phí và tính Hữu dụng	21
Hình 1.14. Mô hình đảm bảo an toàn thông tin với bảy lớp	21
Hình 1.15. Mô hình đảm bảo an toàn thông tin với ba lớp chính	22
Hình 2.1. Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống	24
Hình 2.2. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng	24
Hình 2.3. Báo cáo kết quả quét của Microsoft Baseline Security Analyzer	26
Hình 2.4. Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner	27
Hình 2.5. Giao diện của công cụ Zenmap	28
Hình 2.6. Sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm	28
Hình 2.7. Mô đun Keylogger phần cứng và cài đặt trên máy tính để bàn	29
Hình 2.8. Các vùng bộ nhớ cấp cho chương trình	32
Hình 2.9. Một chương trình minh họa cấp phát bộ nhớ trong ngăn xếp	32
Hình 2.10. Các thành phần được lưu trong vùng bộ nhớ trong ngăn xếp	33
Hình 2.11. Cấp phát bộ nhớ cho các biến nhớ trong vùng bộ nhớ trong ngăn xếp	33
Hình 2.12. Một chương trình minh họa gây tràn bộ nhớ đệm trong ngăn xếp	33
Hình 2.13. Minh họa hiện tượng tràn bộ nhớ đệm trong ngăn xếp	34
Hình 2.14. Một shellcode viết bằng hợp ngữ và chuyển thành chuỗi tấn công	35
Hình 2.15. Chèn và thực hiện shellcode khai thác lỗ tràn bộ đệm	35
Hình 2.16. Chèn shellcode với phần đệm bằng lệnh NOP (N)	35
Hình 2.17. Bản đồ lây nhiễm sâu Slammer (màu xanh) theo trang www.caida.org vào ngày 25/1/2003 lúc 6h00 (giờ UTC) với 74.855 máy chủ bị nhiễm	36
Hình 2.18. Cung cấp dữ liệu quá lớn để gây lỗi cho ứng dụng	38
Hình 2.19. Form đăng nhập (log on) và đoạn mã xử lý xác thực người dùng	40
Hình 2.20. Form tìm kiếm sản phẩm và đoạn mã xử lý tìm sản phẩm	41
Hình 2.21. (a) Thủ tục bắt tay 3 bước của TCP và (b) Tấn công SYN Flood	45
Hình 2.22. Mô hình tấn công Smurf	46
Hình 2.23. Kiến trúc tấn công DDoS trực tiếp	48
Hình 2.24. Kiến trúc tấn công DDoS gián tiếp hay phản xạ	48
Hình 2.25. Minh họa tấn công giả mạo địa chỉ IP	50

Hình 2.26. Một mô hình tấn công nghe lén.....	50
Hình 2.27. Mô hình chung của tấn công kiểu người đứng giữa.....	51
Hình 2.28. Một kịch bản tấn công kiểu người đứng giữa	51
Hình 2.29. Một phishing email gửi cho khách hàng của mạng đấu giá eBay	54
Hình 2.30. Một phishing email gửi cho khách hàng của ngân hàng Royal Bank	54
Hình 2.31. Tấn công pharming "cướp" trình duyệt.....	55
Hình 2.32. Tấn công pharming thông qua tấn công vào máy chủ DNS.....	56
Hình 2.33. Các dạng phần mềm độc hại	58
Hình 2.34. Chèn và gọi thực hiện mã vi rút	60
Hình 2.35. Một email do vi rút gửi đến người dùng	61
Hình 2.36. Một mô hình lây lan của sâu mạng	62
Hình 2.37. Mô hình mô hình giao tiếp giữa các thành phần trong botnet.....	63
Hình 2.38. Mô hình tin tặc sử dụng các máy tính Zombie/Bot để gửi thư rác.....	63
Hình 2.39. Màn hình chính của Microsoft Windows Defender	65
Hình 3.1. Các khâu Mã hóa và Giải mã của một hệ mã hóa	68
Hình 3.2. Mã hóa khóa đối xứng sử dụng chung 1 khóa bí mật	68
Hình 3.3. Mã hóa khóa bất đối xứng sử dụng một cặp khóa.....	69
Hình 3.4. Minh họa đầu vào (Input) và đầu ra (Digest) của hàm băm.....	69
Hình 3.5. Các thành phần của một hệ mã hóa đơn giản.....	70
Hình 3.6. Mô hình phương pháp mã hóa dòng	71
Hình 3.7. Mô hình phương pháp mã hóa khối	71
Hình 3.8. Mã hóa bằng hệ mã hóa Caesar cipher.....	72
Hình 3.9. Phương pháp thay thế với 4 bộ chữ mã.....	73
Hình 3.10. Phương pháp hoán vị thực hiện đổi chỗ các bit	73
Hình 3.11. Phương pháp hoán vị thực hiện đổi chỗ các ký tự	73
Hình 3.12. Ví dụ mã hóa bằng phương pháp XOR	73
Hình 3.13. Mã hóa bằng phương pháp Vernam	74
Hình 3.14. Các khâu mã hóa và giải mã của DES	76
Hình 3.15. Thủ tục sinh các khóa phụ từ khóa chính của DES.....	77
Hình 3.16. Các bước xử lý chuyển khối rõ 64 bit thành khối mã 64 bit của DES.....	77
Hình 3.17. Các bước xử lý của hàm Feistel (F)	78
Hình 3.18. Mã hóa và giải mã với giải thuật 3-DES	79
Hình 3.19. Các bước xử lý mã hóa dữ liệu của AES	80
Hình 3.20. Thủ tục sinh khóa Rijndael.....	81
Hình 3.21. Hàm SubBytes sử dụng Rijndael S-box	82
Hình 3.22. Hàm ShiftRows	82
Hình 3.23. Hàm MixColumns	82
Hình 3.24. Hàm AddRoundKey	82
Hình 3.25. Quá trình mã hóa và giải mã trong AES	83
Hình 3.26. Mô hình nén thông tin của hàm băm.....	86
Hình 3.27. Phân loại các hàm băm theo khóa sử dụng	87
Hình 3.28. Mô hình tổng quát xử lý dữ liệu của hàm băm	88
Hình 3.29. Mô hình chi tiết xử lý dữ liệu của hàm băm	88
Hình 3.30. Lưu đồ xử lý một thao tác của MD5	90
Hình 3.31. Lưu đồ một vòng xử lý của SHA1	91
Hình 3.32. Quá trình tạo chữ ký số và kiểm tra chữ ký số.....	92

Hình 3.33. Giao diện kiểm tra thông tin một chứng chỉ số	95
Hình 3.34. Nội dung chi tiết của một chứng chỉ số.....	96
Hình 3.35. Lưu đồ cấp và sử dụng chứng chỉ số trong PKI.....	97
Hình 3.36. Phân phối khóa điểm – điểm	101
Hình 3.37. Mô hình hoạt động của trung tâm phân phối khóa – KDC	101
Hình 3.38. Mô hình hoạt động của trung tâm dịch chuyển khóa – KTC	102
Hình 3.39. SSL/TLS trong bộ giao thức TCP/IP	105
Hình 3.40. Các giao thức con của SSL/TLS	105
Hình 3.41. Mô hình truyền thông giữa Web Server và Browser dựa trên SSL/TLS	106
Hình 3.42. Khởi tạo phiên làm việc trong SSL/TLS.....	107
Hình 3.43. Quá trình xử lý dữ liệu bởi SSL Record tại bên gửi	108
Hình 3.44. Một mô hình tương tác giữa các thực thể tham gia SET	109
Hình 3.45. Mô hình PGP chỉ đảm bảo tính xác thực thông điệp.....	110
Hình 3.46. Mô hình PGP chỉ đảm bảo tính bí mật thông điệp	111
Hình 3.47. Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp.....	112
Hình 4.1. Các kỹ thuật và công nghệ bảo mật trong các lĩnh vực của ATTT	114
Hình 4.2. Mô hình ma trận kiểm soát truy cập.....	117
Hình 4.3. Mô hình danh sách kiểm soát truy cập	117
Hình 4.4. Mô hình kiểm soát truy cập Bell-LaPadula.....	119
Hình 4.5. Một mô hình RBAC đơn giản	120
Hình 4.6. Một số luật của tường lửa lọc gói tin	121
Hình 4.7. Giao diện kiểm tra thông tin của một chứng chỉ số khóa công khai	123
Hình 4.8. Thẻ thông minh tiếp xúc (a) và thẻ không tiếp xúc (b)	123
Hình 4.9. Một số thẻ bài (Token) của hãng RSA Security.....	124
Hình 4.10. Ví điện tử (một dạng thẻ bài) của công thanh toán trực tuyến Paypal	124
Hình 4.11. Hệ thống ApplePay tích hợp vào điện thoại di động	124
Hình 4.12. (a) Khóa vân tay, (b) Khe xác thực vân tay trên laptop và (c) Xác thực vân tay trên điện thoại thông minh Samsung	125
Hình 4.13. Quét võng mạc nhận dạng tròng mắt	125
Hình 4.14. Một tường lửa phần cứng chuyên dụng của Cisco	126
Hình 4.15. Tường lửa bảo vệ mạng gia đình hoặc văn phòng nhỏ	127
Hình 4.16. Tường lửa bảo vệ các máy chủ dịch vụ.....	127
Hình 4.17. Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm	127
Hình 4.18. Mô hình tường lửa lọc gói (a), Cổng ứng dụng (b) và Cổng chuyển mạch (c).....	128
Hình 4.19. Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động.....	129
Hình 4.20. Vị trí các hệ thống IDS và IPS trong sơ đồ mạng	130
Hình 4.21. Các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng	131
Hình 4.22. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host	132
Hình 4.23. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký	133
Hình 4.24. 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)	134
Hình 5.1. Quan hệ giữa các khâu trong quản lý an toàn thông tin	137
Hình 5.2. Mô hình đánh giá rủi ro an toàn thông tin.....	137
Hình 5.3. Chu trình Plan-Do-Check-Act của ISO/IEC 27001:2005	145

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
ATTT	Information Security	An toàn thông tin
CNTT	Information Technology	Công nghệ thông tin
CRC	Cyclic redundancy checks	Kiểm tra dư thừa vòng
DAC	Discretionary Access Control	Kiểm soát truy cập tự ý chọn
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DNS	Domain Name System	Hệ thống tên miền
FTP	File Transfer Protocol	Giao thức truyền file
HTTT	Information System	Hệ thống thông tin
IDEA	International Data Encryption Algorithm	Giải thuật mã hóa dữ liệu quốc tế
IPSec	Internet Protocol Security	An toàn giao thức Internet
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 Mỹ
PGP	Pretty Good Privacy	Chuẩn bảo mật PGP
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
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
WAN	Wide Area Network	Mạng diện rộng
WLAN	Wireless Local Area Network	Mạng cục bộ không dây

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 và đặc biệt các dạng tấn công, xâm nhập các hệ thống máy tính và mạng xuất hiện ngày càng phổ biến và 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 nhập, 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 bí mật, tính toàn vẹn và tính sẵn dùng 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 thành phần chính: An toàn máy tính và dữ liệu, An ninh mạng và Quản lý an toàn thông tin.

Môn học An toàn và bảo mật hệ thống thông tin là môn học cơ sở chuyên ngành trong chương trình đào tạo đại học ngành Công nghệ thông tin của Học viện Công nghệ Bưu chính Viễn thông. Mục tiêu của môn học là cung cấp cho sinh viên các khái niệm và nguyên tắc cơ bản về đảm bảo an toàn thông tin, an toàn máy tính và an toàn hệ thống thông tin; các khái niệm về nguy cơ gây mất an toàn, các điểm yếu và các lỗ hổng bảo mật tồn tại trong hệ thống; các dạng tấn công, xâm nhập thường gặp vào hệ thống máy tính và mạng; các dạng phần mềm độc hại; các giải pháp, kỹ thuật 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 về an toàn và bảo mật thông tin và hệ thống, tác giả cố gắng trình bày những vấn đề cơ sở nhất phục vụ mục tiêu môn học. Nội dung của tài liệu bài giảng được biên soạn thành 5 chương với tóm tắt nội dung như sau:

Chương 1- Tổng quan về an toàn và bảo mật hệ thống 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 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 hệ thống thông tin.

Chương 2- Các dạng tấn công và phần mềm độc hại giới thiệu khái quát về mối đe dọa, điểm yếu, lỗ hổng tồn tại trong hệ thống và tấn công. Phần tiếp theo phân tích chi tiết 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,... Nửa cuối của chương đề cập đến các dạng phần mềm độc hại, gồm cơ chế lây nhiễm, tác hại và phòng chống.

Chương 3 – 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 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), các hàm băm (MD5 và SHA1), chữ ký số, chứng chỉ số và PKI. Phần cuối của chương đề cập vấn đề quản lý và phân phối khóa, và một số giao thức đảm bảo an toàn thông tin dựa trên mã hóa.

Chương 4- Các kỹ thuật và công nghệ đảm bảo an toàn thông tin giới thiệu khái quát về các kỹ thuật và công nghệ đảm bảo an toàn thông tin, vấn đề 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 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 và ngăn chặn xâm nhập.

Chương 5 – 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 là 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.

Tài liệu được biên soạn dựa trên kinh nghiệm giảng dạy môn học An toàn và bảo mật hệ thống 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 ngành Công nghệ thông tin. Trong quá trình biên soạn và hiệu chỉnh, 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 hơn nữa nội dung của tài liệu.

Hà Nội, Tháng 12 năm 2021

Tác giả

TS. Hoàng Xuân Dậu

CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

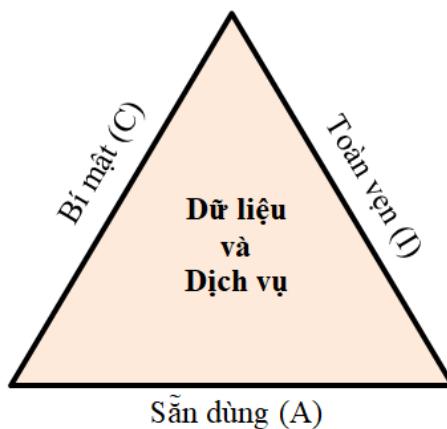
Chương 1 giới thiệu các khái niệm về an toàn thông tin, an toàn hệ thống thông tin và các yêu cầu đảm bảo an toàn thông tin và an toàn hệ thống thông tin. Chương này cũng đề cập các rủi ro và nguy cơ trong các vùng của hạ tầng công nghệ thông tin theo mức kết nối mạng. Phần cuối của chương giới thiệu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

1.1. Khái quát về an toàn thông tin

1.1.1. An toàn thông tin là gì?

An toàn thông tin (Information security) là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép, Viện SAN, Hoa Kỳ (<https://www.sans.org/information-security/>).

Theo cuốn Principles of Information Security, An toàn thông tin là việc bảo vệ các thuộc tính *bí mật*, *tính toàn vẹn* và *tính sẵn dùng* của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải. Hình 1.1 minh họa ba thuộc tính cần bảo vệ nói trên của các tài sản thông tin, bao gồm dữ liệu và dịch vụ trong tam giác CIA (Confidentiality - Integrity - Availability).



Hình 1.1. Các thuộc tính cần bảo vệ của tài sản thông tin: *Bí mật (C)*, *Toàn vẹn (I)* và *Sẵn dùng (A)*

An toàn thông tin gồm hai lĩnh vực chính là *An toàn công nghệ thông tin* (Information technology security, hay IT security) và *Đảm bảo thông tin* (Information assurance). An toàn công nghệ thông tin, hay còn gọi là *An toàn máy tính* (Computer security) 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. Đảm bảo thông tin là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố, như thiên tai, hỏa hoạn, 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 thiết bị lưu trữ vật lý đặt ở một vị trí khác.

Một số khái niệm khác trong an toàn thông tin:

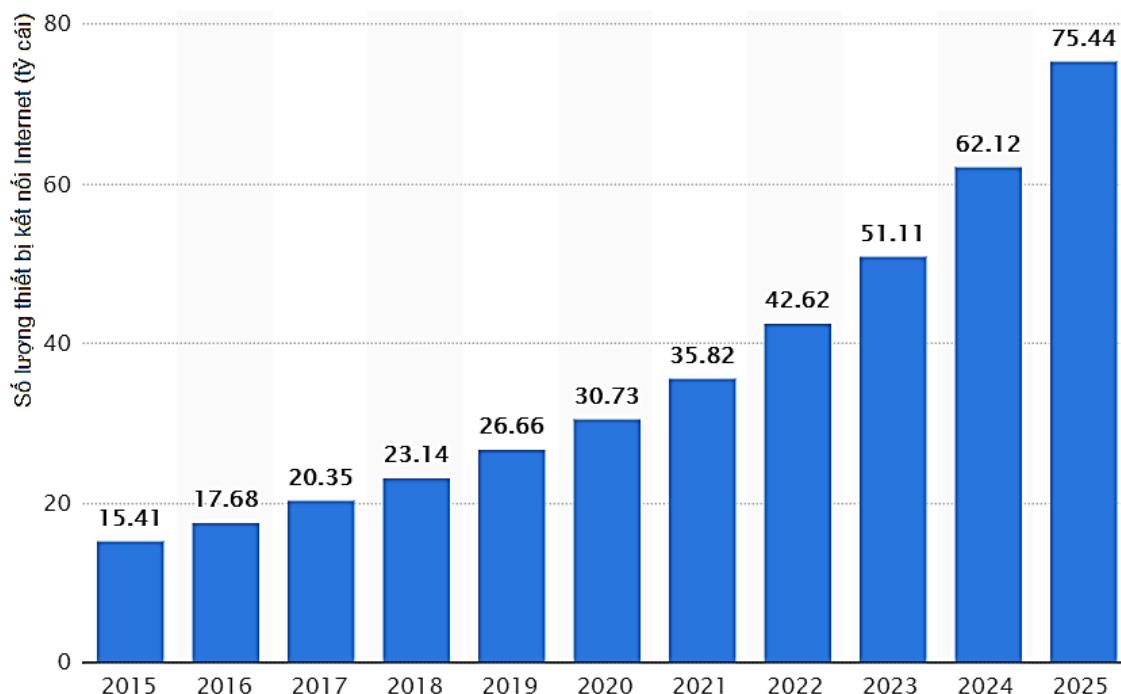
Truy cập (Access) là việc một chủ thể, người dùng hoặc một đối tượng có khả năng sử dụng, xử lý, sửa đổi, hoặc gây ảnh hưởng đến một chủ thể, người dùng hoặc một đối tượng khác. Trong khi người dùng hợp pháp có quyền truy cập hợp pháp đến một hệ thống thì tin tức truy cập bất hợp pháp đến hệ thống.

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 có thể là tài sản vật lý, như hệ thống máy tính, thiết bị mạng, hoặc các tài sản khác.

Tấn công (Attack) là 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 chủ động hoặc thụ động, trực tiếp hoặc gián tiếp.

1.1.2. Sự cần thiết của an toàn thông tin

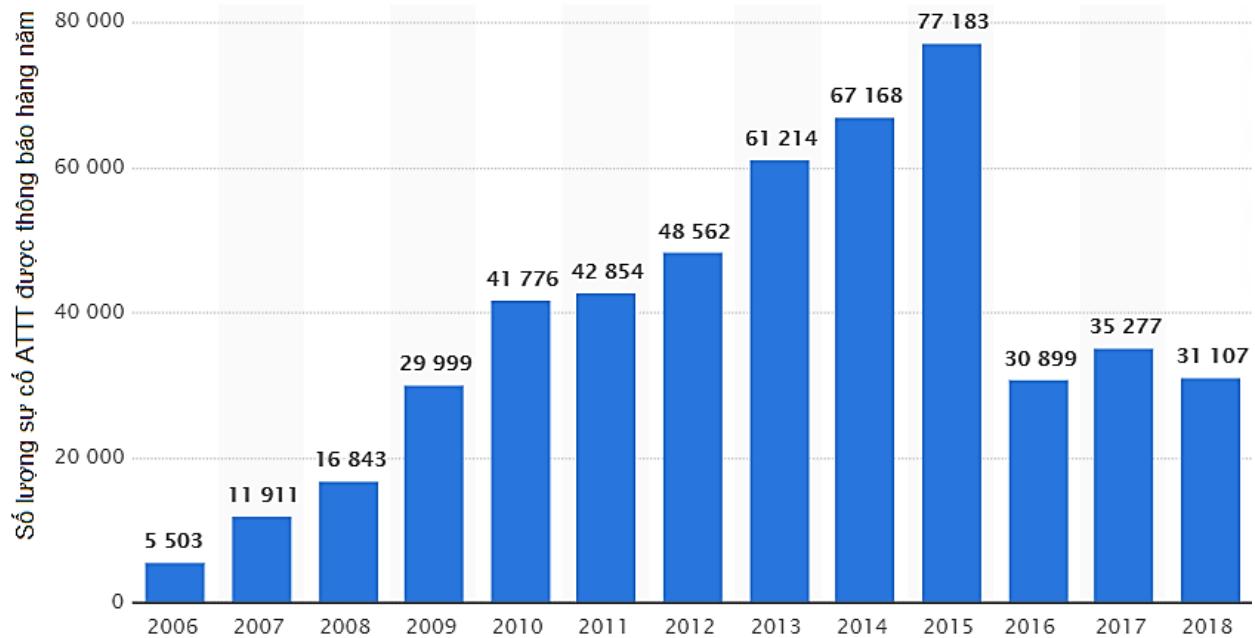
Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của các thiết bị di động, và đặc biệt là các thiết bị IoT, số lượng người dùng mạng Internet và số lượng thiết bị kết nối vào mạng Internet tăng trưởng nhanh chóng. Theo thống kê và dự báo của trang Statista [3] cho trên Hình 1.2, số lượng các thiết 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 1.2. Thống kê và dự báo 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 [4] cho trên Hình 1.3, 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. 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.



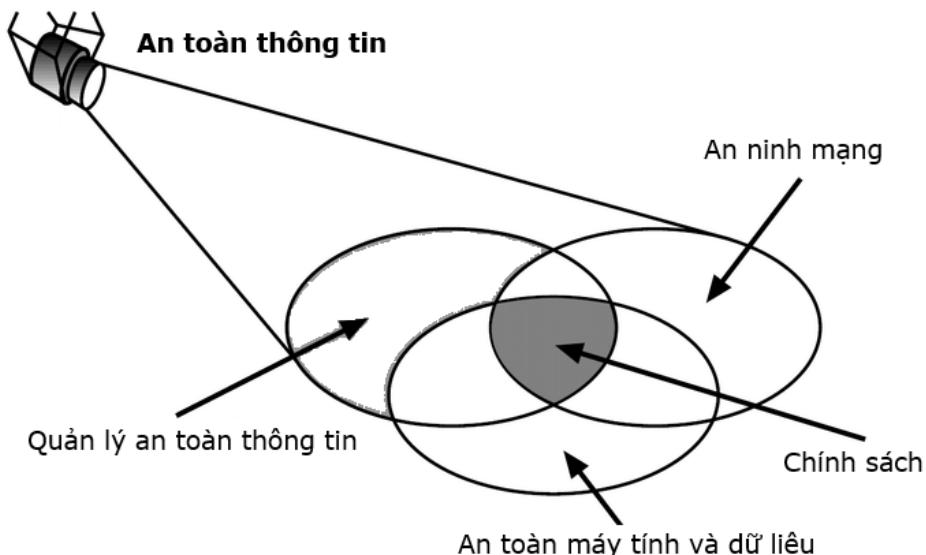
*Hình 1.3. Số lượng sự cố ATTT báo cáo bởi các cơ quan chính phủ Hoa Kỳ
giai đoạn 2006-2018 [3]*

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 tổng tiền (ransomware), mã độc đào tiền ảo...) và các kỹ thuật tấn công, phá hoại ngày càng tinh vi.

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.

1.1.3. 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* (Computer & data security), *an ninh mạng* (Network security) và *quản lý an toàn thông tin* (Management of information security). Ba thành phần 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* (Policy) như minh họa trên Hình 1.4.



Hình 1.4. Các thành phần chính của An toàn thông tin

1.1.3.2. An toàn máy tính và dữ liệu

An toàn máy tính và dữ liệu 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 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:

- Đảm bảo an toàn hệ điều hành, ứng dụng, 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.

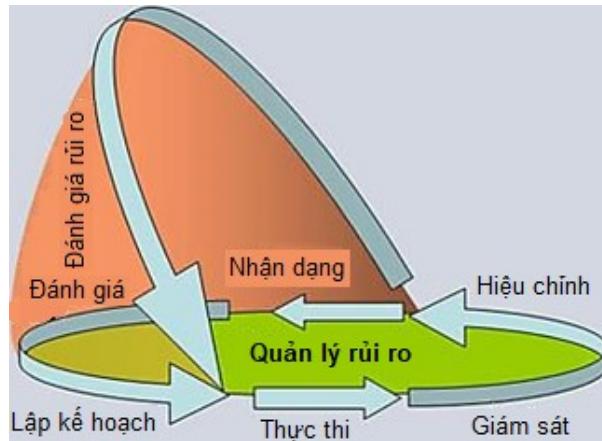
1.1.3.3. An ninh mạng

An ninh mạng là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các 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 mạng.

1.1.3.4. Quản lý an toàn thông tin

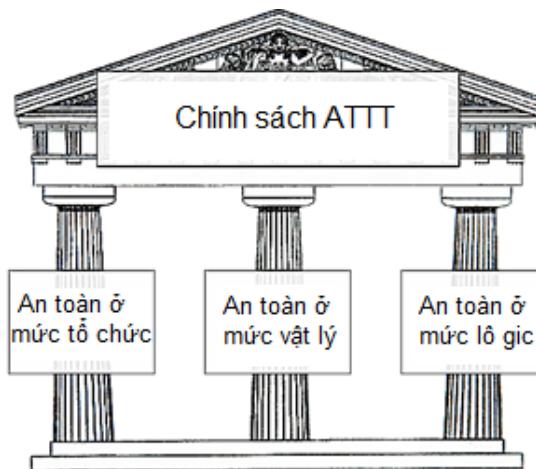
Quản lý an toàn thông tin là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Một trong các nội dung cốt lõi của quản lý an toàn thông tin là việc quản lý các rủi ro (Risk management), trong đó việc nhận dạng và đánh giá rủi ro (Risk assessment) đóng vai trò then chốt. Các nội dung khác của quản lý an toàn thông tin, bao gồm các chuẩn an toàn thông tin, chính sách an toàn thông tin và vấn đề đào tạo, nâng cao ý thức an toàn thông tin của người dùng.



Hình 1.5. Chu trình quản lý an toàn thông tin

Việc thực thi quản lý an toàn thông tin cần được thực hiện theo chu trình lặp lại, từ khâu Lập kế hoạch (Plan), Thực thi kế hoạch (Implement), Giám sát kết quả thực hiện (Monitor) và Hiệu chỉnh kiểm soát (Control) như minh họa trên Hình 1.5, do các điều kiện bên trong và bên ngoài thay đổi theo thời gian.

1.1.3.5. Chính sách an toàn thông tin



Hình 1.6. Chính sách an toàn thông tin

Chính sách an toàn thông tin (Information security policy) là các nội quy, quy định của tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ. Chính sách an toàn thông tin, như minh họa trên Hình 1.6 gồm 3 thành phần:

- Chính sách an toàn ở mức vật lý (Physical security policy);
- Chính sách an toàn ở mức tổ chức (Organizational security policy);

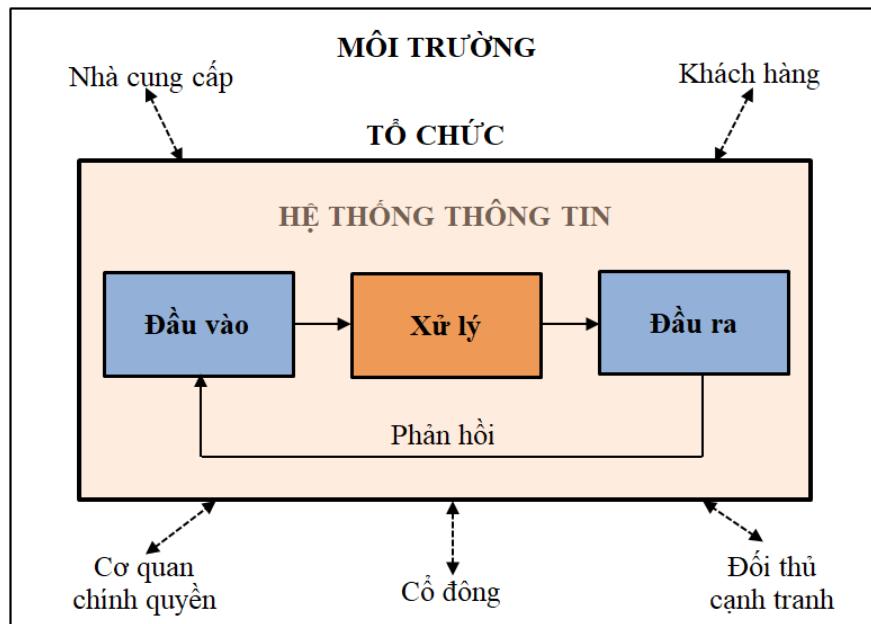
- Chính sách an toàn ở mức logic (Logical security policy).

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’ sử dụng các đặc điểm sinh trắc (Biometrics), 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.

1.2. Khái quát về an toàn hệ thống thông tin

1.2.1. Các thành phần của hệ thống thông tin

Hệ thống thông tin (Information system), theo cuốn sách Fundamentals of Information Systems Security [2] 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. 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 1.7 minh họa mô hình một hệ thống thông tin điển hình. 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.



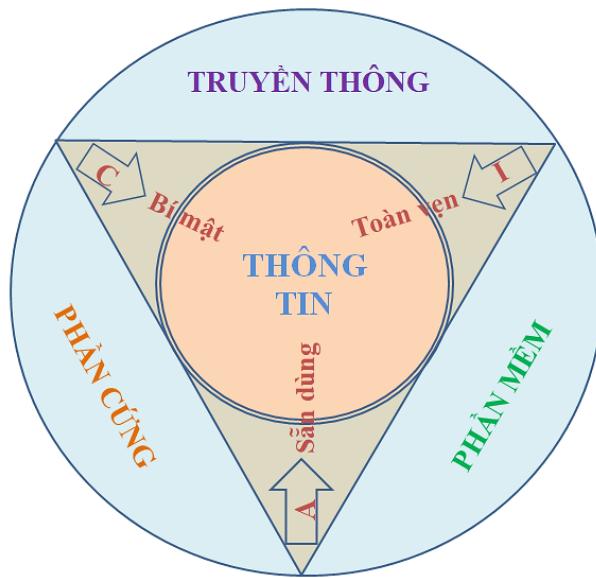
Hình 1.7. Mô hình hệ thống thông tin của cơ quan, tổ chức

Trong lớp các hệ thống thông tin, hệ thống thông tin dựa trên máy tính (Computer-based information system), 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: phần cứng (Hardware) để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu; phần mềm (Software) chạy trên phần cứng để xử lý dữ liệu; cơ sở dữ

liệu (Databases) để lưu trữ dữ liệu; mạng (Networks) là hệ thống truyền dẫn thông tin/dữ liệu; và các thủ tục (Procedures) là tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.

1.2.2. An toàn hệ thống thông tin là gì?

An toàn hệ thống thông tin (Information systems security) 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 *sử dụng*. Hình 1.8 minh họa các thành phần của Hệ thống thông tin dựa trên máy tính và An toàn hệ thống thông tin.



Hình 1.8. Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin

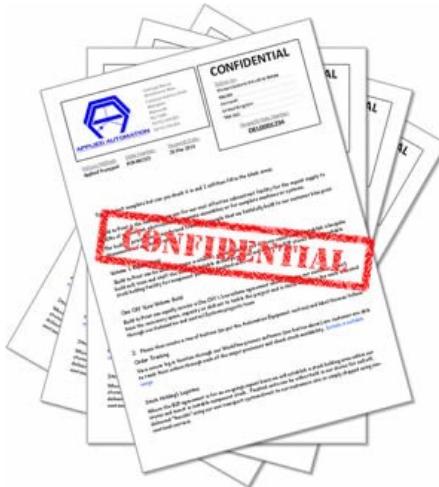
1.3. Các yêu cầu đảm bảo an toàn hệ thống thông tin

Như đã trình bày trong Mục 1.1.1, việc đảm bảo an toàn thông tin, hoặc hệ thống thông tin là việc đảm bảo ba thuộc tính quan trọng của thông tin, hoặc hệ thống, bao gồm tính *Bí mật*, tính *Toàn vẹn* và tính *Sử dụng*. Đây cũng là ba yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin.

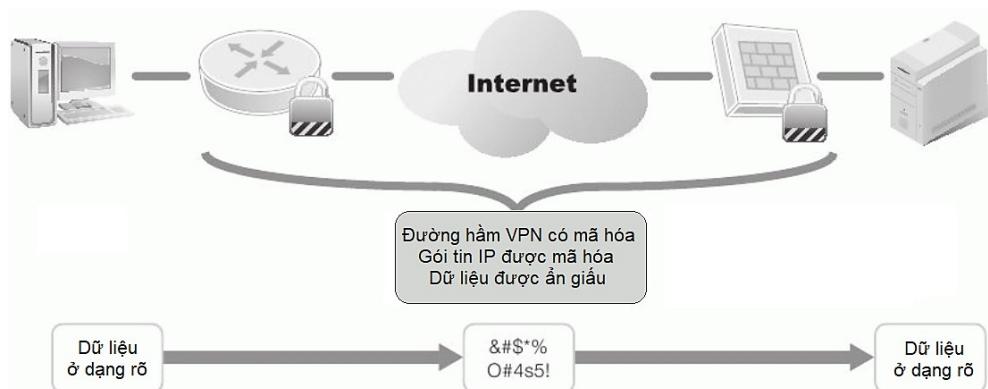
1.3.1. Tính bí mật

Tính bí mật đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy nhập 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 1.9 minh họa một văn bản được đóng dấu *Confidential* (Mật), theo đó chỉ những người có thẩm quyền (có thể không gồm người tạo, hoặc soạn thảo văn bản đó) 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 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 1.10 minh họa việc đảm bảo tính bí mật bằng cách sử dụng đường hầm VPN, hoặc mã hóa để truyền tải thông tin.



Hình 1.9. Một văn bản được đóng dấu Confidential (Mật)



Hình 1.10. Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa

1.3.2. Toàn vẹn

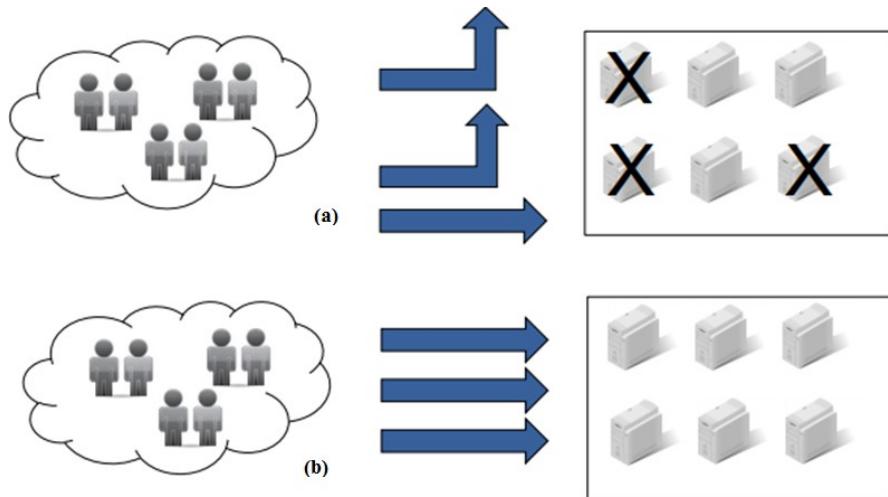
Tính toàn vẹn đảm bảo rằng thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu. Trong nhiều tổ chức, thông tin và dữ liệu có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, 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 thỏa mãn ba điều kiện: (i) không bị thay đổi, (ii) hợp lệ và (iii) chính xác.

1.3.3. Sẵn dùng

Tính sẵn dùng, sẵn sàng, hoặc khả dụng đảm bảo rằng thông tin, hoặc hệ thống có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn dùng có thể được đo bằng 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 1.11 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 tải, hoặc nền tảng điện toán đám mây.

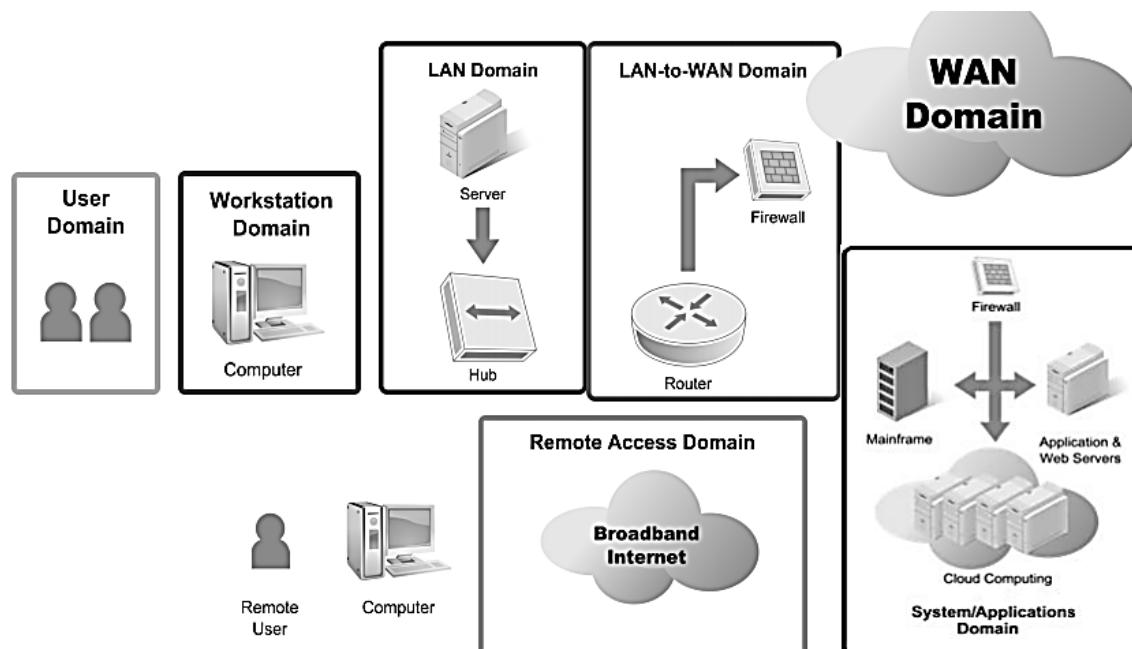


Hình 1.11. Minh họa tính sẵn dùng: (a) không đảm bảo và (b) đảm bảo tính sẵn dùng

1.4. Bảng vùng trong hạ tầng CNTT và các mối đe dọa

1.4.1. Bảng vùng trong cơ sở hạ tầng CNTT

Hạ tầng công nghệ thông tin (IT Infrastructure) của các cơ quan, tổ chức, doanh nghiệp có thể có quy mô lớn hay nhỏ khác nhau, nhưng thường gồm bảy vùng theo mức kết nối mạng như minh họa trên Hình 1.12.



Hình 1.12. Bảng vùng trong hạ tầng CNTT theo mức kết nối mạng

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

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. Các vấn đề thường gặp như thiếu ý thức, coi nhẹ vấn đề an ninh an toàn, vi phạm các chính sách an ninh an toàn; đưa CD/DVD/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; 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 máy trạm tiếp xúc trực tiếp với vùng người dùng. Các nguy cơ thường gặp gồm: truy nhập 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. Ngoài ra, vùng máy trạm cũng chịu các nguy cơ do hành vi bị cấm từ người dùng, như đưa CD/DVD/USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép.

Vùng mạng LAN

Các nguy cơ có thể có đối với vùng mạng LAN bao gồm: truy nhập trái phép vào mạng LAN vật lý, truy nhập 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 trộm. Ngoài ra, các hướng dẫn và cấu hình chuẩn cho máy chủ LAN nếu không được tuân thủ nghiêm ngặt sẽ dẫn đến những lỗ hổng an ninh mà tin tức 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 nguy cơ lớn nhất là tin tức từ mạng WAN có thể thăm dò và rà quét trái phép các cổng dịch vụ, nguy cơ truy nhập 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 mỏ, trong đó hầu hết dữ liệu được truyền dưới dạng rõ, nên các nguy cơ lớn nhất là dễ bị nghe trộm 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.

Vùng truy nhập từ xa

Trong vùng truy nhập từ xa, các 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 nhập 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

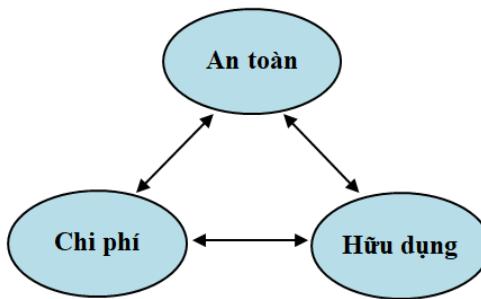
Trong vùng hệ thống và ứng dụng, các nguy cơ có thể bao gồm: truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp; các khó khăn trong quản lý các máy chủ với yêu cầu tính sẵn dùng cao; các lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ; các vấn đề an ninh trong các môi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

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

1.5.1. Giới thiệu

Mô hình tổng quát đảm bảo an toàn hệ thống thông tin là *Phòng vệ theo chiều sâu* (Defence in Depth). Theo mô hình 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.

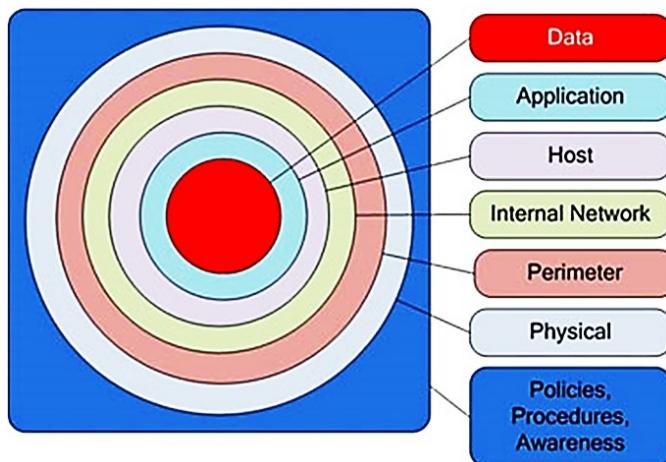
Một điểm khác cần lưu ý khi thiết kế và triển khai hệ thống đảm bảo an toàn thông tin là cần cân bằng giữa *Hữu dụng, Chi phí và An toàn*, như minh họa trên Hình 1.13 **Error! Reference source not found.** Hệ thống đảm bảo an toàn thông tin chỉ thực sự phù hợp và hiệu quả khi hệ thống được bảo vệ đạt mức an toàn phù hợp mà vẫn có khả năng cung cấp các tính năng hữu dụng cho người dùng, với chi phí cho đảm bảo an toàn phù hợp với tài sản được bảo vệ.



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

1.5.2. Một số mô hình đảm bảo an toàn hệ thống thông tin

Hình 1.14 minh họa mô hình đảm bảo an toàn thông tin với bảy 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 host (Host); lớp ứng dụng (Application) và lớp dữ liệu (Data). Trong mô hình này, để truy nhập được đến đối tượng đích là dữ liệu, tin tức cần phải vượt qua cả 7 lớp bảo vệ.

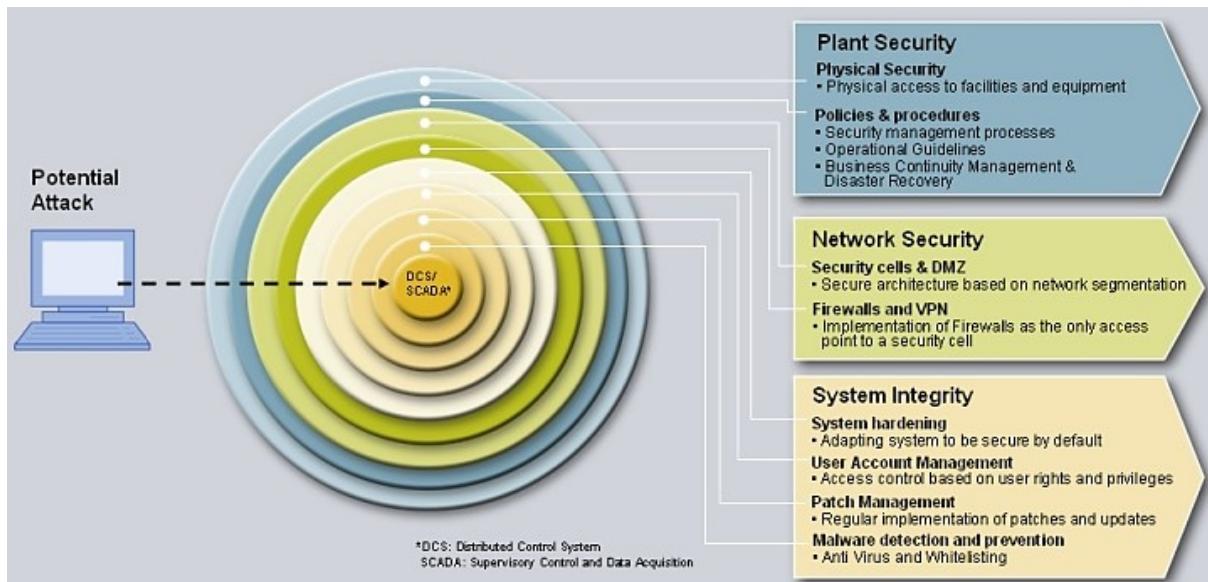


Hình 1.14. Mô hình đảm bảo an toàn thông tin với bảy lớp

Cụ thể hơn, Hình 1.15 minh họa mô hình phòng vệ gồm 3 lớp: lớp an ninh tổ chức, lớp an ninh mạng và lớp an ninh hệ thống. Mỗi lớp trên lại gồm một số lớp con như sau:

- Lớp an ninh cơ quan/tổ chức (Plant Security), gồm 2 lớp con:
 - + Lớp bảo vệ vật lý (Physical Security) có nhiệm vụ kiểm soát các truy nhập 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 ATTT, các hướng dẫn vận hành, quản lý hoạt động liên tục và phục hồi sau sự cố.
- Lớp an ninh mạng (Network Security), gồm 2 lớp con:
 - + Lớp bảo vệ vùng hạn chế truy nhập (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 nhập duy nhất đến một phân đoạn mạng.
- Lớp an ninh hệ thống (System Integrity), 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 nhập 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 và các phần mềm độc hại khác.



Hình 1.15. Mô hình đảm bảo an toàn thông tin với ba lớp chính

1.6. Câu hỏi ôn tập

- 1) An toàn thông tin (Information Security) là gì?
- 2) Tại sao cần phải đảm bảo an toàn cho thông tin?
- 3) An toàn thông tin gồm những thành phần cơ bản nào?
- 4) Đảm bảo thông tin thường được thực hiện bằng cách nào?
- 5) An toàn hệ thống thông tin là gì?
- 6) Nêu các yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin.
- 7) 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 nguy cơ và rủi ro nhất?
- 8) 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 có nguy cơ bị tấn công phá hoại cao?
- 9) Mô hình tổng quát đảm bảo an toàn hệ thống thông tin là gì?
- 10) Mô tả một mô hình tổng quát đảm bảo an toàn hệ thống thông tin.

CHƯƠNG 2. CÁC DẠNG TẤN CÔNG VÀ PHẦN MỀM ĐỘC HẠI

Chương 2 giới thiệu khái quát về mối đe dọa, điểm yếu, lỗ hổng tồn tại trong hệ thống và khái niệm tấn công. Phân tiếp theo phân tích chi tiết 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, ... Nửa cuối của chương đề cập đến các dạng phần mềm độc hại, gồm cơ chế lây nhiễm, tác hại và giải pháp phòng chống.

2.1. Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công

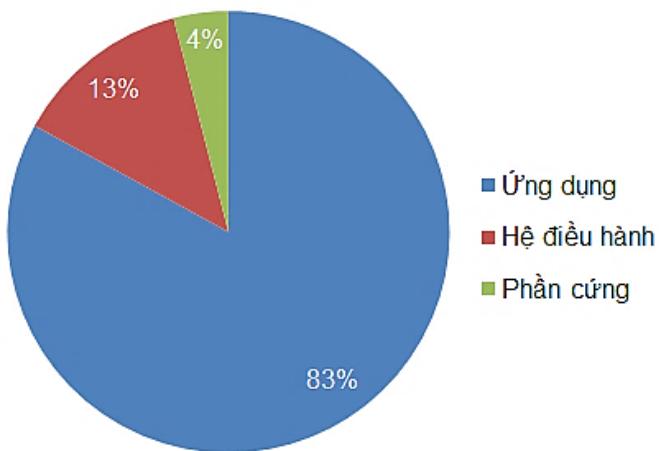
2.1.1. Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công

Mối đe dọa (Threat) là bất kỳ một hành động nào có thể gây hư hại đến 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,...

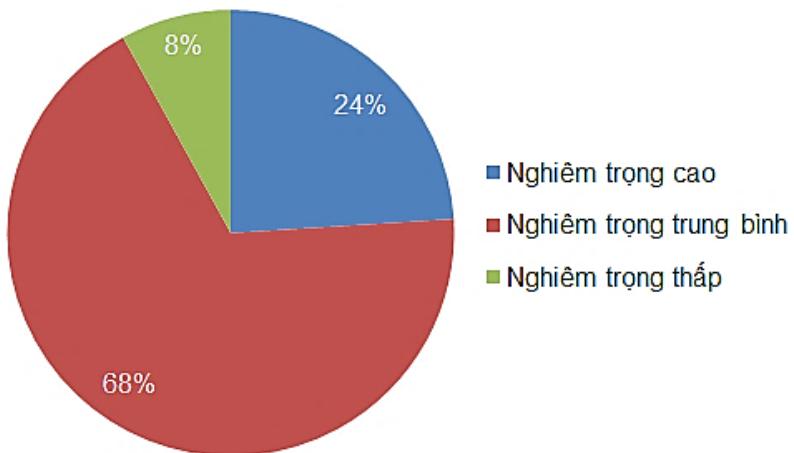
Các điểm yếu hệ thống (System weaknesses) là các lỗi hay các khuyết khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, cấu hình hoạt động. Các điểm yếu có thể tồn tại trong cả các mô đun phần cứng và các mô đun phần mềm. Một số điểm yếu được phát hiện và đã được khắc phục. Tuy nhiên, có một số 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 (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó, bao gồm tính toàn vẹn, tính bí mật, tính sẵn dùng. Nói chung, lỗ hổng bảo mật tồn tại trong tất cả các thành phần của hệ thống, bao gồm phần cứng, hệ điều hành và các phần mềm ứng dụng. Theo số liệu thống kê từ Cơ sở dữ liệu lỗ hổng quốc gia Hoa Kỳ [6], trong năm 2014, phân bố lỗ hổng bảo mật được phát hiện trên các thành phần của hệ thống là: lỗ hổng bảo mật phần cứng – 4%, hệ điều hành – 13% và phần mềm ứng dụng – 83%, như minh họa trên Hình 2.1. 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.

Phụ thuộc vào khả năng bị khai thác, các lỗ hổng bảo mật có mức độ nghiêm trọng (severity) 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). Cũng theo số liệu thống kê năm 2014 từ [6] cho trên Hình 2.2, 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%. 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 2.1. Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống



Hình 2.2. Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng

Tấn công (Attack) là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh an toàn của cơ quan, tổ chức, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn dùng 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 tồn tại trong hệ thống. Như vậy, tấn công chỉ có thể trở thành hiện thực nếu có sự tồn tại đồng thời của mối đe dọa và lỗ hổng, hay có thể nói:

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

Như vậy, mối đe dọa và lỗ hổng bảo mật 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 phá hoại. 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, qua đó giảm thiểu khả năng bị khai thác để thực hiện tấn công.

2.1.2. Các dạng mối đe dọa thường gặp

Trên thực tế, không phải tất cả các mối đe dọa đều là ác tính hay độc hại (malicious). Một số mối đe dọa là chủ động, có 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:

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

2.1.3. Các loại tấn công

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

- Giả mạo (Fabrications): Tấn công giả mạo thông tin thường được sử dụng để đánh lừa người dùng thông thường;
- Chặn bắt (Interceptions): Tấn công chặn bắt thường liên quan đến việc nghe lén trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
- Gây ngắt quãng (Interruptions): Tấn công gây ngắt quãng làm ngắt, hoặc chậm khen truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy nhập dịch vụ của người dùng hợp pháp;
- Sửa đổi (Modifications): Tấn công sửa đổi liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

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

- Tấn công chủ động (Active attacks): Tấn công chủ động là một đột nhập, xâm nhập (intrusion) 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 nhập trái phép vào máy tính hoặc hệ thống mạng.
- Tấn công thụ động (Passive attacks): Tấn công thụ động thường không gây ra thay đổi trên hệ thống. Các tấn công thụ động điển hình là nghe trộm và giám sát lưu lượng trên đường truyền.

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

2.2. Các công cụ hỗ trợ tấn công

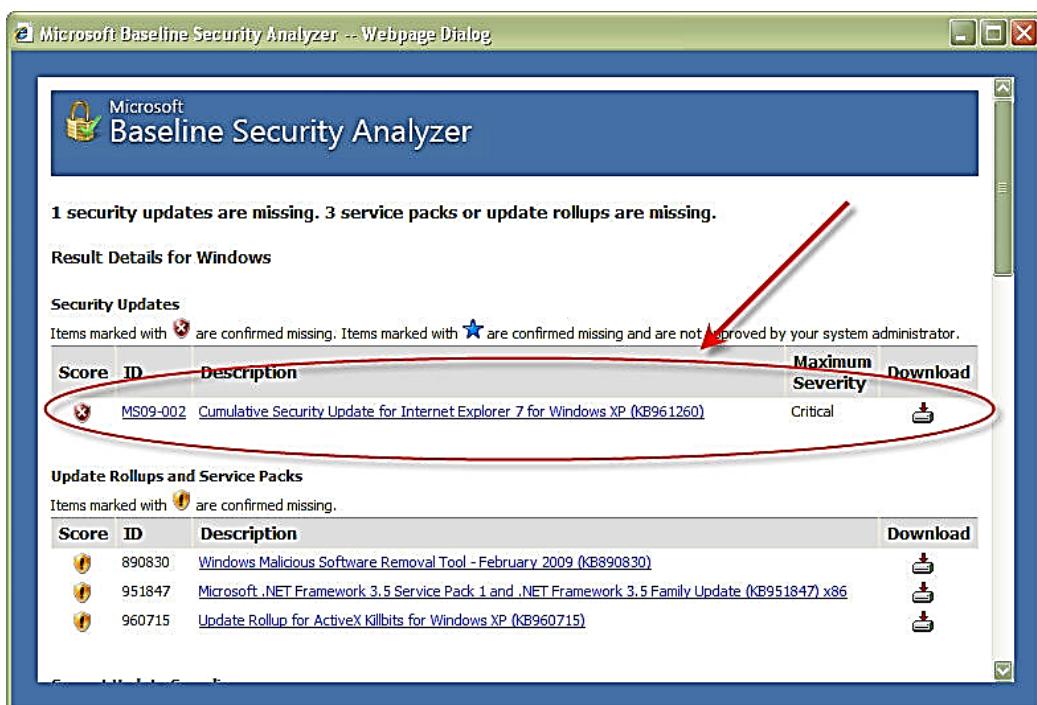
Các công cụ hỗ trợ tấn công (Attacking assistant tools) là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ kẻ tấn công, tin tặc (attacker) thu thập các thông tin về các hệ thống máy tính, hoặc mạng. Trên cơ sở các thông tin thu được, tin tặc sẽ lựa chọn công cụ, kỹ thuật tấn công có xác suất 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 và công cụ ghi phím gõ.

2.2.1. Công cụ rà quét lỗ hổng, điểm yếu hệ thống

Các công cụ rà quét các điểm yếu hệ thống 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, phân tích và đề xuất áp dụng các biện pháp khắc phục phù hợp. Mặt khác, các công cụ này cũng có thể được kẻ tấn công sử dụng để rà quét hệ thống và dựa trên kết quả rà quét điểm yếu, lỗ hổng để quyết định dạng tấn công có khả năng thành công cao nhất. Các công cụ bao gồm, 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.

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

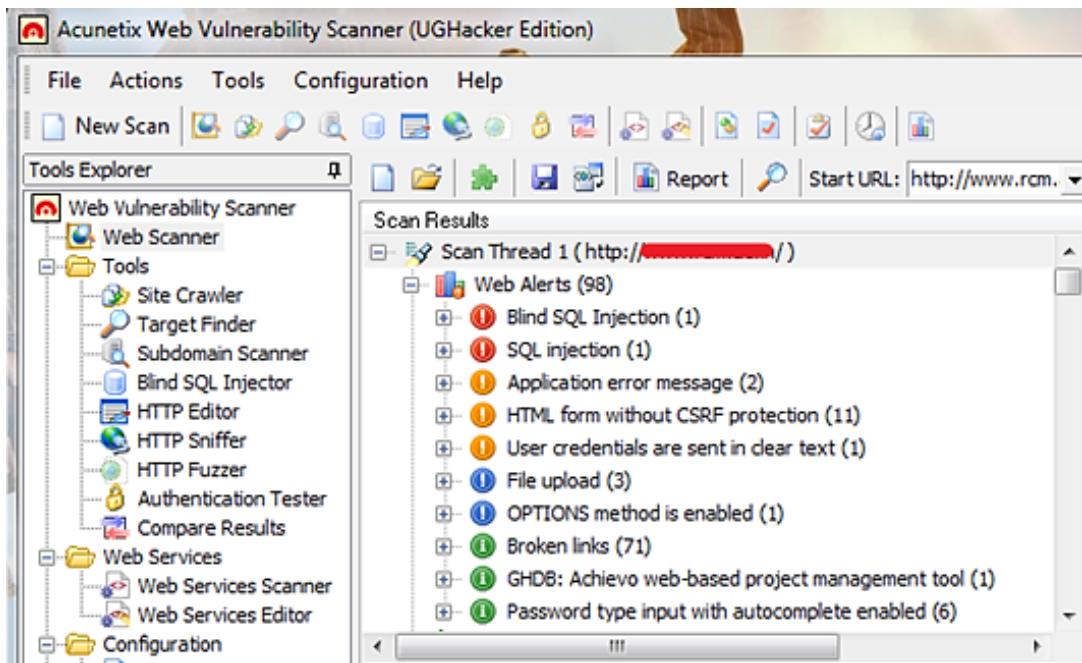
Các công cụ rà quét lỗ hổng bảo mật hệ thống cho phép rà quét hệ thống, tìm các điểm yếu và các lỗ hổng bảo mật. Đồng thời, chúng cũng cung cấp phần phân tích chi tiết từng điểm yếu, lỗ hổng, kèm theo là hướng dẫn khắc phục, sửa chữa. Các công cụ được sử dụng rộng rãi là Microsoft Baseline Security Analyzer (Hình 2.3) cho rà quét các hệ thống chạy hệ điều hành Microsoft Windows và Nessus Vulnerability Scanner cho rà quét các hệ thống chạy nhiều loại hệ điều hành khác nhau.



Hình 2.3. Báo cáo kết quả quét của Microsoft Baseline Security Analyzer

2.2.1.2. 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 lỗi và lỗ hổng bảo mật. Chúng cũng hỗ trợ phân tích tình trạng các lỗi tìm được, như các lỗi XSS, lỗi chèn mã SQL, lỗi CSRF, lỗi bảo mật phiên,... Các công cụ được sử dụng phổ biến bao gồm Acunetix Web Vulnerability Scanner (Hình 2.4), IBM AppScan, Beyond Security AVDS và SQLmap.



Hình 2.4. Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner

2.2.2. 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:

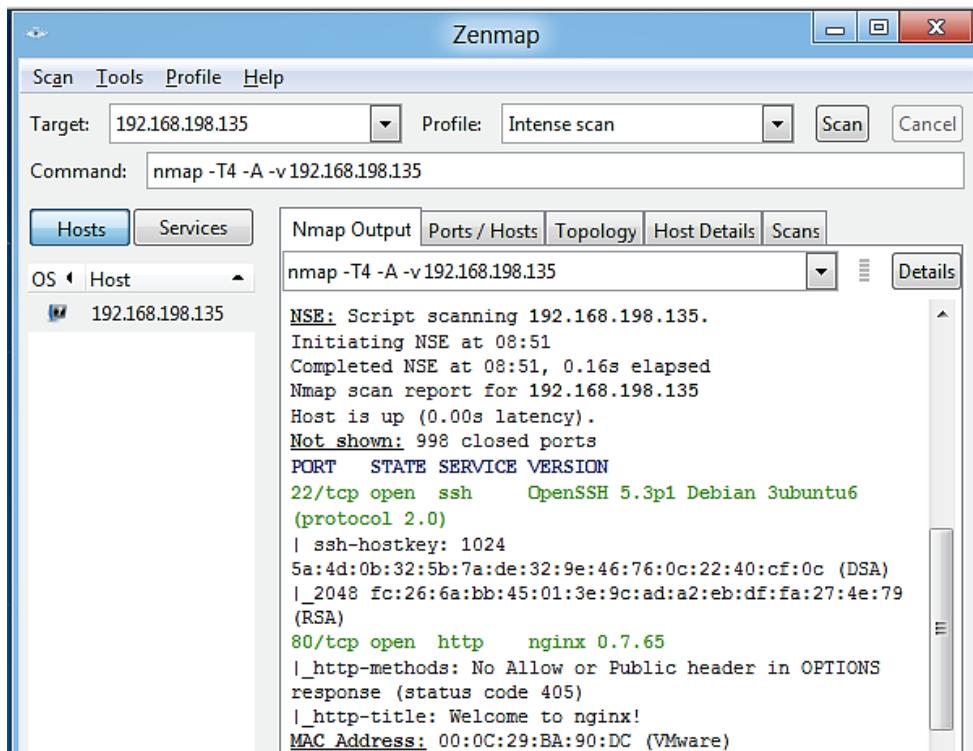
- Cổng 80/443 mở có nghĩa là dịch vụ web đang hoạt động;
- Cổng 25 mở có nghĩa là dịch vụ gửi/nhận email SMTP đang hoạt động;
- Cổng 1433 mở có nghĩa là máy chủ Microsoft SQL Server đang hoạt động;
- Cổng 53 mở có nghĩa là dịch vụ tên miền DNS đang hoạt động,...

Các công cụ quét cổng dịch vụ được sử dụng phổ biến bao gồm: Nmap, Zenmap, Portsweep, Advanced Port Scanner, Angry IP Scanner, SuperScan và NetScanTools. Hình 2.5 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 dùng do chỉ hỗ trợ giao diện dòng lệnh.

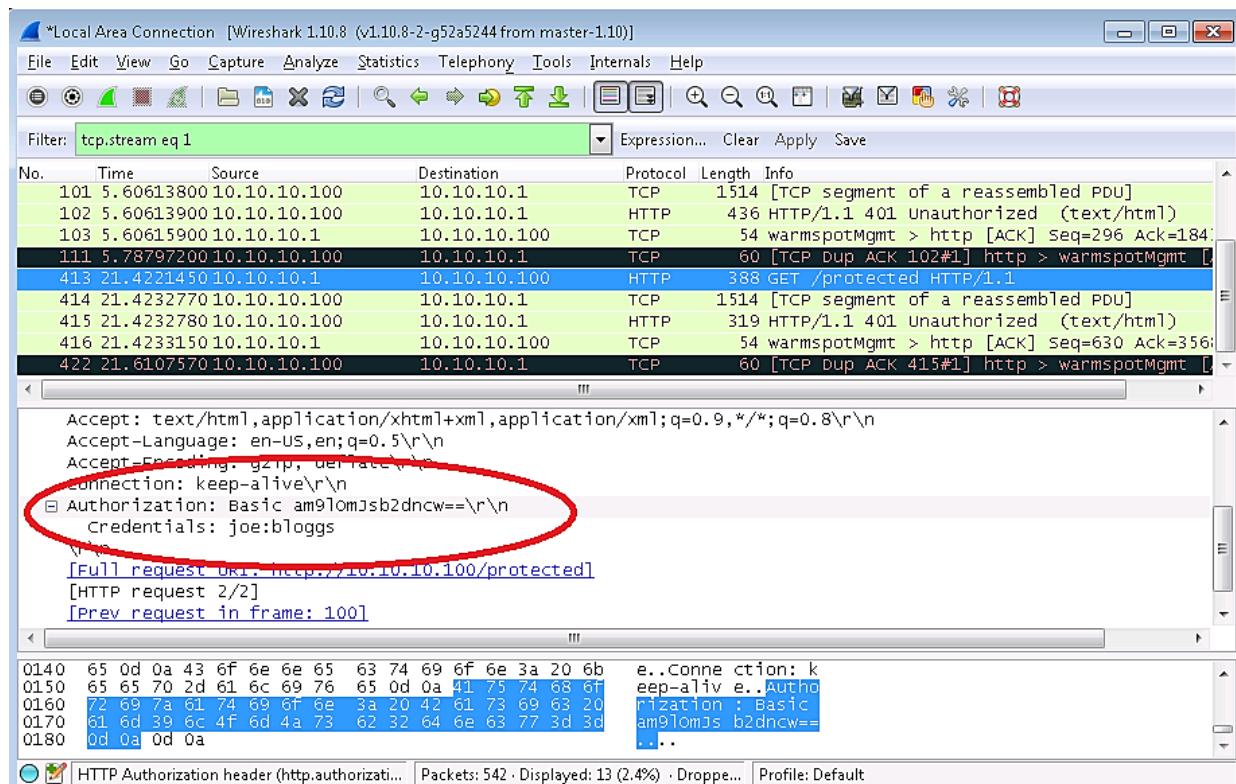
2.2.3. Công cụ nghe lén

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:

- Tcpdump
- Wireshark (minh họa trên Hình 2.6)
- Pcap / Wincap / Libcap (Packet capture)
- IP Tools (<http://www.softpedia.com>).



Hình 2.5. Giao diện của công cụ Zenmap



Hình 2.6. Sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm

2.2.4. 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 chỉ định trước hoặc sao chép trực tiếp. 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 các nhân viên. Việc cài đặt Keylogger có thể được thực hiện tương đối đơn giản: Hình 2.7 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 thông thường và lừa người dùng cài đặt vào máy tính của mình.



Hình 2.7. Mô đun Keylogger phần cứng và cài đặt trên máy tính để bàn

2.3. Các dạng tấn công thường gặp

Các dạng tấn công thường gặp là các dạng tấn công điển hình, xảy ra thường xuyên nhắm vào các 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
- 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.

Phần 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.

2.3.1. Tấn công vào mật khẩu

2.3.1.1. 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 đến máy chủ, hoặc các thông tin này 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 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 bình thường.

2.3.1.2. Mô tả

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

- Tấn công dựa trên từ điển (Dictionary attacks): 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 trong từ điển, nhờ vậy tăng khả năng thành công.
- Tấn công vét cạn (Brute force attacks): Dạng vét cạn sử dụng tổ hợp các ký tự và thử 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 từ tổ hợp ký tự với chuỗi mật khẩu mã hóa thu thập được. Nếu hai bản mã trùng nhau thì tổ hợp ký tự là mật khẩu.

2.3.1.3. 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 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 (?#\$...). Mật khẩu cho người quản trị hệ thống cần có độ dài lớn hơn hoặc bằng 10 ký tự cũng với 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.
- Mật khẩu không nên lưu ở dạng rõ (plaintext). 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.

2.3.2. Tấn công bằng mã độc

2.3.2.1. Giới thiệu

Tấn công bằng mã độc (Malicious code attacks) là dạng tấn công sử dụng các mã độc (Malicious code) làm công cụ để tấn công hệ thống nạn nhân. Tấn công bằng mã độc có thể 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:
 - + Tấn công khai thác lỗi tràn bộ đệm (Buffer Overflow)
 - + Tấn công khai thác lỗi không 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)
- + Vi rút
- + Zombie/Bot
- + Trojan

Dạng tấn công lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại sẽ được đề cập ở Mục 2.4. Mục này chủ yếu đề cập về tấn công khai thác lỗi tràn bộ đệm, tấn công khai thác lỗi không kiểm tra đầu vào, trong đó tập trung phân tích dạng tấn công chèn mã SQL.

2.3.2.2. Tấn công khai thác lỗi tràn bộ đệm

a. Giới thiệu và nguyên nhân

Lỗi tràn bộ đệm (Buffer overflow) là một trong các lỗi thường gặp trong các hệ điều hành và đặc biệt nhiều ở các phần mềm ứng dụng [6]. 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 đệm. Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công chèn, thực hiện mã độc để kiểm soát hệ thống. Lỗi tràn bộ đệm chiếm một tỷ lệ lớn trong số các lỗi gây lỗ hổng bảo mật [6]. Tuy nhiên, trên thực tế không phải tất cả các lỗi tràn bộ đệm đều có thể bị khai thác bởi kẻ tấn công.

Lỗi tràn bộ đệm xuất hiện trong khâu lập trình phần mềm (coding) trong quy 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 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, có thể khiến chương trình bị lỗi và ngừng hoạt động. Một nguyên nhân bổ sung khác là việc sử dụng các ngôn ngữ với các thư viện không an toàn, như hợp ngữ, C và C++.

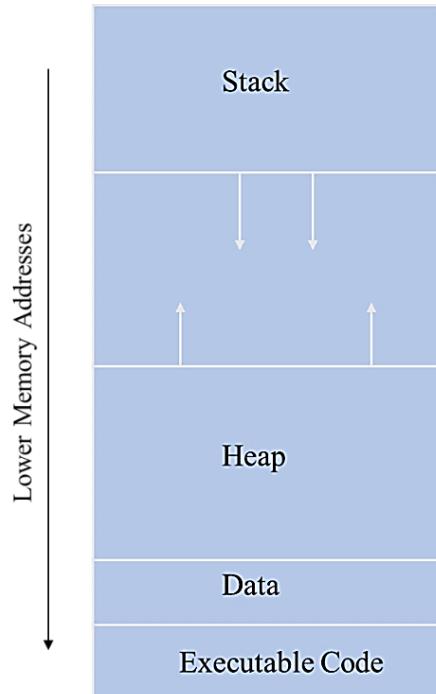
b. Cơ chế gây tràn và khai thác

* Cơ chế gây tràn

Trên hầu hết các nền tảng, khi một 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 2.8 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 dữ liệu cục bộ của chúng. Vùng nhớ cấp phát động là vùng nhớ chung lưu dữ liệu cho ứng dụng, được cấp phát hay giải phóng trong quá trình hoạt động của ứng dụng.

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. Khi việc thực hiện hàm kết thúc, hệ thống nạp địa chỉ trả về đã lưu trong ngăn xếp vào con trả lệnh (còn gọi là bộ đếm chương trình) kích hoạt việc quay trở lại thực hiện lệnh kế tiếp lời gọi hàm ở chương trình gọi.



Hình 2.8. Các vùng bộ nhớ cấp cho chương trình

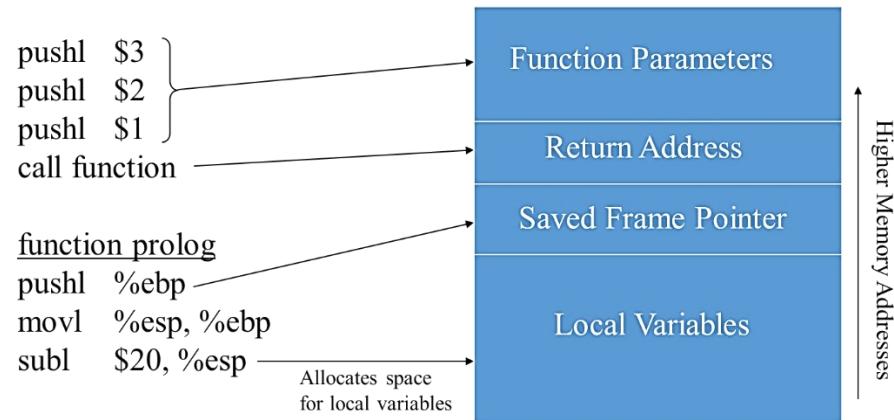
```
// định nghĩa một hàm
void function(int a, int b, int c) {
    char buffer1[8];
    char buffer2[12];
}
// chương trình chính
int main() {
    function(1,2,3); // gọi hàm
}
```

Hình 2.9. Một chương trình minh họa cấp phát bộ nhớ trong ngăn xếp

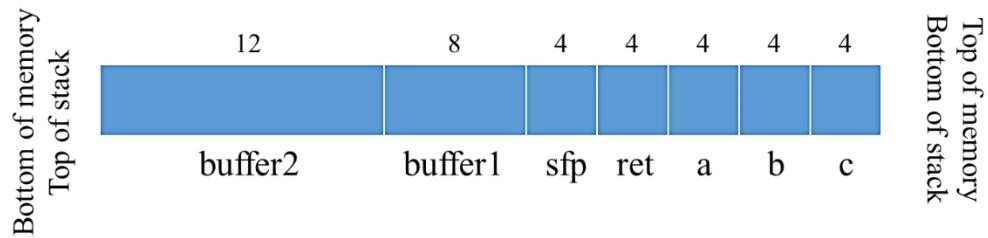
Hình 2.9 là một đoạn chương trình gồm một hàm con (*function()*) và một hàm chính (*main()*) minh họa cho việc gọi làm và cấp phát bộ nhớ trong vùng nhớ ngăn xếp. Hàm *function()* có 3 tham số hình thức kiểu nguyên và khai 2 biến cục bộ *buffer1* và *buffer2* kiểu xâu ký tự. Hàm chính *main()* chỉ chứa lời gọi đến hàm *function()* với 3 tham số thực.

Hình 2.10 biểu diễn việc cấp phát bộ nhớ cho các thành phần trong ngăn xếp: các tham số gọi hàm được lưu vào 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 Local Variables. Hình 2.11 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 – bottom of stack) và các biến cục bộ được cấp các ô nhớ bên trái (phía đỉnh ngăn xếp – top of stack).



Hình 2.10. Các thành phần được lưu trong vùng bộ nhớ trong ngăn xếp



Hình 2.11. Cấp phát bộ nhớ cho các biến nhớ trong vùng bộ nhớ trong ngăn xếp

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

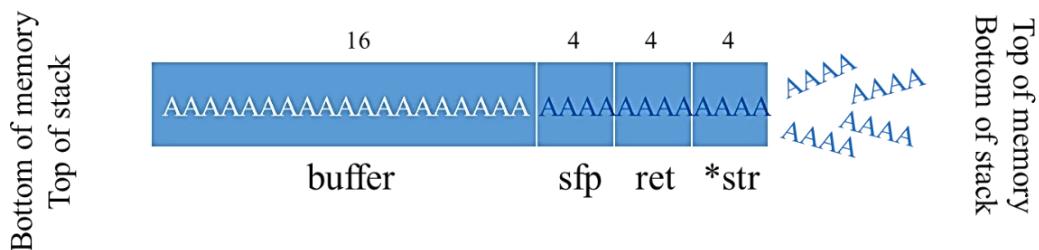
// chương trình chính
int main() {
    char large_string[256];
    int i;
    for (i = 0; i < 255; i++) {
        large_string[i] = 'A';
    }
    function(large_string);
}
```

Hình 2.12. Một chương trình minh họa gây tràn bộ nhớ đệm trong ngăn xếp

Hình 2.12 là một đoạn chương trình minh họa 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 1 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 một 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 2.12 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 2.13, 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 đầu vào `str`. Ô nhớ chưa địa chỉ trỏ về `ret` bị ghi đè và giá trị địa chỉ trỏ 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.



Hình 2.13. Minh họa hiện tượng tràn bộ nhớ đệm 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 thiêu 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 trong ngăn xếp, như các biến cục bộ khác, con trỏ khung, địa chỉ trỏ về, các biến tham số đầu vào,....

* Khai thác lỗi tràn bộ đệm

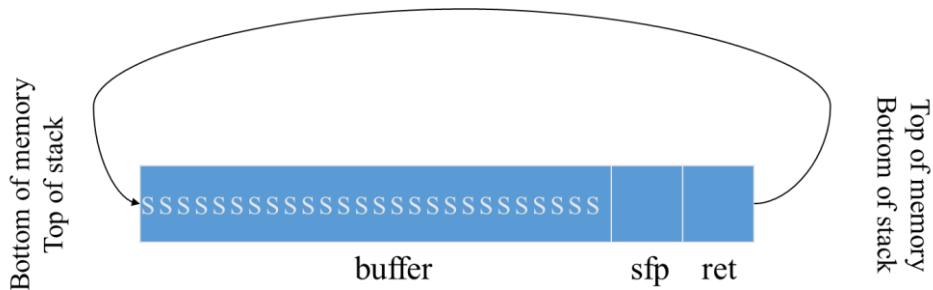
Khi một ứng dụng chứa lỗ hổng tràn bộ đệm, tin tức có thể khai thác bằng cách gửi mã độc dưới dạng dữ liệu đến ứng dụng nhằm ghi đè, thay thế địa chỉ trỏ về với mục đích tái định hướng chương trình đến thực hiện đoạn mã độc mà tin tức gửi đến. Đoạn mã độc tin tức xây dựng là mã máy có thể thực hiện được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

Mã `shellcode` có thể được viết bằng hợp ngữ, C, hoặc các ngôn ngữ lập trình khác, sau đó được chuyển thành mã máy, rồi chuyển định dạng thành một chuỗi dữ liệu và cuối cùng được gửi đến ứng dụng. Hình 2.14 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 `shell sh` trong các hệ thống Linux hoặc Unix thông qua lệnh `/bin/sh`.

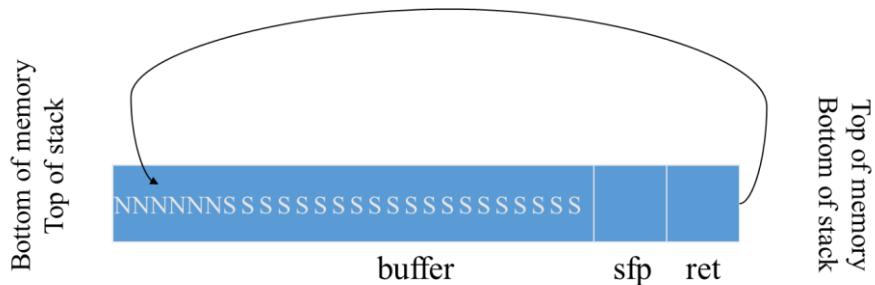
Hình 2.15. minh họa việc chèn *shellcode*, ghi đè lên ô nhớ chứa địa chỉ trả về *ret*, tái định hướng việc trả về từ chương trình con, chuyển đến thực hiện mã *shellcode* được chèn vào. Trên thực tế, để tăng khả năng đoạn mã *shellcode* được thực hiện, người ta thường chèn một số lệnh NOP (N) vào phần đầu *shellcode* để phòng khả năng địa chỉ *ret* mới không trả chính xác đến địa chỉ bắt đầu *shellcode*, như minh họa trên Hình 2.16. Lệnh NOP (No OPeration) là lệnh không thực hiện tác vụ nào cả, chỉ tiêu tốn một số chu kỳ của bộ vi xử lý.

<pre> 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" </pre>	<pre> 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"; </pre>
--	--

Hình 2.14. Một *shellcode* viết bằng ngữ và chuyển thành chuỗi tấn công



Hình 2.15. Chèn và thực hiện *shellcode* khai thác lỗ tràn bộ đệm

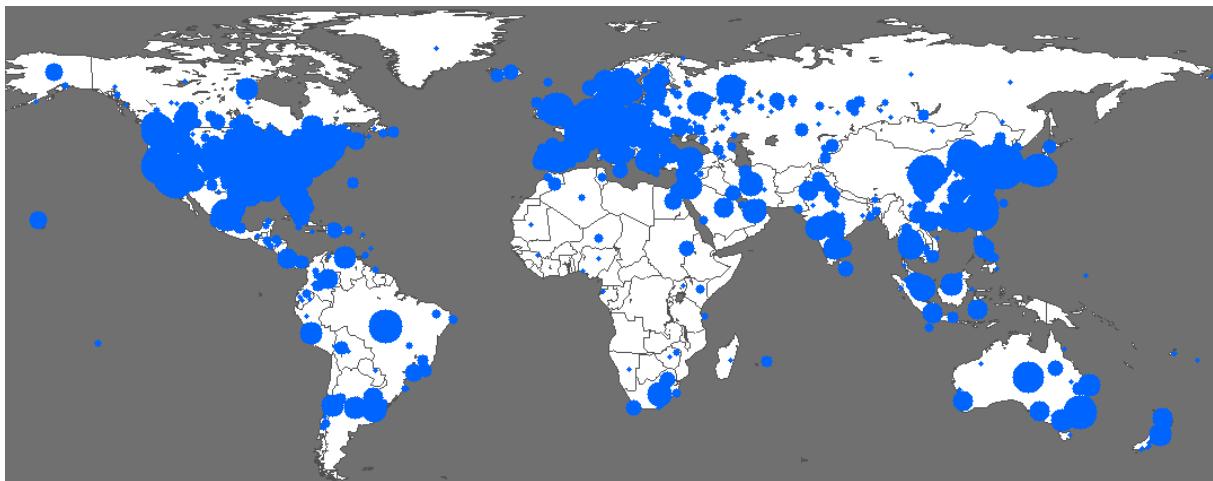


Hình 2.16. Chèn *shellcode* với phần đệm bằng lệnh NOP (N)

* Ví dụ về khai thác lỗ tràn bộ đệm

Sâu SQL Slammer (một số tài liệu gọi là sâu Sapphire) được phát hiện ngày 25/1/2003 lúc 5h30 (UTC) là sâu có tốc độ lây lan nhanh nhất lúc bấy giờ: nó lây nhiễm

ra khoảng 75.000 máy chủ chỉ trong khoảng 30 phút, như minh họa trên Hình 2.17. 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 2.17. Bản đồ lây nhiễm sâu Slammer (màu xanh) theo trang www.caida.org vào ngày 25/1/2003 lúc 6h00 (giờ UTC) với 74.855 máy chủ bị nhiễm

Sâu 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 sâu 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 ở 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 hổng 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>.

c. 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 mã nguồn hay sử dụng các công cụ phân tích mã tự động để tìm và khắc phục các điểm có khả năng xảy ra lỗ 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 Windows XP 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 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) phía trước địa chỉ trả về và kiểm tra 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 Microsoft .Net. Với các ngôn ngữ có thể gây tràn như C, C++, nên sử dụng các thư viện an toàn (Safe C/C++ Libraries) để thay thế các thư viện chuẩn có thể gây tràn.

2.3.2.3. Tấn công khai thác lỗi không kiểm tra đầu vào

a. Giới thiệu

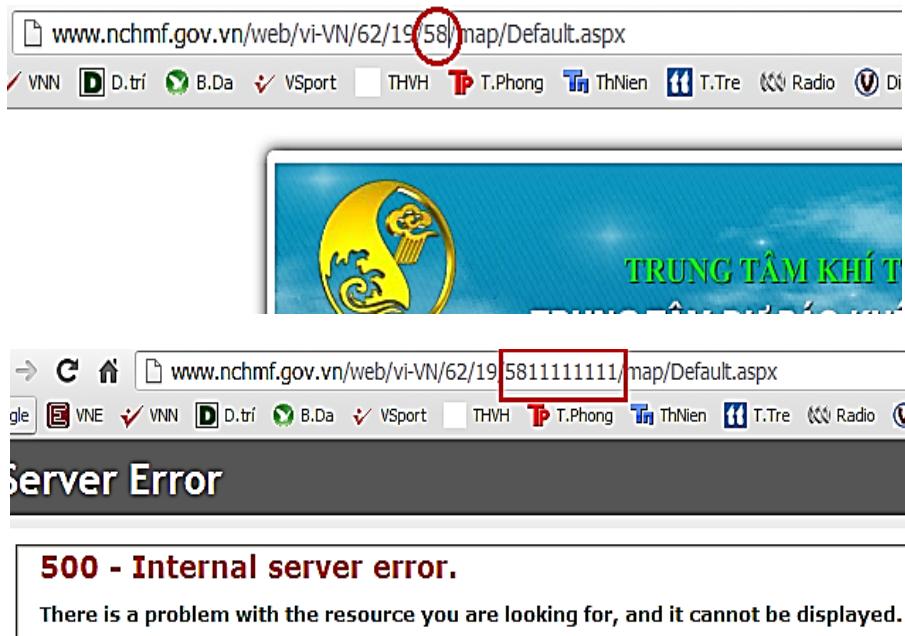
Lỗi không kiểm tra đầu vào (Unvalidated input) là một trong các dạng lỗi hỏng bảo mật phổ biến, trong đó ứng dụng không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào, nhờ đó tin tức có thể khai thác lỗi để tấn công ứng dụng và hệ thống. Dữ liệu đầu vào (Input data) cho ứng dụng rất đa dạng, có thể đến từ nhiều nguồn với nhiều định dạng khác nhau. Các dạng dữ liệu đầu vào điển hình cho ứng dụng:

- Các trường dữ liệu văn bản (text);
- 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, tin tức 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 OWASP (<http://www.owasp.org>), một trang web chuyên về thông kê các lỗi bảo mật ứng dụng web, lỗi không kiểm tra đầu vào luôn chiếm vị trí nhóm dẫn đầu các lỗi bảo mật các trang web trong khoảng 5 năm trở lại đây.

b. Tấn công khai thác

Có hai dạng chính tấn công khai thác lỗi không 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 2.18 minh họa tấn công khai thác lỗi không kiểm tra đầu vào dạng (1) thông qua việc nhập dữ liệu quá lớn, gây lỗi thực hiện cho trang web.



Hình 2.18. Cung cấp dữ liệu quá lớn để gây lỗi cho ứng dụng

Chúng ta minh họa tấn công khai thác lỗ khai thác lỗ không kiểm tra đầu vào dạng (2) bằng việc chèn mã tấn công SQL vào dữ liệu đầu vào, được thực hiện trên hệ quản trị cơ sở dữ liệu nhằm đánh cắp, hoặc phá hủy dữ liệu trong cơ sở dữ liệu. Giả thiết một trang web tìm kiếm sản phẩm 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 từ người dùng form tìm kiếm. Nếu người dùng nhập từ khóa là "iPhone 7", 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. Nếu không có sản phẩm nào thỏa mãn điều kiện tìm kiếm, câu lệnh SQL sẽ trả về tập bản ghi rỗng. 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 tin tức chèn thêm. Câu lệnh "**DELETE FROM** *tbl_products*" sẽ xóa tất cả các bản ghi trong bảng *tbl_products*. Sở dĩ tin tức có thể thực hiện điều này là do hầu hết các hệ quản trị cơ sở dữ liệu cho phép thực hiện nhiều câu lệnh SQL theo *mé* (batch), 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. Ngoài DELETE, tin tức có thể chèn thêm các lệnh SQL khác, như INSERT, UPDATE để thực hiện việc chèn thêm bản ghi hoặc sửa đổi dữ liệu theo ý đồ tấn công của mình.

c. Phòng chống

Biện pháp chủ yếu phòng chống tấn công khai thác lối không kiểm tra đầu vào là 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:
 - + Các ký tự đặc biệt: *, ', =, --
 - + Các từ khóa ngôn ngữ: chặng hạn với dạng tấn công chèn mã SQL, cần lọc các từ khóa như SELECT, INSERT, UPDATE, DELETE, DROP....

2.3.2.4. Tấn công chèn mã SQL

a. Khái quát

Tấn công chèn mã SQL (SQL Injection) 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. Tùy vào mức độ tinh vi, tấn công chèn mã SQL có thể cho phép kẻ tấn công (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. Tấn công chèn mã SQL là dạng tấn công thường gặp ở các ứng dụng web, các trang web có kết nối đến cơ sở dữ liệu.

Có 2 nguyên nhân của lỗ hổng trong ứng dụng nói chung và ứng dụng web nói riêng cho phép thực hiện tấn công chèn mã SQL:

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

Phần tiếp theo mục này là mô tả chi tiết về 4 hành động kẻ tấn công có thể thực hiện trên hệ thống nạn nhân thông qua khai thác lối chèn mã SQL.

b. Vượt qua các khâu xác thực người dùng

Xem xét một form đăng nhập (Log in) và đoạn mã xử lý xác thực người dùng lưu trong bảng cơ sở dữ liệu `tbl_accounts`(`username`, `password`) cho như trên Hình 2.19.

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; 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, chặng 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'
```

```
<!-- 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 >
    <input type=submit name="login" value="Log In">
</form>
<%
' Mã ASP xử lý đăng nhập trong file log_in.asp:
' giả thiết đã kết nối với CSDL SQL qua đối 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 2.19. Form đăng nhập (log on) và đoạn mã xử lý xác thực người dùng

Câu truy vấn sẽ trả về mọi bản ghi trong bảng do thành 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 sau ký hiệu (--) được coi là ghi chú 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 2.20.

```
<!-- Form tìm kiếm sản phẩm -->
<form method="post" action="/search.asp">
```

```

Nhập tên sản phẩm: <input type="text" name="keyword">
<input type="submit" name="search" value="Search">
</form>

<%
' Mã ASP xử lý tìm sản phẩm trong file search.asp:
' giả thiết đã kết nối với CSDL SQL server qua connection
' 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 2.20. Form tìm kiếm sản phẩm và đoạn mã xử lý tìm sản phẩm

Nếu người dùng nhập chuỗi "**Samsung Galaxy S8**" 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; 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 S8';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 S8';DELETE FROM tbl_products;--%**'

Chuỗi lệnh SQL mới gồm 2 lệnh SQL: câu lệnh SELECT tìm kiếm các sản phẩm có tên chứa từ khóa "**Samsung Galaxy S8**" trong bảng *tbl_products* và câu lệnh DELETE xóa tất cả các sản phẩm trong bảng *tbl_products*. Sở dĩ kẻ tấn công có thể làm được điều này là do hệ quản trị cơ sở dữ liệu MS-SQL server nói riêng và hầu hết các hệ quản trị cơ sở dữ liệu nói chung cho phép thực hiện nhiều lệnh SQL theo lô và dùng dấu ; để ngăn cách các 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 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* chứa thông tin người quản trị):

Galaxy S8';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 S8';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 giúp kẻ tấn công đánh cắp dữ liệu trong cơ sở dữ liệu thông qua một số bước như sau:

- 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 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 @@version (với MS-SQL Server), hoặc version() (với MySQL) trong câu lệnh ghép với UNION SELECT.
- 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>
 - + Sử dụng UNION SELECT 1, 2, 3, ...
- Trích xuất thông tin về các bảng, các trường của cơ sở dữ liệu thông qua các bảng hệ thống (metadata).
- Sử dụng lệnh 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: (1) lỗ hổng cho phép tấn công chèn mã SQL và (2) lỗ hổng thiết lập quyền truy nhập cơ sở dữ liệu – sử dụng người dùng có quyền quản trị để truy nhập và thao tác dữ liệu của website. Khai thác 2 lỗ hổng này, kẻ tấn công có thể 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 trên máy chủ. Chẳng hạn, hệ quản trị cơ sở dữ liệu MS-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 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

EXEC xp_cmdshell 'net stop MSSQLSERVER' : dừng hoạt động máy chủ CSDL

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 nhập CSDL: `sp_addlogin <username> <password>`

Đổi mật khẩu tài khoản truy nhập 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 gồm:

- Các biện pháp phòng chống dựa trên kiểm tra và lọc dữ liệu đầu vào:
 - + Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
 - + Kiểm tra kích thước và định dạng dữ liệu đầu vào;
 - + 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 procedures) và cơ chế tham số hóa dữ liệu:
 - + Đưa tất cả các câu truy vấn (SELECT) và 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 hạn 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 hỗ trợ bởi nhiều ngôn ngữ lập trình web như ASP.NET, PHP và JSP.
- Các biện pháp phòng chống dựa trên thiết lập quyền truy nhập 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 nhập dữ liệu. Ví dụ: không dùng người dùng *sa* (Microsoft SQL) hoặc *root* (MySQL) làm người dùng truy nhập dữ liệu. Chỉ dùng các người dùng này cho mục đích quản trị.
 - + Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy nhập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục.
 - + Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp trên các bảng dữ liệu. Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục.

- + Cấm hoặc vô hiệu hóa (disable) việc thực hiện các thủ tục hệ thống (các thủ tục cơ sở dữ liệu có sẵn) 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.

2.3.3. Tấn công từ chối dịch vụ

2.3.3.1. Giới thiệu

Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy nhập các tài nguyên mạng. Tấn công DoS có thể được chia thành 2 loại: (1) tấn công logic (Logic attacks) và (2) tấn công gây ngập lụt (Flooding attacks). Tấn công logic 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 Slammer để cập ở Mục 2.3.2.2 là dạng tấn công 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 Attacks, ICMP Flood, HTTP Flood, UDP Flood,... Trong phạm vi của môn học này, chúng ta chỉ đề cập đến 2 kỹ thuật phổ biến nhất là SYN Flood và Smurf.

2.3.3.2. 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 2.21 (a) gồm 3 bước như sau:

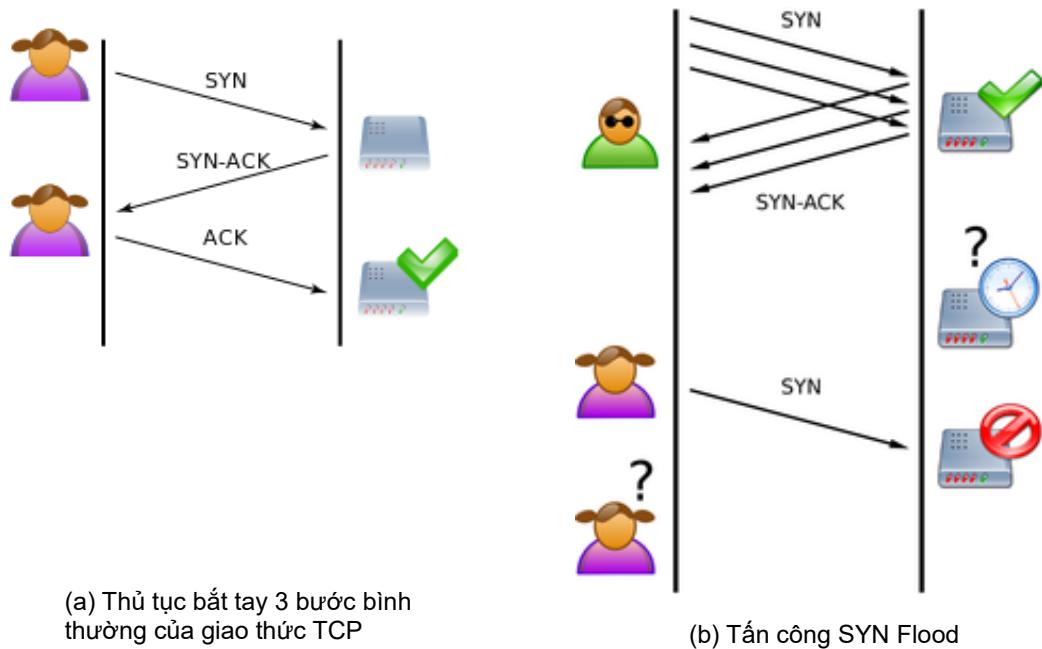
- Người dùng thông qua máy khách gửi yêu cầu mở kết nối (SYN hay SYN-REQ) đến máy chủ;
- Máy chủ nhận được lưu yêu cầu kết nối vào Bảng kết nối (Backlog) và gửi lại xác nhận kết nối SYN-ACK cho máy khách;
- Khi nhận được SYN-ACK từ máy chủ, máy khách gửi lại xác nhận kết nối ACK đến máy chủ. Khi máy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

b. Kịch bản tấn công

Kịch bản tấn công SYN Flood, như minh họa trên Hình 2.21 (b) gồm các bước sau:

- Kẻ tấn công gửi một lượng lớn yêu cầu mở kết nối (SYN-REQ) đến máy nạn nhân;

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



Hình 2.21. (a) Thủ tục bắt tay 3 bước của TCP và (b) Tấn công SYN Flood

Do kẻ tấn công thường sử dụng địa chỉ IP giả mạo, hoặc địa chỉ không có thực làm địa chỉ nguồn (Source IP) trong gói tin IP yêu cầu mở kết nối, nên xác nhận kết nối SYN-ACK của máy nạn nhân không thể đến đích. Đồng thời, kẻ tấn công có thể tạo một lượng rất lớn yêu cầu mở kết nối để chung 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 (cụ thể là bộ nhớ Bảng kết nối) của máy nạn nhân, 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 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:

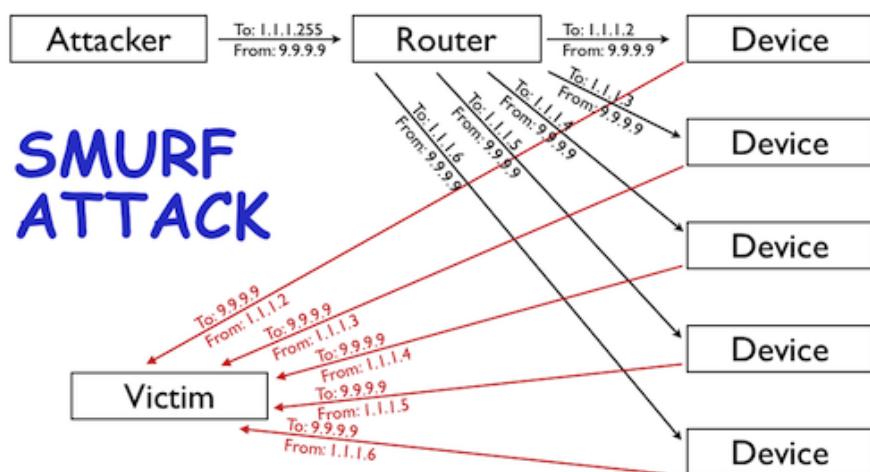
- Sử dụng kỹ thuật lọc địa chỉ giả mạo (Spoofed IP Filtering): Kỹ thuật này đòi hỏi chỉnh sửa giao thức TCP/IP không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước Bảng kết nối: Tăng kích thước Bảng kết nối cho phép tăng khả năng chấp nhận các yêu cầu mở kết nối;

- 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;
- SYN cache: Một yêu cầu mở kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng tường lửa (Firewall) 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.

2.3.3.3. Tấn công Smurf

a. Giới thiệu

Tấn công Smurf là dạng tấn công DoS sử dụng giao thức điều khiển truyền (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 router của mạng chuyển đến tất cả các máy trong mạng đó.



Hình 2.22. Mô hình tấn công Smurf

b. Kịch bản tấn công

Hình 2.22 minh họa mô hình tấn công DoS Smurf. Theo đó, kịch bản tấn công Smurf gồm các bước:

- Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một địa chỉ quảng bá (IP Broadcast address) của một mạng;
- Router 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;
- Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời (reply) đến máy có địa chỉ IP là địa nguồn trong yêu cầu ICMP (là máy nạn nhân). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền, hoặc ngừng hoạt động.

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;
- Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.

Việc cấu hình các router 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 ICMP/Ping.

2.3.4. Tấn công từ chối dịch vụ phân tán

2.3.4.1. Giới thiệu

Tấn công DDoS (Distributed Denial of Service) 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 (scope) 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, và các máy tham gia tấn công DDoS có thể đến từ rất nhiều vị trí địa lý khác nhau trên toàn cầu. Do vậy, việc phòng chống tấn công DDoS gấp nhiều khó khăn hơn so với việc phòng chống tấn công DoS.

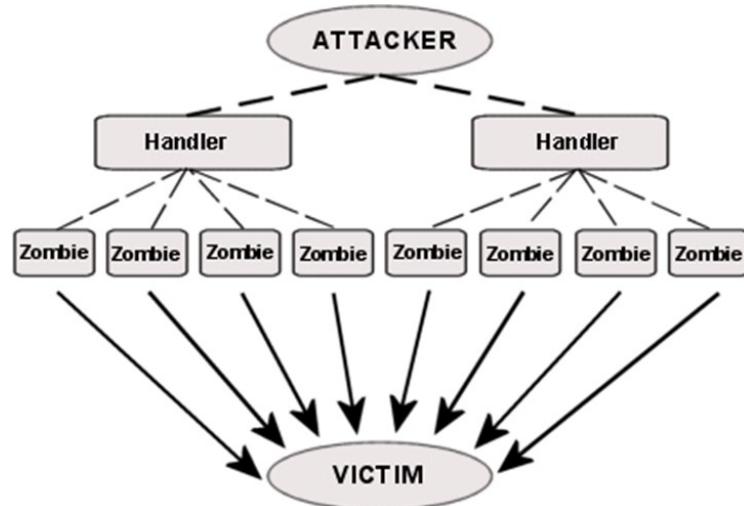
Có thể chia tấn công DDoS thành 2 dạng chính theo mô hình kiến trúc: tấn công DDoS trực tiếp (Direct DDoS) và tấn công DDoS gián tiếp, hay phản xạ (Indirect/Reflective DDoS). Trong tấn công DDoS trực tiếp, các yêu cầu tấn công được các máy tấn công gửi trực tiếp đến máy nạn nhân. Ngược lại, trong tấn công DDoS gián tiếp, các yêu cầu tấn công được gửi đến các máy phản xạ (Reflectors) và sau đó gián tiếp chuyển đến máy nạn nhân.

2.3.4.2. Tấn công DDoS trực tiếp

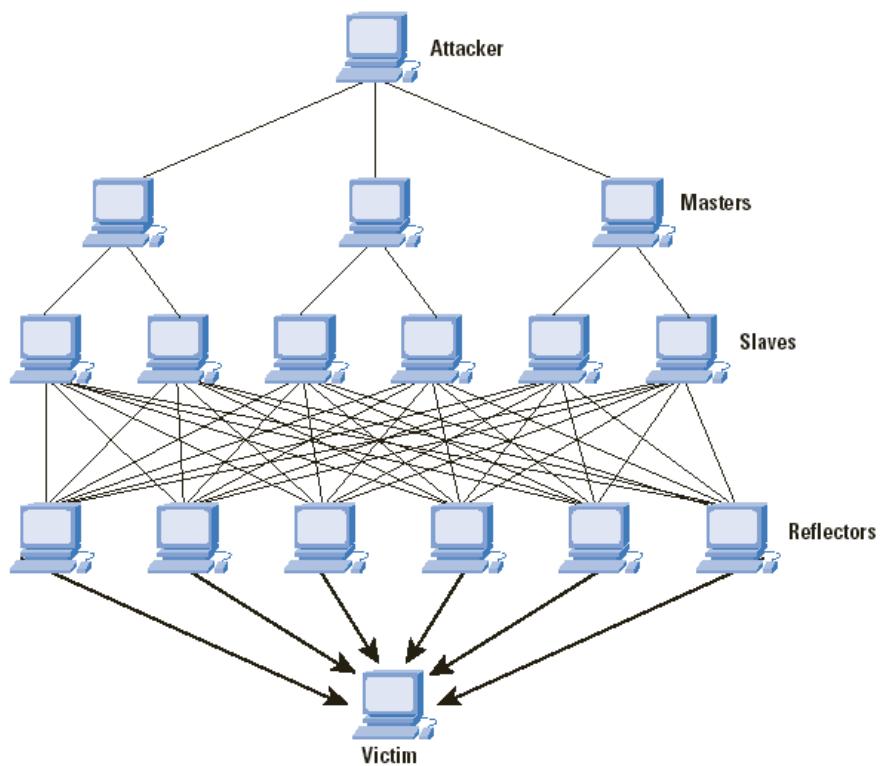
Hình 2.23 minh họa kiến trúc điển hình của dạng tấn công DDoS trực tiếp. Tấn công DDoS trực tiếp được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- Kẻ tấn công (Attacker) chiếm quyền điều khiển hàng ngàn, thậm chí hàng chục ngàn máy tính trên mạng Internet, sau đó bí mật cài các chương trình tấn công tự động (Automated agents) lên các máy này. Các automated agents còn được gọi là các Bot hoặc Zombie (Máy tính ma);
- Các máy bị chiếm quyền điều khiển hình thành mạng máy tính ma, gọi là botnet hay zombie network. Các botnet, hay zombie network không bị giới hạn bởi chủng loại thiết bị và tô pô mạng vật lý;
- Kẻ tấn công có thể giao tiếp với các máy botnet, zombie thông qua một mạng lưới các máy trung gian (handler) gồm nhiều tầng. Phương thức giao tiếp có thể là IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP,...

- Tiếp theo, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân tạo thành cuộc tấn công DDoS;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn, vị trí địa lý khác nhau nên rất khó đối phó và làn vét để tìm ra kẻ tấn công thực sự.



Hình 2.23. Kiến trúc tấn công DDoS trực tiếp



Hình 2.24. Kiến trúc tấn công DDoS gián tiếp hay phản xạ

2.3.4.3. Tấn công DDoS gián tiếp

Hình 2.24 minh họa kiến trúc tấn công DDoS gián tiếp, hay phản xạ. Tấn công DDoS gián tiếp cũng được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- Kẻ tấn công chiếm quyền điều khiển của một lượng lớn máy tính trên mạng Internet, cài đặt phần mềm tấn công tự động bot/zombie (còn gọi là slave), hình thành nên mạng botnet;

- Theo lệnh của kẻ tấn công điều khiển các Slave/Zombie gửi một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác (Reflectors) trên mạng Internet;
- Các Reflectors gửi các phản hồi (Reply) đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;
- Khi các Reflectors có số lượng lớn, số phản hồi sẽ rất lớn và 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 Reflectors bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất lớn trên mạng Internet và không chịu sự điều khiển của kẻ tấn công.

2.3.4.4. 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 (botnet) được hình thành và điều khiển theo nhiều tầng, lớp. 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 khác nhằm loại bỏ các loại bot, zombie, slaves khỏi các hệ thống máy tính;
- Sử dụng các hệ thống lọc đặt trên các router, 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 (block) tạm thời các cổng dịch vụ bị tấn công.

2.3.5. Tấn công giả mạo địa chỉ

2.3.5.1. Giới thiệu

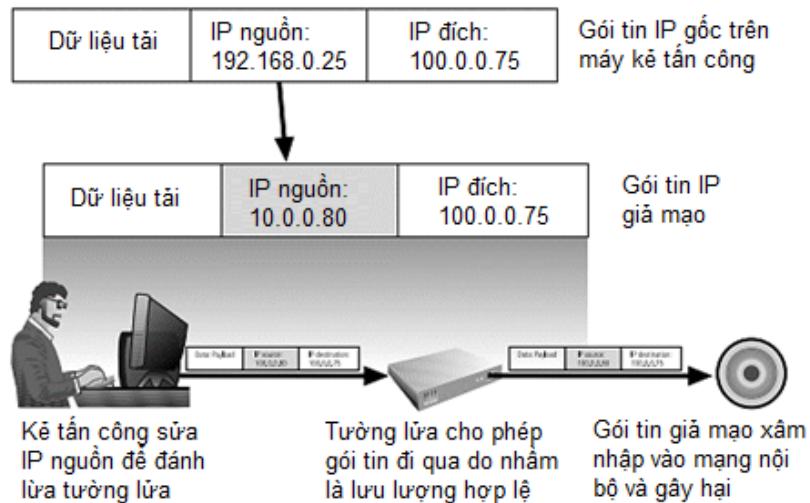
Dạng tấn công giả mạo địa chỉ thường gặp nhất là tấn công giả mạo địa chỉ IP, trong đó kẻ tấn công sử dụng địa chỉ IP giả làm địa chỉ nguồn (Source IP) của các gói tin IP, thường để đánh lừa máy nạn nhân nhằm vượt qua các hàng rào kiểm soát an ninh thông thường. Chẳng hạn, nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của 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 với các máy trong cùng mạng LAN thường được giảm nhẹ.

2.3.5.2. Kịch bản

Hình 2.25 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:

- Giả sử máy 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;
- 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 đến máy nạn nhân. Địa chỉ 100.0.0.80 là địa chỉ cùng mạng LAN với máy nạn nhân 100.0.0.75;

- Nếu tường lửa 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 và gây tác hại cho máy nạn nhân.



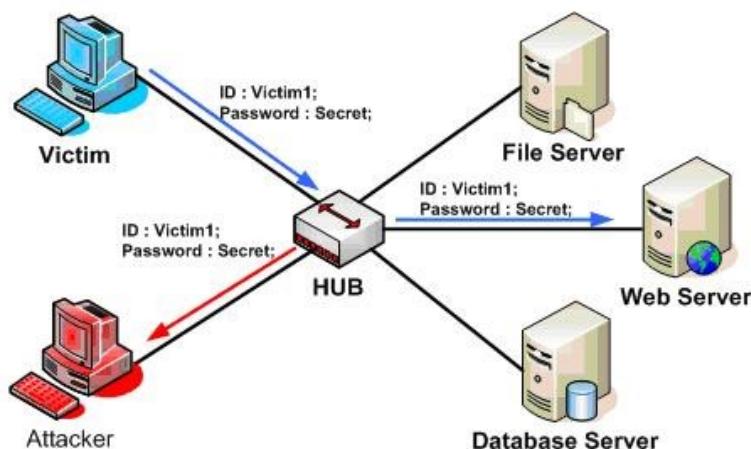
Hình 2.25. Minh họa tấn công giả mạo địa chỉ IP

2.3.5.3. Phòng chống

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 router với nguyên tắc lọc: các gói tin từ mạng ngoài đi vào mạng LAN mà có địa chỉ nguồn là địa chỉ nội bộ của mạng LAN đó thì chúng là các gói tin giả mạo và phải bị chặn.

2.3.6. Tấn công nghe lén

Tấn công nghe lén (Sniffing/Eavesdropping), như minh họa trên Hình 2.26 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 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 2.26. 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.

2.3.7. Tấn công kiểu người đứng giữa

2.3.7.1. Giới thiệu

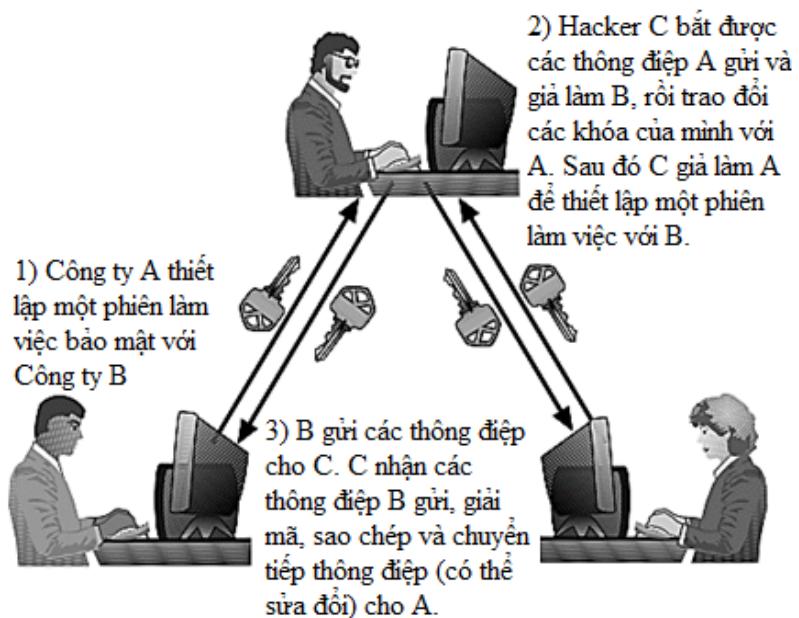
Tấn công kiểu người đứng giữa (Man in the middle) là dạng tấn công dụng quá trình chuyển gói tin đi qua nhiều trạm (hop) thuộc các mạng khác nhau, trong đó kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông và chuyển thông điệp lại cho bên kia. Mục đích chính của dạng tấn công này là đánh cắp thông tin. Hình 2.27 minh họa mô hình tấn công kiểu người đứng giữa trong một phiên truyền file ở dạng rõ (plaintext) sử dụng giao thức FTP giữa máy khách (Client) và máy chủ (Server).



Hình 2.27. Mô hình chung của tấn công kiểu người đứng giữa

2.3.7.2. Kịch bản

Hình 2.28 minh họa 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) bắt và có thể sửa đổi, lạm dụng các thông điệp truyền giữa A và B. Các bước tấn công cụ thể như sau:



Hình 2.28. Một kịch bản tấn công kiểu người đứng giữa

- A gửi các thông điệp để thiết lập một phiên làm việc bảo mật với B;
- 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 với B (có trao đổi khóa với B);
- 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 lạm dụng.

2.3.7.3. Phòng chống

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 chỉ số khóa công khai (Public key certificate) 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.

2.3.8. 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:

- Gửi bom thư bằng cách sử dụng kỹ thuật xã hội, đánh lừa người dùng phát tán email;
- Khai thác lỗi trong hệ thống gửi nhận email SMTP;
- Lợi dụng các máy chủ email không được cấu hình tốt để gửi email (relay) cho chúng.

Tấn công bằng thư rác (Email spamming attack) là dạng tấn công gửi các thư không mong muốn, như thư quảng cáo, thư chứa các phần mềm độc hại. Theo một số thống kê, khoảng 70-80% lượng email gửi trên mạng Internet là thư rác. 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.

2.3.9. Tấn công sử dụng các kỹ thuật xã hội

2.3.9.1. Giới thiệu

Tấn công sử dụng các kỹ thuật xã hội (Social engineering attack) là dạng tấn công phi kỹ thuật nhắm vào người dùng. Dạng tấn công này khai thác các điểm yếu cố hữu của người dùng, như tính 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 nhập hoặc các thông tin có giá trị cho kẻ tấn công. Một số kỹ thuật mà kẻ tấn công thường áp 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/tổ chức;
- Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,...

2.3.9.2. 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, trong đó đã có hàng chục nghìn người ở Mỹ, Canada và Châu Âu đã sập bẫy của kẻ lừa đảo. Kẻ lừa đảo lợi dụng sự ngây thơ và lòng tham của một số người với kịch bản tóm tắt như sau:

- Kẻ lừa đảo gửi thư tay, hoặc email đến nhiều người nhận, mô tả về việc có 1 khoản tiền lớn (từ 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 tham gia một phần số tiền (lên đến 20-30%);
- Nếu người nhận có phản hồi và đồng ý tham gia, kẻ lừa đảo sẽ gửi tiếp thư, hoặc email khác, yêu cầu chuyển cho hắn 1 khoản phí giao dịch (từ vài ngàn đến hàng chục ngàn USD);
- 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, chẳng hạn như thông báo lừa trúng thưởng các tài sản có giá trị lớn để chiếm đoạt khoản "phí trả thưởng", lừa đầu tư vào tài khoản ảo với hứa hẹn lãi suất cao,...

2.3.9.3. Phishing

Phishing là một dạng đặc biệt phát triển rất mạnh của tấn công sử dụng các kỹ thuật xã hội, trong đó kẻ tấn công bẫy người dùng để lấy thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,... Kẻ tấn công có thể giả mạo trang web của các tổ chức tài chính, ngân hàng, sau đó chúng gửi email cho người dùng (địa chỉ email thu thập trên mạng), yêu cầu xác thực thông tin. Hình 2.29 và Hình 2.30 minh họa 2 phishing email gửi cho khách hàng 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 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.



Dear eBay member,

We have reasons to think there are some problems with eBay account. It is possible that these problems may cause your temporary account suspension. Please login to account by [clicking here](#) and check if all your personal informations are right.

Per the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Good luck trading on eBay! .

Regards, Safeharbor Department eBay, Inc .

Hình 2.29. Một phishing email gửi cho khách hàng của mạng đấu giá eBay

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 account⁵. If you would like to continue to use the online banking facility⁶ offered by Royal Bank, please click the link below and renew your security details⁷ immediately. Failure to do so will result in your online account being suspended⁸.

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

We are sorry for any convenience¹⁰ caused and hope you continue to use our online banking facility.

The Royal Bank Online Security Team¹¹

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

Hình 2.30. Một phishing email gửi cho khách hàng của ngân hàng Royal Bank

2.3.9.4. 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, 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 nhập đúng trang web của cơ quan, tổ chức.

2.3.10. Tấn công pharming

Pharming là kiểu tấn công vào trình duyệt của người dùng, trong đó người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu và tải 1 website khác, thường là website 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 vào hệ thống để điều khiển trình duyệt của người dùng và (2) kẻ tấn công có thể tấn công vào hệ thống tên miền (DNS) để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.

Hình 2.31 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 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 điều khiển trình duyệt.

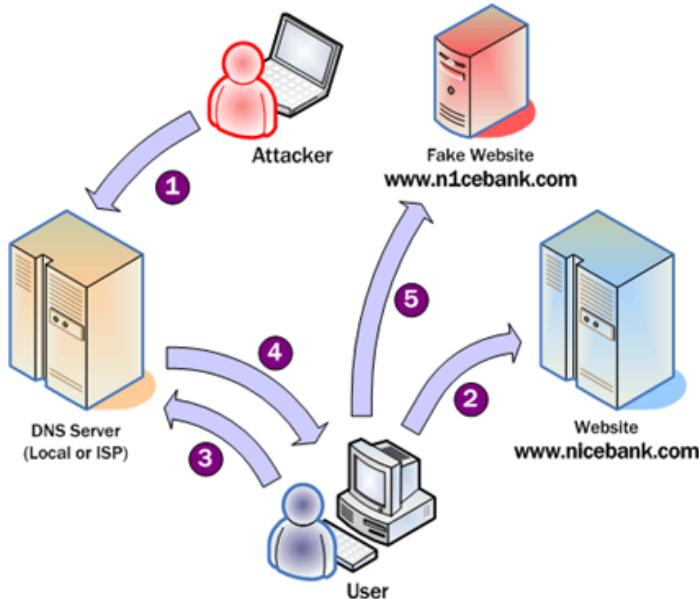


Hình 2.31. Tấn công pharming "cướp" trình duyệt

Hình 2.32 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 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 2.32. Tấn công pharming thông qua tấn công vào máy chủ DNS

2.3.11. 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 [12]. 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 tiến 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.

2.4. Các dạng phần mềm độc hại

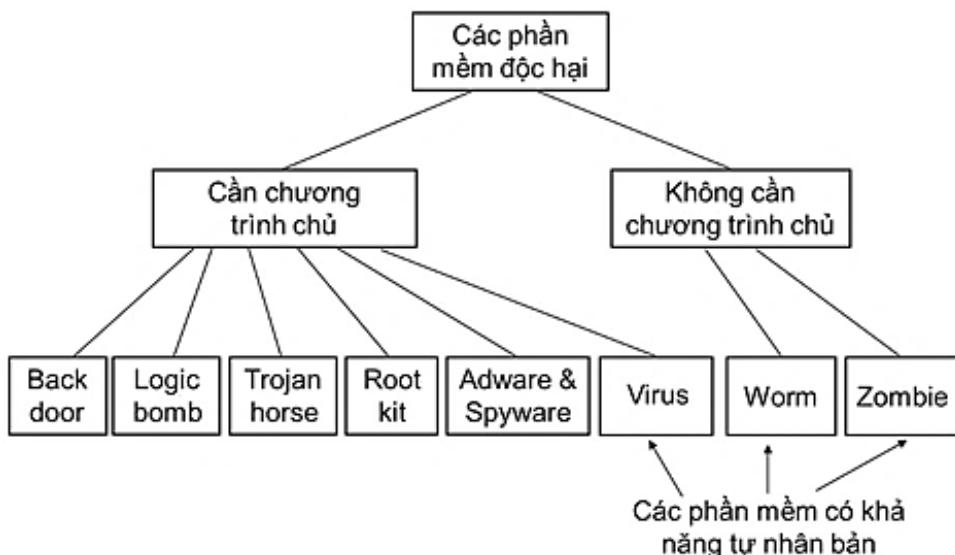
Các phần mềm độc hại, còn gọi là phần mềm mã độc (Malicious software), hay ngắn gọn là mã độc là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống. Khi mới được phát hiện vào những năm 1970-1980, các phần mềm độc hại còn tương đối ít chủng loại và được gọi chung là vi rút (virus). 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) được sử dụng chỉ các dạng mã độc thay thế cho thuật ngữ “vi rút”.

2.4.1. Phân loại

Các phần mềm độc hại (Malware hay Malicious software) 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.

Có nhiều phương pháp phân loại các phần mềm độc hại, trong đó một phương pháp được thừa nhận rộng rãi là chia các phần mềm độc hại thành 2 nhóm chính như biểu diễn trên Hình 2.33. Theo đó, các phần mềm độc hại được chia thành 2 nhóm chính dựa trên phương pháp lây nhiễm như sau:

- Các phần mềm độc hại cần chương trình chủ, vật chủ (host) để ký sinh và lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Logic bomb (Bom logic), Back door (Cửa hậu), Trojan horse (Con ngựa thành Tơ roa), Virus (Vi rút), Rootkit, Adware (Phần mềm quảng cáo) và Spyware (Phần mềm gián điệp).
- Các phần mềm độc hại không cần chương trình chủ, vật chủ để lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Worm (Sâu) và Zombie hay Bot (Phần mềm máy tính ma).



Hình 2.33. Các dạng phần mềm độc hại

Trong số các phần mềm độc hại, 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 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 2.33.

2.4.2. Mô tả các dạng phần mềm độc hại

2.4.2.1. Logic bomb

Logic bomb (Bom lô gíc) là các đoạn mã độc thường được “nhúng” vào các chương trình bình thường và thường 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, hoặc một ngày trong tuần. Khi “phát nổ” bom logic có thể xoá dữ liệu, file, tắt cả hệ thống...

Thực tế đã ghi nhận quả bom logic do Tim Lloyd cài lại đã “phát nổ” tại công ty Omega Engineering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom lô gíc này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD cho công ty. Bản thân Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.

2.4.2.2. Trojan Horse

Trojan horse 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 horse thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập. Chẳng hạn, trong một hệ thống nhiều người dùng, một người dùng (kẻ tấn công) có thể tạo ra một trojan đội lót một chương trình hữu ích đặt ở thư mục chung. Khi trojan này được thực thi bởi một người dùng khác, nó sẽ thay đổi quyền truy nhập các file và thư mục của người dùng đó, cho phép tắt cả người dùng (trong đó có kẻ tấn công) truy nhập vào các file của người dùng đó.

2.4.2.3. Back door

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

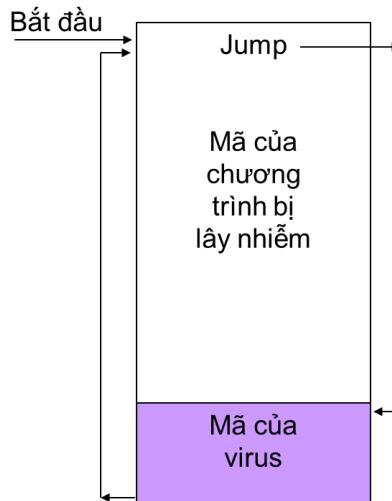
2.4.2.4. Vi rút

a. Giới thiệu

Vi rút (Virus) là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút sẽ tiếp tục “lây nhiễm” sang các chương trình khác. 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 khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...

Vi rút có thể thực hiện được mọi việc mà một chương trình 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 chạy. Hình 2.34 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.



Hình 2.34. Chèn và gọi thực hiện mã vi rút

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.

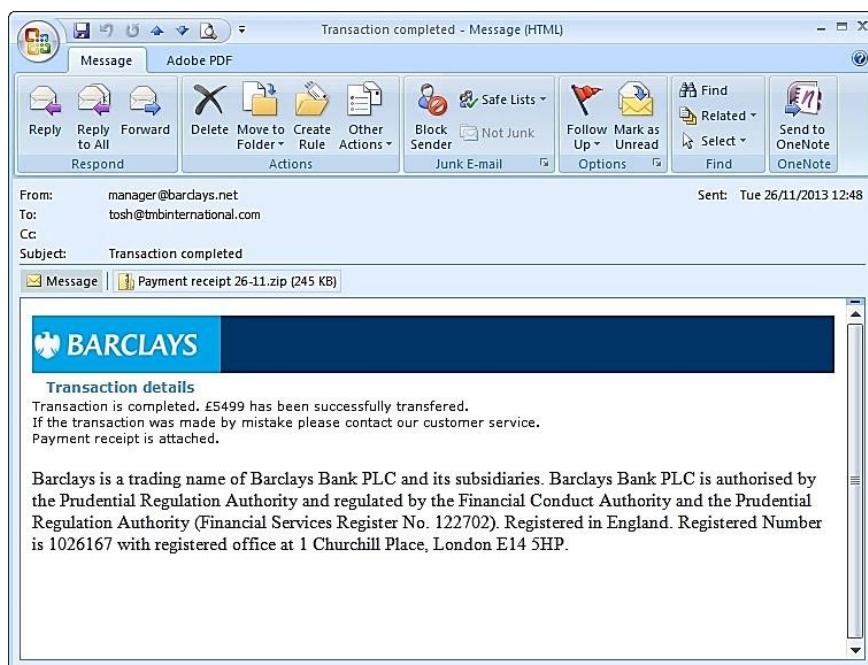
Boot vi rút là dạng vi rút lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record). Do boot vi rút lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động. Boot vi rút có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy nhập 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. Mỗi khi chương trình được kích hoạt hoặc file dữ liệu được nạp vào bộ nhớ, vi rút được kích hoạt. Mọi chương trình tiếp theo được kích hoạt đều bị lây nhiễm vi rút này. File vi rút có thể làm hỏng chương trình, hỏng hoặc phá hủy các file dữ liệu, 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 bộ ứng dụng Microsoft Office, gồm ứng dụng soạn thảo Word, bảng tính Excel, trình email Outlook,... Các đoạn mã macro thường được dùng để tự động hóa 1 số việc 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 auto-executed macros, như AutoExecute, Automacro và Command macro. Theo thống kê, macro vi rút chiếm khoảng 2/3 tổng lượng vi rút đã được phát hiện. Lượng tài liệu bị lây nhiễm macro vi rút đã giảm đáng kể từ khi Microsoft Office 2010 có thiết lập ngầm định không cho phép tự động chạy các macro.

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 2.35 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.

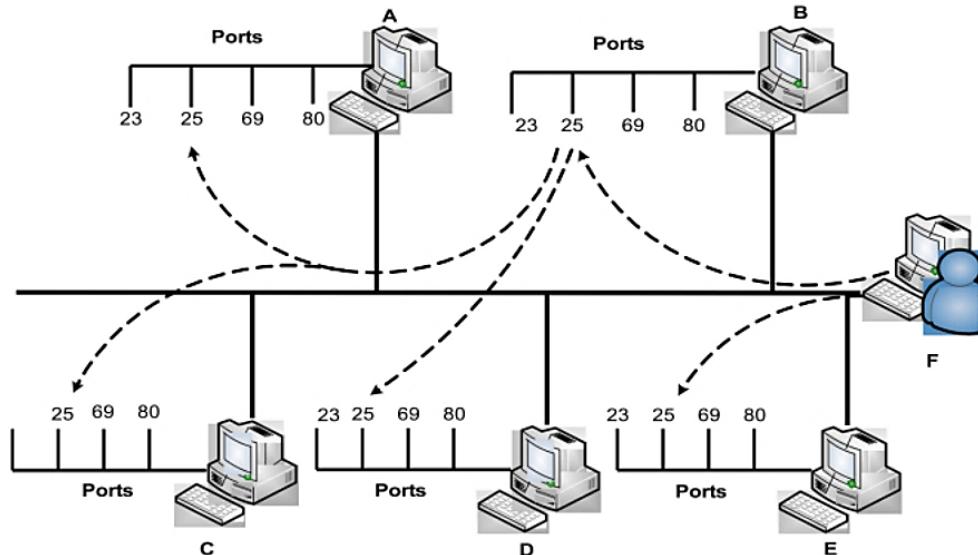


Hình 2.35. Một email do vi rút gửi đến người dùng

2.4.2.5. 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 là sâu mạng (network worm) sử dụng kết nối mạng để lây lan từ máy này sang máy khác. Hình 2.36 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, khi sâu hoạt động, nó tương tự vi rút.

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:



Hình 2.36. Một mô hình lây lan của sâu mạng

- Lây lan qua thư điện tử: Sâu sử dụng email để gửi bản sao của mình đến các máy khác.
- 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 Red 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. Sau đó, sâu Nimda được phát hiện vào tháng 9/2001 là sâu có khả năng lây lan theo nhiều con đường:

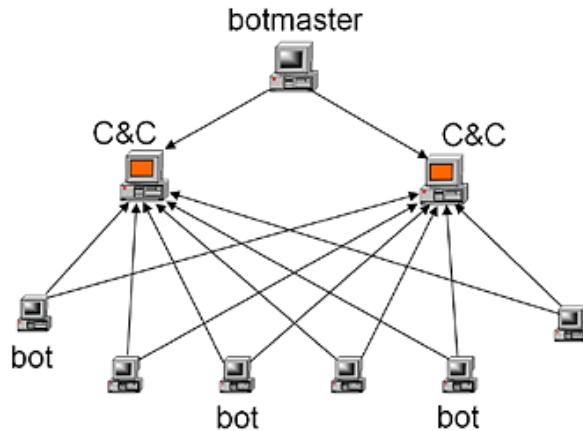
- Qua email từ máy client sang client.
- Qua các thư mục chia sẻ trên mạng.
- Từ máy chủ web sang trình duyệt.
- Từ máy khách đến máy chủ nhờ khai thác các lỗ máy chủ.

Chỉ 22 phút sau khi ra đời, Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet vào thời điểm đó.

2.4.2.6. Zombie/Bot

Zombie/Bot (còn gọi là Automated agent – từ đây thống 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 2.37 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.

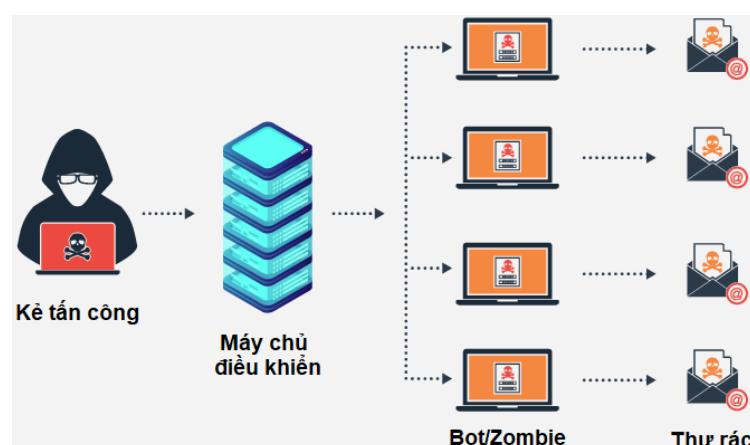


Hình 2.37. Mô hình mô hình giao tiếp giữa các thành phần trong botnet

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 2.23 và Hình 2.24 trong mục 2.3.4. 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 2.38.

2.4.2.7. Rootkit

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



Hình 2.38. Mô hình tin tặc sử dụng các máy tính Zombie/Bot để gửi thư rác

2.4.2.8. 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 hoặc một dịch vụ miễn phí. Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được tự động cài đặt và kích hoạt mà không được sự đồng ý của người dùng.

Spyware 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 (giám sát hệ thống), trojan, adware, and tracking cookies (các cookie theo dõi). 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 tin tức 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.

2.4.3. Phòng chống phần mềm độc hại

2.4.3.1. Nguyên tắc chung

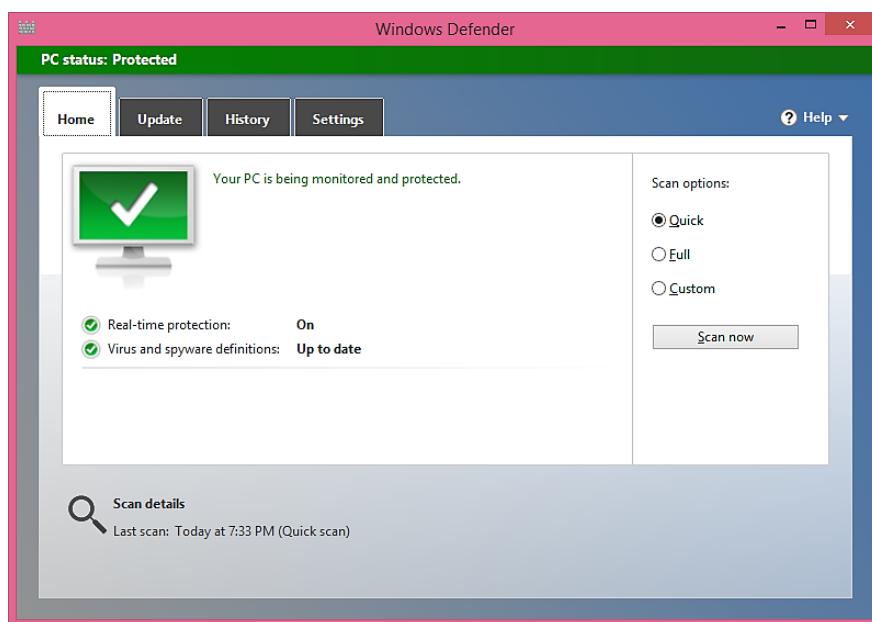
Có thể thấy các phần mềm độc hại là một trong các nguy cơ gây mất an toàn lớn nhất và thường trực nhất đối với thông tin, hệ thống và người dùng do sự bùng nổ về số lượng, mức độ tinh vi ngày càng cao và khả năng phá hoại ngày càng lớn của chúng. Nguyên tắc chung trong phòng chống phần mềm độc hại vẫn 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.

2.4.3.2. 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.



Hình 2.39. Màn hình chính của Microsoft Windows Defender

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 2.39
- Semantec Norton Antivirus
- Kaspersky Antivirus
- BitDefender Antivirus
- AVG Antivirus

- McAfee VirusScan
- Trend Micro Antivirus
- F-secure Antivirus và
- BKAV Antivirus.

2.5. Câu hỏi ôn tập

- 1) Điểm yếu hệ thống là gì? Liệt kê các nguyên nhân của sự tồn tại các điểm yếu trong hệ thống.
- 2) Lỗ hổng bảo mật là gì? Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống?
- 3) Nêu các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng.
- 4) Mối đe dọa (threat) là gì? Nêu quan hệ giữa lỗ hổng và mối đe dọa.
- 5) Tấn công là gì? Có thể giảm thiểu khả năng bị tấn công bằng cách nào?
- 6) Mô tả 4 loại tấn công chính và 2 kiểu tấn công chủ động và thụ động.
- 7) Nêu mục đích và các dạng tấn công vào mật khẩu.
- 8) 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 tin tặc thực hiện hành động gì trên hệ thống nạn nhân?
- 9) Nêu các biện pháp phòng chống tấn công chèn mã SQL.
- 10) Vẽ sơ đồ, mô tả cơ chế tấn công SYN Flood và các biện pháp phòng chống.
- 11) Vẽ sơ đồ, mô tả cơ chế tấn công Smurf và các biện pháp phòng chống.
- 12) Vẽ sơ đồ và mô tả kịch bản tấn công DDoS trực tiếp và tấn công DDoS gián tiếp.
- 13) Mô tả cơ chế và các biện pháp phòng chống tấn công người đứng giữa.
- 14) 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.
- 15) Tấn công pharming là gì? Mô tả các dạng tấn công pharming.
- 16) Tấn công APT là gì? Mô tả các thuộc tính chính của tấn công APT.
- 17) Phần mềm độc hại là gì? Phân loại các phần mềm độc hại.
- 18) Vi rút là gì? Nêu các phương pháp lây nhiễm và các loại vi rút.
- 19) Trojan là gì? Mô tả cơ chế hoạt động của trojan.
- 20) Sâu máy tính là gì? Nêu điểm khác biệt cơ bản của sâu và vi rút. Nêu các phương pháp lây lan của sâu.
- 21) Zombie/Bot là gì? Mô tả cơ chế hoạt động của Zombie/Bot.
- 22) Nêu nguyên tắc chung trong phòng chống phần mềm độc hại. Tại sao chỉ nên cài đặt và chạy một bộ phần mềm quét phần mềm độc hại hoạt động ở chế độ “bảo vệ theo thời gian thực” hại tại mỗi thời điểm?

CHƯƠNG 3. ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

Chương 3 giới thiệu các khái niệm cơ bản về mật mã, hệ mã hóa, các phương pháp mã hóa. Phản tiếp theo của chương 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), các hàm băm (MD5 và SHA1), chữ ký số, chứng chỉ số và PKI. Phần cuối của chương đề cập vấn đề quản lý và phân phối khóa, và một số giao thức đảm bảo an toàn thông tin dựa trên mã hóa.

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

3.1.1. Các khái niệm

Mật mã

Theo từ điển Webster's Revised Unabridged Dictionary: "cryptography is the act or art of writing secret characters", hay *mật mã là một hành động hoặc nghệ thuật viết các ký tự bí mật*. Còn theo từ điển Free Online Dictionary of Computing: "cryptography is encoding data so that it can only be decoded by specific individuals", có nghĩa là *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 (Unencrypted information) là thông tin ở dạng có thể hiểu được.

Bản mã (Ciphertext), hay thông tin đã được mã hóa (Encrypted information) là thông tin ở dạng đã bị xáo trộn.

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

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

Hình 3.1 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.

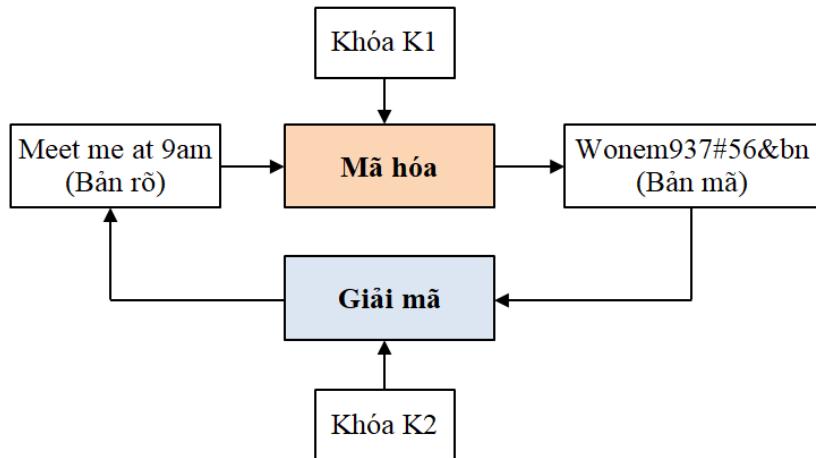
Giải thuật mã hóa & giải mã, Bộ mã hóa, Khóa/Chìa, Không gian khóa

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.

Một bộ mã hóa (Cipher) gồm một giải thuật để mã hóa và một giải thuật để giải mã thông tin.

Khóa/Chìa (Key) là một chuỗi được sử dụng trong giải thuật mã hóa và giải mã.

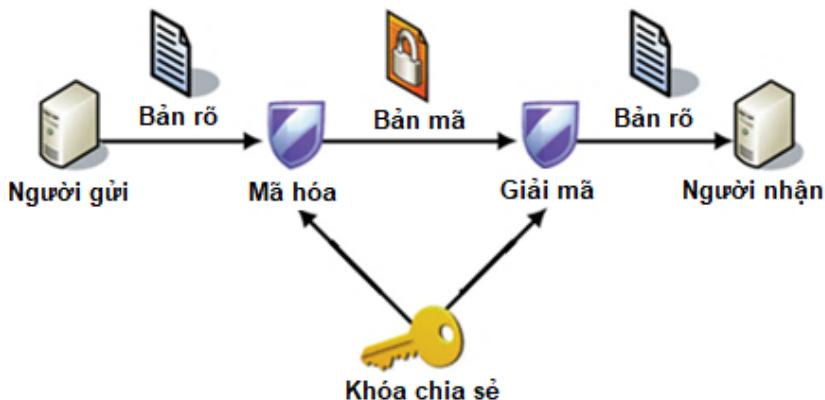
Không gian khóa (Keyspace) là tổng số khóa có thể có của một hệ mã hóa. Ví dụ, nếu sử dụng khóa kích thước 64 bit thì không gian khóa là 2^{64} .



Hình 3.1. Các khâu Mã hóa và Giải mã của một hệ mã hóa

Mã hóa khóa đối xứng, Mã hóa khóa bát 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 3.2 minh họa hoạt động của một hệ mã hóa khóa đối xứng, trong đó một khóa bí mật duy nhất được sử dụng cho cả hai khâu mã hóa và giải mã một thông điệp.

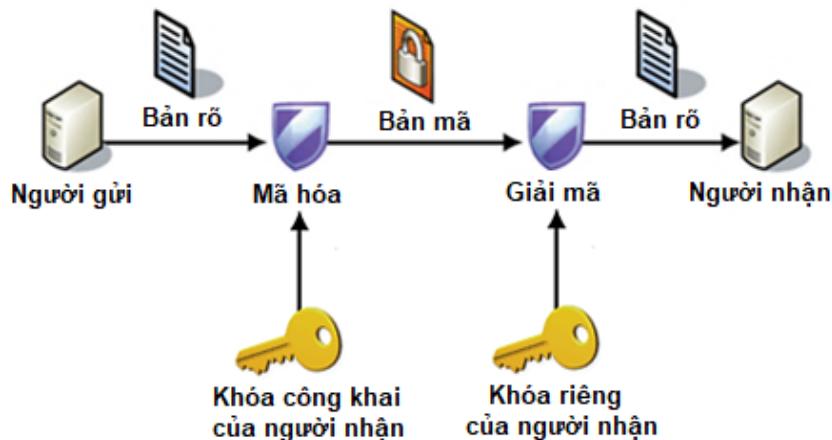


Hình 3.2. Mã hóa khóa đối xứng sử dụng chung 1 khóa bí mật

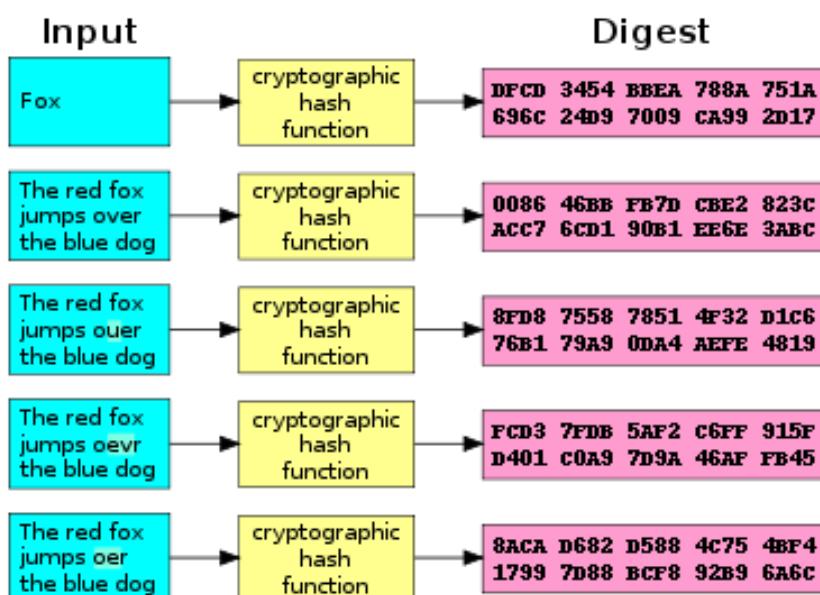
Mã hóa khóa bát đối xứng (Asymmetric key cryptography) là dạng mã hóa trong đó một cặp khóa được sử dụng: khóa công khai (public key) dùng để mã hóa, khóa riêng (private key) dùng để giải mã. Chỉ có khóa riêng cần phải giữ bí mật, còn khóa công khai có thể phổ biến rộng rãi. Do khóa để mã hóa có thể công khai nên đối khi mã hóa khóa bát đối xứng còn được gọi là mã hóa khóa công khai (Public key cryptography). Hình 3.3 minh họa hoạt động của một hệ mã hóa khóa bát đối xứng, trong đó một khóa công khai được sử dụng cho khâu mã hóa và khóa riêng cho khâu giải mã thông điệp.

Hàm băm (Hash function) là một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định. Hình 3.4 minh họa đầu vào (Input) và đầu ra (Digest) của hàm băm. Trong các loại hàm băm, hàm băm 1 chiều (One-way hash function) là hàm

băm, trong đó việc thực hiện mã hóa tương đối đơn giản, còn việc giải mã thường có độ phức tạp rất lớn, hoặc không khả thi về mặt tính toán.



Hình 3.3. Mã hóa khóa bất đối xứng sử dụng một cặp khóa



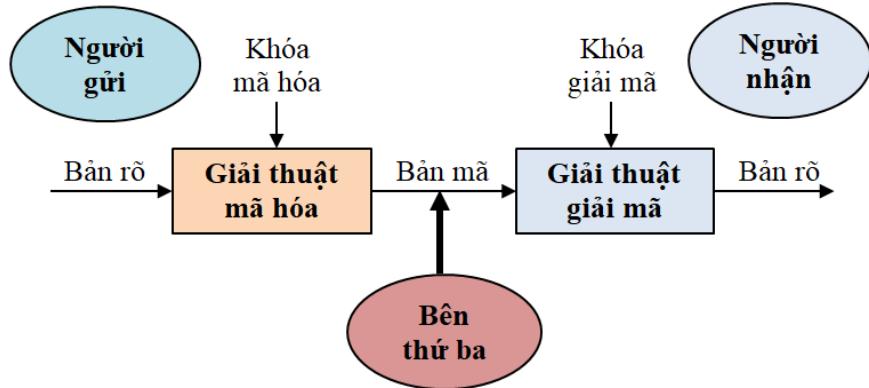
Hình 3.4. Minh họa đầu vào (Input) và đầu ra (Digest) của hàm băm

Thám mã hay phá mã (Cryptanalysis) 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 khói 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.

3.1.2. 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 3.5 nêu các thành phần của một hệ mã hóa đơn giản dùng để đảm bảo tính bí mật của thông tin 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. Một thành phần quan trọng khác của một hệ mã hóa là không gian khóa - là tập hợp tất cả các khóa có thể có. Ví dụ, nếu chọn kích thước khóa là 64 bit thì không gian khóa sẽ là 2^{64} . Nhìn chung, hệ mã hóa có độ an toàn càng cao nếu không gian khóa lựa chọn càng lớn.



Hình 3.5. Các thành phần của một hệ mã hóa đơn giản

3.1.3. Lịch sử mã hóa

Có thể nói mã hóa hay 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 ứng dụng mật mã:

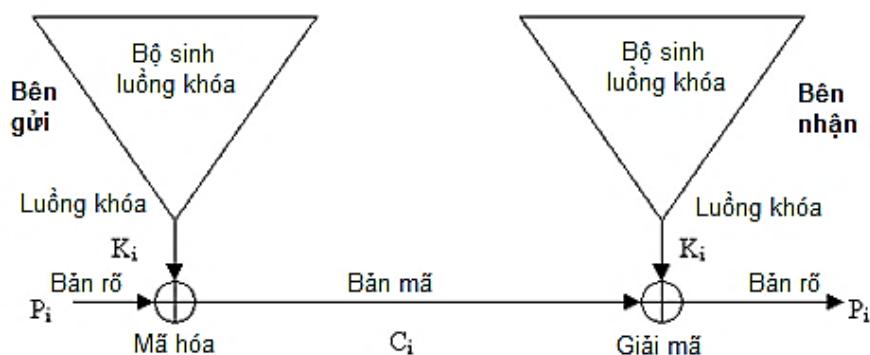
- Các kỹ thuật mã hóa thô sơ đã được người cổ Ai cập sử dụng cách đây 4000 năm.
- Người cổ Hy lạp, Ấn độ cũng đã sử dụng mã hóa cách đây hàng ngàn năm.
- Các kỹ thuật mã hóa chỉ thực sự phát triển mạnh từ thế kỷ 1800 nhờ công cụ toán học, và phát triển vượt bậc trong thế kỷ 20 nhờ sự phát triển của máy tính và ngành công nghệ thông tin.
- 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 Mỹ (NSA – National Security Agency) thừa 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 bất đối xứng (Asymmetric key cryptography), hay mã hóa khóa công khai (Public key cryptography) đưa 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 và do các hệ mã hóa khóa bí mật gấp khó khăn trong quản lý và trao đổi khóa, đặc biệt khi số lượng người dùng lớn.
- Năm 1977, ba nhà khoa học 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 trong chữ ký số.

- Năm 1991, phiên bản đầu tiên của PGP (Pretty Good Privacy) ra đời.
- Năm 2000, chuẩn mã hóa AES (Advanced Encryption Standard) được thừa nhận và ứng dụng rộng rãi.

3.1.4. Mã hóa dòng và mã hóa khối

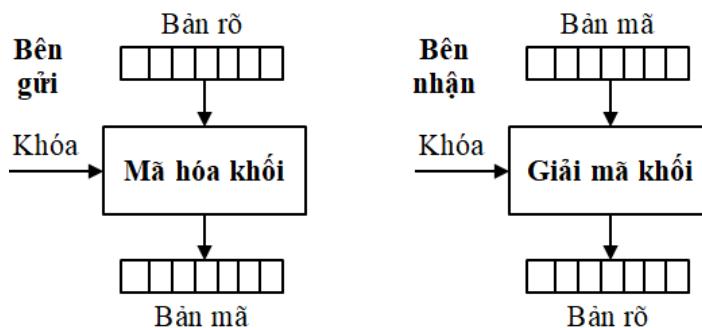
3.1.4.1. Mã hóa dòng

Mã hóa dòng hay mã hóa luồng (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 3.6 biểu diễn quá trình mã hóa và giải mã trong mã hóa dòng. 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 C_i để khôi phục bit rõ P_i . Một bộ sinh luồng khóa được sử dụng để liên tục sinh các bit khóa K_i từ khóa gốc K . Các giải thuật mã hóa dòng tiêu biểu như A5, hoặc RC4 được sử dụng rộng rãi trong truyền thông, viễn thông.



Hình 3.6. Mô hình phương pháp mã hóa dòng

3.1.4.2. Mã hóa khối



Hình 3.7. Mô hình phương pháp 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 3.7 biểu diễn quá trình mã hóa và giải mã trong mã hóa khối. Theo đó, ở bên gửi bản rõ được chia thành các khối 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 lại được chia thành các khối và từng khối lại 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 được sử dụng rất rộng rãi trong mã hóa dữ liệu với kích thước khối 64, hoặc 128 bit.

3.1.5. 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 (confidentiality), toàn vẹn (integrity), 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,...)
- Kiểm soát truy cập
- Các công cụ cho đảm bảo an toàn cho truyền thông không dây
- Các nền tảng bảo mật như PKI, PGP
- 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 khối chuỗi (Blockchain), tiền kỹ thuật số (Bitcoin, Ethereum,...).

3.2. 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 kể trên.

3.2.1. 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 3.8 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 ($A \rightarrow D$, $B \rightarrow E$, $C \rightarrow F$, ...). Bản rõ “LOVE” được mã hóa thành “ORYH”.

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

Hình 3.8. Mã hóa bằng hệ mã hóa Caesar cipher

Để tăng độ an toàn của phương pháp thay thế, người ta có thể sử dụng nhiều bộ chữ mã, như minh họa trên Hình 3.9 với 4 bộ chữ mã (Substitution cipher), với nguyên tắc thay thế: ký tự số 1 ở bản rõ thay thế sử dụng bộ chữ mã số 1, ký tự số 2 sử dụng bộ chữ mã số 2, ..., ký tự số 5 sử dụng bộ chữ mã số 1, ký tự số 6 sử dụng bộ chữ mã số 2, ... Nếu các bộ chữ mã được sắp đặt ngẫu nhiên thì 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.

Bản rõ =	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Bộ mã thay thế 1 =	DEFGHIJKLMNOPQRSTUVWXYZABC
Bộ mã thay thế 2 =	GHIJKLMNOPQRSTUVWXYZABCDEF
Bộ mã thay thế 3 =	JKLMNOPQRSTUVWXYZABCDEFHGI
Bộ mã thay thế 4 =	MNOPQRSTUVWXYZABCDEFHGIJKL
TEXT --> WKGF	

Hình 3.9. Phương pháp thay thế với 4 bộ chữ mã

3.2.2. Phương pháp hoán vị

Phương pháp hoán vị, hoặc đổi chỗ (permutation) thực hiện sắp xếp lại các giá trị trong một khối bản rõ để tạo bản mã. Thao tác hoán vị có thể thực hiện với từng bit hoặc từng byte (ký tự). Hình 3.10 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 3.11 minh họa 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 “SACKGAULSPARENNOONE” ta có 3 khối, 2 khối đầu 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.

Khóa	1→4, 2→8, 3→1, 4→5, 5→7, 6→2, 7→6, 8→3
Vị trí bit	87654321 87654321 87654321 87654321
Các khối bản rõ 8-bit	00100101 01101011 10010101 01010100
Bản mã	00001011 10111010 01001101 01100001

Hình 3.10. Phương pháp hoán vị thực hiện đổi chỗ các bit

Vị trí ký tự:	87654321 87654321 87654321 87654321
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 3.11. Phương pháp hoán vị thực hiện đổi chỗ các ký tự

3.2.3. Phương pháp XOR

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 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 3.12. Ví dụ mã hóa bằng phương pháp XOR

Phương pháp mã hóa XOR sử dụng phép toán logic XOR 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 3.12 minh họa quá trình mã hóa

bản rõ “CAT” với khóa “VVV”. Theo đó, các ký tự của bản rõ và khóa 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.

3.2.4. Phương pháp Vernam

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

- Các ký tự của bản rõ và các ký tự của tập nối thêm (*one-time pad*) được chuyển thành số trong khoảng 1-26;
- Cộng giá trị của ký tự trong bản rõ với giá trị tương ứng trong tập nối thêm;
- Nếu giá trị cộng lớn hơn 26 thì đem trừ cho 26 (đây chính là phép modulo – chia lấy phần dư).
- Chuyển giá trị số thành ký tự mã.

Hình 3.13 minh họa mã hóa bản rõ “SACKGAULSPARENOONE” bằng phương pháp Vernam với tập 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:																		
	03																	18
Bản mã:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

Hình 3.13. Mã hóa bằng phương pháp Vernam

3.2.5. 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 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*

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

3.2.6. Phương pháp hàm băm

Các hàm băm (Hash functions) là các giải thuật để tạo các bản tóm tắt (digest) của thông điệp, thường được sử dụng để nhận dạng và đảm bảo tính toàn vẹn của thông điệp.

Độ dài của thông điệp đầu vào là bất kỳ, nhưng đầu ra hàm băm thường có độ dài cố định. Chi tiết về các hàm băm được ở mục 3.3.3. Các hàm băm thông dụng gồm:

- Các hàm băm MD2, MD4, MD5 với độ dài chuỗi đầu ra là 128 bit;
- Hàm băm MD6 cho chuỗi đầu ra có độ dài trong khoảng 0 đến 512 bit;
- Các hàm băm SHA0, SHA1 với độ dài chuỗi đầu ra là 160 bit;
- Các hàm băm SHA2, gồm SHA256, SHA384, SHA512 cho phép một số lựa chọn chuỗi đầu ra tương ứng 256, 384 và 512 bit;
- Hàm băm SHA3 cho chuỗi đầu ra có độ dài trong khoảng 0 đến 512 bit;
- Hàm băm CRC32 với chuỗi đầu ra 32 bit sử dụng trong kiểm tra dư thừa mạch vòng.

3.3. 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
- Các giải thuật mã hóa khóa bất đối xứng với đại diện tiêu biểu là RSA.

3.3.1. Các giải thuật mã hóa khóa đối xứng

3.3.1.1. 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 3.2, mục 3.1 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 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 có độ an toàn cao và tốc độ thực thi nhanh. Tuy nhiên, nhược điểm lớn nhất của các hệ mã hóa khóa đối xứng 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, Twofish, RC4 và RC5. Phần tiếp theo của mục này là

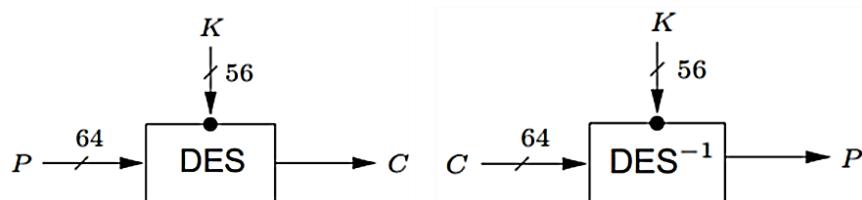
mô tả các giải thuật mã hóa DES, 3-DES và AES do chúng là các giải thuật đã và đang được sử dụng rộng rãi nhất trên thực tế.

3.3.1.2. Giải thuật mã hóa DES

a. Giới thiệu

DES (Data Encryption Standard) được phát triển tại IBM với tên gọi Lucifer vào đầu những năm 1970 và được chấp nhận là chuẩn mã hóa ở Mỹ vào năm 1977. DES được sử dụng rộng rãi trong những năm 1970 và 1980. DES là dạng mã hóa khối với khối dữ liệu vào kích thước 64 bit và khóa 64 bit, trong đó thực sự sử dụng 56 bit (còn gọi là kích thước hiệu dụng của khóa) và 8 bit dùng cho kiểm tra chẵn lẻ.

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 3.14, 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^{-1} biểu diễn khâu giải mã. Hiện nay DES được coi là không an toàn do nó có không gian khóa nhỏ, dễ bị vét cạn và tốc độ tính toán của các hệ thống máy tính ngày càng nhanh trong những năm gần đây.



Hình 3.14. Các khâu mã hóa và giải mã của DES

b. Thủ tục sinh khoá phụ

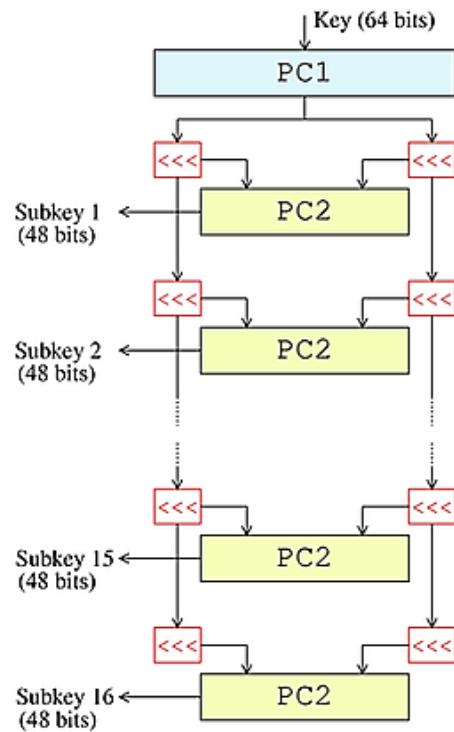
DES sử dụng một thủ tục sinh 16 khóa phụ từ khóa chính để sử dụng trong 16 vòng lặp hàm Feistel. Hình 3.15 minh họa thủ tục sinh 16 khóa phụ từ khóa chính của DES. Các bước xử lý chính của thủ tục sinh khóa phụ như sau:

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

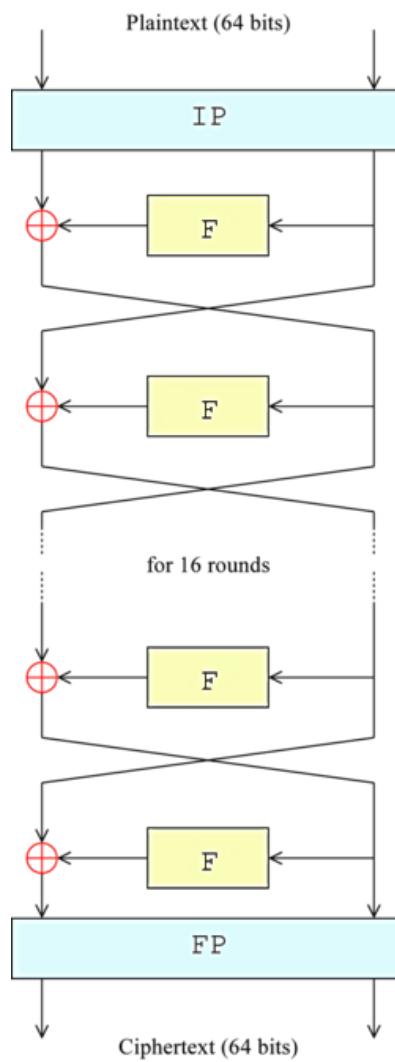
c. Mã hóa khối bản rõ

Với mỗi khối dữ liệu đầu vào 64 bit, DES thực hiện 3 bước xử lý như minh họa trên Hình 3.16 để chuyển nó thành khối 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). 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).



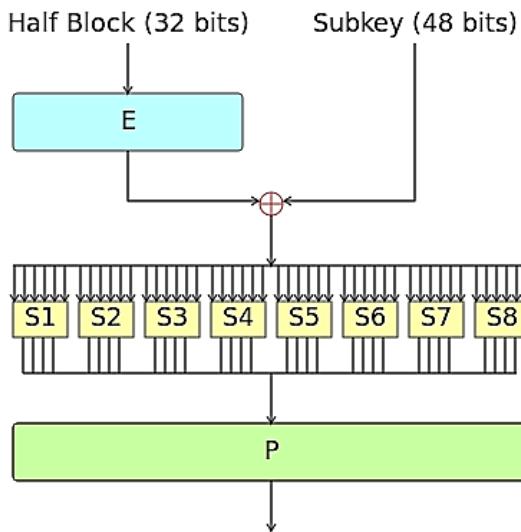
Hình 3.15. Thủ tục sinh các khóa phụ từ khóa chính của DES



Hình 3.16. Các bước xử lý chuyển khói rõ 64 bit thành khói mã 64 bit của DES

Hàm Feistel (F) là hạt nhân trong các vòng lặp xử lý dữ liệu của DES. Trước hết, khối 64 bit được chia thành 2 khối 32 bit và được xử lý lần lượt. Hàm Feistel được thực hiện trên một khối dữ liệu 32 bit gồm 4 bước xử lý như minh họa trên Hình 3.17. Cụ thể, các bước xử lý của DES trên mỗi khối 32 bit (Half Block 32 bits) như sau:

- E (Expansion): thực hiện mở rộng 32 bit khối đầu vào thành 48 bit bằng cách nhân đôi một nửa số bit.
- \oplus : Trộn khối 48 bit kết quả ở bước E với khóa phụ 48 bit. Có 16 khóa phụ (Subkey) được tạo từ khóa chính để sử dụng cho 16 vòng lặp.
- Si (Substitution): Khối dữ liệu 48 bit được chia thành 8 khối 6 bit và được chuyển cho 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 (Security core) của DES.
- P (Permutation): khối 32 bit đầu ra từ các bộ thay thế được sắp xếp bằng phép hoán vị cố định (Fixed permutation) cho ra đầu ra 32 bit.



Hình 3.17. Các bước xử lý của hàm Feistel (F)

d. Giải mã khối bǎn mǎ

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

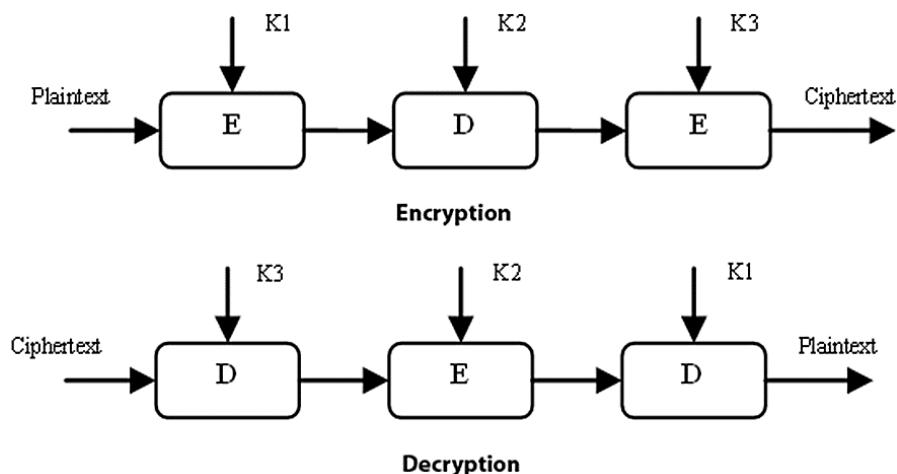
3.3.1.3. 3-DES

3-DES hay Triple DES có tên đầy đủ là Triple Data Encryption Algorithm (TDEA) 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:

- Lựa chọn 1: cả 3 khóa độc lập, với tổng kích thước bộ khóa là 168 bit;
- Lựa chọn 2: K1 và K2 độc lập, K3 = K1, với tổng kích thước bộ khóa là 112 bit;

- Lựa chọn 3: 3 khóa giống nhau, $K_1 = K_2 = K_3$, với tổng kích thước bộ khóa là 56 bit.

Hình 3.18 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 (Plaintext) được mã hóa bằng khóa K_1 , giải mã bằng khóa K_2 và mã hóa bằng khóa K_3 để cho ra bản mã (Ciphertext). Ở bên nhận, quá trình giải mã bắt đầu bằng việc giải mã bằng khóa K_3 , sau đó mã hóa bằng khóa K_2 và cuối cùng giải mã bằng khóa K_1 để khôi phục bản rõ. Ưu điểm của 3-DES là nâng cao được độ an toàn nhờ tăng kích thước khóa. 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 3.18. Mã hóa và giải mã với giải thuật 3-DES

3.3.1.4. 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 Mỹ (NIST) công nhận năm 2001. AES được xây dựng dựa trên Rijndael cipher 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 khối, với khối dữ liệu vào có kích thước là 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 bằng cả phần mềm và phần cứng. 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 chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã như sau:

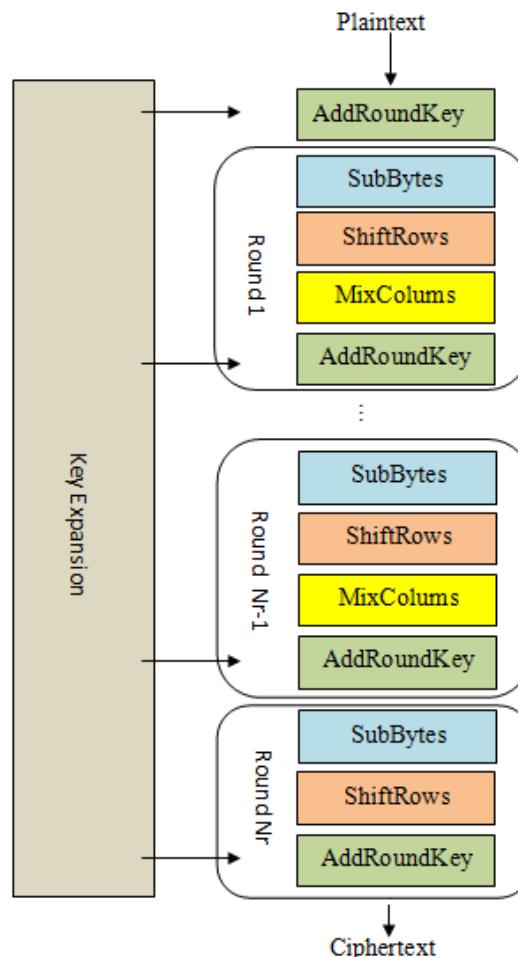
- 10 vòng lặp với khóa 128 bit;

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

b. Quá trình mã hóa

Giải thuật AES cho mã hóa dữ liệu, như minh họa trên Hình 3.19, gồm các bước xử lý chính như sau:

- Mở rộng khóa (Key Expansion): các khóa vòng (Round key) dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.

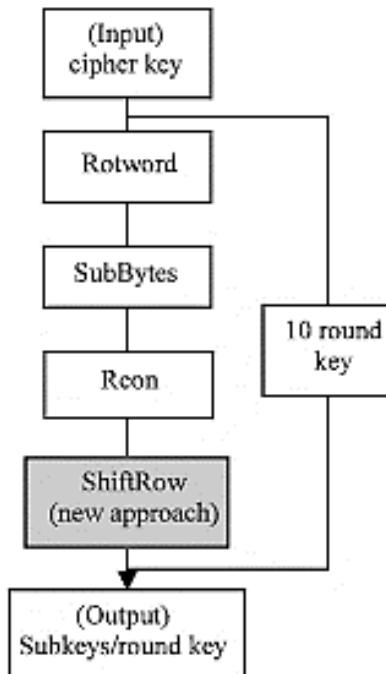


Hình 3.19. Các bước xử lý mã hóa dữ liệu của AES

- Vòng khởi tạo (Initial Round): Thực hiện hàm AddRoundKey, trong đó mỗi byte trong *state* được kết hợp với khóa vòng sử dụng phép XOR.
- Các vòng lặp chính (Rounds): Có 4 hàm biến đổi dữ liệu được thực hiện trong mỗi vòng, gồm:
 - + SubBytes: 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: hàm đổi chỗ, trong đó mỗi dòng trong *state* được dịch một số bước theo chu kỳ;
 - + MixColumns: trộn các cột trong *state*, kết hợp 4 bytes trong mỗi cột.
 - + AddRoundKey.

- Vòng cuối (Final Round): Tương tự các vòng lặp chính, nhưng chỉ thực hiện 3 hàm biến đổi dữ liệu, gồm:
 - + SubBytes;
 - + ShiftRows;
 - + AddRoundKey.

c. Mở rộng khóa



Hình 3.20. Thủ tục sinh khóa Rijndael

Khâu mở rộng khóa AES sử dụng thủ tục sinh khóa Rijndael để sinh các khóa vòng (Round key) cho các vòng lặp xử lý như biểu diễn trên Hình 3.20. Thủ tục Rijndael nhận đầu vào là khóa chính AES (cipher key) và xuất ra một khóa vòng (Subkey/Round key) sau mỗi vòng lặp. Một vòng lặp của thủ tục Rijndael gồm các khâu:

- Rotword: quay trái 8 bit từng từ 32 bit từ khóa gốc;
- SubBytes: thực hiện phép thay thế sử dụng bảng tham chiếu S-box.
- Rcon: tính toán giá trị $Rcon(i) = x^{i-1} \bmod x^8 + x^4 + x^3 + x + 1$
- ShiftRow: thực hiện đổi chỗ tương tự hàm ShiftRows của AES.

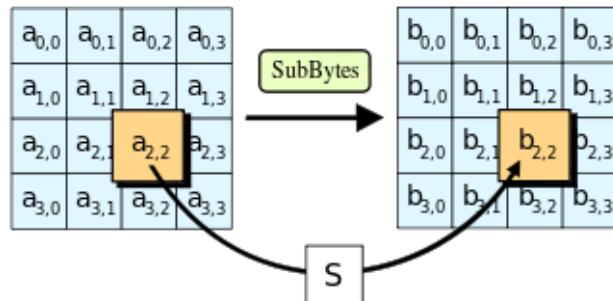
d. Các hàm xử lý chính

Hàm SubBytes: Mỗi byte trong ma trận *state* được thay thế bởi 1 byte trong Rijndael S-box, hay $b_{ij} = S(a_{ij})$ như minh họa trên Hình 3.21. S-box là một bảng tham chiếu phi tuyến tính, được tạo ra bằng phép nhân nghịch đảo một số cho trước trong trường $GF(2^8)$. Nếu như trong khâu mã hóa S-box được sử dụng thì bảng S-box *đảo* được sử dụng trong khâu giải mã.

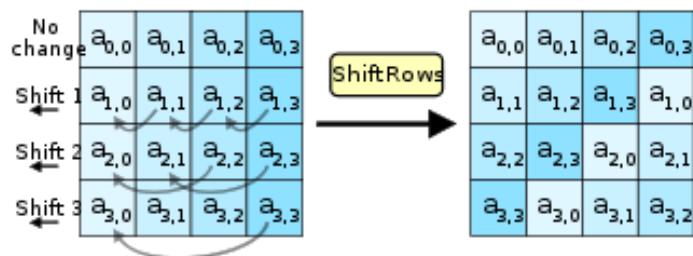
Hàm ShiftRows: Các dòng của ma trận *state* được dịch theo chu kỳ sang trái theo nguyên tắc: hàng số 0 giữ nguyên, hàng số 1 dịch 1 byte sang trái, hàng số 2 dịch 2 byte và hàng số 3 dịch 3 byte, như minh họa trên Hình 3.22.

Hàm MixColumns: Mỗi cột của ma trận *state* được nhân với một đa thức $c(x)$, như minh họa trên Hình 3.23. Đa thức $c(x) = 3x^3 + x^2 + x + 2$.

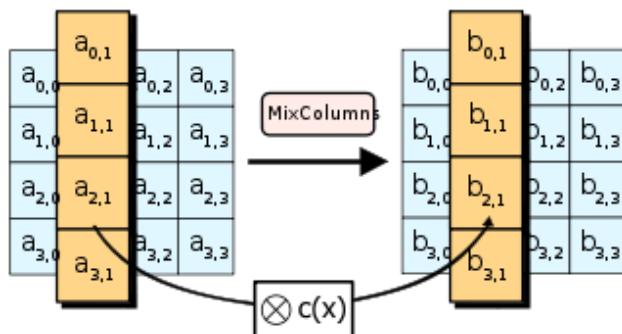
Hàm AddRoundKey: Mỗi byte của ma trận *state* được kết hợp với một byte tương ứng của khóa vòng sử dụng phép \oplus (XOR), như minh họa trên Hình 3.24.



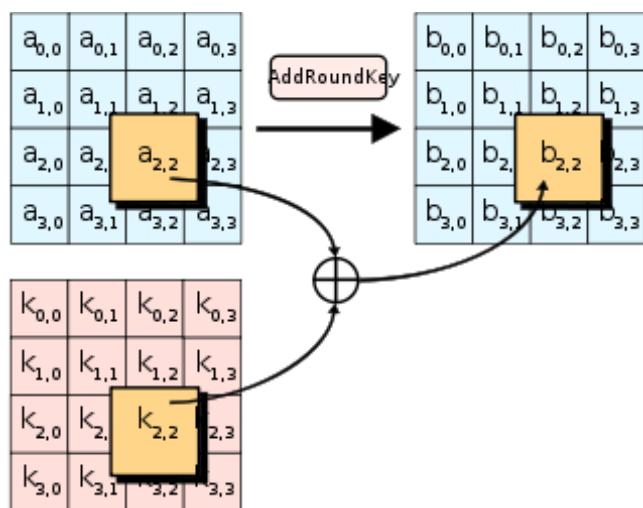
Hình 3.21. Hàm SubBytes sử dụng Rijndael S-box



Hình 3.22. Hàm ShiftRows

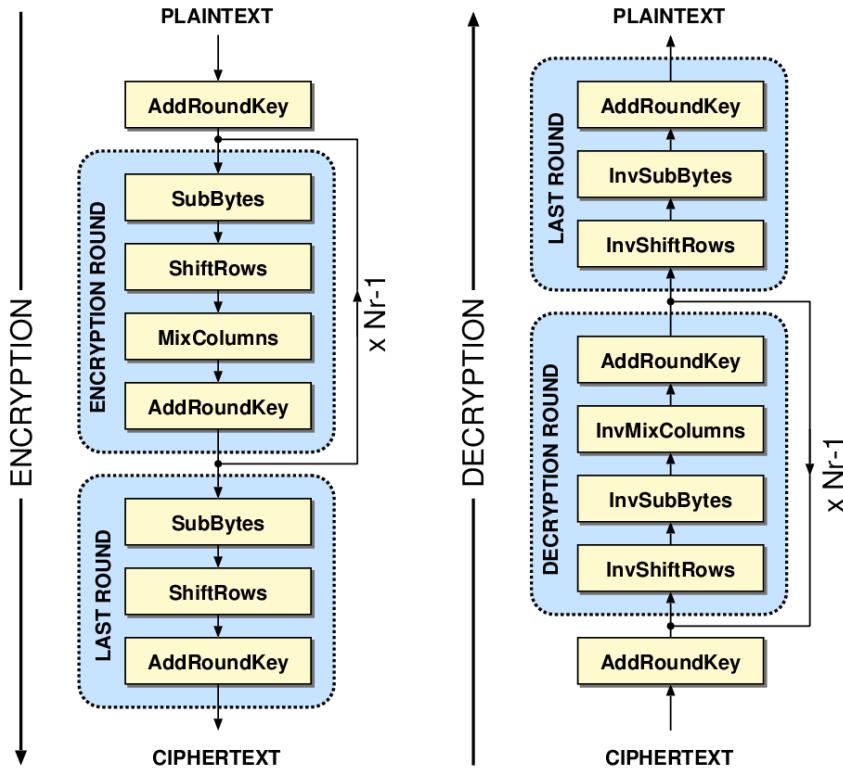


Hình 3.23. Hàm MixColumns



Hình 3.24. Hàm AddRoundKey

e. Quá trình giải mã



Hình 3.25. Quá trình mã hóa và giải mã trong AES

Khâu giải mã trong AES cũng gồm các bước xử lý tương tự như khâu mã hóa. Hình 3.25 biểu diễn quá trình mã hóa và giải mã trong AES. Theo đó, ngoài bước Mở rộng khóa, quá trình giải mã gồm Vòng khởi tạo (AddRoundKey), Các vòng lặp chính (Decryption round) và Vòng cuối (Last round) để chuyển khối mã thành khối rõ. Điểm khác biệt chính của khâu giải mã so với khâu mã hóa là các *hàm đảo* được sử dụng, như các hàm đảo InvSubBytes, InvShiftRows và InvMixColumns tương ứng thay cho các hàm SubBytes, ShiftRows và MixColumns.

3.3.2. Các giải thuật mã hóa khóa bất đối xứng

3.3.2.1. Khái quát

Mã hóa khóa bất đối xứng, đôi khi 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 mã hóa và khóa riêng được sử dụng cho 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 thể của khóa. Hình 3.3, mục 3.1 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.

Đặc điểm nổi bật của các hệ mã hóa khóa bất đối xứng là kích thước khóa lớn, 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 với 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 khóa công khai có thể phân phối rộng rãi.

Các giải thuật mã hóa khóa bất đối xứng điển hình bao gồm: RSA, Rabin, ElGamal, McEliece và Knapsack. Trong mục tiếp theo chúng ta tìm hiểu về giải thuật mã hóa RSA – một trong các giải thuật mã hóa khóa đối xứng được sử dụng rộng rãi nhất trên thực tế.

3.3.2.2. 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 lấy 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. Giải thuật 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. 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 2048 bit trong giai đoạn 2010-2020. Trong tương lai, cần sử dụng khóa RSA có kích thước lớn hơn, chẳng hạn 3072 bit.

b. Sinh khóa

RSA cung cấp một thủ tục sinh cặp khóa (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 e sao cho $1 < e < \Phi(n)$ 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 d sao cho $d \equiv e^{-1} \pmod{\Phi(n)}$,
hoặc $(d \times e) \pmod{\Phi(n)} = 1$
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 $c = m^e \pmod{n}$
- Giải mã
 - + Bản mã c , với $c < n$
 - + Bản rõ $m = c^d \pmod{n}$

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 $1 < e < 20$, và e và $\Phi(n)$ là số nguyên tố cùng nhau ($\Phi(n)$ không chia hết cho e). Chọn $e = 7$
- + Tính $(d \times e) \bmod \Phi(n) \rightarrow (d \times 7) \bmod 20 = 1$

$$d = (20 \times k + 1)/7 \rightarrow d = 3 \ (k=1)$$
- + Ta có: khóa công khai là $(33, 7)$ và khóa riêng là $(33, 3)$
- Mã hóa:
 - + Với bản rõ $m = 6$,
 - + $c = m^e \bmod n = 6^7 \bmod 33 = 279936 \bmod 33 = 30$
 - + Vậy bản mã $c = 30$
- Giải mã:
 - + Với bản mã $c = 30$
 - + $m = c^d \bmod n = 30^3 \bmod 33 = 27000 \bmod 33 = 6$
 - + Vậy bản rõ $m = 6$.

e. Một số yêu cầu với quá trình sinh khóa

Dưới đây liệt kê các yêu cầu đặt ra với các tham số sinh khóa và khóa để đảm bảo sự an toàn cho cặp khóa RSA. Các yêu cầu cụ thể gồm:

- 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. 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.
- 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.

3.3.3. Các hàm băm

Theo định nghĩa trong mục 3.1.1, 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.

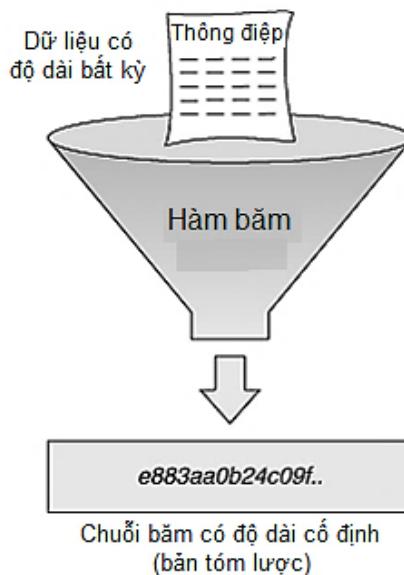
3.3.3.1. Khái quát về hàm băm

a. Giới thiệu

Hàm băm (hash function) là một hàm toán học h có tối thiểu 2 thuộc tính:

- Nén (Compression): 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 (Ease of computation): cho trước hàm h và đầu vào x , việc tính toán $h(x)$ là dễ dàng.

Hình 3.26 minh họa mô hình nén thông tin của hàm băm, theo đó thông điệp (Message) đầu vào với chiều dài tùy ý đi qua nhiều vòng xử lý của hàm băm để tạo chuỗi rút gọn, hay chuỗi đại diện (Digest) có kích thước cố định ở đầu ra.

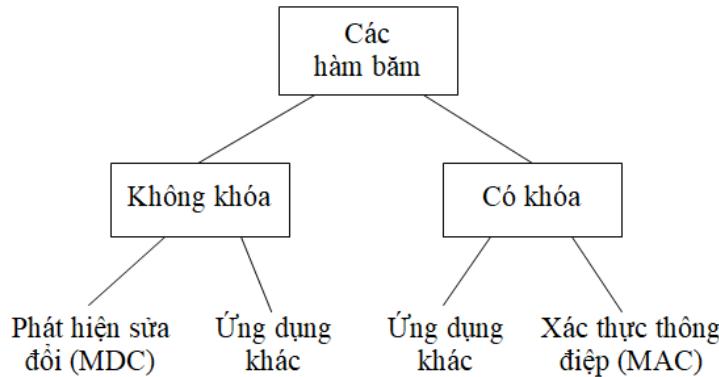


Hình 3.26. Mô hình nén thông tin của hàm băm

b. 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 và hàm băm có khóa, như biểu diễn trên Hình 3.27. Trong khi hàm băm không khóa nhận đầu vào chỉ là thông điệp (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 K là khóa bí mật). Trong 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 khác. Tương tự, trong 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 khác.



Hình 3.27. Phân loại các hàm băm theo khóa sử dụng

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

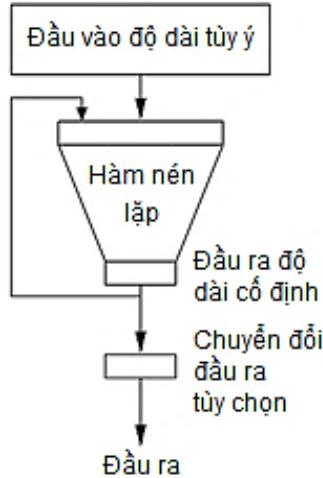
- Mã phát hiện sửa đổi (MDC - Modification Detection Code): MDC thường được sử dụng để tạo chuỗi đại diện cho thông điệp và dùng kết hợp với các kỹ thuật khác (như chữ ký số) để đảm bảo tính toàn vẹn của thông điệp. MDC thuộc loại hàm băm không khóa. MDC gồm 2 loại nhỏ:
 - + Hàm băm một chiều (OWHF - One-way hash functions): Với hàm băm một chiều, việc tính giá trị băm là dễ dàng, nhưng việc khôi phục thông điệp từ giá trị băm là rất khó khăn;
 - + Hàm băm chống đụng độ (CRHF - Collision resistant hash functions): Với hàm băm chống đụng độ, sẽ là rất khó để tìm được 2 thông điệp khác nhau nhưng có cùng giá trị băm.
- Mã xác thực thông điệp (MAC - Message Authentication Code): 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 như đã đề cập ở trên, với đầu vào là thông điệp và một khóa bí mật.

c. Mô hình xử lý dữ liệu

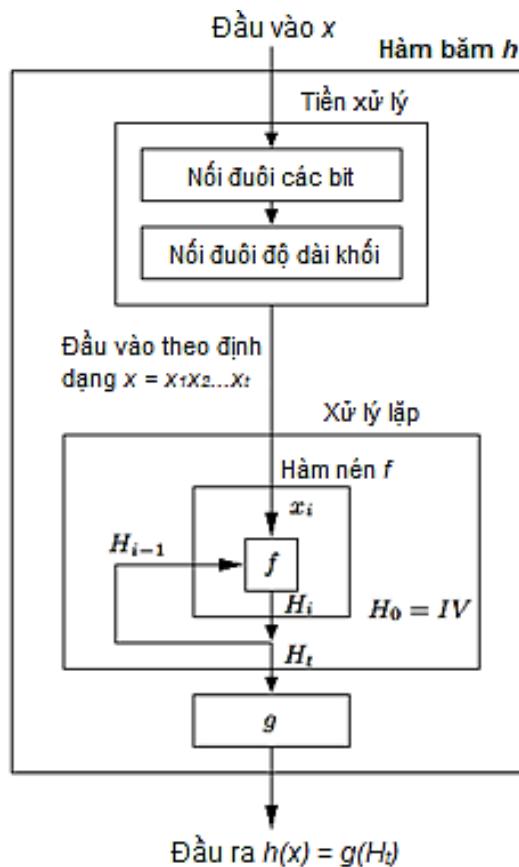
Hình 3.28 biểu diễn mô hình tổng quát xử lý dữ liệu của các hàm băm. Theo đó, thông điệp đầu vào với độ dài tùy ý đi qua hàm nén lặp nhiều vòng để tạo chuỗi đầu ra có kích thước cố định. Chuỗi này đi qua một khâu chuyển đổi định dạng tùy chọn để tạo ra chuỗi băm kết quả.

Hình 3.29 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. Trong bước tiền xử lý, thông điệp đầu vào x trước hết được nối đuôi thêm một số bit và kích

thước khói, sau đó chia thành các khói có kích thước xác định. Kết quả của bước này là t khói dữ liệu có cùng kích thước có dạng $x = x_1x_2\dots x_t$ làm đầu vào cho bước 2. Trong bước 2, từng khói dữ liệu x_i được xử lý thông qua hàm nén f để tạo đầu ra là H_i . Kết quả của bước 2 là chuỗi đầu ra H_t và H_t được chuyển đổi định dạng bởi hàm g để tạo chuỗi giá trị băm hết quả $h(x)$.



Hình 3.28. Mô hình tổng quát xử lý dữ liệu của hàm băm



Hình 3.29. Mô hình chi tiết xử lý dữ liệu của hàm băm

3.3.3.2. Một số hàm băm thông dụng

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

- Họ hàm băm MD (Message Digest) gồm các hàm băm MD2, MD4, MD5 và MD6.
- Họ hàm băm SHA (Secure Hash Algorithm) gồm các hàm băm SHA0, SHA1, SHA2 và SHA3.
- Một số hàm băm khác, gồm CRC (Cyclic redundancy checks), Checksums,...

Các mục con tiếp theo của mục này giới thiệu 2 hàm băm đã và đang được sử dụng rộng rãi nhất là hàm băm MD5 và SHA1.

a. Hàm băm MD5

* Giới thiệu

MD5 (Message Digest) là hàm băm không khóa được Ronald Rivest thiết kế năm 1991 để thay thế MD4. Chuỗi giá trị băm đầu ra của MD5 là 128 bit (16 byte) 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, tạo chuỗi kiểm tra lỗi, hoặc kiểm tra tính toàn vẹn dữ liệu (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 nó không còn đủ an toàn. Nhiều điểm yếu của MD5 đã bị khai thác, như điển hình MD5 bị khai thác bởi mã độc Flame vào năm 2012.

* 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*. Cụ thể, chi tiết về các khâu này như sau:

- **Tiền xử lý:** Thông điệp được chia thành các khối 512 bit (16 từ 32 bit). Nếu kích thước thông điệp không là bội số của 512 thì nối thêm số bit còn thiếu.
- **Các vòng lặp xử lý:** Phần xử lý chính của MD5 làm việc trên *state* 128 bit, chia thành 4 từ 32 bit (A, B, C, D):
 - + 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 (4 dạng hàm khác nhau cho mỗi vòng), Cộng modulo và Quay trái. Hình 3.30 biểu diễn lưu đồ xử lý của một thao tác của 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, $\ll\ll s$ là thao tác dịch trái s bit, \boxplus biểu diễn phép cộng modulo 32 bit và F là hàm phi tuyến tính.

Hàm F gồm 4 dạng được dùng cho 4 vòng lặp. Cụ thể, F có các dạng như sau:

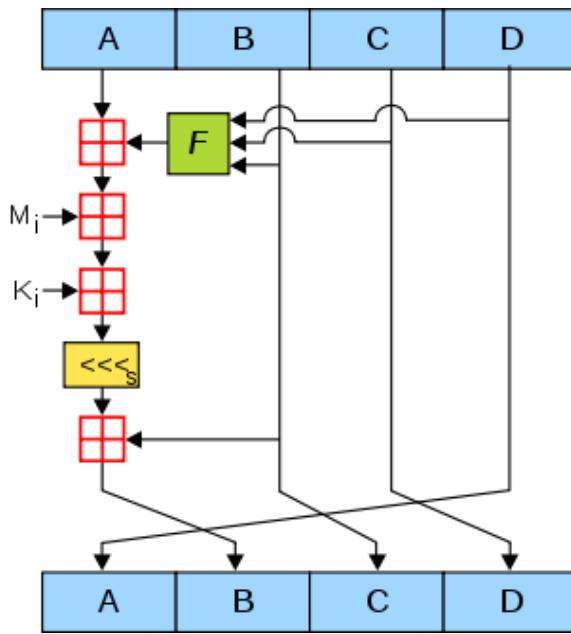
$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$

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

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

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

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



Hình 3.30. Lưu đồ xử lý một thao tác của MD5

b. Hàm băm SHA1

* Giới thiệu

SHA1 (Secure Hash Function) được Cơ quan mật vụ Mỹ 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.

* Quá trình xử lý thông điệp

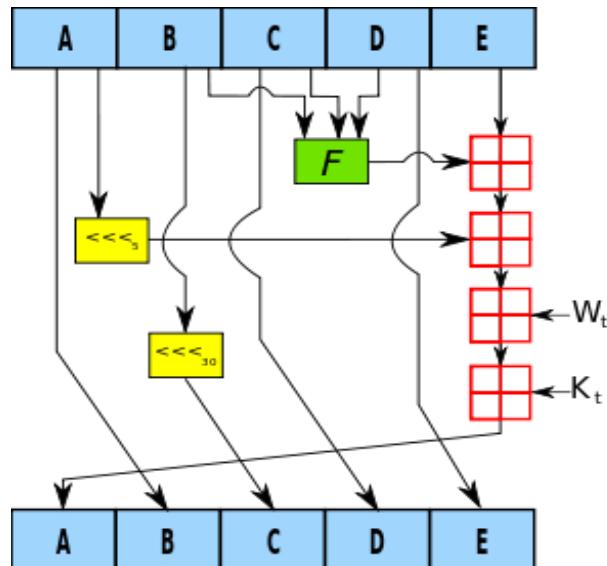
SHA1 sử dụng thủ tục xử lý thông điệp tương tự MD5, cũng gồm 2 khâu là *tiền xử lý* và *các vòng lặp xử lý*. Cụ thể, chi tiết về các khâu này như sau:

- **Tiền xử lý:** Thông điệp được chia thành các khối 512 bit (16 từ 32 bit). Nếu kích thước thông điệp không là bội số của 512 thì nối thêm số bit còn thiếu.
- **Các vòng lặp xử lý:** Phần xử lý chính của SHA1 làm việc trên *state* 160 bit, chia thành 5 từ 32 bit (A, B, C, D, E):
 - + 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 (có nhiều dạng hàm khác nhau), Cộng modulo và Quay trái. Hình 3.31 biểu 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, \boxplus biểu diễn phép cộng modulo 32 bit và F là hàm phi tuyến tính.

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 gíc XOR, AND, OR và NOT.



Hình 3.31. Lưu đồ một vòng xử lý của SHA1

3.4. Chữ ký số, chứng chỉ số và PKI

3.4.1. Chữ ký số

3.4.1.1. Một số khái niệm

Chữ ký số (Digital signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp. Chữ ký số thường được sử dụng để đảm bảo tính toàn vẹn của thông điệp.

Giải thuật tạo chữ ký số (Digital signature generation algorithm) là một phương pháp sinh chữ ký số;

Giải thuật kiểm tra chữ ký số (Digital signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định;

Một hệ chữ ký số (Digital signature scheme) bao gồm giải thuật tạo chữ ký số và giải thuật kiểm tra chữ ký số.

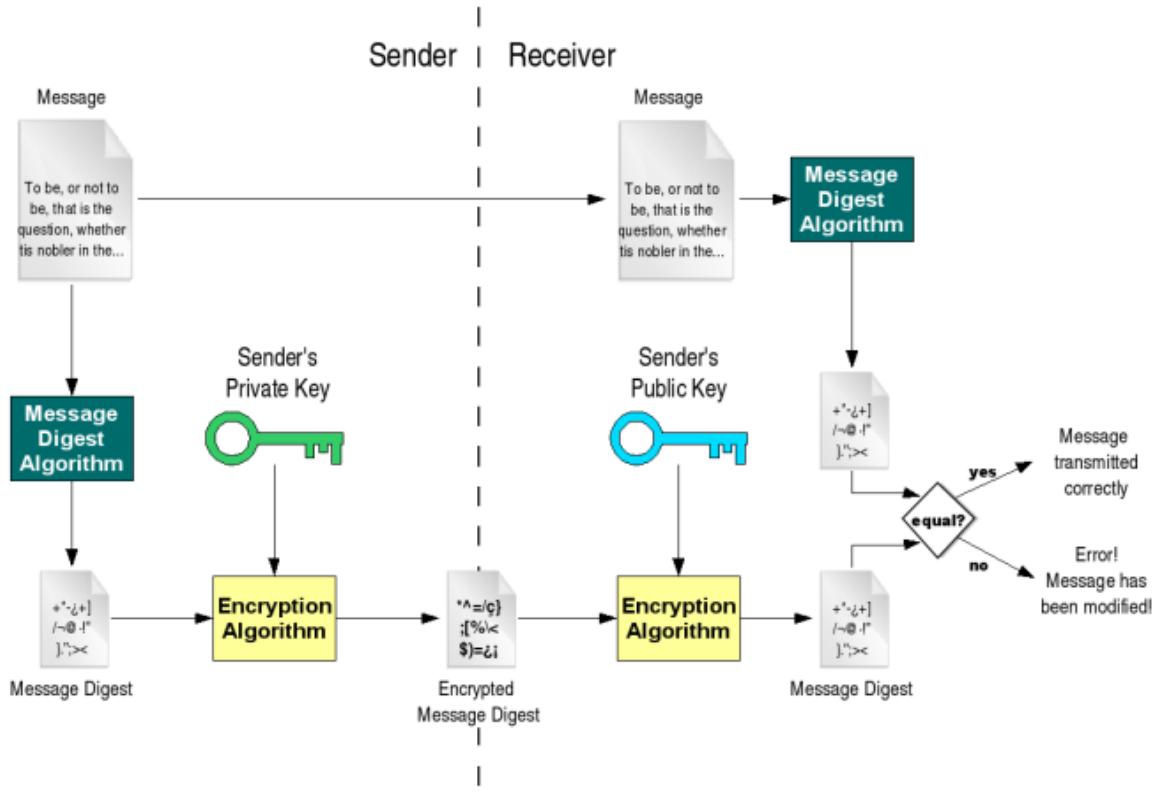
Quá trình tạo chữ ký số (Digital signature signing process) bao gồm:

- Giải thuật tạo chữ ký số, và
- Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.

Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm:

- Giải thuật kiểm tra chữ ký số, và
- Phương pháp khôi phục dữ liệu từ thông điệp.

3.4.1.2. Quá trình ký và kiểm tra



Hình 3.32. Quá trình tạo chữ ký số và kiểm tra chữ ký số

Hình 3.32 biểu diễn quá trình tạo chữ ký số và kiểm tra chữ ký số cho một thông điệp (Message). Trong khi quá trình tạo chữ ký số cho thông điệp được thực hiện ở bên người gửi (Sender) thì quá trình kiểm tra chữ ký số của thông điệp được thực hiện ở bên người nhận (Receiver). Để có thể tạo và kiểm tra chữ ký số cho thông điệp, người gửi phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Khóa riêng dùng để tạo chữ ký số và khóa công khai dùng để kiểm tra chữ ký số.

Các bước của quá trình tạo chữ ký số cho thông điệp (bên người gửi - Sender):

- Tính toán chuỗi đại diện (message digest/hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm);
- Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và một giải thuật tạo chữ ký (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted message digest);
- Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message);
- Thông điệp đã được ký (Signed message) được gửi cho người nhận.

Các bước của quá trình kiểm tra chữ ký số của thông điệp (bên người nhận - Receiver):

- Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;

- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký);
- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số để khôi phục chuỗi đại diện thông điệp MD2. Trên thực tế, người gửi thường chuyển chứng chỉ số khóa công khai của mình cho người nhận và người nhận thực hiện việc kiểm tra chứng chỉ số của người gửi và tách lấy khóa công khai nếu việc kiểm tra thành công.
- So sánh hai chuỗi đại diện MD1 và MD2:
 - + Nếu $MD1 = MD2$: chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
 - + Nếu $MD1 \neq MD2$: chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

3.4.1.3. Các giải thuật chữ ký số

Mục này trình bày 2 giải thuật chữ ký số thông dụng là RSA và DSA. RSA được sử dụng rộng rãi do RSA có thể được sử dụng để mã hóa thông điệp và tạo chữ ký số cho thông điệp. DSA là thuật toán chữ ký chuẩn được Viện NIST (Hoa Kỳ) phát triển.

a. Giải thuật chữ ký số RSA

Giải thuật RSA đề cập ở mục 3.3.2.2 có thể được sử dụng với hai mục đích để mã hóa - giải mã thông điệp và tạo chữ ký số - kiểm tra chữ ký số cho thông điệp. Điểm khác biệt giữa việc sử dụng RSA cho mã hóa và chữ ký số là bên sở hữu các cặp khóa và việc sử dụng các khóa trong quá trình mã hóa và giải mã. Cụ thể:

- RSA sử dụng cho mã hóa thông điệp:
 - + Người nhận phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Người nhận chuyển khóa công khai của mình cho người gửi;
 - + Người gửi mã hóa thông điệp sử dụng khóa công khai của người nhận và chuyển bản mã cho người nhận;
 - + Người nhận giải mã thông điệp sử dụng khóa riêng của mình để khôi phục bản rõ của thông điệp.
- RSA sử dụng cho tạo chữ ký số thông điệp:
 - + Người gửi phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Người gửi chuyển khóa công khai của mình cho người nhận;
 - + Người gửi sử dụng khóa riêng để tạo chữ ký số cho thông điệp (bản chất là sử dụng khóa riêng để mã hóa chuỗi đại diện cho thông điệp);
 - + Người nhận sử dụng khóa công khai của người gửi để kiểm tra chữ ký số của thông điệp (bản chất là sử dụng khóa công khai để giải mã khôi phục chuỗi đại diện cho thông điệp).

Quá trình ký và kiểm tra chữ ký số sử dụng giải thuật RSA tương tự như quá trình ký và kiểm tra chữ ký số tổng quát đã trình bày ở mục 3.4.1.2 và Hình 3.32, trong đó quá

trình ký sử dụng giải thuật mã hóa RSA với khóa riêng của người gửi và quá trình kiểm tra sử dụng giải thuật giải mã RSA với khóa công khai của người gửi.

b. Giải thuật chữ ký số DSA

DSA (Digital Signature Algorithm) là thuật toán chữ ký số được phát triển từ giải thuật ElGamal Signature Algorithm và được công nhận là chuẩn chữ ký số sử dụng trong các cơ quan chính phủ bởi Viện NIST (Hoa Kỳ) vào năm 1991. DSA gồm 3 gòm 3 khâu: (1) sinh cặp khóa, (2) quá trình ký thông điệp và (3) quá trình kiểm tra chữ ký của thông điệp.

* Sinh khóa cho một người dùng:

- Chọn số ngẫu nhiên x sao cho $0 < x < q$;
- Tính $y = g^x \text{ mod } p$;
- Khóa công khai là (q, p, g, y) ;
- Khóa riêng là x .

* Quá trình ký thông điệp:

- H là hàm băm sử dụng và m là thông điệp gốc;
- Tính $H(m)$ từ thông điệp gốc;
- Tạo số ngẫu nhiên k cho mỗi thông điệp, $0 < k < q$;
- Tính $r = (g^k \text{ mod } p) \text{ mod } q$;
- Nếu $r = 0$, chọn một k mới và tính lại r ;
- Tính $s = k^{-1}(H(m) + xr) \text{ mod } q$;
- Nếu $s = 0$, chọn một k mới và tính lại r và s ;
- Chữ ký là cặp (r, s) .

* Quá trình kiểm tra chữ ký

- Loại bỏ chữ ký nếu r và s không thỏa mãn $0 < r, s < q$;
- Tính $H(m)$ từ thông điệp nhận được;
- Tính $w = s^{-1} \text{ mod } q$;
- Tính $u1 = H(m) * w \text{ mod } q$;
- Tính $u2 = r * w \text{ mod } q$;
- Tính $v = ((g^{u1} * y^{u2}) \text{ mod } p) \text{ mod } q$;
- Chữ ký là xác thực nếu $v = r$.

Theo một số nghiên cứu, giải thuật chữ ký số DSA và giải thuật chữ ký số RSA có độ an toàn tương đương. Ưu điểm của giải thuật chữ ký số DSA so với giải thuật chữ ký số RSA là quá trình sinh cặp khóa và quá trình ký nhanh hơn. Tuy nhiên, quá trình kiểm tra chữ ký số bởi DSA thực hiện chậm hơn RSA. Trên thực tế, giải thuật chữ ký số RSA được sử dụng rộng rãi hơn do RSA có thể sử dụng cho cả mục đích mã hóa/giải mã và ký/kiểm tra chữ ký, trong khi DSA chỉ có thể sử dụng để ký/kiểm tra chữ ký.

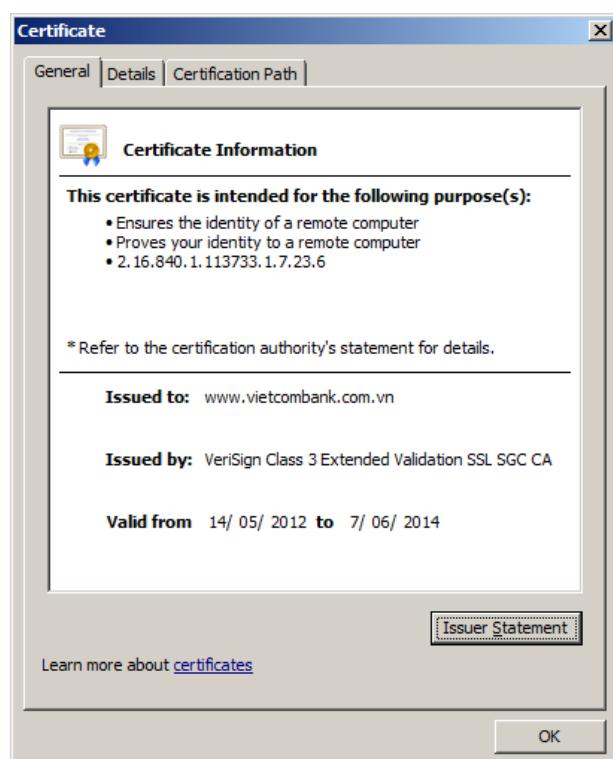
3.4.2. Chứng chỉ số

3.4.2.1. Giới thiệu

Chứng chỉ số (Digital certificate), còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một chữ ký số để liên kết một khóa công khai và thông tin nhận dạng của một thực thể. Ba thành phần cơ bản nhất của một chứng chỉ số gồm:

- Chữ ký số: là chữ ký của một bên thứ 3 tin cậy cung cấp chứng chỉ số, thường gọi là CA – Certificate Authority;
- Khóa công khai: là khóa công khai trong cặp khóa công khai và khóa riêng của thực thể;
- Thông tin nhận dạng: là tên, địa chỉ, tên miền hoặc các thông tin định danh của thực thể.

Chứng chỉ số có thể được sử dụng để xác minh chủ thể thực sự của một khóa công khai. Hình 3.33 là giao diện kiểm tra thông tin một chứng chỉ số do bên thứ 3 là một đơn vị của công ty Verisign cấp cho tên miền www.vietcombank.com.vn của ngân hàng TMCP Ngoại thương Việt Nam.



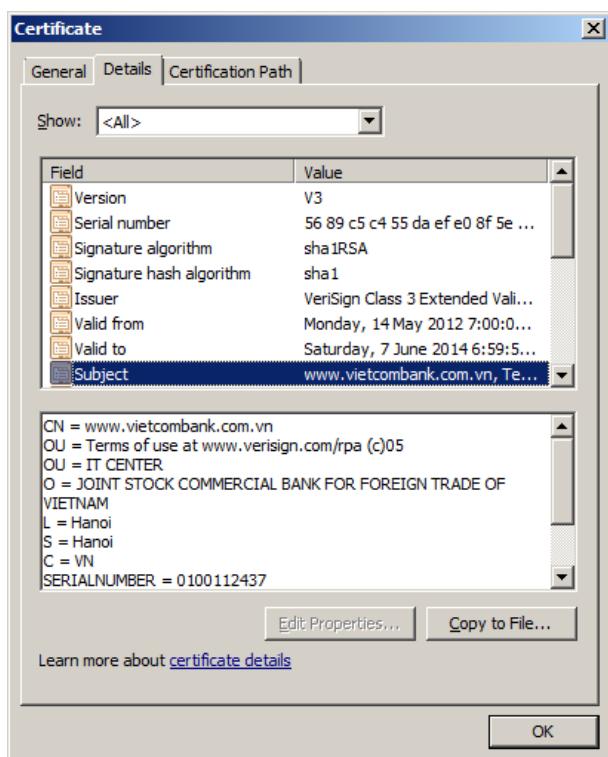
Hình 3.33. Giao diện kiểm tra thông tin một chứng chỉ số

3.4.2.2. Nội dung chứng chỉ số

Như biểu diễn trên Hình 3.34, nội dung của một chứng chỉ số gồm nhiều trường thông tin. Các trường thông tin cụ thể theo chuẩn chứng chỉ số X.509 gồm:

- Serial Number: Số nhận dạng của chứng chỉ số;
- Subject: Thông tin nhận dạng một cá nhân hoặc một tổ chức;
- Signature Algorithm: Giải thuật tạo chữ ký;

- Signature Hash Algorithm: Giải thuật tạo chuỗi băm cho tạo chữ ký;
 - Signature: Chữ ký của người/tổ chức cấp chứng chỉ;
 - Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;
 - Valid-From: Ngày bắt đầu có hiệu lực của chứng chỉ;
 - Valid-To: Ngày hết hạn sử dụng chứng chỉ;
 - Key-Usage: Mục đích sử dụng khóa (chữ ký số, mã hóa,...);
 - Public Key: Khóa công khai của chủ thẻ;
 - Thumbprint Algorithm: Giải thuật băm sử dụng để tạo chuỗi băm cho khóa công khai;
 - Thumbprint: Chuỗi băm tạo từ khóa công khai;
- Các mục thông tin của trường Subject gồm:
- CN (Common Name): Tên chung, nhưng một tên miền được gán chứng chỉ;
 - OU (Organisation Unit): Tên bộ phận/phòng ban;
 - O (Organisation): Tổ chức/Cơ quan/công ty;
 - L (Location): Địa điểm/Quận huyện;
 - S (State/Province): Bang/Tỉnh/Thành phố;
 - C (Country): Đất nước.



Hình 3.34. Nội dung chi tiết của một chứng chỉ số

3.4.2.3. Ứng dụng của chứng chỉ số

Chứng chỉ số được sử dụng rộng rãi trong bảo mật thông tin truyền và xác thực thông tin nhận dạng của các bên tham gia giao dịch điện tử, trao đổi khóa trong nhiều ứng dụng khác nhau. Cụ thể:

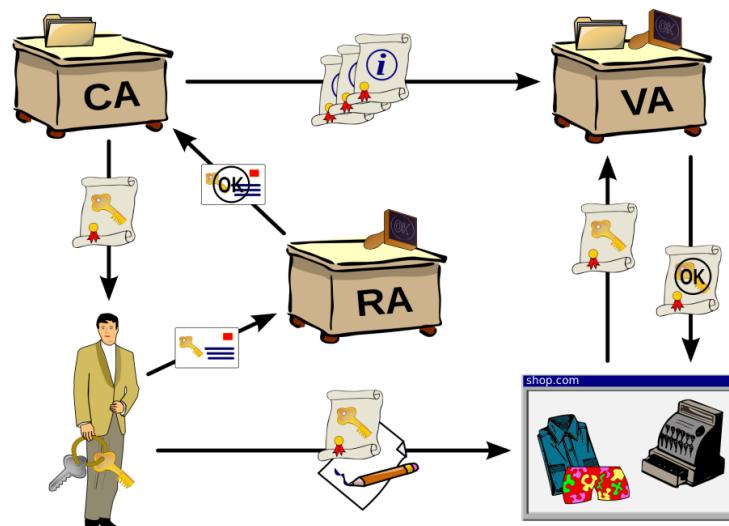
- Sử dụng chứng chỉ số trong đảm bảo an toàn giao dịch trên nền web: với chứng chỉ số, một website có thể được cấu hình để hoạt động theo chế độ “an toàn” (HTTPS), trong đó toàn bộ thông tin trao đổi giữa máy chủ và máy khách được đảm bảo tính bí mật (sử dụng mã hóa khóa đối xứng), tính toàn vẹn và xác thực (sử dụng hàm băm có khóa MAC). Ngoài ra, các máy chủ và máy khách có thể xác thực thông tin nhận dạng của nhau sử dụng chứng chỉ số.
- Chứng chỉ số cũng có thể được sử dụng để bảo mật thông tin truyền trong nhiều ứng dụng khác, như email, truyền file,...
- Sử dụng chứng chỉ số có thể ngăn chặn hiệu quả dạng tấn công người đứng giữa do các bên tham gia giao dịch có thể xác thực thông tin nhận dạng của nhau. Nếu các bên sử dụng thêm chữ ký số thì có thể ngăn chặn việc sửa đổi các thông điệp trao đổi trên đường truyền.
- Chứng chỉ số có thể được sử dụng trong trao đổi khóa.

3.4.3. PKI

Hệ tầng khóa công khai (Public-key infrastructure - PKI) là một tập các phần cứng, phần mềm, nhân lực, chính sách và các thủ tục để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số. Một PKI gồm các thành phần sau:

- Certificate Authority (CA): Cơ quan cấp và kiểm tra chứng chỉ số;
- Registration Authority (RA): Bộ phận tiếp nhận, kiểm tra thông tin nhận dạng của người dùng theo yêu cầu của CA;
- Validation Authority (VA): Cơ quan xác nhận thông tin nhận dạng của người dùng thay mặt CA;
- Central Directory (CD): Là nơi lưu danh mục và lập chỉ số các khóa;
- Certificate Management System: Hệ thống quản lý chứng chỉ;
- Certificate Policy: Chính sách về chứng chỉ.

Hình 3.35 biếu diễn lưu đồ cấp và sử dụng chứng chỉ số trong PKI gồm 2 khâu chính:



Hình 3.35. Lưu đồ cấp và sử dụng chứng chỉ số trong PKI

- Đăng ký, xét duyệt và cấp chứng chỉ số:
 - + Người dùng có yêu cầu cấp chứng chỉ số tạo một cặp khóa, gồm 1 khóa công khai và 1 khóa riêng;
 - + Người dùng tạo yêu cầu cấp chứng chỉ số (Certificate request), trong đó tích hợp khóa công khai và thông tin định danh của mình. Yêu cầu cấp chứng chỉ số thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;
 - + Người dùng gửi yêu cầu cấp chứng chỉ số đến Bộ phận tiếp nhận (RA). RA kiểm tra các thông tin trong yêu cầu cấp chứng chỉ số, nếu hợp lệ thì chuyển yêu cầu đến Cơ quan cấp chứng chỉ (CA);
 - + CA sẽ thực hiện việc xác minh các thông tin nhận dạng của chủ thẻ và nếu xác minh thành công thì cấp chứng chỉ số cho người yêu cầu. Chứng chỉ số được CA ký bằng khóa riêng của mình để đảm bảo tính xác thực và toàn vẹn và thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;
 - + Sau khi phát hành chứng chỉ số cho người dùng, CA chuyển thông tin về chứng chỉ số đã cấp cho thành phần VA để xác nhận thông tin nhận dạng theo yêu cầu;
 - + Người dùng cài đặt chứng chỉ số vào hệ thống và có thể bắt đầu sử dụng trong các ứng dụng của mình.
- Sử dụng và kiểm tra chứng chỉ số:
 - + Người dùng tạo đơn hàng, ký vào đơn hàng bằng khóa riêng, gửi đơn hàng đã ký và chứng chỉ số cho nhà cung cấp;
 - + Nhà cung cấp chuyển chứng chỉ số của người dùng cho VA để kiểm tra, nếu chứng chỉ số hợp lệ thì tiến hành xác thực chữ ký số của người dùng sử dụng khóa công khai của người dùng lấy từ chứng chỉ số. Nếu chữ ký của người dùng xác thực thành công thì đơn hàng được duyệt.

3.5. Quản lý khóa và phân phối khóa

3.5.1. Giới thiệu

3.5.1.1. Một số khái niệm

Quan hệ khóa (Keying relationship) là trạng thái mà trong đó các bên tham gia truyền thông chia sẻ dữ liệu chia sẻ (thường là khóa hoặc thành phần tạo ra khóa) để sử dụng cho các kỹ thuật mã hóa. Các dữ liệu chia sẻ có thể gồm:

- Khóa bí mật
- Khóa công khai
- Các giá trị khởi tạo
- Các tham số bổ sung không bí mật.

Quản lý khóa (Key management) là một tập các kỹ thuật cho phép thiết lập và duy trì các quan hệ khóa giữ các bên có thẩm quyền. Cụ thể, quản lý khóa gồm các kỹ thuật và thủ tục cho phép:

- Khởi tạo các người dùng hệ thống (system users) trong một vùng (domain);

- Sinh khóa, phân phối và cài đặt các dữ liệu khóa;
- Kiểm soát việc sử dụng các dữ liệu khóa;
- Cập nhật, thu hồi và hủy các dữ liệu khóa;
- Lưu, sao lưu/khôi phục và lưu trữ các dữ liệu khóa.

Phân phối khóa (Key distribution) là một thành phần của quản lý khóa, trong đó các khóa mật mã được vận chuyển, hoặc trao đổi giữa các thực thể trong một hệ thống, hay giữa các bên tham gia phiên truyền thông.

3.5.1.2. Vai trò và các nguy cơ mất an toàn quản lý khóa

Quản lý khóa là một khâu có vai trò quan trọng trong việc đảm bảo tính bí mật, toàn vẹn, xác thực, không thể chối bỏ và dịch vụ chữ ký số của một hệ mã hóa. Khâu quản lý khóa được thực hiện phù hợp sẽ đảm bảo cho các thông tin khóa được an toàn, đặc biệt khi có nhiều thực thể tham gia truyền thông. Các thông tin khóa được đảm bảo an toàn là yếu tố tiên quyết cho việc đảm bảo tính an toàn của hệ mã hóa.

Đứng trên góc độ quản lý, vấn đề quản lý khóa phải luôn được thực hiện trong khuôn khổ chính sách an ninh cụ thể. Chính sách an ninh của cơ quan, tổ chức cần có các nội dung mô tả về quản lý khóa, bao gồm:

- Các thực tế và thủ tục cần thực hiện trong các khía cạnh kỹ thuật và quản trị khóa tự động hoặc thủ công;
- Trách nhiệm của các bên có liên quan;
- Các bản ghi dữ liệu cần lưu để tạo các báo cáo về các vấn đề có liên quan đến an toàn khóa.

Ngoài ra, việc phân tích, nhận dạng các nguy cơ đe dọa an toàn của khâu quản lý khóa là một việc cần thiết, từ đó có thể đề ra và áp dụng các biện pháp đảm bảo an toàn phù hợp. Các nguy cơ đối với quản lý khóa bao gồm:

- Các khóa bí mật bị lộ;
- Tính xác thực của các khóa bí mật và công khai bị thỏa hiệp. Tính xác thực bao gồm các hiểu biết và việc kiểm chứng thông tin nhận dạng của một bên mà khóa được chia sẻ;
- Sử dụng trái phép các khóa bí mật và công khai:
 - + Sử dụng các khóa đã hết hiệu lực;
 - + Sử dụng các khóa sai mục đích.

3.5.1.3. Phân loại khóa

Các khóa/chìa mật mã có thể được phân loại theo (1) khả năng sử dụng và (2) thời gian sử dụng. Theo khả năng sử dụng, có thể chia các khóa thành 3 lớp:

- Khóa chủ (Master key):
 - + Là các khóa ở mức cao nhất và không được bảo vệ bằng các kỹ thuật mật mã.
 - + Các khóa chủ thường được chuyển giao trực tiếp và được bảo vệ bằng các cơ chế kiểm soát vật lý.

- Khóa dùng cho trao đổi khóa (Key – encrypting key):
 - + Là những khóa được sử dụng để vận chuyển hoặc lưu trữ các khóa khác.
 - + Các khóa này cũng có thể được bảo vệ bằng khóa khác.
- Khóa dữ liệu (Data keys):
 - + Là các khóa được sử dụng để mã hóa dữ liệu cho người dùng.
 - + Thường là các khóa ngắn hạn.

Theo thời gian sử dụng, có thể chia các khóa thành 2 lớp:

- Khóa dài hạn (long-term key):
 - + Là các khóa được sử dụng trong một khoảng thời gian dài;
 - + Gồm khóa chủ, khóa dùng cho trao đổi khóa, hoặc khóa dùng cho thỏa thuận khóa.
- Khóa ngắn hạn:
 - + Là các khóa được sử dụng trong một khoảng thời gian ngắn hoặc chỉ trong một phiên làm việc;
 - + Gồm các khóa được trao đổi trong quá trình trao đổi khóa, thỏa thuận khóa;
 - + Thường được dùng để mã hóa dữ liệu của người dùng.

3.5.2. Phân phối khóa bí mật

3.5.2.1. Đặt vấn đề

Như đã đề cập trong mục 3.3.1, các hệ mã hóa khóa đối xứng, hay khóa bí mật có ưu điểm là độ an toàn cao và tốc độ xử lý nhanh do kích thước khóa tương đối nhỏ. Tuy nhiên, hạn chế lớn nhất của chúng là khó khăn trong quản lý và phân phối khóa bí mật – các khóa bí mật dùng chung phải được phân phối, chia sẻ an toàn đến các bên tham gia trước khi có thể thực hiện phiên truyền thông an toàn.

Vấn đề phân phối khóa bí mật được khái quát hóa thành bài toán phân phối n^2 khóa. Bài toán này phát biểu như sau: Nếu một hệ thống có n người dùng tham gia truyền thông sử dụng kỹ thuật mã hóa khóa đối xứng và mỗi cặp người dùng cần trao đổi thông tin an toàn, thì mỗi cặp người dùng cần chia sẻ một khóa bí mật duy nhất. Như vậy, mỗi người dùng cần sở hữu $n-1$ khóa bí mật và tổng số khóa cần quản lý trong hệ thống là $n(n-1)/2 \approx n^2$. Ví dụ, nếu hệ thống có 10 người dùng, tổng số khóa cần quản lý là $10 \times 9/2 = 45$ khóa; với 100 người dùng, số khóa là $100 \times 99/2 = 4.950$ khóa; và với 1000 người dùng, số khóa là $1000 \times 999/2 = 499.500$ khóa. Số khóa cần quản lý sẽ rất lớn nếu số người dùng lớn và việc quản lý số lượng lớn khóa đảm bảo an toàn là rất khó khăn.

Để giải quyết bài toán phân phối n^2 khóa và đảm bảo an toàn trong phân phối các khóa bí mật, một số mô hình và kỹ thuật phân phối khóa bí mật được đề xuất và ứng dụng, bao gồm:

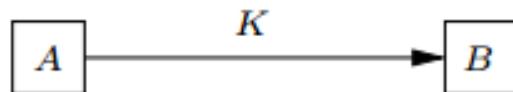
- Phân phối khóa điểm – điểm (Point-to-point key distribution)
- Trung tâm phân phối khóa (Key distribution center – KDC)
- Trung tâm dịch khóa (Key translation center – KTC)

- Sử dụng mã hóa khóa công khai để phân phối khóa bí mật.

Các mục tiếp theo mô tả chi tiết các mô hình và kỹ thuật phân phối khóa bí mật.

3.5.2.2. Phân phối khóa điểm – điểm

Phân phối khóa điểm – điểm (Point-to-point key distribution) là hình thức phân phối khóa chỉ liên quan trực tiếp đến 2 thực thể tham gia truyền thông, như minh họa trên Hình 3.36. Hình thức phân phối khóa điểm – điểm có thể thực hiện thông qua các kênh tin cậy, như kênh truyền thuê riêng, hoặc thư bảo đảm. Phương pháp này có thể sử dụng với các trao đổi không thường xuyên và thích hợp với các hệ thống cỡ nhỏ hoặc đóng kín. Nhược điểm của phương pháp này là trễ có thể lớn (như sử dụng thư bảo đảm) và các kênh tin cậy dùng riêng thường đắt tiền.

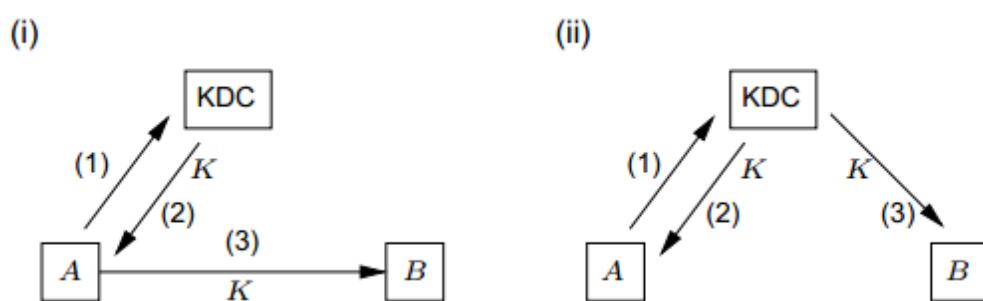


Hình 3.36. Phân phối khóa điểm – điểm

3.5.2.3. Trung tâm phân phối khóa

a. Giới thiệu

Trung tâm phân phối khóa (Key distribution center – KDC) là một trong các kỹ thuật được sử dụng rộng rãi để giải quyết bài toán n^2 khóa trong hệ thống có n người dùng. Mục tiêu là KDC tạo và phân phối khóa bí mật an toàn đến các thực thể trong hệ thống và giảm thiểu số lượng khóa dài hạn mà mỗi thực thể và KDC phải quản lý. Hình 3.37 biểu diễn mô hình hoạt động của hệ thống KDC gồm 3 thực thể: Trung tâm phân phối khóa KDC ký hiệu là T và 2 thực thể thành viên tham gia trao đổi khóa là A và B. Khóa bí mật cần trao đổi là K. Hoạt động của hệ thống KDC gồm 2 khâu: (1) Khởi tạo – thiết lập môi trường và các tham số hoạt động và (2) Thủ tục phân phối khóa sử dụng KDC.



Hình 3.37. Mô hình hoạt động của trung tâm phân phối khóa – KDC

b. Khởi tạo

Trong quá trình khởi tạo, thực thể A sở hữu khóa dài hạn K_{AT} và A chia sẻ K_{AT} với KDC T. Thực thể B sở hữu khóa dài hạn K_{BT} và B chia sẻ K_{BT} với KDC T. Trung tâm phân phối khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn K_{AT} và K_{BT} .

c. Thủ tục phân phối khóa

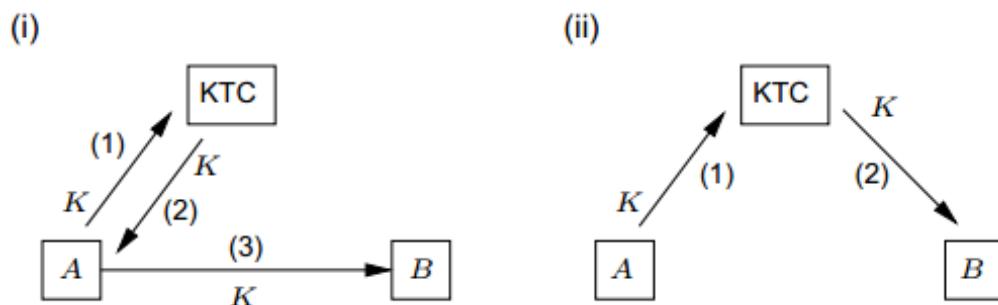
Theo mô hình hoạt động của trung tâm phân phối khóa biểu diễn trên Hình 3.37, gọi E là hàm mã hóa, D là hàm giải mã, thủ tục phân phối khóa sử dụng KDC T như sau:

- A yêu cầu chia sẻ khóa với B;
- T sẽ tạo ra hoặc lấy khóa có sẵn K và mã hóa K thành $E_{KAT}(K)$ và gửi cho A;
- T cũng có thể gửi khóa cho B dưới dạng $E_{KBT}(K)$ thông qua A (hình i);
- T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{KBT}(K)$ (hình ii);
- A nhận được $E_{KAT}(K)$, giải mã sử dụng K_{AT} để có được K: $D_{KAT}(E_{KAT}(K)) = K$
- B nhận được $E_{KBT}(K)$, giải mã sử dụng K_{BT} để có được K: $D_{KBT}(E_{KBT}(K)) = K$

3.5.2.4. Trung tâm dịch khóa

a. Giới thiệu

Trung tâm dịch chuyển khóa (Key translation center – KTC) là một trong các kỹ thuật được sử dụng rộng rãi để giải quyết bài toán n^2 khóa trong hệ thống có n người dùng. Vai trò của KTC tương tự KDC, tuy nhiên một bên tham gia truyền thông sẽ cung cấp khóa trao đổi. Mục tiêu là KTC chuyển khóa bí mật an toàn đến các thực thể còn lại tham gia truyền thông trong hệ thống và giảm thiểu số lượng khóa dài hạn mà mỗi thực thể và KTC phải quản lý. Điểm khác biệt của KTC so với KDC là KTC cho phép sinh khóa phân tán (các thực thể tự sinh khóa), còn KDC cho phép sinh khóa tập trung (KDC sinh khóa). Hình 3.38 biểu diễn mô hình hoạt động của hệ thống KTC gồm 3 thực thể: Trung tâm dịch chuyển khóa KTC ký hiệu là T và 2 thực thể thành viên tham gia trao đổi khóa là A và B. Khóa bí mật cần trao đổi là K. Hoạt động của hệ thống KTC gồm 2 khâu: (1) Khởi tạo – thiết lập môi trường và các tham số hoạt động và (2) Thủ tục phân phối khóa sử dụng KTC.



Hình 3.38. Mô hình hoạt động của trung tâm dịch chuyển khóa – KTC

b. Khởi tạo

Trong quá trình khởi tạo, thực thể A sở hữu khóa dài hạn K_{AT} và A chia sẻ K_{AT} với KTC T. Thực thể B sở hữu khóa dài hạn K_{BT} và B chia sẻ K_{BT} với KTC T. Trung tâm phân phối khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn K_{AT} và K_{BT} .

c. Thủ tục phân phối khóa

Theo mô hình hoạt động của trung tâm dịch chuyển khóa bí ẩn diễn trên Hình 3.38, gọi E là hàm mã hóa, D là hàm giải mã, thủ tục phân phối khóa sử dụng KTC T như sau:

- A tạo ra khóa K và mã hóa K thành $E_{KAT}(K)$ và gửi cho T;
- T nhận được $E_{KAT}(K)$, giải mã sử dụng K_{AT} thu được K: $D_{KAT}(E_{KAT}(K)) = K$
- Sau đó, T mã hóa khóa K sử dụng K_{BT} để có $E_{KBT}(K)$;
- T có thể gửi khóa cho B dưới dạng $E_{KBT}(K)$ thông qua A (hình i);
- T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{KBT}(K)$ (hình ii);
- B nhận được $E_{KBT}(K)$, giải mã sử dụng K_{BT} để có được K: $D_{KBT}(E_{KBT}(K)) = K$

d. Ưu điểm và nhược điểm của quản lý khóa tập trung (KDC và KTC)

- **Ưu điểm:**
 - + Hiệu quả trong lưu trữ khóa: mỗi bên chỉ cần duy trì một khóa bí mật dài hạn với bên tin cậy (không phải với bên trao đổi thông tin);
 - + Tổng số khóa dài hạn cần lưu trữ là n khóa (so với n^2 khóa).
- **Nhược điểm:**
 - + Cả hệ thống có thể bị mất an toàn nếu trung tâm quản lý khóa bị thỏa hiệp (bị điều khiển);
 - + Trung tâm quản lý khóa có thể thành điểm nút cỗ chai;
 - + Dịch vụ sẽ phải ngừng nếu trung tâm quản lý khóa gặp trục trặc;
 - + Cần có một máy chủ tin cậy ở chế độ trực tuyến.

3.5.2.5. Sử dụng mã hóa khóa công khai để phân phối khóa bí mật

Do các hệ mã hóa khóa công khai có ưu điểm là phân phối khóa công khai dễ dàng, có thể sử dụng mã hóa khóa công khai để phân phối khóa bí mật. Giả thiết bên A cần chuyển khóa bí mật K_s cho bên B. Các bước hai bên A và B cần thực hiện để chuyển khóa bí mật K_s từ A đến B sử dụng mã hóa khóa công khai như sau:

- B tạo cặp khóa, khóa công khai K_p và khóa riêng K_r ;
- B gửi khóa công khai K_p của mình cho A (cần đảm bảo tính xác thực và toàn vẹn);
- A sử dụng K_p để mã hóa khóa bí mật K_s tạo bản mã C_s và gửi cho B;
- B sử dụng khóa riêng K_r để giải mã C_s để khôi phục khóa bí mật K_s .

Trên thực tế, các giao thức SSL/TLS và PGP đều sử dụng mã hóa khóa công khai một cách hiệu quả để trao đổi khóa bí mật, hoặc dữ liệu khóa bí mật cho phiên làm việc. Chi tiết về các giao thức này được đề cập ở mục 3.6.

3.5.3. Phân phối khóa công khai

3.5.3.1. Giới thiệu

Khác với khóa bí mật, việc phân phối khóa công khai thuận lợi hơn do khóa công khai có thể trao đổi công khai giữa các thực thể tham gia truyền thông. Tuy nhiên, việc phân phối khóa công khai phải đảm bảo tính xác thực (authentic public keys). Tính xác thực

của khóa công khai thể hiện ở 2 yếu tố: (1) tính toàn vẹn và chủ thể luôn xác định. Các phương pháp phân phối khóa công khai được sử dụng rộng rãi bao gồm:

- Trao đổi kiểu điểm-điểm thông qua kênh tin cậy;
- Truy nhập trực tiếp vào danh mục công cộng (public-key registry);
- Sử dụng một máy chủ trực tuyến tin cậy;
- Sử dụng một máy chủ không trực tuyến và chứng chỉ.

Phương pháp trao đổi khóa công khai kiểu điểm-điểm thông qua kênh tin cậy được thực hiện tương tự như phương pháp trao đổi khóa bí mật kiểu điểm-điểm đã được trình bày ở mục 3.5.2.2. Các phương pháp phân phối khóa công khai còn lại được trình bày trong các mục tiếp theo.

3.5.3.2. Truy nhập trực tiếp vào danh mục công cộng (public-key registry)

Trong phương pháp này, một cơ sở dữ liệu công cộng tin cậy được thiết lập, trong đó mỗi bản ghi gồm tên người dùng và khóa công khai tương ứng. Cơ sở dữ liệu công cộng này có thể được vận hành bởi 1 bên tin cậy và người dùng có thể truy nhập khóa công khai từ cơ sở dữ liệu này nếu biết tên người dùng. Một phương pháp thực hiện được sử dụng phổ biến là cây xác thực khóa công khai (Tree authentication of public keys).

3.5.3.3. Sử dụng một máy chủ trực tuyến tin cậy

Trong phương pháp này, một máy chủ trực tuyến tin cậy được sử dụng để cung cấp truy nhập đến cơ sở dữ liệu công cộng các khóa công khai. Khóa công khai cần phân phối được ký sử dụng khóa riêng của máy chủ và gửi cho bên yêu cầu. Phương pháp này không đòi hỏi phải sử dụng kênh truyền bí mật. Bên yêu cầu sử dụng khóa công khai của máy chủ để xác thực chữ ký của máy chủ và qua đó kiểm tra tính xác thực, toàn vẹn của khóa. Phương pháp này có nhược điểm là máy chủ phải luôn trực tuyến để hệ thống có thể hoạt động và bản thân máy chủ có thể trở thành điểm nút cỗ chai trong hệ thống.

3.5.3.4. Sử dụng một máy chủ không trực tuyến và chứng chỉ

Đây là phương pháp phân phối khóa dựa trên chứng chỉ khóa công khai (Public key certificate) được sử dụng rất rộng rãi trong bảo mật thông tin truyền trên mạng Internet. Các bước thực hiện của phương pháp này gồm:

- Bên A liên hệ với một bên tin cậy (được gọi là Cơ quan cấp chứng chỉ - Certification Authority (CA)) để đăng ký khóa công khai của mình và nhận được chữ ký xác nhận khóa công khai của CA;
- CA cấp một chứng chỉ (Certificate) cho khóa công khai của A, trong đó kết hợp khóa công khai của A với thông tin định danh của A sử dụng chữ ký số của CA;
- Khi A đã có chứng chỉ khóa công khai (Public key certificate), A có thể gửi khóa công khai cho các bên có liên quan bằng cách gửi chứng chỉ khóa công khai.
- Chứng chỉ khóa công khai cũng có thể được đưa vào danh mục công cộng và người dùng khác có thể truy nhập.

Chi tiết về chứng chỉ khóa công khai và quá trình cấp phát – sử dụng chứng chỉ đã được đề cập ở các mục 3.4.2 và 3.4.3.

3.6. Một số giao thức đảm bảo ATTT dựa trên mã hóa

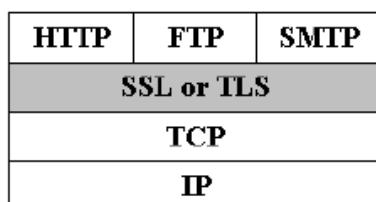
3.6.1. SSL/TLS

3.6.1.1. Giới thiệu

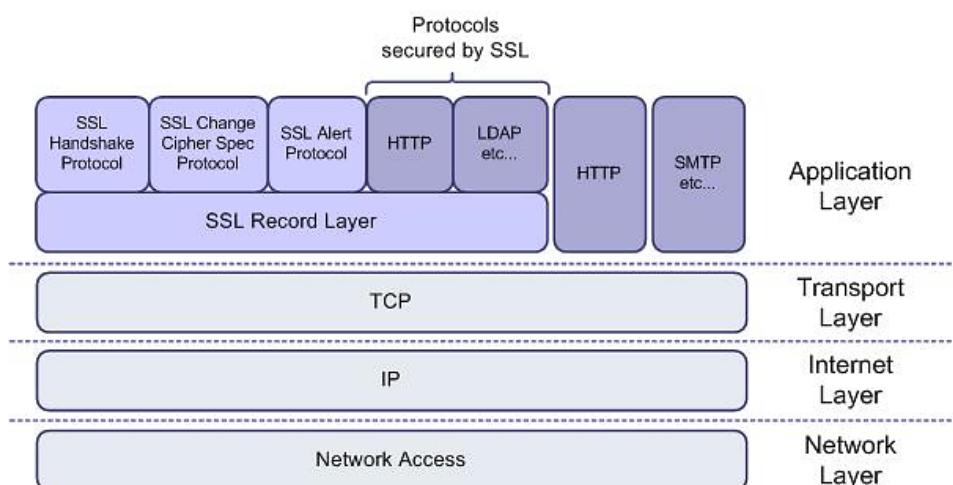
SSL (Secure Socket Layer) là giao thức bảo mật do công ty Netscape phát minh năm 1993. Các phiên bản SSL được phát triển bao gồm: phiên bản 1.0 phát hành năm 1993, phiên bản 2.0 phát hành năm 1995 và phiên bản 3.0 phát hành năm 1996. Sau phiên bản 3.0, SSL chính thức dừng phát triển. SSL hiện ít được sử dụng do có nhiều lỗi và không được cập nhật.

TLS (Transport Layer Security) được phát triển vào năm 1999 dựa trên SSL 3.0 do tổ chức IETF phê chuẩn. Các phiên bản của TLS gồm: phiên bản 1.0 phát hành năm 1999, phiên bản 1.1 phát hành năm 2005, phiên bản 1.2 phát hành năm 2008, phiên bản 1.3 được phát hành chính thức cho vào tháng 10 năm 2017. Hiện nay phiên bản TLS 1.3 được sử dụng rộng rãi nhất, còn SSL chỉ được giữ lại tên với lý do lịch sử.

Hình 3.39 biểu diễn vị trí của giao thức SSL/TLS trong chồng giao thức TCP/IP. Có thể thấy SSL/TLS hoàn toàn độc lập với các giao thức tầng ứng dụng nên nó có thể được sử dụng để bảo mật thông tin truyền cho nhiều giao thức ứng dụng khác nhau, như HTTP, SMTP và FTP. Chẳng hạn, giao thức bảo mật web HTTPS = HTTP + SSL/TLS, có nghĩa là HTTPS tạo ra bởi HTTP chạy trên nền SSL/TLS. Một trong các điều kiện để SSL/TLS có thể hoạt động là ít nhất một thực thể (thường là máy chủ) tham gia phiên truyền thông phải có chứng chỉ số cho khoá công khai (Public key certificate).



Hình 3.39. SSL/TLS trong bộ giao thức TCP/IP



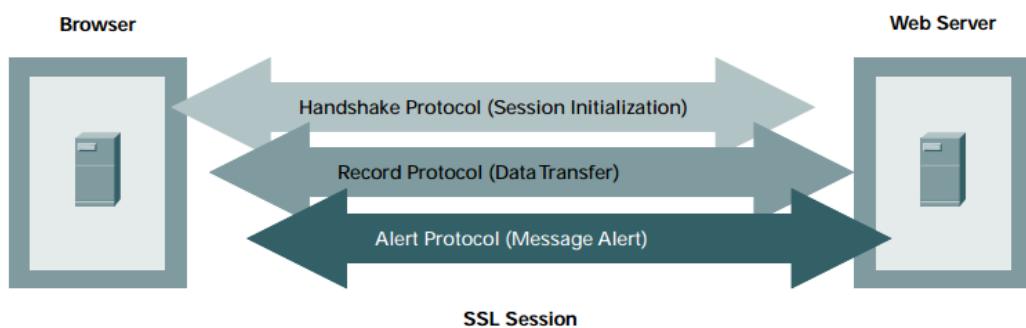
Hình 3.40. Các giao thức con của SSL/TLS

SSL/TLS là một bộ gồm có 4 giao thức con, như minh họa trên Hình 3.40. Các giao thức con của SSL/TLS gồm:

- SSL Handshake Protocol: Giao thức bắt tay của SSL có nhiệm vụ trao đổi các thông điệp xác thực thực thể và thiết lập các thông số cho phiên làm việc;
- SSL Change Cipher Spec Protocol: Giao thức thiết lập việc sử dụng các bộ mã hóa được hỗ trợ bởi cả 2 bên tham gia phiên truyền thông;
- SSL Alert Protocol: Giao thức cảnh báo của SSL;
- SSL Record Protocol: Giao thức bản ghi của SSL có nhiệm vụ tạo đường hầm an toàn để chuyển thông tin đảm bảo tin bí mật, toàn vẹn và xác thực.

3.6.1.2. Hoạt động của SSL/TS

Hình 3.41 biểu diễn mô hình một phiên truyền thông giữa máy chủ web (Web Server) và máy khách web (Browser) dựa trên SSL/TLS. Theo đó, giao thức Bắt tay (Handshake) khởi tạo phiên làm việc (có sự hỗ trợ của giao thức Change Cipher Spec), giao thức Bản ghi (Record) vận chuyển dữ liệu an toàn và giao thức Cảnh báo (Alert) gửi các cảnh báo khi xảy ra lỗi, hoặc một sự kiện đặc biệt.



Hình 3.41. Mô hình truyền thông giữa Web Server và Browser dựa trên SSL/TLS

a. Khởi tạo phiên làm việc

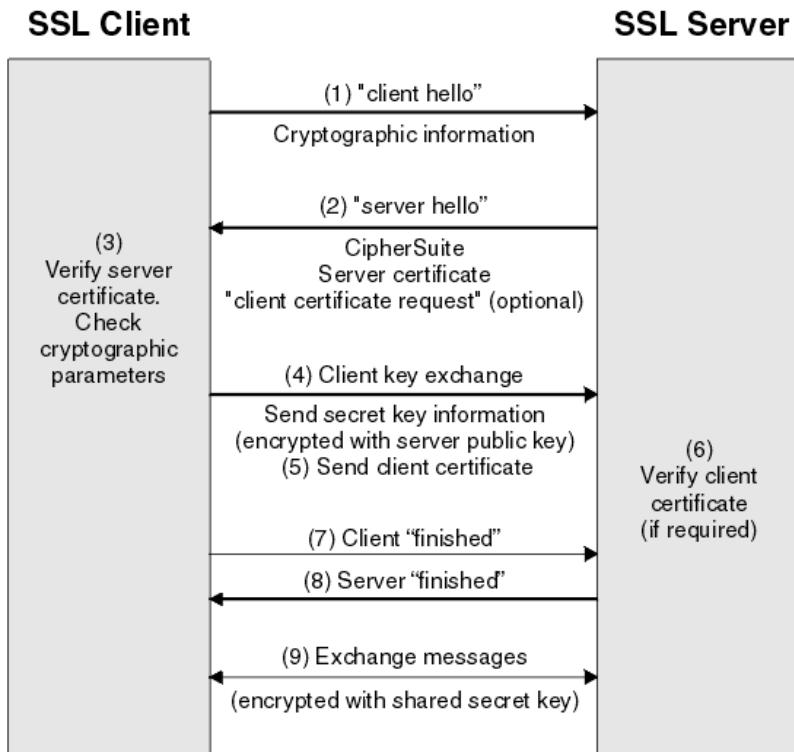
Quá trình khởi tạo phiên làm việc trong SSL/TLS được thực hiện bởi giao thức SSL Handshake với sự hỗ trợ của giao thức SSL Change Cipher Spec. Các nhiệm vụ được các bên tham gia truyền thông thực hiện trong quá trình này bao gồm: (1) xác thực thông tin nhận dạng, (2) đàm phán thống nhất các bộ mã hóa sử dụng và (3) trao đổi khóa và các thông số khác cho phiên truyền thông.

Quá trình khởi tạo phiên làm việc biểu diễn trên Hình 3.42 giữa SSL Client (máy khách) và SSL Server (máy chủ) gồm các bước sau:

1. SSL Client gửi thông điệp “client hello” và thông tin mã hóa (Cryptographic information) đến SSL Server;
2. SSL Server gửi thông điệp “server hello”, các bộ mã hóa hỗ trợ (CipherSuite) và chứng chỉ máy chủ (Server certificate) đến SSL Client. SSL Server cũng có thể gửi yêu cầu máy khách cung cấp chứng chỉ máy khách (Client certificate) nếu cần thiết;
3. Nhận được yêu cầu, SSL Client kiểm tra chứng chỉ máy chủ và kiểm tra các tham số mã hóa. Hai bên thống nhất sử dụng các bộ mã hóa tốt nhất cùng hỗ trợ cho phiên làm việc. Nếu chứng chỉ máy chủ không hợp lệ quá trình khởi tạo

phiên kết thúc không thành công. Nếu chứng chỉ máy chủ hợp lệ tiếp tục bước tiếp theo;

4. Trao đổi khóa máy khách (Client key exchange). SSL Client sinh khóa phiên (hoặc các tham số mã hóa cho phiên), mã hóa khóa phiên sử dụng khóa công khai của SSL Server lấy từ chứng chỉ máy chủ và gửi cho SSL Server;
5. SSL Client cũng có thể gửi chứng chỉ máy khách cho máy chủ nếu được yêu cầu;
6. SSL Server sử dụng khóa riêng của mình để giải mã khôi phục khóa phiên gửi từ SSL Client. SSL Server cũng có thể kiểm tra chứng chỉ máy khách nếu cần thiết;
7. Client gửi thông điệp kết thúc khởi tạo phiên “Finished”;
8. Server gửi thông điệp kết thúc khởi tạo phiên “Finished”.



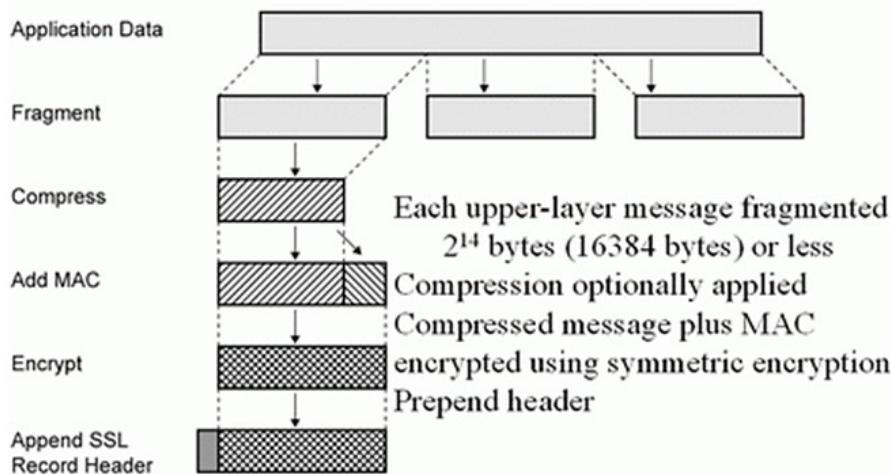
Hình 3.42. Khởi tạo phiên làm việc trong SSL/TLS

Sau khi quá trình khởi tạo thành công, hai bên SSL Client và SSL Server xác thực được các thông tin nhận dạng của nhau sử dụng chứng chỉ số, thông nhất các bộ mã hóa tốt nhất sử dụng và trao đổi được các khóa phiên, hoặc các tham số mã hóa phiên, hai bên thiết lập thành công kênh bảo mật cho truyền dữ liệu trong phiên.

b. Vận chuyển dữ liệu an toàn

Quá trình vận chuyển dữ liệu an toàn thực hiện bởi giao thức SSL Record sau khi khởi tạo phiên làm việc thành công. Giao thức SSL Record sử dụng các tham số mã hóa và các bộ mã hóa thiết lập trong quá trình khởi tạo để tạo đường hầm vận chuyển dữ liệu an toàn. SSL Record đảm bảo tính bí mật cho khối dữ liệu sử dụng mã hóa đối xứng với khóa phiên, và đảm bảo tính toàn vẹn và xác thực cho khối dữ liệu sử dụng hàm băm có khóa (MAC). Hình 3.43 biểu diễn quá trình xử lý dữ liệu bởi SSL Record tại bên gửi, gồm các bước:

SSL Record Protocol Operation



Hình 3.43. Quá trình xử lý dữ liệu bởi SSL Record tại bên gửi

- Phân mảnh dữ liệu (Fragment): Dữ liệu từ ứng dụng (Application Data) được phân mảnh thành các khối cho phù hợp với việc đóng gói và truyền của các lớp giao thức tầng thấp hơn;
- Nén dữ liệu (Compress): Từng khối dữ liệu được được nén để giảm kích thước. Bước nén dữ liệu là không bắt buộc;
- Thêm MAC (Add MAC): Tính toán giá trị MAC (sử dụng hàm băm có khóa) cho khối dữ liệu nén và ghép giá trị MAC vào khối dữ liệu. Việc thêm MAC và kiểm tra MAC ở bên nhận để đảm bảo tính toàn vẹn và xác thực khối dữ liệu;
- Mã hóa (Encrypt): Mã hóa khối dữ liệu (gồm khối dữ liệu nén và MAC) để đảm bảo tính bí mật sử dụng mã hóa khóa đối xứng với khóa phiên;
- Thêm đê mục của SSL Record (Append SSL Record Header): thêm đê mục của SSL Record vào khối dữ liệu đã mã hóa và chuyển xuống tầng giao vận để chuyển sang bên nhận.

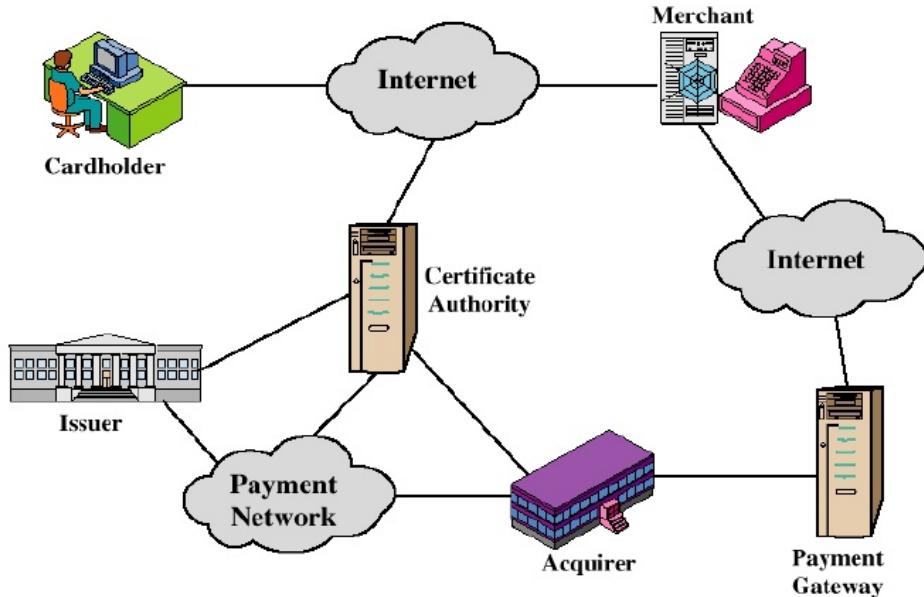
Quá trình xử lý dữ liệu khối dữ liệu nhận được tại bên nhận được thực hiện bởi SSL Record theo trình tự ngược lại, gồm các bước: Tách đê mục của SSL Record, Giải mã, Tách và kiểm tra MAC, Giải nén và Ghép các mảnh dữ liệu thành chuỗi dữ liệu để chuyển cho lớp ứng dụng.

3.6.2. SET

SET (Secure Electronic Transaction) là giao thức cho phép thanh toán điện tử an toàn sử dụng thẻ tín dụng do 2 công ty Visa International và MasterCard (Hoa Kỳ) phát triển. SET có khả năng đảm bảo các thuộc tính bí mật, toàn vẹn thông tin truyền, xác thực tài khoản chủ thẻ và xác thực nhà cung cấp.

Hình 3.44 biểu diễn một mô hình tương tác giữa các thực thể tham gia thực hiện SET. Các thực thể tham gia mô hình này gồm: Chủ thẻ/Khách hàng (Cardholder), Nhà cung cấp dịch vụ/Người bán hàng (Merchant), Cổng thanh toán (Payment Gateway), Ngân hàng của nhà cung cấp/Ngân hàng của người bán (Acquirer), Ngân hàng của chủ

thẻ/Ngân hàng của người mua (Issuer) và Nhà cung cấp chứng chỉ (Certificate Authority). Tất cả các bên tham gia quá trình xử lý giao dịch thanh toán (Cardholder, Merchant, Payment Gateway, Acquirer, Issuer) đều phải đăng ký với Nhà cung cấp chứng chỉ và được cấp chứng chỉ khóa công khai. Các chứng chỉ khóa công khai được các bên sử dụng để xác thực thông tin nhận dạng của nhau và hỗ trợ trao đổi khóa. Quá trình thực hiện một giao dịch dựa trên SET gồm các bước sau:



Hình 3.44. Một mô hình tương tác giữa các thực thể tham gia SET

1. Khách hàng xem các sản phẩm trên website của Người bán hàng và quyết định các mặt hàng sẽ mua;
2. Khách hàng gửi thông điệp gồm thông tin đơn hàng và thanh toán gồm 2 phần: (i) Đơn hàng – dành cho Người bán hàng và (ii) Thông tin thẻ - dành cho hệ thống thanh toán;
3. Người bán hàng chuyển thông tin thẻ cho Cổng thanh toán. Cổng thanh toán chuyển tiếp cho Ngân hàng của người bán;
4. Ngân hàng của người bán gửi yêu cầu xác thực giao dịch thanh toán đến Ngân hàng của người mua;
5. Ngân hàng của người mua gửi xác nhận giao dịch đến Ngân hàng của người bán;
6. Ngân hàng của người bán gửi xác nhận giao dịch đến Người bán hàng;
7. Người bán hàng hoàn tất đơn hàng và gửi xác nhận đơn hàng đến Khách hàng;
8. Người bán hàng ghi nhận giao dịch theo thông tin từ Ngân hàng người bán cung cấp;
9. Ngân hàng của người mua in hóa đơn giao dịch cho thẻ tín dụng của Khách hàng.

3.6.3. PGP

a. Giới thiệu

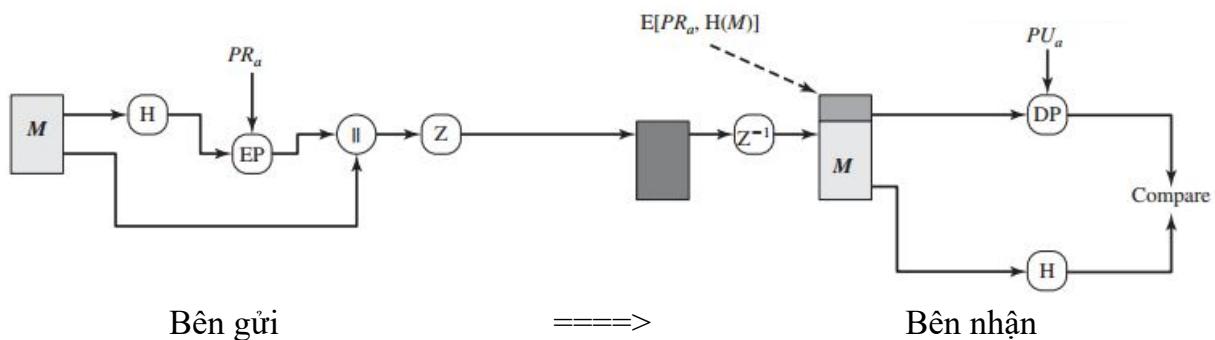
PGP (Pretty Good Privacy) là phương pháp bảo mật do Philip Zimmermann phát triển năm 1991 có khả năng cung cấp tính riêng tư và tính xác thực các thông điệp truyền. PGP

được sử dụng rộng rãi và đã được thừa nhận thành chuẩn thực tế (RFC 3156). PGP hỗ trợ mã hoá dữ liệu sử dụng mã hoá bí mật và mã hóa khoá công khai, đồng thời cho phép tạo và kiểm tra chữ ký số.

PGP được sử dụng rộng rãi để truyền email và file an toàn. PGP hỗ trợ hầu hết các giải thuật mã hóa hiện đại như 3DES, AES, IDEA, RSA, ElGamal. Có nhiều bản cài đặt PGP trên thực tế như OpenPGP, GnuPG, Gpg4win,....

b. Hoạt động của PGP

PGP hỗ trợ 3 mô hình hoạt động, bao gồm (1) Mô hình PGP chỉ đảm bảo tính xác thực thông điệp, (2) Mô hình PGP chỉ đảm bảo tính bí mật thông điệp và (3) Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp. Để thuận tiện cho mô tả hoạt động của các mô hình PGP, gọi H là hàm băm một chiều, EC là hàm mã hóa khóa đối xứng, DC là hàm giải mã khóa đối xứng, EP là hàm mã hóa khóa bất đối xứng, DP là hàm giải mã khóa bất đối xứng, Z là hàm nén, Z^{-1} là hàm giải nén, PUa là khóa công khai của bên A, PRa là khóa riêng của bên A, PUB là khóa công khai của bên B, PRb là khóa riêng của bên B và Ks là khóa phiên. Phần tiếp theo trình bày chi tiết về hoạt động của các mô hình này.

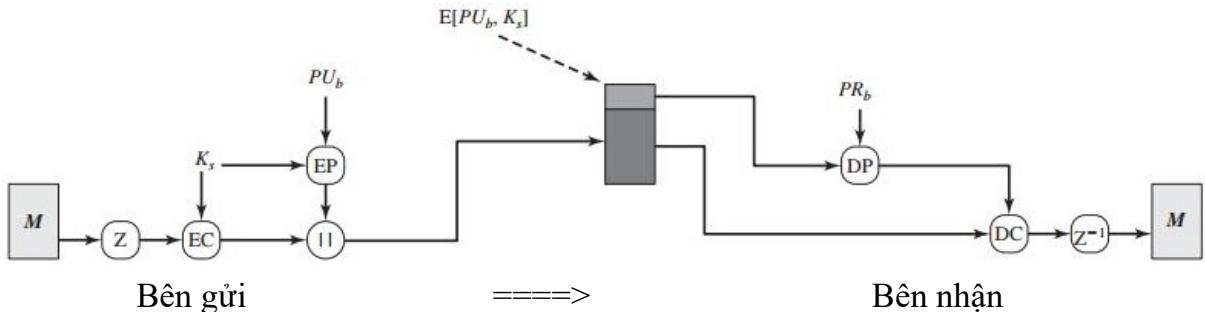


Hình 3.45. Mô hình PGP chỉ đảm bảo tính xác thực thông điệp

Hình 3.45 biểu diễn mô hình PGP chỉ đảm bảo tính xác thực thông điệp truyền. Theo đó, mô hình này sử dụng chữ ký số để xác thực tính toàn vẹn và chủ thể gửi thông điệp. Điều kiện thực hiện mô hình này là bên gửi A phải sở hữu cặp khóa (khóa công khai PUa và khóa riêng PRa). Quá trình thực hiện gửi/nhận thông điệp M đảm bảo tính xác thực tại mỗi bên như sau:

- Bên gửi A:
 - + Tính toán giá trị băm (giá trị đại diện) của thông điệp M sử dụng hàm băm H;
 - + Sử dụng khóa riêng PRa để mã hóa (ký) giá trị băm của M tạo thành chữ ký số;
 - + Ghép chữ ký số vào thông điệp M;
 - + Nén thông điệp và chữ ký số sử dụng hàm nén Z;
 - + Gửi bản dữ liệu đã nén cho người nhận.
- Bên nhận B:
 - + Giải nén dữ liệu nhận được sử dụng hàm Z^{-1} ;

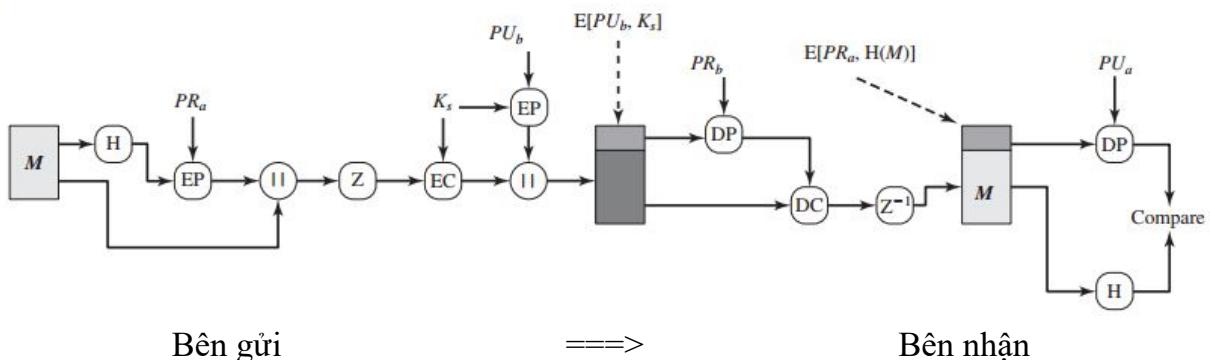
- + Tách chữ ký số khỏi thông điệp M và sử dụng khóa công khai của bên gửi PUb để kiểm tra (giải mã) chữ ký số để khôi phục giá trị băm $h1$. Bên gửi A có thể sử dụng các phương pháp trao đổi khóa công khai đã nêu ở mục 3.5.3 để chuyển khóa công khai PUb cho bên nhận;
- + Tính toán giá trị băm $h2$ của thông điệp M sử dụng hàm băm H ;
- + So sánh 2 giá trị băm $h1$ và $h2$, nếu $h1 = h2$ thì thông điệp truyền là toàn vẹn và thông điệp được gửi bởi bên gửi A. Nếu $h1 \neq h2$ thì thông điệp M có thể đã bị sửa đổi, hoặc không được ký và gửi bởi bên gửi A.



Hình 3.46. Mô hình PGP chỉ đảm bảo tính bí mật thông điệp

Hình 3.46 biểu diễn mô hình PGP chỉ đảm bảo tính bí mật thông điệp truyền. Theo đó, mô hình này sử dụng kết hợp giữa mã hóa khóa đối xứng và mã hóa khóa bất đối xứng để đảm bảo tính bí mật của thông điệp. Điều kiện thực hiện mô hình này là bên nhận B phải sở hữu cặp khóa (khóa công khai PUb và khóa riêng PRb). Quá trình thực hiện gửi/nhận thông điệp M đảm bảo tính bí mật tại mỗi bên như sau:

- Bên gửi A:
 - + Nén thông điệp M sử dụng hàm nén Z ;
 - + Sinh khóa phiên Ks và sử dụng khóa Ks để mã hóa thông điệp M sử dụng hàm mã hóa đối xứng EC;
 - + Sử dụng khóa công khai PUb của bên nhận B để mã hóa khóa phiên Ks sử dụng hàm mã hóa bất đối xứng EP. Bên nhận B có thể sử dụng các phương pháp trao đổi khóa công khai đã nêu ở mục 3.5.3 để chuyển khóa công khai PUb cho bên gửi;
 - + Ghép chữ bắn mã của Ks vào bắn mã của thông điệp M ;
 - + Gửi bắn mã dữ liệu cho người nhận.
- Bên nhận B:
 - + Tách bắn mã của Ks vào bắn mã của thông điệp M ;
 - + Giải mã bắn mã Ks sử dụng hàm giải mã khóa bất đối xứng DP và khóa riêng PRb để khôi phục Ks ;
 - + Sử dụng khóa phiên Ks và hàm giải mã khóa đối xứng DC để giải mã khôi phục thông điệp đã nén M ;
 - + Giải nén khôi phục thông điệp M sử dụng hàm Z^{-1} ;



Hình 3.47. Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp

Hình 3.47 biểu diễn mô hình PGP đảm bảo tính xác thực và bí mật thông điệp truyền. Theo đó, mô hình này sử dụng chữ ký số để xác thực tính toàn vẹn và chủ thể gửi thông điệp. Đồng thời mô hình sử dụng kết hợp giữa mã hóa khóa đối xứng và mã hóa khóa bất đối xứng để đảm bảo tính bí mật của thông điệp. Điều kiện thực hiện mô hình này là bên gửi A phải sở hữu cặp khóa (khóa công khai PUa và khóa riêng PRa) và bên nhận B phải sở hữu cặp khóa (khóa công khai PUB và khóa riêng PRb). Mô hình này là sự kết hợp của mô hình PGP chỉ đảm bảo tính xác thực và mô hình PGP chỉ đảm bảo tính bí mật. Theo đó, bên gửi A thực hiện ký và mã hóa thông điệp, còn bên nhận B thực hiện giải mã và kiểm tra chữ ký của thông điệp.

3.7. Câu hỏi ôn tập

- 1) Mã hóa thông tin là gì? Nêu vai trò của mã hóa.
- 2) Mô tả các thành phần của một hệ mã hóa.
- 3) Mô tả các phương pháp mã hóa dòng và mã hóa khối.
- 4) Nêu các ứng dụng của mã hóa.
- 5) Mô tả phương pháp mã hóa thay thế (substitution).
- 6) Mô tả phương pháp mã hóa hoán vị (permutation).
- 7) Mô tả phương pháp mã hóa XOR.
- 8) Vẽ sơ đồ hoạt động và nêu các đặc điểm hệ mã hóa khóa đối xứng.
- 9) Vẽ sơ đồ hoạt động và nêu các đặc điểm hệ mã hóa khóa bất đối xứng.
- 10) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật mã hóa DES.
- 11) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật mã hóa AES.
- 12) Nêu các đặc điểm, thủ tục sinh khóa, mã hóa và giải mã của giải thuật mã hóa RSA.
- 13) Nêu các yêu cầu đảm bảo an toàn của quá trình sinh khóa RSA.
- 14) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật băm MD5.
- 15) Nêu các đặc điểm và mô tả các bước xử lý dữ liệu của giải thuật băm SHA1.
- 16) Chữ ký số là gì? Mô tả quá trình tạo chữ ký và kiểm tra chữ ký của một thông điệp.
- 17) Chứng chỉ số khóa công khai là gì? Nêu 3 thành phần quan trọng nhất của 1 chứng chỉ số khóa công khai. Nêu các ứng dụng của chứng chỉ số khóa công khai.
- 18) PKI là gì? Nêu các thành phần và mô tả lưu đồ cấp và sử dụng chứng chỉ trong PKI.

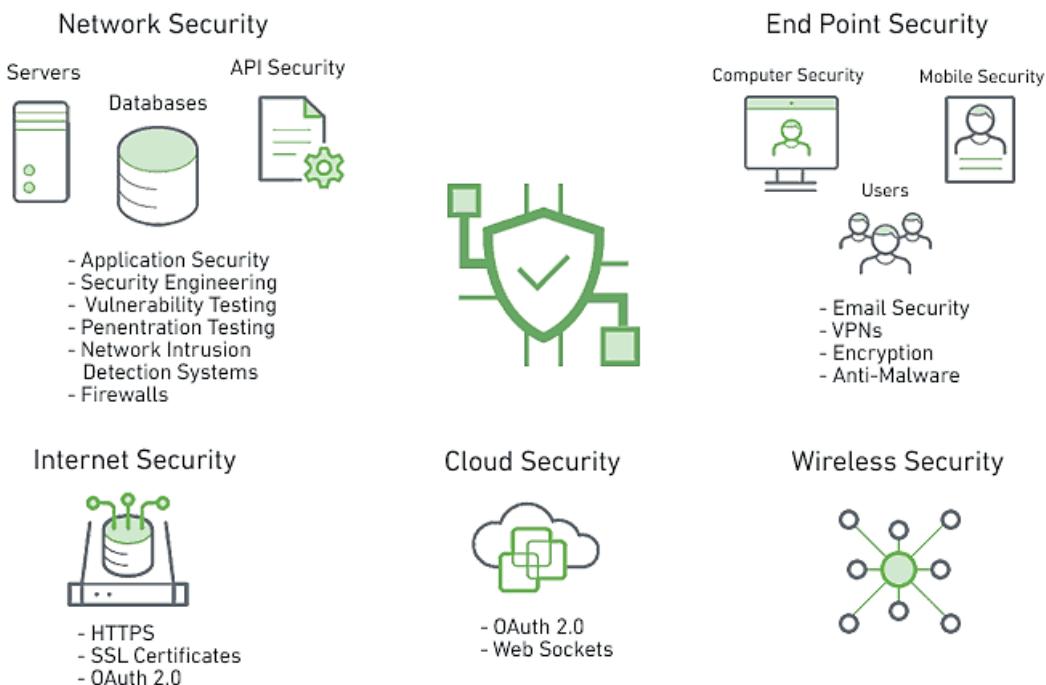
- 19) Mô tả cơ chế hoạt động của phương pháp phân phối khóa dựa trên KDC, KTC.
- 20) Mô tả quá trình khởi tạo phiên làm việc trong SSL/TLS.
- 21) Mô tả quá trình xử lý dữ liệu bởi SSL Record tại bên gửi và bên nhận.
- 22) Mô tả hoạt động của mô hình PGP chỉ đảm bảo tính xác thực và mô hình PGP chỉ đảm bảo tính bí mật.

CHƯƠNG 4. CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐẢM BẢO AN TOÀN THÔNG TIN

Chương 4 giới thiệu khái quát về các kỹ thuật và công nghệ đảm bảo an toàn thông tin, vấn đề 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 giới thiệu về tường lửa – một trong những 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 và ngăn chặn xâm nhập.

4.1. Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

Trong an toàn thông tin, có nhiều kỹ thuật và công nghệ đảm bảo an toàn cho thông tin, hệ thống và mạng trong các lĩnh vực khác nhau của an toàn thông tin, như minh họa trên Hình 4.1.



Hình 4.1. Các kỹ thuật và công nghệ bảo mật trong các lĩnh vực của ATTT

Theo đó, các kỹ thuật, công nghệ và giải pháp đảm bảo an toàn thông tin bao gồm:

- Trong lĩnh vực an ninh mạng (Network Security):
 - + An toàn ứng dụng (Application Security)
 - + Kỹ nghệ an toàn (Security Engineering)
 - + Kiểm thử lỗ hổng (Vulnerability Testing)
 - + Kiểm thử xâm nhập (Penetration Testing)
 - + Các hệ thống phát hiện xâm nhập (Intrusion Detection Systems)
 - + Tường lửa (Firewalls).
- Trong lĩnh vực an ninh thiết bị đầu cuối (End Point Security):

- + Kiểm soát truy cập
- + Bảo mật email (Email Security)
- + Mạng VPNs
- + Mã hóa (Encryption)
- + Quét và ngăn chặn phần mềm độc hại (Anti-Malware).
- Trong lĩnh vực an ninh Internet (Internet Security):
 - + Secure HTTP (HTTPS)
 - + Chứng chỉ SSL (SSL Certificate)
 - + Chuẩn xác thực mở (OAuth 2.0).
- Trong lĩnh vực an ninh đám mây (Cloud Security):
 - + Chuẩn xác thực mở (OAuth 2.0)
 - + Web Sockets.
- Trong lĩnh vực an ninh mạng không dây (Wireless Security):
 - + Mã hóa (Encryption)
 - + Kiểm soát truy cập.

Chương 2 của tài liệu này đã đề cập đến một số kỹ thuật và giải pháp phân tích, kiểm thử lỗ hổng bảo mật, kiểm thử xâm nhập và vấn đề rà quét và ngăn chặn phần mềm độc hại. Chương 3 đã trình bày các kỹ thuật và giải pháp dựa trên mã hóa cho đảm bảo an toàn thông tin, bao gồm chứng chỉ SSL, PGP cho bảo mật file và email, giao thức bảo mật SSL/TLS nền tảng cho HTTPS. Trong phạm vi của môn học này, chương này tiếp tục trình bày một số kỹ thuật, công nghệ và giải pháp quan trọng khác cho đảm bảo an toàn thông tin bao gồm, Kiểm soát truy cập, Tường lửa và Các hệ thống phát hiện tấn công, xâm nhập.

4.2. Kiểm soát truy cập

4.2.1. Khái niệm kiểm soát truy cập

Kiểm soát truy cập (Access control) là quá trình mà trong đó người dùng được *nhận dạng* và *trao quyền* truy nhập đến các thông tin, các hệ thống và tài nguyên. Một hệ thống kiểm soát truy cập có thể được cấu thành từ 3 dịch vụ: Xác thực (Authentication), Trao quyền, hoặc cấp quyền (Authorization) và Quản trị (Administration).

Xác thực là quá trình xác minh tính chân thực 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 đó. 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.

Quản trị là dịch vụ cung cấp khả năng thêm, bớt và sửa đổi các thông tin tài khoản người dùng, cũng như quyền truy cập của người dùng trong hệ thống. Mặc dù quản trị

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.

Mục đích chính của kiểm soát truy cập là để đảm bảo tính bí mật, toàn vẹn và sẵn dùng hoặc khả dụng của thông tin, hệ thống và các tài nguyên. Đây cũng là các yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin đã đề cập trong CHƯƠNG 1.

4.2.2. Các biện pháp kiểm soát truy cập

Các biện pháp hay cơ chế (mechanism) 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.

4.2.2.1. Kiểm soát truy cập tùy chọn

Kiểm soát truy cập tùy chọn (còn gọi là tùy quyền) được định nghĩa là các 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 (còn gọi là các *nhân tố - factor*) có thể gồm:

- Bạn là ai? (CMND, bằng lái xe, vân tay,...)
- Những cái bạn biết (tên truy nhập, 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 (owner of objects) 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 (home directory) 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 các người dùng khác.

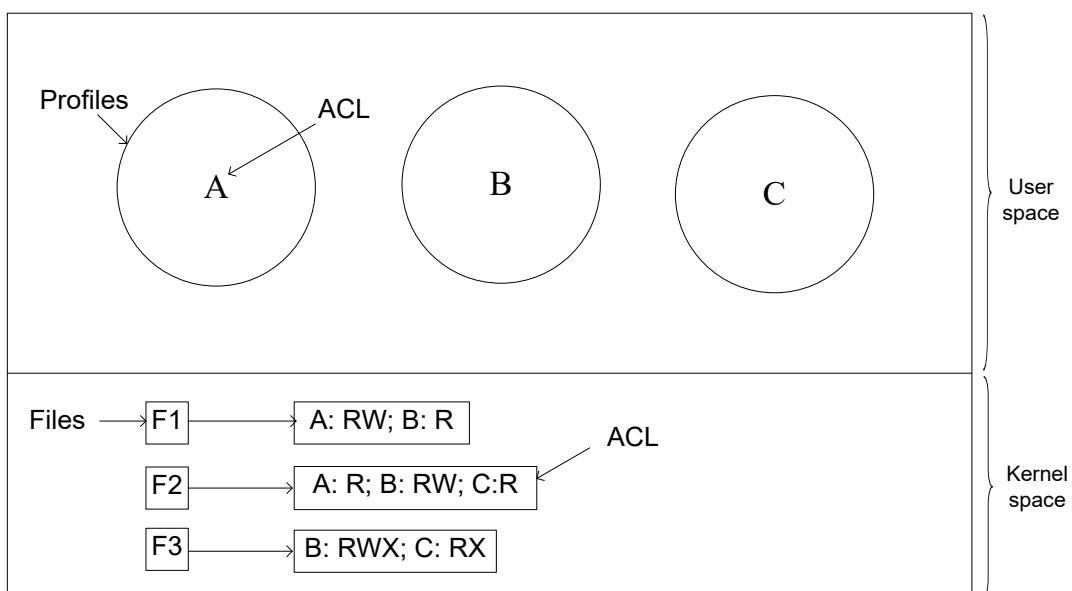
Có nhiều kỹ thuật thực hiện cơ chế kiểm soát truy cập tùy chọn trên thực tế, trong đó 2 kỹ thuật được sử dụng rộng rãi nhất là *Ma trận kiểm soát truy cập* (Access Control Matrix - ACM) và *Danh sách kiểm soát truy cập* (Access Control List - ACL). Ma trận kiểm soát truy cập là một phương pháp thực hiện kiểm soát truy cập thông qua 1 ma trận 2 chiều gồm chủ thể (subject), đối tượng (object) và các quyền truy cập, như biểu diễn trên Hình 4.2. Các đối tượng, hay khách thể (Objects) 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 (process). Các chủ thể (Subjects) là người dùng (users), 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).

Subjects \ Objects	O1	O2	O3	O4
Subjects				
S1	rw	rwxo	r	rwxo
S2	rw	rx	rw	rwx
S3	r	rw	rwo	rw

Hình 4.2. Mô hình ma trận kiểm soát truy cập

Ưu điểm của ma trận kiểm soát truy cập là đơn giản, trực quan 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 vào 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 vào đối tượng 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 (ACL) 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 các 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 (subject, operation). 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 4.3. Mô hình danh sách kiểm soát truy cập

Hình 4.3 biểu diễn mô hình danh sách kiểm soát truy cập trong không gian người dùng (user space) và không gian nhân (kernel space) tổ chức bởi hệ điều hành. Mỗi file (F1, F2, F3,...) có một danh sách kiểm soát truy cập (ACL) của riêng mình lưu trong hò

sơ (profile) của file. Quyền truy cập vào file được tổ chức thành một chuỗi gồm nhiều cặp (subject, operation), với A, B, C là ký hiệu biểu diễn chủ thể (subject) và các thao tác (operation) hay quyền gồm R (Read - đọc), W (Write - ghi), và X (eXecute - thực hiện). Chẳng hạn, trong danh sách kiểm soát truy cập F1(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).

4.2.2.2. Kiểm soát truy cập bắt buộc

Điều khiển truy bắt buộc (MAC) được định nghĩa là các cơ chế hạn chế truy cập đến các đối tượng dựa trên hai yếu tố chính:

- Tính nhạy cảm (sensitivity) của thông tin chứa trong các đối tượng, và
- Sự trao quyền chính thức (formal authorization) cho các chủ thể truy cập các thông tin nhạy cảm này.

Các thông tin nhạy cảm thường được gán nhãn với các *mức nhạy cảm* (Sensitivity level). 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:

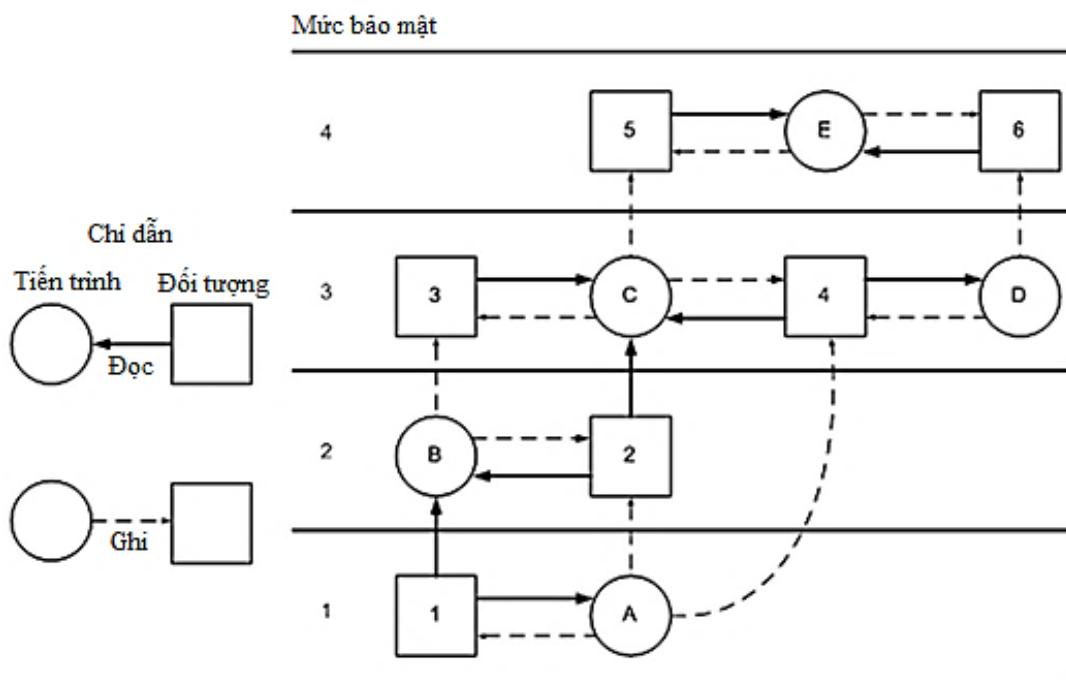
- Tối mật (Top Secret - T): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến những thiệt hại trầm trọng đối với an ninh quốc gia.
- Tuyệt mật (Secret - S): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến một loạt thiệt hại đối với an ninh quốc gia.
- Mật (Confidential - C): Được áp dụng 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 hoàn toàn 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 như, 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.

Có nhiều kỹ thuật thực hiện cơ chế kiểm soát truy cập bắt buộc, trong đó mô hình kiểm soát truy cập Bell-LaPadula là một trong các kỹ thuật được sử dụng rộng rãi nhất. Mô hình Bell-LaPadula 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, bí 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 chạy nhân danh một người sử dụng có được mức độ bảo mật của người dùng đó.

Mô hình Bell-LaPadula sử dụng nguyên tắc “đọc xuống” (read down) và nguyên tắc “ghi lên” (write up) để đảm bảo an toàn trong việc cấp quyền truy cập cho người dùng đến các đối tượng. 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 một trung úy không thể đọc các tài liệu của vị tướng đó. 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 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 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 4.4. Mô hình kiểm soát truy cập Bell-LaPadula

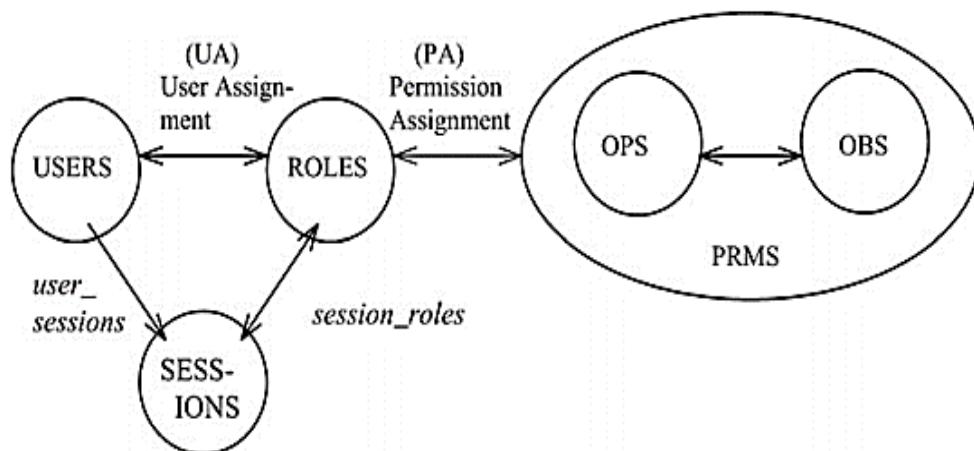
Hình 4.4 minh họa việc thực hiện các nguyên tắc “đọc xuống” và nguyên tắc “ghi lên” trong mô hình Bell-LaPadula. Trong đó, các tiến trình chạy bởi người dùng được ký hiệu A, B, C, D, E được biểu diễn bởi các hình tròn và các đối tượng được đánh số 1, 2, 3, 4, 5. Mũi tên liền nét biểu diễn quyền đọc, mũi tên đứt nét biểu diễn quyền ghi và các mức bảo mật cho cả tiến trình và đối tượng được đánh số 1, 2, 3, 4. 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 2. B không được phép đọc đối tượng số 3 do 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 2. Tuy nhiên, B không được phép ghi đối tượng số 1 do đối tượng này có mức bảo mật thấp hơn.

4.2.2.3. Kiểm soát truy cập dựa trên vai trò

Kiểm soát truy cập dựa trên vai trò (RBAC) 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 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 4.5 minh họa một mô hình RBAC đơn giản, trong đó quyền truy cập vào các đối tượng (PRMS) được tập hợp thành các nhóm vai trò (Roles) và việc cấp quyền truy cập các đối tượng cho người dùng (Users) được thực hiện thông qua thao tác gán quyền (UA – User Assignment). 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 4.5. Một mô hình RBAC đơn giản

4.2.2.4. Kiểm soát truy cập dựa trên luật

Kiểm soát truy cập dựa trên luật (Rule-based Access Control) là cơ chế cho phép người dùng truy cập vào hệ thống và thông tin dựa trên các luật (rules) 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. Các tường lửa (firewalls), hoặc proxies là ví dụ điển hình về việc thực hiện cơ chế kiểm soát truy cập dựa trên luật. Các luật thực hiện kiểm soát truy cập sử dụng các thông tin trích xuất từ các gói tin, thông tin về nội dung truy cập, có thể bao gồm:

- Địa chỉ IP nguồn và đích của các gói tin;
- Phân mỏ rộng các file để lọc các mã độc hại;
- 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 4.6 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 4.6. Một số luật của tường lửa lọc gói tin

4.2.3. 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).

4.2.3.1. 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 rẻ tiền. Thông thường, mỗi người dùng được cấp 1 tài khoản (account) để truy cập vào hệ thống. Mỗi tài khoản người dùng thường gồm 2 thành tố: tên người dùng (username) và mật khẩu (password), 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 hệ thống ở dạng rõ (plaintext) hoặc dạng mã hóa (encrypted text - thường dưới dạng giá trị băm).

Tính bảo mật 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 kích thước đủ lớn. Với các tài khoản của ứng dụng thông thường, khuyến nghị nên sử dụng cả ký tự in thường, ký tự in hoa, chữ số và ký tự đặc biệt trong mật khẩu với độ dài từ 8 ký tự trở lên. Theo tuổi thọ, mật khẩu gồm 3 loại: không hết hạn, có thời hạn sống và mật khẩu sử dụng 1 lần. Để đảm bảo an toàn, khuyến nghị định kỳ đổi mật khẩu. Khoảng thời gian sống 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. 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.

4.2.3.2. Kiểm soát truy cập dựa trên các khóa mã

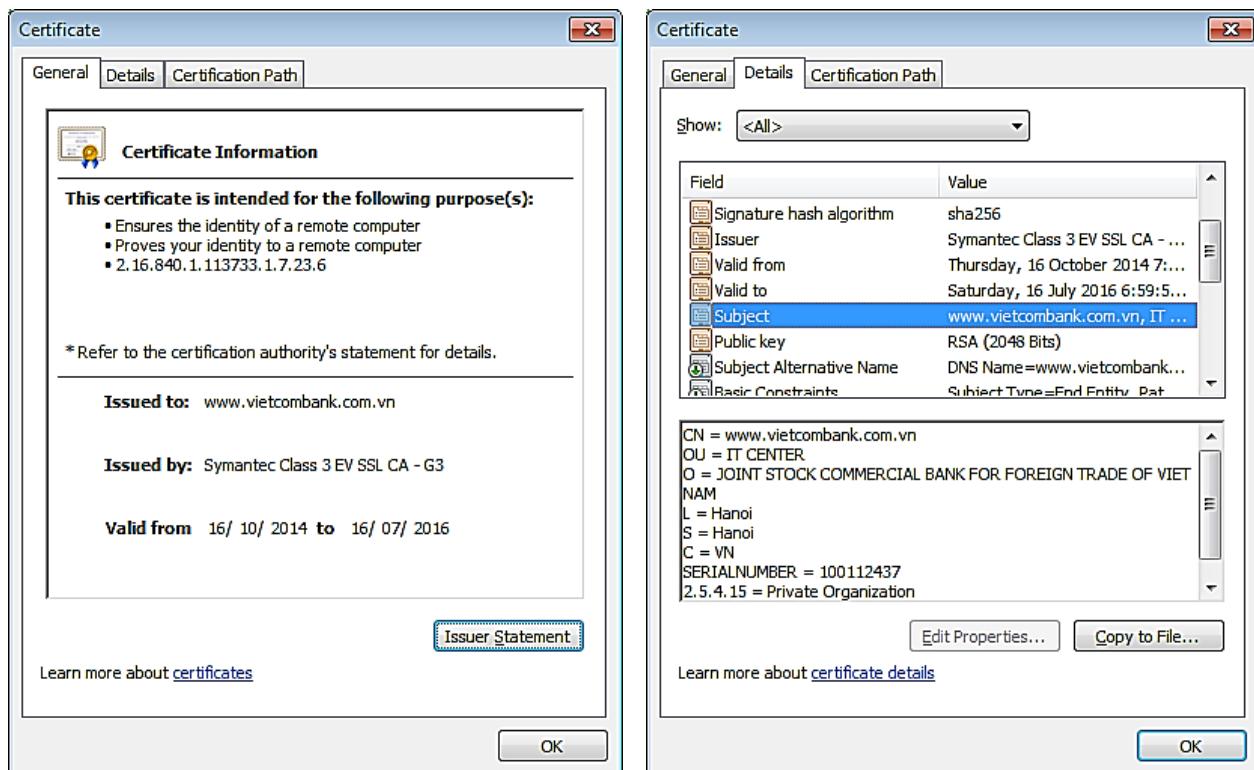
Kiểm soát truy cập dựa trên các *khoá mã* cho phép đảm bảo tính bí mật của thông tin và đồng thời cho phép kiểm tra thông tin nhận dạng của các bên tham gia giao dịch. Một trong các ứng dụng rộng rãi nhất của khóa mã là chứng chỉ số khóa công khai (Public Key Digital Certificate). Một chứng chỉ số khóa công khai thường gồm 3 thông tin quan trọng nhất:

- Thông tin nhận dạng của chủ thẻ (Subject);
- Khoá công khai của chủ thẻ (Public key);
- Chữ ký số của nhà cung cấp chứng chỉ số (Certificate Authority – CA).

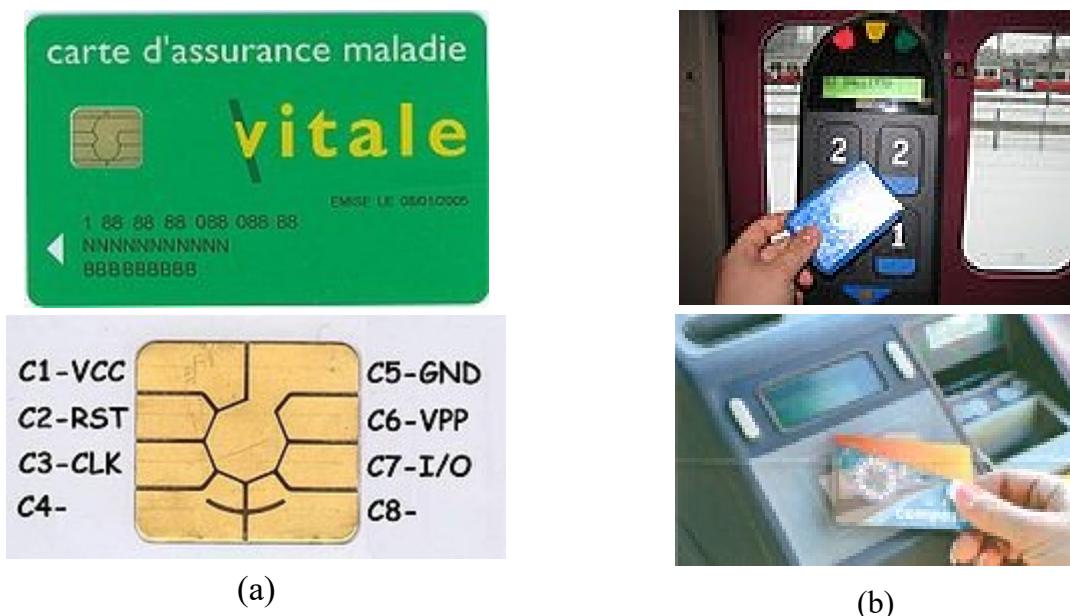
Hình 4.7 là giao diện kiểm tra thông tin của một chứng chỉ số khóa công khai cấp cho tên miền www.vietcombank.com.vn. Chứng chỉ số khóa công khai có thể được sử dụng để xác thực các thực thể tham gia phiên truyền thông, đồng thời hỗ trợ trao đổi khóa cho các khâu mã hóa – giải mã thông điệp, nhằm đảm bảo tính bí mật thông điệp truyền.

4.2.3.3. Kiểm soát truy cập dựa trên thẻ thông minh

Thẻ thông minh (Smartcard) là các thẻ nhựa có gắn các chip điện tử với khả năng tính toán và các thông tin lưu trong thẻ được mã hóa. Kiểm soát truy cập dựa trên thẻ thông minh là phương pháp có độ an toàn cao do smartcard sử dụng hai nhân tố (two-factors) để xác thực và nhận dạng chủ thẻ: (1) cái bạn có (what you have) - thẻ smartcard và (2) cái bạn biết (what you know) - số PIN. Hình 4.8 là hình ảnh thẻ thông minh tiếp xúc (a) và thẻ thông minh không tiếp xúc (b).



Hình 4.7. Giao diện kiểm tra thông tin của một chứng chỉ số khóa công khai



Hình 4.8. Thẻ thông minh tiếp xúc (a) và thẻ không tiếp xúc (b)

4.2.3.4. 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 thẻ 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 (thường dùng 1 lần). 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

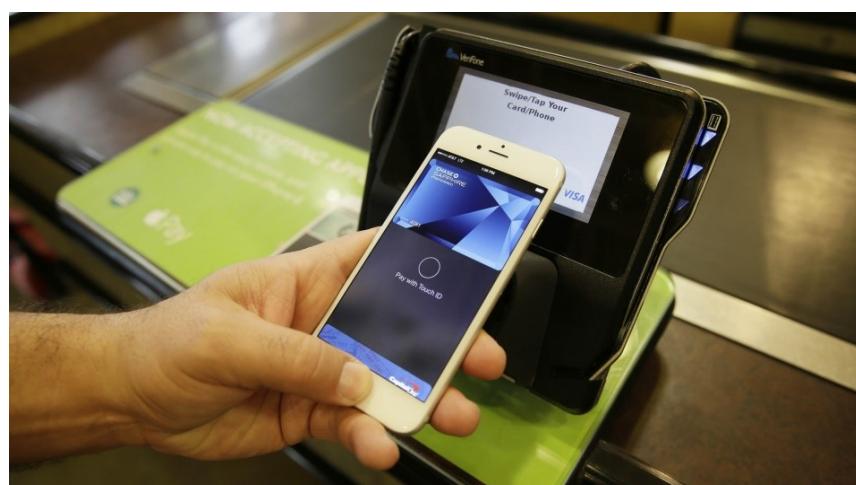
hơn và bộ nhớ lưu trữ lớn hơn. Hình 4.9, Hình 4.10 và Hình 4.11 minh họa một số thẻ bài của hãng RSA Security, ví điện tử của cổng thanh toán trực tuyến Paypal và hệ thống ApplePay tích hợp vào điện thoại di động.



Hình 4.9. Một số thẻ bài (Token) của hãng RSA Security



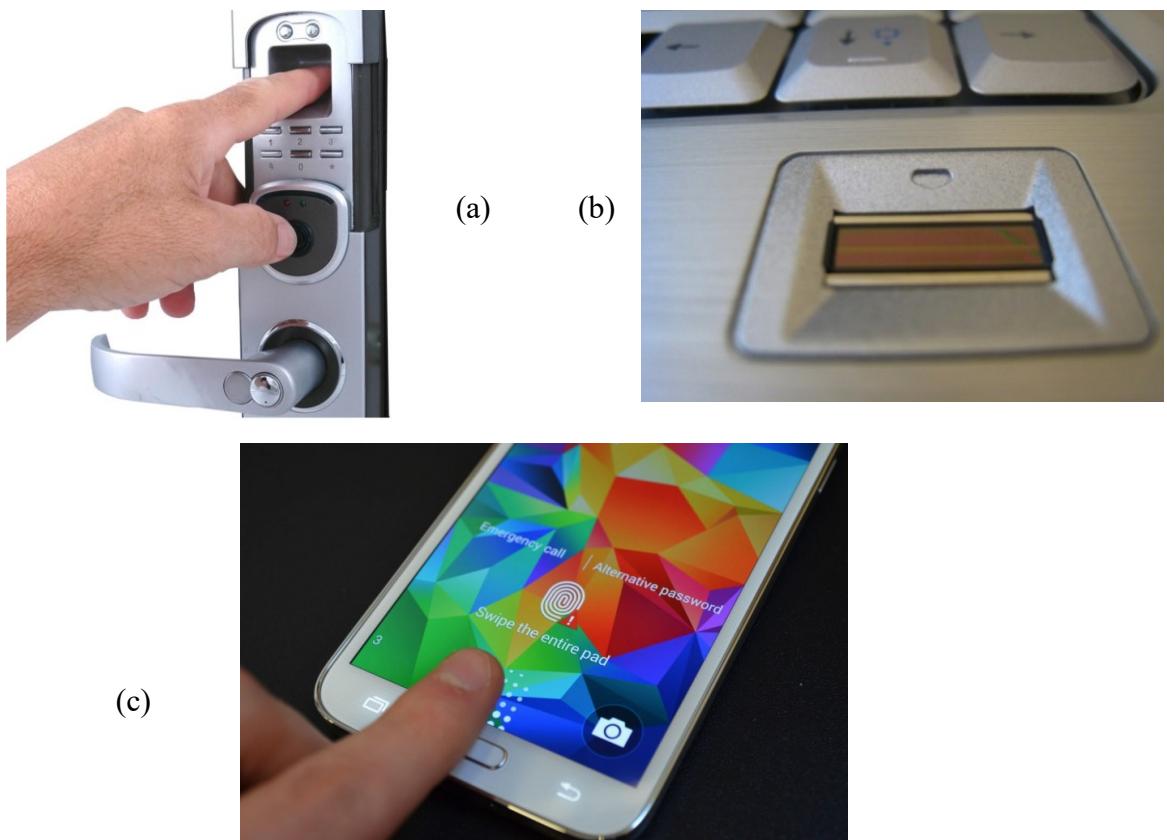
Hình 4.10. Ví điện tử (một dạng thẻ bài) của cổng thanh toán trực tuyến Paypal



Hình 4.11. Hệ thống ApplePay tích hợp vào điện thoại di động

4.2.3.5. 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. Hình 4.12 minh họa (a) Khóa vân tay, (b) Khe xác thực vân tay trên laptop và (c) Xác thực vân tay trên điện thoại thông minh Samsung. Hình 4.13 minh họa việc quét võng mạc để nhận dạng tròng mắt.



Hình 4.12. (a) Khóa vân tay, (b) Khe xác thực vân tay trên laptop và (c) Xác thực vân tay trên điện thoại thông minh Samsung



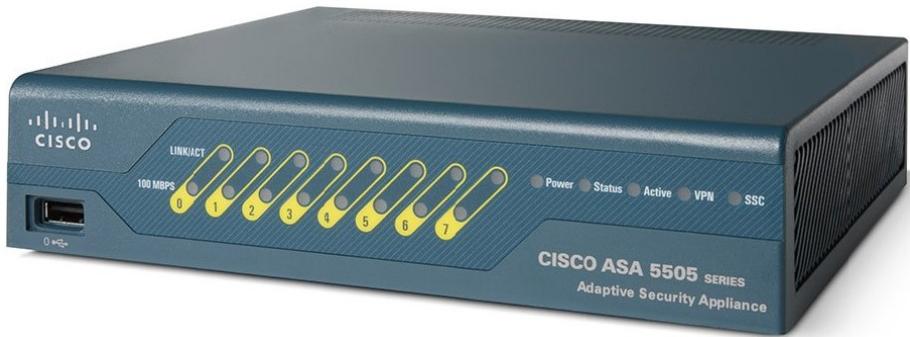
Hình 4.13. Quét võng mạc nhận dạng tròng mắt

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 rất lớn. Một vấn đề khác cần quan tâm là tỷ lệ nhận dạng sai 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.

4.3. Tường lửa

4.3.1. Giới thiệu tường lửa

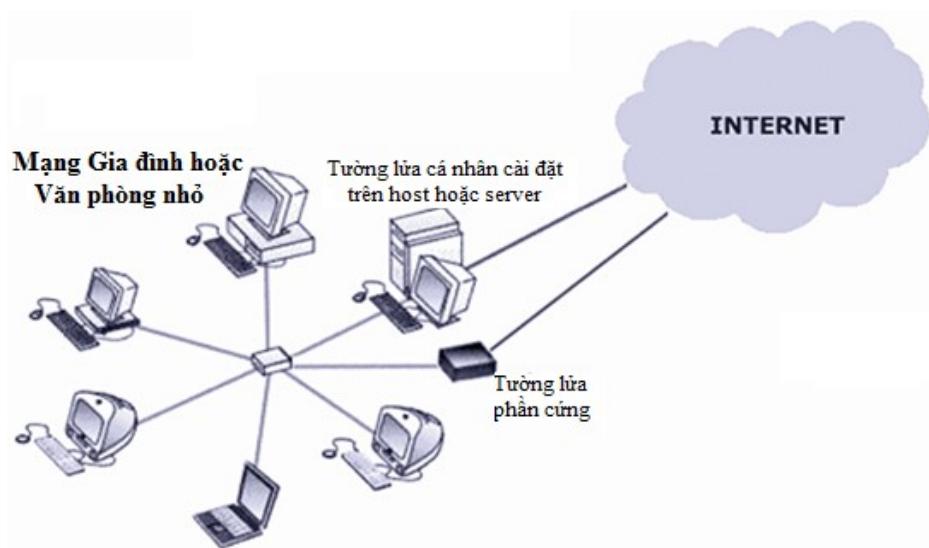
Tường lửa (Firewall) là một trong các kỹ thuật được sử dụng phổ biến nhất để bảo vệ hệ thống và mạng cục bộ tránh các mối đe dọa từ bên ngoài. Tường lửa có thể là một thiết bị phần cứng chuyên dụng, hoặc mô đun phần mềm chạy trên máy tính. Hình 4.14 là hình ảnh một tường lửa phần cứng chuyên dụng của hãng Cisco.



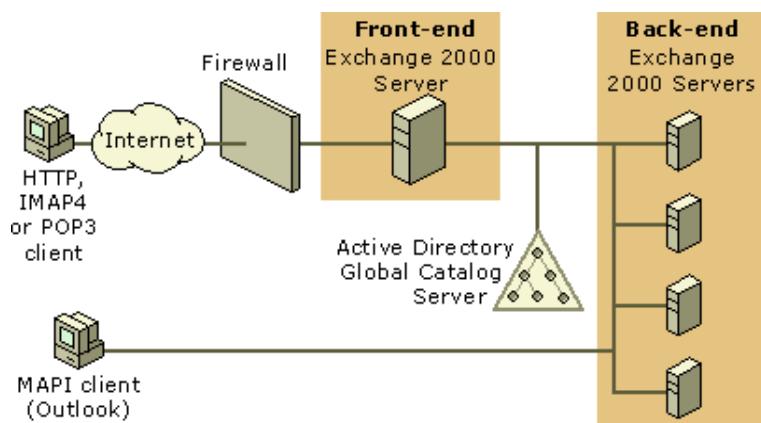
Hình 4.14. Một tường lửa phần cứng chuyên dụng của Cisco

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 4.15. 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 (filtering) dựa trên các luật (rules). Tập các luật sử dụng cho việc lọc các gói tin được tạo ra dựa trên chính sách an ninh của cơ quan, tổ chức.

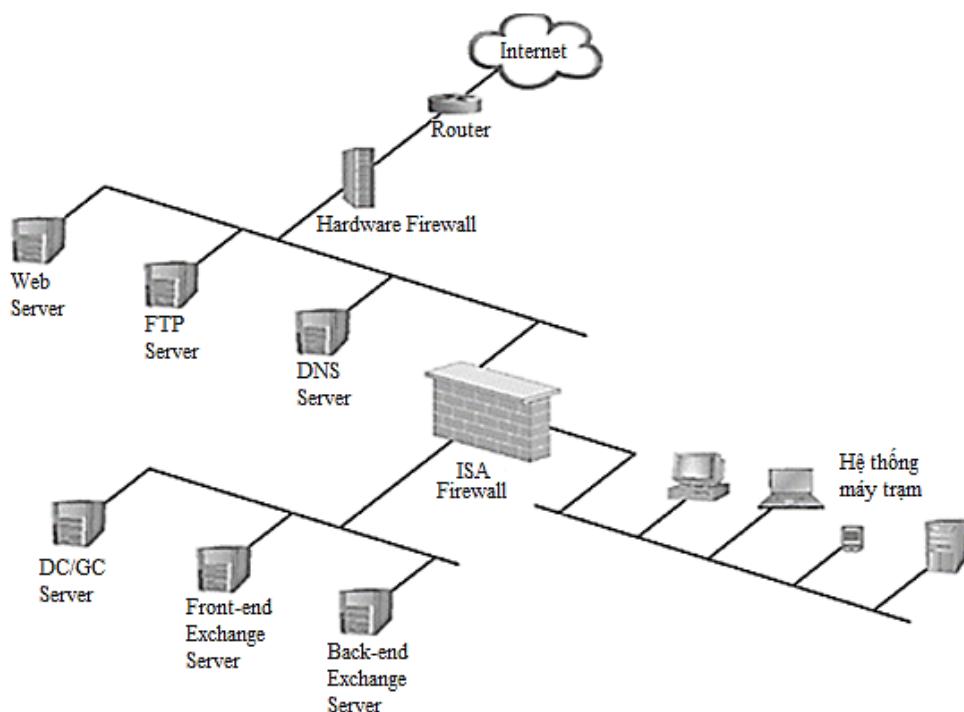
Hình 4.16 biểu diễn sơ đồ mạng trong đó tường lửa được sử dụng để bảo vệ các máy chủ dịch vụ email Microsoft Exchange. Tất cả các kết nối đến hệ thống máy chủ email đều phải đi qua tường lửa. Hình 4.17 sơ đồ mạng sử dụng 2 tường lửa để bảo vệ, trong đó một tường lửa phần cứng (Hardware Firewall) được sử dụng tại cổng kết nối Internet để bảo vệ các máy chủ dịch vụ (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 đối tượng bảo vệ khác nhau.



Hình 4.15. Tường lửa bảo vệ mạng gia đình hoặc văn phòng nhỏ



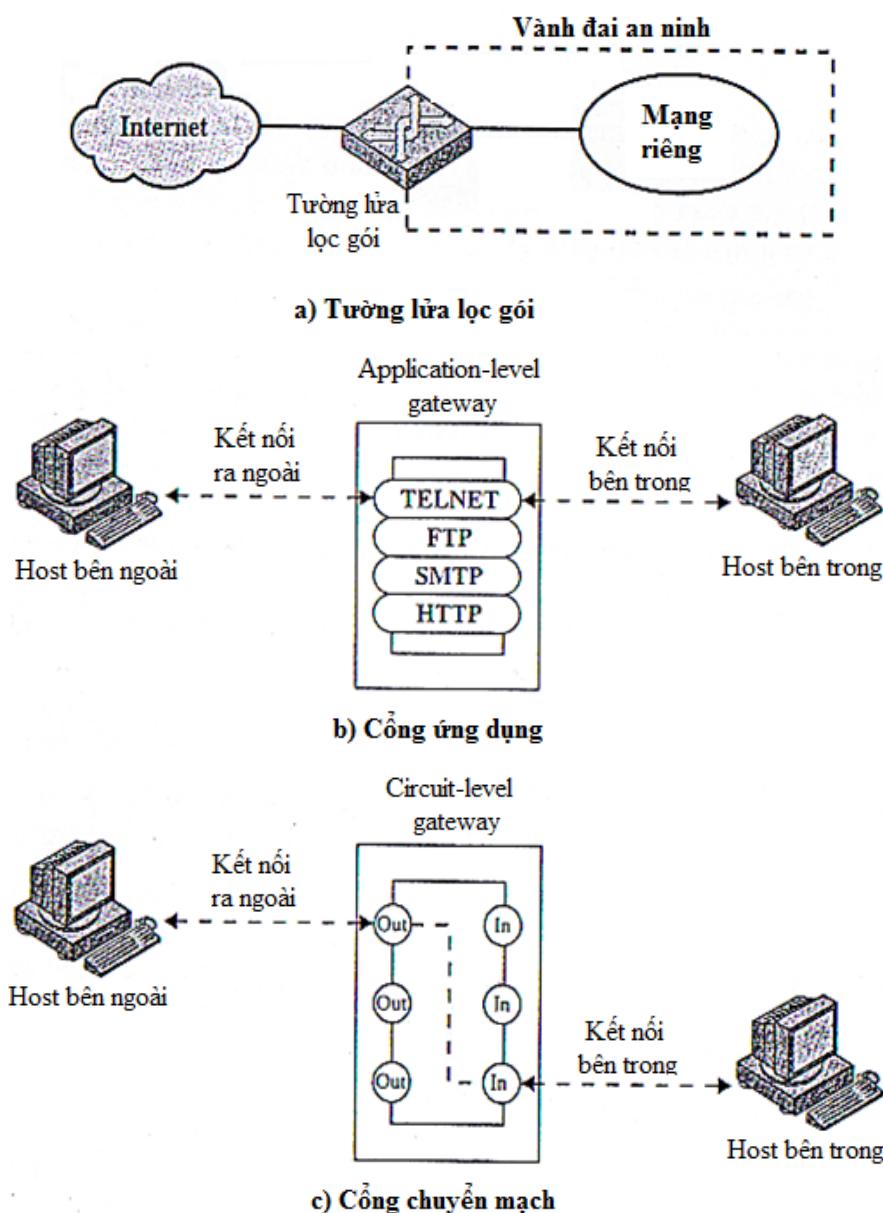
Hình 4.16. Tường lửa bảo vệ các máy chủ dịch vụ



Hình 4.17. Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm

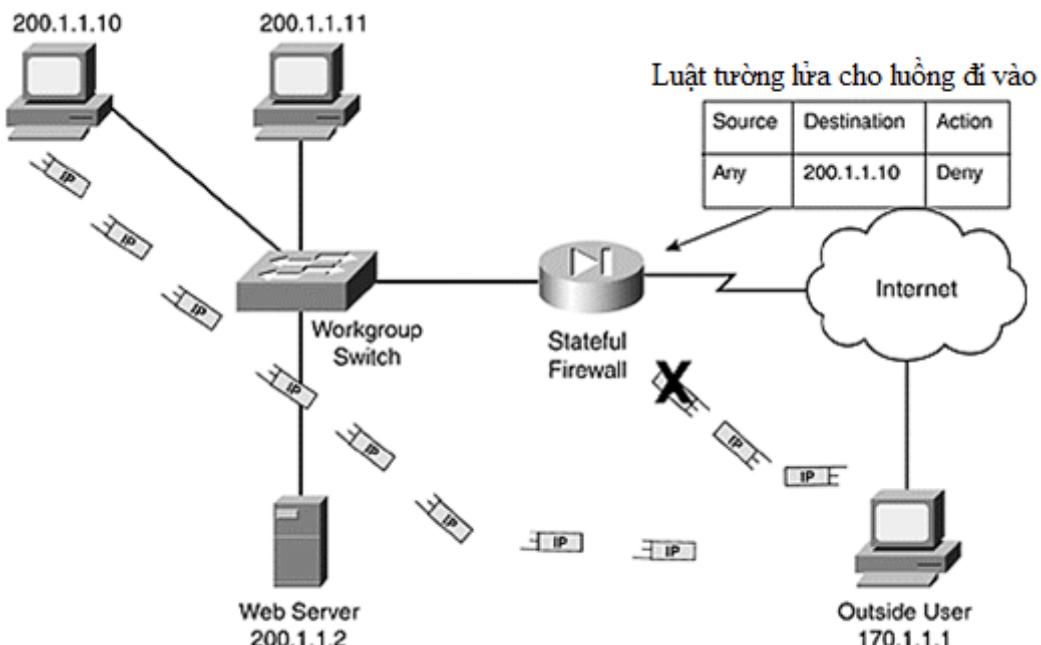
4.3.2. Các loại tường lửa

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), 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, hoặc hồi đáp (request/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 4.18 minh họa mô hình tường lửa lọc gói (a), cổng ứng dụng (b) và cổng chuyển mạch (c).



Hình 4.18. Mô hình tường lửa lọc gói (a), Cổng ứng dụng (b) và Cổng chuyển mạch (c)

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 4.19 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 4.19. Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động

4.3.3. 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. Cụ thể:

- 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 các thư rác, hoặc hạn chế truy cập đến một bộ phận thông tin của máy chủ web.

4.3.4. Các hạn chế của tường lửa

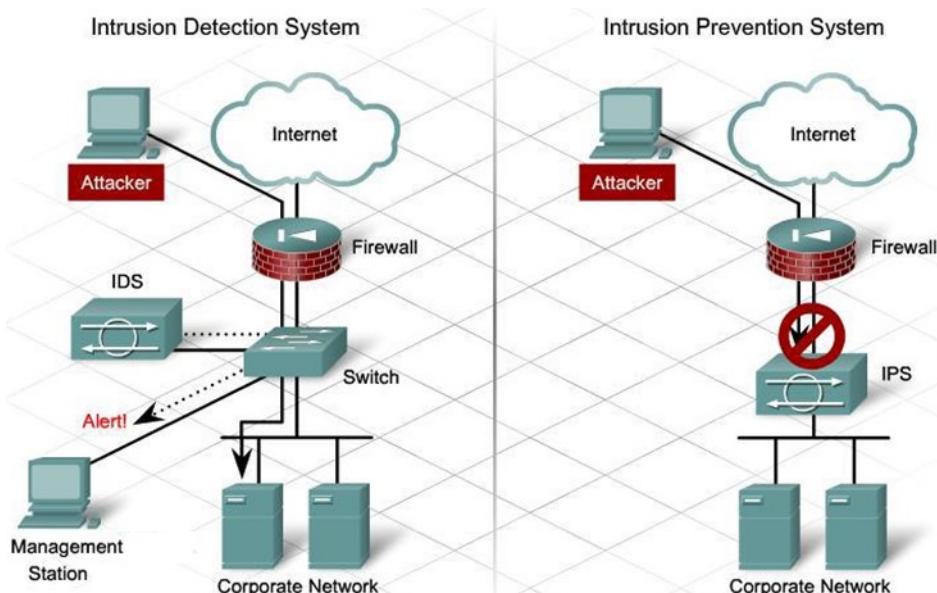
Mặc dù tường lửa được sử dụng rộng rãi để bảo vệ mạng nội bộ khỏi các cuộc tấn công, xâm nhập, nhưng cũng như hầu hết các kỹ thuật và công cụ đảm bảo an toàn khác, tường lửa cũng có những hạn chế. Các hạn chế của tường lửa gồm:

- 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 tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng bảo mật của các phần mềm.
- Không thể chống lại các hiểm họa từ bên trong, như 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 (thường ở dạng nén hoặc mã hóa).

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

4.4.1. Giới thiệu

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 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 đặt trước hoặc sau tường lửa trong mô hình mạng, tùy theo mục đích sử dụng. Hình 4.20 cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ switch phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa.



Hình 4.20. Vị trí các hệ thống IDS và IPS trong sơ đồ mạng

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

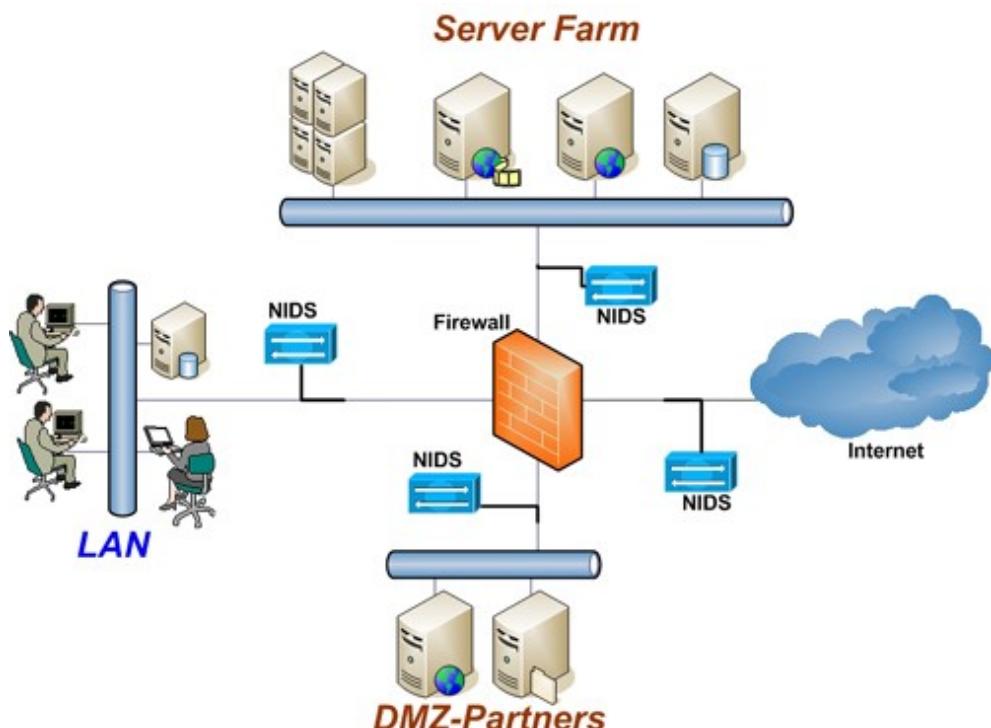
- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập;
- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này;
- Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập;
- Gửi thông báo cho người quản 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 bị phát hiện. 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.

4.4.2. Phân loại

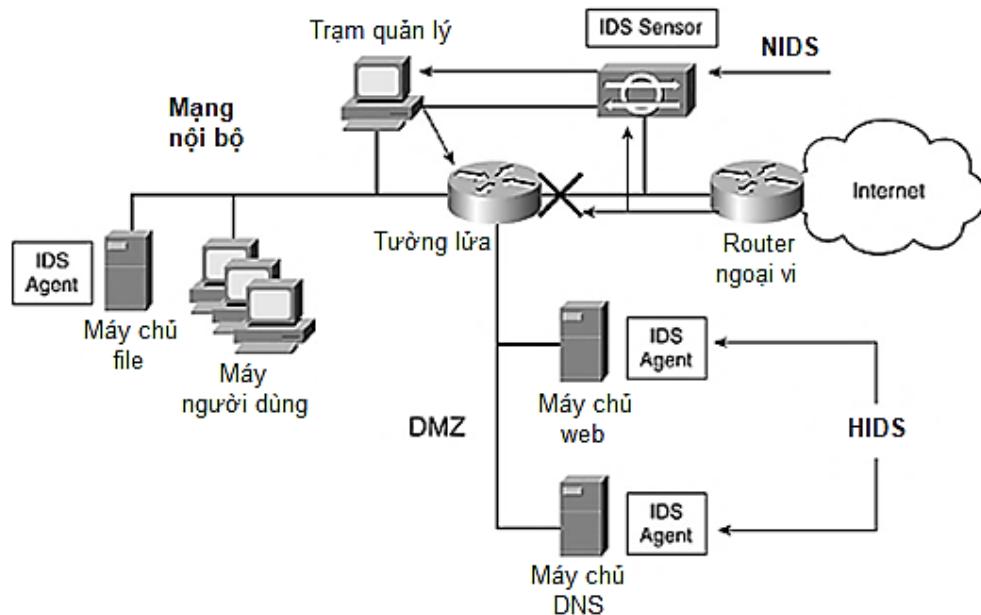
Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu. Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): NIDS phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng. Hình 4.21 biểu diễn một sơ đồ mạng, trong đó các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng. Một số NIDS điển hình như Snort, Suricata...



Hình 4.21. Các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng

- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): HIDS phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó. Hình 4.22 minh họa một sơ đồ mạng, trong đó sử dụng NIDS để giám sát lưu lượng tại cổng mạng và HIDS để giám sát các host thông qua các IDS agent. Một trạm quản lý (Management station) được thiết lập để thu nhập các thông tin từ các NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng. Một trong các HIDS tiêu biểu có thể kể đến là OSSEC.



Hình 4.22. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host

Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính, gồm (1) phát hiện xâm nhập dựa trên chữ ký/dấu hiệu, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection) và (2) phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection). Mục tiếp theo trình bày chi tiết hơn về hai kỹ thuật phát hiện này.

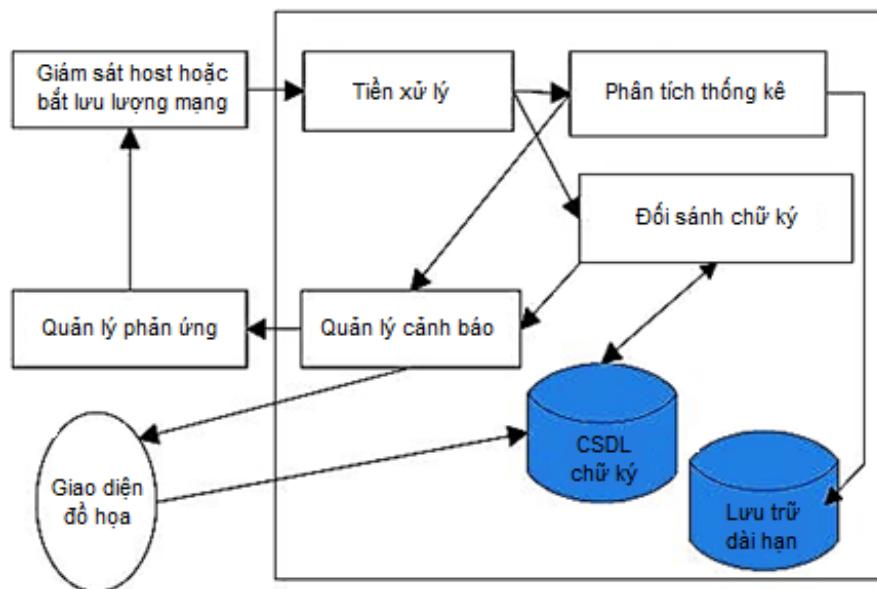
4.4.3. Các kỹ thuật phát hiện xâm nhập

4.4.3.1. Phát hiện xâm nhập dựa trên chữ ký

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 gấp là các luật phát hiện (Detection rule). 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 chữ ký của tấn công, xâm nhập. Hình 4.23 biểu diễn lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký điển hình.

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 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, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu các chữ ký. Hơn

nữa, nó cũng đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.



Hình 4.23. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

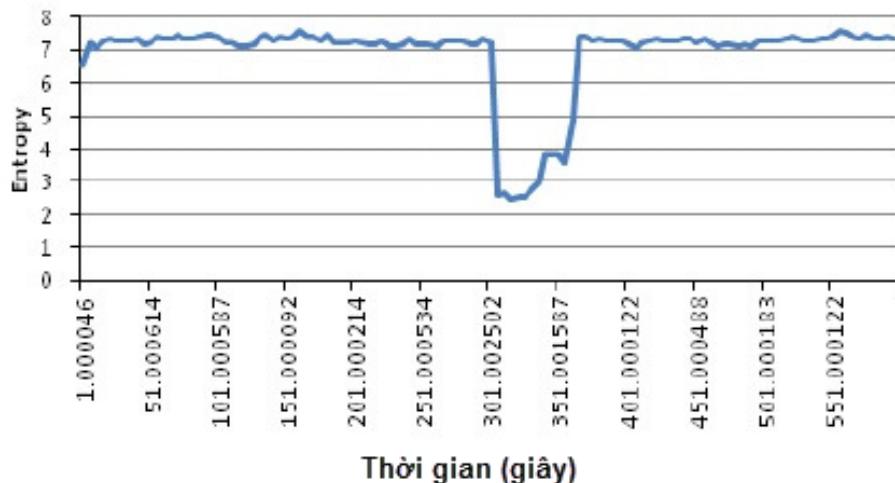
4.4.3.2. Phát hiện xâm nhập dựa trên bất thường

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 gồm 2 giai đoạn: (1) huấn luyện và (2) phát hiện. Trong giai đoạn huấn luyện, hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện này, 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 hệ thống 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.

Hình 4.24 biểu diễn giá trị entropy của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS. Có thể thấy sự khác biệt rõ nét giữa giá trị 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.

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, phương pháp này có tỷ lệ cảnh báo sai tương đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, nó 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.



Hình 4.24. 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)

4.5. Câu hỏi ôn tập

- 1) Nêu khái niệm, các thành phần và mục đích của kiểm soát truy cập.
- 2) Nêu cơ chế hoạt động của mô hình (biện pháp) kiểm soát truy cập tùy chọn (DAC).
- 3) Nêu cơ chế hoạt động của mô hình (biện pháp) kiểm soát truy cập bắt buộc (MAC).
- 4) Nêu cơ chế hoạt động của mô hình (biện pháp) kiểm soát truy cập dựa trên vai trò (RBAC).
- 5) Nêu cơ chế hoạt động của mô hình (biện pháp) kiểm soát truy cập dựa trên luật (Rule-based access control).
- 6) So sánh 2 kỹ thuật thực hiện mô hình kiểm soát truy cập tùy chọn (DAC): ma trận kiểm soát truy cập và danh sách kiểm soát truy cập.
- 7) Mô tả cơ chế hoạt động của mô hình bảo mật đa cấp Bell-LaPadula.
- 8) Mô tả công nghệ kiểm soát truy cập dựa trên mật khẩu.
- 9) 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?
- 10) Tường lửa là gì? Nêu vai trò của tường lửa. Nêu các phương pháp phân loại tường lửa.
- 11) Nêu các kỹ thuật kiểm soát truy cập và các hạn chế của tường lửa.
- 12) 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?
- 13) Nêu các phương pháp phân loại IDS/IPS. Có thể sử dụng kết hợp NIDS và HIDS trong cùng một mạng được không?

- 14) Mô tả và nêu ưu nhược điểm của phương pháp phát hiện xâm nhập dựa trên chữ ký.
- 15) Mô tả phương pháp phát hiện xâm nhập dựa trên bát thường. Nêu ưu nhược điểm của phương pháp này.
- 16) Tại sao phát hiện xâm nhập dựa trên bát thường có khả năng phát hiện các tấn công xâm nhập mới? Tại sao phát hiện xâm nhập dựa trên bát thường thường có tỷ lệ cảnh báo sai cao hơn phát hiện xâm nhập dựa trên chữ ký?

CHƯƠNG 5. 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.

5.1. Quản lý an toàn thông tin

5.1.1. Khái quát về quản lý an toàn thông tin

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:

- Phần cứng (máy chủ, các thiết bị mạng,...);
- Phần 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* (Information security management). 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.

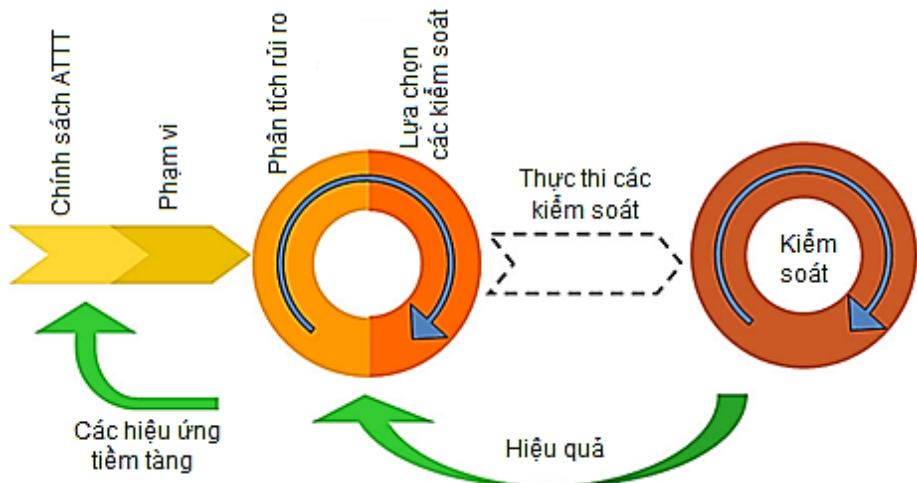
Quản lý an toàn thông tin là một thành phần rất quan trọng trong an toàn thông tin và nó phải trả lời được 3 câu hỏi:

1. Những tài sản nào cần được bảo vệ?
2. Những mối 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 mối đe dọa đó?

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 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 5.1 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.



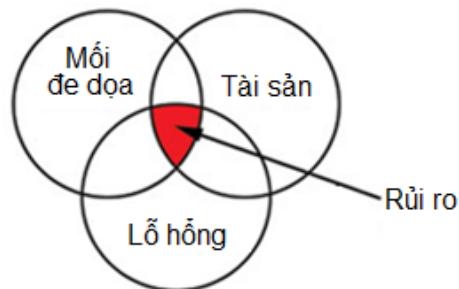
Hình 5.1. Quan hệ giữa các khâu trong quản lý an toàn thông tin

5.1.2. Đánh giá rủi ro an toàn thông tin

5.1.2.1. Giới thiệu

Đánh giá rủi ro an toàn thông tin (Security risk assessment) là một bộ phận quan trọng của vấn đề 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 5.2 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 cần được bảo vệ, (2) Các mối đe dọa đối với các tài sản an toàn thông tin và (3) Các lỗ hổng bảo mật 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 dọa).



Hình 5.2. Mô hình đánh giá rủi ro an toàn thông tin

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.

5.1.2.2. Các phương pháp đánh giá rủi ro

a. Phương pháp đánh giá rủi ro đường cơ sở

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 độ rủi ro 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 với hệ thống công nghệ thông tin có quy mô nhỏ, có nguồn lực hạn chế.

b. Phương pháp không chính thức

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 nhà 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, và 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 là:

- 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 với hệ thống công nghệ thông tin có quy mô nhỏ và vừa, có nguồn lực tương đối hạn chế.

c. Phương pháp phân tích chi tiết rủi ro

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 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 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 là:

- 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.

d. Phương pháp kết hợp

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 các mục tiêu là cung cấp mức bảo vệ hợp lý càng nhanh càng tốt và sau đó 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 việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ 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, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết. Nói chung, phương pháp kết hợp phù hợp các tổ chức với hệ thống công nghệ thông tin quy mô vừa và lớn.

5.1.3. Phân tích chi tiết rủi ro an toàn thông tin

5.1.3.1. 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 được chia thành 9 bước:

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.

5.1.3.2. Nội dung phân tích chi tiết rủi ro

Nội dung cụ thể từng bước của phân tích chi tiết rủi ro an toàn thông tin như sau.

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 (control)

- 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 dùng 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 môi 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.

5.1.4. Thực thi quản lý an toàn thông tin

5.1.4.1. 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 (control) nhằm đảm bảo an toàn thông tin 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): Thực thi các kiểm soát, và nâng cao ý thức và đào tạo an toàn thông tin.
- Thực thi tiếp tục (Implementation follow-up): Bảo trì, kiểm tra hợp chuẩn, quản lý thay đổi và xử lý sự cố.

Kiểm soát (control), đảm bảo an toàn (safeguard), hoặc biện pháp đối phó (countermeasure) là các thuật ngữ có thể được sử dụng tương đương, hoặc tráo đổi cho nhau trong quản lý an toàn thông tin. 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 controls)
- Kiểm soát vận hành (Operational controls)
- Kiểm soát kỹ thuật (Technical controls)
- Kiểm soát hỗ trợ (Supportive controls)
- Kiểm soát ngăn ngừa (Preventive controls)
- Kiểm soát phát hiện và phục hồi (Detection and recovery controls).

5.1.4.2. 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 các 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:

- 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: 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 với 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.

5.1.4.3. Xây dựng kế hoạch đảm bảo an toàn

Kế hoạch đảm bảo an toàn (Security plan) 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. Kế hoạch đảm bảo an toàn nên gồm các thông tin chi tiết sau (theo chuẩn hướng dẫn quản lý rủi ro năm 2002 của NIST):

- 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.

5.1.4.4. Nội dung thực thi quản lý an toàn thông tin

Như đã đề cập trong mục 5.1.4.1, việc thực thi quản lý an toàn thông tin gồm 2 khâu là (1) *thực thi* (Implementation) và (2) *thực thi tiếp tục* (Implementation follow-up). Khâu *thực thi* gồm 2 phần việc là thực thi các kiểm soát, và nâng cao ý thức và đào tạo 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 an toàn 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 cần được xem xét nếu cần thiết. 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 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 pháp 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 tiến trình được sử dụng để 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 cả vấn đề vận hành, tính năng và vấn đề an toàn,... Quản lý cấu hình liên quan đến việc lưu vết các 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.

5.2. Các chuẩn quản lý an toàn thông tin

5.2.1. Giới thiệu

Trong các chuẩn quản lý an toàn thông tin, bộ chuẩn NIST SP 800 của Viện tiêu chuẩn và công nghệ Mỹ 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. Theo đó, bộ chuẩn ISO/IEC 27000:2014 được Việt Nam dịch và chấp thuận nguyên vẹn thành chuẩn TCVN 11238:2015. Trong phạm vi của môn học, mục này giới thiệu khái quát về bộ chuẩn quản lý an toàn thông tin ISO/IEC 27000.

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 17799 được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC) là tiền thân của 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.

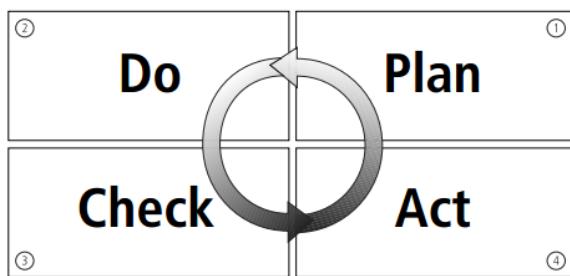
Chuẩn ISO/IEC 27001:2005 chuyên về hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS). Chuẩn này cung cấp các thông tin để thực thi các yêu cầu của ISO/IEC 27002 và cài đặt một hệ thống quản lý an toàn thông tin. Trong việc xây dựng hệ thống ISMS, chuẩn cung cấp các chi tiết cho thực hiện chu kỳ Lập kế hoạch – Thực hiện – Giám sát – Hành động (Plan-Do-Check-Act). 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 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.

Chuẩn ISO/IEC 27005: 2009 chuyên về quản lý rủi ro cho hệ thống quản lý an toàn thông tin. Chuẩn này hỗ trợ ISO/IEC 27001, nhưng nó không đề cập đến phương pháp kiểm soát rủi ro cụ thể.

5.2.2. 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 5.3. Theo đó, chi tiết 4 pha trong chu trình này như sau:



Hình 5.3. Chu trình Plan-Do-Check-Act của ISO/IEC 27001:2005

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 (audits) 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.

5.3. Pháp luật và chính sách an toàn thông tin

5.3.1. Giới thiệu về pháp luật và chính sách an toàn thông tin

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 rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho thông tin, hệ thống và mạng và giảm thiệt hại nếu xảy ra sự cố. Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức an toàn thông tin. Theo đó, họ phải luôn nắm vững môi trường pháp lý hiện tại (các luật và các quy định luật pháp) 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 (Policy - 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 thiêu 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 là 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 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 – cần 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 – thông qua ký văn bản cam kết hoặc tick 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.

5.3.2. 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 Mỹ 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 nước Mỹ 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 và tội phạm mạng 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: 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, gồm:

- Federal Privacy Act, 1974: luật Liên bang Mỹ bảo vệ quyền riêng tư của người dùng;
- Electronic Communications Privacy Act, 1986: luật bảo vệ quyền riêng tư trong các giao tiếp điện tử;
- Health Insurance Portability and Accountability Act, 1996 (HIPAA): 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: điều chỉnh các hoạt động liên quan đến nhà nước của các ngân hàng, bảo hiểm và các hăng an ninh.

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, gồm:

- Economic Espionage Act, 1996: 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 Mỹ, 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)): do Tổ chức Thương mại thế giới WTO chủ trì đàm phán trong giai đoạn 1986–1994;
- Digital Millennium Copyright Act (DMCA): Luật bản quyền số Thiên niên kỷ.

5.3.3. Luật Việt Nam về an toàn thông tin

Luật an toàn thông tin mạng là bộ luật đầu tiên về lĩnh vực an toàn thông được Quốc hội thông qua vào tháng 11 năm 2015 và chính thức có hiệu lực từ ngày 01/7/2016. Tiếp

theo Luật an toàn thông tin mạng, Luật an ninh mạng được Quốc hội thông qua vào ngày 12/6/2018 và chính thức có hiệu lực từ ngày 01/01/2019. Đây là các cơ sở pháp lý rất quan trọng cho việc quản lý các hoạt động liên quan đến an toàn thông tin, an toàn không gian mạng ở Việt Nam. Ngoài hai bộ luật trên, 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 CP "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 CP "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.

5.4. Vấn đề đạo đức an toàn thông tin

5.4.1. Sự cần thiết của 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 liên quan đến an toàn thông tin có thể liên quan đến các thông tin nhạy cảm, như thông tin, hệ thống bí mật quốc gia, 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 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.

5.4.2. 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 luật sư, bác sĩ và các 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) 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 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, đưa ra một số quy tắc và khuyến nghị về những việc không được làm cho các thành viên và các nhân viên của các tổ chức hoạt động trong lĩnh vực an toàn thông tin. Ở bình diện quốc tế, Viện đạo đức máy tính, Mỹ 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.

5.4.3. 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 là (1) sự khác biệt về vấn đề đạo đức giữa các nền văn hóa, (2) vấn đề vi phạm bản quyền phần mềm 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 Mỹ và châu Âu.

Vấn đề vi phạm bản quyền phần mềm 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, 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 thiếu các chế tài xử lý vi phạm.

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 phạt nghiêm minh. Các hành vi lạm dụng thường gặp, 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.

5.5. 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 văn tắt các phương pháp tiếp cận đánh giá rủi ro an toàn thông tin.
- 3) Mô tả văn tắt các bước của phân tích chi tiết rủi ro an toàn thông tin.
- 4) Mô tả các loại kiểm soát trong thực thi quản lý an toàn thông tin.
- 5) Mô tả nội dung thực thi quản lý an toàn thông tin.
- 6) Mô tả văn tắt các chuẩn ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 và ISO/IEC 27005.
- 7) Mô tả chu trình Plan-Do-Check-Act của chuẩn ISO/IEC 27001.
- 8) Phân biệt pháp luật và chính sách. Nêu các yêu cầu của chính sách có thể được áp dụng hiệu quả.
- 9) Mô tả văn tắt các văn bản luật có liên quan đến an toàn thông tin của Việt Nam.
- 10) 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 (Mỹ).

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 11.2021.
- [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 11.2021.
- [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 11.2021.
- [6] US National Vulnerability Database, <https://nvd.nist.gov>, truy cập tháng 11.2021.
- [7] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Fifth Printing, August 2001.
- [8] Bruce Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, 1996.
- [9] Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. New York: John Wiley and Sons.
- [10] Webster's Online Dictionary, <http://www.websters-online-dictionary.org>, truy cập tháng 11.2021.
- [11] The Free Online Dictionary of Computing, <http://foldoc.org>, truy cập tháng 11.2021.
- [12] Eric Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Elsevier, USA, 2013.