

Network Security



Ha Van Thao

Faculty of Maths & CS

College of Science

lvthao@mathdep.hcmuns.edu.vn

+84913742791



Nội dung

- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security
- Internet standards and RFCs

Attacks, Services and Mechanisms

- **Security Attack – Tấn công bảo mật:** Hành động nhằm tiết lộ bí mật thông tin.
- **Security Mechanism – Kỹ thuật bảo mật:** Kỹ thuật được thiết kế để phát hiện, ngăn ngừa, hay phục hồi sau một tấn công bảo mật.
- **Security Service – Dịch vụ bảo mật:** Dịch vụ nhằm nâng cao tính bảo mật của hệ thống xử lý dữ liệu và vận chuyển thông tin. Dịch vụ bảo mật sử dụng một hay nhiều kỹ thuật bảo mật.

Security Attacks

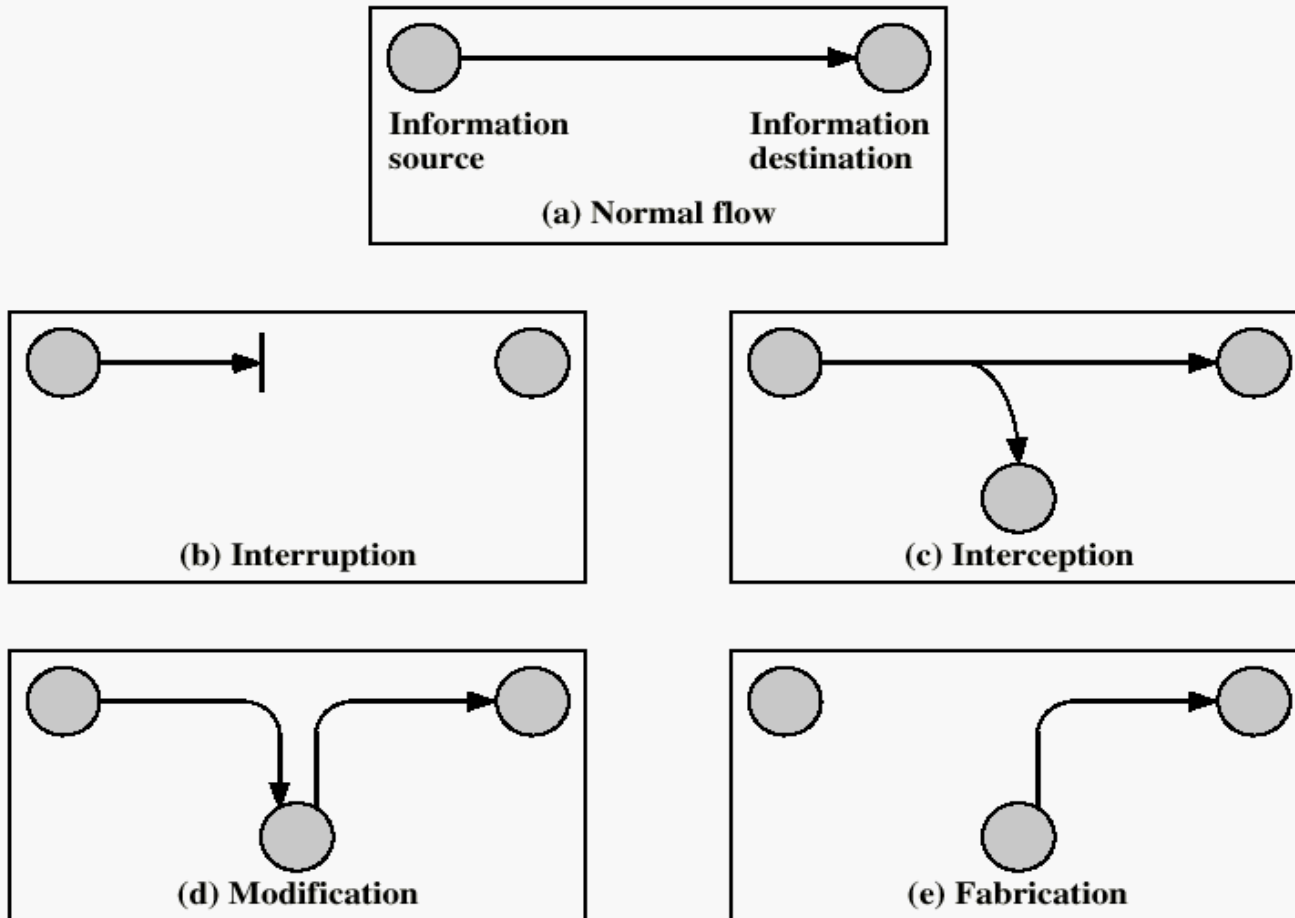
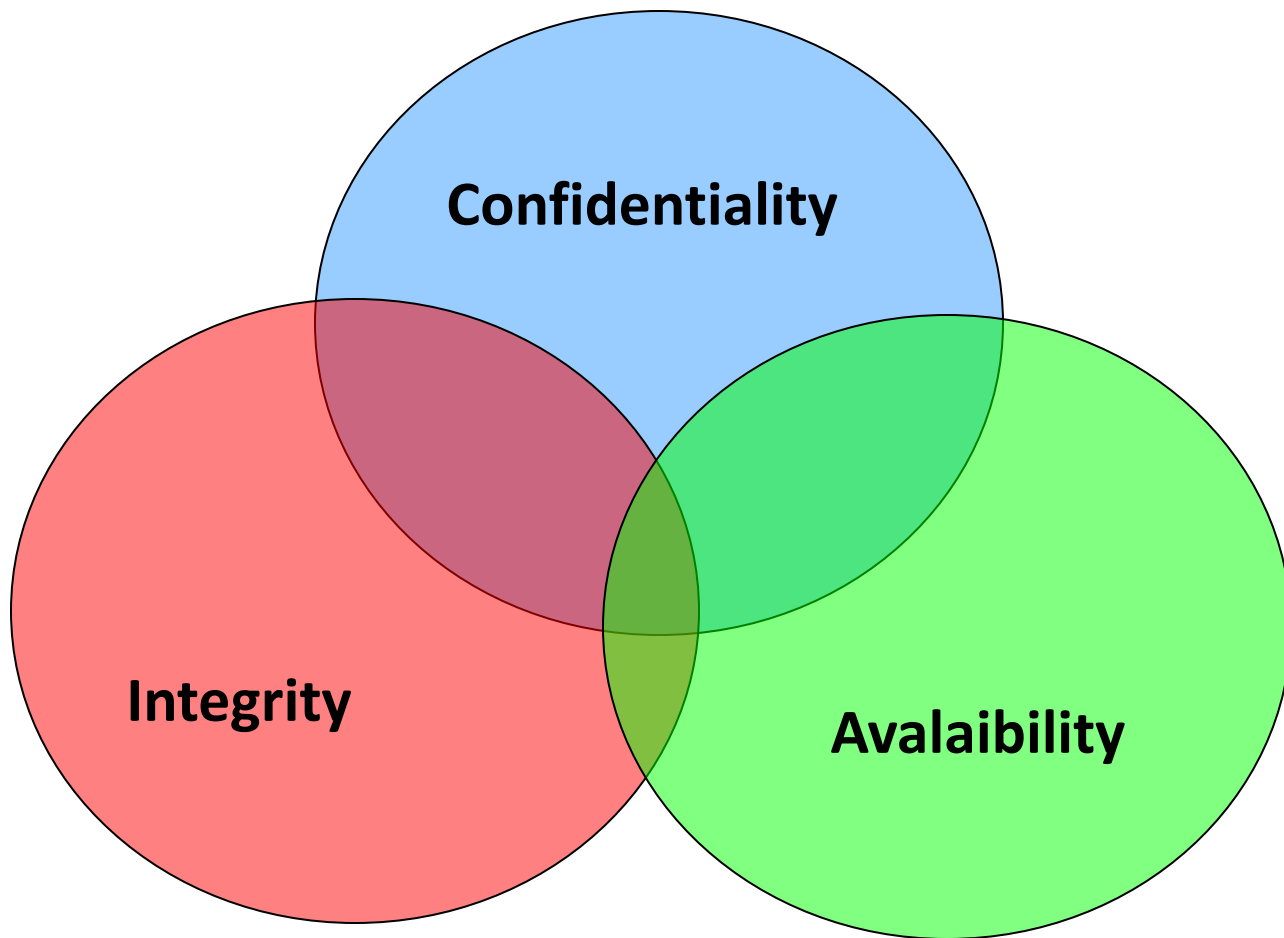


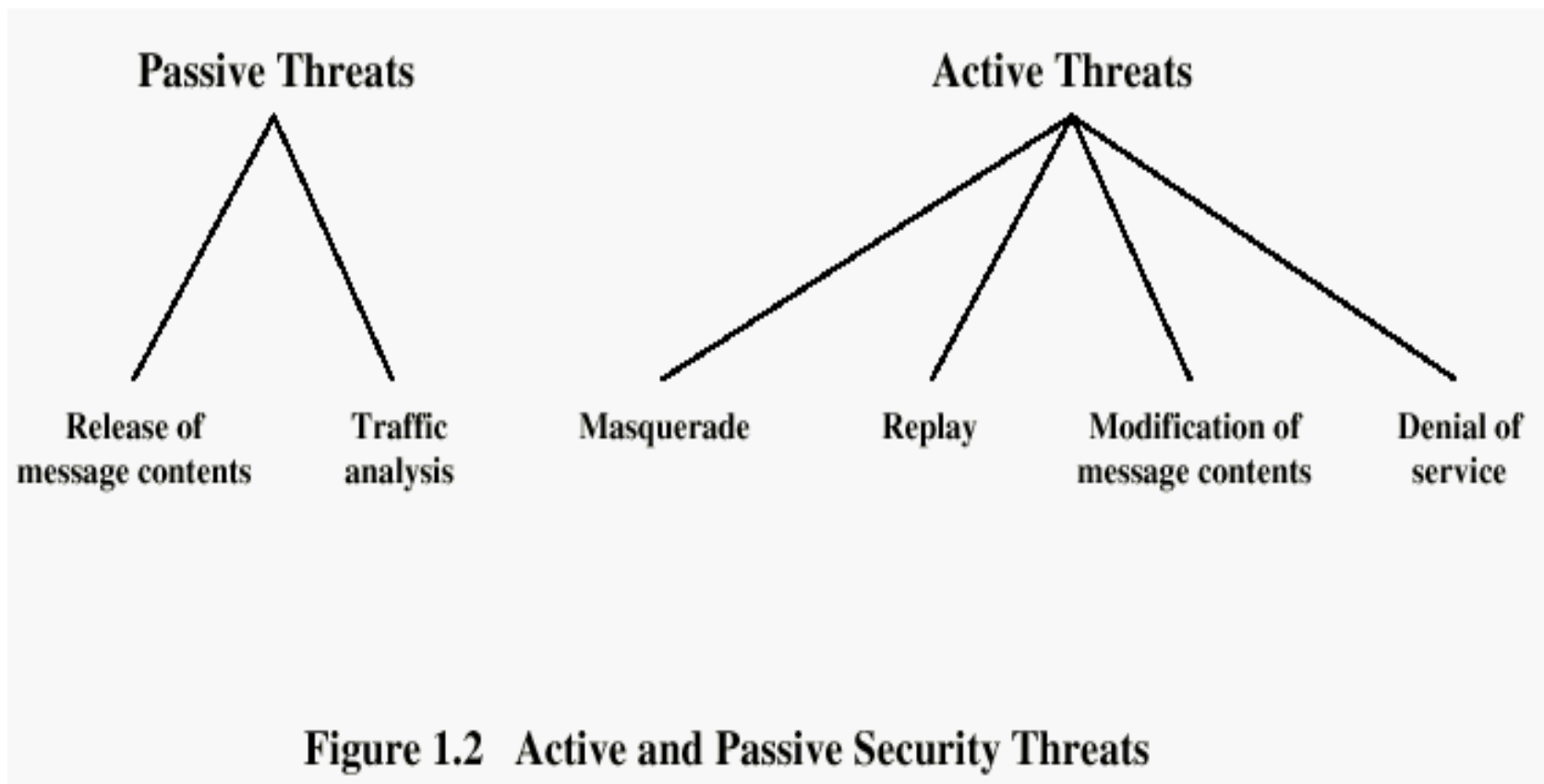
Figure 1.1 Security Threats

Security Attacks

- **Interruption:** Tấn công vào availability – Sự khả dụng của dịch vụ
- **Interception:** Tấn công vào confidentiality – Thông tin không bị tiết lộ
- **Modification:** Tấn công vào integrity – Sự bảo toàn của thông tin, không bị thay đổi
- **Fabrication:** Tấn công vào authenticity – Xác thực

Security Goals





Security Services

- Confidentiality (bí mật)
- Authentication (xác thực người gửi hay tạo dữ liệu)
- Integrity (không bị thay đổi)
- Non-repudiation (xác thực người gửi và đảm bảo nhận được thông điệp)
- Access control (ngăn ngừa sử dụng sai tài nguyên)
- Availability (có thể truy cập và sử dụng được)
 - Tấn công từ chối dịch vụ - DoS
 - Virus xóa tập tin

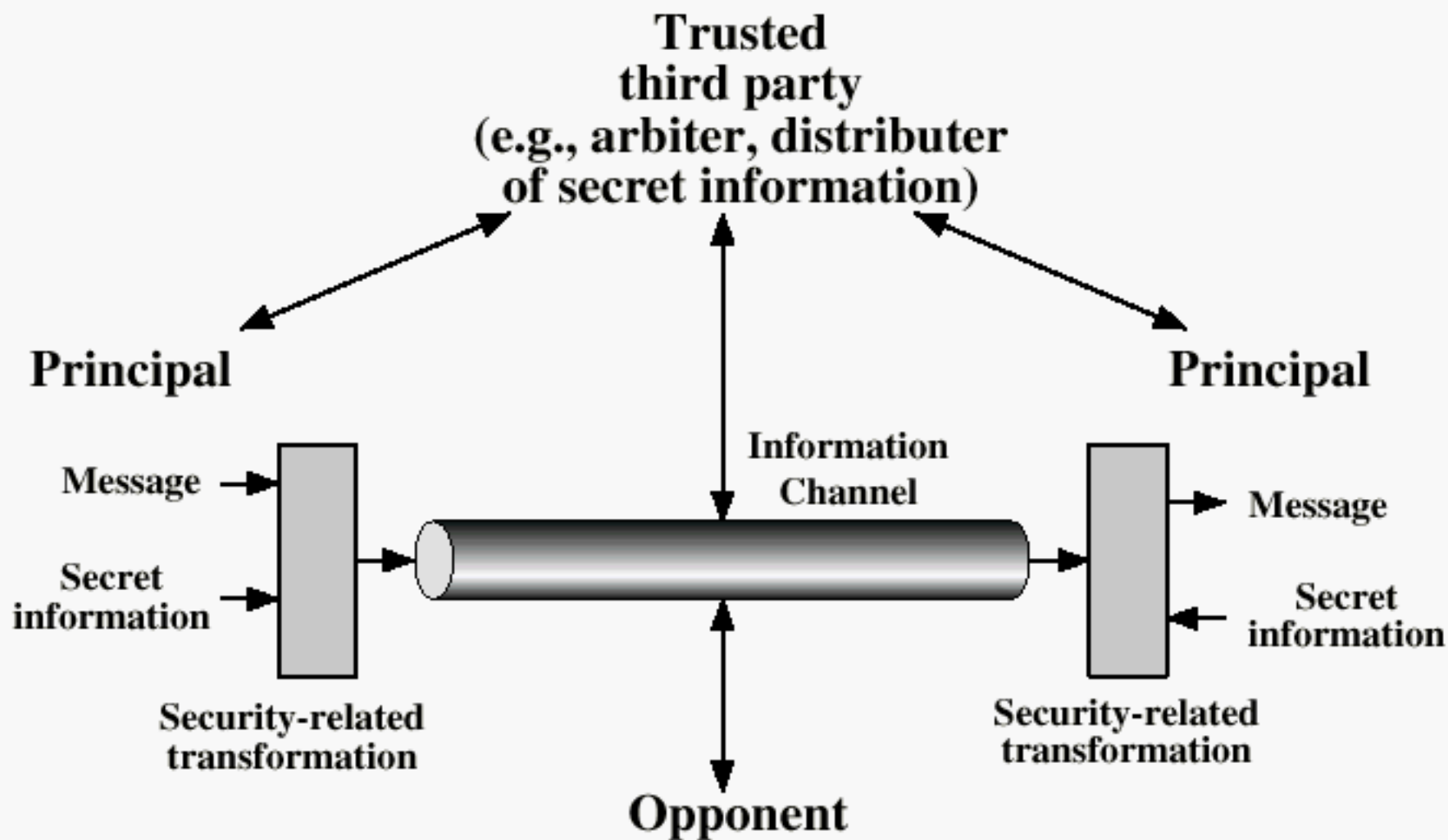


Figure 1.3 Model for Network Security

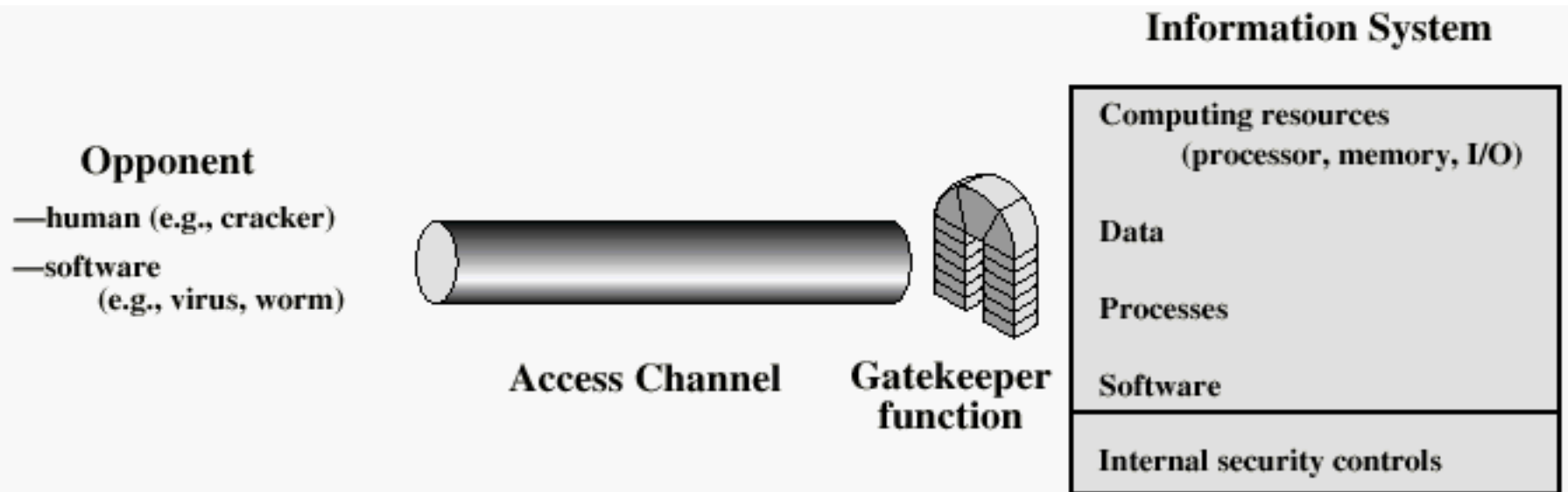


Figure 1.4 Network Access Security Model

Methods of Defense

- Encryption – Mã hóa
- Software Controls – Điều khiển bằng phần mềm (giới hạn truy cập cơ sở dữ liệu, hệ điều hành, bảo vệ người dùng khỏi các người dùng khác)
- Hardware Controls – Điều khiển bằng phần cứng (smartcard – thẻ thông minh)
- Policies – Chính sách (thay đổi thường xuyên mật khẩu)
- Physical Controls – Điều khiển bằng vật lí

Internet standards and RFCs

Các chuẩn Internet và RFC

- Các tổ chức Internet
 - Internet Architecture Board (IAB)
 - Internet Engineering Task Force (IETF)
 - Internet Engineering Steering Group (IESG)

Internet RFC Publication Process

Qui trình xuất bản chuẩn Internet

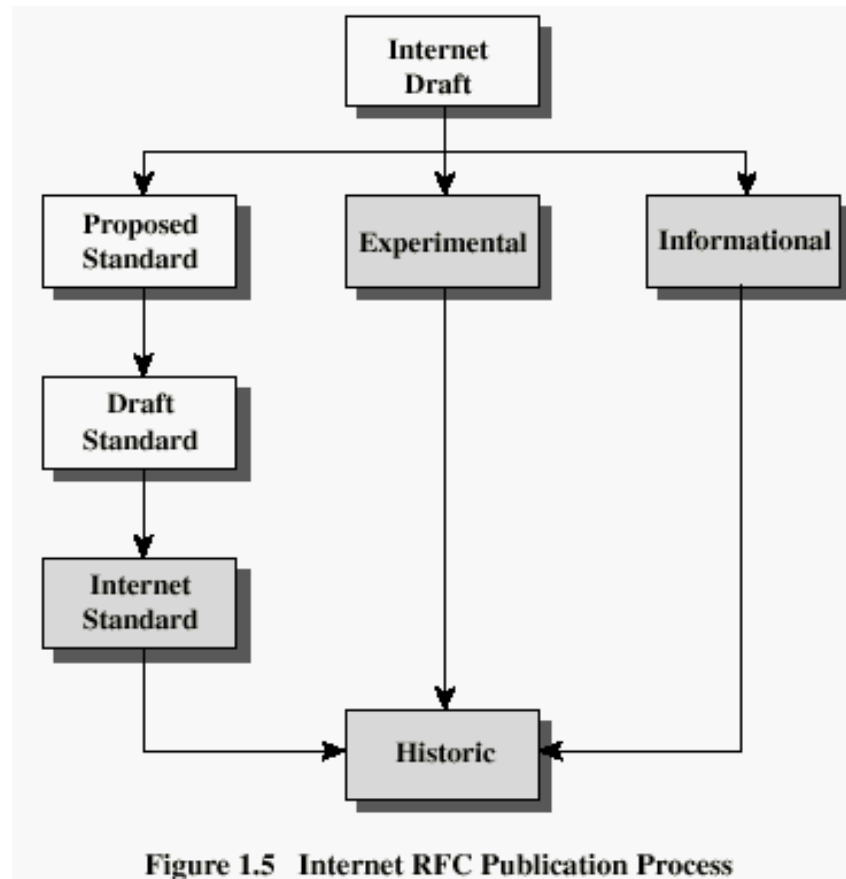


Figure 1.5 Internet RFC Publication Process

Tài liệu tham khảo

- Pfleeger, C. *Security in Computing*. Prentice Hall, 1997.
- Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001.