

NỘI DUNG

Chương 1: Các hiểm họa đối với an toàn thương mại điện tử.....	4
1.1 Giới thiệu	4
1.2 Các hiểm họa đối với sở hữu trí tuệ	7
1.3 Các hiểm họa đối với thương mại điện tử	8
Chương 2: Thực thi an toàn cho thương mại điện tử.....	20
2.1 Bảo vệ các tài sản thương mại điện tử.....	20
2.2 Bảo vệ sở hữu trí tuệ.....	21
2.3 Bảo vệ các máy khách.....	22
2.4 Bảo vệ các kênh thương mại điện tử	27
2.5 Đảm bảo tính toàn vẹn giao dịch	36
2.6 Bảo vệ máy chủ thương mại.....	39
2.7 Tóm tắt.....	41
Chương 3: Một số kỹ thuật an toàn áp dụng cho thương mại điện	43
3.1 Mật mã đối xứng.....	43
3.2 Mật mã khoá công khai.....	45
3.3 Xác thực thông báo và các hàm băm	60
3.4 Chữ ký số	71
Chương 4: Chứng chỉ điện tử	79
4.1 Giới thiệu về các chứng chỉ khoá công khai	79
4.2 Quản lý cặp khoá công khai và khoá riêng	85
4.3 Phát hành các chứng chỉ.....	89
4.4 Phân phối chứng chỉ.....	92
4.5 Khuôn dạng chứng chỉ X.509	94
4.6 Việc thu hồi chứng chỉ.....	107
4.7 CRL theo X.509.....	114
4.8 Cặp khoá và thời hạn hợp lệ của chứng chỉ.....	121
4.9 Chứng thực thông tin uỷ quyền.....	123
4.10 Tóm tắt.....	128
Chương 5: Cơ sở Hạ tầng khoá công khai.....	131
5.1 Các yêu cầu	131
5.2 Các cấu trúc quan hệ của CA	132
5.3 Các chính sách của chứng chỉ X.509	145
5.4 Các ràng buộc tên X.509.....	150
5.5 Tìm các đường dẫn chứng thực và phê chuẩn	152
5.6 Các giao thức quản lý chứng chỉ	154
5.7 Ban hành luật	155
Chữ ký điện tử trong hoạt động thương mại điện tử	156
Phần A: Cơ sở công nghệ cho chữ ký số.....	170
Phần B: Cơ sở pháp lý cho chữ ký số.....	195

CÁC VẤN ĐỀ LÝ THUYẾT

Trong phần này trình bày những vấn đề lý thuyết cơ bản phục vụ cho việc xây dựng các giải pháp an toàn TMĐT sẽ trình bày trong phần 2.