

E-Mail and Mail Gateway Security

Anton J Aylward
System Integrity
Aja@SI.ON.CA
(416) 421-8182

E-Mail and Mail Gateway Security

Objectives

- **Learn**
 - Basic Concepts
 - Key Terms
 - Security Concepts
- **Raise Consciousness**
- **See Demo**

E-Mail and Mail Gateway Security

- Fundamentals and Background
- Design Examples
- Secure Messaging

The Foundations of Information Security

- Confidentiality
- Integrity
- Availability
- Authentication
- Auditability

E-Mail and Mail Gateway Security

- **Fundamentals and Background**
- Design Examples
- Secure Messaging

E-Mail Fundamentals

Analogy with Physical Mail

- Envelope and Contents
- Post Offices
- Franking
- Postcards vs Sealed letters
- Signatures
- Guarantee Delivery or Return to Sender
- Confirm Delivery
- Proof of Delivery

E-Mail Fundamentals

**This is NOT
Rocket
Science**

E-Mail Terminology

TCP/IP - The Internet's Connection Protocol

SMTP - Simple Mail Transfer Protocol

POP - Post Office Protocol, Client/Server

Envelope - Contains Address Information

MUA - Mail User Agent, User's Interface

MTA - Mail Transfer Agent, The Postman

E-Mail Fundamentals

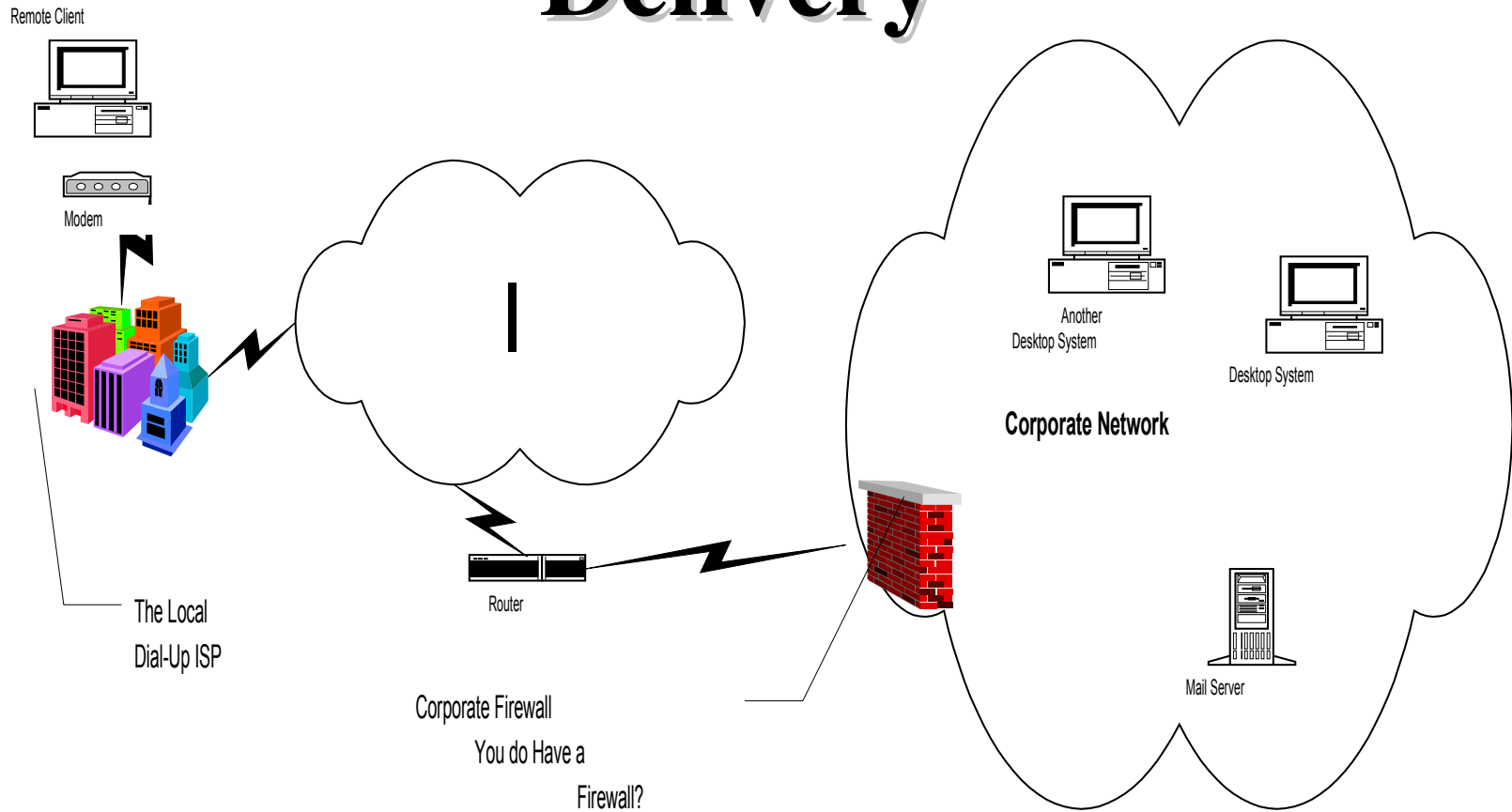
Email Isn't Just Mail Any More

- Mail of Messaging ?
- Desktop or Transaction ?
- User or Application ?
- Mailbox or Process ?

E-Mail Fundamentals

- **Low bandwidth method of Messaging**
- “Real Time” ??
- **Guarenteed Delivery ??**
- **Pre-Delivery Processing**
- **Not a Mailbox Processing**

E-Mail Fundamentals - Delivery



E-Mail Fundamentals - Delivery

Remote Client

- Is a Mail User Interface (MUI)
- Downloads from ISP using POP
- Uploads to ISP using SMTP

E-Mail Fundamentals - Delivery

Remote Client - Examples

- Eudora
- Pegasus
- Netscape Mail

E-Mail Fundamentals - Delivery

Relaying E-Mail

- Mail Transfer Agents - MTA
- Store and Forward
- Routing issues & DNS

E-Mail Fundamentals - Delivery

Acceptance

- MTA At Destination Host
- “Internal” Knowledge of Corporate LAN
- Deliver or Bounce
- Aliases
- Other Processing

E-Mail Fundamentals - Delivery

Storage

- Is it a Mailbox or a Database?
- Second Stage Delivery
- “Real names”
- Autoresponders
 - Vacation
 - Information
 - FTP-by-Mail

E-Mail Fundamentals

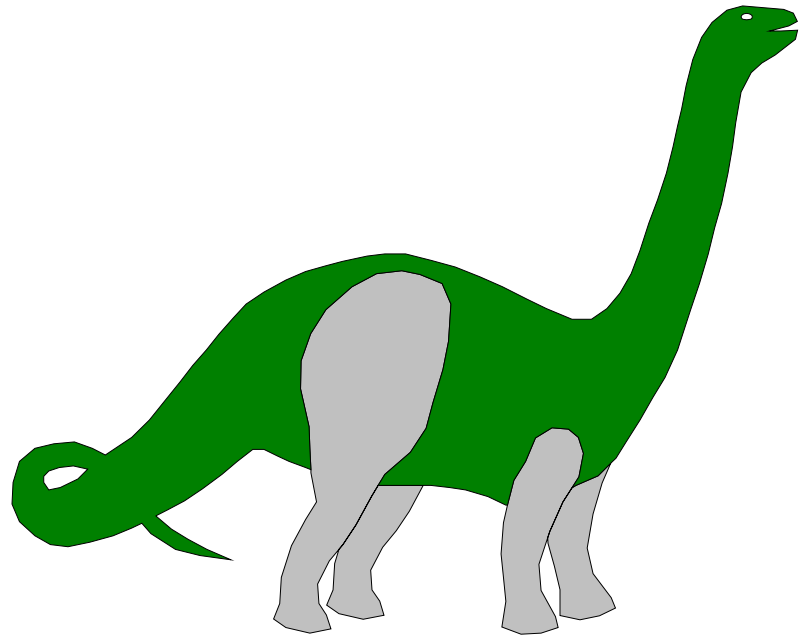
Mail Transfer Agent

- Sendmail
 - Monolithic
 - Configuration
 - High Privileges
 - History of Bugs

=====

POOR SECURITY

- Legal Issues



E-Mail Fundamentals

Other Mail Transfer Agents

- **qmail**
 - Designed for Security & Reliability
 - Dan Bernstein
 - Easy to Configure
 - Only One File
 - Low Privileges
 - Modern Design & Architecture
 - Modular - each part does only one thing
 - Legal Issues

E-Mail Fundamentals



Pause for Questions

E-Mail and Mail Gateway Security

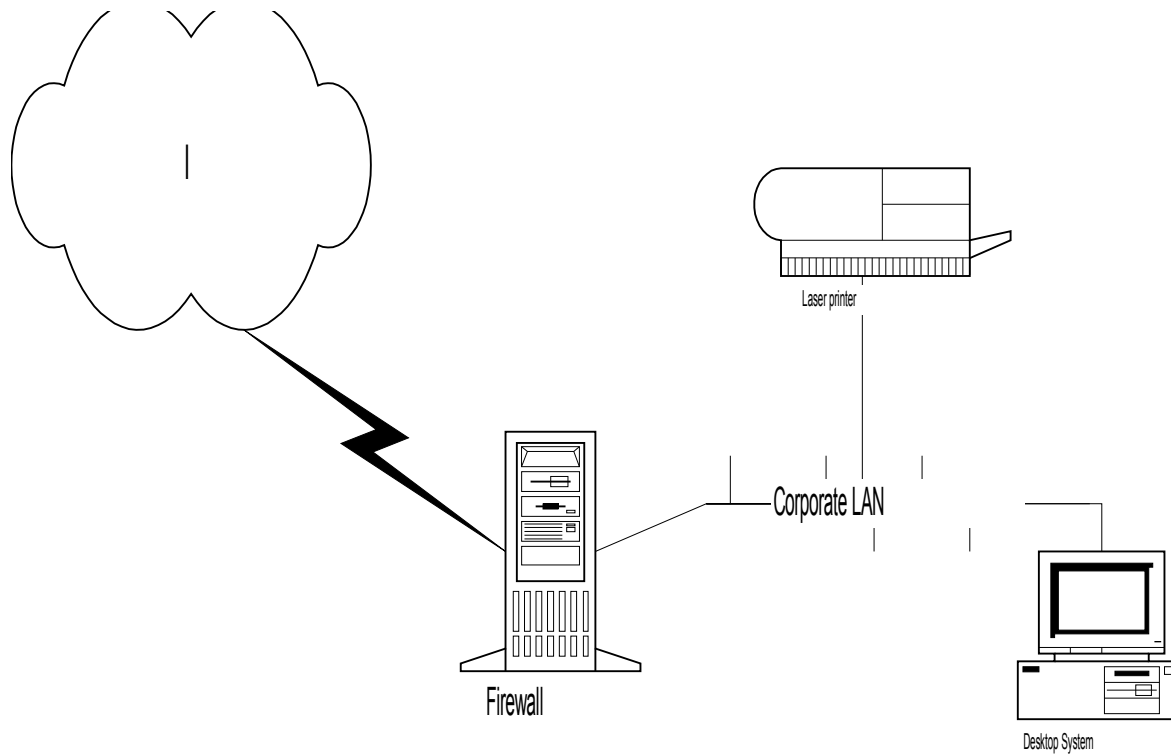
- Fundamentals and Background
- **Design Examples**
- Secure Messaging

Design Examples

AGENDA

- The Myth of the Firewall
 - What it Isn't
 - Perimeter
 - Policy
- An Example Gateway
 - Firewall Components
 - Mail Handling

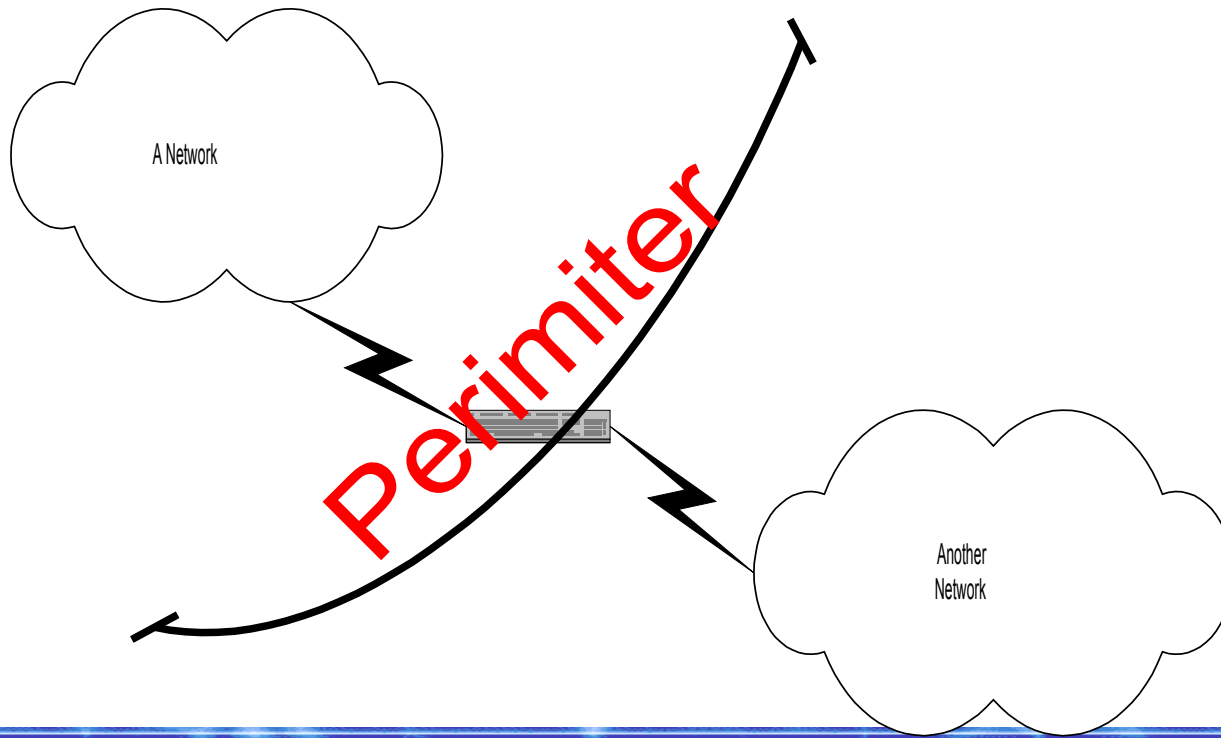
The Myth of The Firewall



The Myth of The Firewall

- You can't buy it in a box ready built
 - Despite what salesmen tell you
- Its not a Firewall, its a **Perimeter Protection Policy Enforcement Mechanism**
- If you don't have Policy
- You're working blind
- If you don't define the Perimeter
- You can't defend it

The Myth of The Firewall

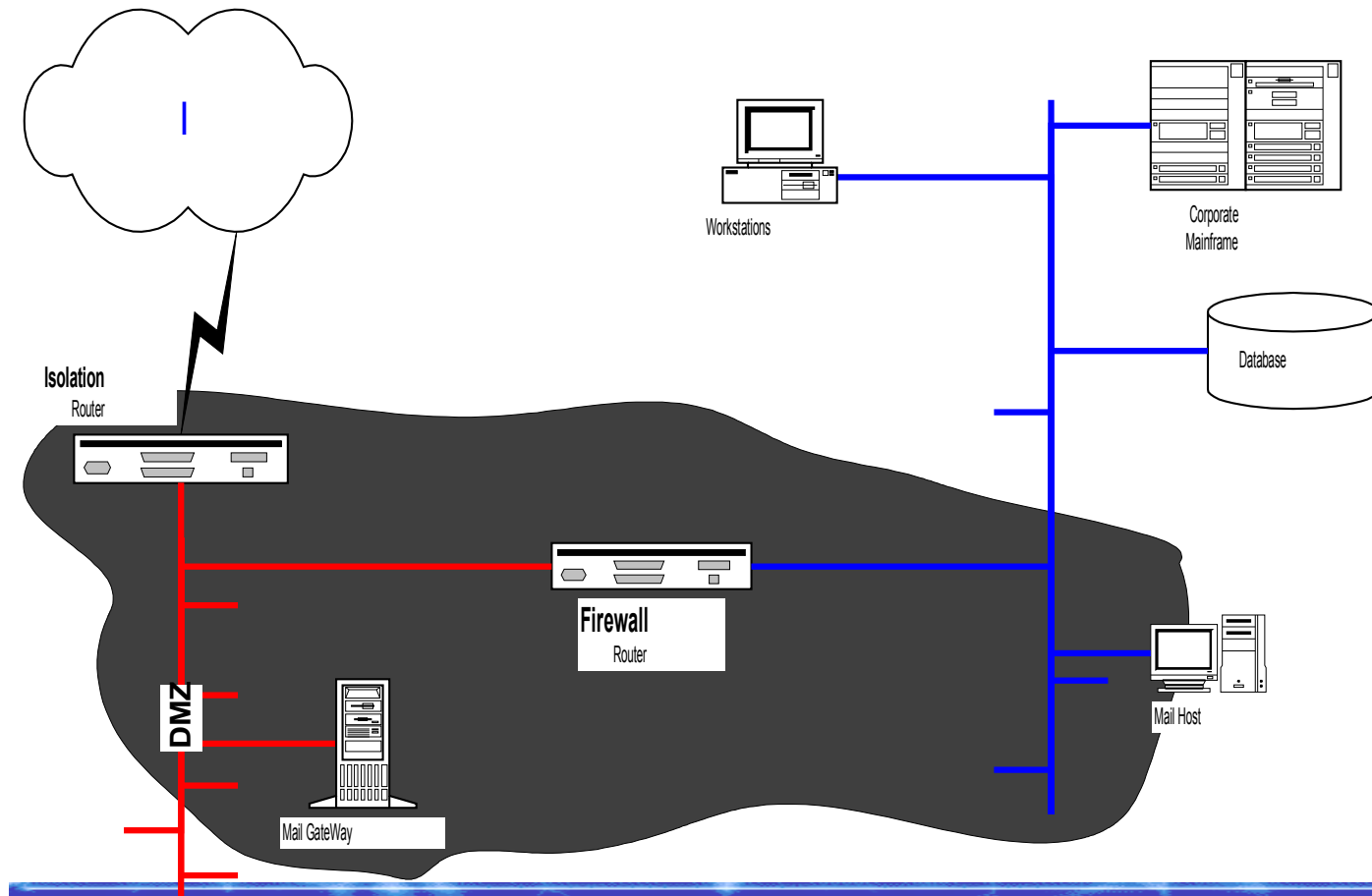


The Myth of The Firewall

Where to Put the Firewall

- At the Single Point of Access to the Internet
- Internally?
 - Do you want the guys in R&D to access Payroll?
 - The Executive Suite
 - Different policies in different places

Design Example - Real System



Design Example - Real System

Security Benefits

- Isolation
- Failure Resistant
- Layered Protection
- Separation of Duties/Functions
- Least Privilege
- Manual Operations

Design Example - Real System

Isolation Router Filters

- Only permit incoming SMTP to Mailgate
- Only Permit outgoing SMTP from Mailgate
- Deny ALL traffic to and from internal network

Design Example - Real System

Mail Gateway (Bastion)

- One of the of PROXY servers in the DMZ
- SMTP is a self-proxying protocol
- Spooling
- Anti-Spamming/Anti-Forwarding
- Content Filtering? Macro Virus?
- Single or Double Homed ?

Design Example - Real System

Firewall Router Filters

- Only permit incoming SMTP to MailHost from MailGate
- Only Permit outgoing SMTP to Mailgate from MailHost
- Deny ALL traffic to and from the Internet

Design Example - Real System

Internal Mail Host

- Handles Purely INTERNAL Mail
- Enforces access policy
- Translates internal names to external

Design Examples



**Pause for
Questions**

E-Mail and Mail Gateway Security

- Fundamentals and Background
- Design Examples
- **Secure Messaging**

Secure Messaging

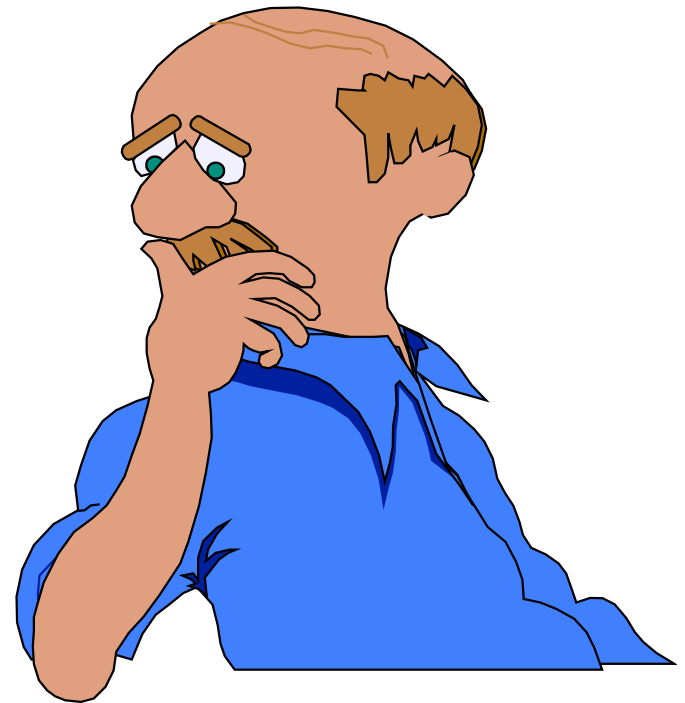
Main Areas of Exposure:

- Crossing Insecure Networks
 - Store and Forward Protocols
 - Snooping
- Storing on Unsecured Servers
 - Poor Host Security
 - Store and Forward servers
 - Unsecured Mailbox

Secure Messaging

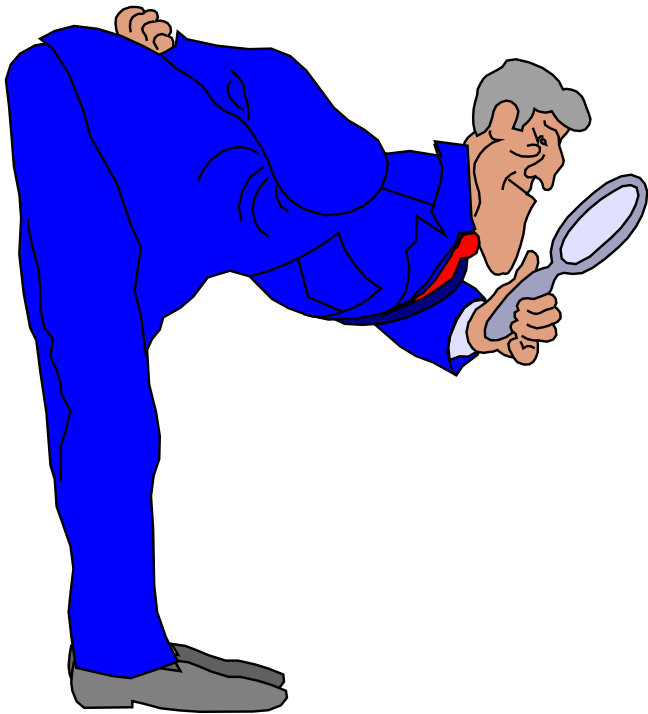
What do we mean by Security?

- Is privacy enough?
- If not then what?
- Is privacy necessary?
- If not then when?



Secure Messaging

Privacy?



When does not it
matter if someone
reads your mail ?

Secure Messaging

Privacy?



When does not it matter if someone alters your mail ?

Secure Messaging

Authentication?



Can you prove you
did or didn't send
that piece of mail?

Secure Messaging

Cryptographic Solutions

- Privacy
 - Encrypt the message body
- Integrity
 - Cryptographic checksum
- Authentication
 - Cryptographic Signature

Secure Messaging

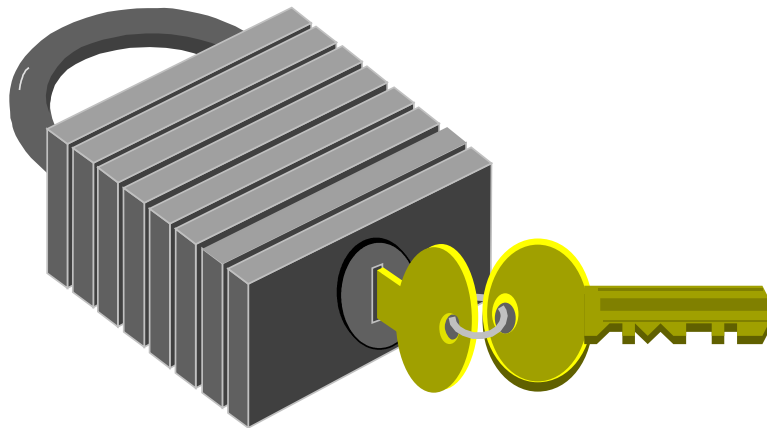
Cryptographic Solutions

- Private Key Cryptography
 - Pros & Cons
- Public Key Cryptography
 - Mostly Pros
 - Other Benefits

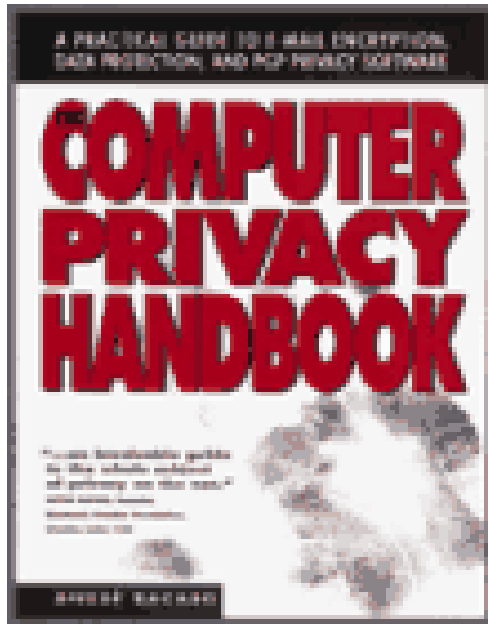
Secure Messaging

Public Key Cryptographic Solutions

- Who Creates, Owns and Manages the keys?



Secure Messaging

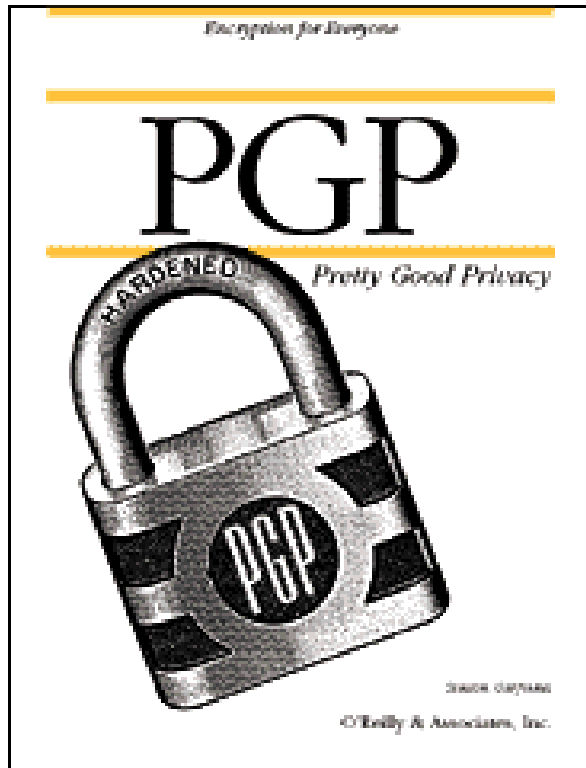


The Computer Privacy Handbook :
A Practical Guide to E-Mail
Encryption, Data Protection, and
PGP Privacy Software

by Andre Bacard

List: \$24.95 ISBN: 1566091713

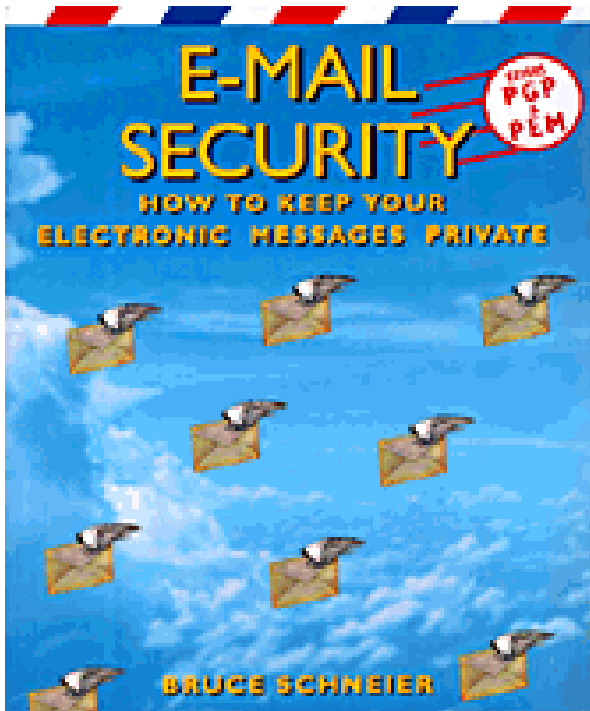
Secure Messaging



PGP: Pretty Good Privacy
by List: \$29.95
O'Reilly <http://www.ora.com>



Secure Messaging



E-Mail Security

by Bruce Schneier

John Wiley & Sons

<http://counterpane.com>

Secure Messaging

Secure Mail Techniques

- PEM
 - Privacy Enhanced Mail
- PGP
 - Pretty Good Privacy

Secure Messaging

Privacy Enhanced Mail

- (Draft?) Internet Standard
- Designed to work with existing systems
- Uses X.509 certificates

Secure Messaging

Pretty Good Privacy

- Written by Philip Zimmermann, June 1991
- An Implementation not a ‘standard’
- Now free of legal problems
- Used by CERT & Many Others

Secure Messaging - 5.0

- New algorithms for public key & conventional encryption.
- The Diffie-Hellman key exchange key size limit is larger than the old RSA limit
- New SHA1 hash function better than MD5, so signatures are more secure
- Backward Compatible

Secure Messaging - PGP 5.0

- Passport or Driver's Licence?
- Trust Relationships
 - Decentralised Authority
 - Who Do You Trust?
 - Degree of Separation
 - Marginal Trust

Secure Messaging

Demonstration of PGP With Eudora Follows

E-Mail and Mail Gateway Security

Thank you for
Attending