

# Security, Part 2

Mark Hendricks and Ron Roeber

October 17, 2002

## Preview of Security Topics:

- ! Definitions
- ! Commerce
- ! Encryption - SSH, SSL -Transmission of Data
- ! Passwords, Authentication & Authorization

## Why are we here?

- ! To learn about security
- ! To justify security to peers
- ! To learn how to manage security

## The Nature of Security

- ! Security is a process
- ! Security starts at the beginning
- ! Security is never finished
- ! Security is a state of mind

## Fundamental Uncertainty Principle

You cannot know that your site (computer) is secure.

*Jim Dennis, Linux World Expo, 3/1/99*

## Encryption

Encryption - scrambling or coding data in a way that only the authorized recipient can unscramble or read it

## Commerce/E-commerce

- ! Commerce - conducting financial transactions
- ! E-commerce - conducting financial transactions by electronic means

## Pillars of Security

- ! Authentication
  - " Who
- ! Authorization
  - " What

## Authentication

- ! Authentication - the process of determining whether someone or something is who or what it is stated to be
- ! Machine addresses (IP addresses or DNS names) should not be used for authentication... they are easily spoofed

## Authorization

Authorization - the process of determining whether or not a user has the authority to perform an activity or access specific data

## Public Key Infrastructure

PKI - public key infrastructure, a method of verification of encrypted data, using public encryption keys

## Certificate Authority

- ! CA (Certificate Authority) - a recognized company or service that validates digital certificates
- ! VeriSign and Thawte are examples of CAs.

## Security issues for users

- ! Know your rights
- ! Do you *trust* the vendor?
- ! Is the data encrypted?
- ! Is the data authenticated?

## Know your rights

- ! If there is an error, how much are you liable for?
- ! Is the company governed by USA laws?

## Do you trust the vendor?

- ! Is the vendor well known?
- ! Does the company use PKI?
- ! Does the company have a stated e-commerce policy?

## Is the data encrypted?

If you are using a web browser, is the lock locked?

## Does the vendor use PKI?

Is the vendor using a public key infrastructure to authenticate itself to you?

## Security issues for vendors

- ! Know exactly what you are doing
  - " Technology
  - " Obligations
  - " Liabilities
- ! Zero margin for error...Zero

## E-commerce Technology

- ! If you do not know exactly what you are doing hire someone who does and will sign off on the fact...
- ! Use SSL and authenticate users

## Use a well-trusted security software vendor

- ! Set up system by their rules and live by them
- ! Violations of their rules may make you liable
- ! Use a PKI strategy

## E-commerce Obligations

- ! Encrypt and authenticate data and state how you do these things
  - ! Tell users how your data is verified and encrypted; what is and is not stored
  - ! Never store data that shouldn't be stored
    - " DO NOT store credit card
    - " Personal information
- (remember the Fundamental Uncertainty Principle)*

## University of Nebraska

Remember - the University of Nebraska has an agreement with a e-commerce vendor, which controls e-commerce campus-wide

## Encryption/Data Transmission Topics

- ! Methods of Encryption
- ! SSH (Secure Shell) - remote access
- ! SSL (Secure Socket Layer) - http
- ! PGP (Pretty Good Protection) - email

### Methods of encryption

- ! Most modern encryption strategies use key pairs and algorithms
- ! SSH, SSL and PGP use this strategy

### SSH - secure shell (and SCP)

Secure shell program that replaces telnet and ftp with tools to do the same work in an encrypted environment

### How it works - SSH

- ! Owner creates a private and public key
- ! Private key goes on personal machine, public key on host
- ! At login, private and public keys MUST match, algorithm may also require pass phrase or password
- ! If the match is correct data between machines is encrypted using an algorithm such as RSA, DSA, etc.
- ! File transfers are also encrypted, using scp (secure copy)

### “Free” SSH client software

- ! OpenSSH (make sure and use current version)
- ! Putty (Windows)
- ! NiftyTelnet (<=Mac OS 9)

### Some SSH server software

- ! OpenSSH ([www.openssh.org](http://www.openssh.org))
- ! SSH ([www.ssh.com](http://www.ssh.com))
- ! Fsecure ([www.f-secure.com](http://www.f-secure.com))

### How it works - SSL

- ! Client opens a https URL in a SSL aware browser
- ! Server sends a digital certificate to a CA
- ! CA sends digital certificate to clients browser for review and acceptance
- ! If user accepts, browser shows a lock and data is encrypted until user leaves SSL pages

### Some SSL server software

- ! OpenSSL ([www.openssl.com](http://www.openssl.com))
- ! Covalent ([www.covalent.net](http://www.covalent.net))
- ! Lantia ([www.ssl.com](http://www.ssl.com))
- ! Stronghold ([www.redhat.com/software/stronghold/](http://www.redhat.com/software/stronghold/))

### How it works - PGP

- ! User 1 creates document
- ! User 1 encrypts document using recipients' public key (must have this from key server or from recipient)
- ! User 1 attaches document to normal email and sends document
- ! User 2 (recipient) opens mail, detaches document and decrypts using his/her pass phrase

## What it looks like - PGP

```
@ PGP;N ,,)X/ie ?mã{.Í?À~@deê‘(.’ Ø~p-
A@ Ò?Îî=<vÁÈæàªÚp¶{-@ü%Èv É+ÆÕOI%ç|ncC
*?... A6ç?sUn" ßØ$ '+?>?ÖnD-Â{ßS ? 8}>Éπj5ó‘?^?i?
f.?Á,uü ¶±çqM~ëIÏ ?ZTM-nT?~
?ÁÔ]“8cà±+âyn>ÓÇp-äjÑ
```

### Good passwords

- ! Words that are not in the dictionary
- ! Combinations of words, numbers and other characters
- ! Words longer than eight characters
- ! They can still be easy to remember

### Bad passwords

- ! Publicly available information about you
- ! Your department or building name
- ! Number sequences like 123

### Clear text passwords

- ! Sniffers can listen to a port and watch you enter your username and password
- ! Telnet, ftp and http are open to this type of exploit

### Even good passwords

- ! On Windows 95/98/ME
  - " Password system is not robust
  - " Brute force password cracking software can decrypt file shares

### Absence of passwords

- ! Without a password, anyone can login and use your stuff
- ! Many programs come with a widely known default password, which needs to be changed

Resources: [www.ianr.unl.edu/excite/](http://www.ianr.unl.edu/excite/)