

CS574

Computer Security

San Diego State University

Spring 2008

Lecture #6

Today's Structure

- Administrivia
- Questions
- Recent News
- Lecture

Administrivia

- Rohan Phishing Page
<http://www-rohan.sdsu.edu/phishing.html>
- Rohan Software
<http://www-rohan.sdsu.edu/rohansoft.html>
- Crashers: Too Late Now!
- Roll
(Or, who I think is registered for the class)

Questions?

Recent News

- Undersea cables
- P and NP
- PGP Encryption
- UNIX viruses
- Linux exploit
- Tradeoffs

Lecture

This Lecture

- Digital Signatures
- PKI
- OpenSSL
- Web of Trust
- GPG
- Assignment #1
- Version Control

Using Public Key Cryptography

- Encrypting with public keys is too slow, so we encrypt just a symmetric key that we make up on the spot and call a “session key”.
- We can also encrypt a hash (or a digest) of a message to verify the integrity of the content and to “digitally sign” the message.

Digital Signatures

- We “sign” a message by encrypting a hash of a message with our private key.
- Third parties can decrypt the encrypted hash, compute the hash against the message, and compare.
- We need secure hashing algorithms.

Hashing Algorithms

- *Hash (or digest) algorithms are an example of one-way functions.*
- Take as input a variable-length message, and return a fixed-size value.
- The pigeon-hole principle applies.

Desirable Features of a Hashing Algorithm

- It should not be easy to find two messages that hash to the same value.
- It should not be easy to find a message that hashes to a particular value.
- Small changes to input message should result in a large change to the result.

Algorithms

- SHA-1 and MD5 most common hash algorithms in widespread use.
- Both are “broken,” if not cracked.
- SHA-256 on up still considered “okay”.

Pfleeger

- Defines a **digital signature** as
...a protocol that produces the same effect as a real signature: It is a mark that only the sender can make, but other people can easily recognize as belonging to the sender.
- Four properties

Pfleeger

- Primary properties of a digital signature
 - *It must be unforgeable.*
 - *It must be authentic.*
- Desirable properties of a digital signature
 - *It is not alterable.*
 - *It is not reusable.*

Putting It All Together

- Public Key Infrastructure (PKI)
- Web of Trust

Public Key Infrastructure

- Hierarchies of Authority
- Certificates
- Certificate Authority
- Chaining Authorities
- Cross-certification

PKCS

PKCS #1	RSA encryption standard
PKCS #3	Diffie-Hellman key-exchange protocol
PKCS #5	Generate a secret key based on a password
PKCS #6	(Phased out in favor of X.509v3)
PKCS #7	Cryptographic Message Syntax
PKCS #8	Private-Key Information
PKCS #9	Attribute type definitions
PKCS #10	Certificate request syntax
PKCS #11	Cryptographic Token Interface
PKCS #12	Personal Information exchange syntax
PKCS #13	Elliptic-curve Cryptography
PKCS #14	Pseudo-Random Number Generation
PKCS #15	Cryptographic Token information format
	<i>see http://www.rsa.com/rsalabs/node.asp?id=2124</i>

PKI Example

- OpenSSL
 - Creating a Certificate
 - Self-Signing a Certificate
 - Generating a Request
- Looking at your trusted certificates

Public Key Infrastructure

- Certificate expirations
 - why might we want this?
- Key revocation
 - why/when might we want this?
- Centralized approach
 - is this the only way?

Web Of Trust

- You trust your friends.
- You trust the judgement of your friends.
- You sort of trust your friends of your friends.
- The more of your friends that trust someone, the more trust you'll have in that person.
- PGP / GPG

PGP

- PGP = Pretty Good Privacy
- Creation of Phil Zimmerman
- Uses RSA for keys, IDEA for encryption
- Alternate implementation from FSF:
GNU Privacy Guard

GPG Example

- Creating a GPG Key
- Key Fingerprints
- Signing a GPG Key
- Signing Parties

Project #1

Assignment #1

- Program Details
- MASC Accounts?
- Grading Style
- Version Control
 - RCS
 - CVS
 - Mercurial

Lecture References

- Pfleeger, *Security in Computing*, 3rd & 4th edition
- Bishop, *Introduction to Computer Security*
- Schneier, *Applied Cryptography*
- Schneier, *Practical Cryptography*
- Schneier, *The Crypto-Gram Newsletter*, Sep. 15, 2002
- Singh, *The Code Book*
- RSA Laboratories, *RSA Crypto FAQ*
- Gutman, *Lessons Learned in Implementing and Deploying Crypto Software*
- Rothenburg, et al., *The Snake-Oil FAQ*
- *They Cryptography FAQ*

End Lecture

Version Control Basics (Demonstration)

Reading

(For the next few classes)

- Pfleeger, Chapter 3

(Keep Reading)

Finis