6.857 Computer and Network Security October 8, 2002

Lecture Notes 10 : CCA, OAEP, Cramer-Shoup, Certificates

Lecturer: Ron Rivest *Scribe: Armour/Johann-Berkel/Owsley/Quealy*

[These notes come from Fall 2001. These notes are neither sound nor complete. There is more material than is covered in lecture, and some is missing. Check with students' notes for new topics brought up in 2002.]

1 Outline

- Plaintext-aware
- OAEP
- Adaptive Chosen-Ciphertext Attack
- Cramer-Shoup
- Public-Key Infrastructure

2 Public-Key Infrastructure (PKI)

2.1 Introduction

In cyberspace there is a need to verify the identities of individuals for a number of purposes. Some of these events include sending and receiving secure email, sending and receiving signed email, setting up a secure session (SSL), and accessing a protected resource. The way in which this goal of authentication is accomplished is by verifying that a public key belongs to an individual that you know and trust. Public-Key Infrastructure is designed to allow this kind of authentication.

2.2 Diffie Hellman Public-Key Encryption

"Public-Key Directory"

One way to associate public keys to individuals is by publishing a mapping of names to keys. This directory would act much like the WhitePages does for distributing phone numbers based on name. The directory must be trusted, therefore it must be authentic but need not be secret. Entries would be of the form:

$$\text{Alice} \longrightarrow (RSA, n = ..., e = 3)$$

$$\text{Bob} \longrightarrow (RSA, n = ..., e = 17)$$

Problem: Need to authenticate the issuer of the directory.
Solution: A possible solution would be for the issuer to sign the whole directory. (how do we get the issuer's PK? must be recursive)

Digital Certificates

Digital Certificates were proposed by Loren Kohnfelder here at MIT in a B.S. thesis in '78. They are an authenticated identifier pairing the public key to a significant name. This allows any user to identify themselves and establishes trust between themselves and a verifier who trusts the certificate authority. The CA is assumed to correctly identify the person who has requested the certificate.

This is the structure of a signed digital certificate.

$$\{\text{“}Alice\text{''}, (RSA, ...)\}_{CA}$$

Here is a representation of the exchange between a user with a certificate and a verifier.

$$(M)_{SK_A, cert} \longrightarrow Bob \text{ “relying party”}$$

Question: How does PKI deal with issues of dynamics in naming such as changing email addresses?
Answer: This does present a problem since information can change. The major issue becomes one of database update however.

Advantages

- Alice can include her certificate in an email or post it on the Web
- Bob only needs to know the Certificate Authority and its PK
- Alice may have more than one key (e.g., one for signing, one for encryption)
- Certificates can have a validity period (not before / not after a certain time)

Difficulty Issues

- Scalability
  - need multiple CAs
  - naming (unique? human-readable?)

- Robustness

  -compromised keys? (especially the root key!)

  -revoked certificate

- Certificate as Credential (Attribute Certificate instead of ID certificate)
- Trustworthiness of CA and procedures; liability?
- Privacy, Anonymity

Question: How do we deal with privacy issues in the CA?
Answer: Use certificate serial numbers instead of names.

2.3 Naming

PK infrastructure has a very intimate link with naming. We want a system that is easy to use for people, similar to that of file names. The naming relationship should be as follows:

- **Names** are for people to use.
- **Keys** are for machines to use.
- **PKI** can provide a binding between the two.

Naming is a large issue. Since the CA has the burden of properly identifying and labeling the parties with certificates, names must be made clear and accurate.

Naming provides an interface between people and cyberspace. People must then write security policy based on the name associated with a PK used to sign message. Writers of such policies need to know/understand the relationship between keys and names.

Desirable naming properties

- Descriptive
- Global uniqueness
- Dynamic

Examples

- Role (purchasing agent at IBM)
- Legal names
- Email

- Phone #'s ("enum")
- Mail address

Certificates can also be used for identifying much more about an individual than just identity. Attributes of a person can be given by certificates. For attributes, what exactly is the CA allowed to certify?

Example: John has brown hair.

How do they know?

Why should we believe them?