A presentation on

Public Key Infrastructure: Overview and Risks involved

Guided by
Riccardo Pucella
Assistant Prof.
CCIS Northeastern University

Presented by
Harsha Suleballe Jagadish
CCIS Northeastern

OVERVIEW

- Introduction
- The Certificate
- Components of a PKI
- PKI examples
- Ten risks of the PKI

INTRODUCTION

- What is PKI?
- What PKI infrastructure is expected to offer its users?
- Where is it used primarily?
- How Public Key Cryptography concept works?

The Certificate

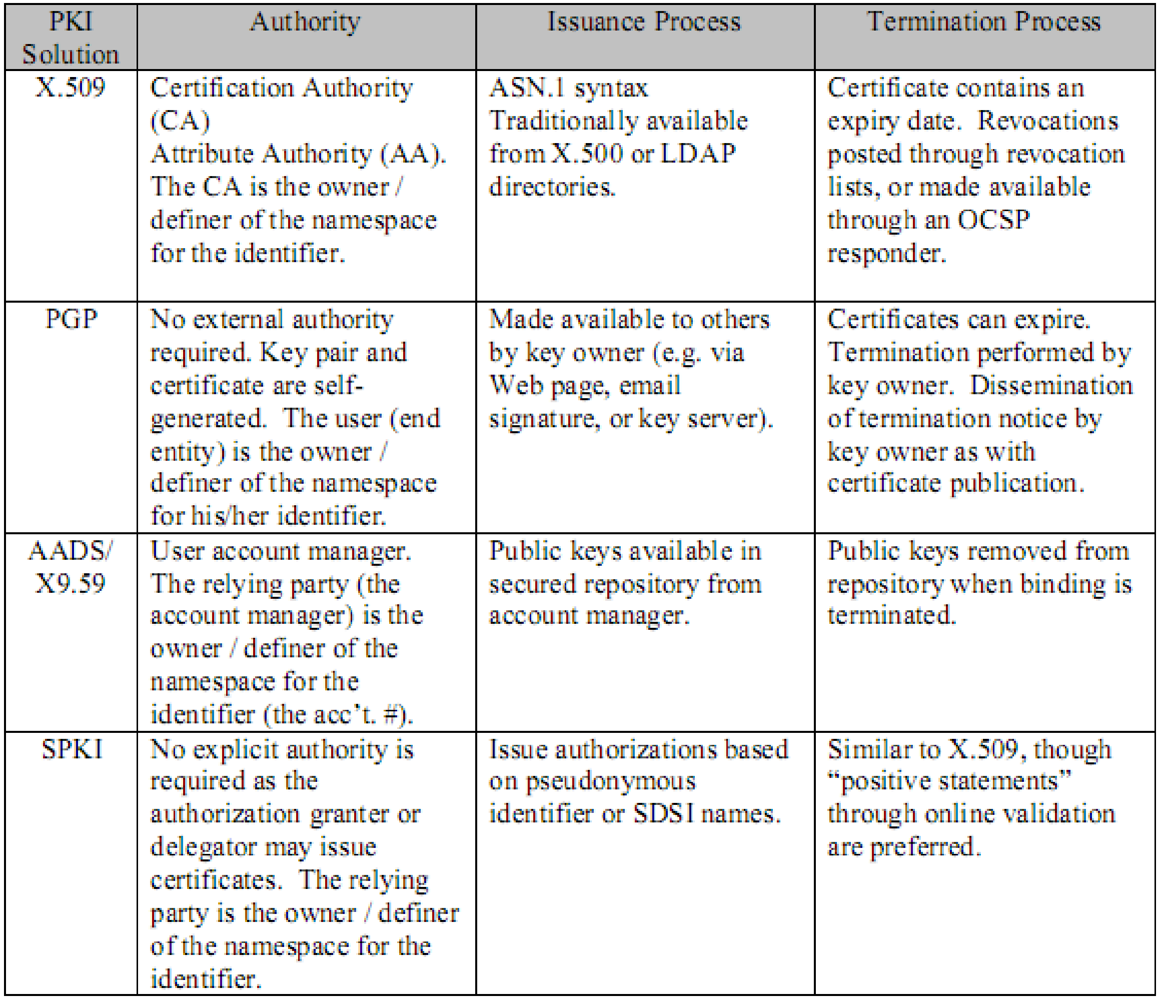
- What is a Certificate?
- What information does it contain?
- Controlling the Key usage.
- Storing methods for Public and Private keys.

Components of a PKI

A public key infrastructure is created by combining a number of services and technologies:

- Certification authority (CA)
- Revocation
- Registration Authority (RA)
- Key Update/Backup/Recovery
- Certificate publishing methods
- Certificate Management System

PKI Examples



PKI Solution	Authority	Issuance Process	Termination Process
X.509	Certification Authority (CA) Attribute Authority (AA). The CA is the owner / definer of the namespace for the identifier.	ASN.1 syntax Traditionally available from X.500 or LDAP directories.	Certificate contains an expiry date. Revocations posted through revocation lists, or made available through an OCSP responder.
PGP	No external authority required. Key pair and certificate are self-generated. The user (end entity) is the owner / definer of the namespace for his/her identifier.	Made available to others by key owner (e.g. via Web page, email signature, or key server).	Certificates can expire. Termination performed by key owner. Dissemination of termination notice by key owner as with certificate publication.
AADS/ X9.59	User account manager. The relying party (the account manager) is the owner / definer of the namespace for the identifier (the acc't. #).	Public keys available in secured repository from account manager.	Public keys removed from repository when binding is terminated.
SPKI	No explicit authority is required as the authorization granter or delegator may issue certificates. The relying party is the owner / definer of the namespace for the identifier.	Issue authorizations based on pseudonymous identifier or SDSI names.	Similar to X.509, though "positive statements" through online validation are preferred.

Ten Risks of PKI

- This is an overview of one of many perspectives of PKI technologies :
  - PKI was, like many security technologies, claimed to be a panacea.
  - It was intended to solve a very hard problem: build trust on a global level.
  - Running a CA -- "license to print money".

- Basic Premise :
  - Assertion #1 - e-commerce does not need PKI
  - Assertion #2 - PKI needs e-commerce

Risk 1 : who do we trust, and for what?

- Argument : CA is not inherently trustworthy
  - Why do/should you trust a CA?
  - In reality, they defer all legal liability for running a bad CA.
  - Risk in the hands of the certificate holder.
- Counter Argument : Incentives
  - Any CA caught misbehaving is going to be out of business tomorrow
  - This scenario is much worse than getting sued.
  - Risk held by everybody, which is what you want
  - Everyone has reason to be diligent.

Risk 2 : who is using my key?

- Argument: key is basically insecure
  - Your key is vulnerable, deal with it
  - In some places, you are being held responsible after a compromise.
- Counter Argument : this is the price of technology
  - You have to accept some responsibility in order to get benefit.
  - Will encourage people to use only safe technology

Risk 3 : How secure is the Verifier(s)?

- Argument: the computer that verifies your credential is fundamentally vulnerable.
  - ➢ Everything is based on the legitimacy of the verifier root public key (integrity of certificate files).
  - ➢ Browsers transparently use certificates.
- Counter Argument : this is the price of technology
  - ➢ You have to accept some responsibility in order to get benefit.
  - ➢ Will encourage people to use only safe technology

Risk 4 : Which John Robinson is he?

- Argument : identity in PKI is really too loosely defined
  - ➢ No standards for getting credential
  - ➢ No publicly known unique identifiers for people
  - ➢ So, how do you tell people apart
- Counter Argument : due diligence
  - ➢ Only use certificates in well known circumstances
  - ➢ When in doubt, use other channels to help.

Risk 5: Is the CA an authority?

- Argument : there are things in certificates that claim authenticity and authorization of which they have no dominion.
  - "rights" (such as the right to perform SSL) - this confuses authorization authority with authentication authority
  - DNS, attributes -- the CA is not the arbiter of these things
- Counter Argument : this is OK, because it is part of the implicit charge we give our CA -- we implicitly accept the CA as authority in several domains

Risks 6 & 7

- 6: Is the user part of the design?
  - Argument: too many things hidden in use, user has no ability to affect or see what is going on.
  - Counter-Argument: too sophisticated for user to understand

- 7: Was it one CA or CA+RA?
  - Argument: separation of registration from issuance allows forgery.
  - e.g., RA handles vetting, CA makes certificates, so, you better have good binding between these entities or bad things can happen.
  - Counter-Argument: this is an artifact of organization, only a problem when CA is bad (you are doomed anyway)

Risk 8 : How did the CA identify the Certificate Holder?

- Argument:
  - CAs do not have good information to work with, so real identification is poor.
- Counter Argument :
  - It has worked well in the physical work, why not here?

Risk 9: How secure are Cert. Practices?

- Argument : certificates have to be used properly to be secure.
  - Everything is based on the legitimacy of the verifier root public key, protection of its key
  - Lifetime & revocation have to be done.
- Counter Argument : This is the price of technology
  - You have to accept some risk in order to get benefit.
  - Will encourage people to use only safe technology.

Risk 10:Why are we using the CA process, anyway?

- Argument : We are trying to solve a painful problem: authenticating users.
  - However, certificates don't really solve the problem, just give you another tool to implement it.
  - Hence, its not a panacea.
  - Not delivered on its promises.
  - Caveat-Emptor, A commercial principle that without a warranty the buyer takes upon himself the risk of quality

Questions???

THANK YOU!!!!!

Misc : "Two can keep a secret when either of them is dead"