About the Talk

- Concerns about the deployment Issues of PKI
- Assessing the Trustworthiness of CA
- A Better Trust Management
- Research Challenges
X.509 Trust Model

Certification authority (CA)

Relying party (RP)

Certificate holder

X.509

Indirect contractual relation

Direct contractual relation
Motivation for Talk

- Why RP should "TRUST" CA?
- Computational Trust in PKI
Problems persisting in present PKI implementations:

- Computers don’t understand the semantics of a policy
- Cross Certification requires equal policies
- PKIs don’t handle trust dilution
- PKIs don’t take into account parallel certification paths
- PKIs give little support for decision making
Trust management includes methods for assessing policies regarding issuance and handling of public-key certificates and for determining whether these policies are adhered to by CAs and users, with the purpose of making decisions.

Trust Assessment must be based on some initial trust combined with trust propagating mechanisms, and should provide a basis for decision making.
Two Definitions of Trust:

- **Belief Trust**: The subjective belief by which an individual, A, thinks that another entity B performs a given action on which A’s welfare depends (Gambetta 1998)

- **Decision Trust**: The decision to depend on something or somebody in a given situation with a feeling of relativity, even though negative consequences are possible (Mcknight & Chervang 1996)
Some Trust Semantics

- **Trust Scope**: The combined set of functions that the relying party depends on & trusts
- **Functional Trust**: The trusted party actually performs the functions of the trust scope.
- **Referral Trust**: The trusted party recommends a party that can perform the functions of the trust scope.
Trust Transitivity

Thanks to Bob’s advice, Alice trusts Eric to be a good mechanic.

间接功能信任

直接推荐信任

直接功能信任

建议

Bob has proven to Alice that he is knowledgeable in matters relating to car maintenance.

Eric has proven to Bob that he is a good mechanic.
Computational Trust in PKI

- Trust Modelling
- Subjective Logic Based Trust Networks
- Computing Trust in PKI
Subjective Logic

- Formalized by Prof. Audung Josang
- It is a type of probabilistic logic that explicitly takes uncertainty & belief ownership into account
- Suitable for modeling and analyzing situations involving uncertainty & incomplete knowledge

E.g. Modeling Trust Networks, Analysing Bayesian Networks.
Subjective Trust Networks

Trust Network based on Subjective Logic can be modelled with a combination of the transitivity/discounting & fusion operator.
A PKI allows to be propagated from where it exists to where it is needed (Simmons and Meadows, 1995)

Where trust exists

Trust anchor = Root of trust

The root public key is assumed to be authentic

PKI

Where trust is needed

We need to determine if user keys are authentic
PKI and Trust Transitivity

- Functional trust in the public key
  (I have the CA/entity’s authentic and uncompromised public key)

- Referral trust in the CA
  (I trust the CA to issue correct public-key certificates)
Computing Trust in PKI Certificates

Relying Party $A$

$\omega^A_{\text{trust}(B)}$

$\omega^A_{\text{pubk}(B)}$

Product rule

Relying Party $A$

$\omega^A_B = \omega^A_{\text{trust}(B)} \times \omega^A_{\text{pubk}(B)}$

Note that $\omega^A_B$ can also be denoted as $\omega^A_{\text{trust}(B)} \times \text{pubk}(B)$.

$\omega^A_B$ expresses $A$'s trust in certificates signed by $B$'s public key.
PKI and Trust Transitivity

\[ \omega^A_{\text{pubk}(E)} = \omega^A_B \otimes \omega^B_{\text{pubk}(E)} \]

\( \omega^A_{\text{pubk}(E)} \) expresses \( A \)'s belief in the authenticity of \( E \)'s public key
X.509 Digital Certificate

- Version
- Serial Number
- Algorithm Identifier
- Issuer Name
- Issuer Unique Identifier
- Subject Name
- Subject Unique Name
- Subject Public Key
- Validity Period
- Extensions
  - Opinion about public-key authenticity
  - Trust in CA (for certificates on CAs)

CA Digital Signature
The PKI Trust model assumes that relying party generates self-signed certificates for the root CAs.

Certification by relying parties transforms traditional PKIs into user-centric PKIs similarly to the PGP PKI.
A’s derived opinion about the authenticity of E’s public key can be computed as:

$$\omega^A_{\text{pubk}(E)} = \omega^A_B \otimes \omega^B_C \otimes \omega^C_{\text{pubk}(E)}$$
Research Challenges

- Reliable Trust Evaluation methods for closed deployment PKI
- Interoperability Issue of open deployment PKI
References

- "PKI seeks a Trusting Relationship", by Audun Josang
- Subjective Logic, A formalism for reasoning under uncertainty, springer 2016, Audun Josang
- Trust Management for Public Key Infrastructures: Implementing the X.509 Trust Broker, Chadwick et al, 2017
THANKS FOR LISTENING !!