Modeling Public Key Infrastructures in the Real World

John Marchesini and Sean Smith

BindView Corporation
Dept. of Computer Science - Dartmouth College

Making Trust Judgements

- PKIs give users information to make *trust judgements*
- Based on initial assumptions and a pile of certificates
- If PKI works, we can deduce what we should and can't deduce what we shouldn't
- Complex and important decision: use formal methods
- PKI designers can verify their designs

Maurer's Deterministic Model

- In 1996, Maurer released his *deterministic model*
- 4 statements: Authenticity, Trust, Recommendation, Certificate
- 2 inference rules:
  - ⋆ Derive authenticity
  - ⋆ Derive trust
- Initial View is the set of beliefs and observable statements
- Derived View is the intial view closed under inference rules
- If *Aut* is in my derived view, I can use the public key

The Limits of Maurer's Model

- Authenticity of public keys
- Names = limited applicability
- Recommendation = all-or-none
- No time = no revocation or past
- No verification = bad deductions

The Limits of Maurer's Model

- Authenticity of public keys $\rightarrow$ Binding b/t key and cert info
- Names = limited applicability $\rightarrow$ Properties, maybe name
- Recommendation = all-or-none $\rightarrow$ Trust transfer of properties
- No time = no revocation or past $\rightarrow$ Added time
- No verification = bad deductions $\rightarrow$ Added validity templates

Definition 1: Statements

- **Authenticity of binding**: *Aut*$(A, X, \mathcal{P}, \mathcal{I}) \stackrel{def}{=} A \xrightarrow{\mathcal{P},\mathcal{I}} X$
- **Trust**: *Trust*$(A, X, \mathcal{D}, \mathcal{I}) \stackrel{def}{=} A \overset{\mathcal{D},\mathcal{I}}{\dashrightarrow} X$
- **Certificates**: *Cert*$(X, B, \mathcal{P}, \mathcal{I}) \stackrel{def}{=} X \xrightarrow{\mathcal{P},\mathcal{I}} B$
- **Trust Transfers**: *Tran*$(X, Y, \mathcal{P}, \mathcal{I}) \stackrel{def}{=} X \overset{\mathcal{P},\mathcal{I}}{\dashrightarrow} Y$
- We added second-order structures
  - ⋆ **Certificate Validity Templates**: *Valid*$\langle A, Cert, t\rangle$
  - ⋆ **Transfer Validity Templates**: *Valid*$\langle A, Tran, t\rangle$

Definition 2: Inference Rules

- View_A is Alice's initial view
- $\overline{\mathit{View}_A(t)}$ is Alice's derived view at time t where:

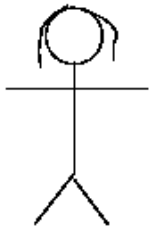
  $\forall X, Y, t \in \{\mathcal{I}_0 \cap \mathcal{I}_1\}, \mathcal{Q} \subseteq \mathcal{D}$:

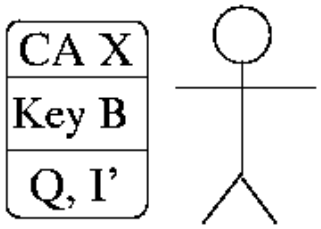
  $\mathit{Aut}(A, X, \mathcal{P}, \mathcal{I}_0),\ \mathit{Trust}(A, X, \mathcal{D}, \mathcal{I}_1),\ \mathit{Valid}\langle A, \mathit{Tran}(X, Y, \mathcal{Q}, \mathcal{I}_2), t\rangle$
  $\vdash\ \mathit{Trust}(A, Y, \mathcal{Q}, \mathcal{I}_2)$

  $\mathit{Aut}(A, X, \mathcal{P}, \mathcal{I}_0), \mathit{Trust}(A, X, \mathcal{D}, \mathcal{I}_1), \mathit{Valid}\langle A, \mathit{Cert}(X, B, \mathcal{Q}, \mathcal{I}_2), t\rangle$
  $\vdash\ \mathit{Aut}(A, B, \mathcal{Q}, \mathcal{I}_2)$

- For A to believe B at time t, $\mathit{Aut}(A, B, \mathcal{Q}, \mathcal{I}_2) \in \overline{\mathit{View}_A(t)}$

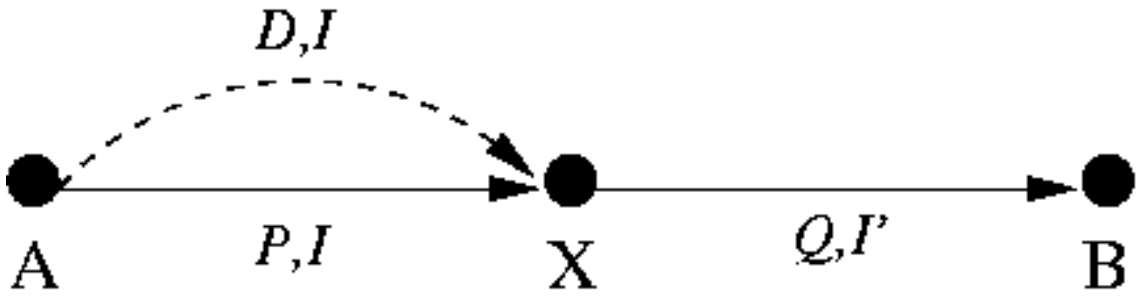
An Example





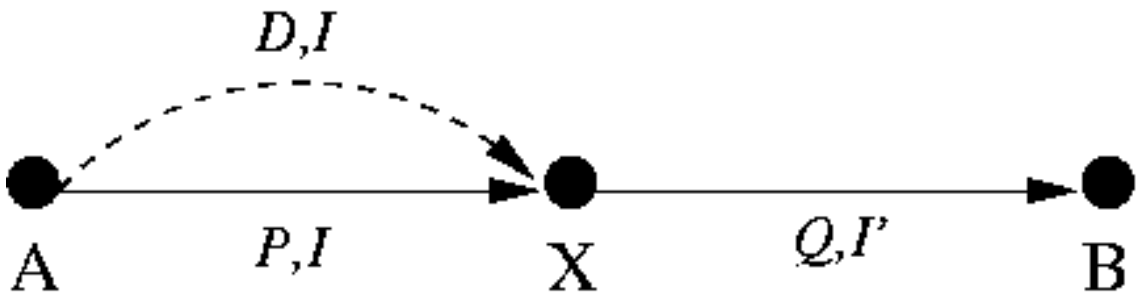
- Alice and Bob both use CA X
- X certified Bob and assigned him properties $\mathcal{Q}$ for $\mathcal{I}'$

Statement Graph



- $\mathit{View}_A = \{\mathit{Aut}(A, X, \mathcal{P}, \mathcal{I}), \mathit{Trust}(A, X, \mathcal{D}, \mathcal{I}), \mathit{Cert}(X, B, \mathcal{Q}, \mathcal{I}')\}$

Statement Graph



- $\mathit{View}_A = \{\mathit{Aut}(A, X, \mathcal{P}, \mathcal{I}), \mathit{Trust}(A, X, \mathcal{D}, \mathcal{I}), \mathit{Cert}(X, B, \mathcal{Q}, \mathcal{I}')\}$
- Using the inference rules:

  $\mathit{Aut}(A, X, \mathcal{P}, \mathcal{I}), \mathit{Trust}(A, X, \mathcal{D}, \mathcal{I}), \mathit{Valid}\langle A, \mathit{Cert}(X, B, \mathcal{Q}, \mathcal{I}'), t\rangle$
  $\vdash \mathit{Aut}(A, B, \mathcal{Q}, \mathcal{I}')$

- $\overline{\mathit{View}_A(t)} = \mathit{View}_A \cup \mathit{Aut}(A, B, \mathcal{Q}, \mathcal{I}')$
- Since $\mathit{Aut}(A, B, \mathcal{Q}, \mathcal{I}') \in \overline{\mathit{View}_A(t)}$, Alice uses Bob's cert

Using the New Model

- Properties allow multiple cert families: X.509, ACs, PCs, SDSI/SPKI
- Time allows revocation and events in the past/future
- Properties allow for authorization scenarios
- Trust Transfers and domains enable delegation
- Time and Properties allow us to model hybrid PKIs: Greenpass and MyProxy

Conclusions and Future Work

- New model can handle many types of real-world systems
- How well do the cert properties match the real world?
- Nonmonotonicity: decoupling cert lifespans from beliefs
- What kind of set operations on properties should we allow?