Credential Networks: a General Model for Distributed Trust and Authenticity Management

Jacek Jonczy & Rolf Haenni

Reasoning under **UN**certainty Group
Institute of Computer Science and Applied Mathematics
University of Berne, Switzerland

PST'05

October 12-14, 2005

Outline

Outline

Outline

Outline

Outline

Authenticity and Trust

World 1: (Public Key) Cryptography

- PKI
- Certificates → **Authenticity**
- *Question*: Is the certifying entity **trustworthy**?

World 2: E-Business

- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- *Question*: Is an entity's public key **authentic**?

Authenticity and Trust

Aut_X?

World 1: (Public Key) Cryptography

- PKI
- Certificates → **Authenticity**
- *Question*: Is the certifying entity **trustworthy**?

User X

$Trust_X$?

World 2: E-Business

- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- *Question*: Is an entity's public key **authentic**?

Authenticity and Trust

$Aut_X?$

World 1: (Public Key) Cryptography

- PKI
- Certificates → **Authenticity**
- *Question*: Is the certifying entity **trustworthy**?

User X

$Trust_X?$

World 2: E-Business

- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- *Question*: Is an entity's public key **authentic**?

Authenticity and Trust

Aut_X?

World 1: (Public Key) Cryptography

- PKI
- Certificates → **Authenticity**
- *Question*: Is the certifying entity **trustworthy**?

User X

$Trust_X$?

World 2: E-Business

- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- *Question*: Is an entity's public key **authentic**?

Authenticity and Trust

Aut_X?

User X

$Trust_X$?

World 1: (Public Key) Cryptography

- PKI
- Certificates → **Authenticity**
- *Question*: Is the certifying entity **trustworthy**?

Two-Layer Model

World 2: E-Business

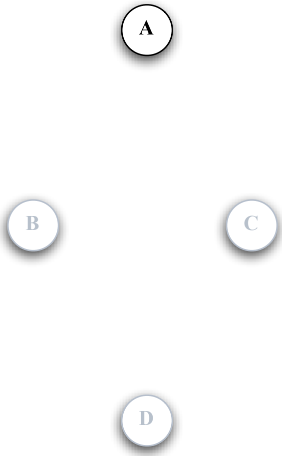
- Reputation Network
- Ratings/Recommendations (digitally signed) → **Trust**
- Question: Is an entity's public key **authentic**?

Outline

1. Introduction
2. Credential Networks
3. Evaluation
4. Conclusion

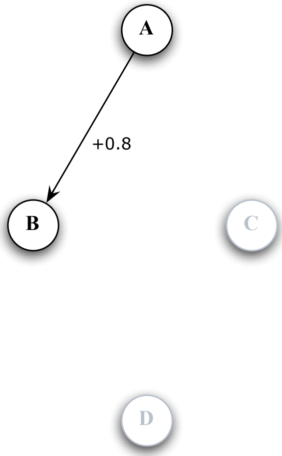
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



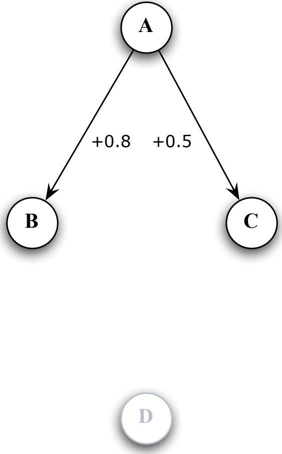
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



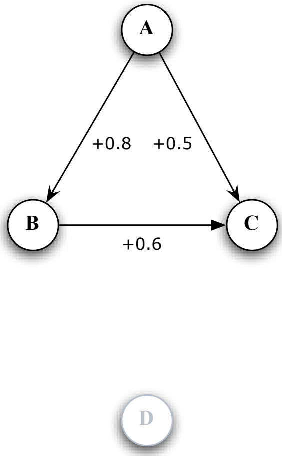
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



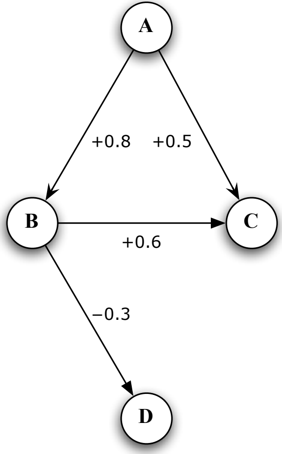
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



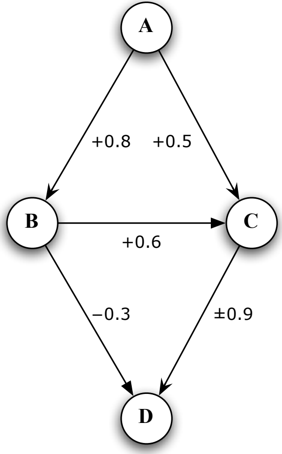
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



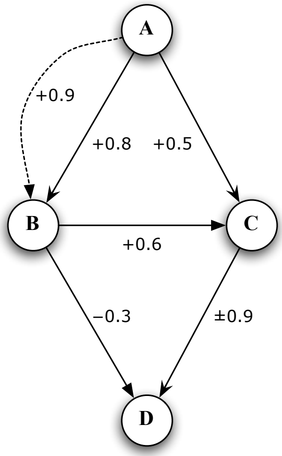
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



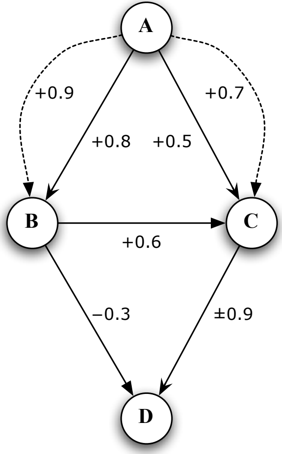
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



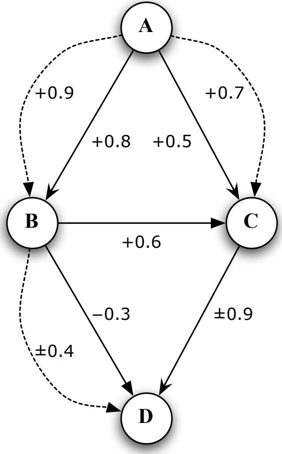
Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



Example

- C1 A: "I am quite sure (80%) that B's public key is authentic."
- C2 A: "I assume (50%) that C's public key is authentic."
- C3 B: "I believe (60%) in the authenticity of C's public key."
- C4 B: "I have some doubts (30%) that D's public key is authentic."
- C5 C: "On a scale between 0 and 1, I would rate the authenticity of D's public key with 0.9."
- C6 A: "I am almost sure (90%) that B is trustworthy."
- C7 A: "I believe (70%) in C's trustworthiness."
- C8 B: "On a scale between 0 and 1, I would rate D's trustworthiness with 0.4."



Credentials

- A **credential** is a digitally signed statement concerning a user's X authenticity (Aut_X) or trustworthiness ($Trust_X$)
- Credential $C = (class, sign, issuer, recipient, weight)$

$$class \in \{\mathrm{T},\mathrm{A}\}, \qquad sign \in \{+,-,\pm\},$$
$$issuer, recipient \in \mathcal{U}_0, \qquad weight \in [0,1].$$

- Six possible credential types: $\{\mathrm{T}, \mathrm{A}\} \times \{+, -, \pm\}$
- A-**credentials:**

$$A^{sign,weight}_{issuer,recipient} = (\mathrm{A}, sign, issuer, recipient, weight)$$

- T-**credentials:**

$$T^{sign,weight}_{issuer,recipient} = (\mathrm{T}, sign, issuer, recipient, weight)$$

Credential Networks: The Model

Definition

A credential network is a tuple

$$\mathcal{N} = (\mathcal{U}_0, X_0, \mathcal{C})$$

where

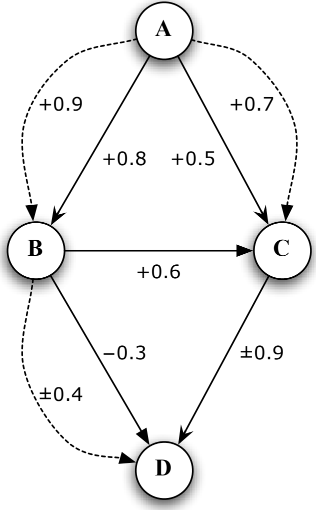
$$\begin{aligned} \mathcal{U}_0 &= \text{set of all users } X_0, X_1, X_2, \ldots, X_n \\ X_0 &= \text{owner of the network} \\ \mathcal{C} &= \text{set of credentials } C_1, C_2, \ldots, C_m \end{aligned}$$

Example

$$\mathcal{U}_0 = \{A, B, C, D\}$$

$$X_0 = A$$

$$\mathcal{C} = \left\{ \begin{array}{l} A_{AB}^{+0.8}, A_{AC}^{+0.5}, A_{BC}^{+0.6}, \\ T_{AB}^{+0.9}, T_{AC}^{+0.7}, \\ A_{BD}^{-0.3}, \\ A_{CD}^{\pm 0.9}, \\ T_{BC}^{\pm 0.4} \end{array} \right\}$$



Certificates & Recommendations

- Type 1: Certificate
  - is a positive A-credential $A_{XY}^{+\pi}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{A}_{XY}^{+} \rightarrow Aut_Y$
  - $p(\mathrm{A}_{XY}^{+}) = \pi$
- Type 2: Recommendation
  - is a positive T-credential $T_{XY}^{+\pi}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{T}_{XY}^{+} \rightarrow Trust_Y$
  - $p(\mathrm{T}_{XY}^{+}) = \pi$

Certificates & Recommendations

- Type 1: Certificate
  - is a positive A-credential $A^{+\pi}_{XY}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{A}^{+}_{XY} \rightarrow Aut_Y$
  - $p(\mathrm{A}^{+}_{XY}) = \pi$
- Type 2: Recommendation
  - is a positive T-credential $T^{+\pi}_{XY}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{T}^{+}_{XY} \rightarrow Trust_Y$
  - $p(\mathrm{T}^{+}_{XY}) = \pi$

Revocations & Discredits

- Type 3: Revocation
  - is a negative A-credential $A^{-\pi}_{XY}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{A}^{-}_{XY} \rightarrow \neg Aut_Y$
  - $p(\mathrm{A}^{-}_{XY}) = \pi$
- Type 4: Discredit
  - is a negative T-credential $T^{-\pi}_{XY}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{T}^{-}_{XY} \rightarrow \neg Trust_Y$
  - $p(\mathrm{T}^{-}_{XY}) = \pi$

Revocations & Discredits

- Type 3: Revocation
  - is a negative A-credential $A_{XY}^{-\pi}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{A}_{XY}^{-} \rightarrow \neg Aut_Y$
  - $p(\mathrm{A}_{XY}^{-}) = \pi$
- Type 4: Discredit
  - is a negative T-credential $T_{XY}^{-\pi}$ issued by X for Y
  - $Aut_X \wedge Trust_X \wedge \mathrm{T}_{XY}^{-} \rightarrow \neg Trust_Y$
  - $p(\mathrm{T}_{XY}^{-}) = \pi$

Mixed Ratings

- Type 5: Authenticity Rating
  - is a mixed A-credential $A^{\pm\pi}_{XY}$ issued by X for Y

$$Aut_X \wedge Trust_X \wedge \mathrm{A}^{\pm}_{XY} \rightarrow Aut_Y,$$

$$Aut_X \wedge Trust_X \wedge \neg\mathrm{A}^{\pm}_{XY} \rightarrow \neg Aut_Y.$$

  - $p(\mathrm{A}^{\pm}_{XY}) = \pi, \ p(\neg\mathrm{A}^{\pm}_{XY}) = 1 - \pi$
- Type 6: Trust Rating
  - is a mixed T-credential $T^{\pm\pi}_{XY}$ issued by X for Y

$$Aut_X \wedge Trust_X \wedge \mathrm{T}^{\pm}_{XY} \rightarrow Trust_Y,$$

$$Aut_X \wedge Trust_X \wedge \neg\mathrm{T}^{\pm}_{XY} \rightarrow \neg Trust_Y.$$

  - $p(\mathrm{T}^{\pm}_{XY}) = \pi, \ p(\neg\mathrm{T}^{\pm}_{XY}) = 1 - \pi$

Mixed Ratings

- Type 5: Authenticity Rating
  - is a mixed A-credential $A^{\pm\pi}_{XY}$ issued by X for Y

$$Aut_X \wedge Trust_X \wedge \mathrm{A}^{\pm}_{XY} \rightarrow Aut_Y,$$

$$Aut_X \wedge Trust_X \wedge \neg \mathrm{A}^{\pm}_{XY} \rightarrow \neg Aut_Y.$$

  - $p(\mathrm{A}^{\pm}_{XY}) = \pi, \; p(\neg \mathrm{A}^{\pm}_{XY}) = 1 - \pi$

- Type 6: Trust Rating
  - is a mixed T-credential $T^{\pm\pi}_{XY}$ issued by X for Y

$$Aut_X \wedge Trust_X \wedge \mathrm{T}^{\pm}_{XY} \rightarrow Trust_Y,$$

$$Aut_X \wedge Trust_X \wedge \neg \mathrm{T}^{\pm}_{XY} \rightarrow \neg Trust_Y.$$

  - $p(\mathrm{T}^{\pm}_{XY}) = \pi, \; p(\neg \mathrm{T}^{\pm}_{XY}) = 1 - \pi$

Special Cases

Credential Networks include the following special cases:

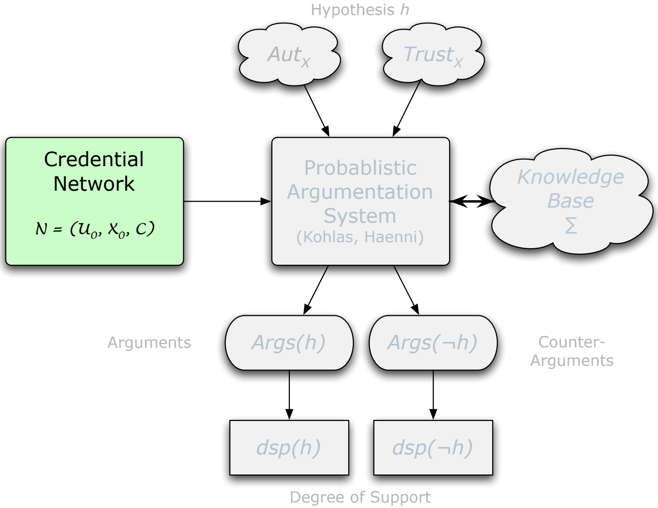
- PGP's Web of Trust
- Maurer's Model
- Haenni's Model
- Centralized Model (CA)
- Reputation Networks (in some sense)
- etc.

Similar models:

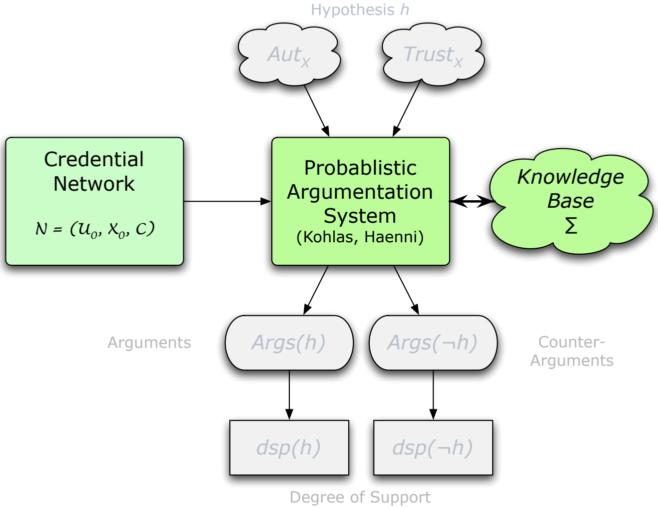
- Certificate Algebra (A. Jøsang)
- etc.

Outline

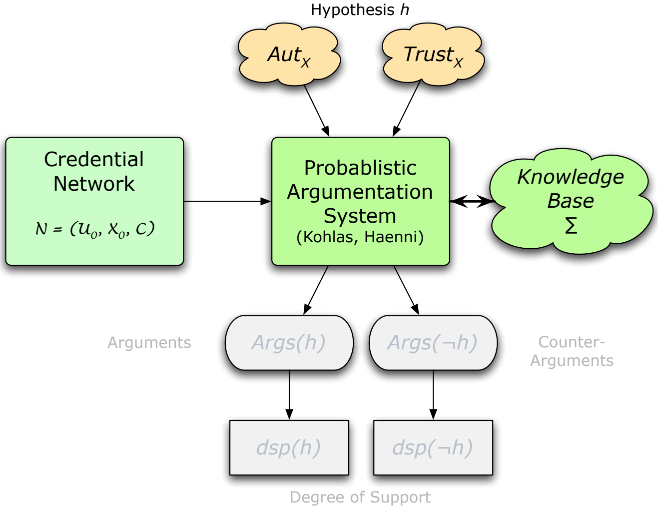
Evaluation: An Uncertain Reasoning Approach



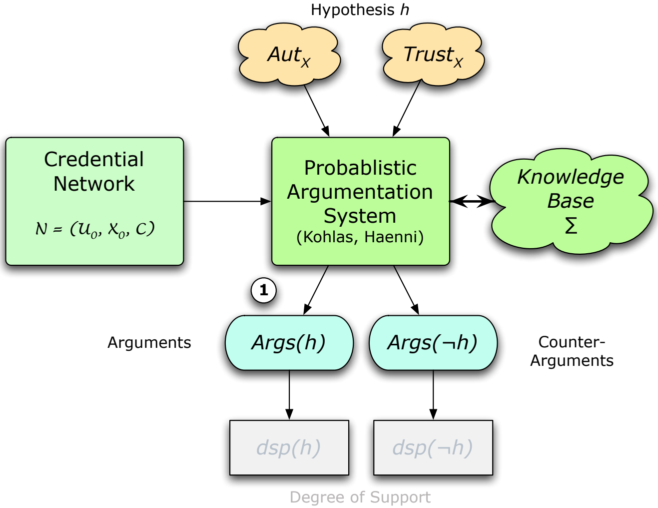
Evaluation: An Uncertain Reasoning Approach



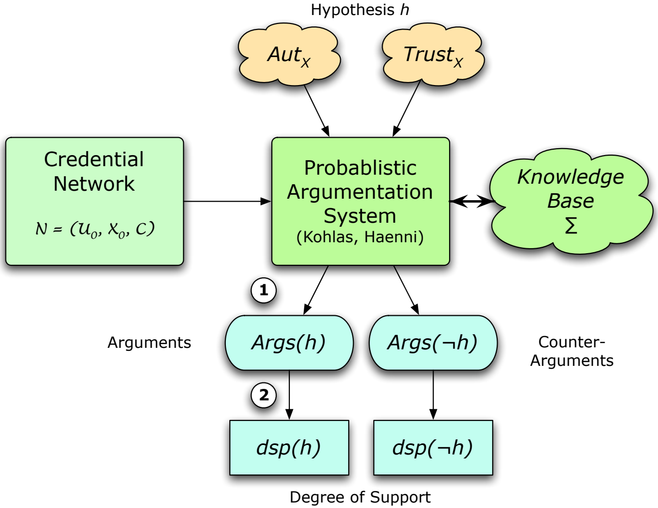
Evaluation: An Uncertain Reasoning Approach



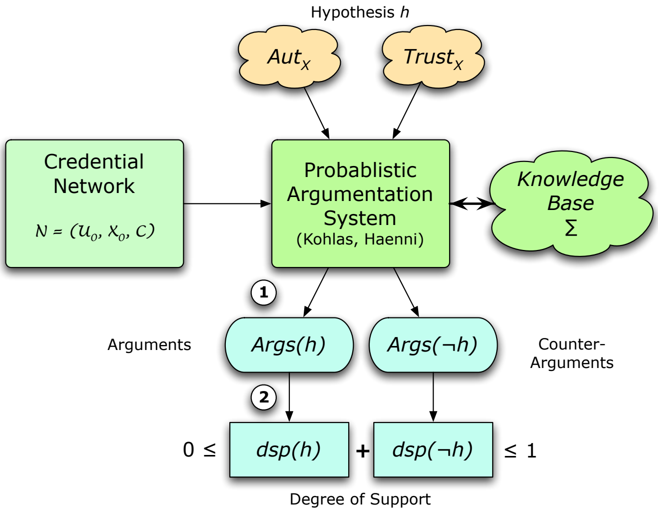
Evaluation: An Uncertain Reasoning Approach



Evaluation: An Uncertain Reasoning Approach



Evaluation: An Uncertain Reasoning Approach



Probabilistic Argumentation System (PAS)

Definition

A PAS is a tuple

$$\mathcal{S} = (V, W, \mathbf{P}, \Sigma)$$

such that

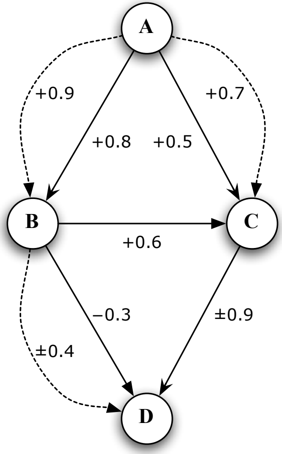
$$\begin{aligned} V &= \text{set of propostional variables}, \\ \mathcal{L}_V &= \text{propositional language over } V, \\ W &= \text{subset of } V \text{ with } \mathbf{P}(W), \\ \Sigma &= \text{logical knowledge base } \subseteq \mathcal{L}_V. \end{aligned}$$

Example

$$W = \{\mathrm{A}^{+}_{AB}, \mathrm{A}^{+}_{AC}, \mathrm{A}^{\pm}_{CD}, \mathrm{T}^{+}_{AB}, \mathrm{T}^{+}_{AC}, \mathrm{A}^{+}_{BC}, \mathrm{A}^{-}_{BD}, \mathrm{T}^{\pm}_{BD}\}$$

$$V = W \cup \{Aut_X, Trust_X \,:\, X \in \{A,B,C,D\}\}$$

$$\Sigma = \left\{ \begin{array}{l} Aut_A \\ Trust_A \\ Aut_A \wedge Trust_A \wedge \mathrm{A}^{+}_{AB} \rightarrow Aut_B \\ Aut_A \wedge Trust_A \wedge \mathrm{A}^{+}_{AC} \rightarrow Aut_C \\ Aut_A \wedge Trust_A \wedge \mathrm{T}^{+}_{AB} \rightarrow Trust_B \\ Aut_A \wedge Trust_A \wedge \mathrm{T}^{+}_{AC} \rightarrow Trust_C \\ Aut_B \wedge Trust_B \wedge \mathrm{A}^{+}_{BC} \rightarrow Aut_C \\ Aut_B \wedge Trust_B \wedge \mathrm{T}^{-}_{BD} \rightarrow \neg Aut_D \\ Aut_B \wedge Trust_B \wedge \mathrm{T}^{\pm}_{BD} \rightarrow Aut_D \\ Aut_B \wedge Trust_B \wedge \neg\mathrm{T}^{\pm}_{BD} \rightarrow \neg Aut_D \\ Aut_C \wedge Trust_C \wedge \mathrm{A}^{\pm}_{CD} \rightarrow Aut_D \\ Aut_C \wedge Trust_C \wedge \neg\mathrm{A}^{\pm}_{CD} \rightarrow \neg Aut_D \end{array} \right\}$$



$\mathbf{P}(W)$: $p(\mathrm{A}^{+}_{AB})=0.8$, $p(\mathrm{T}^{+}_{AB})=0.9$, $p(\mathrm{A}^{+}_{BC})=0.6$, ...

Qualitative Approach

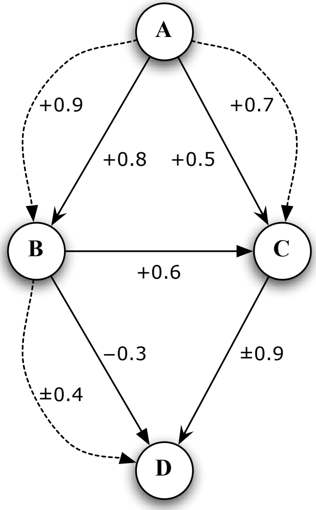
Arguments for $Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

$$args(Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AC}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(\neg Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{A}^-_{BD}\mathrm{T}^+_{AB}, \\ \mathrm{A}^+_{AC}\neg\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\neg\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{T}^+_{AB}\mathrm{T}^\pm_{BD}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{AC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(\neg Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{T}^+_{AB}\neg\mathrm{T}^\pm_{BD}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{AC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$



Qualitative Approach

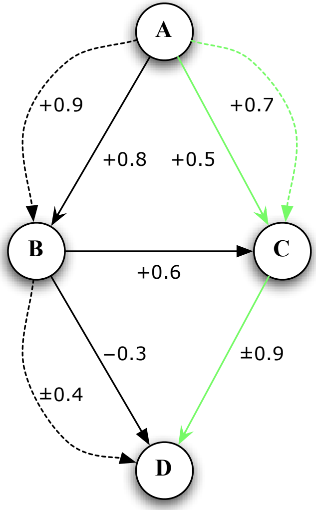
Arguments for $Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

$$args(Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AC}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{BC}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(\neg Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\,\mathrm{A}^{-}_{BD}\,\mathrm{T}^{+}_{AB}, \\ \mathrm{A}^{+}_{AC}\,\neg\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{BC}\,\neg\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{\pm}_{BD}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{BC}\,\mathrm{A}^{-}_{BD}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{AC}\,\mathrm{A}^{-}_{BD}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(\neg Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\,\mathrm{T}^{+}_{AB}\,\neg\mathrm{T}^{\pm}_{BD}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{BC}\,\mathrm{A}^{-}_{BD}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\,\mathrm{A}^{+}_{AC}\,\mathrm{A}^{-}_{BD}\,\mathrm{A}^{\pm}_{CD}\,\mathrm{T}^{+}_{AB}\,\mathrm{T}^{+}_{AC} \end{array} \right\}$$



Qualitative Approach

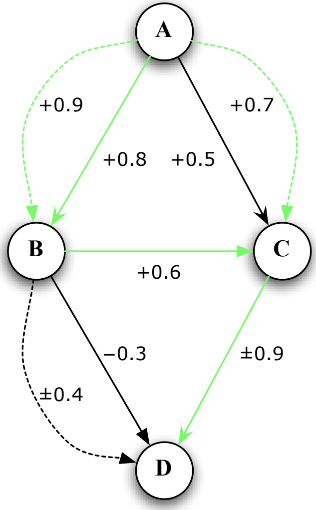
Arguments for $Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

$$args(Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AC}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(\neg Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{A}^-_{BD}\mathrm{T}^+_{AB}, \\ \mathrm{A}^+_{AC}\neg\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\neg\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{T}^+_{AB}\mathrm{T}^\pm_{BD}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{AC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$

$$args(\neg Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^+_{AB}\mathrm{T}^+_{AB}\neg\mathrm{T}^\pm_{BD}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{BC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC}, \\ \mathrm{A}^+_{AB}\mathrm{A}^+_{AC}\mathrm{A}^-_{BD}\mathrm{A}^\pm_{CD}\mathrm{T}^+_{AB}\mathrm{T}^+_{AC} \end{array} \right\}$$



Qualitative Approach

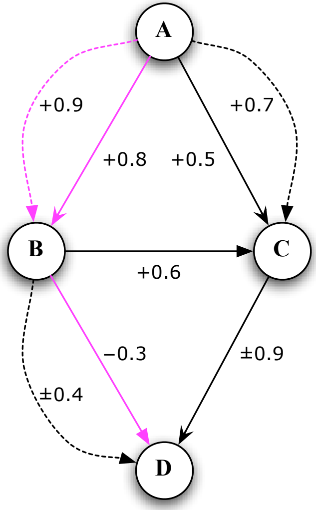
Arguments for $Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

$$args(Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AC}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{BC}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(\neg Aut_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\mathrm{A}^{-}_{BD}\mathrm{T}^{+}_{AB}, \\ \mathrm{A}^{+}_{AC}\neg\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{BC}\neg\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\mathrm{T}^{+}_{AB}\mathrm{T}^{\pm}_{BD}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{BC}\mathrm{A}^{-}_{BD}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{AC}\mathrm{A}^{-}_{BD}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC} \end{array} \right\}$$

$$args(\neg Trust_D) = \left\{ \begin{array}{l} \mathrm{A}^{+}_{AB}\mathrm{T}^{+}_{AB}\neg\mathrm{T}^{\pm}_{BD}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{BC}\mathrm{A}^{-}_{BD}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC}, \\ \mathrm{A}^{+}_{AB}\mathrm{A}^{+}_{AC}\mathrm{A}^{-}_{BD}\mathrm{A}^{\pm}_{CD}\mathrm{T}^{+}_{AB}\mathrm{T}^{+}_{AC} \end{array} \right\}$$



Quantitative Approach

Computing **degrees of support** for
$Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

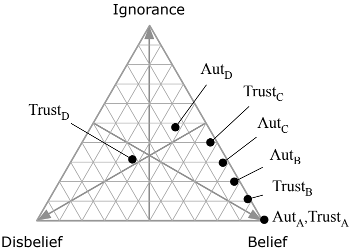
- Suppose threshold $\lambda = 0.7$ for *accepting* a hypotheses

$\Rightarrow$ $Aut_A, Trust_A, Aut_B$ and $Trust_B$ accepted

- Suppose threshold $\eta = 0.4$ for *rejecting* a hypotheses

$\Rightarrow$ $Trust_D$ rejected

	A	B	C	D
$dsp(Aut_X)$	1	0.78	0.68	0.38
$dsp(\neg Aut_X)$	0	0.03	0.03	0.16
$dsp(Trust_X)$	1	0.89	0.66	0.27
$dsp(\neg Trust_X)$	0	0.01	0.05	0.41



Quantitative Approach

Computing **degrees of support** for
$Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

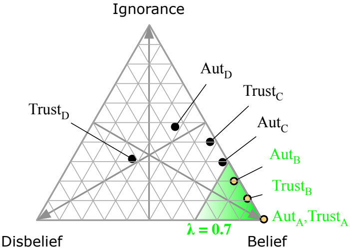
- Suppose threshold $\lambda = 0.7$ for *accepting* a hypotheses

$\Rightarrow$ $Aut_A, Trust_A, Aut_B$ and $Trust_B$ accepted

- Suppose threshold $\eta = 0.4$ for *rejecting* a hypotheses

$\Rightarrow$ $Trust_D$ rejected

	A	B	C	D
$dsp(Aut_X)$	1	0.78	0.68	0.38
$dsp(\neg Aut_X)$	0	0.03	0.03	0.16
$dsp(Trust_X)$	1	0.89	0.66	0.27
$dsp(\neg Trust_X)$	0	0.01	0.05	0.41



Quantitative Approach

Computing **degrees of support** for
$Aut_X, Trust_X, \neg Aut_X, \neg Trust_X$:

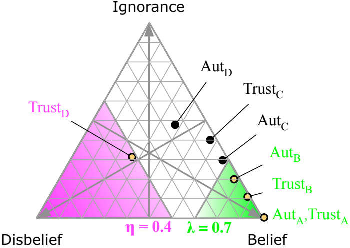
- Suppose threshold $\lambda = 0.7$ for *accepting* a hypotheses

$\Rightarrow$ $Aut_A, Trust_A, Aut_B$ and $Trust_B$ accepted

- Suppose threshold $\eta = 0.4$ for *rejecting* a hypotheses

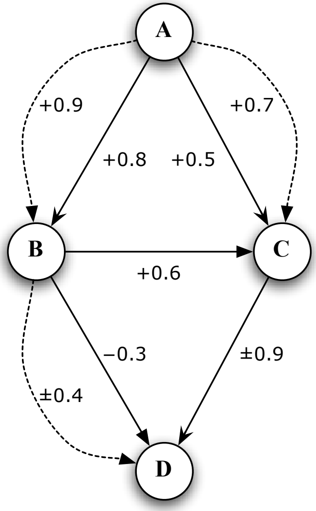
$\Rightarrow$ $Trust_D$ rejected

	A	B	C	D
$dsp(Aut_X)$	1	0.78	0.68	0.38
$dsp(\neg Aut_X)$	0	0.03	0.03	0.16
$dsp(Trust_X)$	1	0.89	0.66	0.27
$dsp(\neg Trust_X)$	0	0.01	0.05	0.41



Implementation

```
(users a b c d)
(owner a)
(cert a b 0.9)
(cert a c 0.5)
(cert b c 0.6)
(a-rate c d 0.9)
(rev b d 0.3)
(t-rate b c 0.6)
(rec a b 0.8)
(rec a c 0.7)
(t-rate b d 0.7)
(show-args)
(show-dsp)
```



http://www.iam.unibe.ch/∼run/trust.html

Outline

Conclusion

- Credential networks: new model for authenticity and trust evaluation
- A two-layer approach
- Allows gradual levels of trust and authenticity
- Evaluation is based on PAS
- A framework for specifying and evaluating credential networks has been implemented
  http://www.iam.unibe.ch/∼run/trust.html

Conclusion

Thank you.
Any questions?