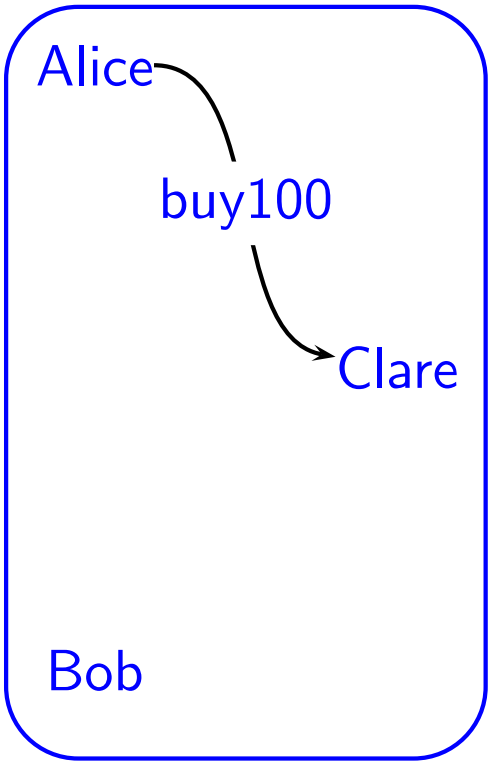
Noninterference Analysis of Delegation Subterfuge

Simon Foley Hongbin Zhou

June 30, 2006

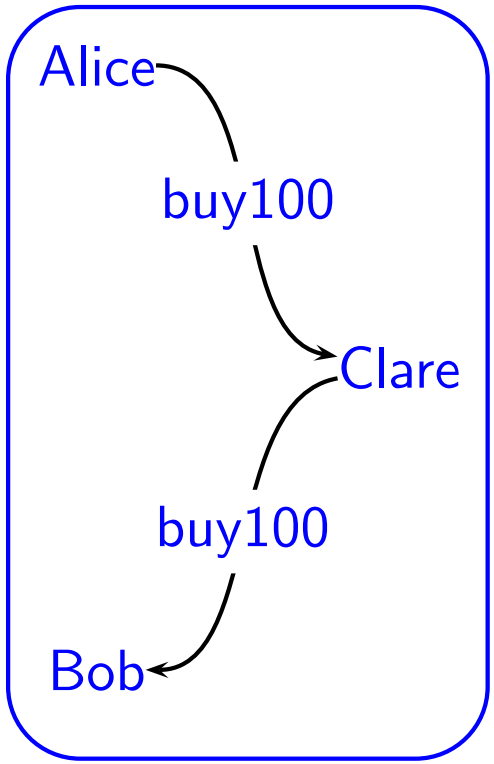
Delegation Subterfuge

Alice, Bob and Clare members of Blue coalition



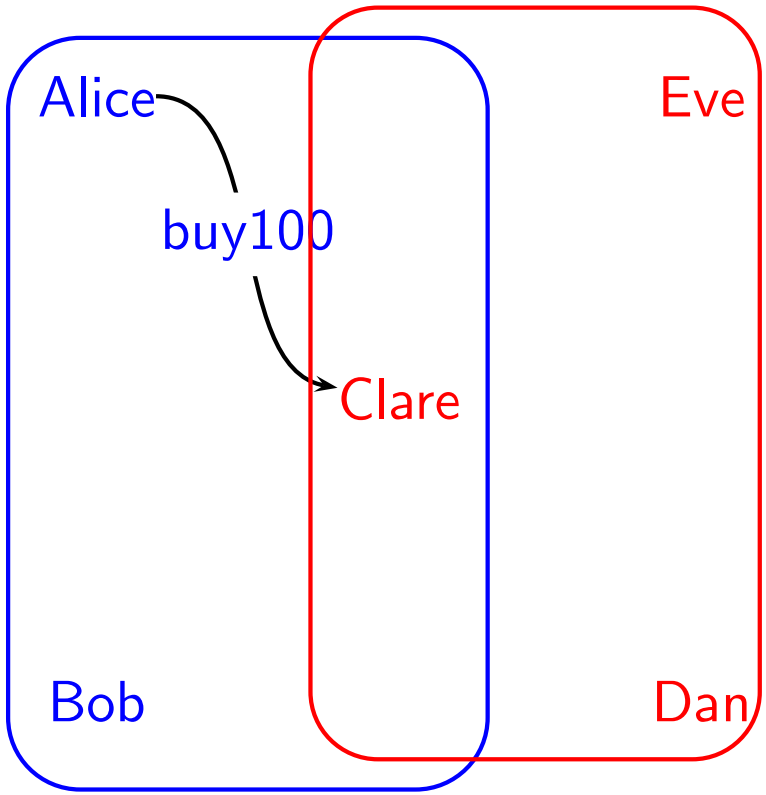
Delegation Subterfuge

By transitivity, Bob can prove authorization buy100 from Alice



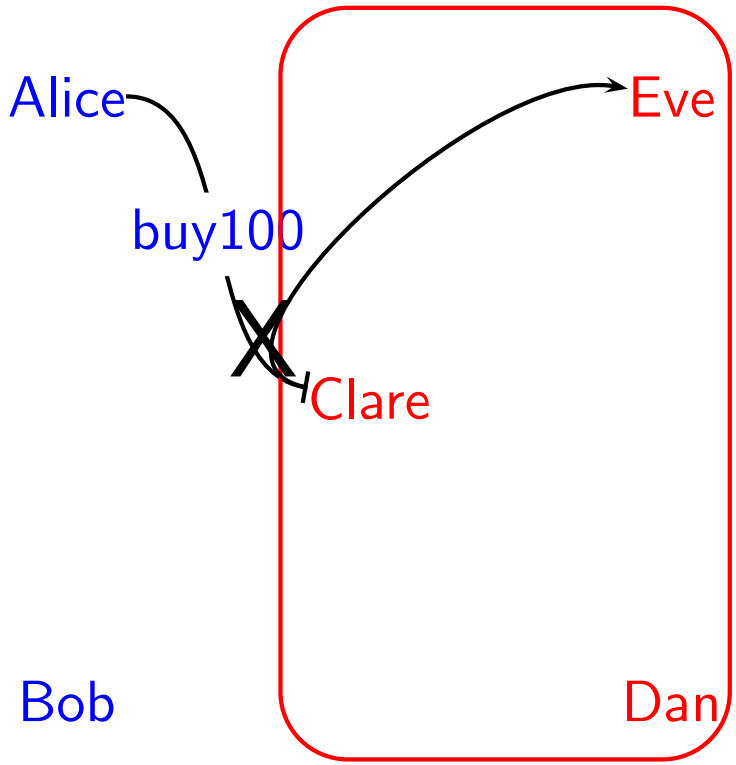
Delegation Subterfuge

Eve, Clare and Dan members of Red coalition



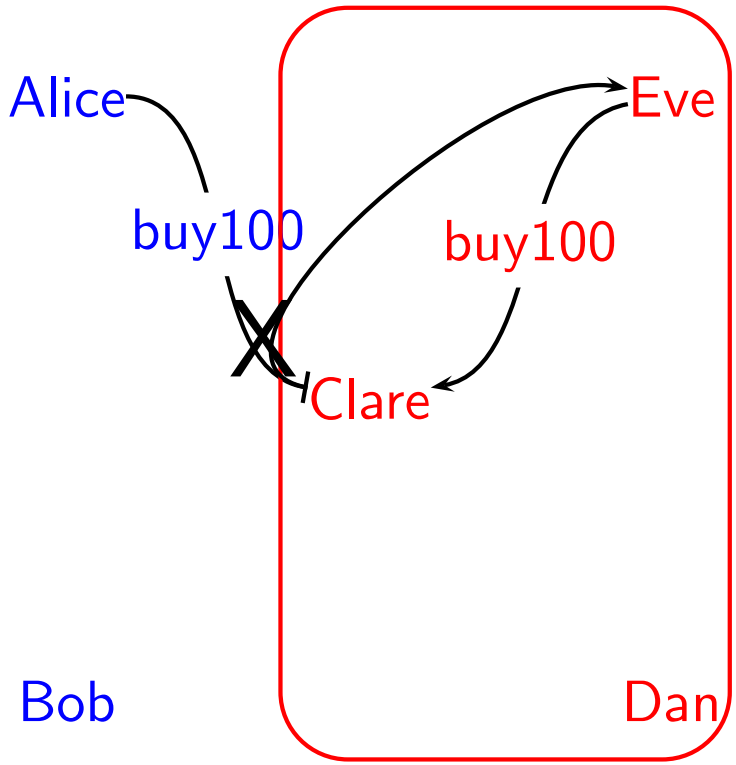
Delegation Subterfuge

Eve intercepts buy100 credential from Alice



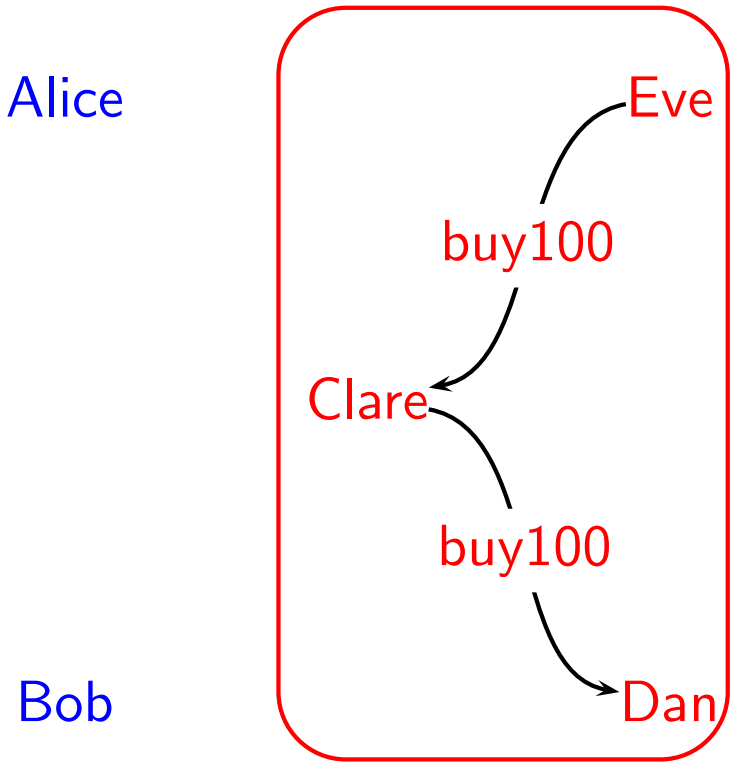
Delegation Subterfuge

Eve delegates buy100 to Clare



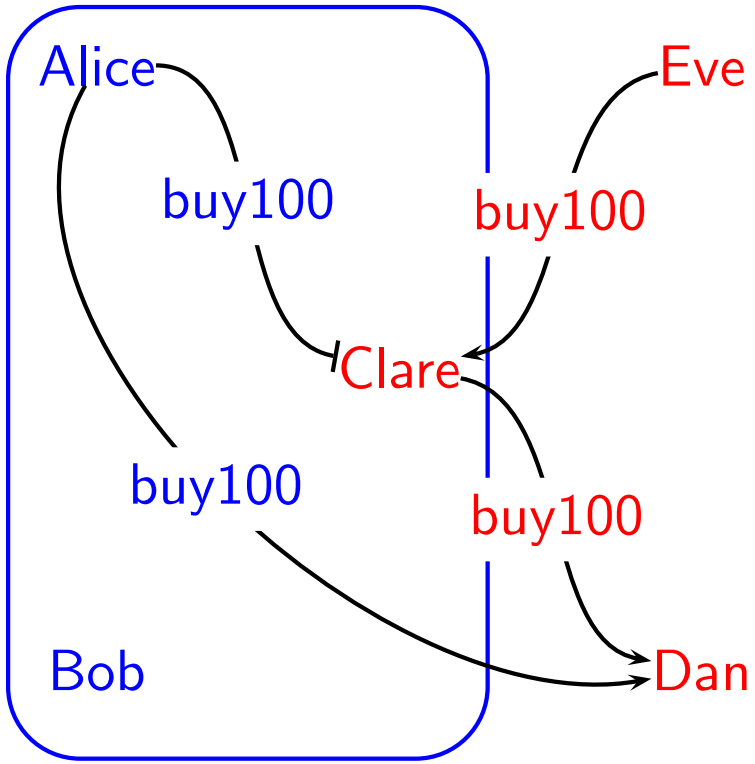
Delegation Subterfuge

Clare, thinking authorization is from Eve, delegates to Dan



Delegation Subterfuge

Surprise: Dan can prove authorization buy100 from Alice



Different public keys for different roles of user

$$K_A^{blue} \xrightarrow{\text{buy100}} K_C^{blue} \xrightarrow{\text{buy100}} K_B^{blue}$$

Ad-hoc Strategies to Avoid Delegation Subterfuge

Different public keys for different roles of user

$$K_A^{blue} \xrightarrow{\text{buy100}} K_C^{blue} \xrightarrow{\text{buy100}} K_B^{blue}$$

More precision in permission names

$$K_A \xrightarrow{\text{blue:buy100}} K_C \xrightarrow{\text{blue:buy100}} K_B$$

Ad-hoc Strategies to Avoid Delegation Subterfuge

Different public keys for different roles of user

$$K_A^{blue} \xrightarrow{\text{buy100}} K_C^{blue} \xrightarrow{\text{buy100}} K_B^{blue}$$

More precision in permission names

$$K_A \xrightarrow{\text{blue:buy100}} K_C \xrightarrow{\text{blue:buy100}} K_B$$

Public Keys as global identifiers

$$K_A \xrightarrow{K_A\text{:buy100}} K_C \xrightarrow{K_A\text{:buy100}} K_B$$

Ad-hoc Strategies to Avoid Delegation Subterfuge

Different public keys for different roles of user

$$K_A^{blue} \xrightarrow{\text{buy100}} K_C^{blue} \xrightarrow{\text{buy100}} K_B^{blue}$$

More precision in permission names

$$K_A \xrightarrow{\text{blue:buy100}} K_C \xrightarrow{\text{blue:buy100}} K_B$$

Public Keys as global identifiers

$$K_A \xrightarrow{K_A\text{:buy100}} K_C \xrightarrow{K_A\text{:buy100}} K_B$$

Use a subterfuge-safe delegation language

Distributed Authorization Language (DAL)

Ad-hoc Strategies to Avoid Delegation Subterfuge

Different public keys for different roles of user

$$K_A^{blue} \xrightarrow{\text{buy100}} K_C^{blue} \xrightarrow{\text{buy100}} K_B^{blue}$$

More precision in permission names

$$K_A \xrightarrow{\text{blue:buy100}} K_C \xrightarrow{\text{blue:buy100}} K_B$$

Public Keys as global identifiers

$$K_A \xrightarrow{K_A\text{:buy100}} K_C \xrightarrow{K_A\text{:buy100}} K_B$$

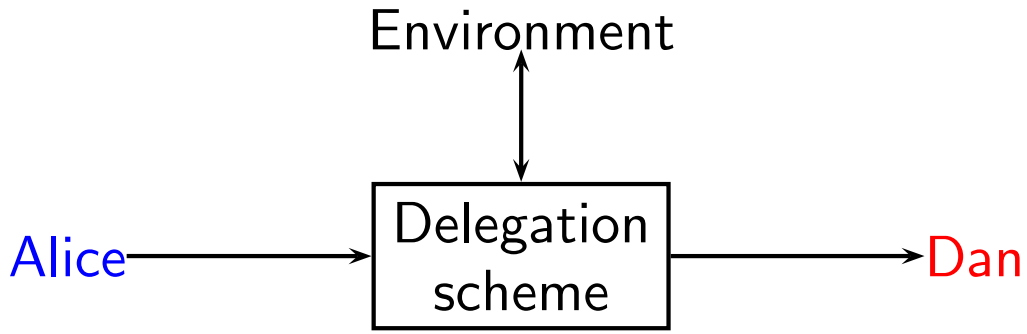
Use a subterfuge-safe delegation language

Distributed Authorization Language (DAL)

What *property* are these strategies intended to uphold?

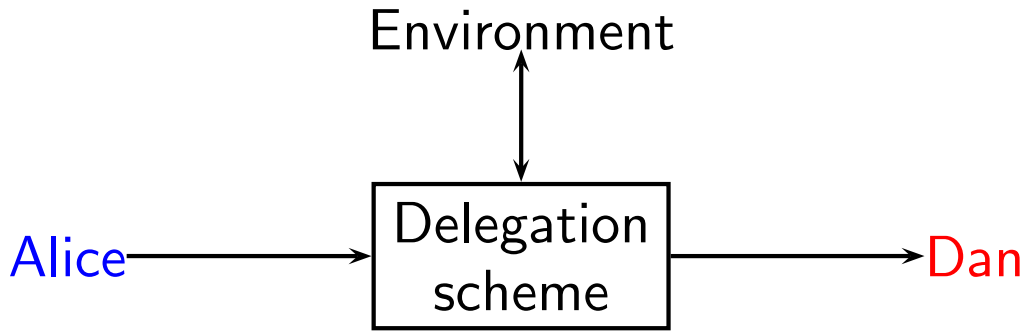
Analyzing Delegation Sugterfuge

Delegation scheme must be sufficiently robust to provide consistent delegation from Alice to Dan, regardless of 'threats' from the environment



Analyzing Delegation Sugterfuge

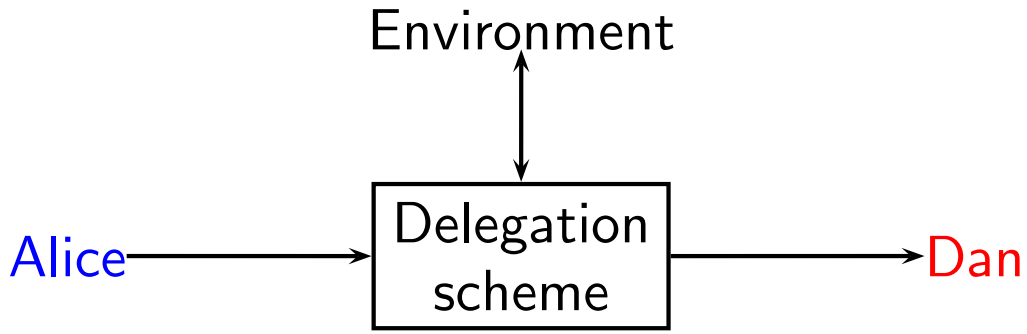
Delegation scheme must be sufficiently robust to provide consistent delegation from Alice to Dan, regardless of 'threats' from the environment



Security Protocol Analysis: can a malicious principal interfere with messages in a protocol?

Analyzing Delegation Sugterfuge

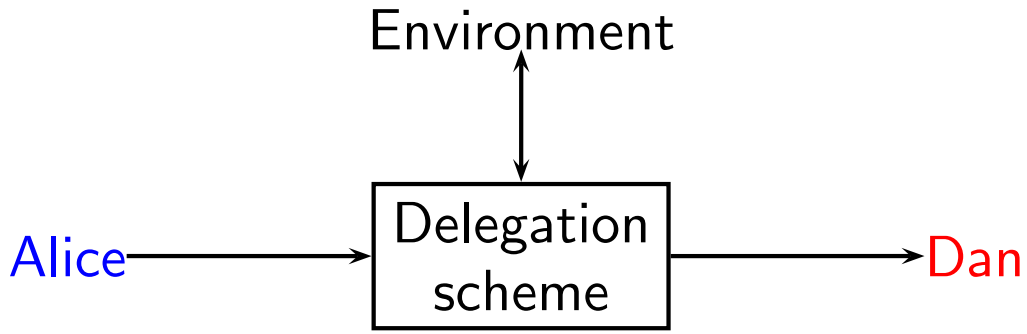
Delegation scheme must be sufficiently robust to provide consistent delegation from Alice to Dan, regardless of 'threats' from the environment



Noninterference Analysis: can a high user interfere with a low user view of the system?

Analyzing Delegation Sugterfuge

Delegation scheme must be sufficiently robust to provide consistent delegation from Alice to Dan, regardless of 'threats' from the environment



Subterfuge analysis: can a malicious principal interfere with a certificate chain and influence intended authorisation?

Defining Delegation

Authorization Veracity

Principal P originates permission x
P willing to be held accountable for actions authorized by x

Delegation Scheme of Coalition C

prefix-closed set $\delta(C)$ of all potential delegation sequences:

$\langle\rangle_x$: permission x understood by C
$\langle P\rangle_x$: principal P originates permission x
$\langle P, Q\rangle_x$: direct delegation of x from P to Q
$\langle P_0, P_1, \ldots P_n\rangle_x$: delegation chain.

Delegation Refinement

coalition C_2 preserves delegation scheme of coalition C_1:

$$C_1 \sqsubseteq C_2 \quad \equiv \quad \delta(C_2) \subseteq \delta(C_1)$$

References

1. S.N. Foley, H. Zhou. *Authorisation Subterfuge by Delegation in Decentralised Networks* In Proceedings of International Security Protocols Workshop, Cambridge UK. April, 2005. Springer LNCS
2. H. Zhou, S.N. Foley. *A Logic for Analysing Subterfuge in Delegation Chains*. Workshop on Formal Aspects in Security and Trust (FAST2005), Newcastle upon Tyne, UK. June 2005. Springer LNCS.
3. H. Zhou and S.N. Foley, *A Framework for Establishing Decentralized Secure Coalitions* Proceedings of IEEE Computer Security Foundations Workshop, Venice, July 2006, IEEE CS Press