# Delegation of Responsibility

Bruno Crispo
University of Cambridge

23 February 1999

# Changing Environment

- 2-party system → 3-party system
- Public Available → Public Offered
- Computer system security → Infrastructure policy +
  Service provider policy +
  Customer policy
- Trust Assumptions

# Problem

President delegates the power to sign certain documents on her behalf to her secretary.

The president announces the sacking of the secretary because of a mistake in a very important document. The secretary has signed the document in place of the president but she has not made a mistake.

How she can defend herself?

How she can build evidence to corroborate her innocence?

# Notation

- Principal: generic entity of the system.
- Grantor: principal that delegates.
- Grantee: principal that has been delegated.
- End-Point: principal where delegation is used.
- $A \rightarrow B \rightarrow C \rightarrow D \longrightarrow$ End-Point, B and C are intermediaries.

# Delegation of Responsibility

**Delegation of Rights:** process whereby a principal authorises an agent to act on her behalf, by transferring a set of rights to the agent, possibly for a specific period of time

Grantor is trusted

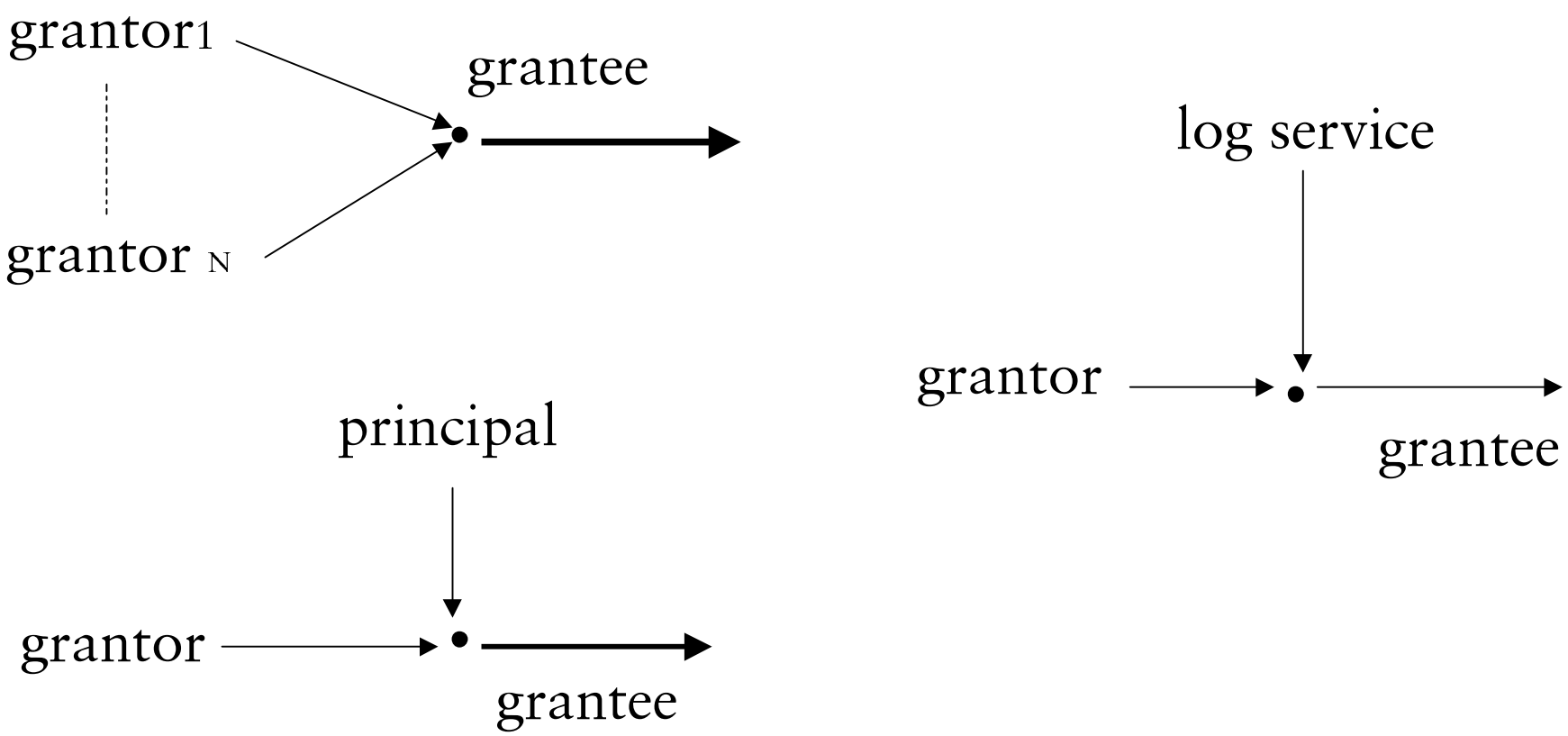
**Delegation of Responsibility:** process whereby a principal authorises an agent to act on her behalf, possibly for a specific period of time, during which it is always possible to distinguish whether a particular delegated task was performed by the principal or by the agent acting on her behalf.

Grantor is not trusted

# Delegation of Responsibility (cont'd)

| Delegation of Rights | Delegation of Responsibility |
| --- | --- |
| ⇓ | ⇓ |
| Trust | No Trust |
| ⇓ | ⇓ |
| shared responsibility | responsibility |
| only rights | and rights |
| ⇓ | ⇓ |
| no auditing | auditing |

# Other Semantics of Delegation



# Necessary Conditions to Delegate

- Right to Delegate.
- Freedom to choose the principal that will act as grantee.

# Taxonomy

| Type of delegation | Grantor | | Grantee | |
|---|---|---|---|---|
| | before | after | before | after |
| Rights G | G | G | ∅ | G |
| Partial Right G' | G' | G' | G'' | G'''=G'∪ G'' |
| Responsibility R | R | ∅ | ∅ or G | R or R + G |
| Responsibility and Rights R+G | R + G | ∅ or G | ∅ | R + G |
| Responsibility and Partial Rights R + G' | R + G' | ∅ or G' | G'' | R + G'''<br>G'''= G'∪G'' |

# Capability (1)

- Free Propagation: capability can be freely propagated in the system through principals.
- Free Access: whoever possess the capability can use the rights bound to this capability.

# Capability

- SCAP [Karger 1988]
- Amoeba [Mullender 1985]
- ICAP [Gong 1990]
- Limitations:
  - Extended TCB and no use of cryptography.
  - Client-Server-Client instead of Client-Client.
  - Security policy dictated and enforced by the infrastructure.

# Delegation Token (1)

[Sollins “Cascaded Authentication” IEEE SSP 1988]

[Gasser and McDermott “An Architecture for Practical Delegation in a Distributed System” IEEE SSP 1990]

[Varadharajan et.al. “An Analysis of the Proxy Problem in Distributed System” IEEE SSP 1991]

[Neuman “Proxy-Based Authorization and Accounting for Distributed System” CDS 1993]

$$\{Grantor, Grantee, Rights, Validity, Others\}_{K Grantor}$$

Delegation key

# Delegation Token (2)

- Problems:
  - Trustworthy intermediaries.
  - Chains of delegation.
  - Grantors are trusted:
    - not to abuse their power to delegate.
    - not to abuse their knowledge of delegation keys.
  - Grantees are trusted:
    - not to abuse the delegated rights.

# Untrusted Grantee

[Abadi,Burrows,Kaufman,Lampson "Authentication and Delegation with Smart-Cards" TR. 67 1992]

[Abadi, Burrows,Lamspon,Plotkin "A Calculus for Access Control in Distributed Systems" ACM ToPLaS 1993]

[Lampson, Abadi,Burrows, Wobber "Authentication in Distributed Systems: Theory and Practice" ACM ToCS 1992]

- Auditing: detecting grantee's misbehaviors.

$A \rightarrow B$ A

B

(B for A)

# Principle of Consent

[Abadi,Burrows,Kaufman,Lampson "Authentication and Delegation with Smart-Cards" TR. 67 1992]

[Abadi, Burrows,Lamspon,Plotkin "A Calculus for Access Control in Distributed Systems" ACM ToPLaS 1993]

[Lampson, Abadi,Burrows, Wobber "Authentication in Distributed Systems: Theory and Practice" ACM ToCS 1992]

- *PoC: Delegated rights must always be explicitly accepted by the grantee.*
- Grantor and grantee share responsibilities for the delegated rights.

# Delegation of Responsibility

- Self-Authenticating Proxy

[Low, Christianson “Self Authenticating Proxies” IEE EE 1994]

[Low, Christianson “A Technique for Authentication, Access Control and Resource Management in Open Distributed Systems” IEE EE 1994]

- Cryptographic Solution

[Mambo et al. “Proxy Signatures: Delegation of the Power to Sign Messages” IEICE 1996]

[Kim et al. “Proxy Signatures Revisited” ICICS 1997]

# Delegation Protocol

M=" G wishes to delegate to g $\Omega$ using $K^{+}_{G_{R\_t\_D}}$ "

1. G $\rightarrow$ g: M, $SIG(\mathrm{M}, K_G{}^{-})$

M′=" g accepts $\Omega$ using $K^{+}_{g_{R\_t\_A}}$ and exercise $\Omega$ using $K^{+}_{g_{R\_t\_E}}$ "

2. g $\rightarrow$ G: M′, $SIG(\mathrm{M}', K^{-}_{g})$

M″=" g, G, $\Omega$, $K^{+}_{G_{R\_t\_D}}, K^{+}_{g_{R\_t\_E}}, K^{+}_{g_{R\_t\_A}}$ "

3. G $\rightarrow$ g: T = M″, $SIG(\mathrm{M}'', K^{-}_{G_{R\_t\_D}})$

4. g then signs T producing the delegation token: T, $SIG(\mathrm{T}, K^{-}_{g_{R\_t\_A}})$

# Logic of Delegation

- Need of formalism to analyse delegation protocols.

[Abadi, Burrows,Lamspon,Plotkin "A Calculus for Access Control in Distributed Systems" ACM ToPLaS 1993]

- Cannot express the difference between the two semantics
- Not general
- No distinction between *active* and *passive* entities

# Future Work

- Interactions between these semantics of delegation with those defined in other areas (e.g., Object-oriented)
- Formal approach
- Implementation of auditing mechanisms
- *Principle of the least trust*