Unità di Pescara
“Tecniche di Astrazione, Concorrenza e Vincoli (Soft) per Sicurezza Informatica”

PRIN

“Vincoli e preferenze come formalismo unificante per l'analisi di sistemi informatici e la soluzione di problemi reali”

Componenti Unità

- Stefano Bistarelli (resp)
  - Vincoli soft, security
- Gianluca Amato
  - astrazione
- Fabio Fioravanti
  - CLP, security
- MariaChiara Meo
  - Concorrenza, (temporal) cc
- Pamela Peretti
  - Security and economics
- Francesco Santini
  - Constraints, networking and QoS
- Donatella Gubiani
  - (Unità di Udine)

Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)

Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)

Astrazione per analisi di protocolli di sicurezza

- Controllo del flusso di esecuzione:
  - Partizionare i dati in classi di sicurezza
  - Controllare che non vi siano flussi di informazioni tra le classi
- Metodi per effettuare il controllo:
  - Type system
  - Interpretazione astratta

Interpretazione astratta

- Data una funzione semantica F sul dominio C:
  - Sostituisco a C un dominio astratto A
  - Calcolo F sul dominio A
  - Se A è scelto opportunamente, il calcolo termina
- Dato A, come ottenere altri domini più o meno precisi?
  - Operatori di raffinamento
  - Diversi operatori garantiscono diverse proprietà del dominio risultante (e quindi dell'analisi)

Raffinamenti e sicurezza

- Due fasi:

  1. studiare l'efficacia dei protocolli di raffinamento già noti per l'analisi dei protocolli di sicurezza;
  2. sviluppare nuovi operatori di raffinamento.

- Necessità di scegliere un framework di riferimento per la specifica dei protocolli:
  - Spi-calcolo?
  - (temporal/soft) cc?

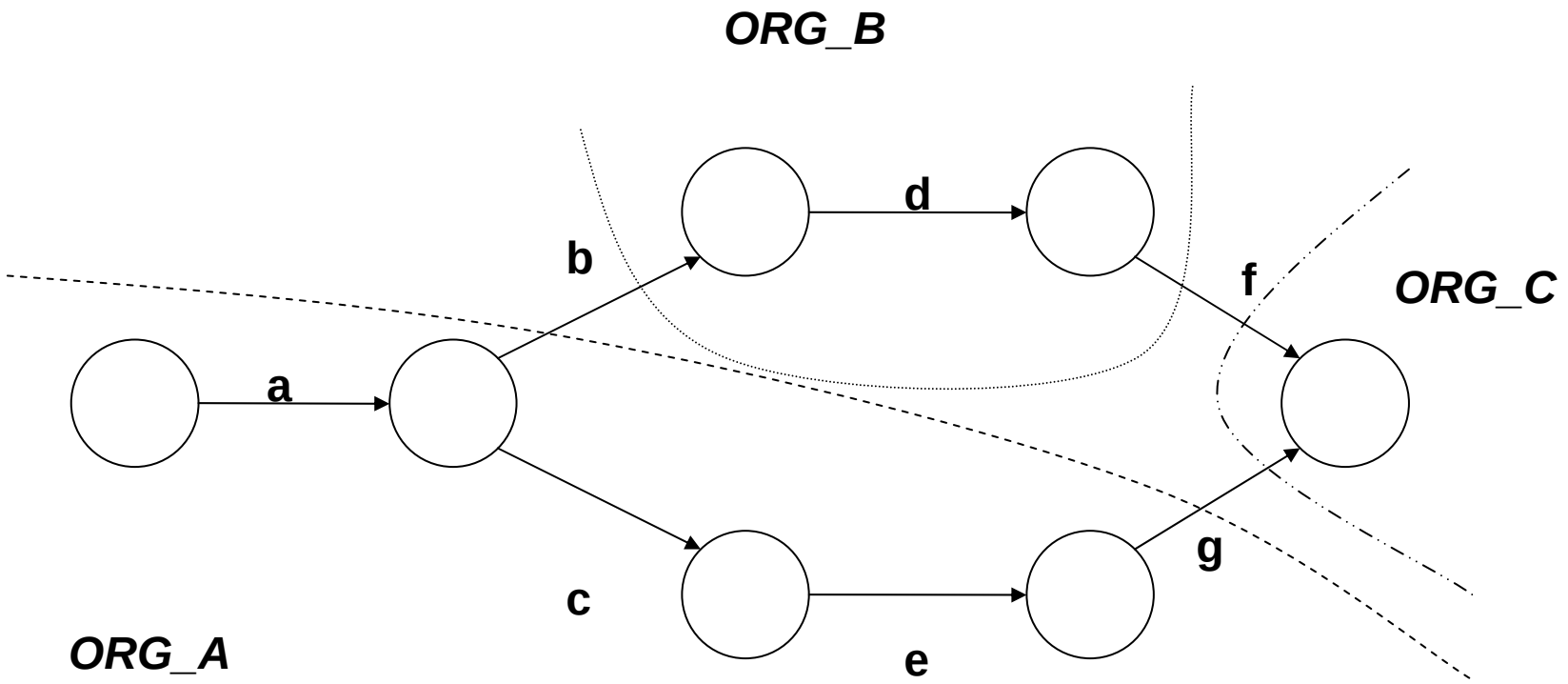
Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)

Controllo degli accessi su workflow inter-organizzativi

- Usare workflow (o altri formalismi) per specificare l'interazione e la composizione di servizi su rete tra organizzazioni diverse.
- Usare (programmazione logica con) **vincoli per specificare i workflow** (vincoli temporali, contenuto dei messaggi scambiati, relazioni input/output dei task).
- La specifica, condivisa e partecipata, serve da "**contratto**" tra le organizzazioni partecipanti sulle modalità di interazione.

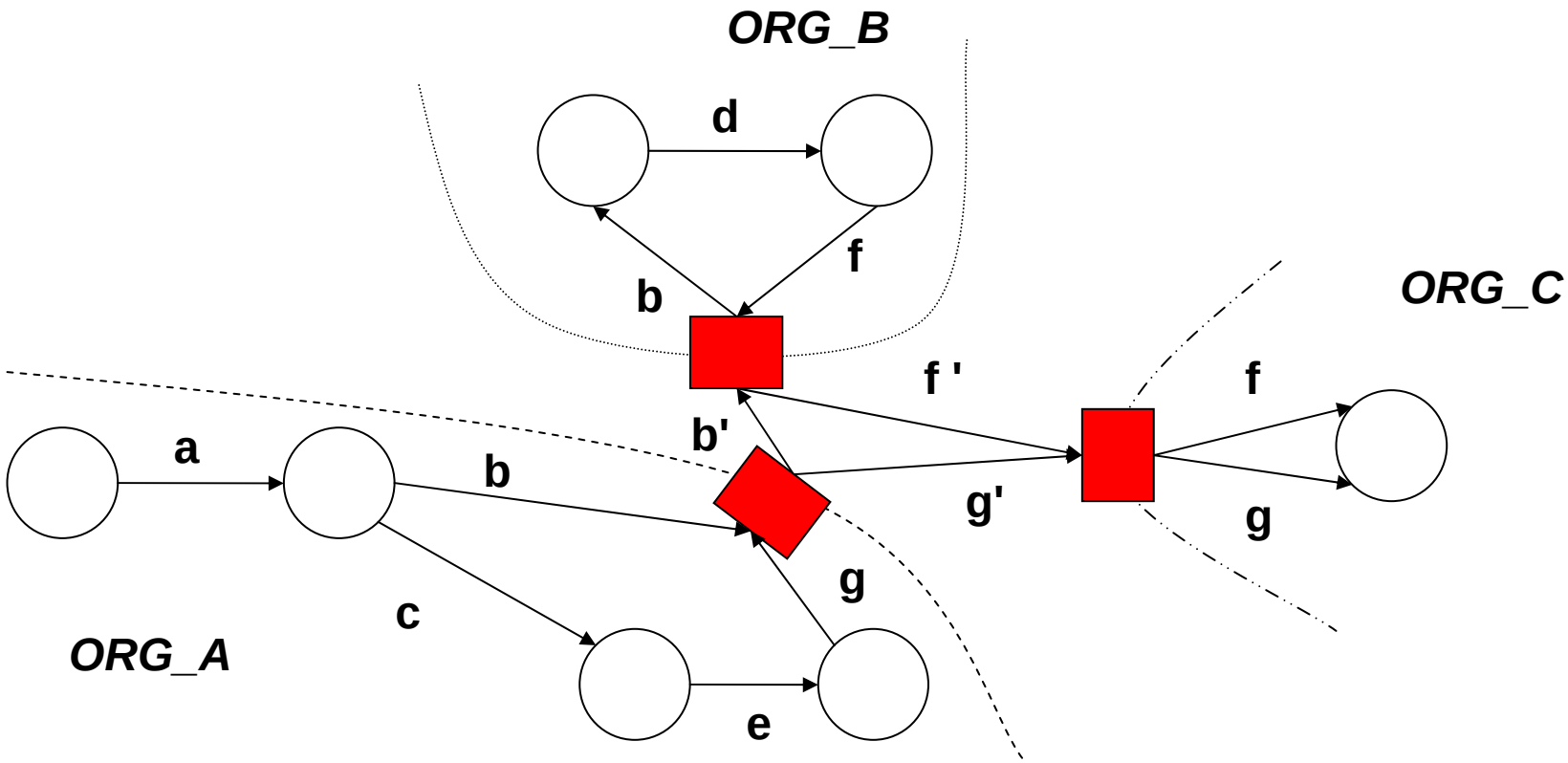
Workflow inter-organizzativo



Controllo degli accessi su workflow inter-organizzativi

- Dalla specifica del comportamento “globale”, si vuole **generare**, per ciascuna organizzazione, una **specifica del comportamento “locale”** necessario al completamento del workflow.
- La specifica generata dovrebbe essere **eseguibile**, e permettere il transito del solo traffico necessario al completamento del workflow.
- Questo permetterebbe la creazione di **proxy** **per filtrare il traffico** derivante dalla partecipazione in un determinato workflow.
- Analogia Web Services: from “choreography” to “orchestration”.
- Analogia distributed constraint solving (?).

Workflow inter-organizzativo con proxy



Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)

Estensione framework Soft CSPs (operatore di divisione ')

- Semiring <A,+ §, 0, 1> esteso per uso algoritmi di consistenza locale quando § non idempotente
- Strettamente connesso ad algoritmi per risoluzione di vincoli con preferenze positive/negative
  - $a \S (b^{-1}) = a \mathbin{'} b$
- Utilizza residuation theory per calcolare una approssimazione dell'equazione
  - b § x = a
  - $a \mathbin{'} b = \max \{x \in A \mid b \S x \leq a\}$
  - senza aggiungere nuovi elementi all'insieme (e.s. senza symmetrization/completion/localization per aggiunta preferenze positive)

Local consistency per times non idempotente

Definition 1 (local consistency rule) *A* local consistency rule *involving a constraint c and a unary constraint c_x with $supp(c_x) = \{x\} \subset supp(c)$ consists of the following phases*

- *the substitution of the original constraint c_x with c'_x computed as usual [?]*

$$c'_x = c_x \otimes (c \Downarrow_x)$$

- *the modification of the constraint c in a new constraint c' that takes into account the changes performed on c_x (Since constraint c_x is combined with $c \Downarrow_x$, c' is divided by the same value)*

$$c' = c \oslash (c \Downarrow_x),$$

compensation

where the constraint division function $\oslash : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ is defined as $(c_1 \oslash c_2)\eta = c_1\eta \div c_2\eta$.

subtraction

- a - b = glb {x ma ‰ b + x}.
- Operatore estende differenza insiemistica per passare da CDB a soft CDB
- … ancora brain storming ☹
  - Barbara Catania
  - Barry O'Sullivan
  - Nic Wilson

Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)

(temporal) cc e QoS

- Uso di (temporal) cc per specifica protocolli comunicazione (sicurezza)
- Estensione del formalismo a vincoli soft per rappresentare nozioni di QoS
- Studio di algoritmi su DisCSPs per implementazione politiche di QoS
- Suggestions??

Attività

- Astrazione per analisi di protocolli di sicurezza
- CLP per controllo degli accessi su workflow inter-organizzativi
- Estensione framework Soft CSPs
  - preferenze positive/negative (PD)
  - divisione [BG2006]
  - Sottrazione e Soft CDB
- Temporal (soft) cc
  - Definizione del framework
  - Applicazione a protocolli di comunicazione e QoS
- Analisi quantitativa della sicurezza
  - Economics and Security
  - Protocolli (livelli di autenticazione, post-mortem protocols, retaliation, protocolli doppio goal)
  - Secure interoperation (cascading paths as soft constraint problems, minima riduzione di diritti/collegamenti per mantenere policy, studio su speciali tipologie di rete: small world)