MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA
DIREZIONE GENERALE DELLA RICERCA
PROGRAMMI DI RICERCA SCIENTIFICA DI RILEVANTE INTERESSE NAZIONALE
RICHIESTA DI COFINANZIAMENTO (DM n. 1407 del 4 dicembre 2008)

PROGETTO DI UNITÀ DI RICERCA - MODELLO B
Anno 2008 - prot. 20084JE75C_004

1 - Area Scientifico-disciplinare

01: Scienze matematiche e informatiche 100%

2 - Coordinatore Scientifico

BRUNI *ROBERTO*

Ricercatore confermato

Università degli Studi di PISA

Facoltà di SCIENZE MATEMATICHE FISICHE e NATURALI

Dipartimento di INFORMATICA

3 - Responsabile dell'Unità di Ricerca

BUGLIESI	*MICHELE*	
Professore Straordinario	*31/05/1962*	*BGLMHL62E31L483K*
Università "Ca' Foscari" di VENEZIA		
Dipartimento di INFORMATICA		
041-2348437 *(Prefisso e telefono)*	*041-2348419* *(Numero fax)*	*michele@dsi.unive.it*

4 - Curriculum scientifico

Testo italiano
Michele Bugliesi è Professore Staordinario di Informatica all'Università di Venezia "Ca' Foscari" da Novembew 2006, ed è stato professore associato da Settembre 2000. In passato è stato Ricercatore Confermato all'Università di Padova, (Dicembre 1992 - Ottobre 1998), e di Venezia (Novembre 1998 - Agosto 2000). Ha avuto posizioni di visiting researcher all'università del Sussex (Maggio 2003 e Agosto 2004), è stato professore invitato all'Ecole Normale Superieure di Parigi (Febbraio 2000), e visiting lecturer a Boston University (Gennaio - Maggio 1999).

Michele Bugliesi ha preso parte a numerosi progetti di ricerca finanziati dai principali enti italiani e internazionali, tra cui la Comunità Europea, la NSF statunitense, e il Ministero Italiano dell'Università e Ricerca. È coordinatore nazionale del progetto ``Fondamenti Logici dei Sistemi Distribuiti e Codice Mobile" finanziato dal MIUR (contratto n. 2005015785), ed è stato coordinatore scientifico dell'unità di Venezia per il Progetto MyThS (FET-GC IST-2001-32617) finanziato dalla Comunità Europea per gli anni 2002-2005 (siti: ENS Paris, Univ. of Venice, Univ. of Sussex).

Negli ultimi anni è stato coinvolto come membro dei comitati di programma delle seguenti conferenze: COMPSAC'09, FCS'09, ESOP'09, ESOP´06, FOSSACS'05, EXPRESS'05, FMOODS'05, FCS'04, CSFW'03, FMOODS'03. Nell'anno 2006 è stato General Chair per ICALP'06. Dal 2005 al 2008 è stato membro dello Steering Committee del Workshop FOOL (Foundations of Object-Oriented Languages), e membro del Consiglio Direttivo del Capitolo Italiano dell´EATCS.

Bugliesi è autore di più di sessanta articoli in riviste e conferenze internazionali.
Recentemente, le sue ricerche si sono incentrate su sistemi concorrenti distribuiti. In tale ambito ha sviluppato teorie di tipi avanzate per l'analisi di protocolli di autenticazione (di messaggi ed entità) e metodi per l'analisi di protocolli di fair exchange basati su teorie algebriche di equivalenza Nell'ambito della programmazione mobile e distribuita, ha ideato, in collaborazione con altri autori, il calcolo dei Boxed Ambients, ampiamente citato in letteratura. In una serie di lavori ha studiato i fondamenti semantici e teorie di tipi per questo calcolo, sviluppando sistemi di tipi per l'analisi del controllo degli accessi alle risorse ed il flusso di informazione.

In passato le sue ricerche si sono focalizzate sullo studio dei fondamenti semantici delle estensioni di linguaggi dichiarativi con costrutti per la modularità, e su teorie di tipi e calcoli fondazionali per sistemi orientati agli oggetti. In una serie di lavori ha studiato teorie di tipo per calcoli ad oggetti con primitive per l'estensione di oggetti mediante l'aggiunta di metodi. Tra i risultati di tali ricerche rcordiamo i seguenti: (i) la caratterizzazione di sistemi di tipi per oggetti estensibili basati su row-polimorfismo in termini di polimorfismo match bounded; (ii) la prima definizione in letteratura di una interpretazione di oggetti estensibili in lambda calcolo di ordine superiore che preserva la relazione di sottotipo e soddisfa la proprietà di adeguatezza computazionale; (iii)
lo sviluppo di un algoritmo di inferenza di complessità O(n^3) per un sistema di tipo del primo ordine per un calcolo ad oggetti con relazione di sottotipo variante: il sistema generalizza tutti i sistemi di tipo della stessa classe presenti in letteratura.

Testo inglese

Michele Bugliesi is Professor of Computer Science at the University of Venice "Ca' Foscari" since November 2006, and has been Associate Professor since Sept 2000. Previously, he has been tenured researcher in Computer Science at the University of Padova (Dec 1992 - Oct 1998), and Venice (Nov 1998 - Aug 2000). He has held research/teaching positions at the University of Sussex (May 2003, August 2004), Ecole Normale Superieure in Paris (Feb 2000), and Boston University (Jan - May 1999).

Michele Bugliesi has partecipated in several research projects, funded by major national and international funding agencies among which EU, NSF, and the Italian Ministry of Scientific and Technological Research (formerly MURST). He has coordinated the Project ``Logical Foundations of Distributed Systems and Mobile Code´´ (MiUR project n. 2005015785) funded by the Italian Ministry of University and Research, has been the Scientific Coordinator of the Venice site of Project MyThS (FET-GC IST-2001-32617) funded by EU (years 2002-2005, sites: ENS Paris, Univ of Venice, Univ of Sussex).

Recently, he has served as program committee member for the following international conferences and workshops: COMPSAC 2009, FCS'09, ESOP'09, ESOP´06, EXPRESS'06, FOSSACS'05, FMOODS'05, FCS'04, CSFW'03, FMOODS'03. In 2006 he served as General Chair for ICALP'06. From Jan 2005 to Jan 2008 he has been member of the Steering Committee of the FOOL Workshop series (Foundations of Object-Oriented Languages). He is currently member of the Council of the Italian Chapter of EATCS.

He is the (co-) author of over sixty articles in international journals and conferences. His current research is centered on formal calculi for concurrent distributed systems, and the study of their implementation. He co-developed advanced typed theories for the analysis of entity and message authentication and of behavioral theories for the analysis of fair exchange. He is the co-inventor of the calculus of Boxed Ambients which has been highly influential in the area: in a series of papers he co-developed typed theories for access control and information flow, as well as the semantic foundations for this calculus.
His past research has focused on the semantics of modular extension of declarative languages, and typed theoretical calculi for object-oriented systems. He co-developed an O(n^3) inference algorithm for a first-order object-type system with variant subtyping that generalises all previous first-order object-types systems in the literature. In a series of papers he studied the typed foundations for object-calculi with primitives for object extension by way of method addition. The first result of this line of research was a characterisation of row-polymorphism in terms of match-bounded polymorphism. Based on that, he co-developed the first subtype preserving and computationally adequate interpretation of extensible objects into a higher-order lambda-calculus with polymorphic types, recursive types and subtyping.

5 - Pubblicazioni scientifiche più significative del Responsabile dell'Unità di Ricerca

1. *BUGLIESI M., FOCARDI, R (2008). Language Based Secure Communication. In: CSF 2008 - 21st IEEE Symposium on Computer Security Foundations. Pittsburg, 23 - 25 June 2008IEEE Computer Society, p. 3-16, ISBN/ISSN: ISBN 978-0-7695-3182-3*
2. *BARBANERA F, BUGLIESI M., DEZANI-CIANCAGLINI M, SASSONE V (2007). Space-aware ambients and processes. THEORETICAL COMPUTER SCIENCE, vol. 373(1-2); p. 41-69, ISSN: 0304-3975*
3. *BUGLIESI M., D. MACEDONIO, S. ROSSI (2007). Static vs Dynamic Typing for Access Control in Pi-Calculus. In: ASIAN07 Computer and Network Security, 12th Asian Computing Science Conference. Doha, Qatar, December 9-11, 2007Springer--Verlag, vol. 4846 of LNCS, p. 282-296, ISBN/ISSN: 978-3-540-76927-9*
4. *BUGLIESI M., GIUNTI M (2007). Secure implementations of typed channel abstractions. POPL 2007. p. 251-262ACM Press, ISBN/ISSN: ISBN 1-59593-575-4*
5. *BUGLIESI M., RICCARDO FOCARDI, MATTEO MAFFEI (2007). Dynamic types for authentication. JOURNAL OF COMPUTER SECURITY, vol. 15(6); p. 563-617, ISSN: 0926-227X*
6. *BUGLIESI M., CRAFA S, MERRO M, SASSONE V (2005). Communication and Mobility Control in Boxed Ambients. INFORMATION AND COMPUTATION, vol. 202 (1); p. 39-86, ISSN: 0890-5401*
7. *BUGLIESI M., FOCARDI R, MAFFEI M (2005). Analysis of Typed Analyses of Authentication Protocols. In: CSFW 2005 - Computer Security Foundation Workshop. Aix-en-Provence, France}, 20-22 June 2005IEEE, p. 112-125*
8. *BUGLIESI M., GIUNTI M (2005). Typed Processes in Untyped Contexts. In: Trustworthy Global Computing, International Symposium, TGC 2005. Edinburgh, UK,, April 7-9, 2005SPRINGER-VERLAG, vol. LNCS 3705, p. 19-32, ISBN/ISSN: 3-540-30007-4*
9. *BUGLIESI M., ROSSI S. (2005). Non Interference Proof Techniques for the Analysis of Cryptographic Protocols. JOURNAL OF COMPUTER SECURITY, vol. 13; p. 83-113, ISSN: 0926-227X*
10. *BUGLIESI M., CASTAGNA G., CRAFA S. (2004). Access Control for Mobile Agents: the Calculus of Boxed Ambients. ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, vol. 26; p. 57-124, ISSN: 0164-0925*
11. *BUGLIESI M., RICCARDO FOCARDI, MATTEO MAFFEI (2004). Authenticity by tagging and typing. In: FMSE. Washingtion, DC, USA, October 2004ACM, p. 1-12, ISBN/ISSN: 1-58113-971-3*
12. *BUGLIESI M., RICCARDO FOCARDI, MATTEO MAFFEI (2004). Compositional Analysis of Authentication Protocols. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2986; p. 140-154, ISSN: 0302-9743*
13. *BUGLIESI M., AMBRA CECCATO, SABINA ROSSI (2003). Context-Sensitive Equivalences for Non-interference Based Protocol Analysis. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2751; p. 364-375, ISSN: 0302-9743*
14. *BUGLIESI M., CRAFA S, PRELIC A, SASSONE V (2003). Secrecy in Untrusted Networks. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2719; p. 969-983, ISSN: 0302-9743*
15. *BUGLIESI M., RICCARDO FOCARDI, MATTEO MAFFEI (2003). Principles for Entity Authentication. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2890; p. 294-306, ISSN: 0302-9743*
16. *BONO V., BUGLIESI M., CRAFA S. (2002). Typed Interpretations of Extensible Objects. ACM TRANSACTIONS ON COMPUTATIONAL LOGIC, vol. 3(4); p. 562-603, ISSN: 1529-3785*
17. *BUGLIESI M., GIUSEPPE CASTAGNA, SILVIA CRAFA, RICCARDO FOCARDI, VLADIMIRO SASSONE (2002). A Survey of Name-Passing Calculi and Crypto-Primitives. In: RICCARDO FOCARDI; ROBERTO GORRIERI EDITORS. Foundations of Security Analysis and Design II, FOSAD 2001/2002 Tutorial Lectures. vol. 2946 of LNCS, Springer, ISBN/ISSN: 3-540-20955-7*
18. *BUGLIESI M., PERICAS-G S. (2002). Type Inference for Variant Object Types. INFORMATION AND COMPUTATION, vol. 177(1); p. 2-27, ISSN: 0890-5401*
19. *CASTAGNA G, BUGLIESI M. (2002). Behavioural typing for safe ambients. COMPUTER LANGUAGES, vol. 28(1); p. 62-99, ISSN: 0096-0551*
20. *SILVIA CRAFA, BUGLIESI M., GIUSEPPE CASTAGNA (2002). Information Flow Security for Boxed Ambients. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 66(1), ISSN: 1571-0661*
21. *BUGLIESI M., CASTAGNA G, CRAFA S (2001). Boxed Ambients. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2215; p. 38-63, ISSN: 0302-9743*
22. *BUGLIESI M., CASTAGNA G. (2001). Secure Safe Ambients. In: 28th ACM Symp. on Principles of Progrogramming Languages, Boston, Jan. 2001, p. 222-235*
23. *BUGLIESI M., DELZANNO G, LIQUORI L, MARTELLI M (2000). Object Calculi in Linear Logic. JOURNAL OF LOGIC AND COMPUTATION, vol. 10(1); p. 75-104, ISSN: 0955-792X*

6 - Elenco dei partecipanti all'Unità di Ricerca

6.1 - Componenti

Componenti della sede dell'Unità di Ricerca

nº	Cognome	Nome	Università/Ente	Qualifica	Disponibilità temporale indicativa prevista	
					1° anno	2° anno
1.	*BUGLIESI*	*Michele*	*Università "Ca' Foscari" di VENEZIA*	*Professore Straordinario*	*6*	*4*
2.	*ROSSI*	*Sabina*	*Università "Ca' Foscari" di VENEZIA*	*Ricercatore confermato*	*4*	*4*
	TOTALE				**10**	**8**

Componenti di altre Università / Enti vigilati

Nessuno

Titolari di assegni di ricerca

nº	Cognome	Nome	Università/Ente	Disponibilità temporale indicativa prevista	
				1° anno	2° anno
1.	*MACEDONIO*	*Damiano*	*Università "Ca' Foscari" di VENEZIA*	*7*	*2*
	TOTALE			**7**	**2**

Titolari di borse

nº	Cognome	Nome	Università/Ente	Qualifica	Disponibilità temporale indicativa prevista	
					1° anno	2° anno
1.	*MODESTI*	*Paolo*	*Università "Ca' Foscari" di VENEZIA*	*Dottorando*	*4*	*4*
	TOTALE				**4**	**4**

6.1 bis Vice-responsabile

6.2 - Altro personale

Nessuno

6.3 - Personale a contratto da destinare a questo specifico Progetto

nº	Tipologia di contratto	Costo previsto	Disponibilità temporale indicativa prevista		Note
			1° anno	2° anno	
1.	*Assegnista*	*22.000*	*2*	*10*	
	TOTALE	**22.000**	**2**	**10**	

6.4 - Dottorati a carico del PRIN da destinare a questo specifico Progetto

Nessuno

7 - Titolo specifico del Progetto svolto dall'Unità di Ricerca

Testo italiano
Sicurezza per Applicazioni Distribuite in Sistemi Aperti

Testo inglese
Securing distributed applications in open-ended systems

8 - Abstract del Progetto svolto dall'Unità di Ricerca

Testo italiano
Programmare applicazioni distribuite e' un compito complesso a causa della natura dinamica e spesso inaffidabile dell'ambiente che le ospita.

I linguaggi di specifica moderni forniscono delle astrazioni che consentono di strutturare il progetto dell'applicazione in un insieme pre-definito di patterns che regolano l'interazione tra le diverse componenti distribuite. Questi patterns, detti contratti o sessioni in letteratura, rendono possibile specificare l'intero flusso di esecuzione in una applicazione a piu' componenti e, basandosi su cio', codificare ogni componente mediante istruzioni che la forzano a seguire il comportamento specificato dalla descrizione del contrattostesso. Fintantoche' tutte le componenti sono note a priori e ci si puo' fidare che rispettano i rispettivi ruoli, questo metodo di specifica funziona molto bene e produce strumenti potenti per la progettazione e la verifica statica.

Nei sistemi aperti, questa tecnica e' meno efficace per varie ragioni. Prima di tutto, i sistemi aperti hanno una struttura intrinsecamente dinamica, rendendo difficile, se non impossibile, anticipare l'intero flusso delle interazioni dell'applicazione in fase di progettazione. In secondo luogo, in tali sistemi si deve sempre tener conto della possibile presenza di componenti ostili che potrebbero modificare gli invarianti delle interazioni specificate per ricavare informazioni segrete e/o ottenere illegalmente accesso alle risorse del sistema. Ancora piu' sottilmente, le componenti stesse potrebbero non essere affidabili riguardo al fatto di rispettare i propri ruoli, per esempio a causa di un fallimento accidentale o di un comportamento volutamente ostile. Di conseguenza e' necessario realizzare delle implementazioni difensive che incorporano nelle componenti verificate staticamente dei meccanismi di protezione dinamici al fine di proteggerle contro gli attacchi alla sicurezza da parte di eventuali avversari e, piu' in generale, al fine di renderle adattabili ad ambienti diversi e condizioni di esecuzione mutevoli.

Il nostro contributo alla realizzazione del progetto sara' orientato allo sviluppo di tecniche di analisi e verifica per gli aspetti relativi alla sicurezza nei modelli formali considerati nella presente proposta di ricerca. Abbiamo due obiettivi principali. Da un lato intendiamo esplorare l'uso di tecniche formali per esprimere e verificare proprieta' sui dati e sulle risorse utilizzati durante le interazioni. La nostra attivita' si concentrera' principalmente sullo studio di nuove astrazioni (tipate) e meccanismi per esprimere politiche relative a specifiche proprieta' di sicurezza che regolano l'uso dei dati, l'accesso alle risorse e il flusso di informazioni nei sistemi a piu' componenti. Basandoci su questi risultati, intendiamo sviluppare tecniche automatiche per verificare (i) la compatibilita' delle specifiche di sicurezza per le diverse componenti e, (ii) la conformita' di ogni componente ai vincoli di sicurezza imposti su di essi dai rispettivi ruoli nelle specifiche stesse.

Intendiamo inoltre sviluppare implementazioni sicure delle astrazioni tipate che abbiamo discusso sopra. Se da un lato sono convenienti come costrutti di programmazione, dall'altro tali astrazioni devono essere progettate con cura: per esssere effettive su piattaforme distribuite essere devono infatti incapsulare tutti i protocolli di basso livello necesari per garantire le proprieta' di mutua autenticazione tra i partecipanti, e di correlazione e dipendenza causale tra i dati scambiati nelle comunicazioni necessarie per garantire che i partecipanti vengano eseguiti in modo sicuro, corretto e fedele alla speficica.

La nostra ricerca si pone come obiettivo lo sviluppo di traduzioni guidate dai tipi per le astrazioni di alto livello nei corrispondenti protoolli di basso livello che le realizzano. A tal fine, nella prima fase del lavoro ci concentremo sul progetto di un linguaggio intermedio tipato per la comunicazione remota che sia al tempo stesso adeguato per esprimere le astrazioni di alto livello ed efficace come piattaforma dove sia possibile formalizzare gli aspetti specificamente di sicurezza dell'interazione e verificare le proprieta' desiderate.

Svilpperemo quindi uno schema di compilazione per stadi successivi che si basa sulla definizione (i) di traduzioni type-preserving e fully-abstract delle astrazioni per contratti e sessioni nel linguaggio intermedio per la comunicazione, e quindi (ii) di traduzioni guidate dai tipi dei costrutti del linguaggio intermedio nei protocolli crittografici che li realizzano.

Testo inglese
Programming distributed applications is complex because of the dynamic and often unreliable nature of the hosting environment.

Modern specification languages provide abstractions to structure the application design around a set of pre-arranged patterns that regulate the interaction of the distributed parties. These patterns, which are sometimes referred to as contracts or sessions in the literature, make it possible to specify the overall execution flow in a multi-party application and, based on that, to code each party by instructing it to follow the behavior extracted from the contract description. As long as all parties are known in advance and may be trusted to comply with their intended roles, this specification practice works very well and yields powerful tools for design and static verification.

In open systems, however, this technique is way less effective, for various reasons. First, open systems are inherently dynamic in their structure, making it difficult/impossible to anticipate the entire interaction flow of the application at design time. Secondly, in such systems one must always account for the presence of hostile components willing to break the intended interaction invariants to steal information and/or gain illegal access to the resources of the system. Even more subtly, the parties themselves may not be trusted to always play by their role, because of accidental failure, or intended hostility. As a result, defensive

implementations are required to instrument the statically verified components with dynamic safeguards protecting them against the security attacks mounted by an adversary, and more generally to make them adaptable to a varying environment and to mutable execution conditions.

Our efforts within the project will generally be targeted at the development of analysis and verification techniques for the security aspects of the interaction models of interest in the research proposal. The objective of our work is twofold. On one side, we will explore formal techniques to express and verify data and resource-centric properties of the interaction. Our activities will focus on the investigation of new (typed) abstractions and mechanisms to express policies on security-specific properties for data-usage, resource access and information flow in multi-party systems. Based on that, we will develop automated techniques to verify (i) the compatibility of the security specifications by the different parties and, (ii) the compliance of each party to the security constraints imposed on them by their role in the specification.

A complementary objective is the development of secure implementations of the typed abstractions we just discussed. While convenient for programming, such abstractions must be designed with care: in fact, to be effective in distributed settings, they must encapsulate all the low-level coding required to ensure the properties of mutual authentication among remote peers, of data correlation and causal dependency required for a safe, secure and faithful-to-the-specification execution at the end-points. Our work here will target the systematic development of type-driven encodings for the high-level abstractions into the corresponding low-level distributed protocols realizing them. In that direction we will first work on designing a typed intermediate language for remote communication adequate to support the high-level abstractions and at the same time effective as a framework in which the security-specific aspects of the interactions can be made explicit and the relevant properties formally verified. We will then develop a staged encoding scheme involving the development of (i) type-preserving and fully-abstract encodings of the contract and session abstractions into the typed intermediate language, and then (ii) type-driven translations of the intermediate language into their cryptographic implementation.

9 - Settori di ricerca ERC (European Research Council)

PE Mathematics, physical sciences, information and communication, engineering, universe and earth sciences

PE1 Mathematical foundations: all areas of mathematics, pure and applied,plus mathematical aspects of theoretical computer science, and mathematical physics
PE1_10 Theoretical computer science

PE5 Information and communication: informatics and information systems,computer science, scientific computing, communication technology, intelligent systems
PE5_3 Formal methods

10 - Parole chiave

Testo italiano

SISTEMI DI TIPO PER LA SICUREZZA
TEORIE EQUAZIONALI E OSSERVAZIONALI PER LA SICUREZZA

Testo inglese

TYPE SYSTEMS FOR SECURITY
EQUATIONAL AND OBSERVATIONAL THEORIES FOR SECURITY

11 - Stato dell'arte

Testo italiano
La nostra ricerca, in generale, riguarda i modelli fondazionali per i sistemi aperti e distribuiti e ha l'obiettivo di fornire strumenti formali di analisi e verifica basati su sistemi di tipi e tecniche algebriche che esprimono teorie equazionali ed osservazionali.

Di seguito, diamo una breve panoramica dello stato dell'arte in queste aree ed elenchiamo i corrispondenti riferimenti in letteratura. La descrizione non intende essere esaustiva, ma si focalizza sugli aspetti che sono di interesse specifico al programma.

ASTRAZIONI TIPATE PER LA SICUREZZA

A partire dal lavoro seminale in [PS96], i sistemi di tipi sono stati ampiamente applicati ai calcoli di processi in modo da fornire garanzie statiche (e talvolta anche dinamiche) per proprietà di correttezza e sicurezza. Diversi sistemi di tipi sono stati definiti per esprimere varie forme di politiche di controllo degli accessi in sistemi distribuiti. [CDV03] propone una forma di controllo degli accessi distribuito basato su operazioni crittografiche tipate; [HR02a,HRY05] propongono dei sistemi di tipi per il controllo dell'accesso alle risorse che appaiono nelle diverse locazioni di un sistema distribuito. Un buon numero di sistemi di tipi è stato proposto per calcoli simili all'ambient calculus sia per gestire il controllo degli accessi [BCC04b, CGG05, HR02, HMR04, GBCD07, DGPV08], sia per controllare la mobilità [BC02] anche basati sull'uso di risorse [BBDS07]. Altri lavori relativi al controllo degli accessi nei sistemi distribuiti sono stati sviluppati nel contesto del linguaggio KLAIM e le sue estensioni al muKLAIM [GP03] e utilizzano i sistemi di tipi che permettono lo scambio dinamico di diritti di accesso, anche basati sulla nozione di regione [DGP06].

I sistemi di tipo sono stati utilizzati con successo per l'analisi di diverse proprietà di segretezza [Aba99,AB03,AB05], di protocolli a basso livello per l'autenticazione, [GJ04,BFM07]. I sistemi di tipo sono stati anche applicati a politiche di autorizzazione ad alto livello [FGM07a,FGM07b, CHPR07], anche nel contesto di architetture orientate ai servizi [LPT07]. Infine, i sistemi di tipi sono stati proposti anche per controllare il flusso delle informazioni implicito determinato dal comportamento dei componenti di un sistema (cf. [Kob05,Pot02,HVY00,SV03] tra gli altri). Tali sistemi di tipi tracciano le relazioni causali tra gli stati di computazione in modo da individuare i canali nascosti. Molti articoli hanno studiato come implementare le astrazioni di alto livello in termini di codifiche in calcoli con primitive crittografiche e hanno provato risultati di correttezza formale e/o computazionale. Tra questi, vi sono approcci che si focalizzano su primitive di comunicazione relativamente semplici, sia tipate [BG05,BG07] che non tipate [AFG02], altri invece si focalizzano su schemi di comunicazione più strutturati [AF06,Cor07].

EQUIVALENZE COMPORTAMENTALI PER LA SICUREZZA

La sicurezza del flusso delle informazioni mira a proteggere la riservatezza e l'integrità delle informazioni rilevando e/o impedendo che informazioni sensibili possano fluire verso utenti non autorizzati in sistemi che prevedono vari livelli di sicurezza e diverse categorie di utenti.

La sicurezza del flusso delle informazioni è rilevante per un ampia gamma di problematiche di sicurezza. In particolare, complementa l'attività di controllo dell'accesso alle risorse, limitando la propagazione delle informazioni (piuttosto che l'accesso e il rilascio delle stesse) e individuando i flussi di informazione

impliciti, flussi che derivano da trasmissioni delle informazioni che avvengono in modo indiretto attraverso le risorse condivise del sistema o della rete.

La sicurezza del flusso delle informazioni è stata studiata tradizionalmente in termini di non-interferenza [GM82], una proprietà che garantisce che i dati riservati non influenzino mai il comportamento pubblico e osservabile del sistema. La teoria della non-interferenza e` stata studiata in diversi contesti: linguaggi di programmazione [SV98,SM03,BPR07], calcoli di processi [RS01,FG01,HR02,CR07], modelli probabilistici [ABG04], modelli temporizzati [GLM03], protocolli crittografici [Aba99,FGM00]. Nella maggior parte di questi sistemi, la non-interferenza è formalizzata tramite equivalenze comportamentali basate sulle tracce di esecuzione [McL94,Man00]. Esistono inoltre caratterizzazioni basate su equivalenze nello stile della bisimulazione [FG01].

L'implementazione di proprietà di sicurezza del flusso delle informazioni, quali la non-interferenza, che impediscono ogni flusso indebito di informazione può essere molto problematica. In effetti, nelle applicazioni reali, il rilascio di alcune informazioni e` spesso un fatto previsto nel funzionamento del sistema stesso. Questo ha condotto a nozioni più fini di non-interferenza che definiscono i flussi di informazione sicuri in presenza di politiche di sicurezza basate su meccanismi come la declassificazione ed il downgrading. Questa linea di ricerca
si sviluppa a partire dai lavori sulla non-interferenza intransitiva [GM84,Rus92,Pin95,SD07]. Recentemente sono stati proposti meccanismi per la declassificazione selettiva o robusta [MSZ06], e framework generali per lo studio del downgrading nei calcoli di processi del primo ordine [BPR04].

Testo inglese
Broadly stated, our research draws on foundational models of open and distributed systems with the goal of providing formal tools for the analysis and verification based on type theories and process algebraic techniques for equational and observational reasoning.

Below we give a brief survey of the state of the art in these areas providing some of the relevant references to the literature. The description is not intended to be exhaustive: rather, it focuses on the aspects which are of specific interest to the program.

TYPED ABSTRACTIONS FOR SECURITY

Starting with the seminal work in [PS96], type systems have been applied widely in process calculi to provide static (sometimes also dynamic) guarantees for a variety of safety and security properties.
Several type systems encompass various forms of access control policies in distributed systems. [CDV03] proposes a form of distributed access control based on typed cryptographic operations; [HR02a,HRY05] propose expressive type systems to control the access to the resources advertised at the different locations of a distributed system. A number of type systems have been proposed for ambient-like calculi to support access control, [BCC04b, CGG05, HR02, HMR04, GBCD07, DGPV08], or to control mobility [BC02] also based on resource usage [BBDS07]. Other related work on access control in distributed systems has been carried out in the context of the language KLAIM and its extensions to muKLAIM [GP03] with type systems that enable the dynamic exchange of access rights, also based on a notion of region [DGP06].

Type systems have been successfully employed in the analysis of diverse properties of secrecy [Aba99,AB03,AB05], low-level protocols for authentication, [GJ04,BFM07] and of higher-level authorization policies [FGM07a,FGM07b, CHPR07], also in the context of service oriented architectures [LPT07]. Finally, type systems have also been proposed to control implicit information flow determined by the behavior of system components (cf. [Kob05,Pot02,HVY00,SV03] among others). These type systems trace the causality relations between computational steps in order to detect covert channels.

A number of papers have investigated implementations of high-level abstractions in terms of encodings into cryptographic calculi providing results of formal and/or computational soundness. They include approaches that focus on relatively simple primitives for communications, either untyped [AFG02] or typed [BG05,BG07], as well as for more structured communication patterns [AF06,Cor07].

BEHAVIORAL EQUIVALENCES FOR SECURITY

Information flow security aims at protecting confidentiality and integrity of information by detecting and/or preventing flow of sensitive information to non-authorized subjects inside systems with multiple security levels and classes of users.

Information flow security is relevant to a wide range of security aspects. Specifically, it complements resource access control by placing restrictions on the propagation of information (rather than on access and release) and by detecting implicit flow of information, resulting from indirect ways of transmitting information via shared system or network resources.

Information flow security has traditionally been studied in terms of non-interference [GM82], a property which guarantees that confidential data never affect the public observable behavior of the system. Non-interference has been developed in different settings, from programming languages [SV98,SM03,BPR07], to process calculi [RS01,FG01,HR02,CR07], probabilistic models [ABG04], timed models [GLM03], and cryptographic protocols [Aba99,FGM00]. In most of these systems, non-interference is formalized in terms of theories of behavioral equivalences based on execution traces [McL94,Man00]. Work has also been developed on similar characterizations based on bisimulation equivalences [FG01].

Information flow security which prevents any information release, like non-interference, can hardly be achieved in real systems. Indeed real applications often release some information as part of their intended functioning. This has led to refined notions of non-interference which characterize secure information flows in the presence of security policies based on mechanisms such as declassification and downgrading. This line of research builds on work on intransitive non-interference [GM84,Rus92,Pin95,SD07], and develops new mechanisms for selective or robust [MSZ06] declassification, as well as general frameworks for downgrading in first-order process algebras [BPR04].

12 - Riferimenti bibliografici

[Aba99] Secrecy by Typing in Security Protocols J. ACM 46(5):749-786. 1999.

[AB03] M. Abadi, B. Blanchet. Secrecy Types for Asymmetric Communication. TCS 298(3), 387-415, 2003.

[AB05] M. Abadi, B. Blanchet. Analyzing security protocols with secrecy types and logic programs. J. ACM, 52(1):102-146, 2005.

[ABG04] A. Aldini, M. Bravetti, R. Gorrieri. A Process-algebraic Approach for the Analysis of Probabilistic Non-interference. JCS, 12(2):191-245, 2004.

[AF06] P. Adao and C. Fournet. Cryptographically sound implementations for communicating processes. ICALP'06, LNCS 4052, 83-94. 2006.

[AFG02] M. Abadi, C. Fournet, G. Gonthier. Secure implementation of channel abstractions. I&C, 174(1):37-83, 2002.

[BBDS07] F. Barbanera, M. Bugliesi, M. Dezani-Ciancaglini, V. Sassone: Space-aware ambients and processes. Theor. Comput. Sci. 373(1-2): 41-69, 2007.

[BBMR08] G. Bernardi, M. Bugliesi, D. Macedonio, S. Rossi. A Theory of Adaptable Contract-Based Service Composition. SYNASC 2008. To appear.

[BC02] M. Bugliesi, G. Castagna. Behavioural typing for safe ambients. Comput. Lang. 28(1): 61-99, 2002.

[BCC04] M. Bugliesi, D. Colazzo, S. Crafa. Type based Discretionary Access Control. CONCUR'04, LNCS 3170, 225-239. 2004.

[BCC04b] M. Bugliesi, G. Castagna, S. Crafa. Access control for mobile agents: The calculus of boxed ambients. TOPLAS 26(1): 57-124. 2004.

[BCCM08] M. Bugliesi, D. Colazzo, S. Crafa, D.Macedonio: A Type System for Discretionary Access Control. Submitted for publication.

[BF08] M. Bugliesi, R. Focardi: Language Based Secure Communication. CSF'08: 3-16. 2008.

[BFM07] M. Bugliesi, R. Focardi, M. Maffei: Dynamic types for authentication. Journal of Computer Security 15(6): 563-617, 2007.

[BG05] M. Bugliesi M. Giunti. Typed processes in untyped contexts. TGC'05, LNCS 3705, 19-32., 2005.

[BG07] M. Bugliesi, M. Giunti. Secure implementations of typed channel abstractions. POPL'07, 251-262. 2007.

[BPR04] A. Bossi, C. Piazza, S. Rossi: Modelling Downgrading in Information Flow Security. CSFW 2004: 187-203

[BPR07] A. Bossi, C. Piazza, S. Rossi. Compositional Information Flow Security for Concurrent Programs. JCS, 15(3), 373-416, 2007.

[BR05] M. Bugliesi, S. Rossi. Non-interference proof techniques for the analysis of cryptographic protocols. JCS 13(1): 87-113. 2005

[CDV03] T. Chothia, D. Duggan, J. Vitek. Type-based Distributed Access Control. CSFW'03 170-184. 2003.

[CGG05] L. Cardelli, G. Ghelli, A.D. Gordon. Secrecy and group creation. I&C, 196(2):127-155. 2005.

[CHPR07] A. Cirillo, R. Jagadeesan, C. Pitcher, J. Riely. Do As I SaY! Programmatic Access Control with Explicit Identities. CSF'07, IEEE, 2007.

[CHY07] M. Carbone, K. Honda, N. Yoshida. Structured communication-centred programming for web services. ESOP'07, 2-17. 2007.

[CGP08] G. Castagna, N. Gesbert, L. Padovani: A Theory of Contracts for Web Services. POPL'08: 261-272. 2008

[CL06] S. Carpineti, C. Laneve: A Basic Contract Language for Web Services. ESOP 2006: 197-213

[CR07] S. Crafa, S. Rossi. Controlling information release in the pi-calculus. Inf. Comput. 205(8): 1235-1273. 2007.

[Cor07] R. Corin et al. Secure Implementations for Typed Session Abstractions CSF'07, 170-186. 2007.

[DGP06] R. De Nicola, D. Gorla, R. Pugliese. Confining data and processes in global computing applications. Sci. Comput. Program., 63(1):57-87. 2006.

[DGPV08] M. Dezani, S. Ghilezan, J. Pantovic, D. Varacca. Security Types for Dynamic Web Data, TCS 402:156-171, 2008.

[FG01] R. Focardi, R. Gorrieri. Classification of Security Properties (Part I). Foundations of Security Analysis and Design. LNCS 2171, Springer, 2001.

[FGM00] R. Focardi, R. Gorrieri, F. Martinelli. Non Interference for the Analysis of Cryptographic Protocols. ICALP'00, 744-755. Springer, 2000.

[FGM07a] C. Fournet, A.D. Gordon, S. Maffeis. A type discipline for authorization in distributed systems. CSF'07, 31-48. 2007.

[FGM07b] C. Fournet, A.D. Gordon, S. Maffeis. A Type Discipline for Authorization Policies. TOPLAS 29(5) 2007.

[GBCD07] P. Garralda, E. Bonelli, A. Compagnoni, M. Dezani. Boxed Ambients with Communication Interfaces, MSCS 17:1-59, 2007.

[GJ04] A. Gordon, A. Jeffrey. Types and effects for asymmetric cryptographic protocols. JCS, 12(3-4):435-483.

[GLM03] R. Gorrieri, E. Locatelli, and F. Martinelli. A simple language for real-time cryptographic protocol analysis. ESOP'03, LNCS 2618, 114-128. Springer, 2003.

[GM82] J.A. Goguen, J. Meseguer. Security Policies and Security Models. IEEE Symposium on Security and Privacy, 11-20, 1982.

[GM84] J.A. Goguen, J. Meseguer. Unwinding and Inference Control. IEEE Symposium on Security and Privacy, 75-86, 1984.

[GP03] D. Gorla, R. Pugliese. Resource access and mobility control with dynamic privileges acquisition. ICALP'03, 119-132. 2003

[HMR04] M. Hennessy, M. Merro, J. Rathke. Towards a Behavioural Theory of Access and Mobility Control in Distributed Systems. TCS 322(3):615-669, 2004.

[HRY05] M. Hennessy, J. Rathke, N. Yoshida. SafeDpi: a language for controlling mobile code. Acta Informatica, 42(4-5):227-290.

[HR02a] M. Hennessy, J. Riely. Information flow vs resource access in the asynchronous pi-calculus. TOPLAS 24(5):566-591. 2002.

[HR02] M. Hennessy, J. Riely. Resource access control in systems of mobile agents. I&C, 173:82-120. 2002

[HVY00] K. Honda, V. Vasconcelos, N. Yoshida. Secure information flow as typed process behaviour. ESOP'00, LNCS 1782, 188-199. 2000.

[HYC08] K. Honda, N. Yoshida, M. Carbone. Multiparty asynchronous session types. POPL'08, 273-284. 2008.

[Kob05] N. Kobayashi. Type-based information flow analysis for the pi-calculus. Acta Informatica, 42(4):291-347. 2005.

[LP07] C. Laneve, L. Padovani. The Must Preorder Revisited. CONCUR'07: 212-225. 2007

[LPT07] A. Lapadula, R. Pugliese, F. Tiezzi: Regulating data exchange in service oriented applications. FSEN 2007. 223-239.

[Man00] H. Mantel. Possibilistic Definitions of Security - An Assembly Kit. IEEE CSFW'00 , 185-199, 2000.

[McL94] J. McLean. Security Models. Encyclopedia of Software Engineering, 1994.

[MSZ06] Andrew C. Myers, Andrei Sabelfeld, Steve Zdancewic: Enforcing Robust Declassification and Qualified Robustness. JCS 14(2): 157-196, 2006.

[Pin95] S. Pinsky. Absorbing Covers and Intransitive Noninterference. IEEE Symposium on Security and Privacy, 102-113, 1995.

[Pot02] F. Pottier. A simple view of type-secure information flow in the pi-calculus. CSFW'02, 320-330. 2002.

[PS96] B. Pierce, D. Sangiorgi. Typing and subtyping for mobile processes. MSCS, 6(5). 1996.

[RS01] P.Y.A. Ryan, S. Schneider. Process Algebra and Non-Interference. JCS, 9(1/2):75-103, 2001.

[Rus92] J. Rushby. Noninterference, Transitivity, and Channel-Control Security Policies. Technical Report, CSL-92-02, SRI International, 1992.

[SD07] A. Sabelfeld and D. Sands. Declassification: Dimensions and Principles. Journal of Computer Security, 2007,

[SdV01] P. Samarati, S. D. C. di Vimercati. Access control: Policies, models, and mechanisms. FOSAD'01, LNCS 2171. 2001.

[SM03] A. Sabelfeld and A.C. Myers. Language-Based Information-Flow Security. IEEE Journal on Selected Areas in Communications, 21(1):5 19, 2003.

[SV98] G. Smith and D.M. Volpano. Secure Information Flow in a Multi-threaded Imperative Language. POPL'98, 355-364, 1998.

[SV03] P. Sewell, J. Vitek. Secure composition of untrusted code: Box pi, wrappers and causality types. Journal of Computer Security, 11(2):135-188.

13 - Descrizione del programma e dei compiti dell'Unità di Ricerca

Testo italiano

La nostra ricerca è incentrata sullo sviluppo di un supporto language-based per la sicurezza nella specifica e nella verifica dei modelli per l'interazione identificati all'interno del progetto.

Possiamo raggruppare le nostre attività attorno ai seguenti temi specifici e relative linee di lavoro.

SICUREZZA E SISTEMI DI TIPI PER LA SICUREZZA DISTRIBUITA

Tale linea di ricerca fa parte delle attività dei work-packages WP1.1, WP2.1 and WP2.2 della proposta.

Il suo scopo generale è lo sviluppo di risultati di "correttezza robusta" ("robust safety") per calcoli tipati che impongano un controllo degli accessi discrezionale basato sul ruolo e applichino politiche di autorizzazione per dati e risorse basate su identità. La sicurezza dei dati e la gestione delle risorse sono di interesse centrale per i modelli di studio del progetto: esse richiedono sempre un supporto dinamico durante l'esecuzione (spesso con l'aiuto di una infrastruttura crittografica), e molto spesso costituiscono esse stesse sia un'importante questione di negoziazione che un pre-requisito per l'intesa in un sistema con più attori.

Il nostro piano è quello di contribuire all'avanzamento dello stato dell'arte nel campo del controllo (discrezionale) dell'accesso delle risorse, integrando il lavoro esistente in quest'area (in parte anche nostro) usando meccanismi di autenticazione basati sull'identità, e meccanismi di autorizzazione basati sul ruolo, e ove possibile/richiesto garantendo diverse forme di anonimato e riservatezza.

WP 1.1 and WP 2.1 - Calcoli di Processo e Tipi per Interazioni aperte

Come primo passo studieremo delle nuove classi di tipi (dipendenti) per esprimere proprietà di segretezza di base e di autenticazione di basso livello per i dati scambiati nei protocolli distribuiti. Studieremo inoltre la correlazione tra queste due proprietà: infatti, la segretezza di un dato potrebbe implicare l'autenticità di altri dati scambiati all'interno dello stesso messaggio. Questo lavoro sui tipi per la sicurezza sarà parte di una attività di ricerca più estesa centrata sul disegno di un calcolo tipato intermedio per la comunicazione remota, che sia adatto a supportare astrazioni di alto livello per sessioni/cotratti, e al tempo stesso che sia efficace come struttura in cui gli aspetti dell'interazione specifici della sicurezza possano essere esplicitati in modo da verificare formalmente le principali proprietà. Per esemplificare, ci aspettiamo che il calcolo intermedio sia abbastanza espressivo da codificare e studiare le principali proprietà di sicurezza dei protocolli di pagamento elettronico (e-payment) che coinvolgano un mediatore per il pagamento. Tali protocolli richiedono che il mediatore ottenga prova che i clienti abbiano effettivamente ordinato il pagamento (e tale prova deve essere associata ad esattamente una transazione) e che i venditori lo abbiano effettivamente richiesto. Simili garanzie e certificazioni sono richieste anche agli altri attori quando, per esempio, i clienti devono essere protetti da ogni tentativo di impersonificazione da parte di estranei che cercano di replicare vecchi ordini di pagamento. Alcune di queste proprietà sono studiate in letteratura, ma sono ben comprese solo in scenari semplici: in effetti, le tecniche correnti sono carenti nel fornire supporto adeguato nelle situazioni come quella che abbiamo appena descritto, che richiedono tecniche di analisi di per l'autenticazione a più passi (ovvero, entro una sessione).

Due sono i due risultati chiave per il calcolo intermedio, necessari per rendere il calcolo una base effettiva per il nostro programma di lavoro. Da un lato, abbiamo chiaramente bisogno della correttezza del sistema di tipi, in modo da assicurare che il codice intermedio ben tipato fornisca le garanzie di sicurezza che è inteso rispettare. Dall'altro lato, la sfida è quella di trovare una codifica corretta e completa del codice intermedio ben tipato nei protocolli distribuiti di basso livello, in modo da assicurare che le garanzie di sicurezza siano preservate anche in un ambiente antagonistico.

WP 2.2 - Tipi per la Gestione di Risorse e Controllo degli accessi

Ricorrendo al calcolo intermedio ben tipato, noi studieremo sia le astrazioni di tipo ad alto livello che le primitive tipate per le interazioni basate sulle sessioni e i contratti. Queste includeranno tipi in grado di esprimere politiche di autorizzazione basate sull'identità e politiche di controllo degli accessi basate sui ruoli come quelle che abbiamo proposto in scenari più semplici in [BCC04,BCCM08], in modo da supportare meccanismi a grana fina per regolare l'uso e la trasmissione di diritti di accesso, limitandone la ri-trasmissione (iterata) o inibendone la comunicazione a terze parti. Questa linea di ricerca sarà sviluppata in collaborazione con l'unità di Torino.

EQUIVALENZE COMPORTAMENTALI PER LA COMPOSIZIONE SICURA DI SERVIZI

Una linea complementare di ricerca di questa unità è lo studio di tecniche per l'analisi di sistemi di servizi a più partecipanti in cui i servizi sono descritti in maniera astratta in termini di contratti. Questa linea di ricerca rientra nei work-packages WP3.1 e WP3.2 della proposta di ricerca.

WP 3.1 - Conformità dei partecipanti

Il nostro lavoro si focalizzerà nello sviluppo di tecniche accurate ed efficienti per specificare e validare politiche di sicurezza utili per regolare il flusso delle informazioni in un sistema a più partecipanti. In particolare il nostro obiettivo è di definire un framework generale per l'analisi e la verifica seguendo le idee di [BPR04]. Estenderemo tale approccio in modo da permettere l'espressione di politiche di sicurezza per la declassificazione e per supportare la specifica si cambiamenti dinamici dei livelli di sicurezza associati sia ai vari partecipanti che interagiscono, che ai dati scambiati nelle interazioni. Una declassificazione controllata, per mezzo di primitive di downgrading basate sui ruoli, è cruciale per assicurare che nessuna informazione trapeli verso partecipanti non previsti e per permettere allo stesso tempo il flusso di informazione necessario in una negoziazione all'interno del sistema stesso. Similmente, una declassificazione dinamica ci permetterà di analizzare i sistemi che evolvono con l'aggiunta di nuovi e potenzialmente inaffidabili componenti che si aggiungono alla computazione. La declassificazione e controllo del flusso delle informazioni sono particolarmente importanti nei sistemi che comprendono meccanismi di delega come quelli descritti nella presente proposta di ricerca, al fine di assicurare che i delegati non abbiano accesso a in formazioni che erano intese essere riservate per la componente delegante.

Il nostro approccio si occuperà di metodi di verifica per la non-interferenza, basati a loro volta sull'analisi di equivalenze osservazionali tipate, con tipi che danno informazioni sui livelli di sicurezza e affidabilità associati ai partecipanti e ai dati che essi scambiano.

Oltre a sviluppare metodi di verifica, studieremo nuove tecniche per nascondere, rendere anonimi o in casi estremi bloccare gli scambi di dati critici per la sicurezza e le sincronizzazioni che potrebbero minare la sicurezza del flusso di informazioni all'interno di un sistema. Partendo dal nostro recente lavoro in [BBMR08], indagheremo la possibilità di effettuare trasformazioni basate su filtri [CGP08] che agiscono sia come strumenti che aiutano a definire i servizi in una composizione sicura, sia come monitor a tempo di esecuzione che forzano le garanzie di sicurezza desiderate qualora esse non fossero rispettate staticamente. In particolare, studieremo tecniche per determinare l'esistenza di un filtro di sicurezza per una composizione, e metodi automatici per sintetizzare filtri ottimali, cioè filtri che riducono la loro azione al minimo richiesto per far rispettare le politiche di flusso di informazione desiderate.

WP 3.2 - Rimpiazzamento Sicuro

Come ulteriore attività correlata alla precedente, studieranno l'uso dei filtri come strumenti per generare raffinamenti dei servizi che preservino la sicurezza e dunque che permettano di ottenere un solido fondamento per giustificare la correttezza e la sicureza delle operazioni di rimpiazzamento dei componenti in un sistema.

L'unita' di ricerca di Venezia ha una riconosciuta esperienza nei metodi formali per la sicurezza in sistemi concorrenti e distribuiti, e più precisamente nelle seguenti aree.

Tipi e Logiche per il Controllo degli Accessi alle Risorse nei Sistemi Distribuiti.

Abbiamo sviluppato teorie di tipi per il controllo degli accessi nei sistemi distribuiti e mobili [BC02,BCC04,BCC04b,BBDS07,BCCM08], e abbiamo studiato le loro estensioni ai sistemi che combinano componenti tipate e non tipate [BG05]. Tali teorie saranno rilevanti per l'analisi dei contratti/sessioni, al fine di controllare l'accesso alle risorse richieste dai servizi e negoziate attraverso i contratti.

Tipi e Tecniche Comportamentali per la Sicurezza del Flusso delle Informazioni

Abbiamo sviluppato uno schema generale, basato sulla non-interferenza, per la specifica e l'analisi del flusso delle informazioni in processi concorrenti e distribuiti, e abbiamo sviluppato strumenti automatici di analisi basati su tali teorie (si vedano ad esempio [BPR04,BPR07,CR07]). Queste teorie saranno rilevanti nel contesto della presente proposta: in particolare, il nostro lavoro sull'analisi del flusso delle informazioni in presenza di primitive di declassificazione sara' certamente utile per garantire le proprietà di sicurezza richieste per lo scambio di dati privati nelle negoziazioni dei contratti.

Analisi di Protocolli Crittografici.

Il nostro lavoro in quest'area si è sviluppato in diverse direzioni, ciascuna delle quali sara' rilevante nelle attività programmate nella presente proposta. Abbiamo studiato una caratterizzazione comportamentale per diverse proprietà di sicurezza di protocolli crittografici, che includono la segretezza, l'autenticazione, lo scambio fair e la non-ripudio [BR05]. D'altro canto, abbiamo sviluppato un framework per l'analisi statica di protocolli di sicurezza per l'autenticazione, basati su sistemi di tipi-ed-effetti (type-and-effect). Infine, abbiamo studiato varie astrazioni di alto livello per la comunicazione (tipata e non tipata) e abbiamo studiati i problemi relativi alla loro codifica fully-abstract in protocolli di basso livello [BF08,BG07].

Testo inglese
Our research is centered on the development of language-based support for security in the specification and verification of the interaction models identified within the project.

We may group our activities around the following specific themes and lines of work.

SECURITY TYPES AND TYPED ABSTRACTIONS FOR DISTRIBUTED SECURITY

This line of research is part of the activities of work-packages WP1.1, WP2.1 and WP2.2 of the proposal.

Its overall goal is the development of "robust safety" results for typed calculi enforcing discretionary, role-based access control and identity-based authorization policies for data and resources. Data security and resource management are central concerns for the interaction models of interest in the project: they always require dynamic support during execution (often with the aid of a cryptographic infrastructure), and more often than not they constitute themselves an important matter of negotiation as well as a pre-requisite for commit in multi-party agreements.

Our plan is to advance the state of the art on (discretionary) resource access control, by complementing existing (partly our own) work in this area with identity-based mechanisms for authentication, and role-based mechanisms for authorization, possibly supporting forms of identity-confidentiality and anonymity.

WP 1.1 and WP 2.1 - Calculi and Types for Interaction

As a first step we will explore new classes of (dependent) types to express basic, low-level secrecy and authentication properties for the data exchanged in a distributed protocol and their correlation (the secrecy of a piece of data may imply the authenticity of other data exchanged within the same message). This work on security types will be part of a wider research activity centered on the design of a typed intermediate calculus for remote communication, adequate to support higher-level abstractions for sessions/contracts, and at the same time effective as a framework in which the security-specific aspects of the interactions can be made explicit and the relevant properties formally verified. To exemplify, we expect the intermediate calculus to be expressive enough to code and reason about the core safety properties of e-payment protocols involving a payment-gateway. Such protocols require the gateway to obtain proofs that clients have ordered payment (and such proofs must be associated with just one transaction) and that the merchants have requested the payments. Similar guarantees and proofs are required at the other peers as, say, clients must be protected against any impersonation attempt by intruders trying to replicate stale payment orders. Some of theses properties are studied in the literature, but they are well understood only in simpler scenarios: indeed, current techniques fall short of providing adequate support for situations like the one we have outlined, which require techniques to reason on multi-hop (or session) authentication.

There are two key results we seek for the intermediate calculus, to make it an effective basis for our endeavor. On the one side, we clearly need type safety, to ensure that well-typed intermediate code provides the security guarantees it is intended to convey. On the other side, the challenge is to find fully abstract encodings of well-typed intermediate code into lower-level distributed protocols, so as to ensure that the security guarantees are preserved in adversarial settings.

WP 2.2 - Types for Resource Management and Access Control

Drawing on the typed intermediate calculus, we will then explore higher-level type abstractions and typed primitives for session and contract based interactions. These will include types to express identity-based authorization and role-based access control policies such as those we proposed in a simpler setting in [BCC04,BCCM08], to support fine-grained mechanisms to govern the use and transmission of authorization rights, to bound their (iterated) re-transmission or predicate their use on the inability to pass them to third parties. This line of work will be developed in collaboration with the unit in Torino.

BEHAVIORAL TECHNIQUES FOR SECURE SERVICE COMPOSITION

A complementary line of research of this unit is in the investigation of techniques for the analysis of multi-party systems of services in which services are described abstractly in terms of contracts. This line of research is part of the activities in Work Package 3 of the research proposal.

WP 3.1 - Participant Conformance

Our work will focus on developing accurate and efficient techniques for specifying and validating policies to govern the flow of information in multi-party systems. In particular, we aim at developing a framework for analysis and verification along the lines of [BPR04], extending that approach to allow one to express security policies for declassification and to support the specification of dynamic changes of the security levels associated with the interacting principals, and with the data exchanged in the interaction. Controlled declassification, by means of role-based downgrading primitives, is crucial to ensure that no information is leaked to unintended parties while at the same time allowing flow of information necessary in the negotiation withing the system. Dynamic declassification will similarly allow us to analyze systems that evolve with the addition of new, potentially untrusted components joining the computation. Declassification and information-flow control are particularly challenging, and important, in the presence of mechanisms that support delegation such as those advocated in the present research proposal, to ensure that delegates do not get access to information that was only intended for the delegating component.

Our approach will draw on verification methods for non-interference, in turn based on the analysis of typed behavioral equivalences, with types informing on the

security and trust levels associated with the participants and on the data they exchange.

Besides developing verification methods, we will also explore novel techniques to hide, anonymize or in the extreme case block the security-critical data exchanges and synchronizations that may undermine the information-flow security of a system. Drawing on our recent work in [BBMR08], we will explore transformations based on filters [CGP08] acting both as design tools that help shape the services in a secure composition, and as run-time monitors enforcing the desired security guarantees whenever this may not be accomplished statically. In particular, we will investigate techniques to determine the existence of a securing filter for a composition, and automatic methods for synthesizing optimal filters, i.e. filters minimizing their action to the minimum required to enforce the desired information-flow policies.

WP 3.2 - Secure Replacement

Further, related work, will explore the use of filters to obtain the security-preserving refinement of services, and based on that, to support the secure replacement of components in a system.

The research unit of Venice has a well recognized expertise in formal methods for security in concurrent and distributed systems, and more specifically in the following areas.

Types and Logics for Resource Access Control in Distributed Systems.

We have developed typed theories of access control for distributed and mobile systems [BC02,BCC04,BCC04b,BBDS07,BCCM08] , and studied their extensions to systems combining typed and untyped components [BG05]. Such theories will be relevant for the design of typed abstractions for contracts/sessions, to control the access to the resources required by the services, and negotiated in the contracts.

Types and Behavioral Techniques for Information Flow Security.

We have elaborated a general scheme, based on non-interference, for the specification and analysis of the flow of information in concurrent distributed processes and developed tools for automatic analysis based on such theories (see e.g. [BPR04,BPR07,CR07]). Such theories will be relevant in the context of the present proposal: in particular, our work on information-flow analysis in the presence of primitives of declassification will certainly be useful to assess the security guarantees provided for the private data exchanged in the interaction.

Analysis of Cryptographic Protocols.

Our work in this area has unfolded along various directions, all of which will be relevant in the activities planned in the present proposal. We have investigated a behavioral characterization for diverse security properties of cryptographic protocols, including secrecy, authentication [BFM07], fair-exchange and non-repudiation [BR05], Oand devised a framework for the static analysis of security protocols for authentication, based on type-and-effect systems. Also have investigated various high-level abstractions for (typed and untyped) communication and studied the problems related to their fully abstract encoding into low-level network protocols [BF08,BG07].

14 - Descrizione delle attrezzature già disponibili ed utilizzabili per la ricerca proposta

Testo italiano

nº	anno di acquisizione	Descrizione
1.	*2005*	*Desktop DELL 1.6 GHz*
2.	*2004*	*Desktop ATLON 1.2 GHz*
3.	*2004*	*Desktop ATLON 1.2 GHz*
4.	*2007*	*Laptop MAXDATA, 800 MHz*

Testo inglese

nº	anno di acquisizione	Descrizione
1.	*2005*	*Desktop DELL 1.6 GHz*
2.	*2004*	*Desktop ATLON 1.2 GHz*
3.	*2004*	*Desktop ATLON 1.2 GHz*
4.	*2007*	*Laptop MAXDATA, 800 MHz*

15 - Descrizione delle Grandi attrezzature da acquisire (GA)

Testo italiano

Nessuna

Testo inglese

Nessuna

16 - Mesi persona complessivi dedicati al Progetto

		Numero	Disponibilità temporale indicativa prevista		Totale mesi persona
			1° anno	2° anno	
Componenti della sede dell'Unità di Ricerca		*2*	*10*	*8*	*18*
Componenti di altre Università/Enti vigilati		*0*			
Titolari di assegni di ricerca		*1*	*7*	*2*	*9*
Titolari di borse	*Dottorato*	*1*	*4*	*4*	*8*
	Post-dottorato	*0*			
	Scuola di Specializzazione	*0*			
Personale a contratto	*Assegnisti*	*1*	*2*	*10*	*12*
	Borsisti	*0*			
	Altre tipologie	*0*			
Dottorati a carico del PRIN da destinare a questo specifico progetto		*0*	*0*	*0*	*0*
Altro personale		*0*			
TOTALE		**5**	**23**	**24**	**47**

17 - Costo complessivo del Progetto dell'Unità articolato per voci

Voce di spesa	Spesa in Euro	Descrizione dettagliata (in italiano)	Descrizione dettagliata (in inglese)
Materiale inventariabile	*4.000*	*Computers, altro hardware, libri*	*Computers, hardware, books*
Grandi Attrezzature	*0*		
Materiale di consumo e funzionamento (comprensivo di eventuale quota forfettaria)	*6.000*	*spese di gestione, materiale di consumo*	*Department overhead, consumables*
Spese per calcolo ed elaborazione dati			
Personale a contratto	*22.000*	*un assegnista di ricerca, dal mese 12 al mese 24 del progetto*	*1 full-time research fellow, from month 12 to month 24.*
Dottorati a carico del PRIN da destinare a questo specifico progetto	*0*		
Servizi esterni			
Missioni	*18.000*	*Spese di viaggio per conferenze, visite ad altri centri di ricerca per collaborazioni scientifiche*	*Conference travel, research visits to other institutions.*
Pubblicazioni (*)			
Partecipazione / Organizzazione convegni (*)	*5.000*	*Spese di iscrizione a convegni, meeting di progetto.*	*conference fees, project meetings*
Altro (voce da utilizzare solo in caso di spese non riconducibili alle voci sopraindicate)			
Subtotale	*55.000*		
Costo convenzionale	*7.000*		
Totale	*62.000*		

Tutti gli importi devono essere espressi in Euro arrotondati alle centinaia

(*) sono comunque rendicontabili le spese da effettuare per pubblicazioni e presentazione dei risultati finali della ricerca nei dodici mesi successivi alla conclusione del progetto, purché le relative spese siano impegnate entro la data di scadenza del progetto e purché le pubblicazioni e la presentazione dei risultati avvengano entro nove mesi dalla conclusione del progetto.

18 - Prospetto finanziario dell'Unità di Ricerca

Voce di spesa	Importo in Euro
a.1) finanziamenti diretti, disponibili da parte di Università/Enti vigilati di appartenenza dei ricercatori dell'unità operativa	*5.000*
a.2) finanziamenti diretti acquisibili con certezza da parte di Università/Enti vigilati di appartenenza dei ricercatori	*6.600*

dell'unità operativa	
a.3) finanziamenti connessi al costo convenzionale	7.000
b.1) finanziamenti diretti disponibili messi a disposizione da parte di soggetti esterni	
b.2) finanziamenti diretti acquisibili con certezza, messi a disposizione da parte di soggetti esterni	
c) cofinanziamento richiesto al MIUR (max 70% del costo complessivo)	*43.400*
Totale	*62.000*

19 - Certifico la dichiarata disponibilità e l'utilizzabilità dei finanziamenti a.1) a.2) a.3) b.1) b.2)

SI

Firma _____

I dati contenuti nella domanda di finanziamento sono trattati esclusivamente per lo svolgimento delle funzioni istituzionali del MIUR. Incaricato del trattamento è il CINECA- Dipartimento Servizi per il MIUR. La consultazione è altresì riservata al MIUR - D.G. della Ricerca -- Ufficio IV -- Settore PRIN, alla Commissione di Garanzia e ai referee scientifici. Il MIUR potrà anche procedere alla diffusione dei principali dati economici e scientifici relativi ai progetti finanziati. Responsabile del procedimento è il coordinatore del settore PRIN dell'ufficio IV della D.G. della Ricerca del MIUR.

Firma _____ Data 16/02/2009 ore 02:57

ALLEGATO

Curricula scientifici dei componenti il gruppo di ricerca

Testo italiano

1. ***MACEDONIO Damiano***

Curriculum:
Titoli di Studio-

21 marzo 2006. Dottorato di Ricerca in Informatica con menzione di Doctor Europaeus, presso l'Universita' Ca' Foscari di Venezia. Supervisori: Prof. Annalisa Bossi e Prof. Vladimiro Sassone.

27 marzo 2001. Laurea in Matematica, presso l'Universita' degli Studi di Padova. Voto finale: 110/110 cum laude. Supervisore: Prof. G. Sambin.

30 Giugno 1992. Diploma di Maturita' Scientifica, presso il Liceo Scientifico I. Nievo, Padova.

Formazione -

Gen. 2005 - Mar. 2006. Ph.D. student in Computer Science presso il Dipartimento di Informatica, University of Sussex (Brighton, Regno Unito). Supervisore: Prof. V. Sassone.

Nov. 2001 - Nov. 2005. Studente di Dottorato in Informatica presso l'Universit`a Ca' Foscari di Venezia. Titolare di borsa di studio ministeriale. Supervisore: Prof. A. Bossi.

Settembre 2003. First Advanced School on Mobile Computing per 20 partecipanti selezionati. Scuola Normale Superiore, Pisa. Superati tutti gli esami finali.

Settembre 2002. 3rd International School on Foundations of Security Analysis and Design (FOSAD). Bertinoro (Forli'-Cesena).

Maggio 2002. International Summer School for Graduate Studies in Computer Science (BISS'02). Bertinoro (Forli'-Cesena). Superati tutti gli esami finali.

Attivita' Professionali -

Ott. 2008 - Presente Assegnista di ricerca presso il Dipartimento di Informatica, Universita' Ca' Foscari di Venezia. Programma di ricerca del Dipartimento di Informatica 2008: Modelli formali per la
sicurezza in Service Oriented Computing. Responsabile: Prof. M. Bugliesi.

Giu. 2007 - Mag. 2008 Assegnista di ricerca presso il Dipartimento di Informatica, Universita' Ca' Foscari di Venezia. Programma di ricerca del Dipartimento di Informatica 2007: Sviluppo di metodi formali
per la verifica di proprieta' di sicurezza di sistemi software. Responsabile: Prof. A. Bossi.

Giu. 2006 - Mag. 2007. Assegnista di ricerca presso il Dipartimento di Informatica, Universita' Ca' Foscari di Venezia. Progetto PRIN 2005: Fondamenti logici dei sistemi distribuiti e codice mobile.
Responsabile: Prof. M. Bugliesi.

Nov. 2004 - Apr. 2005. Research fellow presso il Dipartimento di Informatica, University of Sussex (Brighton, Regno Unito). Progetto EU FET-GC IST-2001-32617: MyThS - Models and Types for Security
in Mobile Distributed Systems. Responsabile: Prof. V. Sassone.
Ott. 2003 - Set. 2004. Marie Curie fellow presso il Dipartimento di Informatica, University of Sussex (Brighton, Regno Unito). Progetto EU IHP HPMT-CT-2001-00290: DisCo - Semantic Foundations
of Distributed Computation. Responsabile: Prof. V. Sassone.

Apr. 2001 - Ago. 2001. Contratto post lauream presso il Dipartimento di Matematica Pura e Applicata, Universita' di Padova. Computazione e logica: la logica di base come strumento per un nuovo approccio
unitario. Responsabile: Prof. G. Sambin.

Pubblicazioni:

- *G. CONFORTI, MACEDONIO D., V. SASSONE (2007). Static BiLog: a Unifying Language for Spatial Structures. FUNDAMENTA INFORMATICAE, vol. 80; p. 91-110, ISSN: 0169-2968*
- *M. BUGLIESI, MACEDONIO D., S. ROSSI (2007). Static vs Dynamic Typing for Access Control in Pi-Calculus. In: Advances in Computer Science - ASIAN 2007. Computer and Network Security, 12th Asian Computing Science Conference, ProceedingsLNCS - Springer, vol. 4846, p. 282-296, ISBN/ISSN: 978-3-540-76927-9*

- *CHADHA R, MACEDONIO D., SASSONE V (2006). A Hybrid Intuitionistic Logic: Semantics and Decidability. JOURNAL OF LOGIC AND COMPUTATION, vol. 16(1); p. 27-59, ISSN: 0955-792X*

- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2005). Information flow in secure contexts. JOURNAL OF COMPUTER SECURITY, vol. 13(3); p. 391-422, ISSN: 0926-227X*
- *CONFORTI G, MACEDONIO D., SASSONE V (2005). Spatial Logics for Bigraphs. In: Automata, Languages and Programming, 32nd International Colloquium (ICALP), Proceedings, July 11-15, 2005, vol. 3580 LNCS, p. 766-778, ISBN/ISSN: 3-540-27580-0*

- *BOSSI A, FOCARDI R, MACEDONIO D., PIAZZA C, ROSSI S (2004). Unwinding in Information Flow Security. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 99; p. 127-154, ISSN: 1571-0661*

- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2003). Information Flow Security and Recursive Systems. In: 8th Italian Conference on Theoretical Computer Science (ICTCS 2003), Proceedings., October 13-15, 2003, vol. 2841 LNCS, p. 369-382, ISBN/ISSN: 3-540-20216-1*
- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2003). Secure Contexts for Confidential Data. In: 16th IEEE Computer Security Foundations Workshop (CSFW), Proceedings, 30 June - 2 July 2003, p. 14-28, ISBN/ISSN: 0-7695-1927-X*

2. ***MODESTI Paolo***

Curriculum:
Curriculum vitae:

---------- Personal information ----------

Surname/Name: MODESTI PAOLO
Home Address: Viale Q.Sella 44, 36100, Vicenza, Italy
Phone(s): +39-0444-570326
Mobile: +39-328-4669829
E-mail(s): modesti@dsi.unive.it paolo.modesti@gmail.com
Nationality Italian
Date of birth April 11, 1966
Gender Male

---------- Education ----------

(o) 1986-1990, Master's Degree in Computer Science (Laurea in Scienze dell'Informazione)
Organization: University of Udine (Italy)
Principal subjects: Cryptography, Operating Systems, Programming.
My thesis title is "Cryptographic threshold schemes".

(o) 1997-1999, Master in Software Engineering
Organization: Software Engineering Research Center (USA) - Tecnopadova (Padova, Italy)
My main project focused on interoperability in a distributed environment.
Courses, assignments and final project all completed in English.

(o) 2002-2003, Master's Degree in Informatics (Laurea specialistica in Informatica)
Principal subjects: IT Security, Cryptography, Operating Systems, Networks, Programming.
Organization: University of Udine (Italy)

I successfully participated to several courses and seminars.
Some of them are the following:
"IT Security" (2005)
** "Open Environments and Distributed Systems" (2001)*
** "Application Development in distributed environments" (2001)*
** "Process Reengineering and Workflow Management" (1999)*
"Unix"(1997)
"Oracle" (1997)
"Lan Manager" (1997)

** These courses were organized by CNIPA (formerly AIPA) "Italian National Centre for IT in the Public Administration", the others by "Agenzia delle Entrate" and "Italian Ministry of Finance".*

---------- Current position ----------

(o) Jan 2008 to present
Position: PhD student in Computer Science
Employer: University Ca'Foscari of Venice - Department of Computer Science, Via Torino 155, Mestre (VE), Italy
Sector: Academic Research
Research Area: IT Security, Language Based Security, Web Services
Past Exams:
"Models and Calculi for security", UniVE, P.Degano (University of Pisa)
"Fault Tolerance in Distributed Algorithms", BISS2008, P.Verissimo (University of Lisboa)
"Context-Aware Database", BISS2008, L.Tanca (Politecnico di Milano)
"Distributed Algorithms", UniVE, F.Luccio (University of Venezia)
"Intellectual Property and Patents", UniVE, E.Toniolo (Treviso Tecnologie)
Attended schools:
Fosad "International School on Foundations of Security Analysis and Design" 2008

---------- Work experience ----------

(o) Jan 1994 - Jan 2008 (currently on leave to participate to the PhD program)
Position: IT system Manager
Employer: Agenzia delle Entrate (Italian Revenue Service), UL Vicenza 1, Corso Palladio 149, 36100 Vicenza, Italy
Sector: Public Administration IT systems
Activities: Responsible for Information System management and administration for my branch; implementation of IT security. I organized and supervised the work of 2 system administrators.
1996-2000 - Advisor for the teaching of computer skills working group, "Italian Ministry of Finance" , "Central Tributary School", Rome.
1997 - I was an advisor for IT projects evaluation and contracts working group, "Italian Ministry of Finance", Rome

(o) May 1, 2007 - June 22, 2007
Position: IТ Security Advisor
Employer: EU-Cafao BiH, Fra Andela Zvizdovica 1, 71000 Sarajevo, Bosnia and Herzegovina
Sector: European Union mission in Bosnia and Herzegovina
Activities: Carried out a security audit of the Bosnian Indirect Taxation Authority's IT system in the HQ and Regional Centres, considering the security and integrity of HW,SW, networks, data, management procedures.

(o) Jul 1997 - Sep 1997
Position: Summer intern
Employer: Bellcore (now Telcordia), Applied Research, 445 South Street, Morristown, NJ, USA
Sector: Applied Research
Activities: Participated to a research program on distributed object technology.

(o) Oct 1990 - Jan 1994
Position: Computer Science Professor
Employer: IISSS "Boscardin", via Baden Powell 35, 36100 Vicenza (Italy)
Sector: High School
Activities: Taught programming languages and operating systems

(o) Dec 1989 - Jan 1994
Position: Office Automation Consultant
Employer: Several
Sector: IT consultancy
Activities: Organized and developed training courses in Computer Usage

---------- Languages ----------

Mother tongue Italian

Other language(s)
Self-assessment (*) Understanding Speaking Writing
English C2 C1 C1
French C1 B2 B2
Bulgarian C1 B2 B1
(*) Common European Framework of Reference (CEF) level [A1(lower)->C2(higher)]

---------- Technical skills and competences ----------

Excellent knowledge of:
IT Security: HW, SW, Networks, Cryptography, procedures and policies
Operating Systems: UNIX, Windows, OS/2, DOS
Networking: Internet, TCP/IP, ISO/OSI, LAN Server, network devices
Programming Languages: Java, Visual Basic, C/C++, Pascal, OCAML, Assembler
Web design: HTML, ASP, MS FrontPage
Database design and programming (mainly MS Access and VBA)
Office Automation: MS Office (Word, Excel, PowerPoint, Access)

----
pubblicazioni non disponibili

3. ***ROSSI Sabina***

Curriculum:
Sabina Rossi è ricercatrice presso l'Università di Venezia "Ca' Foscari" dal Settembre 2000.
Ha ottenuto il Dottorato di Ricerca in Matematica Computazionale e Informatica Matematica presso l'Università di Padova nel Luglio 1994.
Ha avuto posizioni di visiting researcher presso l'università di Namur, Belgio, (da Settembre 1994 ad Agosto 1995), presso l'università Catholique de Louvain-la-Neuve, Belgio, (da Settembre a Dicembre 1995), e presso il Laboratorio PPS dell'università di Parigi Diderot, Paris 7, (da Giugno a Luglio 2007).

Sabina Rossi ha preso parte a numerosi progetti di ricerca finanziati dai principali enti italiani e internazionali, tra cui la Comunità Europea e il Ministero Italiano dell'Istruzione, dell'Università e della Ricerca.

Negli ultimi anni è stata coinvolta come membro dei comitati di programma di diverse conferenze e workshop internazionali: LOPSTR'02, LOPSTR'03, FMSE'04, LOPSTR'06, VERIFY'06, LOPSTR'08, CILC'08, INFORMATICS'08, WLPE'08, CILC'09.

Sabina Rossi è autrice di più di 40 articoli in riviste e conferenze internazionali. Attualmente, i suoi interessi di ricerca riguardano i calcoli formali per la specifica e l'analisi di sistemi concorrenti e distribuiti con particolare attenzione all'analisi e alla verifica di proprietà di sicurezza, quali proprietà di iformation flow
e non-interferenza.

Pubblicazioni:

- *BOSSI A, PIAZZA C, ROSSI S. (2008). Action Refinement in Process Algebra and Security Issues. LECTURE NOTES IN COMPUTER SCIENCE, vol. 4915; p. 201-217, ISSN: 0302-9743*
- *BOSSI A, PIAZZA C, ROSSI S. (2007). Compositional Information Flow Security for Concurrent Programs. JOURNAL OF COMPUTER SECURITY, vol. 15(3); p. 373-416, ISSN: 0926-227X*
- *CRAFA S, ROSSI S. (2007). Controlling Information Release in the pi-calculus. INFORMATION AND COMPUTATION, vol. 285 (8); p. 1235-1273, ISSN: 0890-5401*
- *M. BUGLIESI, D. MACEDONIO, ROSSI S. (2007). Static vs Dynamic Typing for Access Control in Pi-Calculus. LECTURE NOTES IN COMPUTER SCIENCE, vol. 4846; p. 282-296, ISSN: 0302-9743*
- *FOCARDI R, ROSSI S. (2006). Information Flow Security in Dynamic Contexts. JOURNAL OF COMPUTER SECURITY, vol. 14, n. 1; p. 65-110, ISSN: 0926-227X*
- *BOSSI A, PIAZZA C, ROSSI S. (2005). Unwinding Conditions for Security in Imperative Languages. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3573; p. 85-100, ISSN: 0302-9743*
- *BOSSI A. MACEDONIO D, PIAZZA C, ROSSI S. (2005). Information Flow in Secure Contexts. JOURNAL OF COMPUTER SECURITY, vol. 13, n. 3; p. 391-422, ISSN: 0926-227X*
- *BUGLIESI M, ROSSI S. (2005). Non-Interference Proof Techniques for the Analysis of Cryptographic Protocols. JOURNAL OF COMPUTER SECURITY, vol. 13, n. 1; p. 87-113, ISSN: 0926-227X*
- *CRAFA S, ROSSI S. (2005). A Theory of Noninterference for the pi-calculus. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3705; p. 2-18, ISSN: 0302-9743*
- *FOCARDI R, ROSSI S., SABELFELD A (2005). Bridging Language-Based and Process Calculi Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3441; p. 299-315, ISSN: 0302-9743*
- *BOSSI A, COCCO N, ETALLE S, ROSSI S. (2004). Declarative Semantics of Input Consuming Logic Programs. LECTURE NOTES IN COMPUTER*

SCIENCE, vol. 3049; p. 90-114, ISSN: 0302-9743

- *BOSSI A, ETALLE S, ROSSI S., SMAUS J.-G (2004). Termination of Simply Moded Logic Programs with Dynamic Scheduling. ACM TRANSACTIONS ON COMPUTATIONAL LOGIC, vol. 5, n. 3; p. 470-507, ISSN: 1529-3785*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2004). Unwinding in Information Flow Security. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 99; p. 127-154, ISSN: 1571-0661*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2004). Verifying Persistent Security Properties. COMPUTER LANGUAGES, SYSTEMS AND STRUCTURES, vol. 30, n. 3-4; p. 231-258, ISSN: 1477-8424*
- *PIAZZA C, PIVATO E, ROSSI S. (2004). CoPS - Checker of Persistent Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2988; p. 144-152, ISSN: 0302-9743*

- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2003). A Proof System for Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2664; p. 199-218, ISSN: 0302-9743*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2003). Bisimulation and Unwinding for Verifying Possibilistic Security Properties. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2575; p. 223-237, ISSN: 0302-9743*
- *BOSSI A, MACEDONIO D, PIAZZA C, ROSSI S. (2003). Information Flow Security and Recursive Systems. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2841; p. 369-382, ISSN: 0302-9743*
- *BUGLIESI M, CECCATO A, ROSSI S. (2003). Context-Sensitive Equivalences for Non-Interference based Protocol Analysis. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2751; p. 364-375, ISSN: 0302-9743*

- *BOSSI A, COCCO N, ETALLE S, ROSSI S. (2002). On Modular Termination Proofs of General Logic Programs. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n. 3; p. 263-291, ISSN: 1471-0684*
- *BOSSI A, ETALLE S, ROSSI S. (2002). Properties of Input-Consuming Derivations. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n.2; p. 125-154, ISSN: 1471-0684*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2002). Transforming Processes to Check and Ensure Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2422; p. 271-286, ISSN: 0302-9743*
- *FOCARDI R, PIAZZA C, ROSSI S. (2002). Proofs Methods for Bisimulation based Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2294; p. 16-31, ISSN: 0302-9743*
- *LE CHARLIER B, ROSSI S., VAN HENTENRYCK P (2002). Sequence-based Abstract Interpretation of Prolog. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n. 1; p. 25-84, ISSN: 1471-0684*

- *BOSSI A, ETALLE S, ROSSI S., SMAUS J.-G (2001). Semantics and Termination of Simply-moded Logic Programs with Dynamic Scheduling. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2028; p. 402-416, ISSN: 0302-9743*
- *CORTESI A, LE CHARLIER B, ROSSI S. (2001). Reexecution-based Analysis of Logic Programs with Delay Declarations. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2244; p. 395-405, ISSN: 0302-9743*
- *CORTESI A, ROSSI S., LE CHARLIER B (2001). Operational Semantics for Reexecution-based Analysis of Logic Programs with Delay Declarations. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 48, ISSN: 1571-0661*

- *BOSSI A, ETALLE S, ROSSI S. (2000). Semantics of input-consuming programs. LECTURE NOTES IN COMPUTER SCIENCE, vol. 1861; p. 194-208, ISSN: 0302-9743*
- *BOSSI A, ETALLE S, ROSSI S. (2000). Semantics of well-moded input-consuming logic programs. COMPUTER LANGUAGES, vol. 26, n. 1; p. 1-25, ISSN: 0096-0551*

- *BOSSI A, ETALLE S, ROSSI S. (1999). Properties of Input-Consuming Derivations. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 30, n. 1, ISSN: 1571-0661*

Testo inglese

1. ***MACEDONIO Damiano***

Curriculum:
I was born in Padova on March 13th, 1973.
I attended my secondary school at Liceo Scientifico "I. Nievo" in Padova.
On March 27th, 2001 I graduated cum laude in Mathematics at Università di Padova.
From November 2001 to November 2005 I was a Ph.D. student in Computer Science at Università Ca' Foscari di Venezia.
From October 2003 to February 2006 I visited the Informatics Department, University of Sussex, Brighton (UK): from October 2003 to October 2004 I was a Marie Curie student funded by the EU project DisCo; from November 2004 to May 2005 I was a research fellow funded by the EU research project MyThS.
On June 1st, 2006 I received my PhD in Computer Science with European Doctor mention.
From June 2006 to May 2007 I was a research fellow founded by the PRIN project 2005 "Fondamenti logici dei sistemi distribuiti e codice mobile", at the Dipartimento di Informatica, Università Ca' Foscari di Venezia.
From June 2007 to May 2008 I was a research fellow founded by the Research Project "Sviluppo di metodi formali per la verifica di proprieta' di sicurezza di sistemi software", at the Dipartimento di Informatica, Università Ca' Foscari di Venezia.
From October 2008 I am a research fellow founded by the Research Project "Modelli formali per la sicurezza in Service Oriented Computing", at the Dipartimento di Informatica, Università Ca' Foscari di Venezia.
I am also a member of the Logic Group at the University of Padova, the Foundations of Computation Group at the Department of Informatics, University of Sussex, and GULP, the Italian Association for Logic Programming.

Pubblicazioni:

- *G. CONFORTI, MACEDONIO D., V. SASSONE (2007). Static BiLog: a Unifying Language for Spatial Structures. FUNDAMENTA INFORMATICAE, vol. 80; p. 91-110, ISSN: 0169-2968*
- *M. BUGLIESI, MACEDONIO D., S. ROSSI (2007). Static vs Dynamic Typing for Access Control in Pi-Calculus. In: Advances in Computer Science - ASIAN 2007. Computer and Network Security, 12th Asian Computing Science Conference, ProceedingsLNCS - Springer, vol. 4846, p. 282-296, ISBN/ISSN: 978-3-540-76927-9*

- *CHADHA R, MACEDONIO D., SASSONE V (2006). A Hybrid Intuitionistic Logic: Semantics and Decidability. JOURNAL OF LOGIC AND COMPUTATION, vol. 16(1); p. 27-59, ISSN: 0955-792X*

- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2005). Information flow in secure contexts. JOURNAL OF COMPUTER SECURITY, vol. 13(3); p. 391-422, ISSN: 0926-227X*
- *CONFORTI G, MACEDONIO D., SASSONE V (2005). Spatial Logics for Bigraphs. In: Automata, Languages and Programming, 32nd International Colloquium (ICALP), Proceedings, July 11-15, 2005, vol. 3580 LNCS, p. 766-778, ISBN/ISSN: 3-540-27580-0*

- *BOSSI A, FOCARDI R, MACEDONIO D., PIAZZA C, ROSSI S (2004). Unwinding in Information Flow Security. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 99; p. 127-154, ISSN: 1571-0661*

- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2003). Information Flow Security and Recursive Systems. In: 8th Italian Conference on Theoretical Computer Science (ICTCS 2003), Proceedings., October 13-15, 2003, vol. 2841 LNCS, p. 369-382, ISBN/ISSN: 3-540-20216-1*
- *BOSSI A, MACEDONIO D., PIAZZA C, ROSSI S (2003). Secure Contexts for Confidential Data. In: 16th IEEE Computer Security Foundations Workshop (CSFW), Proceedings, 30 June - 2 July 2003, p. 14-28, ISBN/ISSN: 0-7695-1927-X*

2. ***MODESTI Paolo***

Curriculum:
Curriculum vitae:

---------- Personal information ----------

Surname/Name: MODESTI PAOLO
Home Address: Viale Q.Sella 44, 36100, Vicenza, Italy
Phone(s): +39-0444-570326
Mobile: +39-328-4669829
E-mail(s): modesti@dsi.unive.it paolo.modesti@gmail.com
Nationality Italian
Date of birth April 11, 1966
Gender Male

---------- Education ----------

(o) 1986-1990, Master's Degree in Computer Science (Laurea in Scienze dell'Informazione)
Organization: University of Udine (Italy)
Principal subjects: Cryptography, Operating Systems, Programming.
My thesis title is "Cryptographic threshold schemes".

(o) 1997-1999, Master in Software Engineering
Organization: Software Engineering Research Center (USA) - Tecnopadova (Padova, Italy)
My main project focused on interoperability in a distributed environment.
Courses, assignments and final project all completed in English.

(o) 2002-2003, Master's Degree in Informatics (Laurea specialistica in Informatica)
Principal subjects: IT Security, Cryptography, Operating Systems, Networks, Programming.
Organization: University of Udine (Italy)

I successfully participated to several courses and seminars.
Some of them are the following:
"IT Security" (2005)
** "Open Environments and Distributed Systems" (2001)*
** "Application Development in distributed environments" (2001)*
** "Process Reengineering and Workflow Management" (1999)*
"Unix"(1997)
"Oracle" (1997)
"Lan Manager" (1997)

** These courses were organized by CNIPA (formerly AIPA) "Italian National Centre for IT in the Public Administration", the others by "Agenzia delle Entrate" and "Italian Ministry of Finance".*

---------- Current position ----------

(o) Jan 2008 to present
Position: PhD student in Computer Science
Employer: University Ca'Foscari of Venice - Department of Computer Science, Via Torino 155, Mestre (VE), Italy
Sector: Academic Research
Research Area: IT Security, Language Based Security, Web Services
Past Exams:
"Models and Calculi for security", UniVE, P.Degano (University of Pisa)
"Fault Tolerance in Distributed Algorithms", BISS2008, P.Verissimo (University of Lisboa)
"Context-Aware Database", BISS2008, L.Tanca (Politecnico di Milano)
"Distributed Algorithms", UniVE, F.Luccio (University of Venezia)
"Intellectual Property and Patents", UniVE, E.Toniolo (Treviso Tecnologie)
Attended schools:
Fosad "International School on Foundations of Security Analysis and Design" 2008

---------- Work experience ----------

(o) Jan 1994 - Jan 2008 (currently on leave to participate to the PhD program)
Position: IT system Manager
Employer: Agenzia delle Entrate (Italian Revenue Service), UL Vicenza 1, Corso Palladio 149, 36100 Vicenza, Italy

Sector: Public Administration IT systems
Activities: Responsible for Information System management and administration for my branch; implementation of IT security. I organized and supervised the work of 2 system administrators.
1996-2000 - Advisor for the teaching of computer skills working group, "Italian Ministry of Finance" , "Central Tributary School", Rome.
1997 - I was an advisor for IT projects evaluation and contracts working group, "Italian Ministry of Finance", Rome

(o) May 1, 2007 - June 22, 2007
Position: IТ Security Advisor
Employer: EU-Cafao BiH, Fra Andela Zvizdovica 1, 71000 Sarajevo, Bosnia and Herzegovina
Sector: European Union mission in Bosnia and Herzegovina
Activities: Carried out a security audit of the Bosnian Indirect Taxation Authority's IT system in the HQ and Regional Centres, considering the security and integrity of HW,SW, networks, data, management procedures.

(o) Jul 1997 - Sep 1997
Position: Summer intern
Employer: Bellcore (now Telcordia), Applied Research, 445 South Street, Morristown, NJ, USA
Sector: Applied Research
Activities: Participated to a research program on distributed object technology.

(o) Oct 1990 - Jan 1994
Position: Computer Science Professor
Employer: IISSS "Boscardin", via Baden Powell 35, 36100 Vicenza (Italy)
Sector: High School
Activities: Taught programming languages and operating systems

(o) Dec 1989 - Jan 1994
Position: Office Automation Consultant
Employer: Several
Sector: IT consultancy
Activities: Organized and developed training courses in Computer Usage

---------- Languages ----------

Mother tongue Italian

Other language(s)
Self-assessment (*) Understanding Speaking Writing
English C2 C1 C1
French C1 B2 B2
Bulgarian C1 B2 B1
(*) Common European Framework of Reference (CEF) level [A1(lower)->C2(higher)]

---------- Technical skills and competences ----------

Excellent knowledge of:
IT Security: HW, SW, Networks, Cryptography, procedures and policies
Operating Systems: UNIX, Windows, OS/2, DOS
Networking: Internet, TCP/IP, ISO/OSI, LAN Server, network devices
Programming Languages: Java, Visual Basic, C/C++, Pascal, OCAML, Assembler
Web design: HTML, ASP, MS FrontPage
Database design and programming (mainly MS Access and VBA)
Office Automation: MS Office (Word, Excel, PowerPoint, Access)

----

3. ***ROSSI Sabina***

Curriculum:
Sabina Rossi is Assistant Professor at the University Ca' Foscari of Venice since September 2000.
She received her PhD in Computational Mathematics and Informatics at the University of Padova in July 1994.
She has held research positions at the University of Namur, Belgium, (September 1994 - August 1995), University Catholique de Louvain-la-Neuve, Belgium, (September-December 1995), and at the Laboratoire PPS of the University Paris Diderot, Paris 7, (June-July 2007).

Sabina Rossi has partecipated in several research projects, funded by the major national and international funding agencies among which EU and the Italian Ministry of Scientific and Technological Research (formely MURST).

Recently, she has served as program committee member for several international conferences and workshops: LOPSTR'02, LOPSTR'03, FMSE'04, LOPSTR'06, VERIFY'06, LOPSTR'08, CILC'08, INFORMATICS'08, WLPE'08, CILC'09.

She is co-author of over 40 articles in international journals and conferences with program committees. Her current research is centered on formal calculi for concurrent and distributed systems, with specific focus of the analysis and verification of security properties, information-flow properties and non-interference.

Pubblicazioni:

- *BOSSI A, PIAZZA C, ROSSI S. (2008). Action Refinement in Process Algebra and Security Issues. LECTURE NOTES IN COMPUTER SCIENCE, vol. 4915; p. 201-217, ISSN: 0302-9743*
- *BOSSI A, PIAZZA C, ROSSI S. (2007). Compositional Information Flow Security for Concurrent Programs. JOURNAL OF COMPUTER SECURITY, vol. 15(3); p. 373-416, ISSN: 0926-227X*
- *CRAFA S, ROSSI S. (2007). Controlling Information Release in the pi-calculus. INFORMATION AND COMPUTATION, vol. 285 (8); p. 1235-1273, ISSN: 0890-5401*
- *M. BUGLIESI, D. MACEDONIO, ROSSI S. (2007). Static vs Dynamic Typing for Access Control in Pi-Calculus. LECTURE NOTES IN COMPUTER SCIENCE, vol. 4846; p. 282-296, ISSN: 0302-9743*
- *FOCARDI R, ROSSI S. (2006). Information Flow Security in Dynamic Contexts. JOURNAL OF COMPUTER SECURITY, vol. 14, n. 1; p. 65-110, ISSN:*

0926-227X

- *BOSSI A, PIAZZA C, ROSSI S. (2005). Unwinding Conditions for Security in Imperative Languages. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3573; p. 85-100, ISSN: 0302-9743*
- *BOSSI A. MACEDONIO D, PIAZZA C, ROSSI S. (2005). Information Flow in Secure Contexts. JOURNAL OF COMPUTER SECURITY, vol. 13, n. 3; p. 391-422, ISSN: 0926-227X*
- *BUGLIESI M, ROSSI S. (2005). Non-Interference Proof Techniques for the Analysis of Cryptographic Protocols. JOURNAL OF COMPUTER SECURITY, vol. 13, n. 1; p. 87-113, ISSN: 0926-227X*
- *CRAFA S, ROSSI S. (2005). A Theory of Noninterference for the pi-calculus. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3705; p. 2-18, ISSN: 0302-9743*
- *FOCARDI R, ROSSI S., SABELFELD A (2005). Bridging Language-Based and Process Calculi Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3441; p. 299-315, ISSN: 0302-9743*

- *BOSSI A, COCCO N, ETALLE S, ROSSI S. (2004). Declarative Semantics of Input Consuming Logic Programs. LECTURE NOTES IN COMPUTER SCIENCE, vol. 3049; p. 90-114, ISSN: 0302-9743*
- *BOSSI A, ETALLE S, ROSSI S., SMAUS J.-G (2004). Termination of Simply Moded Logic Programs with Dynamic Scheduling. ACM TRANSACTIONS ON COMPUTATIONAL LOGIC, vol. 5, n. 3; p. 470-507, ISSN: 1529-3785*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2004). Unwinding in Information Flow Security. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 99; p. 127-154, ISSN: 1571-0661*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2004). Verifying Persistent Security Properties. COMPUTER LANGUAGES, SYSTEMS AND STRUCTURES, vol. 30, n. 3-4; p. 231-258, ISSN: 1477-8424*
- *PIAZZA C, PIVATO E, ROSSI S. (2004). CoPS - Checker of Persistent Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2988; p. 144-152, ISSN: 0302-9743*

- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2003). A Proof System for Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2664; p. 199-218, ISSN: 0302-9743*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2003). Bisimulation and Unwinding for Verifying Possibilistic Security Properties. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2575; p. 223-237, ISSN: 0302-9743*
- *BOSSI A, MACEDONIO D, PIAZZA C, ROSSI S. (2003). Information Flow Security and Recursive Systems. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2841; p. 369-382, ISSN: 0302-9743*
- *BUGLIESI M, CECCATO A, ROSSI S. (2003). Context-Sensitive Equivalences for Non-Interference based Protocol Analysis. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2751; p. 364-375, ISSN: 0302-9743*

- *BOSSI A, COCCO N, ETALLE S, ROSSI S. (2002). On Modular Termination Proofs of General Logic Programs. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n. 3; p. 263-291, ISSN: 1471-0684*
- *BOSSI A, ETALLE S, ROSSI S. (2002). Properties of Input-Consuming Derivations. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n.2; p. 125-154, ISSN: 1471-0684*
- *BOSSI A, FOCARDI R, PIAZZA C, ROSSI S. (2002). Transforming Processes to Check and Ensure Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2422; p. 271-286, ISSN: 0302-9743*
- *FOCARDI R, PIAZZA C, ROSSI S. (2002). Proofs Methods for Bisimulation based Information Flow Security. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2294; p. 16-31, ISSN: 0302-9743*
- *LE CHARLIER B, ROSSI S., VAN HENTENRYCK P (2002). Sequence-based Abstract Interpretation of Prolog. THEORY AND PRACTICE OF LOGIC PROGRAMMING, vol. 2, n. 1; p. 25-84, ISSN: 1471-0684*

- *BOSSI A, ETALLE S, ROSSI S., SMAUS J.-G (2001). Semantics and Termination of Simply-moded Logic Programs with Dynamic Scheduling. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2028; p. 402-416, ISSN: 0302-9743*
- *CORTESI A, LE CHARLIER B, ROSSI S. (2001). Reexecution-based Analysis of Logic Programs with Delay Declarations. LECTURE NOTES IN COMPUTER SCIENCE, vol. 2244; p. 395-405, ISSN: 0302-9743*
- *CORTESI A, ROSSI S., LE CHARLIER B (2001). Operational Semantics for Reexecution-based Analysis of Logic Programs with Delay Declarations. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 48, ISSN: 1571-0661*

- *BOSSI A, ETALLE S, ROSSI S. (2000). Semantics of input-consuming programs. LECTURE NOTES IN COMPUTER SCIENCE, vol. 1861; p. 194-208, ISSN: 0302-9743*
- *BOSSI A, ETALLE S, ROSSI S. (2000). Semantics of well-moded input-consuming logic programs. COMPUTER LANGUAGES, vol. 26, n. 1; p. 1-25, ISSN: 0096-0551*

- *BOSSI A, ETALLE S, ROSSI S. (1999). Properties of Input-Consuming Derivations. ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE, vol. 30, n. 1, ISSN: 1571-0661*