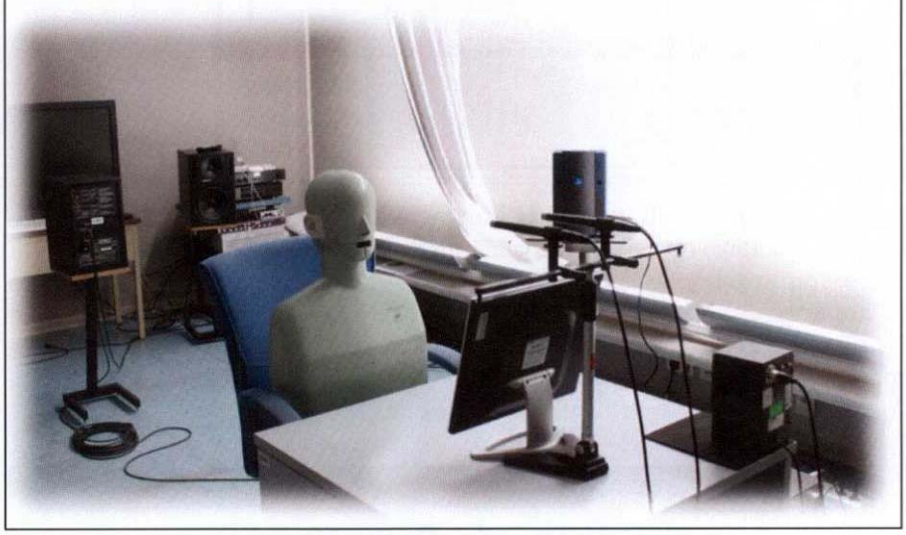
ALTRE ATTIVITÀ SULLE TEMATICHE DELLA QUALITÀ AUDIO

Nell'ambito delle comunicazioni audio personali, un problema attualmente molto sentito è quello dell'ottimizzazione della "realtà aumentata", ovvero lo sforzo di aumentare la qualità percepita dei servizi disponibili a livelli tali da renderla trasparente al confronto di un'esperienza reale.

L'evoluzione delle interfacce di nuova generazione nelle comunicazioni personali prevede il progressivo distacco dell'utente dal vincolo fisico di utilizzo di supporti, come potrebbero essere una cuffia con microfono, oppure la cornetta del telefono o comunque un terminale "scomodo". Il chiaro vantaggio è l'aumento della naturalezza nelle conversazioni, confluente in un notevole aumento della percezione qualitativa.

Figura 5: Set-up sperimentale per la simulazione di una comunicazione viva-voce con rumore e interferenti audio.



Lo sviluppo di questo obiettivo ha condotto alla definizione di numerose problematiche sulla qualità dell'audio percepito nei sistemi hands-free. I temi principali sono sicuramente: la cancellazione d'eco acustica, ovvero la cancellazione del feedback audio di ritorno (tipicamente dal sistema di riproduzione in quello microfonico) in un sistema a viva voce; la cancellazione attiva di rumore, ossia l'uso di sistemi adattativi per la soppressione del rumore di sottofondo in una conversazione; il "beamforming", cioè l'uso di una schiera di microfoni per isolare il suono proveniente da una specifica direzione rispetto a tutte le altre fonti diffuse e/o puntuali.

FUB, in collaborazione con l'Università di Roma "La Sapienza", Facoltà di Ingegneria, si dedica allo studio sia dei sistemi sia delle metriche che possono definire lo standard qualitativo di un sistema viva-voce che utilizzi una o più delle predette tecnologie.

PUBBLICAZIONI E INTERVENTI

Conferenze internazionali

[1] D. Comminiello, M. Scarpiniti, R. Parisi, A. Uncini, "A Functional Link Based Nonlinear Echo Canceller Exploiting Sparsity", Proceedings of *IWAENC*, Tel Aviv, agosto 2010.

[2] A. Cirillo, R. Parisi, M. Scarpiniti, A. Uncini, "Simplified Optimal Line Selection for Acoustic Localization in the Presence of Reverberation", Proceedings of the *EUSIPCO 2010 conference*, Aalborg, Denmark, agosto 2010.

[3] E. Mammi, G. Russo, P. Talone, "Television over IP Overview", Atti di *EUVIP 2010, 2nd European Workshop on Visual Information Processing*, Paris, France, 5-7 luglio 2010.

[4] D. Comminiello, M. Scarpiniti, R. Parisi, A. Uncini, "A Novel Affine Projection Algorithm for Superdirective Microphone Array Beamforming", Proceedings of *ISCAS 2010 Conference*, Paris, France, maggio 2010.

[5] C. M. Zannini, A. Cirillo, R. Parisi, A. Uncini, "Improved TDOA Disambiguation Techniques for Sound Source Localization in Reverberant Environments", Proceedings of the *ISCAS 2010 Conference*, Paris, France, maggio 2010.

[6] E. Mammi, G. Russo, A. Neri, "Evaluation of AL-FEC Performance for IP Television Services QoS", Atti di *IS&T/SPIE Electronic Imaging Science and Technology*, San Jose, California, USA, 17-21 gennaio 2010.

Conferenze nazionali

[7] E. Mammi, S. Pompei, A. Valenti, G. Russo, D. Milanesio, V. Sardella, "Valutazione Sperimentale delle prestazioni di servizi televisivi su reti ottiche GbE di tipo Unmanaged e Managed", *Fotonica 2010*, Pisa, 25-27 maggio 2010.

[8] G. Russo, P. Talone, "RFID: Tecnologia e Normativa", *La tecnologia RFID: normativa, aspetti teorici, implementazioni pratiche*, Ordine degli Ingegneri, Roma, 15 marzo 2010.

Tesi di Laurea e Dottorato

[9] S. Mastrodascio, *Codici di protezione per la diffusione televisiva su rete IP*, Tesi di Laurea in Comunicazioni Mobili 1, Relatore Prof. Aldo Roveri, Università di Roma "La Sapienza", Co-relatori G.Russo, E. Mammi, FUB, luglio 2010.

[10] E. Mammi, *Codifica di canale orientata al pacchetto*, Tesi di Dottorato in Ingegneria delle Telecomunicazioni, Tutor Prof. Alessandro Neri, Università degli Studi Roma Tre, Paolo Talone, FUB.

Partecipazione a Gruppi di normativa, Tavoli tecnici e Comitati scientifici

M. Falcone, Partecipazione alla Commissione Nazionale ITU-R SG6 "Broadcasting service".

M. Falcone, Partecipazione al Working Group EBU P/LOUD "Loudness in Broadcasting".

M. Falcone, Partecipazione al Working Group EBU ECA "Audio Expert Community".

E. Mammi, G. Russo, P. Talone, Partecipazione al Tavolo Tecnico AGCOM sulla delibera AGCOM n. 244/08/CSP sulla qualità di accesso a Internet da postazione fissa.

M. Falcone, Membro del Comitato Scientifico della Conferenza Internazionale ICASSP 2010, Dallas, Texas, USA.

M. Falcone, Membro del Comitato Scientifico della Conferenza Internazionale INTERSPEECH 2010, Makuhari, Japan.

M. Falcone, Membro del Comitato Scientifico della Conferenza Internazionale Speaker Odyssey 2010, Brno, Czech Republic.

M. Falcone, Contributo al corso "Strumentazione avanzata di misura" presso Dipartimento Ingegneria Elettronica di Roma Tre.

E. Mammi, Contributo al corso "Teoria dell'informazione e codici" presso Dipartimento Ingegneria Elettronica di Roma Tre.

E. Mammi, Contributo al corso "Comunicazioni Multimediali" presso Dipartimento Ingegneria Elettronica di Roma Tre.

M. Falcone, Scientific coordinators for Speech Technology Evaluation in EVALITA 2009 "International Conference for Evaluation of NPL and Speech Tools for Italian", Reggio Emilia, dicembre 2009.

Area 4
PROCEDURE CRITICHE PER LA P.A. E LE ORGANIZZAZIONI COMPLESSE

RESPONSABILE DI AREA

DANIELE PERUCCHINI

Quest'Area è dedicata allo studio delle metodologie e delle strategie di protezione delle Infrastrutture Critiche nazionali ed europee.

Negli ultimi anni, in tutti i paesi occidentali, si è diffusa la consapevolezza che alcune delle infrastrutture (energia, trasporti, sanità, distribuzione degli alimenti, ecc.) che assicurano la qualità di vita dei cittadini sono altamente vulnerabili nei confronti di minacce sia di origine antropica sia di eventi naturali. Tali infrastrutture sono considerate critiche per il funzionamento stesso delle democrazie occidentali e, quindi, devono essere protette in modo adeguato per contrastare, in particolare, il temibile effetto domino che consiste, in estrema sintesi, nella propagazione a molte infrastrutture di un malfunzionamento che inizialmente colpisce una sola infrastruttura (ad esempio, si ricordi cosa è successo in Italia in occasione del blackout elettrico del 28 settembre 2003 o dello sciopero degli autotrasportatori nel maggio 2005).

Il 5 giugno 2008, il Consiglio dei Ministri Europei di Giustizia e Affari Interni ha approvato la direttiva europea 114/08, sull'identificazione e designazione delle Infrastrutture Critiche (IC) Europee. Tale direttiva individua la strategia comunitaria per migliorare la protezione delle infrastrutture critiche di rilevanza europea, richiedendo, tra l'altro, a ogni Stato Membro la realizzazione di un insieme di adempimenti "minimi", tra i quali l'individuazione delle Infrastrutture Critiche nazionali e l'attuazione a livello governativo di un'attività di controllo su tali infrastrutture[1].

In questo quadro di riferimento, l'Area 4 studia e analizza modelli di caratterizzazione degli effetti domino su scala nazionale e transnazionale. Questi studi scientifici hanno portato alla definizione di una metodologia originale sviluppata in cooperazione con la Presidenza del Consiglio e pubblicata sulla più importante rivista internazionale del settore. L'Area, inoltre, fornisce (ormai da alcuni anni) supporto scientifico al Punto di contatto nazionale per la protezione delle infrastrutture critiche (istituito presso la Presidenza del Consiglio dei Ministri) nelle sue attività istituzionali di negoziazione con gli altri Stati membri dell'UE relative sia alle modalità attuative della direttiva europea, sia alle iniziative scientifiche e metodologiche per la realizzazione delle misure di protezione delle infrastrutture critiche.

A corredo e completamento delle attività principali so-

[1] La direttiva europea 114/08 è stata recepita con provvedimento del Consiglio dei Ministri in data 11 gennaio 2011.

pra descritte, l'Area 4 intrattiene rapporti scientifici con i principali istituti omologhi a livello europeo, in primis l'IPSC (Institute for the Protection and Security of the Citizen) del Centro Comune di Ricerca di Ispra, con il mondo accademico nazionale e con le associazioni nazionali dedicate alle problematiche di *business continuity*, *disaster recovery* e di gestione delle emergenze.

Infine, la cultura generale e specifica necessaria per affrontare gli argomenti suesposti è stata utilizzata anche in ambiti diversi dalla protezione delle infrastrutture critiche e, in particolare, nel supporto alla Pubblica Amministrazione centrale nei processi decisionali di elevata valenza strategica. Tipicamente, tale esigenza si presenta in tutte le fasi (individuazione delle priorità di intervento, studio di fattibilità, progetto, realizzazione, gestione operativa, controllo e verifica delle prestazioni) di introduzione delle tecnologie ICT che richiedano anche il ricorso a soggetti esterni all'amministrazione stessa.

ANALISI DEGLI EFFETTI DOMINO

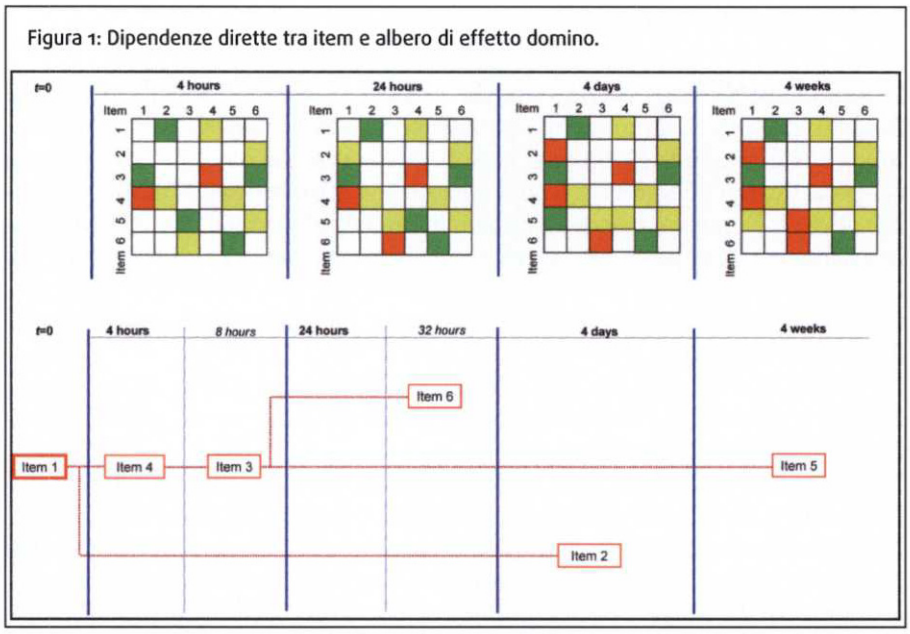
La letteratura scientifica ha tentato negli ultimi anni di fornire degli strumenti metodologici per studiare il problema dell'effetto domino e per definire un metodo scientifico condiviso per l'individuazione delle infrastrutture critiche e per la valutazione degli impatti susseguenti a malfunzionamenti. La complessità del problema affrontato non ha ancora consentito un approccio unificante dei diversi punti di vista.

Il modello di analisi perseguito dall'Area tende a soddisfare le esigenze del decisore istituzionale incaricato di governare ed aumentare la protezione delle infrastrutture critiche nazionali nel loro complesso e di migliorare la resilienza dell'intero Paese, inteso come un'unica entità complessa. Tale approccio necessita di analisi scientifiche multidisciplinari che coinvolgano aspetti sociologici, economici e tecnici.

Partendo da una definizione di derivazione sociologica dei bisogni della popolazione, si identificano innanzitutto le risorse sociali e di rilevanza economica (indicate con il termine *item*) che soddisfano, a vari livelli di importanza, i bisogni dei cittadini. La metodologia FUB ha individuato circa 110 *item*, tra cui, per esempio, sono contemplati i settori *fornitura di acqua potabile*, *trasporti*, *settori industriali* e, come esempio di risorse sociali, la disponibilità dei *luoghi di culto*, di *manodopera*, dei *mezzi di informazione*.

Successivamente, si passa alla descrizione di una serie di strumenti di analisi che, attraverso la formalizzazione matematica di vettori aggregati descriventi le dipendenze dirette tra *item*, consentono di ricavare, mediante elaborazioni statistiche e di carattere tecnico, una descrizione sufficientemente dettagliata dell'evoluzione del degrado della qualità del servizio in tutti i settori a seguito di un malfunzionamento originato da un singolo *item*.

A partire da queste descrizioni aggregate, si costruiscono, *ex ante*, le mappe dell'effetto domino, di cui un esempio generico è riportato in Figura 1. Nella parte alta della Figura, sono riportate le dipendenze dirette tra *item* in funzione del tempo trascorso dal verificarsi del malfunzionamento, mentre, nella parte inferiore, è riportato un tipico albero di effetto domino. La presenza di un particolare item ad un certo istante di tempo indica che tale *item* fornisce alla società prestazioni talmente degradate da poterlo considerare come "fuori servizio".



A partire dagli alberi di effetto domino, che sono caratteristici per ogni Paese e per ogni sua suddivisione territoriale significativa (regioni, province, città), è possibile valutare gli impatti complessivi del malfunzionamento originario, utilizzando tre differenti metriche (prescritte dalla direttiva europea) finalizzate a valutare i danni economici, quelli sociali (ad esempio, calo della fiducia dei cittadini nelle Istituzioni) e gli effetti sulla salute dei cittadini (in termini di morti o di feriti gravi). Quest'ultimo passaggio concettuale viene realizzato, tra l'altro, correlando opportunamente l'analisi degli effetti domino con i dati economici disponibili in banche dati pubblicamente consultabili (ad esempio, le banche dati dell'ISTAT).

I risultati che si possono ottenere dall'applicazione del modello presentato nei paragrafi precedenti costituiscono al contempo un'informazione semplice da elaborare e utile per delle analisi *ex ante* ed *ex post* (analisi di incidenti già avvenuti). L'applicazione a casi reali della metodologia proposta consente di evidenziare ulteriori punti di forza che consolidano l'utilità di questo modello per studiare le interdipendenze e gli effetti domino sia a livello di nazione sia a livello transazionale e, in particolare, la sua utilità per il decisore istituzionale.

Uno dei punti di forza del modello studiato in FUB risiede nella sua scalabilità sia territoriale, sia temporale, che, in dipendenza del livello di dettaglio delle informazioni fornite come input, consente di fornire indicazioni utili al Governo circa le dipendenze e la valutazione *ex ante* degli impatti. Tale circostanza differenzia ulteriormente il modello descritto rispetto ad altre metodologie utilizzate che, per fornire indicazioni attendibili e/o utili, necessitano di informazioni molto dettagliate e omogenee (quindi, difficilmente reperibili su vasta scala) e di tempi estremamente lunghi per l'elaborazione.

PROSPETTIVE FUTURE

La metodologia sopra descritta è in via di applicazione pratica nel contesto del Progetto DOMINO, un progetto biennale cofinanziato dalla Commissione europea che contempla FUB come gestore e leader tecnico del progetto, con la cooperazione di due partner tecnologici italiani (Fondazione FORMIT e Theorematica) e di quattro partner istituzionali (la Presidenza del Consiglio dei Ministri italiana, l'Home Office britannico, il Segretariato Generale Nazionale per la Sicurezza e la Difesa francese e l'Ufficio del Primo Ministro bulgaro). Per dettagli su DOMINO, si può consultare in questo volume la sezione appositamente dedicata ai Progetti.

DOMINO affronta il problema dell'analisi delle interdipendenze a livello nazionale, e non anche a livello territoriale più ampio (inter-nazionale) o più circoscritto (a livello regionale o locale).

L'esperienza maturata "sul campo" ha evidenziato la necessità di ulteriori studi teorici per l'estensione pratica a contesti differenti. Le ulteriori analisi che verranno intraprese nel 2011 saranno finalizzate principalmente a individuare una maggiore e più profonda integrazione multidisciplinare tra le competenze sociali, economiche, statistiche e tecnologiche che tengano in conto anche variabilità territoriali (differenti organizzazioni del tessuto sociale) e temporali, come, ad esempio, l'analisi di sensitività rispetto a cambiamenti nel tempo delle interdipendenze tra *item*.

PUBBLICAZIONI

Conferenze internazionali

D. Perucchini, "DOMINO Project: State of the Art", *JRC 2010*, 9 dicembre 2010.

D. Perucchini, "A Methodology to Preview and Evaluate Cross Sectorial Domino Effects", *JRC 2010*, 19 ottobre 2010.

Conferenze nazionali

D. Perucchini, "Protezione delle infrastrutture critiche", Congresso Nazionale *Aica 2010*, Universita degli Studi dell'Aquila, 29 settembre - 1 ottobre 2010.

D. Perucchini, "Il Progetto DOMINO", *ANSSAIF - VII Congresso Nazionale*, Roma, 8 ottobre 2010.

Riviste internazionali

D. Perucchini, M. Carbonelli, L. Franchina, L. Gratta, F. Guasconi, "Defending Quality of Life through Critical Infrastructure Protection", *UNICRI Freedom from Fear Magazine*, luglio 2010.

Area 5
SICUREZZA ICT

RESPONSABILE DI AREA

FRANCO GUIDA

La sempre maggiore diffusione dei processi di automazione nel trattamento delle informazioni sta portando ad una continua crescita della quantità e dell'importanza dei dati e dei servizi gestiti avvalendosi di sistemi informatici e delle relative reti. Inoltre, la digitalizzazione delle reti TLC ha per molti aspetti accomunato tali reti a quelle informatiche, rendendo simili le modalità di violazione e gli strumenti utilizzabili per cercare di evitarle. Di conseguenza, sta diventando sempre più pressante l'esigenza di proteggere adeguatamente il patrimonio informativo trattato dai sistemi basati sull'impiego delle tecnologie ICT.

Tradizionalmente, lo scopo principale della sicurezza ICT consiste nella protezione della riservatezza, dell'integrità e della disponibilità delle informazioni a fronte di eventi sia intenzionali (i cosiddetti "attacchi", ossia le azioni perpetrate da soggetti che deliberatamente cercano di violare informazioni e servizi) sia accidentali (ad esempio, malfunzionamenti hardware o software, calamità naturali o errori umani). Gli strumenti di protezione (contromisure) che possono essere utilizzati per ridurre sia la probabilità di eventi dannosi sia l'entità del danno da essi prodotto (e quindi anche il cosiddetto "rischio" che da tali parametri dipende strettamente) sono di vario tipo. Più precisamente possono essere adottate contromisure di tipo organizzativo (ad esempio, assegnazione di ruoli e responsabilità, selezione di personale competente e fidato, e definizione di procedure finalizzate a garantire il rispetto di norme di legge o di politiche di sicurezza aziendali), contromisure di tipo fisico (porte blindate per l'accesso ai locali, contenitori antieffrazione per gli apparati ICT, ecc.) e contromisure di tipo tecnico (le cosiddette "funzioni di sicurezza").

L'Area "Sicurezza ICT" si occupa principalmente di quest'ultimo tipo di contromisure sviluppando le conoscenze necessarie a svolgere tutte le attività attinenti alla progettazione, selezione, installazione, configurazione e verifica delle funzioni di sicurezza. Le suddette conoscenze sono sia di carattere marcatamente teorico, come nel caso degli algoritmi e protocolli crittografici che rappresentano gli elementi basilari di alcune fondamentali funzionalità di sicurezza (protezione della riservatezza e integrità dei dati, autenticazione, ecc.) sia di tipo implementativo, per ciò che concerne la realizzazione in software, firmware e hardware delle funzionalità di sicurezza. Per questo secondo tipo di conoscenze è prioritario mantenere un costante aggiornamento circa le vulnerabilità che vengono quotidianamente scoperte nei prodotti software di maggiore diffusione, le modalità di attacco che consentono lo sfruttamento di tali vulnerabilità e le contromisure che possono essere adottate al fine di contrastare gli attacchi.

Lo sviluppo delle conoscenze fin qui descritte costituisce anche la necessaria premessa per poter svolgere attivi-

tà nel settore delle verifiche riguardanti il grado di affidabilità, dal punto di vista teorico e implementativo, delle funzionalità di sicurezza.

Le tematiche su cui si focalizza l'attività dell'Area "Sicurezza ICT" sono numerose e differenziate. Ciò deriva dalla crescente complessità dei sistemi ICT e, di conseguenza, dalla grande varietà di attacchi ed eventi accidentali che possono compromettere la riservatezza, integrità e disponibilità delle informazioni trattate. In particolare, nel corso degli ultimi tre anni l'Area si è confrontata con le seguenti tematiche, fornendo consulenza e rapporti sullo stato dell'arte:

- crittografia e relative applicazioni, tra cui quelle disciplinate dalla normativa italiana (ad esempio firma digitale e posta elettronica certificata);
- sicurezza di sistemi operativi e di programmi applicativi;
- sicurezza dei servizi Internet;
- architettura e configurazioni di sicurezza di reti ICT;
- dispositivi di rete con funzionalità di sicurezza (ad esempio *firewall*);
- autenticazione e controllo d'accesso a informazioni e servizi (soluzioni distribuite e soluzioni centralizzate);
- tecniche di autenticazione forte (ad esempio basate sull'uso di dispositivi biometrici, firma digitale, *token*, ecc.);
- sistemi di *auditing* e sistemi per la rivelazione e gestione di intrusioni (soluzioni distribuite e soluzioni centralizzate);
- sistemi per la scansione automatizzata di vulnerabilità;
- tecniche di *penetration testing*;
- metriche per la quantificazione della onerosità e difficoltà di esecuzione di attacchi;
- protezione da virus e da altro codice malevolo;
- *business continuity* e *disaster recovery* (sistemi e reti ad elevata affidabilità, tecniche di *back-up*, ecc.);
- analisi e gestione dei rischi;
- valutazione e certificazione della sicurezza, con eventuali specializzazioni in particolari contesti (ad esempio, quello della *privacy*).

Nel corso del 2010, sono state svolte sia attività di studio, approfondimento e ricerca sia attività consulenziali a beneficio di soggetti istituzionali e privati. Di seguito, viene fornita una breve descrizione delle attività di maggiore rilevanza, con la sola esclusione di quelle riguardanti studi riservati svolti nell'ambito di una Convenzione con la Presidenza del Consiglio dei Ministri.

GESTIONE AUTOMATICA DI INFORMAZIONI SU CARATTERISTICHE E GARANZIE DI SICUREZZA DI MODULI SOFTWARE IN AMBIENTE DISTRIBUITO

Negli ultimi anni è andata sempre più diffondendosi la fornitura di servizi attraverso applicazioni software distribuite, ossia composte da svariati moduli disponibili in rete che svolgono funzioni utili per una pluralità di contesti applicativi. Per questi moduli sono già previsti protocolli per la pubblicazione in ambiente informatico delle funzioni di base che ciascuno può eseguire, al fine di fornire alle applicazioni gli elementi per stabilire se farne uso o meno. Nei casi in cui i moduli non siano proprio moduli di sicurezza (le cui funzioni di base siano cioè progettate al fine di proteggere dati e servizi), attualmente non sono visibili alle applicazioni che utilizzano i moduli né eventuali funzioni di

sicurezza che non richiedano interazioni con le applicazioni, né le garanzie eventualmente associabili alle funzioni di sicurezza presenti nei moduli. Tali garanzie possono andare da varie forme di verifica del comportamento delle funzioni a vere e proprie certificazioni di sicurezza. Se tali funzioni e garanzie fossero visibili alle applicazioni, queste avrebbero la possibilità di selezionare i moduli da utilizzare anche in base alla protezione di dati e servizi che sono in grado di fornire e in funzione del grado di affidabilità che caratterizza la protezione offerta.

Nell'ambito di questa tematica, l'Area "Sicurezza ICT" ha iniziato a contribuire nel corso del 2010 al Progetto di ricerca "Advanced Security Service Certificate for SOA - ASSERT4SOA", finanziato dall'Unione europea nell'ambito del 7° Programma Quadro e descritto nella sezione dedicata ai Progetti.

Alcune delle attività che l'Area ha svolto per il Progetto "ASSERT4SOA" hanno consentito di contribuire a due pubblicazioni internazionali [1] [2].

SICUREZZA NEI SISTEMI DI PAGAMENTO MOBILI

I sistemi di pagamento mobili generalmente non richiedono la presenza dell'utente in punti prestabiliti e, in virtù di questa caratteristica che ne rende molto comoda l'utilizzazione, sono visti con crescente interesse. Quest'ultimo è ulteriormente aumentato dopo le novità introdotte dalla direttiva 2007/64/CE del Parlamento europeo e del Consiglio europeo del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno, recentemente recepita in Italia dal decreto legislativo 27 gennaio 2010, n. 11. Tali novità prevedono principalmente una netta semplificazione dei requisiti che devono soddisfare i soggetti che forniscono servizi di pagamento nel caso in cui gli importi delle transazioni siano di "basso valore" (secondo il significato attribuito dal citato decreto). Per tali motivi l'Area "Sicurezza ICT" ha avviato attività di ricerca in questo contesto partecipando al Progetto "SESAMO - Sistemi di pagamento mobili e smart card: aspetti di sicurezza" finanziato da ISCTI e descritto nella sezione dedicata ai Progetti. L'Area "Sicurezza ICT" ha anche partecipato alle attività di un gruppo di lavoro comprendente rappresentanti tecnici dei Soci Fondatori e dedicato ai sistemi di pagamento mobili. Su queste tematiche FUB ha organizzato il workshop "Mobile Payment. Sfide e opportunità per il Paese" tenutosi a Roma il 15 luglio 2010.

RICERCHE SUGLI ATTACCHI HARDWARE DI TIPO SIDE-CHANNEL

Negli ultimi anni, nel contesto della valutazione di sicurezza di prodotti ICT, si è affermato l'approccio detto Side Channel Analysis (SCA), da integrarsi con le normali attività di valutazione. L'approccio SCA si basa sull'osservazione controllata del comportamento fisico di un dispositivo ICT realizzante funzioni di sicurezza e ha l'obiettivo di ridurre (o eliminare del tutto) l'incertezza dell'osservatore (o attaccante) sui dati sensibili che regolano il funzionamento del dispositivo stesso. L'approccio SCA ha generato finora un insieme di analisi che possono essere raggruppate secondo diversi criteri, per esempio sulla base del tipo di misure da eseguire sul dispositivo.

Inizialmente, la letteratura di pubblico dominio si è focalizzata su dispositivi di sicurezza di grande diffusione, come smart card o equivalenti, e su attac-

chi semplici e rilevanti, tendenti ad esempio a determinare la chiave segreta custodita nel dispositivo preso di mira sulla base della potenza consumata dal dispositivo (*power analysis*). Successivamente, ricerche e pubblicazioni hanno esplorato attacchi e contromisure di diversa natura e rilevanza.

Al momento, l'approccio SCA (attacchi e contromisure) è considerato rilevante in diversi contesti quali ricerca e sviluppo industriale (settore dispositivi di sicurezza), ricerca accademica, pratica della valutazione di sicurezza di dispositivi ICT, normazione della valutazione di sicurezza di dispositivi ICT. Più specificamente:

- L'Unione europea ha ufficializzato (per dispostivi sicuri di firma e passaporti elettronici) o sta ufficializzando (per sistemi di pagamento) delle procedure di convalida, per dispositivi ICT, che prevedono esplicitamente l'uso dell'approccio SCA.
- Il futuro standard americano FIPS 140-3 per la convalida di moduli crittografici (attualmente in stato di bozza, sostituirà FIPS 140-2, già assorbito nello standard ISO/IEC 19790) fa esplicitamente riferimento alla validazione di contromisure SCA.
- La versione corrente (3.1) dei Common Criteria per la valutazione di sicurezza di prodotti ICT richiede l'uso dell'approccio SCA nell'ambito delle attività associate alla *vulnerability analysis*.

Nel 2010, l'Area "Sicurezza ICT" ha svolto attività di ricerca sulle tematiche SCA sia attraverso studi documentati da una pubblicazione internazionale [3], sia attraverso la partecipazione al Progetto "SESAMO - Sistemi di pagamento mobili e smart card: aspetti di sicurezza" finanziato da ISCOM del Ministero dello sviluppo economico e descritto nella sezione dedicata ai Progetti.

EVOLUZIONE DELLO STANDARD ISO 15408 (COMMON CRITERIA) PER LA CERTIFICAZIONE DELLA SICUREZZA INFORMATICA

Da vari anni, FUB contribuisce ai gruppi internazionali che aggiornano lo standard ISO 15408 (Common Criteria) utilizzato per la certificazione di sicurezza di dispositivi ICT. Nel corso del 2010 sono stati presentati alla Conferenza internazionale che si tiene annualmente sullo standard i risultati di un lavoro mirante al miglioramento dello standard stesso [4].

MONITORAGGIO E INCREMENTO DEL LIVELLO DI SICUREZZA NELLE PUBBLICHE AMMINISTRAZIONI (PROGETTO ITALIASICUR@)

Il Progetto denominato "Italia Sicur@" è stato varato nel corso del 2010 dal Consiglio Nazionale degli Ingegneri (CNI) e dalla Fondazione Ugo Bordoni (FUB) sotto il patrocinio del Ministero per la pubblica amministrazione e l'innovazione. Il Progetto è stato sviluppato al fine di monitorare e intervenire efficacemente sui livelli di sicurezza informatica della Pubblica Amministrazione, con particolare riferimento alle Amministrazioni locali.

La crescente utilizzazione delle tecnologie ICT nei processi interni alla Pubblica Amministrazione e nei servizi da essa offerti ai cittadini richiede, nella maggior parte dei casi, la sicurezza del trattamento dei dati. Per ridurre si-

gnificativamente i rischi di violazione dei sistemi ICT e non compromettere dati e servizi (che in certi casi, come ad esempio in ambito sanitario, presentano forti requisiti di protezione) verrà pianificato un intervento che, nella prima fase, prevede un monitoraggio presso le Amministrazioni interessate a verificare e, eventualmente, migliorare il livello di sicurezza informatica. Il monitoraggio sarà eseguito da ingegneri iscritti all'Albo esperti delle tecnologie ICT e indirizzati sulle modalità di esecuzione del monitoraggio da un apposito corso di specializzazione. I contenuti di tale corso, che sarà erogato da FUB, verranno definiti dal Tavolo Tecnico del Progetto. Nelle fasi successive dell'intervento, che verranno attuate presso le Amministrazioni interessate, sono invece previste azioni mirate di miglioramento del livello di sicurezza informatica eseguite secondo modalità analoghe a quelle descritte per la fase iniziale di monitoraggio (azioni eseguite da ingegneri iscritti all'Albo che avranno preliminarmente frequentato corsi di specializzazione mirati definiti dal Tavolo Tecnico ed erogati da FUB). Nell'attuazione delle azioni di miglioramento, il Tavolo Tecnico svolgerà una costante supervisione, anche al fine di rilevare tempestivamente l'eventuale necessità di ulteriori indirizzi specialistici da parte di FUB a beneficio degli ingegneri che eseguono l'intervento migliorativo. Al Tavolo Tecnico del Progetto partecipano il Ministero per la pubblica amministrazione e l'innovazione attraverso DigitPA, il Consiglio Nazionale degli Ingegneri (CNI) e la Fondazione Ugo Bordoni (FUB).

ATTIVITÀ DI CONSULENZA ISTITUZIONALE

Organismo di Certificazione della Sicurezza Informatica (OCSI). Supporto è stato fornito per i seguenti ruoli assegnati ad OCSI:

- certificatore unico nazionale della sicurezza di sistemi ICT e loro componenti (DPCM 30 ottobre 2003 "Approvazione dello Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione");
- organismo incaricato di verificare il soddisfacimento dei requisiti di sicurezza fissati dalla direttiva europea 1999-93-CE per i dispositivi di firma digitale con valore legale (art. 35 comma 5 del DL 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale).

Centro di Valutazione della sicurezza informatica (Ce.Va.). Supporto è stato fornito al laboratorio dell'ISCTI accreditato da ANS/UCSe per eseguire valutazioni di sicurezza su sistemi e componenti ICT che trattano informazioni per le quali sono applicabili la legge 24 ottobre 1977, n. 801, recante "Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato" e dal DPCM 3 febbraio 2006 "Norme unificate per la protezione e la tutela delle informazioni classificate".

Gestore del Registro delle opposizioni. Con il DL del 30 giugno 2003, n. 196 e con il DPR 7 settembre 2010, n. 178, di attuazione è stato avviato in Italia il Registro delle opposizioni. Il supporto ha riguardato l'individuazione e realizzazione delle misure di sicurezza ICT per il Registro delle Opposizioni, eseguita tenendo conto sia di quanto richiesto dal DPR, sia di ulteriori requisiti di sicurezza che si è ritenuto opportuno soddisfare nell'interesse di FUB e degli altri soggetti che possono interagire con il Registro.

Verifica della qualità dei servizi di accesso a Internet da postazione fissa. Con la delibera AGCOM n. 244/08/CSP e altre ad essa collegate, l'Autorità per le ga-

ranzie nelle comunicazioni ha avviato un Progetto nazionale ad hoc, affidato a FUB. L'Area "Sicurezza ICT" ha fornito contributi relativamente alle misure di sicurezza che si è ritenuto opportuno introdurre per proteggere e rendere affidabili gli strumenti preposti all'esecuzione della verifica. Quest'attività è descritta con dettaglio nella sezione dedicata ai Progetti.

INTERVENTI E PUBBLICAZIONI

[1] M. Anisetti, C. A. Ardagna, F. Guida, S. Gürgens and V. Lotz, et al., "ASSERT4SOA: Toward Security Certification of Service-Oriented Applications", Lecture Notes in *Computer Science*, 2010, Vol. 6428, *On the Move to Meaningful Internet Systems: OTM 2010 Workshops*, pp. 38-40.

[2] J.-C. Pazzaglia, V. Lotz, V. Campos Cerda, E. Damiani, C. Ardagna, S. Gürgens, A. Maña, C. Pandolfo, G. Spanoudakis, F. Guida, R. Menicocci, "Advanced Security Service cERTificate for SOA: Certified Services go Digital!", *ISSE 2010, Information Security Solutions Europe*, Germany, ottobre 2010.

[3] R. Menicocci, A. Simonetti, G. Scotti, A. Trifiletti, "On Practical Second-Order Power Analysis Attacks for Block Ciphers", Lecture Notes in *Computer Science*, 2010, Vol. 6476, *Information and Communications Security*, pp. 155-170.

[4] V. Bagini, F. Guida, C. Majorani, R. Menicocci, M. Orazi, "CC approaches to the certification of the components of a system when the system certification is not possible", *11th ICCC* (*International Common Criteria Conference*), Turkey, settembre 2010.

Area 6
INFORMATION MINING

RESPONSABILE DI AREA

CLAUDIO CARPINETO

Nel corso del 2010, sono stati investigati un ventaglio di temi che hanno riguardato, in generale, il reperimento e l'analisi delle informazioni contenute nel Web o in basi dati di grandi dimensioni, con particolare enfasi sul miglioramento delle fasi di pre e post-elaborazione dei motori di ricerca, sulla definizione di nuove tecniche per il *clustering* e la classificazione automatica dei dati, e sullo sviluppo di metodologie e strumenti per *opinion mining*. Di seguito, per ciascun argomento, si descrivono le attività svolte e i principali risultati che sono stati conseguiti, con le relative pubblicazioni scientifiche. Infine, si fornisce l'elenco delle partecipazioni ai Comitati di Programma di conferenze internazionali tenute nel 2010 e di conferenze o seminari organizzati direttamente dai ricercatori dell'Area.

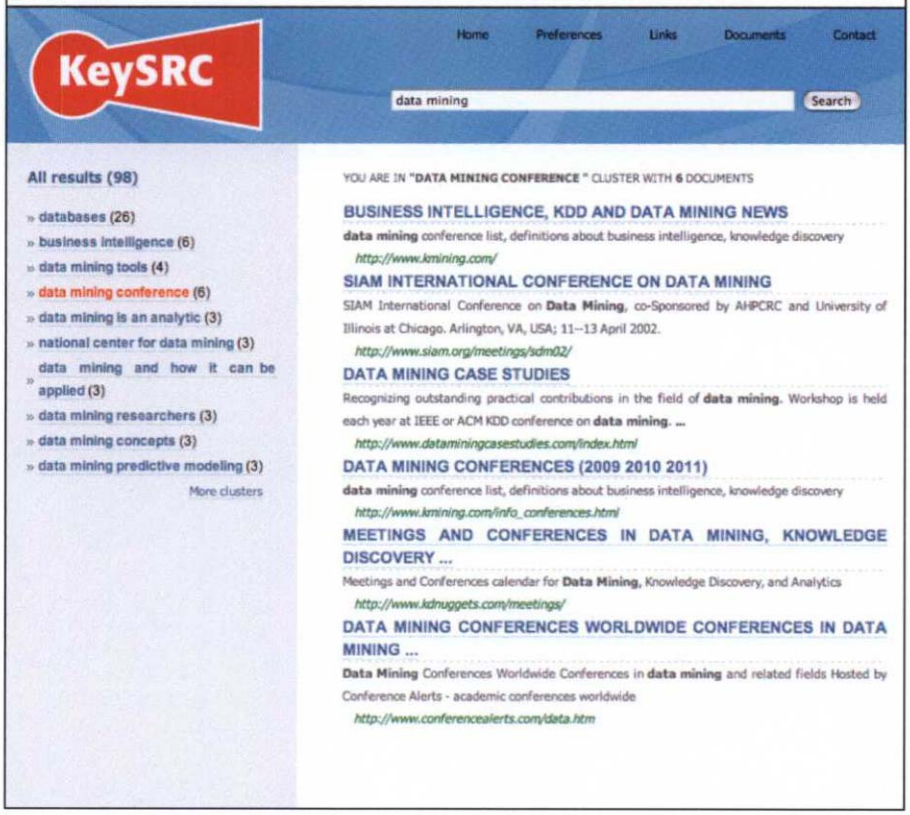
CLUSTERING E DIVERSIFICAZIONE DEI RISULTATI DI RICERCA

Uno dei punti deboli dell'attuale tecnologia dei motori di ricerca è costituito dalla modalità di presentazione dei risultati, offerti come una lista di elementi spesso ridondanti e senza nessuna organizzazione logica. I motori di ricerca a categorie (*clustering engines*) offrono uno schema di visualizzazione complementare, in cui i risultati recuperati da un motore di ricerca tradizionale vengono successivamente raggruppati in categorie omogenee, alle quali l'utente può accedere in modo indipendente. Nell'articolo [6] sono state analizzate le direzioni di ricerca più promettenti emerse recentemente all'interno di questo paradigma di visualizzazione.

KeySRC (Keyphrase-based Search Results Clustering) è un esempio di clustering engine innovativo, sviluppato negli ultimi due anni in FUB e accessibile su Web (http://keysrc.fub.it/Keysrc/), che si caratterizza per l'elevata espressività delle descrizioni delle categorie.

La Figura 1 ne illustra il funzionamento, utilizzando l'interrogazione "data mining" come esempio. A sinistra sono visibili le etichette dei cluster creati automaticamente da KeySRC esaminando i primi 100 risultati, le quali evidenziano una serie di aspetti afferenti il data mining. In questo caso, l'utente ha cliccato sul cluster "data mining conference" (in rosso) e il sistema ha visualizzato sulla parte destra i risultati contenuti nel cluster selezionato, che effettivamente si riferiscono a conferenze del settore.

Figura 1: Schermata del motore di ricerca KeySRC relativa all'interrogazione "data mining".



Nel 2010, KeySRC è stato esteso per farne anche uno strumento di diversificazione dei risultati. La diversificazione è la seconda strategia più diffusa per migliorare l'output dei motori di ricerca, e si basa sul principio che la collocazione di un risultato ai primi posti dipenda non soltanto dal valore intrinseco di quel risultato, ma anche dalla ridondanza rispetto agli elementi che lo precedono.

FUB ha quindi sviluppato una tecnica di diversificazione basata sui rappresentanti dei cluster creati da KeySRC, i quali vengono selezionati "a carosello" per apparire in testa alla lista riordinata dei risultati. Le prestazioni di KeySRC, utilizzato nelle due modalità, sono state confrontate con sistemi alternativi, ottenendo risultati generalmente positivi ed ascrivibili alla precisione con la quale l'utente riesce a discriminare il contenuto dei cluster creati da KeySRC. Queste ricerche sono descritte in [9].

L'analisi delle prestazioni di KeySRC si è successivamente evoluta in una valutazione complessiva dell'efficacia dei sistemi per *subtopic retrieval*, mettendo direttamente a confronto le due strategie principali, cioe clustering e diversificazione. Si noti che è il primo studio di questo tipo, perché nonostante la letteratura su clustering e diversificazione sia stata fiorente negli ultimissimi anni, i due filoni sono progrediti in parallelo. Per tentare di riconciliare questi due approcci, abbiamo definito una metodologia di valutazione unificata, inclusiva di nuovi indici di prestazione e di *benchmark* specializzati. Inoltre, per ciascuna strategia sono stati esaminati vari sistemi, in parte acquisiti dai loro sviluppatori, in parte reimplementati. In sostanza, si è visto che le due strategie sono essenzialmente complementari. Il clustering funziona meglio quando siamo interessati a recuperare documenti multipli che afferiscono a ciascuna subtopic, la diversificazione è preferibile quando l'obiettivo è coprire il maggior numero possibile di subtopic con almeno un documento. Inoltre, il clustering risulta penalizzato quando gli aspetti distinti di una interrogazione divergono debolmente, principalmente a causa della difficoltà di generare etichette con un buon potere discriminativo. Queste ricerche sono descritte in [10].

META-CLUSTERING

Così come i risultati prodotti da motori di ricerca distinti possono essere fusi in un *meta* motore di ricerca, con l'obiettivo di valorizzare gli elementi presenti in più ranking, anche per i clustering engine (descritti nella sezione precedente) è pensabile combinarne gli output in un unico clustering di risultati più robusto e preciso. Questa analogia ha condotto alla definizione, implementazione e validazione di un metodo per fondere i clustering (partizioni) prodotti da un insieme di clustering engine di input in un *meta clustering engine*. È un approccio nuovo, proposto da FUB per la prima volta.

Dopo aver verificato sperimentalmente che i risultati di clustering engine distinti non sono né troppo simili né troppo differenti, e quindi si prestano ad essere combinati, abbiamo definito un indice di somiglianza fra due partizioni basato sulla concordanza probabilistica delle decisioni assunte dalle due partizioni rispetto alle possibili coppie di risultati da partizionare. Successivamente, abbiamo formulato il problema di meta-clustering come un problema di ottimizzazione della concordanza fra la meta partizione e le partizioni di input, e abbiamo dimostrato che metodi di calcolo euristici molto efficienti producono soluzioni con un buon grado di approssimazione. La validazione è consistita nell'esaminare le proprietà della meta partizione rispetto alle partizioni individuali, ed ha