in fibra ottica di tipo passivo (PON). Il segnale radio captato da un'antenna posta sul tetto dell'edificio è stato convertito nel dominio ottico e ricevuto da un terminale di utente (ONT) a cui è stato collegato, tramite la specifica interfaccia, un decoder per il digitale terrestre. Questa sperimentazione ha avuto come obiettivo la dimostrazione della possibilità concreta di utilizzare la futura rete di accesso ottica anche per una nuova piattaforma TV di tipo via cavo.

Un'altra delle finalità di questo progetto è la realizzazione di contributi in ambito ITU-T (SG12, SG13, SG15) che possano favorire la crescita di imprese italiane in ambito ICT. Gli studi in ambito ATENA hanno permesso di produrre una serie di contributi per l'SG15, con particolare attenzione al backhouling in fibra per reti 3G-4G, alle retri metro WDM e alle prestazioni di reti core WDM.

Nel 2013, nell'ambito del progetto ATENA, la FUB ha conseguito i seguenti risultati:

- Sono state effettuate misure di correlazione tra la qualità del servizio e la qualità dell'esperienza per servizi video HD sulla rete sperimentale NGN, utilizzando accessi VDSL e in fibra ottica (GPON, P2P) e impiegando diverse tecniche d'instradamento ai fini di realizzare opportune classi di servizio in grado di rendere robusto un servizio rispetto alle tante forme di degradazione che possono esser presenti nella rete (dalla congestione dal traffico alla degradazione nel segnale nella propagazione).
- È stata ottimizzata la trasmissione del segnale digitale terrestre (DVB-T) in una rete di accesso in fibra ottica di tipo passivo (PON). Sono state analizzate le distorsioni prodotte dal modulatore ottico sul segnale DVB-T ricevuto da un'antenna terrestre.
- Gli studi sul Carrier Ethernet e le relative sperimentazioni sul PBB-TE nel laboratorio ISCOM hanno permesso di proporre e testare nuove configurazioni di rete idonee ai processi multicast per servizi televisivi.
- Sono state studiate nuove tecniche per il risparmio energetico nelle reti WDM basate sullo spegnimento di link e canali ottici. Lo studio ha riguardato l'ottimizzazione della distribuzione delle lunghezze d'onda nello spettro ottico, prendendo in considerazione i limiti indotti dalle fibre ottiche e dai vari dispositivi che compongono i collegamenti. Sono quindi stati proposti degli algoritmi che permettono risparmi fino al 40% del consumo energetico nell'arco della giornata. È stato inoltre mostrato che, ai fini di una corretta realizzazione di reti core dal punto di vista energetico, sarebbe necessario limitare il processo di routing all'interno della rete, relegandolo il più possibile ai bordi (edge), e aumentando quindi il numero delle connessioni ottiche nel trasporto.
- I principi di funzionamento dei suddetti algoritmi per il risparmio energetico sono stati sperimentati sulla rete NGN, utilizzando una procedura di tipo dinamico basata sul monitoraggio del traffico in rete. È questa la prima applicazione del principio su cui si basano le Software Defined Networks (SDN) sulla rete NGN.
- Sono continuati gli studi sulle capacità dei sistemi ottici multilivello con la multiplazione di polarizzazione. In particolare, è stata ottenuta una semplice formulazione analitica per il calcolo delle prestazioni dei sistemi ottici WDM di tipo multilivello che è stata verificata con simulazioni numeriche. Questa formulazione analitica potrebbe avere importanti utilizzi nel design delle reti ottiche e, nel 2014, dovrebbero esser fatte delle proposte in ambito ITU-T SG15 su questi argomenti.
- FUB e ISCOM hanno partecipato alla realizzazione della puntata di TG2 Dossier "Quando arriverà la larga banda" del 1° settembre 2013, dove sono stati mostrati tutti i laboratori ISCOM.

Gli studi realizzati nell'ambito del progetto ATENA, hanno tratto alcuni input dalle collaborazioni FUB con il progetto FP7 TREND, riguardante il risparmio energetico nelle reti di telecomunicazioni, e con il progetto nazionale PRIN ROAD-NGN, riguardante la rete di accesso ottica.

Output scientifici

Pubblicazioni

- Bonadonna A., Matera F., "Spectral Efficiency Comparison for Long-Haul Optical Dispersion Management Multi-Level Wavelength Division Multiplexing Systems", Fiber and Integrated Optics, Volume 32, Issue 1, January 2013, pp. 42-53.
- Valenti A., et al, "TREND Towards More Energy-Efficient Optical Networks", 17th International Conference on Optical Network Design and Modeling (ONDM 2013), Telecom Bretagne, Brest, France, April 16-19, 2013.
- Rufini A., Matera F., Valenti A., Tosi Beleffi G. M., Del Buono S., "Complete Digital Television Platform Based on Optical Fiber Access Architecture", Fotonica 2013, Milano, 21-23 maggio 2013.
- Matera F., "Simple Performance Calculation for Multilevel Optical Transmission Systems Operating in the Dispersion Management Regime", Fotonica 2013, Milano, 21-23 maggio 2013.
- Matera F., Valenti A., Coiro A., Listanti M., "Comparison Among Energy Saving Techniques Operating at IP and Optical Layer in Wide WDM Networks", Fotonica 2013, Milano, 21-23 maggio 2013.
- Maier G., Pattavina A., Siracusa D., Valenti A., Matera F., "Advantages of a Content Delivery Network Architecture Based on Wdm and Carrier Ethernet Multicasting", Fotonica 2013, Milano, 21-23 maggio 2013.
- Matera F., "Nonlinear performance limits in higly dispersive transmission systems", proceedings of 39th European Conference and Exhibition on Optical Communication (ECOC 2013), London, September 22-26, pp. 1-3, 2013.

Software / tool

- Programma in MATLAB per la valutazione delle prestazioni di sistemi WDM

Laboratori

- Montaggio e verifica sperimentale della nuova rete GPON-VDSL

NGN

mPlane

An Intelligent Measurement Plane for Future Network and Application Management

Progetto di ricerca nel VII Programma Quadro della Commissione europea

mPlane è un progetto IP (Large-scale Integrating Project) del 7° Programma Quadro UE al quale partecipano 16 partner europei. È coordinato dal Politecnico di Torino (Prof. Marco Mellia) e presenta una grande componente italiana con la presenza, oltre che della FUB e del Politecnico di Torino, anche di Telecom Italia, SBB Progetti e FASTWEB.

Questo progetto può esser considerato come un'importante evoluzione del progetto "MisuraInternet", definito dalla Delibera 244 dell'AGCOM, e si pone l'ambizioso obiettivo di rivedere profondamente l'infrastruttura di una rete IP, inserendo un piano che controlli lo stato delle prestazioni.

Gli studi che verranno effettuati per questo progetto potranno essere di grande supporto a tutte le attività che riguarderanno la realizzazione delle infrastrutture per le reti nell'ambito dell'Agenda Digitale.

Il progetto mira a costituire un'infrastruttura di misura della Qualità del Servizio distribuita, atta ad eseguire misurazioni attive, passive e ibride. Tale infrastruttura conterrà, oltre ai dispositivi per la misura, uno strato di repository e analisi che raccoglierà e analizzerà i dati attraverso strumenti di elaborazione parallela e data mining. Inoltre verrà introdotto un *intelligent reasoner* in grado di analizzare le cause dei problemi identificati da ogni test, consentendo la comprensione delle condizioni che generano criticità.

Più dettagliatamente, il progetto prevede la realizzazione di un'architettura all'interno della rete IP dedicata al monitoraggio delle prestazioni della rete a tutti i livelli della "Pila OSI"; verranno quindi effettuate misure di prestazione dal livello fisico (ad esempio, verifica del Service Level Agreement tra un operatore di rete e un utente) fino al livello di applicazione (ad esempio verifica della qualità di un video fornito da un operatore web).

A tal fine, è prevista la realizzazione di sonde, sia attive sia passive, da distribuire nella rete; di un sistema per l'immagazzinamento dei dati; di un sistema che riassume le caratteristiche delle misure visualizzando i risultati secondo alcune metodologie consolidate (per esempio throughput, jitter, delay, packet loss). Inoltre, l'architettura prevede delle metodologie di allarme per segnalare malfunzionamenti nella rete.

Come fase preliminare il progetto farà un'analisi di tutti gli scenari presenti e futuri delle reti di TLC, prendendo in considerazione sia le topologie di accesso (rame, fibra, radio) sia i dispositivi utilizzati (PC, smartphone, smart TV) e analizzando anche architetture complesse come quelle delle Content Delivery Networks, del Cloud Computing e dei Data Center.

Un importante aspetto sarà la definizione dei parametri da misurare, anche in relazione alla QoE. La FUB contribuirà in particolare alla definizione e alla misura dei parametri, guardando alle ultrabroadband networks, alla progettazione delle sonde e dell'architettura completa. Inoltre collaborerà alla sperimentazione di quest'architettura su alcune reti utilizzate come test.

Nel corso del primo anno, FUB ha definito le metodologie per misure attive della QoS rivolte ad accessi ultrabroadband e per le verifiche SLA di tipo multilivello.

Nel 2013, FUB ha realizzato una sonda attiva in grado di misurare la capacità di linea (misura a livello L2 della pila OSI), la capacità effettiva per un utente in ambiente TCP (a livello L4 e denominata throu-

ghput) e a livello di applicazione (a livello L7 e denominata goodput). La sonda è un programma software che viene installato su un PC ed è costituito da una serie di test di tipo TCP e UDP. La sonda è stata testata in laboratorio utilizzando accessi di tipo ADSL2+ e GPON selezionando bande tra i 10 e i 100 Mb/s. In particolare, è stato verificato il comportamento della capacità di linea, del throughput e del goodput in funzione del ritardo del collegamento, testando l'affidabilità di questa sonda.

È stata quindi studiata la modalità di inserimento di questa sonda nell'architettura completa mPlane e sono state definite le prime modalità di analisi dei dati da essa ottenuti.

La FUB si è anche occupata della definizione di una metodologia per la misura della QoE per servizi YouTube e ha verificato sperimentalmente la correlazione tra misure di QoS e QoE (servizi YouTube) per accessi GPON e con chiavetta 3G.

Deliverable / Rapporti tecnici

La FUB ha contribuito alla redazione di 6 Deliverable. Di seguito si riporta in sintesi il tipo di apporto fornito:

- D1.1: Use Case Elaboration and Requirements Specification, Contributo FUB sulla definizione del metodo di misura Multilevel Service Agreement e suo inserimento nell'architettura mPlane.
- D2.1: Selection of Existing Probes and Datasets. Contributo FUB sulle caratteristiche e funzionamento delle sonde attive.
- D3.1: Basic Network Data Analysis. Contributo FUB su analisi dei dati da misure QoS attive.
- D4.1: Design of Analysis Modules. Contributo FUB su algoritmi per sonde attive.
- D5.1: First Data Collection Track Record. Contributo FUB sulle misure in laboratorio di QoS in reti GPON.
- D7.2: Plans for Using and Disseminating mPlane Knowledge. Contributo FUB sulla disseminazione di misure QoS.

Output scientifici

- Sottomissione di un lavoro alla rivista IET Communications.
- Realizzazione della sonda attiva per la misura della QoS Multilivello.
- Test in reti GPON.

SICUREZZA ICT

Sesamo II

Sistemi di pagamento mobili e smart-card: aspetti di sicurezza

Progetto in convenzione con MiSE - ISCOM

Il progetto SESAMO II nasce con lo scopo d'individuare azioni concrete per l'attuazione degli obiettivi perseguiti dall'Agenda Digitale Europea, all'interno del pilastro "Fiducia e sicurezza".

SESAMO II, come evoluzione del progetto SESAMO I, si focalizza essenzialmente sull'analisi della sicurezza del software impiegato nei sistemi di pagamento mobili. Questi sistemi offrono all'utente la possibilità di eseguire transazioni economiche sfruttando caratteristiche di mobilità dei terminali impiegati. Per l'esecuzione di queste transazioni, l'utente si avvale di terminali portatili (ad esempio smartphone o tablet) i cui componenti, come il software applicativo e le smart-card di tipo SIM, e in alcuni sistemi le interfacce che utilizzano la tecnologia NFC (Near Field Communication), si rivelano fondamentali per la funzionalità e per la sicurezza del sistema di pagamento stesso.

Con la finalità di analizzare gli aspetti di sicurezza correlati all'utilizzo di metodologie software e di tecnologie radio NFC per la realizzazione di sistemi di pagamento in mobilità, il progetto ha previsto la realizzazione di un laboratorio di analisi, mediante metodologie innovative d'individuazione dei requisiti e delle funzionalità richieste. Accanto al problema della tutela delle transazioni in mobilità e della prevenzione di frodi informatiche, si aggiunge la questione rilevante della tutela dei dati personali dei soggetti coinvolti. Sebbene il laboratorio embrionale costituito in SESAMO II sia stato progettato anche nell'ottica di studiare tali aspetti, l'argomento della tutela dei dati personali dei soggetti coinvolti nelle transazioni in mobilità sarà approfondito nella successiva evoluzione del progetto, SESAMO III.

Durante il 2013 è stata completata l'analisi preliminare dello stato dell'arte della sicurezza del software nei sistemi di pagamento in mobilità: tale analisi, condotta in collaborazione con l'Università di Roma Tre attraverso una tesi di laurea di primo livello, è stata specializzata sugli aspetti di sicurezza dei sistemi Android.

Il 2013 ha visto, inoltre, il completamento del benchmark avviato nel 2012 circa i sistemi di pagamento in mobilità: tale benchmark, insieme all'analisi dello stato dell'arte della sicurezza del software nei sistemi di pagamento in mobilità, ha costituito il punto di partenza per la specializzazione e l'aggiornamento dei requisiti del laboratorio individuati in forma preliminare durante le attività del 2012.

Nel 2013 è stata dunque portata a termine la realizzazione delle funzionalità di base del laboratorio per l'analisi della sicurezza del software impiegato nei sistemi di pagamento in mobilità. In attesa della finalizzazione degli acquisti per la sperimentazione, è stata completata una prima configurazione per il laboratorio embrionale SESAMO II: a tal proposito sono state realizzate le principali funzioni di sicurezza previste dall'analisi dei requisiti (ad esempio funzionalità di controllo del traffico, funzionalità di monitoraggio ed ispezione del traffico attraverso reti dedicate isolate, funzionalità di analisi e scansione di vulnerabilità, funzionalità di rilevamento di anomalie ed intrusioni).

È stata inoltre completata l'analisi dell'architettura funzionale e protocollare dei dispositivi mobili che implementano la tecnologia NFC focalizzando le problematiche di sicurezza ed i possibili casi di studio per le sperimentazioni da svolgere negli eventuali sviluppi futuri del progetto.

In attesa della fornitura da parte di ISCOM dei dispositivi per il laboratorio oggetto della sperimentazione (fornitura che è stata rimandata al progetto SESAMO III), durante la collaborazione con Roma Tre, è stata eseguita una sperimentazione su un dispositivo mobile utilizzando tecniche di analisi del

traffico e di reverse engineering mirate a rilevare le azioni di potenziale software malevolo che potrebbe prendere il controllo del telefono durante l'esecuzione di pagamenti in mobilità; le due sperimentazioni, eseguite su emulazioni virtuali dei dispositivi mobili e su un dispositivo reale, hanno condotto alla definizione di linee guida per la verifica, in caso di dispositivi con S.O. Android, dell'adeguatezza dei permessi richiesti dalle applicazioni che s'intende istallare sul dispositivo mobile.

In conclusione di progetto è stata predisposta una presentazione interattiva contenente sia la descrizione dei risultati ottenuti, sia una dimostrazione in tempo reale delle metodologie per l'analisi del software impiegato nei dispositivi mobili.

SICUREZZA ICT

Sesamo III

Sistemi di pagamento mobili e smart-card: aspetti di sicurezza

Progetto in convenzione con MiSE - ISCOM

Il progetto ha i seguenti obiettivi:

- individuare azioni concrete per l'attuazione degli obiettivi perseguiti dall'Agenda Digitale Europea, all'interno del pilastro "Fiducia e sicurezza";
- fornire supporto alle attività dell'Organismo di Certificazione della Sicurezza Informatica (OCSI) nell'ambito degli aspetti di ricerca relativi alle metodologie di valutazione e certificazione della sicurezza di sistemi e prodotti ICT.

SESAMO III, come evoluzione del progetto SESAMO II, si occupa in particolare dell'analisi della sicurezza del software impiegato nei sistemi di pagamento mobili.

Tra gli obiettivi principali del progetto figura il supporto all'OCSI non solo in ambito di metodologie di valutazione e certificazione, ma anche relativamente all'innovazione di processi di gestione e alla partecipazione ai gruppi internazionali del CCRA (Common Criteria Recognition Arrangement) con le finalità di:

- affiancare l'organismo nella predisposizione del nuovo arrangement, la cui firma è prevista per settembre 2014;
- segnalare e indicare attività che l'OCSI deve completare per ottenere l'approvazione della valutazione operata in ambito internazionale dagli altri organismi di certificazione (VPA – Voluntary Periodic Assessment). Tale VPA, prevista per marzo 2014, è necessaria per mantenere lo status di "certificate authorizing participant", ovvero di Organismo in grado di emettere certificati riconosciuti in tutti i paesi che aderiscono al CCRA.

Il progetto prevede il completamento della realizzazione di un laboratorio per l'analisi del software impiegato nei dispositivi mobili per l'esecuzione di operazioni di pagamento "in mobilità" e la sperimentazione degli acquisti individuati insieme ai rispettivi responsabili OCSI. La realizzazione di requisiti specifici di sicurezza, quali le funzionalità di rilevamento delle intrusioni, di controllo e filtraggio del traffico e delle attività svolte in laboratorio, di strumenti per la corretta gestione di software e documenti, risultano essenziali per garantire l'affidabilità dei risultati della sperimentazione e la ripetibilità delle attività svolte (anche a beneficio di soggetti terzi come le autorità).

Avendo completato i requisiti essenziali richiesti per la definizione del laboratorio indicato, è stata avviata la sperimentazione del software impiegato nei dispositivi mobili acquisitati da ISCOM (acquisto completato a dicembre 2013).

Al fine di estendere l'ambito di applicazione degli strumenti predisposti in laboratorio ai temi più attuali delle comunicazioni mobili, è stata condotta un'analisi degli aspetti di privacy nei dispositivi mobili finalizzata anche all'individuazione di possibili sperimentazioni da avviare nel laboratorio predisposto durante SESAMO II.

Come anticipato, il supporto all'OCSI costituisce un'attività cardine del progetto SESAMO III. La certificazione della sicurezza di sistemi e prodotti ICT costituisce oggi lo strumento più idoneo a fornire garanzie in merito all'attuazione di misure di sicurezza ICT applicabili a tutte le tipologie di sistemi e prodotto. Lo standard di riferimento ISO/IEC 15408, meglio noto come "Common Criteria for ICT security product evaluation", presenta tuttavia ampi gradi di libertà e margini di perfezionamento,

lasciando spazio ad attività di ricerca finalizzate alla specializzazione dei requisiti dello standard sulle nuove categorie di prodotti. In questo ambito, s'inserisce SESAMO III, fornendo supporto all'OCSI, incaricato in Italia di emettere certificati di sicurezza. In questa prospettiva sono stati analizzati i possibili ambiti di coinvolgimento dell'OCSI in merito ad attività scaturite dagli aggiornamenti del CAD (Codice dell'Amministrazione Digitale) e, più in generale, della regolamentazione nazionale ed europea.

Come unico organismo italiano deputato alla gestione/emissione dei certificati di sicurezza di sistemi e prodotti ICT secondo lo standard ISO/IEC 15408, l'OCSI partecipa ad un circuito internazionale incaricato di mantenere e perfezionare lo standard stesso al fine di uniformare le attività di valutazione e poter assicurare nel circuito stesso il mutuo riconoscimento dei certificati emessi dai diversi partecipanti. Tale circuito, CCRA (Common Criteria Recognition Arrangment) prevede verifiche periodiche (VPA, Voluntary Periodic Assessment) di ogni organismo (riferito anche come "Schema di certificazione") da parte di ispettori degli altri schemi nazionali per avere garanzie nel tempo circa la conformità dell'operato dell'organismo stesso ai dettami del CCRA. Una parte consistente delle risorse di SESAMO III è stata destinata al supporto all'Organismo OCSI per l'individuazione di criticità potenziali durante lo svolgimento della VPA, prevista per giugno 2014.

È stata quindi condotta un'analisi approfondita del rapporto prodotto dalla comunità CCRA durante l'ultima valutazione (shadow evaluation) cui si è sottoposto l'OCSI. Tale analisi ha individuato gli argomenti da curare con maggiore attenzione in previsione della VPA di giugno 2014.

È stata eseguita una revisione delle nuove linee guida prodotte da OCSI (nella forma di NIS, Note Informative dello Schema) che recepiscono le migliorie previste da ISCOM e che sostituiscono le precedenti NIS. La revisione ha prodotto dei suggerimenti/commenti inoltrati ad ISCOM ed implementati nella versione in procinto di essere emessa entro la fine dell'anno.

È stata condotta un'analisi delle possibili azioni in carico ad OCSI relativamente alle attività di certificazione degli HSM.

È stato fornito all'OCSI un supporto nell'aggiornamento dei Corsi e degli Esami di abilitazione OCSI (destinati a valutatori di laboratori e assistenti). Tale supporto ha preso anche la forma di revisione degli strumenti impiegati per verificare le competenze operative dei soggetti che richiedono le abilitazioni indicate.

È stato inoltre fornito supporto nell'individuazione di eventuali problematiche di natura tecnica nelle certificazioni in corso, nell'ottica di utilizzare tali certificazioni come evidenze per la VPA.

La Fondazione ha inoltre contribuito alle attività di aggiornamento tecnico dell'OCSI partecipando ai gruppi di lavoro CCRA[1], ai gruppi di lavoro SOG-IS[2] e fornendo contributi tecnici al gruppo di lavoro CCMB orientato alla risoluzione di problematiche di natura tecnica dello standard.

1 Parigi (CCDB, CCES, CCMC, Settembre 2012); Ottawa (CCDB, CCES, CCMC, Maggio 2013); Orlando US (CCDB, CCES, CCMC, Settembre 2013).

2 Berlino (JILWG, MC, Febbraio 2012); L'Aia (JILWG, Maggio 2012); Parigi (JILWG, MC, Febbraio 2013); Londra (JILWG, Ottobre 2013).

SICUREZZA ICT

ASSERT4SOA

Advanced Security Service cERTificate for SOA

Progetto di ricerca nel VII Programma Quadro della Commissione europea

Il paradigma SOA (Service Oriented Architecture) è il riferimento architetturale per i sistemi software basati sul concetto di servizio.

Un servizio è una funzionalità resa disponibile da un service provider a un service consumer. Il service discovery è un componente che offre ai service provider la possibilità di registrare servizi con funzionalità definite e ai service consumer la possibilità di richiedere servizi con funzionalità specificate.

ASSERT4SOA ha origine dalle osservazioni seguenti:

- il service consumer può avere necessità di specificare, per il servizio desiderato, proprietà di sicurezza ICT e relative garanzie (tipicamente, un certificato di sicurezza ICT)
- gli attuali sistemi SOA non sono capaci di soddisfare automaticamente questa necessità

ASSERT4SOA mira a definire sistemi SOA avanzati (ASSERT-aware) basati sull'uso di un particolare certificato di sicurezza ICT (detto ASSERT) e opportunamente estesi, per rispondere alla suddetta necessità dei service consumer. Obiettivo del progetto è, inoltre, l'implementazione e validazione di un sistema prototipale.

FUB partecipa al progetto con varie responsabilità tecniche ed è il riferimento fondamentale per gli aspetti di certificazione di sicurezza ICT.

Di seguito i deliverable pianificati:

1. Online Collaboration Platform
2. Intermediate Project Report
3. Model Composition
4. ASSERTs aware service query language and discovery engine
5. Requirements for an ontology supporting certificates interoperability
6. Design and description of evidence-based certificates artifacts for services
7. Architecture and High level design
8. Project Web Site and First Dissemination Report
9. Yearly Project Report - Y1
10. First version of the ASSERT Ontology
11. Intermediate Project Report
12. Updated Implementation Plan
13. ASSERTs aware service orchestration patterns
14. Guidelines for plug-ins development
15. ASSERTs aware service based systems adaptation policy language
16. Matching algorithm for evidence-based certification v2, and proof-of-concept
17. Model Based Certification Artifacts
18. Security Property Language
19. ASSERT sofware infrastucture for SOA v1.0

20. Yearly Project Report -Y2
21. Evaluation of the Certificate Ontology v1
22. ASSERTs aware service based systems adaptation tool
23. Partial Order on ASSERT-M Certificates
24. Intermediate Project Report
25. Second version of the ASSERT Ontology
26. ASSERT Model and Language v3
27. Mechanisms for managing ASSERTs in SBS life cycle
28. Architectural solutions for evidence-based certification
29. Validation of WP5 Methods and Techniques
30. ASSERT sofware infrastucture for SOA v2.0
31. Final Project Report -Y3
32. Report on the distribution of the community Financial Distribution

FUB, in particolare, contribuisce alla produzione dei seguenti deliverable[3]:

33. Framework requirements [FUB]
34. ASSERT language v1
35. Communication Plan
36. ASSERT profiles
37. Case Study: a complete walkthrough from usage scenario to certification artefacts
38. Advisory Board Session Report [FUB]
39. ASSERT language v2
40. AB & Sustainability report [FUB]
41. Report on the identified certificational requirements [FUB]
42. Validation of the ASSERT4SOA Framework based on the study case
43. Final Dissemination report
44. Standardization report

La Fondazione fornisce (nei tre anni di progetto) consulenza ai partner sul tema Certificazione della Sicurezza ICT.

Nel ruolo di Advisory Board (AB) Chair, FUB coordina l'istituzione dell'AB e le interazioni tra AB e consorzio, inclusa l'organizzazione delle sessioni pianificate (2011, 2012, 2013).

FUB, inoltre, dissemina i risultati del progetto nella comunità dei Common Criteria (International Common Criteria Conference) (2011, 2012, 2013).

La Fondazione ha partecipato a ICCC2013 e ha ospitato due eventi di progetto:

- Tenth General Meeting
- Third Advisory Board Session

Del secondo, in particolare, ha coordinato direttamente l'organizzazione.

[3] [FUB] indica che FUB è responsabile della produzione del deliverable.

FUB ha fornito consulenza ai partner sui seguenti aspetti della Certificazione della Sicurezza ICT:

- Common Criteria extension to SOA
- Verification of the revocation status of an ASSERT
- Attestation and verification of the ASSERT Issuer competence
- Definition of realistic ASSERT Profiles

Deliverable / Rapporti tecnici

Nel 2013, la Fondazione ha contribuito alla produzione dei seguenti deliverable:

- AB & Sustainability report [FUB].
- Report on the identified certificational requirements [FUB].
- Validation of the ASSERT4SOA Framework based on the study case.
- Final Dissemination report.
- Standardization report.

Output scientifici

- Anisetti M., Ardagna C.A., Guida F., Gürgens S., Lotz V., et al., "ASSERT4SOA: Toward Security Certification of Service-Oriented Applications", Lecture Notes in Computer Science, 2010, Volume 6428, On the Move to Meaningful Internet Systems: OTM 2010 Workshops, November 2010.
- Pazzaglia J.C., Lotz V., Campos Cerda V., Damiani E., Ardagna C., Gürgens S., Maña A., Pandolfo C., Spanoudakis G., Guida F., Menicocci R., "Advanced Security Service cERTificate for SOA: Certified Services go Digital!", ISSE 2010 Securing Electronic Business Processes, Vieweg+Teubner Verlag, 2011.
- Bagini V., Guida F., Majorani C., Menicocci R., Orazi M., Riccardi A., "The EU Project ASSERT4SOA (Advanced Security Service cERTificate for SOA): Objectives, approach, and status (after one year)", 12th ICCC (International Common Criteria Conference), Petaling Jaya, Malaysia, September 27-29, 2011.
- Kaluvuri S.P., Bezzi M., Sabetta A., Roudier Y., Menicocci R., Bagini V., Riccardi A., Orazi M., "Applying Common Criteria to Service Oriented Architectures", 13th ICCC (International Common Criteria Conference), Paris, September 18-20, 2012.
- Kaluvuri S.P., Bezzi M., Bagini V., Menicocci R., Orazi M., Riccardi A., "Applying CC to SOA - Dynamic Certification Lifecycle", Alternate Presenter at the 14th International Common Criteria Conference (ICCC 2013) (not presented), Orlando, FL, USA, September 2013.
- Kaluvuri S.P., Koshutanski H., Di Cerbo F., Menicocci R., Maña A., "A Digital Security Certificate Framework for Services", International Journal of Services Computing, 2013, Vol. 1, N. 1.

SICUREZZA ICT

CUMULUS

Certification infrastrUcture for MUlti-Layer cloUd Services

Progetto di ricerca nel VII Programma Quadro della Commissione europea

La tecnologia cloud offre un approccio efficace per la realizzazione di infrastrutture, piattaforme e servizi software senza dover sostenere costi ingenti di possesso, esercizio e manutenzione delle infrastrutture computazionali necessarie a tal fine.

Nonostante il suo fascino dal punto di vista dei costi, la tecnologia cloud solleva ancora preoccupazioni per quanto riguarda la sicurezza software, la privacy, la governance e la conformità dei dati e dei servizi software offerti attraverso di essa. Tali preoccupazioni nascono dalla difficoltà di garantire proprietà di sicurezza dei diversi tipi di servizi disponibili attraverso il cloud. I fornitori di servizi sono riluttanti ad assumersi la piena responsabilità della sicurezza dei loro servizi una volta che questi vengono caricati e offerti attraverso il cloud. Inoltre, i fornitori di cloud hanno storicamente evitato di accettare responsabilità per falle nella sicurezza.

CUMULUS affronta questi limiti attraverso lo sviluppo di un quadro integrato di modelli, processi e strumenti di supporto alla certificazione di proprietà della sicurezza dei servizi software a livello delle infrastrutture (IaaS), piattaforme (PaaS) e applicazioni (SaaS) nel cloud. La struttura CUMULUS porterà utenti di servizi, fornitori di servizi e fornitori di cloud a collaborare con le autorità di certificazione al fine di garantire la validità del certificato di sicurezza nel mutevole ambiente cloud.

Di seguito i deliverable pianificati:

1. CUMULUS Framework Architecture v1
2. Security-aware SLA specification language and loud security dependency model
3. Core Certification mechanisms 1
4. CUMULUS-aware engineering process specification v1
5. Tools supporting CUMULUS-aware engineering process v1
6. Core Certification Mechanisms 2
7. CUMULUS Infrastructure v1
8. SmartCities pilot
9. eHealth pilot
10. CUMULUS-aware engineering process specification v2
11. CUMULUS Framework Architecture v2
12. Certification Mechanisms for incremental and hybrid certification
13. Tools supporting CUMULUS-aware engineering process v2
14. CUMULUS Infrastructure v2

FUB, in particolare, contribuisce alla produzione dei seguenti deliverable[4]:

15. Quality plan [FUB]
16. Project website

[4] [FUB] indica che FUB è responsabile della produzione del deliverable.

17. First intermediate project technical and financial report [FUB]
18. Specification of pilot scenarios and requirements
19. First annual project technical and financial report [FUB]
20. Certification models v1
21. Dissemination plan report (1st Year)
22. First exploitation plan and market analysis
23. First Advisory board report [FUB]
24. Second intermediate project technical and financial report [FUB]
25. Specification of CUMULUS evaluation criteria
26. Certification models v2
27. Second annual project technical and financial report [FUB]
28. Dissemination plan report (2nd Year)
29. Second exploitation plan and market analysis
30. Second Advisory board report [FUB]
31. Initial evaluation report
32. Third intermediate project technical and financial report [FUB]
33. Final CUMULUS certification models
34. Final project technical and financial report [FUB]
35. Distribution of financial contribution report [FUB]
36. Final evaluation report
37. Dissemination plan report (3rd Year)
38. Final exploitation plan, market analysis and IPR
39. Third Advisory board report [FUB]
40. Final project report

FUB è coordinatore dell'intero progetto CUMULUS.

Nel ruolo di Advisory Board (AB) Chair, coordina l'istituzione dell'AB e le interazioni tra AB e consorzio, inclusa l'organizzazione delle sessioni pianificate (2013, 2014, 2015).

FUB, inoltre, dissemina i risultati del progetto nella comunità dei Common Criteria (International Common Criteria Conference) (2013, 2014, 2015).

La Fondazione ha contribuito ai seguenti eventi di progetto, anche coordinandone organizzazione ed esecuzione:

- General Meeting 2013-1
- General Meeting 2013-2
- General Meeting 2013-3
- Advisory Board Meeting 2013
- Rehearsal Meeting 2013
- EU Technical Review Meeting 2013
- General Meeting 2013-4
- Ad Hoc Meeting 2013

Deliverable / Rapporti tecnici

Nel 2013, FUB ha contribuito alla produzione dei seguenti deliverable:

- First intermediate project technical and financial report [FUB].
- Specification of pilot scenarios and requirements.
- First annual project technical and financial report [FUB].
- Certification models v1.
- Dissemination plan report (1st Year).
- First exploitation plan and market analysis.

Output scientifici

Per finire, nel corso del 2013, FUB ha contribuito ai seguenti lavori:

- "The EU Project CUMULUS (Certification infrastrUcture for MUlti-Layer cloUd Services): Objectives, approach, and status". Abstract sottomesso a ICCC 2013 (14th International Common Criteria Conference), Orlando, Florida (USA), September 10-14, 2013, e selezionato per "alternative presentation" (non presentato).
- Cimato S., Damiani E., Menicocci R., Zavatarelli F., "Towards the certification of cloud services", IEEE 2013 International Workshop On Security and Privacy Engineering, Assurance, and Certification (SPEAC 2013), Santa Clara, USA, June 27th-July 2nd, 2013.

SICUREZZA ICT

SAFETRIP

Satellite Application For Emergency handling, Traffic alerts, Road safety and Incident Prevention

Progetto di ricerca nel VII Programma Quadro della Commissione europea

Il progetto ha l'obiettivo di realizzare un sistema integrato per i servizi di infomobilità e sicurezza stradale, attraverso la raccolta di informazioni trasmesse dai veicoli su strada. L'obiettivo è di rendere più efficiente l'uso delle infrastrutture di trasporto stradale e la catena di segnalazione (informazione / prevenzione / intervento) in caso di incidenti.

SAFETRIP impiega una nuova tecnologia satellitare operante in banda S (intorno ai 2GHz) e supportata dal satellite W2A, che è stato lanciato nel mese di aprile 2009. Grazie a questa tecnologia, è possibile realizzare un servizio di connettività bidirezionale a bordo dei veicoli, continuativo e interattivo, che sia anche interoperabile con i sistemi Galileo e UMTS.

La nuova tecnologia garantisce:

- la copertura globale del servizio sul continente europeo;
- la trasmissione dei dati in formato multicast, di rapida e facile implementazione;
- l'eco-compatibilità dovuta alla caratteristica del satellite di alimentarsi attraverso pannelli solari.

La piattaforma "open" messa a disposizione dal progetto offre a società terze la possibilità di sviluppare applicazioni per il mercato del trasporto stradale. Infatti, i tre servizi di comunicazione sperimentati in SafeTRIP (broadcast, messaggistica, bi-direzionale), associati alle funzionalità di posizionamento e autenticazione, autorizzazione e accounting (AAA), risultano idonee a fornire soluzioni in molti settori, da quello Pubblico a quello della gestione di flotte di veicoli, fino a quello dell'intrattenimento.

Il terminale da istallare a bordo del veicolo, la On-Board Unit (OBU), sarà in grado di fornire servizi personalizzati, quali: chiamate di emergenza, avvisi sul traffico, allarme incidenti, monitoraggio del comportamento del conducente (ad esempio, eccesso di velocità), monitoraggio della funzionalità dei veicoli, rintracciabilità del veicolo, ecc.

Con sempre più veicoli dotati di OBU, permanentemente connesse ai centri servizio tanto da rappresentare nodi mobili di rete, capaci di operare anche con le reti 3G/4G "tradizionali" per servizi connection-based, la piattaforma SafeTRIP mette a disposizione un canale di ritorno in banda S, a basso costo e message-based, aprendo la strada alla potenziale diffusione di un ampio spettro di servizi in cui i veicoli possono realmente rappresentare un'inestimabile fonte di informazione per società di gestione della rete di trasporto, assicurazioni, autorità (protezione civile e servizi di vigilanza).

FUB contribuisce alla definizione dell'architettura della parte di sistema dedicata al supporto del canale interattivo terrestre per la comunicazione tra utente e centro servizi, nonché alla fase di valutazione delle prestazioni complessive del sistema basata sulla realizzazione di field-trials realizzati in condizioni operative reali e con utenti reali. In particolare, in aggiunta alla predisposizione del materiale di supporto alla fase di valutazione (questionari, interviste, ecc.) impiegato nei trials, FUB ha partecipato attivamente alla valutazione dei trials condotti in Spagna.

FUB, inoltre, offre il necessario supporto tecnico-scientifico alla progettazione di una soluzione integrata, basata sull'impiego di tecnologie radio terrestri (UMTS, WiMAX, WiFi, ecc.) e satellitari in banda S, anche con la possibilità di definire alcune parti del terminale che s'intende realizzare, personalizzandolo in base alle esigenze dell'utenza.

Nel corso del 2013, la Fondazione ha svolto le seguenti attività:

- revisione del materiale da utilizzare nella fase di valutazione dei field-trials (questionari, interviste, ecc.);
- supervisione e realizzazione della valutazione dei field-trials condotti a Barcellona;
- analisi dei dati raccolti nei field-trials;
- contribuzione al deliverable D7.1.2 " Trial Results – User Assessment".

Deliverable / Rapporti tecnici

- Celidonio M., Di Zenobio D., Fionda E., Pulcini L., Sergio E., "D7.1.1 User Assessment Plan", 5 febbraio 2013.
- D7.1.2 " Trial Results – User Assessment", marzo 2013.