



Verbale di incontro	<i>Meeting</i>	
Data: 23 luglio 2013	Orario: 9.30 – 18.00	Luogo: Firenze
Argomenti principali	<ul style="list-style-type: none"> • Aggiornamento sulle attività svolte fino a Mese 6 • Pianificazione delle attività del primo anno di progetto 	
Agenda	<ul style="list-style-type: none"> • Punto sulle regole di rendicontazione fornite dalla RT • Aggiornamento sullo stato delle attività a Mese 6 • Analisi dei requisiti e casi d'uso – D1.1 • Analisi dei requisiti di affidabilità, sicurezza, ... – D2.1 • Tecniche e servizi di raccolta dati – D3.2 • Architettura logica <i>Secure! FRW</i> – Task1.2 • Tassonomia eventi e <i>Event Information Model</i> • Tecniche di estrazione e correlazione di informazioni per l'individuazione degli eventi – Task3.3 • Modelli e soluzioni di affidabilità, sicur ... – Task2.2 • Aggregazione e correlazione di eventi – Task3. 4 • Aggiornamenti <i>workplan</i> OO1, OO4 e OO5 • Aggiornamenti <i>workplan</i> OO2 • Aggiornamenti <i>workplan</i> OO3 • Prossimi passi e conclusioni 	
Organizzatore	UniFi - DiMaI	
Partecipanti	<p>Engineering: Gabriele Giunta, Giovanni Bianco</p> <p>CNR: Marinella Petrocchi, Gianpiero Costantino, Giuseppe Amato, Franco Alberto Cardillo, Cristina Muntean, Diego Ceccarelli, Lucia Ghelardi</p> <p>UniFi – DiMaI: Andrea Bondavalli, Andrea Ceccarelli, Nicola Nostro, Leonardo Montecchi</p> <p>UniFi – MICC: Roberto Caldelli, Rudy Becarelli, Andrea Del Mastio</p> <p>Resiltech: Alessandro Daidone, Antonio Bovenzi, Massimiliano Itria</p> <p>Iamboo: Davide Silvestri, Paola Gori, Filippo Mannari</p>	



Emesso da	<i>Gabriele Giunta (ENG)</i>	In data <i>25 Luglio 2013</i>
Distribuzione	<i>ai partecipanti</i>	
Costituiscono parte integrante del verbale i documenti seguenti: <i>Secure!_agenda meeting 23 07 2013.pptx; Secure!_Deliverable 1.1 ENG_23 07 2013.pptx; Secure! D2.1_Final_ver0.1.pptx; Source Integration Framework.pptx; presentazione23-07-13.pptx; A3.3_meeting Firenze.pptx; A2.2-meeting Firenze 17 Luglio 2013 v2.0.pptx; Secure! A2.2 Monitoring_ver0.1.pptx; Secure!_Architettura Logica ENG_23 07 2013.pptx; Secure!_Event Information Model e Tassonomia_ENG_23 07 2013.pptx; Secure! A3.4- Descrizione attività - rev1.1.pptx; Secure!_Workplan ENG_23 07 2013.pptx; Presentazione_IAMBOO_WorkPlan_OO3_23_07_13.pptx; LINEE GUIDA VARIANTI.pdf; linee_guida_BU_RS_2012_rev_0_19_4_13.pdf.</i>		
Punti di discussione <u><i>Punto sulle regole di rendicontazione fornite dalla Regione Toscana</i></u> Il decreto è stato firmato e l'ATS regolarmente costituita. E' stato evidenziato che per la rendicontazione si stanno seguendo le linee guida definite dall'ARTEA (<i>cf. linee_guida_BU_RS_2012_rev_0_19_4_13.pdf</i>). Per poter richiedere l'anticipo è necessario che la domanda sia obbligatoriamente corredata da idonea garanzia fideiussoria rilasciata a favore di ARTEA. Nel caso di soggetti beneficiari in forma aggregata (partenariato) è obbligatorio presentare un'unica polizza intestata al capofila del partenariato. Entro 45 giorni dal termine del primo periodo di rendicontazione (entro l'11/02/2014), il beneficiario/capofila deve rendicontare il 40% dell'investimento ammesso, presentando una domanda di pagamento a titolo di stato avanzamento. La domanda deve essere presentata unitamente alla relazione tecnica di medio periodo sullo stato di avanzamento del progetto, elaborata in base allo schema fornito dalla Regione Toscana, disponibile sul sito di ARTEA. Sono stati inoltre richiesti chiarimenti in merito alla variazione del budget iniziale di IAMBOO e all'estensione di 6 mesi relativamente alle attività 3.3 e 3.4. Si è concordato di fissare un incontro amministrativo interno, possibilmente entro la metà di settembre, per stabilire tutte le variazioni da comunicare in un secondo momento ad ARTEA. <u><i>Aggiornamento sullo stato delle attività dopo 6 mesi</i></u> Si è fatto il punto sullo stato delle attività concluse a Mese 6. In particolare, l'attenzione è stata posta sullo stato di avanzamento dei seguenti <i>deliverable</i> : <ul style="list-style-type: none">• <i>deliverable 1.1</i>: il documento è nella versione finale. Si è deciso di affidare la <i>peer review</i> al DiMaI e al CNR (gruppo Martinelli).• <i>deliverable 2.1</i>: il documento ha già avuto la <i>peer review</i> ed è in attesa di essere rilasciato.• <i>deliverable 3.1</i>: il documento è già stato rilasciato. Allo stato attuale manca il contributo		



su “*crowd-sensing vs sensori standard*”. ENG e IAMBOO stanno valutando di chiuderlo con un loro contributo.

- *deliverable 3.2*: la versione draft del documento sarà rilasciata entro la fine del mese di luglio.

Analisi dei requisiti e casi d'uso – D1.1

Sono stati presentati e condivisi tutti i casi d'uso presenti all'interno della versione finale del *deliverable 1.1*.

Analisi dei requisiti di affidabilità, sicurezza, ... – D2.1

E' stato mostrato il risultato finale dell'analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy. Nell'elenco dei requisiti sono stati inseriti anche gli aspetti di *dependability*, *performance* e *maintenance*, non previsti nel capitolato tecnico. Di conseguenza, si è deciso di considerarli come opzionali. Per quanto riguarda l'assegnazione dell'*ownership* ai vari requisiti specificati, si è deciso di usare il criterio della distribuzione dell'effort nelle attività dell'OO2 .

Tecniche e servizi di raccolta dati – D3.2

Sono stati presentati i risultati parziali del *deliverable 3.2*. In particolare, è stata presentata l'architettura del *Source Integration Framework* (SIF) e dei suoi componenti costitutivi.

La questione principale ha riguardato le tecniche di *crowd-sensing* per la raccolta dati da parte dei dispositivi mobili. Secondo lo schema di funzionamento definito nel documento, il SIF inoltrerà una richiesta al dispositivo a seguito di una situazione di anomalia. A quel punto, il dispositivo attiverà i sensori richiesti e invierà i dati raccolti al SIF (eventualmente verrà scattata una foto o verrà prodotto un video). Durante la discussione è stato proposto di mantenere i sensori del dispositivo sempre attivi, consentendo l'invio di dati nell'eventualità di situazioni pericolose. Questa soluzione presenta però una criticità dovuta al maggiore consumo energetico del dispositivo mobile quando si attivano i sensori. Per rispondere a questa criticità, si è deciso di definire gli scenari di *crowd-sensing* in modo da giustificare come e quando sfruttare i sensori presenti nel dispositivo mobile.

E' stata inoltre affrontata la questione relativa alla segnalazione di eventi da parte di utenti che hanno poca propensione e dimestichezza con le tecnologie moderne. Si è deciso di inserire questi nuovi utenti nella lista degli utenti del sistema e di definire per loro un'interfaccia grafica molto semplice ed intuitiva.

Tecniche di estrazione e correlazione di informazioni per l'individuazione degli eventi

Sono state presentate e affrontate alcune questioni relative all'analisi e all'elaborazione delle immagini (attività 3.3). Si è discusso sul fatto che il modulo di autenticazione delle immagini non è in grado di produrre in output degli eventi. La discussione ha portato a concludere che le informazioni restituite sono invece delle *useful info* e che il modulo potrebbe essere inserito



anche nell'attività 2.5. Un altro punto di discussione è stato quello di capire se l'analisi dei dati provenienti dalla Web TV e dai dispositivi mobili sia da inserire all'interno dell'attività 3.3. A tal riguardo, si è deciso di non considerarla in questo modulo, in quanto restituiscono già degli eventi, anche se si è ritenuto comunque necessario eseguire su tali dati un'operazione di prefiltraggio.

Sono state inoltre assegnate le responsabilità di gestione di ciascun micro-evento definito nella tassonomia. In particolare, per ciascun micro-evento, si è deciso di inserire nel *deliverable* 3.3 una descrizione del problema e alcune possibili soluzioni, anche se, verranno sperimentate solo quelle relative ad alcuni degli eventi individuati. Si è deciso, infine, di non considerare i micro-eventi *Human Health Danger Detection* e *Accident Detection* e di rinominare *Suspicious Community Discovery* in *Trend Discovery*.

Modelli e soluzioni di affidabilità, sicurezza, privacy e trust

Sono stati presentati i risultati dell'attività relativa all'architettura della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (attività 2.2). In particolare, sono state affrontate le problematiche di disponibilità (*dependability*) descritte nel *deliverable* 2.1 mediante l'impiego di soluzioni per il *monitoring* di anomalie del sistema.

Relativamente all'attività di *security* (attività 2.3), *privacy* (attività 2.4) e *trust* 2.5 sono stati descritti alcuni approcci basati rispettivamente su autenticazione biometrica, *secure two-part computation* e *multi-criteria decision making*.

Tassonomia Eventi e Event Information Model

E' stata presentata una proposta iniziale dell'*Event Information Model* e dei relativi descrittori degli eventi e delle sorgenti informative. Si è discusso, in particolare, sulle definizioni di un micro-evento e di un *Secure! Event*, e su quali devono essere gli input e gli output dei componenti definiti nelle attività 3.2, 3.3 e 3.4. Si è deciso di ridiscutere tali tematiche per giungere a decisione condivisa e definitiva.

Prossimi passi e conclusioni

Per mancanza di tempo, si è deciso di rinviare la discussione sulle attività di *preparazione delle informazioni per la successiva fase di decisioning/acting* (attività 3.4), organizzando una *conference call* tra i partner coinvolti nell'attività.

Il prossimo meeting è stato programmato per tra il **20/09** e il **20/10** a Firenze, presso la sede del MICC.

Alle 18.00 si sono chiusi i lavori.

Action plan

- *Peer review deliverable 1.1 (DiMaI, CNR, **entro 2 Agosto**)*



- Rilascio versione finale *deliverable 1.1* (*Engineering*, **entro 9 Agosto**)
- Modifiche modulo di pre-filtraggio architettura *Secure! Framework* (*Engineering*, **entro 31 Luglio**)
- Modifiche *Event Information Model* (*Tutti*, **entro 2 Agosto**)
- Definizione ToC *deliverable 1.2* (*Engineering*, **entro 2 Agosto**)
- Prima raccolta contributi *deliverable 1.2* (*Tutti*, **entro 9 Agosto**)
- Seconda raccolta contributi *deliverable 1.2* (*Tutti*, **entro 31 Agosto**)
- Rilascio versione *draft deliverable 1.2* (*Engineering*, **entro 6 Settembre**)
- Contributi alla versione *draft* del *deliverable 3.2* (*IAMBOO, MICC, CNR, Engineering*, **entro 1 Agosto**)
- Rilascio versione *draft deliverable 3.2* (*IAMBOO*, **entro 9 Agosto**)
- Definizione scenari applicativi e casi d'uso per i piloti (*Engineering*, **entro 13 Settembre**)
- Definizione piano di sperimentazione (*Engineering*, **entro 13 Settembre**)

I contenuti del documento s'intendono approvati automaticamente dai partecipanti se entro 2 giorni lavorativi, successivi alla data di distribuzione dello stesso, non si richiedano modifiche.