La sicurezza dei dati numerici : gestione delle identità, della fiducia e della vita privata nel mondo numerico

IBM *Software Group*

Siamo lieti di accogliervi al podcast sulla sicurezza dei dati numerici. Christian Achermann s'intrattiene con Jan Camenisch, scienziato presso il laboratorio di ricerca IBM a Rüschlikon.

Christian Achermann: «Può darci qualche informazione su di lei e sulla sua funzione presso IBM?»

Jan Camenisch: «Faccio parte del team di ricercatori di questo laboratorio e sono crittografo. Ma sono anche responsabile del progetto europeo PrimeLife, che concerne la protezione delle informazioni personali su Internet e che interessa la gestione delle identità, della fiducia e della vita privata nel mondo numerico.»

Christian Achermann: «Oggi, quando si utilizzano dei servizi on-line, spesso viene chiesto di comunicare un gran numero di dati personali. Quali sono i rischi inerenti queste attività?»

Jan Camenisch: «Da un lato, il rischio è che i dati comunicati vadano a finire in cattive mani, sia semplicemente perché vengono persi, come si legge tutti i giorni sulla stampa, sia perché vengono utilizzati abusivamente dai collaboratori dell'azienda alla quale vengono trasmessi. Dall'altro lato, esiste anche il rischio che i dati vengano utilizzati per creare un «profilo». Per esempio, se lei rivela un'informazioni personale su una rete sociale, questa potrà servire a un potenziale datore di lavoro per decidere se assumerla o no.»

Christian Achermann: «Nell'ultima edizione di THINK!, la rivista per i clienti di IBM, si può leggere che lei e il suo team lavorate ad una soluzione innovativa destinata a proteggere i dati sensibili, chiamati «Identity Mixer». Potrebbe dirci a che punto si trova attualmente questo progetto, spiegandoci le funzioni della sua soluzione ?»

Jan Camenisch: «Grazie a questa soluzione, cerchiamo di divulgare il problema di un eccesso di informazioni e ciò da tre prospettive diverse. Prima di tutto cerchiamo di ridurre al minimo i dati che le persone devono comunicare, secondariamente, di aiutare gli utenti a fidarsi dei loro partner on-line e, terzo punto, di restituire agli utenti il controllo dei loro dati. Ecco un esempio di minimizzazione del numero dei dati: se ha una carta d'identità elettronica e desidera prendere una birra al bar, spesso deve provare di avere l'età minima. Con una carta d'identità elettronica, divulga tutte le informazioni in essa contenute, compresi i suoi dati personali. Grazie alla nostra tecnologia, potrà rivelare al barman di avere più di 18 anni e niente altro. Questa è la minimizzazione del numero dei dati. Al contrario, quando entra in un bar, vuole essere certo che si tratti veramente di un bar e che lei stia realmente parlando con un barman. Naturalmente nel caso di un bar, è facile. Ma su Internet, non si è mai sicuri del sito con il quale si comunica e se c'è da fidarsi.
Le applicazioni che stiamo sviluppando permettono di creare facilmente questa fiducia.

Per quanto concerne i dati personali, la cui divulgazione è evidentemente inevitabile, noi informiamo innanzitutto l'utente della sorte loro riservata - i dati saranno conservati per dieci anni o, al contrario, cancellati alla fine della transazione? – e che è autorizzato ad utilizzarli e a quale scopo.
Alcune di queste soluzioni sono già disponibili per la trasmissione elettronica e una parte del codice di base esiste. Siamo tuttavia ancora in fase di costruzione e di espansione. Siamo alla ricerca di un metodo di standardizzazione e interfacce utenti che rendano accessibile la tecnologia al maggior numero possibile, permettendo al settore industriale di integrare queste tecnologie nei loro software, consentendo l'evoluzione verso una soluzione standard.»

Christian Achermann: «Quali difficoltà ha incontrato durante il processo di sviluppo? Cosa ha fatto per evitare questi inconvenienti?»

Jan Camenisch: «Da ormai oltre dieci anni lavoriamo a queste soluzioni e da quando abbiamo iniziato, si trattava principalmente d'identificare le sfide matematiche alle quali siamo confrontati in materia di crittografia. Se ho una carta d'identità numerica che conferma la mia data di nascita, come posso utilizzarla per convincere il barman che ho più di 18 anni, senza rivelare la mia data di nascita? Come elaborare i meccanismi crittografici necessari? Una volta trovate le soluzioni, il difficile è stato spiegare il loro funzionamento ai nostri colleghi, affinché sviluppassero le interfacce utenti permettendo l'uso intuitivo di queste tecnologie. Penso che qui si tratti della parte più importante. Senza buone interfacce utenti, questa tecnologia non sarà mai messa in funzione e penso che siamo ancora in alto mare in materia di ricerca in questo campo. Abbiamo alcune bozze di soluzioni, ma sono convinto che possiamo fare molto meglio.»

Christian Achermann: «Guardando al futuro, come continuerà lo sviluppo della vostra soluzione nei prossimi mesi e negli anni a venire?»

Jan Camenisch: «Direi che siamo arrivati a buon punto per quanto concerne la tecnologia di base degli algoritmi crittografici. Sappiamo come emettere carte d'identità elettroniche e certificati. Per quanto concerne la fase successiva, sapere come trasmettere i dati, stiamo standardizzando il tutto e stiamo creando delle norme e dei protocolli di comunicazione. Qui, parliamo di processi di standardizzazione.
A livello superiore, quello delle interfacce utenti, abbiamo già le prime soluzioni, ma la ricerca in questo campo non è terminata. D'altra parte, se consideriamo il modo in cui le persone utilizzano Internet oggi, per esempio inviando una grande quantità di dati tramite le reti sociali ed i wikis, la nostra tecnologia non può essere applicata facilmente in questo campo e dobbiamo quindi proseguire le nostre ricerche, ipotizzando il miglior modo per proteggere le persone. Così che un futuro datore di lavoro, non dovrà necessariamente vedere le immagini dell'ultima ubriacatura ad una festa.»

Christian Achermann: «Per concludere, se nessuno di questi tipi di prodotto esiste attualmente sul mercato, come si possono proteggere al meglio i dati personali? Potrebbe dare qualche suggerimento?»

Jan Camenisch: «Penso che la miglior cosa da fare sia quella di stare molto attenti ai partner con i quali si comunica e ai dati che si trasmettono.

Potreste per esempio tentare di leggere le loro condizioni concernenti il rispetto e la riservatezza della vita privata, ma spesso sono molto difficili da trovare. Altrimenti, credo che sarebbe meglio non utilizzare le carte di credito e gli indirizzi e-mail e non dare informazioni personali, se non è necessario. Naturalmente, se desiderate farvi recapitare qualcosa a casa, dovrete comunque indicare il vostro vero indirizzo.»

Christian Achermann: «La ringrazio molto per il tempo che ci ha dedicato e per le sue interessanti informazioni.»