

Presentazioni finali dei progetti di master *e-Service Technologies unit*



Consorzio per la Formazione e la Ricerca
in Ingegneria dell'Informazione

Politecnico di Milano

martedì 2 luglio 2002, ore 9.30
CEFRIEL - Aula Bellisario

Agenda:

- | | | | |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ore 9.30 | Maurizio Brioschi | | <i>Presentazione e-Service Technologies unit</i> |
| ore 9.40 | Giovanni Rosso |  | <i>Prestazioni delle applicazioni e dei protocolli Internet nelle reti radiomobili UMTS</i> |
| ore 10.00 | Luca Venturi |  | <i>Valutazione degli aspetti di sicurezza per la trasmissione di informazioni in modalità multicast</i> |
| ore 10.20 | Dario Boninsegni |  | <i>Bandwidth Estimation: algoritmi per la stima della banda</i> |
| ore 10.40 | Carmelo Silvestro |  | <i>Intrusion Detection Systems e Log Correlation</i> |
| ore 11.00 | <i>Coffee break</i> | | |
| ore 11.20 | Filippo Consonni |  | <i>Tecnologie multimodali per servizi mobili</i> |
| ore 11.35 |  DEMO - M³L (MultiModal Markup Language): piattaforma per servizi multimodali fruibili simultaneamente da Web e voce | | |
| ore 11.45 | Daniela Farulla |  | <i>Servizi a valore aggiunto per terminali mobili</i> |
| ore 12.00 |  DEMO - Java Mobile Messaging System: middleware per lo scambio di messaggi XML tra terminali mobili | | |
| ore 12.10 | Luca Pezzilli |  | <i>Firma digitale in ambito wireless</i> |
| ore 12.25 |  DEMO - Mobile Strong Authentication: architettura per l'autenticazione tramite certificati digitali su terminali mobili | | |
| ore 12.35 | Marco Bua |  | <i>Semantic Knowledge Management: il significato dell'informazione</i> |
| ore 12.50 |  DEMO - VisualOIL e ReportOIL: metodologia e strumenti per il Semantic Knowledge Management | | |

Prestazioni delle applicazioni e dei protocolli Internet nelle reti radiomobili UMTS

Tutor: Michele Milani

Studente: *Giovanni Rosso*

In collaborazione con:



Con la disponibilità ormai prossima di tecnologie di trasmissione radiomobili a pacchetto, diventa effettivamente attuabile la diffusione di tradizionali servizi e applicazioni Internet su dispositivi mobili. La realizzazione di nuove reti a pacchetto (in particolare GPRS a breve termine e UMTS in una seconda fase), offre la reale possibilità di fruire di applicazioni IP esistenti tramite smart phone o PDA.

Tali applicazioni sono basate sull'ormai consolidata pila protocollare TCP/IP; sebbene questi protocolli siano stati progettati per funzionare con qualsiasi tipo di collegamento e di protocollo di livello Datalink, le prestazioni ottimali del protocollo TCP si ottengono quando si lavora su reti fisse: con le reti radiomobili si evidenzia una loro degradazione, causata da fattori quali l'elevato tasso di perdita e i lunghi e improvvisi ritardi, tipici del mezzo radio.

Migliorare le prestazioni del protocollo TCP e, di conseguenza, delle applicazioni Internet, in ambito radiomobile è un obiettivo essenziale, visto che tali reti offrono una banda limitata. Per tale scopo, sono stati proposti diversi approcci, sia in ambito scientifico che industriale, distinti in due diverse categorie: proposte di modifica di alcuni parametri del protocollo TCP e proposte di nuove architetture di rete.

Scopo del presente lavoro è proporre e valutare un meccanismo per l'ottimizzazione delle prestazioni delle applicazioni Internet su rete UMTS. Tale valutazione viene effettuata tramite una serie di simulazioni e di confronti con altri possibili approcci.

Keywords: *UMTS, mobile Internet, TCP, performance, QoS*

Valutazione degli aspetti di sicurezza per la trasmissione di informazioni in modalità multicast

Tutor: Davide Cerri

Studente: *Luca Venturi*

In collaborazione con:



L'importanza della trasmissione di dati in modalità multicast, in applicazioni quali streaming audio/video, video-conferenza, invio di notizie "push", aggiornamento di software, è cresciuta con l'espandersi delle possibilità di utilizzo della rete Internet. La tecnologia multicast offre funzionalità vantaggiose per la creazione di gruppi di utenti interessati allo stesso servizio in un contesto Internet, ma non fornisce al momento funzionalità di sicurezza che permettano di garantire, ad esempio, la riservatezza e l'integrità della comunicazione e l'autenticazione dei partecipanti, funzioni che in molte applicazioni sarebbero invece desiderabili o necessarie.

Per fornire servizi di sicurezza in contesti di questo tipo è necessario considerare le particolarità e le diversità che il caso multicast presenta rispetto alle normali connessioni uno ad uno, in quanto la comunicazione che deve essere protetta riguarda un intero gruppo di utenti, e non una singola coppia di interlocutori.

Obiettivo di questo progetto è lo studio di architetture che permettano di gestire le chiavi associate ad una comunicazione di gruppo, siano esse di tipo centralizzato oppure distribuito, e la loro valutazione tramite simulazioni. È, infatti, importante tenere in considerazione l'aspetto prestazionale, in modo da non imporre un eccessivo sovraccarico (sia in termini di occupazione di banda che di carico computazionale) dovuto alle funzionalità di sicurezza e alle operazioni relative alla loro gestione. Sempre dal punto di vista delle prestazioni, è necessario valutare le caratteristiche di scalabilità e robustezza delle varie soluzioni, al variare dei diversi parametri che possono influire su di esse.

Keywords: *multicast, comunicazione sicura, gestione chiavi, prestazioni*

Bandwidth Estimation: algoritmi per la stima della banda

Tutor: Paolo Castagna

Studente: *Dario Boninsegni*

In collaborazione con:



Con l'aumentare del numero degli host e dei dispositivi che accedono ad Internet diventano sempre più pressanti i problemi di scalabilità, di gestione della banda disponibile e di prestazioni. In ultima analisi, ciò che determina il throughput di una trasmissione dati, e quindi le prestazioni raggiungibili da un protocollo di trasporto, è la banda disponibile nell'istante in cui avviene l'invio dei dati. In particolare, è determinante il link che ha la minima banda disponibile: il collo di bottiglia (bottleneck).

Risulta quindi molto importante avere strumenti e mezzi per stimare con un certo grado di affidabilità la banda disponibile, e quindi il bottleneck, lungo un dato percorso in Internet e, se possibile, individuarne la posizione tra due nodi della rete. I contesti pratici in cui sono richiesti metodi per la stima della banda sono diversi: verifica di Service Level Agreement, sistemi di gestione della banda, sistemi per il load balancing distribuito, architetture per la QoS. Per questi motivi, nell'ambito delle reti IP, sono stati proposti alcuni possibili metodi e algoritmi per stimare, indirettamente, la banda disponibile di un determinato percorso.

Obiettivo di questo progetto è quello di studiare i differenti algoritmi finora proposti per la stima della banda fisica e della banda disponibile; dal loro studio se ne spiega il comportamento e si ricavano dei parametri per descriverne le prestazioni. Da ultimo si definiscono possibili nuove proposte o miglioramenti per un algoritmo di stima della banda disponibile che operi senza immettere traffico in rete, in modalità end to end.

Keywords: *TCP, bandwidth estimation, bottleneck bandwidth, performance, QoS*

Intrusion Detection Systems e Log Correlation

Tutor: Davide Cerri

Studente: *Carmelo Silvestro*

In collaborazione con: **key.consultants**

Per assicurare un adeguato livello di sicurezza all'interno di una rete telematica e nell'ottica di costruire un'infrastruttura integrata di sicurezza, tra i diversi dispositivi e metodologie adottabili gli Intrusion Detection System (IDS) rivestono un ruolo fondamentale, in particolare per quanto riguarda il monitoraggio attivo per il rilevamento di eventuali attacchi in atto.

Gli IDS si possono classificare in due categorie a seconda delle tecniche che adottano per individuare eventuali attacchi: con "misuse detection" si intende il rilevamento di comportamenti non corretti, utilizzando una base di dati contenente le "firme" di attacchi noti, mentre con "anomaly detection" si intende il rilevamento di comportamenti inusuali, ovvero di attività che deviano dal comportamento osservato in condizioni normali. In entrambi i casi, quando gli IDS ritengono che un evento o una serie di eventi possa essere riconducibile ad un attacco in corso producono delle segnalazioni di allarme, tuttavia a volte segnalano un allarme per eventi che non sono dovuti ad attacchi in atto (falsi positivi), mentre altre volte non riescono a rilevare attività effettivamente nocive (falsi negativi).

Gli attacchi sono spesso complessi e difficili da rilevare, e una maggiore efficacia si può ottenere monitorando mediante IDS diversi sistemi e diversi punti di una rete, ed elaborando poi opportunamente tutte le segnalazioni provenienti dai vari sensori. Obiettivo di questo progetto è lo studio di questa elaborazione centralizzata, che dovrebbe eliminare i falsi allarmi e contemporaneamente rilevare reali attacchi in atto, aggregando e correlando le informazioni provenienti dai diversi sensori presenti sulla rete.

Keywords: *intrusion detection, log correlation*

Tecnologie multimodali per servizi mobili

Tutor: Marco Riva

Studente: Filippo Consonni

In collaborazione con:



Ormai da quasi tre anni è in corso un'attività del World Wide Web Consortium (W3C) per la definizione e la prototipazione di "browser multimodali": browser nei quali l'interazione con l'utente non è limitata all'uso dello schermo, della tastiera e dei dispositivi di puntamento, ma si appoggia anche sulle tecnologie per il riconoscimento automatico della voce (Automatic Speech Recognition - ASR) e di traduzione da testo a voce (Text To Speech - TTS). In questa visione, l'utente può servirsi a suo piacimento sia della modalità classica, sia della modalità vocale. Questa attività, tuttavia, non ha ancora portato alla diffusione di un reale prodotto sul mercato; la causa è, forse, da ricercarsi nell'abitudine, ormai consolidata, degli utenti di ricorrere a tastiera e mouse per interagire, alla praticità di utilizzo dei dispositivi stessi e alla mancanza di linguaggi standard per la realizzazione di applicazioni multimodali.

Un dispositivo mobile, però, proprio per le sue limitate dimensioni e per la difficoltà intrinseca che gli utenti sperimentano durante l'interazione, potrebbe sfruttare a pieno le potenzialità offerte dalle tecnologie multimodali, facendo allo stesso tempo tesoro dell'esperienza accumulata in questi anni in ambito Internet. Portare le tecnologie multimodali in un contesto Mobile introduce, tuttavia, una serie di nuove problematiche da affrontare: architetture, di sincronizzazione tra canali, di usabilità per l'utente finale.

Lo scopo del progetto è identificare tutte le architetture e le soluzioni proposte dai vari produttori, confrontarle e proporre una nuova soluzione in grado di risolvere i problemi tipici dovuti all'utilizzo contemporaneo di più media, primo tra tutti la sincronizzazione di input e output. Inoltre, il progetto intende proporre un linguaggio appositamente studiato per la realizzazioni di applicazioni multimodali.

Keywords: *multimodal, multichannel, XML, VoiceXML, WML, HTML, channel synchronization*

Servizi a valore aggiunto per terminali mobili

Tutor: Nicola Simeoni

Studente: Daniela Farulla

In collaborazione con:



Lo sviluppo del cosiddetto "Wireless Internet", ovvero la possibilità per l'utente di usufruire di un insieme esteso di servizi a valore aggiunto (siano essi informativi, di intrattenimento, dispositivi o in generale transazionali) attraverso terminali mobili di vario tipo (come telefoni cellulari o palmari), rappresenta oggi un obiettivo strategico per tutto l'ambito dell'Information & Communication Technology.

Attualmente, quindi, grande è l'interesse nello sviluppo di soluzioni per questo mercato, ma non molte sono le tecnologie di front-end disponibili per questo tipo di applicazioni. Una soluzione promettente è quella proposta da Sun Microsystems con il suo ambiente Java 2 Micro Edition (J2ME). L'utilizzo di Java all'interno del contesto mobile, in sinergia con le altre tecnologie disponibili allo stato attuale quali ad esempio SMS o WAP, allarga lo spettro dei possibili servizi per l'utente, fornendo funzionalità aggiuntive per il download on-the-fly delle applicazioni, l'immagazzinamento, l'elaborazione (anche in modalità offline), la presentazione e la trasmissione dei dati da e verso i dispositivi mobili.

L'ambito di interesse del tema di ricerca in oggetto è focalizzato proprio sui servizi a valore aggiunto e sulle tecnologie che si possono utilizzare per la loro realizzazione e fornitura, in particolare sulla tecnologia Java 2 Micro Edition. Le applicazioni di interesse all'interno dello scenario delineato sono diverse: streaming di contenuti audio/video, m-commerce, sistemi di pagamento sicuro, giochi, instant messaging, ecc. Un successivo ambito di indagine dell'attività riguarda, inoltre, le modalità di accesso ai *Web Services* da terminali mobili.

Keywords: *mobile Internet, mobile VAS, Java Phone, J2ME, Web Services*

Firma digitale in ambito wireless

Tutor: Alessandro Ghioni

Studente: Luca Pezzilli



In collaborazione con: SECURITY™

Gli algoritmi per il calcolo della firma digitale si basano sui principi della crittografia asimmetrica, altrimenti detta crittografia a chiave pubblica, mentre con il termine "Public Key Infrastructure" (PKI) s'intende l'infrastruttura che consente la gestione e la distribuzione delle chiavi e le operazioni di firma.

Le tecnologie di PKI esistenti per il contesto wired hanno raggiunto un livello di maturità e di affidabilità che ne rende possibile l'utilizzo su vasta scala; tra gli aspetti critici del sistema riveste un ruolo fondamentale la gestione delle credenziali digitali personali. Tipicamente la fase di firma può richiedere la presenza di un PC con un lettore di smart card collegato, un software di firma, la smart card con le credenziali digitali ed il codice per attivarla.

Se si varia lo scenario applicativo, introducendo nell'infrastruttura PKI un terminale wireless, diventa possibile associare le credenziali digitali ad un "Personal Trusted Device" legato univocamente al proprietario. Si aggiungono, però, nuove problematiche da analizzare e affrontare. Il mobile device è inoltre un terminale poco adatto per la fruizione di contenuti o l'invocazione di servizi web-like.

Scopo di questo lavoro è l'analisi approfondita dello scenario applicativo e delle tecnologie abilitanti la firma digitale wireless e la realizzazione di una soluzione prototipale per fornire un servizio di firma digitale da un wireless device. Il prototipo realizzato permette operazioni di Strong Authentication tramite firma digitale, con fruizione del servizio da un terminale flessibile, quale un PC, e operazioni di firma/autenticazione da un terminale fidato, quale un mobile device. Tali operazioni sono invocabili da terze parti mediante metodi esportati via SOAP. L'architettura studiata rende anche possibile l'estensione dell'applicazione verso un servizio di firma di piccoli contratti.

Keywords: *mobile, digital signature, WPKI, Web Services, Multichannel, J2ME*

Semantic Knowledge Management: il significato dell'informazione

Tutor: Emanuele Della Valle

Studente: Marco Bua



In collaborazione con:

In tutto il mondo un numero sempre maggiore di imprese si è reso conto di quanto sia importante non solo accumulare conoscenza, ma anche conoscere ciò che come azienda si conosce. Proprio per far fronte alla crescente necessità di gestire la conoscenza aziendale, molte imprese si stanno dotando di portali intranet. Questi, tuttavia, si tramutano spesso in centri di costo più che in centri di conoscenza, a causa della grossa mole di informazione da gestire e dell'assenza di chiare linee guida redazionali. Non è difficile immaginare come il costo di gestione possa diventare rapidamente insostenibile se non ci si preoccupa di gestire la "qualità" dell'informazione in ingresso. In particolare, si osserva un lento, ma continuo divaricarsi del "gap" tra la mole di informazione immagazzinata e il "significato" di questa informazione.

Un accesso veloce e diretto all'informazione aziendale può essere ottenuto solo attraverso un sistema di Knowledge Management in grado di elaborare il "significato" dell'informazione contenuta nei dati immagazzinati. Il Semantic Knowledge Management propone di affiancare ai classici metadati una "ontologia", ossia un modello del dominio applicativo, proprio dell'organizzazione, che ne catturi i concetti e ne espliciti le interdipendenze. In altre parole, propone di utilizzare una solida concettualizzazione sulla quale costruire applicazioni capaci di processare il "significato" dell'informazione.

Obiettivo della borsa è, pertanto, far evolvere la metodologia di knowledge management di Getronics attraverso l'introduzione del concetto di metodologia. Esso permette di facilitare la fase di analisi e valutazione delle aree di conoscenza, tramite l'utilizzo di strumenti realizzati ad hoc, caratterizzati dal fornire sia una "visione d'insieme" che una "visione puntuale" degli elementi di conoscenza, di verificare la consistenza e la coerenza dei contenuti e di configurare in modo semiautomatico un sistema di Content Management.

Keywords: *ontology, metadata, RDF, RDFSchema, OIL, DAML+OIL*

Per ulteriori informazioni rivolgersi a:

Ing. Michele Milani - ***e-Service Technologies unit***

CEFRIEL via Fucini, 2 - 20133 Milano

Tel. 02 23954 210 - Fax. 02 23954 254

michele.milani@cefriel.it

Sito web e-Service Technologies unit:

www.cefriel.it/etech