Scuola Universitaria Professionale della Svizzera Italiana
SUPSI
Dipartimento Tecnologie Innovative

Aspetti di sicurezza nelle comunicazioni mobili e pervasive

Silvano Marioni, CISSP

Lugano, 8 aprile 2004

Scuola Universitaria Professionale della Svizzera Italiana
SUPSI
Dipartimento Tecnologie Innovative

Uno studio di caso

Utile annuale non-voice per utente

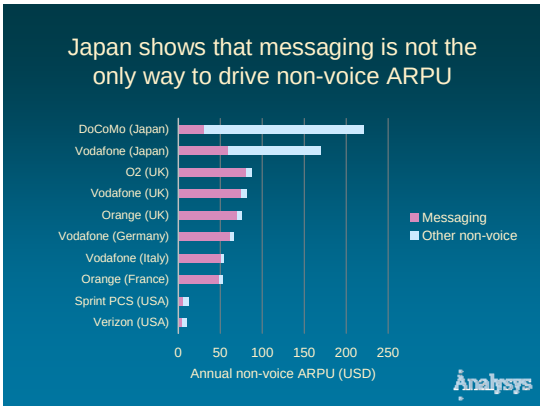


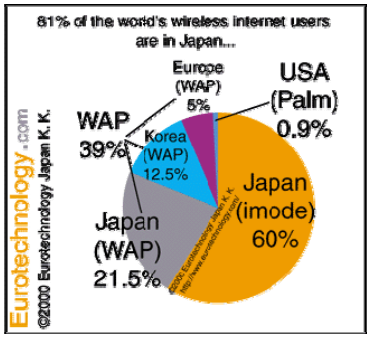
Figure 1: Annual non-voice Annual Revenue Per Users of selected major operators worldwide [Source: Sound Partners/Analysys Research, 2004]

Uno studio di caso

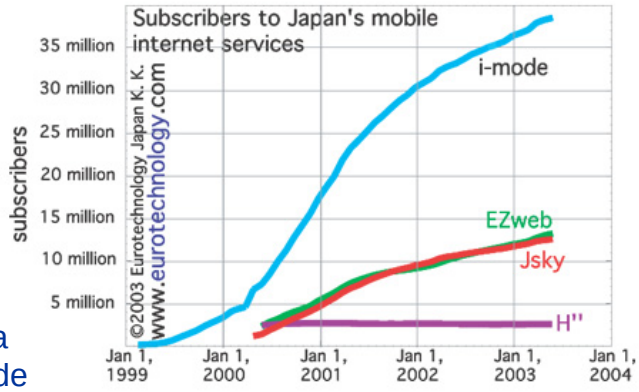
Distribuzione dell'Internet mobile

A Novembre 2000 gli utenti mondiali dell'Internet Mobile erano distribuiti in questo modo (numero di abbonati):

- Giappone: 20 millioni di utenti (I-mode e WAP)
- Corea: 2-3 millioni di utenti (WAP)
- Europe: 1-2 millioni di utenti (WAP)
- USA: 0.5 millioni di utenti (WAP e PALM)



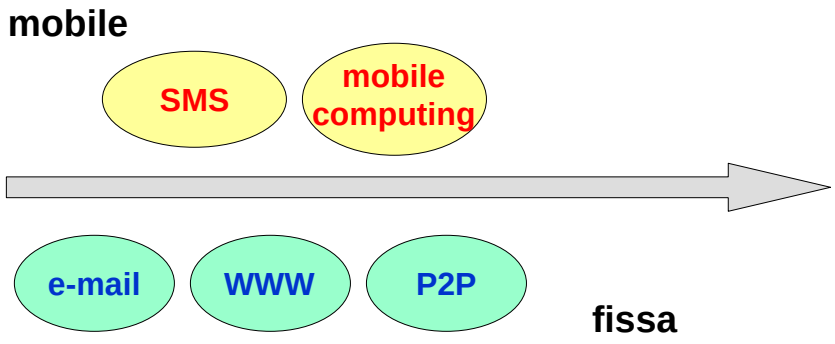
Uno studio di caso



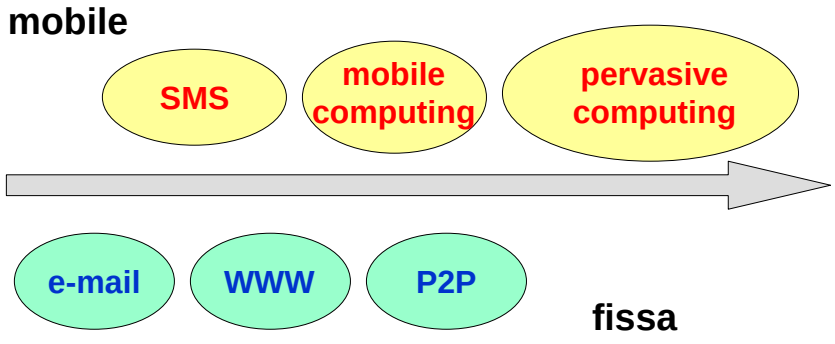
Evoluzione della tecnologia i-mode

popolazione giapponese 127 milioni

La comunicazione dati

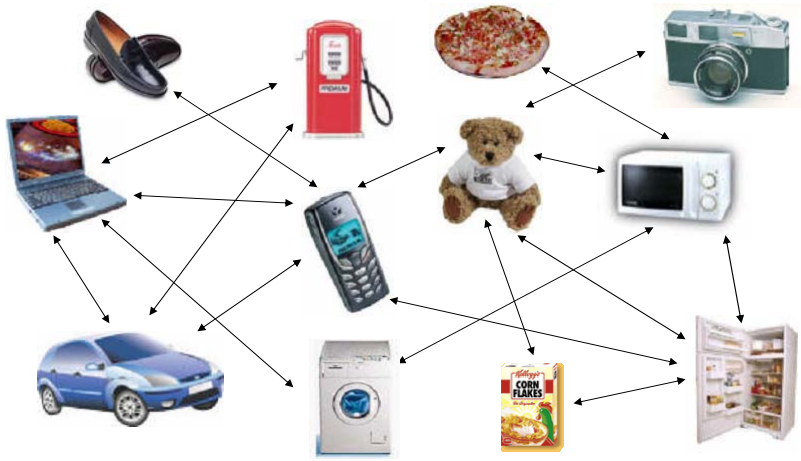


L'evoluzione della comunicazione dati



Scuola Universitaria Professionale della Svizzera Italiana SUPSI — Dipartimento Tecnologie Innovative

Oggetti intelligenti e interconnessi



Scuola Universitaria Professionale della Svizzera Italiana SUPSI — Dipartimento Tecnologie Innovative

Architetture di comunicazione

	fissa	mobile
centralizzata	WWW E-mail	SMS WAP, I-mode
paritetica	P2P	Ad hoc network

Sicurezza dei sistemi pervasivi

- Un sistema informativo e di comunicazione pervasivo presenta nuovi problemi di sicurezza rispetto alle altre architetture
- Questo dipende da:
  - La mancanza di strutture centrali di controllo e coordinamento
  - La natura dinamica dei collegamenti tra i vari nodi

Aspetti fondamentali di sicurezza

Un sistema informativo e di comunicazione deve:

- essere utilizzabile
- proteggere le informazioni
- comprovare le attività svolte
- fornire il servizio atteso

Scuola Universitaria Professionale della Svizzera Italiana SUPSI Dipartimento Tecnologie Innovative

Essere utilizzabile

- Disponibilità
  - Capacità di fornire il servizio quando è richiesto
  - Punti aperti
    - Non esistono nodi specializzati nella gestione di rete
    - Problemi di istradamento
    - Problemi di di scalabilità
    - Problemi di “egoismo” dei nodi

Scuola Universitaria Professionale della Svizzera Italiana SUPSI Dipartimento Tecnologie Innovative

Proteggere le informazioni

- Controllo accessi
  - Identificazione, autenticazione, autorizzazione
  - Punti aperti
    - In un sistema gestito da un’autorità di fiducia, esiste sempre la possibilità di intrusioni, sia via etere sia a livello fisico sui nodi. Nel sistema potrebbe non esistere un’autorità di fiducia
    - In tutti i casi deve essere previsto un sistema di sicurezza cooperativo, dove la maggior parte dei nodi “onesti” collabora all’identificazione e all’esclusione dei nodi “disonesti”

Scuola Universitaria Professionale della Svizzera Italiana SUPSI Dipartimento Tecnologie Innovative

Proteggere le informazioni

- Riservatezza
  - Informazioni disponibili solo agli utenti autorizzati
  - Punti aperti
    - La riservatezza può essere garantita con la crittografia.
    - Non esiste un organismo centrale di gestione delle chiavi
    - Il problema della distribuzione delle chiavi può essere risolto con un sistema cooperativo ispirato a PGP dove ogni nodo condivide con gli altri nodi le chiavi che ritiene fidate.

Scuola Universitaria Professionale della Svizzera Italiana SUPSI Dipartimento Tecnologie Innovative

Proteggere le informazioni

- Integrità
  - Informazioni protette da modifiche o cancellazioni non autorizzate
  - Punti aperti
    - L'integrità può essere garantita con la firma digitale.
    - Non esiste un organismo centrale di gestione delle chiavi
    - Il problema della distribuzione delle chiavi può essere risolto con un sistema cooperativo ispirato a PGP dove ogni nodo condivide con gli altri nodi le chiavi che ritiene fidate.

Comprovare le attività svolte

- Tracciabilità
  - Memorizzazione degli eventi per verifiche future
  - Punti aperti
    - Un giornale degli eventi è fondamentale per motivi tecnici, organizzativi, legali, ecc..
    - Ogni nodo dovrebbe mantenere un proprio giornale
    - Non esistendo un organismo centrale incaricato di controllare la correttezza dei giornali, questa attività dovrebbe essere fatta tra i vari nodi cooperando tra di loro

Comprovare le attività svolte

- Non ripudio
  - Prova che una comunicazione ha avuto luogo
  - Punti aperti
    - Il non ripudio può essere garantito con la firma digitale.
    - Non esiste un organismo centrale di gestione delle chiavi
    - Il problema della distribuzione delle chiavi può essere risolto con un sistema cooperativo ispirato a PGP dove ogni nodo condivide con gli altri nodi le chiavi che ritiene fidate.

Fornire il servizio atteso

- Affidabilità
  - Garanzia di qualità del servizio
  - Punti aperti
    - Manca un organismo che si impegna formalmente sulla qualità del servizio
    - Questa può essere garantita attraverso la ridondanza e la riconfigurazione dei percorsi.

Fornire il servizio atteso

- Privacy
  - Diritto a proteggere i propri dati personali
  - Punti aperti
    - Ogni nodo dovrebbe essere in grado di proteggere i dati che sono considerati privati con la blindatura di particolari aree di dati

Fornire il servizio atteso

- Anonimità
  - Diritto a nascondere la propria identità
  - Punti aperti
    - I nodi dovrebbero definire dei comportamenti che evitino di essere tracciati e identificati ma che non pregiudichino le necessità di autenticazione.

Fornire il servizio atteso

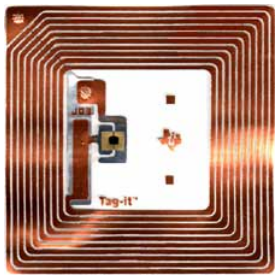
- Usabilità
  - Trasparenza per l'utente nell'uso del servizio
  - Punti aperti
    - La semplicità e la praticità d'uso riducono la consapevolezza dell'utente su quello che avviene nella realtà della comunicazione, rendendolo meno responsabile delle conseguenze delle sue azioni

RFID - Radio Frequency Identification

« These tiny tags, predicted to cost less than 1 cent each by 2004, are "somewhere between the size of a grain of sand and a speck of dust." They are to be built directly into food, clothes, drugs, or auto-parts during the manufacturing process »

« Theft will be drastically reduced because items will report when they are stolen, their smart tags also serving as a homing device toward their exact location. »

« … a world in which every item on the planet is numbered, identified, catalogued, and tracked. And the technology exists to make this a reality »



Conclusioni

- Il mobile computing è una realtà consolidata
- Il pervasive computing si sta affacciando sulla scena tecnologica
- I requisiti di sicurezza possono diventare una componente critica per l'affermazione di queste tecnologie
- La mancanza di alcuni requisiti di sicurezza potrà creare il rifiuto di queste tecnologie?
- Siamo tutti d'accordo di avviarci verso una società senza privacy?

La SUPSI e la gestione della sicurezza

- La Formazione Continua SUPSI offre i seguenti corsi sul tema della sicurezza:

- 1.12 – La sicurezza informatica in azienda
- 1.15 – La sicurezza dei sistemi e delle reti
- 1.36 – Introduzione alla revisione informatica

- E' in fase di preparazione il Corso Post Diploma sulla Sicurezza Informatica.

Domande ?