La sicurezza nelle gare telematiche

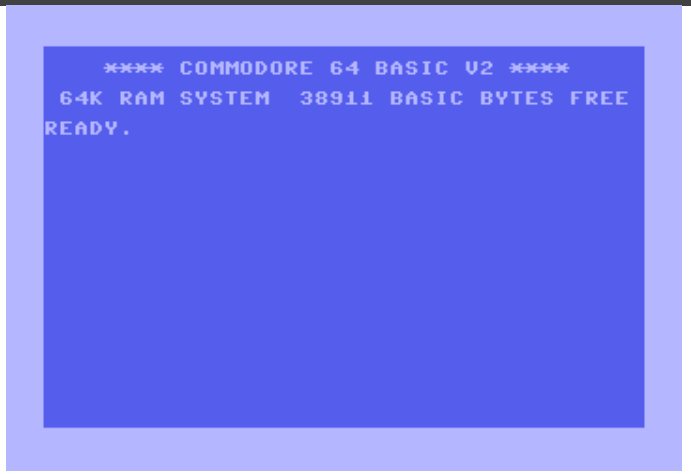
Luciano Baresi

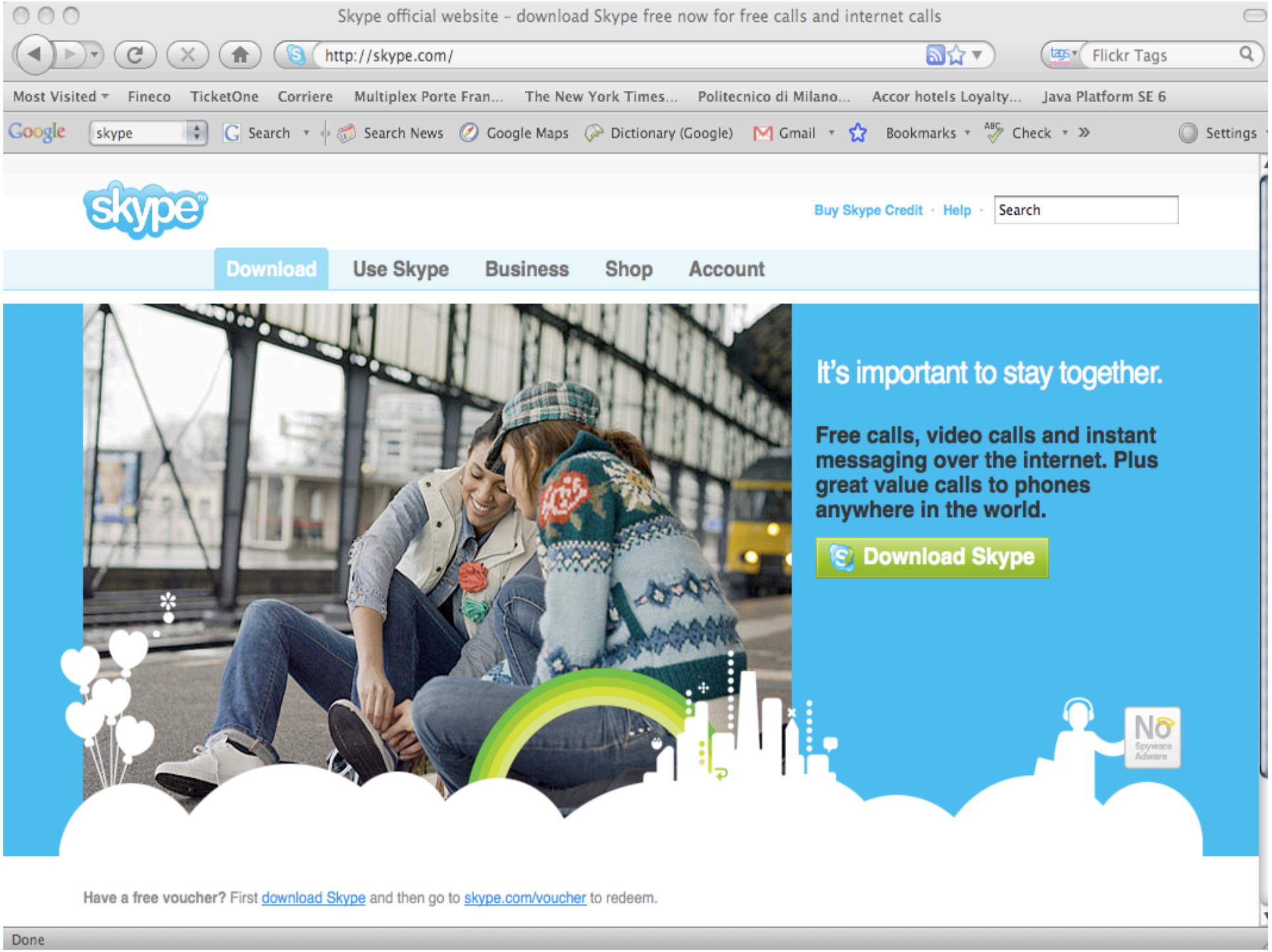
Politecnico di Milano

luciano.baresi@polimi.it

Il mio primo computer

- CPU: 1,01 Mhz
- RAM: 5-27 Kb
- Grafica: 176 x 184 16 colori
- Floppy disk da 170 Kb o nastri




Skype official website - download Skype free now for free calls and internet calls
http://skype.com/
Flickr Tags
Most Visited
Fineco
TicketOne
Corriere
Multiplex Porte Fran...
The New York Times...
Politecnico di Milano...
Accor hotels Loyalty...
Java Platform SE 6
Google
skype
Search
Search News
Google Maps
Dictionary (Google)
Gmail
Bookmarks
Check
Settings
skype
Buy Skype Credit · Help ·
Search
Download
Use Skype
Business
Shop
Account
It's important to stay together.
Free calls, video calls and instant messaging over the internet. Plus great value calls to phones anywhere in the world.
Download Skype
No Spyware Adware
Have a free voucher? First download Skype and then go to skype.com/voucher to redeem.
Done

Quindi

- Oggi tutto si fa “su Internet”
- Non essendo visibile, non abbiamo una chiara percezione dei problemi e della complessità
- Diamo per scontate molte cose che non dovrebbero esserlo
  - Ci pensiamo solo in caso di problemi

Mondo ideale

- Tutto perfetto
- Velocità “infinita”
- Nessun malfunzionamento
- Nessun dolo e nessun tentativo di truffa

Mondo reale

- Il software può fare errori
- La banda può non essere sufficiente
- Dolo e truffe sono in agguato

Come possiamo difenderci?

Sicurezza

- Autenticazione
  - Come possiamo provare di essere chi dicono di essere
- Autorizzazione
  - Come possiamo essere certi che certe operazioni vengano fatte solo da chi è autorizzato
- Confidenzialità
  - Come evitare che informazioni riservate sia visibili a chi non è autorizzato
- Integrità
  - Come evitare che i messaggi vengano manomessi

Modello classico

- Offerta presentata per via telematica
- Ricevuta di consegna

- File di log
- Fiducia delle persone coinvolte

Qualcosa di più efficiente

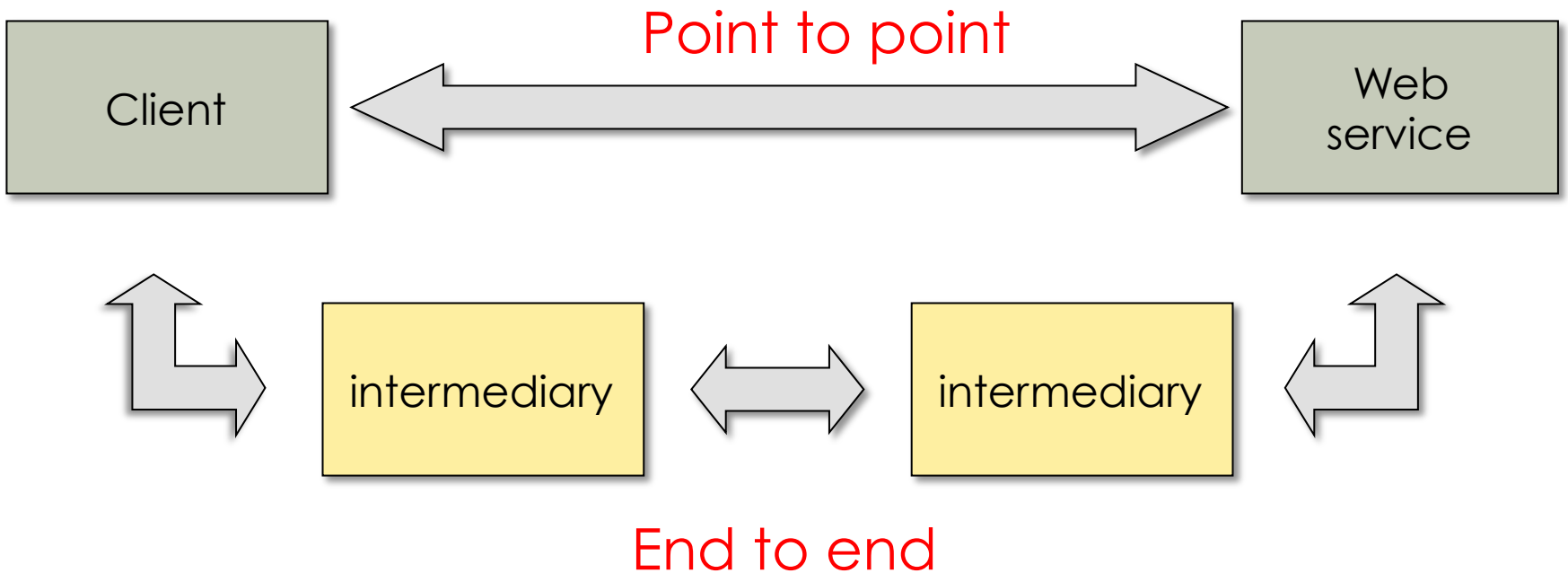
- L'offerta viene marcata, ma resta sulle macchine del partecipante
  - Firma digitale e marca temporale
- Gli elementi identificativi del file marcato vengono caricati sul server del gestore
- Caricamento dell'offerta sul server del gestore
- Controllo delle credenziali

Tutti qui?

- Chiaramente no

- Criticità delle applicazioni coinvolte
- Hosting del sistema
- Business continuity
- Vincoli di legge

Sicurezza end-to-end



Futuro

- Problemi relativamente nuovi

- Di cosa abbiamo bisogno
  - Nuovi processi e modelli di lavoro
  - Nuovi algoritmi di cifratura
  - Nuove tecnologie

Grazie !!!

“Things should be made as simple as possible,
but no simpler”

Albert Einstein

Luciano Baresi

luciano.baresi@polimi.it