

Language-based Security



C. Bodei **P.Degano** G.L. Ferrari



Bet with **me**: I won't loose
against who ever you wish!



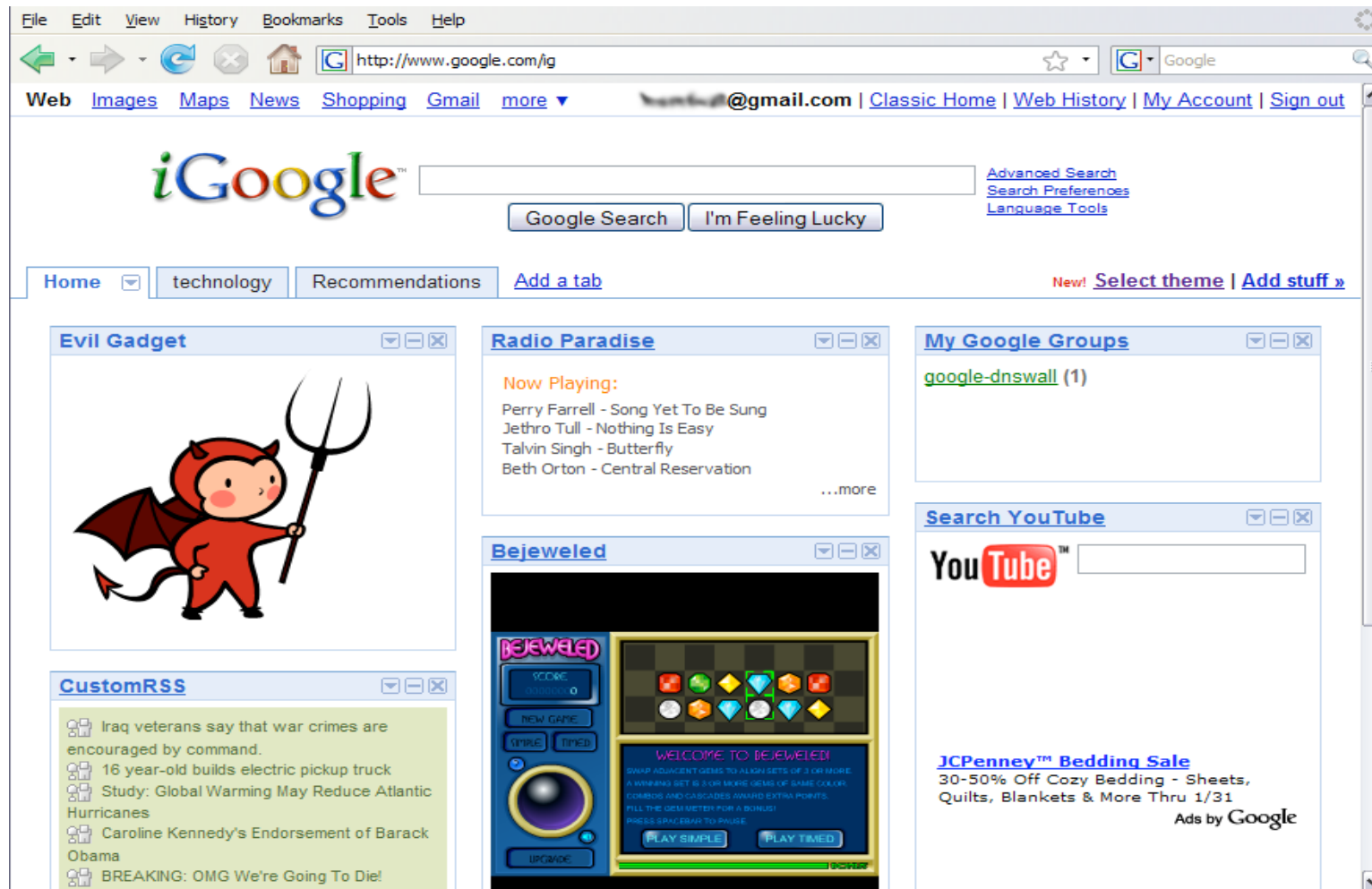


Bet with **me**: I won't loose
against who ever you wish!





Today Challenge: Mash-ups



Yesterday attack

LA STAMPA.it CRONACHE

TORINO - CUNEO - AOSTA - ASTI - NOVARA - VCO - VERCELLI - BIELLA - ALESSANDRIA - SAVONA - IMPERIA e SANR

ATTUALITÀ OPINIONI ECONOMIA SPORT TORINO CULTURA SPETTACOLI COSTUME MOTORI DONN
HOME POLITICA ESTERI CRONACHE TECNOLOGIA TUTTOGREEN LAZAMPA I TUOI DIRITTI DESI

Consiglia

90

Tweet

29

10

Indoona

Print

Email

Google

+

CRONACHE
15/09/2013

Alpitour, cyber-attacco via Facebook: false offerte per rubare dati agli utenti

Violato il profilo dell'azienda che ha subito avvertito i propri "fan". La situazione è già stata risolta, ma si tratta del primo tentativo di frode attraverso i social network

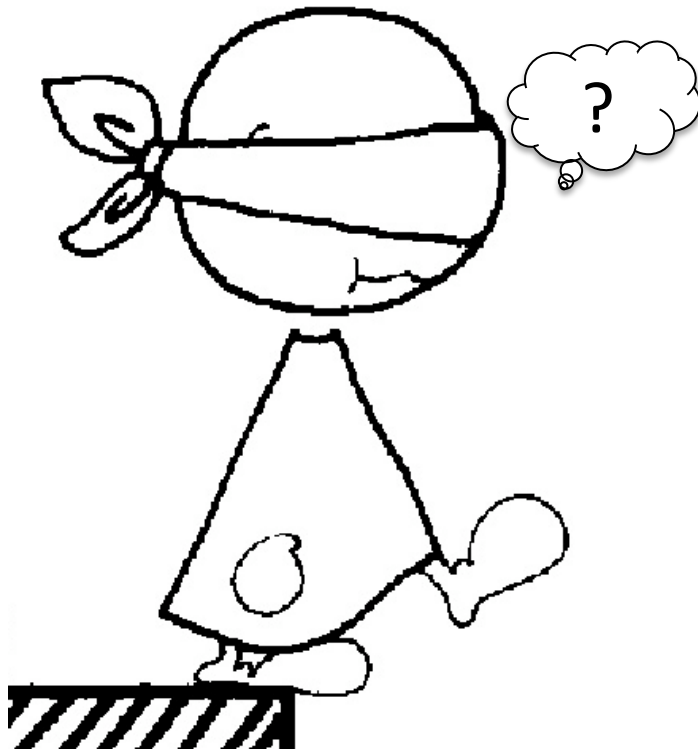
TORINO

Dopo Associated Press, Burger King, Dodge, New York Times, adesso è una grande azienda italiana a subire un attacco informatico attraverso un social network. Sono i primi casi al mondo, ma per gli esperti potrebbe essere solo l'inizio di un fenomeno che sempre di più potrebbe vedere coinvolta la criminalità organizzata.



Secure Web Applications

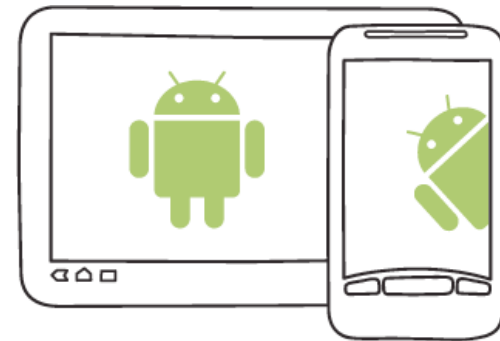
Challenge



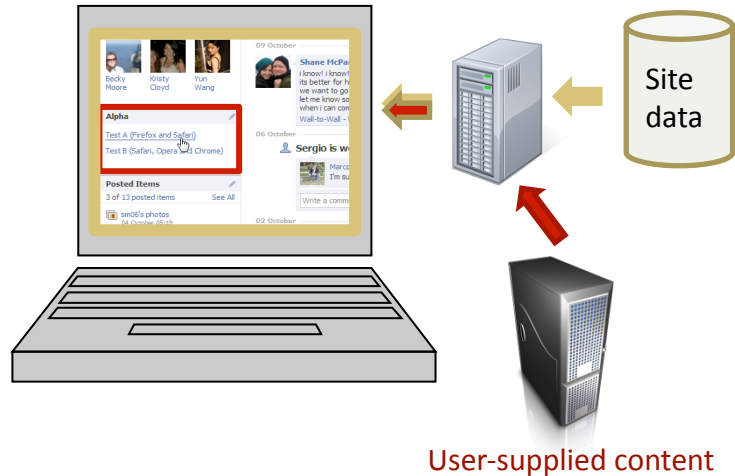
Decisions are usually trust-driven. Can we trust **code coming from the net**?

How can trusted and **untrusted code** be executed in the same environment, without compromising functionality or security?

a posteriori? too late ...



Our Approach at Work



- **Secure Web Mash-ups: code isolation**

- analyse the code to identify potential violations
- insert dynamic checks into programs to enforce isolation

- **Language-based security**

- Programming-language and compiler design techniques to enforce software security
- Analyse (statically) existing source-code
- Analyse object-code when source unavailable





Web Security

CHALLENGE: Web platform and application security are not based on precise model



Support trustworthy design
web applications
verify & repair methodology

SOME RESULTS (and TOOLS)

- CRYPTOGRAPHIC PROTOCOLS analysis (LySa protocol analyser)
- Secure ORCHESTRATION OF WEB SERVICES (Locust: planning orchestration)
- JAVA BASED MIDDLEWARE (Choreography Rehearsal: statically analysed)
- Checking USAGE POLICIES (Locust: model checking usages)
- JAVA EXTENSION: securing Java with local policies (New Java API)
- Checking CONTEXT DEPENDENT web applications (in progress)



GOALS

More theory + practice problems

Modelling a wider class of properties of web platforms

Guide the design of emerging feature

Analyse and prove correctness of accepted security policies

Improve the design of crucial components



Research Projects and Relations

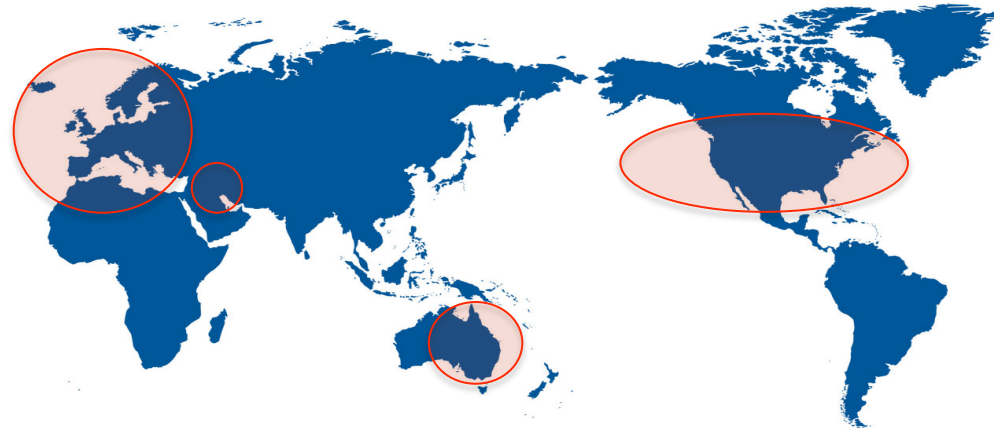
PRIN MEFISTO

LOMAPS EU-FST

SENSORIA EU-FST

PRIN SOFT

PRIN SECURITY HORIZONS



IFIP WORKING GROUP 1.7

W/S – Conferences: WITS, HotSpot,..., (FAST), **POST**