Ingegneria del Software e sicurezza

La Ricerca Avanzata:

- ***I gruppi / laboratori di ricerca***
- ***Il dottorato di ricerca***
- ***Le opportunità dei progetti europei***

Luca Viganò

Dipartimento di Informatica, Università di Verona

Aula Gino Tessari, Mercoledì 25 Gennaio 2012, 16:30-19:10

I gruppi / laboratori di ricerca

Permanent staff directly involved:

- Prof.ssa Maria Paola Bonacina
- Prof.ssa Alessandra Di Pierro
- Prof. Roberto Giacobazzi
- Dr.ssa Isabella Mastroeni
- Prof. Roberto Segala
- Prof. Nicola Fausto Spoto
- Prof. Luca Viganò

Related permanent staff:

- Prof. Alberto Belussi
- Prof. Carlo Combi
- Dr. Matteo Cristani
- Dr. Alessandro Farinelli
- Prof. Andrea Masini
- Prof. Massimo Merro
- Dr.ssa Barbara Oliboni
- Dr. Ugo Solitro

- 8 research assistants
- 14 PhD students
- *n* graduate students

REGIS
research group in information security

Hundreds of papers published

REGIS
research group in information security

Laboratorio REGIS (Research Group in Information Security)

La ricerca svolta all'interno del laboratorio si occupa principalmente dello studio e sviluppo di metodologie formali (basate su modelli matematici precisi) per

- la specifica,
- l'analisi,
- Il testing,
- l'ottimizzazione,
- la certificazione,
- la robustezza e
- la sicurezza

di sistemi software complessi,quali

- security protocols,
- web services e
- architetetture orientate ai servizi.

regis.sci.univr.it

SPY Lab (Static Program analysis by Abstract Interpretation)

The lab is devoted to the design and development of automatic tools based on formal methods and abstract interpretation theory for

- program analysis,
- automatic program certification,
- system testing, and
- security analysis of software.

The following is a list of topics which are studied in this Lab:

- Semantics and abstract interpretation theory
- Semantics based program analysis
- Security analysis
- Program and system certification
- Model checking and program verification
- Programming environments
- Domain specific languages and tools

spy.sci.univr.it

Related Labs and research groups

- **K.Re.Art.I.:** Rappresentazione della conoscenza tramite tecniche di Intelligenza Artificiale
- **STARS**: Semistructured Temporal clinicAl GeogRaphical Systems
- Laboratorio di informatica

- **ESD**: Electronic Systems Design
- **NES**: Networked Embedded Systems

Presented later today

Il dottorato di ricerca

Il dottorato di ricerca è il III livello di studi universitari, dopo la laurea e la laurea specialistica/magistrale, a cui si accede per concorso e che mira alla formazione attraverso la ricerca.

- L'obiettivo del dottorato in Informatica è quello di formare persone con una profonda ed ampia conoscenza dell'informatica e con un'elevata capacità di apprendimento delle metodologie di ricerca avanzate.

- I dottori di ricerca dovranno essere capaci di affrontare un'esperienza lavorativa sia nel campo della ricerca pura e di base che nel campo della ricerca applicata e industriale.

- Gli obiettivi saranno raggiunti prevedendo per i dottorandi una adeguata attività di istruzione e la redazione di una tesi di dottorato conforme ai più elevati standard internazionali.

- Collaborazioni industriali e internazionali.

- 3 anni
- Bando con scadenza 31 Agosto, concorso a Ottobre
- Posti con borsa di studio e senza borsa (Adr o altri finanziamenti)

Il dottorato di ricerca

Alcuni argomenti di ricerca:

- Algorithms
- **Artificial intelligence**
- Bioinformatics
- Bio-inspired and surgical robotics
- **Computer architectures and networks**
- Computer graphics
- **Computer science logic and formal methods**
- **Databases and information systems**
- Electronic systems design
- Embedded systems
- **Foundations of computing**
- Image processing and computer vision
- Medical imaging and visual perception
- **Programming languages**
- Quantum computing
- **Security**
- **Software engineering**
- Sound and music computing

Le opportunità dei progetti europei

Cosa sono i progetti EU ?

- **Progetti pluriennali finanziati (con M€) dalla Comunità Europea allo scopo di:**
  - rafforzare le basi scientifiche e tecnologiche delle industrie europee
  - incoraggiare la competitività internazionale promuovendo la ricerca nei più svariati settori

- **Possono partecipare:**
  - consorzi composti da università, industrie, organizzazioni internazionali e centri di ricerca con sede in Europa (ma non solo)

- **Il finanziamento avviene in seguito a una selezione altamente competitiva**
  - durante la quale i progetti presentati vengono valutati secondo standard di qualità scientifica, sostenibilità della proposta e impatto dei risultati del progetto sulla società

A cosa servono i progetti EU ?

- **Le risposte di domani cominciano oggi...**
- **… nell'ambito specifico della ICT portano vantaggi**
  - *per il cittadino:*
    - migliorie su un'ampia gamma di applicazioni tra cui
      - fornitura di servizi sanitari;
      - sistemi di trasporto;
      - sistemi interattivi innovativi di intrattenimento e apprendimento;
      - ...
  - *per il ricercatore:*
    - le attività di ricerca nel settore ICT si concentrano su priorità strategiche in settori industriali e tecnologici in cui l'Europa eccelle
  - *per le industrie:*
    - sviluppo accelerato dei prodotti;
    - riduzione di costi e spese generali;
    - transazioni più veloci e più attendibili;
    - migliori relazioni con i clienti e i fornitori;
    - livelli più alti di servizio e supporto clienti;
    - ...

Vantaggi per gli studenti ?

- **Vantaggi indiretti:**
  - Formazione continua dei docenti coinvolti e rinnovabilità dei corsi offerti.
  - Attività didattica supportata da sperimentazioni / tool legati ai progetti.

- **Vantaggi diretti:**
  - Possibilità di lavorare nell'ambito dei progetti EU come:
    - stage / tesi / erasmus
    - attività retribuita
  - sperimentando con mano cosa significa:
    - lavorare in gruppo / in collaborazione con le industrie
    - lavorare in condizioni di stress legato al rispetto delle promesse / deadline
  - con la possibilità di partecipare a:
    - meeting di progetto
    - conferenze e meeting internazionali

Come si usano i fondi ?

	SI	NO
Acquistare attrezzature per migliorare la ricerca e la didattica nei laboratori	✓	
Pagare assegni di ricerca per neo laureati/neo dottorati interessati a seguire un percorso "vocazionale"	✓	
Pagare borse di dottorato	✓	
Pagare borse di ricerca (a studenti che lavorano in attività a supporto della ricerca)	✓	
Sostenere la partecipazione a conferenze/scuole internazionali per la formazione di docenti e collaboratori alla ricerca	✓	
Sostenere la nascita di spin-off universitarie	✓	
Arricchire i professori		✗

Solo progetti EU ?

- **Esistono numerose tipologie di progetti europei e non, a cui si applica comunque quanto scritto nelle slide precedenti**

- **La partecipazione a progetti complessi permette agli studenti del CV in "Ingegneria del Software e Sicurezza" di confrontarsi:**
  - all'interno di team ben organizzati
  - pesantemente coinvolti in ambiti di ricerca di base e applicata
  - legati a spin-off universitarie ideate per creare un ponte tra università e industria
  - in un contesto internazionale
  - per lavorare su temi all'avanguardia
  - permettendo di iniziare un percorso alla scoperta della propria vocazione (ricerca, sviluppo, educazione, …) per il post-laurea

Due esempi di progetti EU

AVANTSSAR has developed the **AVANTSSAR Validation Platform**, a rigorous technology for the formal specification and Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures, which has been tuned on relevant industrial case studies.

01.01.2008 – 31.12.2010, budget 6M€ (3.8M€ EU)

SPaCIoS aims to develop the SPaCIoS Tool, which combines state-of-the-art technologies for penetration testing, security testing, model checking and automatic learning, which shall be applied proof of concept on a set of security testing problem cases drawn from industrial and open-source IoS application scenarios.

01.01.2010 – 30.09.2013, budget 6M€ (3.8M€ EU)

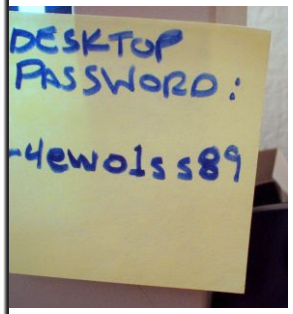
Accesso a servizi Internet (protetti)... qualche statistica

- L'utente tipico ha bisogno di almeno **9 password**
- **Uomini:** password salvate su **carta** o **PC**
- **Donne:** usano **nomi familiari**
- 30% **non cambiano mai password**, 29% meno di una volta all'anno
- 35% usano la stessa password per diverse applicazioni
- 60% ruotano 2 password tra tutte le loro applicazioni
- 70% hanno **dimenticato una password** almeno una volta

Accesso
qualche

- L'utente
- **Uomini:**
- **Donne:**
- 30% **non**
  29% me
- 35% usa
  applicaz
- 60% ruo
  applicaz
- 70% har
  una volta

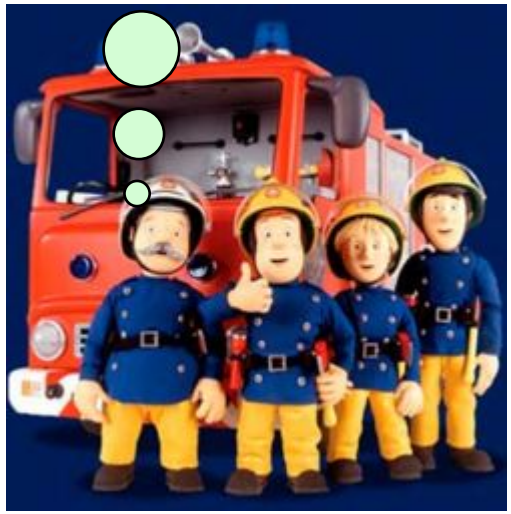
word



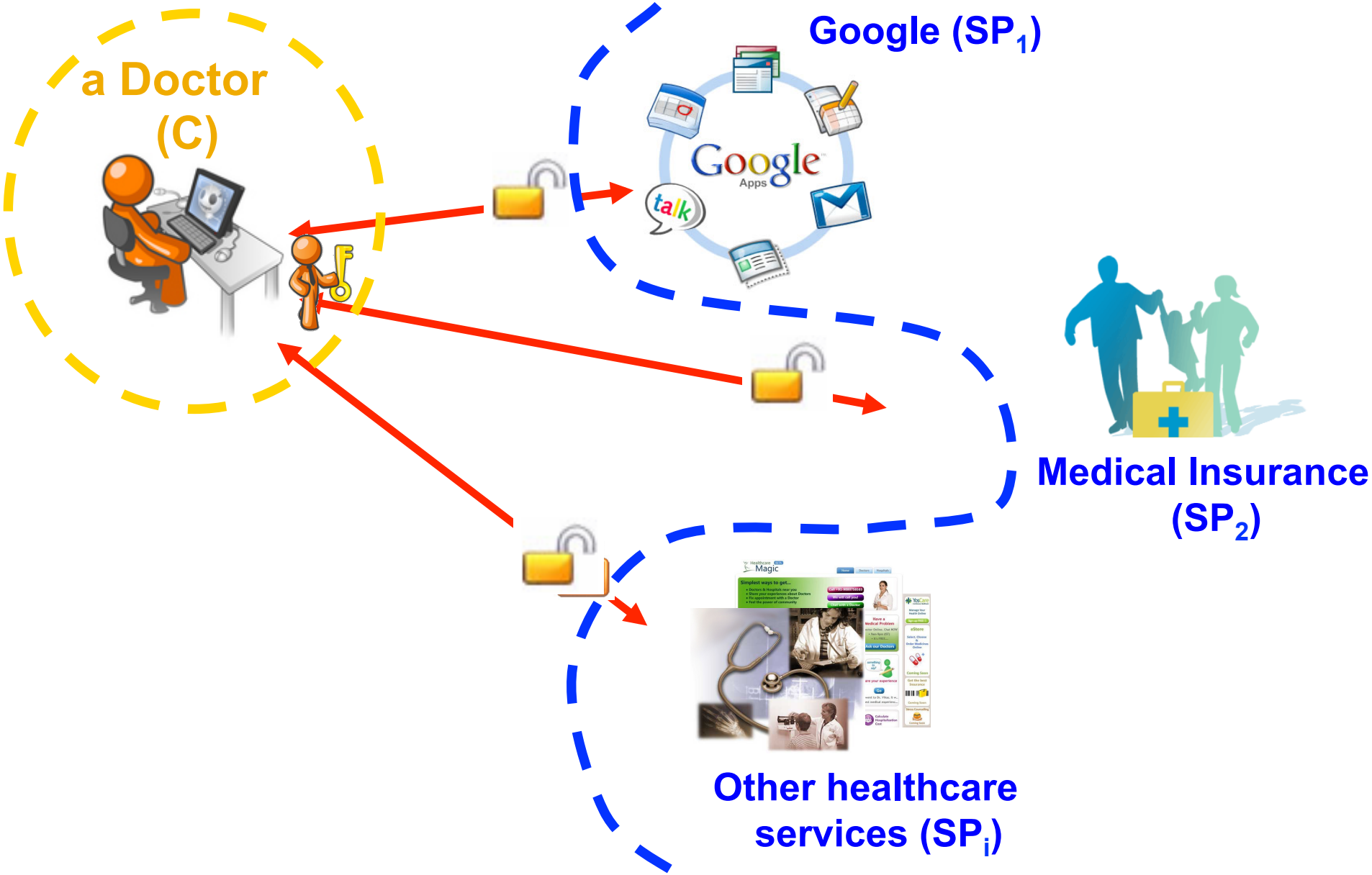
eno

Accesso a servizi Internet (protetti)...

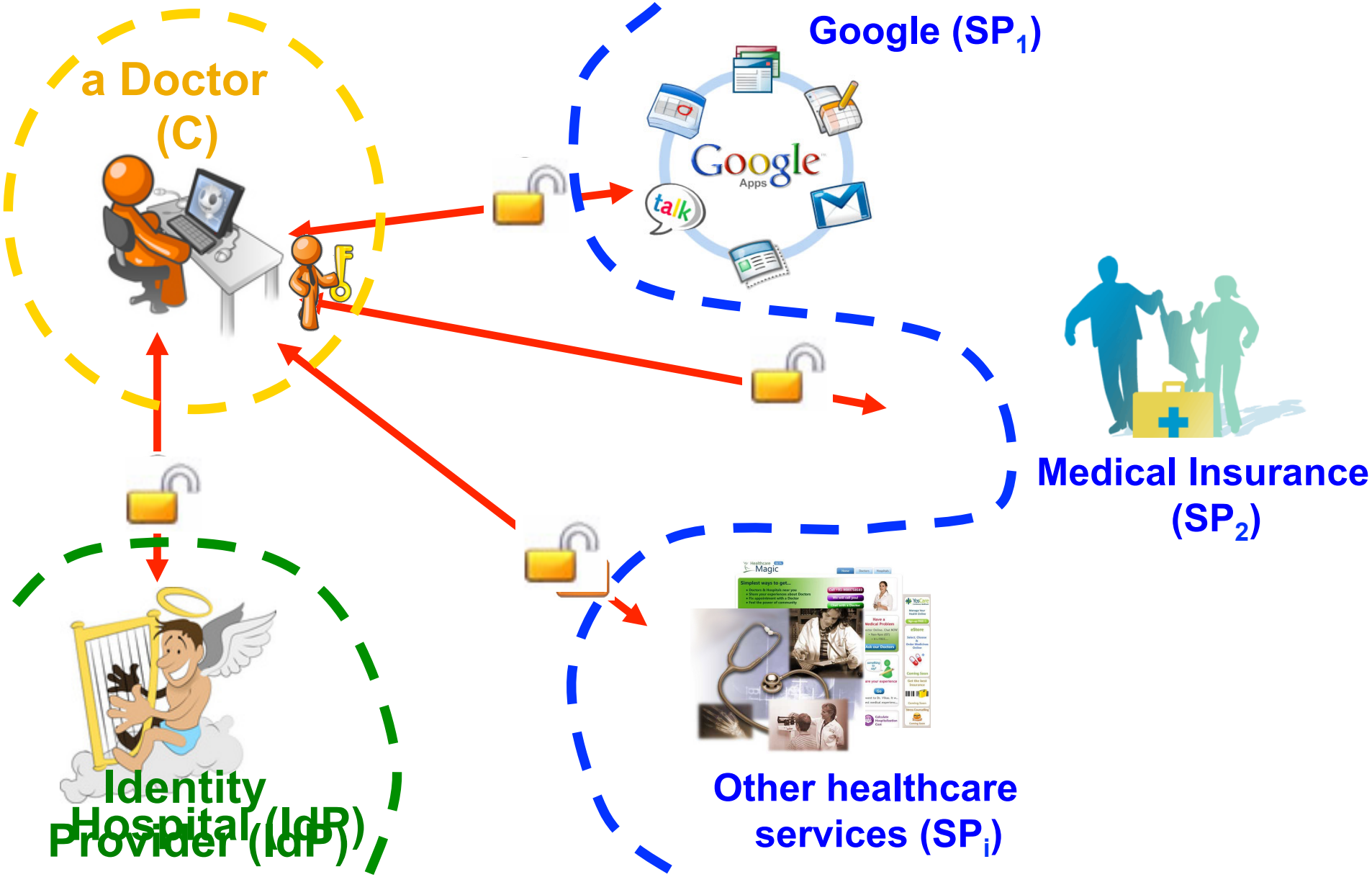
SSO:
Single Sign-On



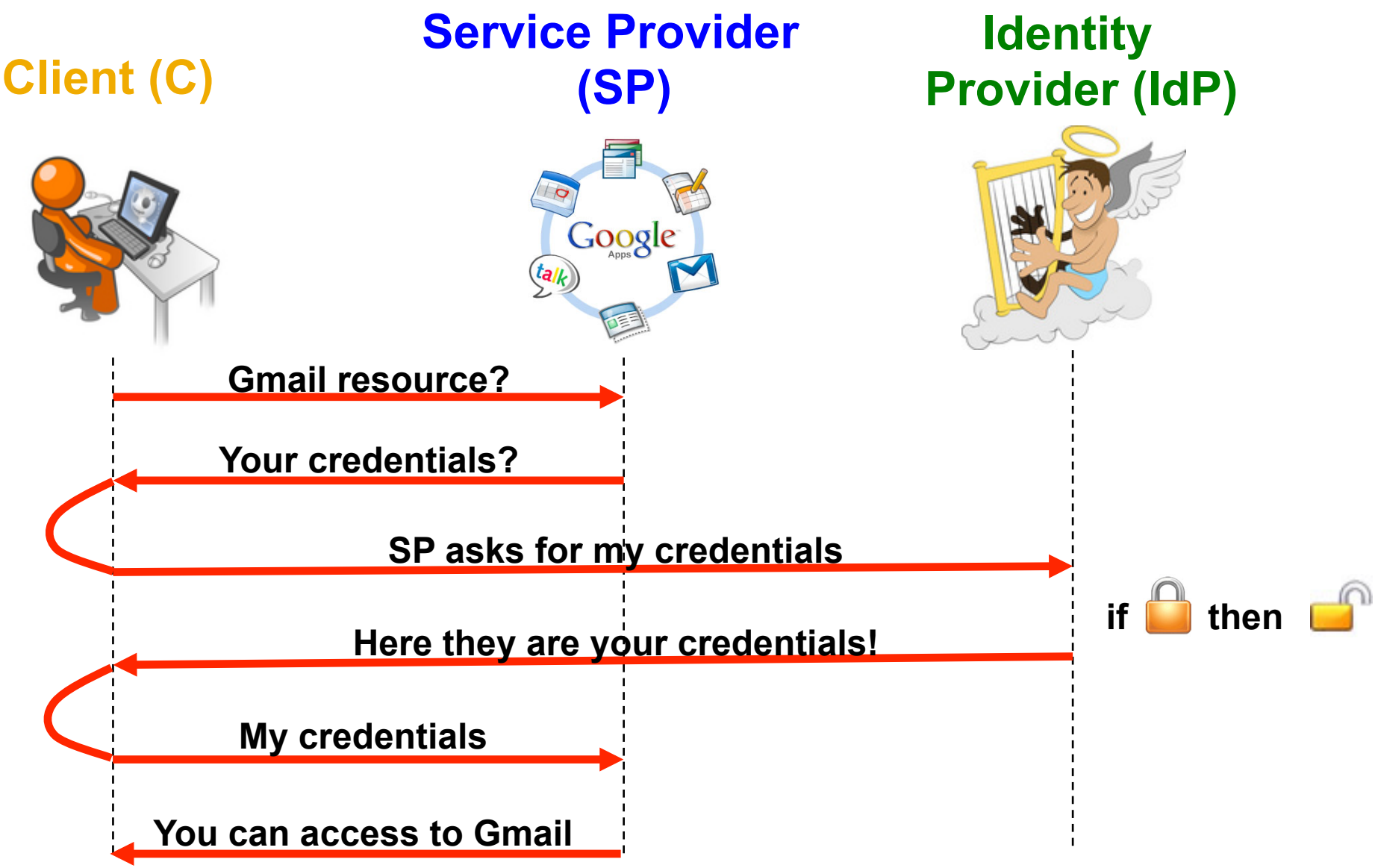
SSO: invece di aprire diversi lucchetti...



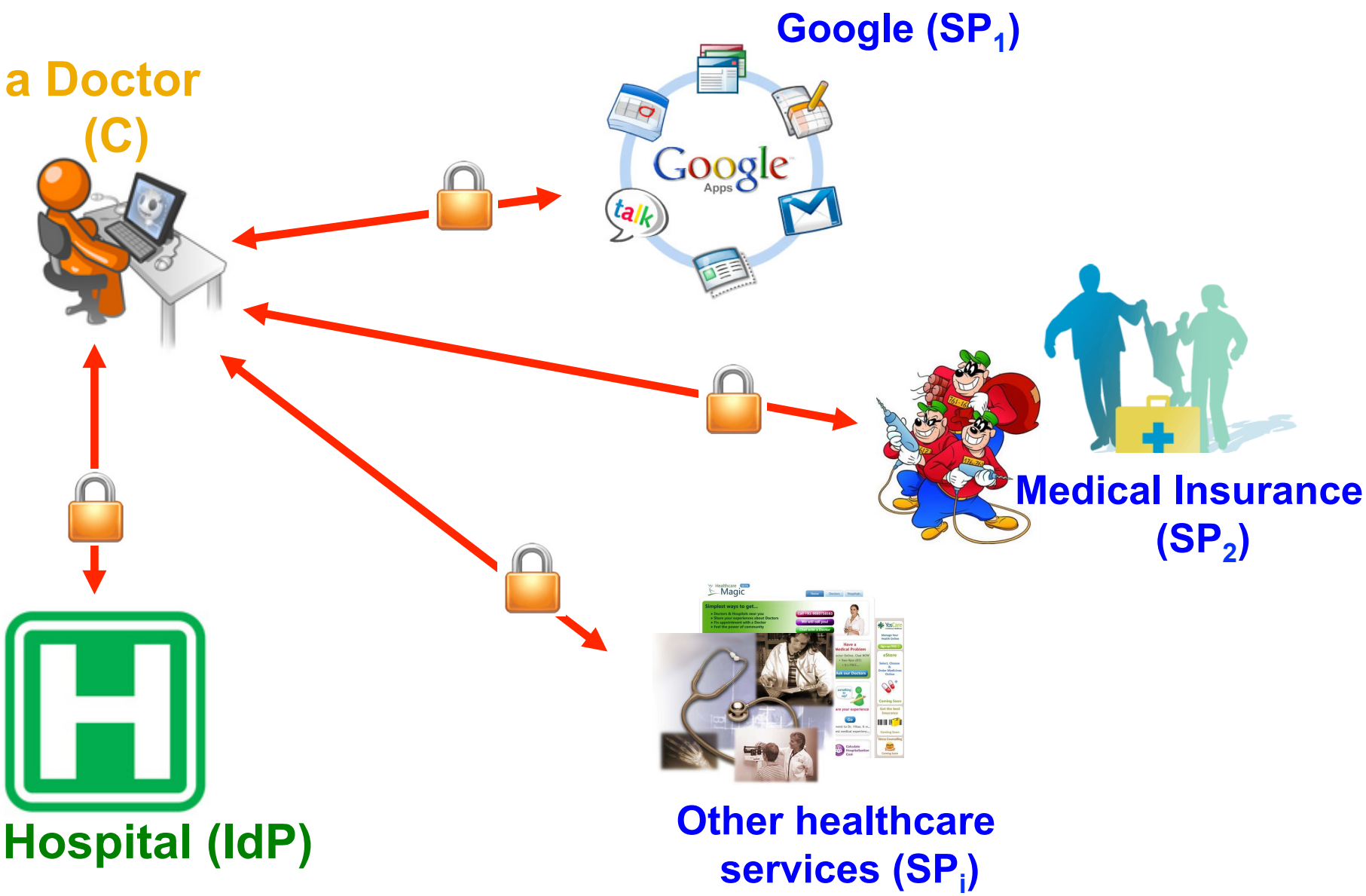
SSO: …apri un unico lucchetto



SSO: come

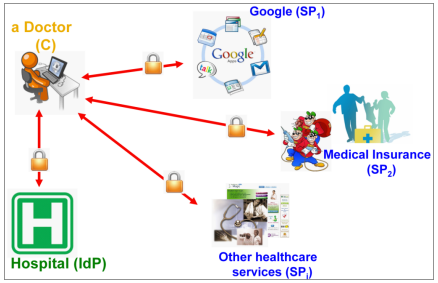

Client (C)
Service Provider (SP)
Identity Provider (IdP)
Google
Apps
talk
Gmail resource?
Your credentials?
SP asks for my credentials
if
then
Here they are your credentials!
My credentials
You can access to Gmail

SAML-based SSO for Google Apps: caso d'uso



Scoperta di una grave vulnerabilità

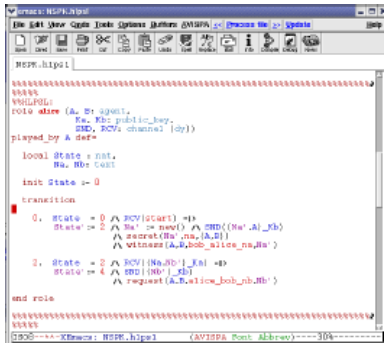
Real world



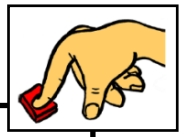
Abstract/Formal world

abstraction

formalization



input

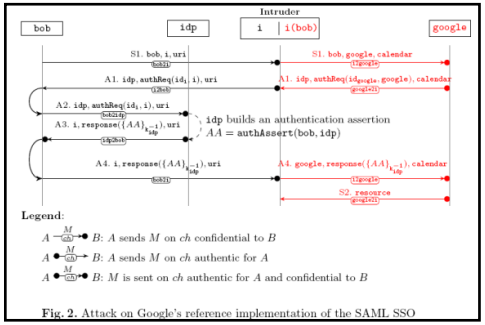


AVANTSSAR Platform

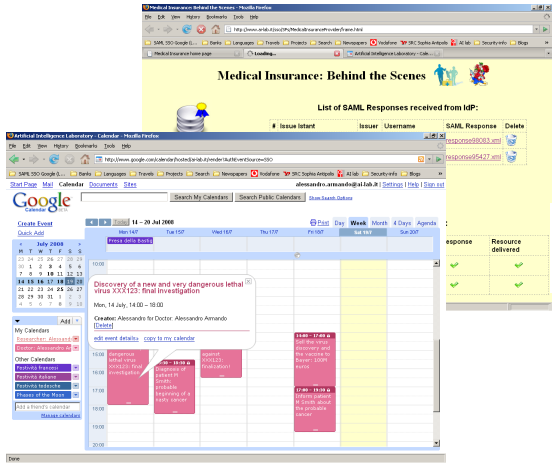
either

attack

no attack discovered



attack reproduction



Scoperta di una grave vulnerabilità

Real world : **Abstract/Formal**

Vulnerabilità astratta scoperta con le tecniche di ragionamento automatico della piattaforma AVANTSSAR

Attacco testato manualmente… è possibile automatizzarne la scoperta?

E non è l'unico attacco…

SPaCIoS

combinazione di tecniche di ragionamento automatico e testing per scoprire e testare attacchi in maniera completamente automatica

Fig. 2. Attack on Google's reference implementation of the SAML SSO