



consorzio nazionale
interuniversitario
per le telecomunicazioni

INCONTRO RINA/D'APPOLONIA-CNIT

TEMA 4: Security, inclusa Cybersecurity

Franco Davoli

franco.davoli@cnit.it

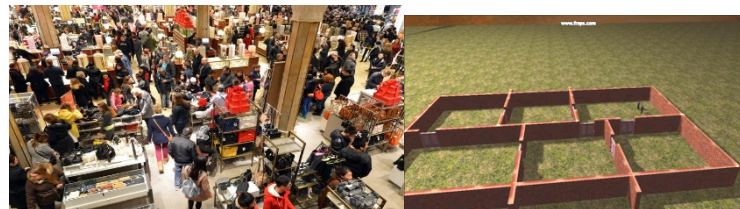
**UdR CNIT di Genova e Laboratorio Nazionale CNIT di
*Smart, Sustainable and Secure Internet Technologies and
Infrastructures, Genova***

Progetti europei (ARTEMIS) e
progetti con aziende
(Telecom, SelexES, ...)

- Sistemi dinamici cognitivi
- Elaborazione di segnali multi-sensoriali per sorveglianza
- *Software e Cognitive Radio*
- Valutazione Bayesiana di oggetti e situazioni (*Bayesian Object and Situation Assessment*)
- Ambienti interattivi e cognitivi

Cognitive Dynamic Systems

Cognitive crowd analysis



Bayesian Object and Situation assessment

Activity Recognition and Abnormality Detection In Safety and Surveillance

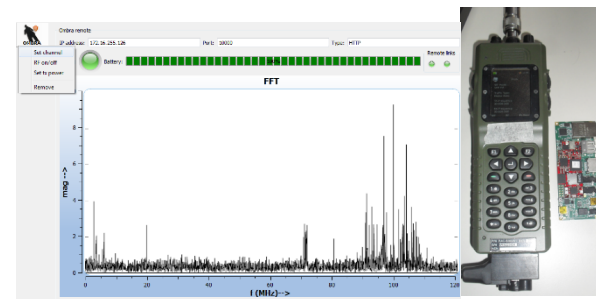
Applications



Routine behaviours
can be defined by
domain experts,
simulation or learned
from data

Software and Cognitive Radio

Spectrum Intelligence for jamming mitigation

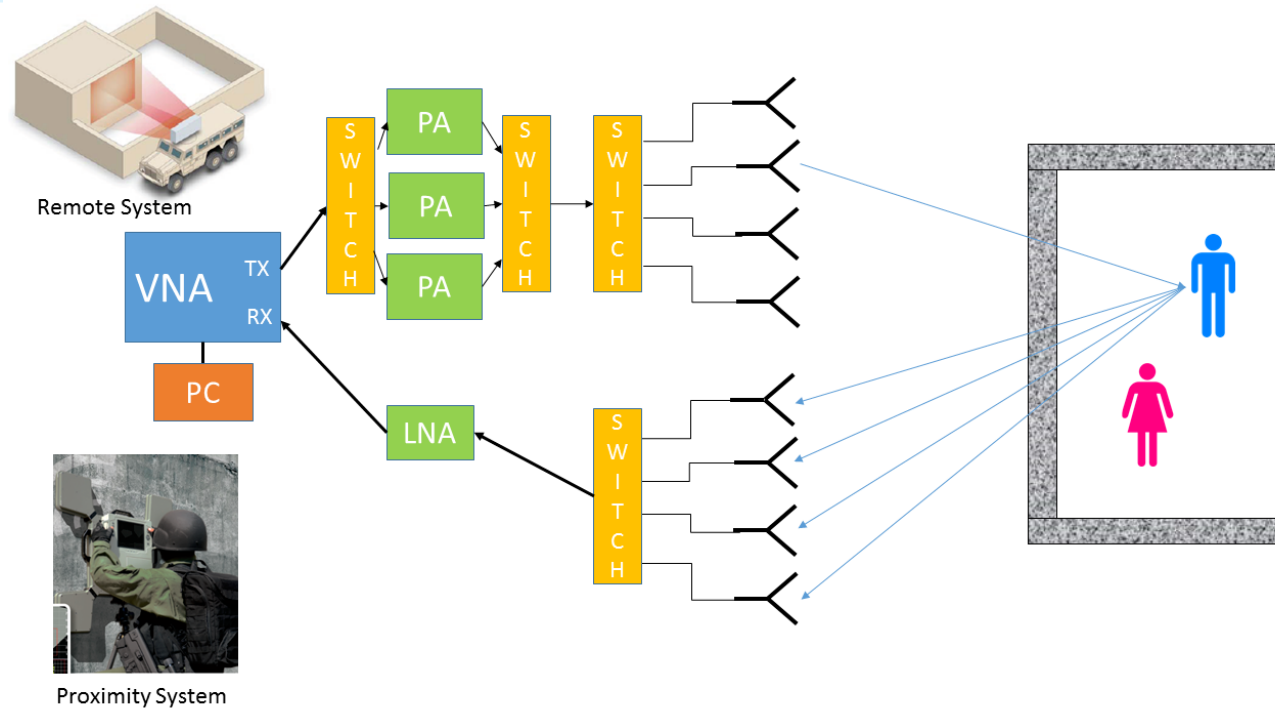


Text Mining e Semantic Analysis per Cyber Intelligence

- Metodi per *Preventive Cyber Security*
- *Early threat detection* da *Open Sources*
- Tecnologie di *Text Mining* per *Open Source INTelligence* (OSINT)
- Tecnologie di *Sentiment Analysis* per *profiling*
- Tecnologie di *Intelligence* da fonti *Social* (S/N e *blog*)

Collaborazioni con Aziende e Forze dell'Ordine

Attività: sviluppo di sistemi elettromagnetici innovativi di tipo *through-the-wall radar imaging*



Progetti attivi: Progetto PRIN 2015 (UniGE, UniCAL, UniRoma3, UniRoma1)

”U-VIEW (Ultra-wideband Virtual Imaging Extra Wall for high-penetration high quality imagery of enclosed structures)”

Physical-layer Security

Cos'è la Physical-layer Security?

Un insieme di meccanismi che sfruttano le proprietà del livello fisico per rendere più difficoltoso un attacco

Noise-Loop Modulation

Cos'è la Noise-Loop Modulation?

Lo sfruttamento della casualità intrinseca ai canali rumorosi per fornire un ulteriore livello di protezione

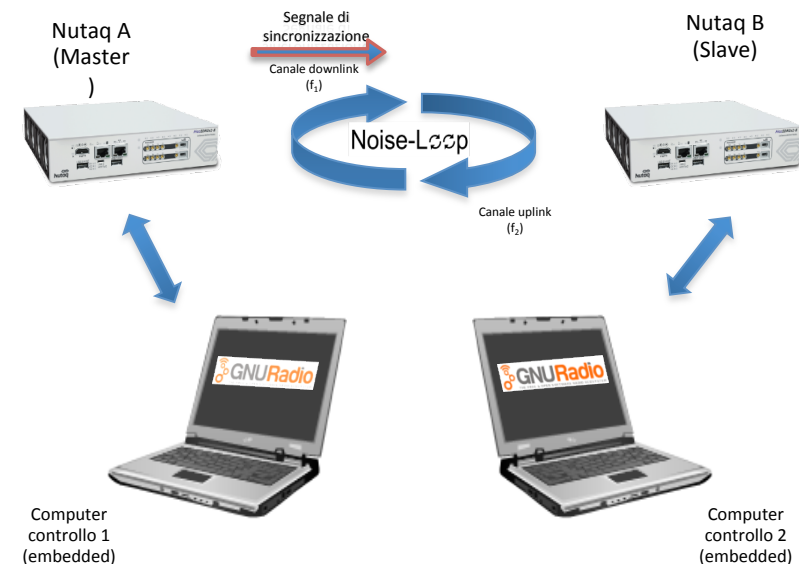
Cos'è il quid novi di questo metodo?

L'informazione di entrambe le sorgenti è contemporaneamente modulata con rumore. La violazione del meccanismo è matematicamente impossibile

Progetti:

1. WiSEC, Ministero della Difesa, 2011-2016
2. iPhySec, sottoposto a ONRG (*Office of Naval Research Grant*), 2016
3. Progetto FIRB "Enhancing communication security by cross-layer physical and data-link techniques"

- *Noise-Loop Modulation*
- *Physical layer security* per sistemi *wireless*, con particolare esperienza per la generazione di chiavi e l'autenticazione



Il sistema è stato realizzato e tutte le caratteristiche teoriche sono state dimostrate

Cifratura biometrica (*Biometric encryption*)

- Estrazione di un «segno» dal corpo (impronta digitale, retina, voce, DNA, ecc.)
- Il segno è elaborato numericamente e se ne estrae una chiave di cifratura
- La chiave può essere applicata per:
 - Cifratura (Forte)
 - Autenticazione (del corpo)



Multimedia forensics

- Il dispositivo di acquisizione lascia tracce specifiche nelle immagini e nel video, dovute alle sue caratteristiche intrinseche
- Tali tracce possono essere studiate per capire se un contenuto visuale è stato manipolato, e per identificare il dispositivo che lo ha generato



Progetti: FENCE, DARPA, 2014-2018

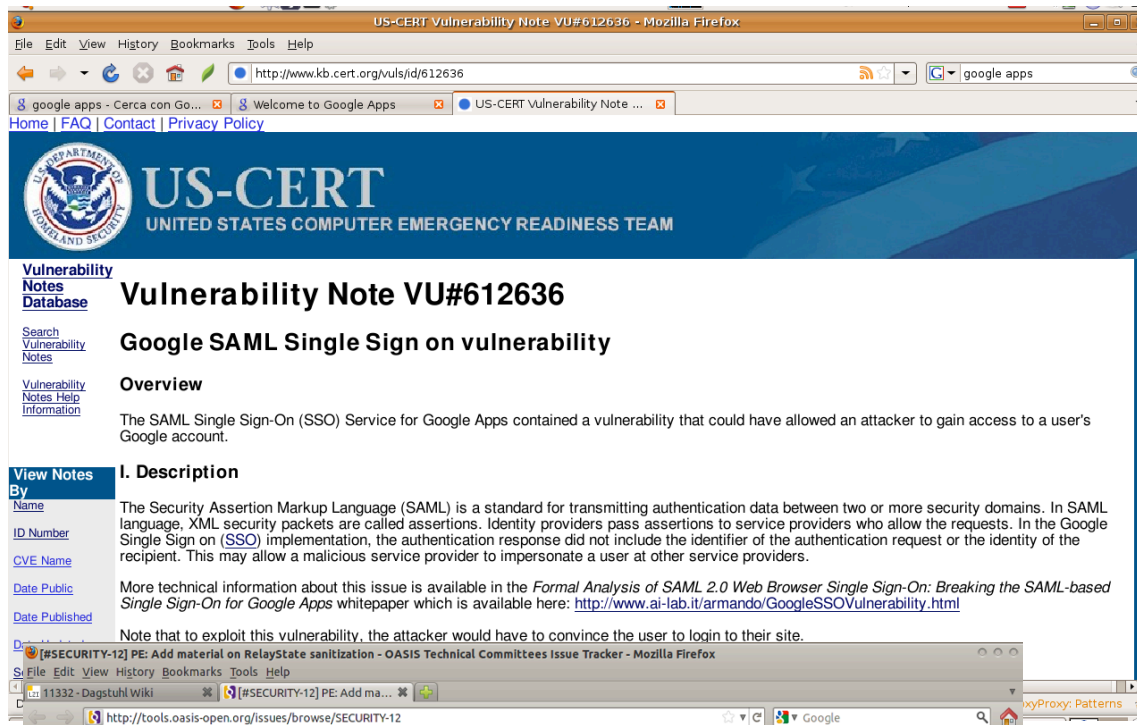
Proposte progettuali: Biologin, H2020 FET, Sept. 2016

Sviluppo di tecniche e strumenti automatici per l'analisi dei sistemi “security-critical”

- Storie di Successo: identificate vulnerabilità in
 - Single Sing-On for Google Apps
 - *Man-in-the-middle attack* nel protocollo di autenticazione usato da Google per il SSO delle Google Apps (utilizzato da 5ML di aziende nel mondo).
 - SAML Single Sign-On v.2.0 standard
 - Identificata violazione alla proprietà fondamentale dello standard SAML per il SSO.
 - La scoperta ha indotto OASIS a pubblicare Errata Corrige.
 - Android OS
 - Identificata vulnerabilità in Android che consente di realizzare un “fork-bomb attack” sui dispositivi.
 - Se sfruttato da malintenzionati avrebbe potuto portare ad attacco di *Denial-of-Service* su vasta scala. *Patch* proposta introdotta nelle ultime versioni di Android.
 - *Protocol for Strong Authentication (multi-factor and multi-channel)*
 - Modellazione formale e analisi della sicurezza di soluzioni per l'Autenticazione Forte
 - NATO High-Assurance Automated Guard
 - Obiettivo: condivisione di informazioni importanti per una missione NATO tra partner (inclusi civili, ad es. Croce Rossa) - Definito modello e linguaggio per il controllo degli accessi - Sviluppate prototipi per l'analisi delle politiche di autorizzazione e per la loro applicazione (*enforcement*)

Progetti

- European Industrial Doctorate on “Security & Trust of Next Generation of Enterprise Information Systems”, www.secentis.eu, in partnership with SAP, Marie-Curie Action
- Automated Validation of Trust and Security of Service-oriented Architectures (www.avanstssar.eu), FP7
- Security Horizons, PRIN Project, MIUR
- FilieraSicura: Cybersecurity for the supply Chain, funded by CISCO



US-CERT Vulnerability Note VU#612636 - Mozilla Firefox

http://www.kb.cert.org/vuls/id/612636

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

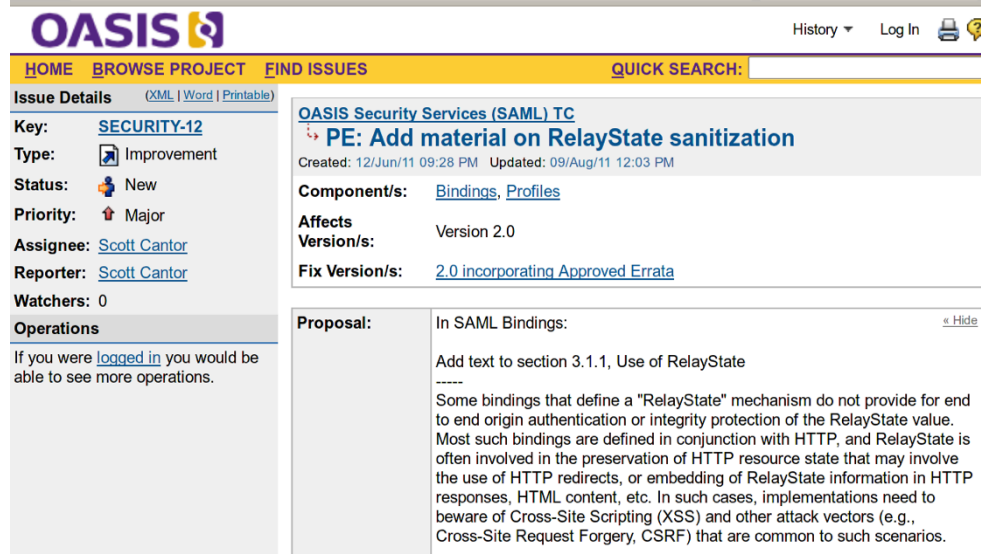
Vulnerability Note VU#612636
Google SAML Single Sign on vulnerability

Overview
The SAML Single Sign-On (SSO) Service for Google Apps contained a vulnerability that could have allowed an attacker to gain access to a user's Google account.

I. Description
The Security Assertion Markup Language (SAML) is a standard for transmitting authentication data between two or more security domains. In SAML language, XML security packets are called assertions. Identity providers pass assertions to service providers who allow the requests. In the Google Single Sign on (SSO) implementation, the authentication response did not include the identifier of the authentication request or the identity of the recipient. This may allow a malicious service provider to impersonate a user at other service providers.

More technical information about this issue is available in the *Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps* whitepaper which is available here: <http://www.ai-lab.it/armando/GoogleSSOVulnerability.html>

Note that to exploit this vulnerability, the attacker would have to convince the user to login to their site.



OASIS Security Services (SAML) TC

PE: Add material on RelayState sanitization

Created: 12/Jun/11 09:28 PM Updated: 09/Aug/11 12:03 PM

Component/s: [Bindings](#), [Profiles](#)

Affects Version/s: Version 2.0

Fix Version/s: [2.0 incorporating Approved Errata](#)

Proposal: In SAML Bindings:
Add text to section 3.1.1, Use of RelayState

Some bindings that define a "RelayState" mechanism do not provide for end to end origin authentication or integrity protection of the RelayState value. Most such bindings are defined in conjunction with HTTP, and RelayState is often involved in the preservation of HTTP resource state that may involve the use of HTTP redirects, or embedding of RelayState information in HTTP responses, HTML content, etc. In such cases, implementations need to beware of Cross-Site Scripting (XSS) and other attack vectors (e.g., Cross-Site Request Forgery, CSRF) that are common to such scenarios.



National Vulnerability Database (NVD) National Vulnerability database [CVE-2011-3918] - Google Chrome

web.nvd.nist.gov/view/viewDetail?detail=CVE:2011-3918

Sponsored by DHS National Cyber Security Division/US-CERT
NIST National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Mission and Overview
NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Vulnerability Summary for CVE-2011-3918
Original release date: 10/07/2012
Last revised: 10/08/2012
Source: US-CERT/NIST

Overview
The Zygote process in Android 4.0.3 and earlier accepts fork requests from processes with arbitrary UIDs, which allows remote attackers to cause a denial of service (reboot loop) via a crafted application.

Impact
CVSS Severity (version 2.0):
CVSS v2 Base Score: 7.8 (HIGH) (AV:N/AC:L/Au:N/C:N/I:N/A:C)

Resource Status
NVD contains:
55834 CVE Vulnerabilities
207 Last updated: Fri 24 Aug 12 21:54:14
2708 FDJ 2013 Vuln Notes
8140 CVE Publication
71375 CVE 1.3.23

Email List
NVD provides four mailing lists to the public. For information and subscription instructions please visit: [NVD Mailing Lists](#)

Workload Index
Vulnerability Workload

References to Advisories, Solutions, and Tools

Gestione dell'identità digitale: Scenario Mobile

Obiettivi:

- Nuove soluzioni per la gestione delle identità digitali (autenticazione-autorizzazione) sui dispositivi mobili
- Conformità alle normative sulla gestione dell'identità digitale (SPID, eIDAS) e sulla *privacy*
- Supporto di diversi livelli di autenticazione (autenticazione a più fattori)
- Implementazione di riferimento *open source*

Scenario e-Health cartella clinica del cittadino

Piattaforma di servizi che supporta **dottori e pazienti** nella gestione dei *Personal Health Records*

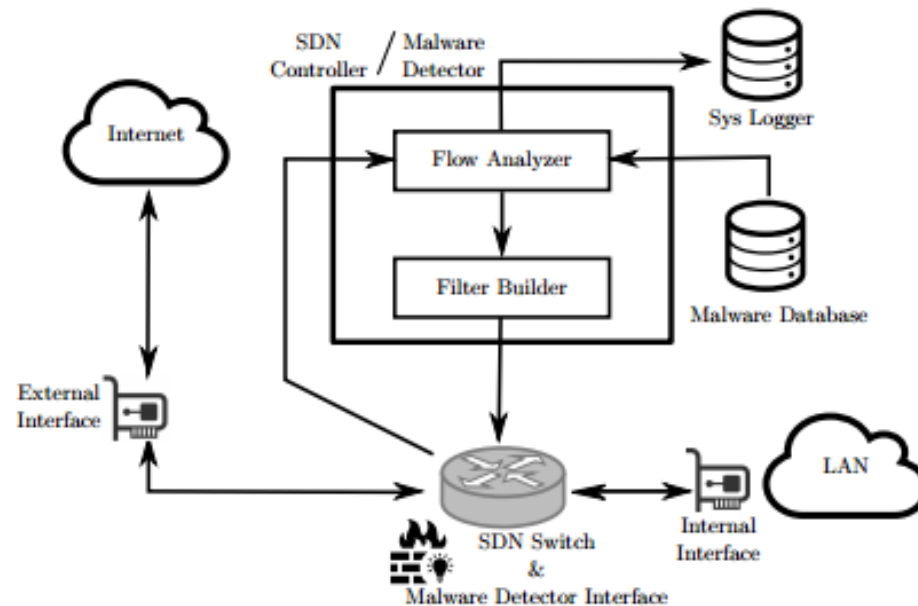
Soluzione innovativa che consente agli utenti di autorizzare in sicurezza *third party apps* ad accedere alla propria cartella clinica.

Sviluppo di una soluzione che garantisca:

- Autenticazione Forte dell'utente da piattaforma *mobile*
- Gestione dell'identità in rapporto con App sviluppate da terze parti
- Erogazione di un servizio di Single-Sign-On in ambito *mobile*

- Statistical Analysis Based Intrusion Detection Systems e SDN*

	Deep Packet Inspection MD	Statistical Analysis Based AD
Processing method	It examines the whole packet content, analysing data at application layer looking for signatures/rules	It opens packet headers (e.g. at the IP and TCP/UDP layers) to identify flows and examines traffic statistically
Complexity	High	Low
Speed	Slow	Fast
Limitations	It cannot detect new virus or encrypted flow	A training data set is involved



- Cyber Security, Business Continuity e Robustezza di Reti Elettriche*

Security monitoring / intrusion detection

- Tecnologie di sonde di rete
- Algoritmi per analisi traffico in *stream mode (real time, on the fly)* e per *complex event processing*
- Firme "comportamentali" per minacce multi-stage che superino i limiti delle firme tradizionali *rule-based*
- Applicazione a scenari avanzati di APT (*Advanced Persistent Threat*) e *lateral movement detection*
- *Deep Packet Inspection* (anche hardware).

Progetti EU FP7 PRISM, EU FP7 DEMONS, entrambi su tecnologie di monitoring.

Infrastrutture critiche (ICS) e sistemi SCADA

- Tecniche di monitoraggio adattate a sistemi e protocolli SCADA
- *Security information and event management* (SIEM) per correlazione eventi su infrastrutture critiche
- *Vulnerability assessment e penetration testing* per sistemi SCADA.

Progetto H2020-SCISSOR, *Security in Smart Grids*, Architettura di *security monitoring* per sistema SCADA della Società Energia Favignana (sull'isola).

Controllo di accesso Attribute Based (ABAC)

- Tecniche di controllo di accesso basate su attributi (piuttosto che su ruoli) – di forte interesse NIST dal 2013
- Integrazione con tecniche crittografiche (*Attribute Based Encryption*)
- Applicazione ABAC a scenari IoT

Progetto H2020-RECREED, su *access control e identity management* nella *call Digital Security*; progetto H2020-SYMBIOTE per la parte IoT

Altre attività

- *RFID security* e relativi attacchi (*wormhole attack* ai sistemi di pagamento *Near Field Communication* – NFC)
- Sicurezza in SDN
- Tecniche per la *privacy* e *business confidentiality*, tra cui tecniche crittografiche per *data sharing* e *secure multiparty computation* tra domini eterogenei.
- Sviluppo di protocolli per sicurezza ed integrazione di algoritmi proprietari in protocolli esistenti (integrazione di soluzioni proprietarie in *Transport Layer Security* – TLS).
- Sistemi di raccomandazione (ed in parte anche sistemi di reputazione)
- Ingegnerizzazione e programmazione di *malware* polimorfi
- Autenticazione per sistemi di navigazione satellitari
 - Progetto ESA su autenticazione per sistemi di navigazione satellitare globali (GNSS, Galileo); Attività per la Commissione Europea (collab. Quascom, GMV) su autenticazione SBAS (EGNOS); Progetto per ESA (collaborazione Quascom, CGI) su *key management* per GNSS

UdR CNIT coinvolte

- UdR di Genova e Laboratorio Nazionale CNIT di *Smart, Sustainable and Secure Internet Technologies and Infrastructures*, Genova
 - Prof. Franco Davoli, Prof. Alessandro Armando, Prof. Mario Marchese, Prof. Matteo Pastorino, Prof. Carlo Regazzoni, Prof. Rodolfo Zunino (nome.cognome@unige.it)
- UdR di Firenze
 - Prof. Enrico Del Re (enrico.delre@unifi.it), Dr. Lorenzo Mucchi (lorenzo.mucchi@unifi.it)
- UdR di Roma Tor Vergata
 - Prof. Giuseppe Bianchi (giuseppe.bianchi@uniroma2.it)
- UdR di Bari (collabora con Roma 2)
- UdR di Padova
 - Prof. Stefano Tomasin (tomasin@dei.unipd.it)
- UdR Università della Calabria
 - Prof. Sandra Costanzo (costanzo@deis.unical.it)
- UdR Roma3
 - Prof. Giuseppe Schettini (giuseppe.schettini@uniroma3.it)
- UdR Roma La Sapienza
 - Prof. Renato Cicchetti (cicchetti@diet.uniroma1.it)