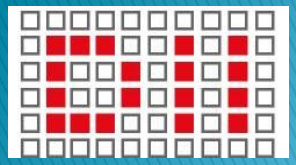
Attività del gruppo cyber security del DII – UnivPM

Marco Baldi

Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione

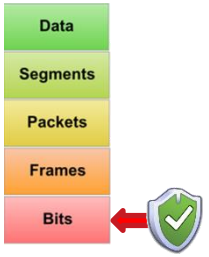


Ancona, 27 Aprile 2015

Sicurezza a tutti i livelli

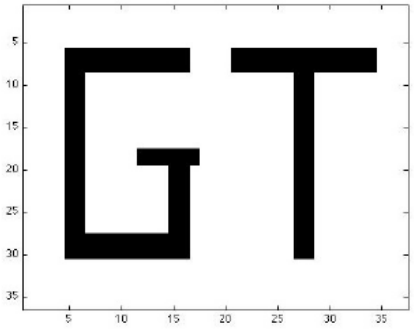
Data	**Application** Network Process to Application
Data	**Presentation** Data Representation and Encryption
Data	**Session** Interhost Communication
Segments	**Transport** End-to-End Connections and Reliability
Packets	**Network** Path Determination and IP (Logical Addressing)
Frames	**Data Link** MAC and LLC (Physical Addressing)
Bits	**Physical** Media, Signal, and Binary Transmission

PHY security

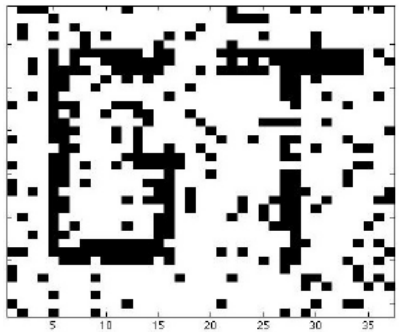


Basata sull'aleatorietà del **canale di trasmissione**

La rumorosità del canale, con opportune tecniche di codifica, aiuta ad **offuscare** l'informazione trasmessa

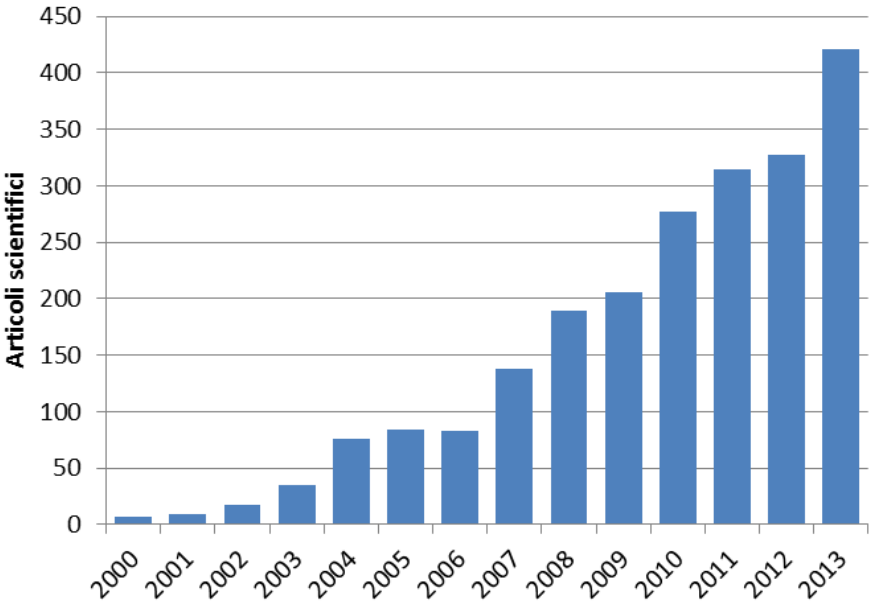


Original image



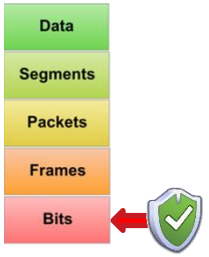
Messages transmitted

BER = 0.150



Tema di ricerca «caldo»

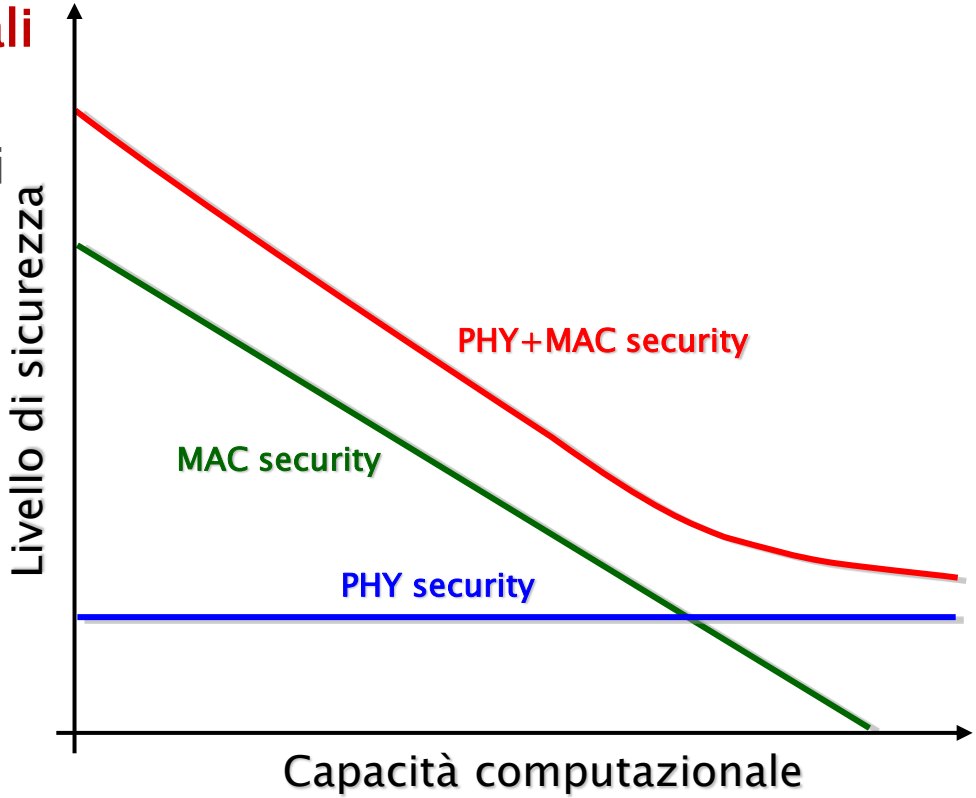
PHY security (2)



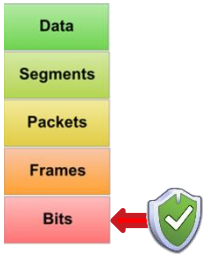
Importanti vantaggi:

- No **assunzioni computazionali** sugli attaccanti
- Base più solida per protocolli dei livelli più alti
- Eliminazione delle **chiavi precondivise**

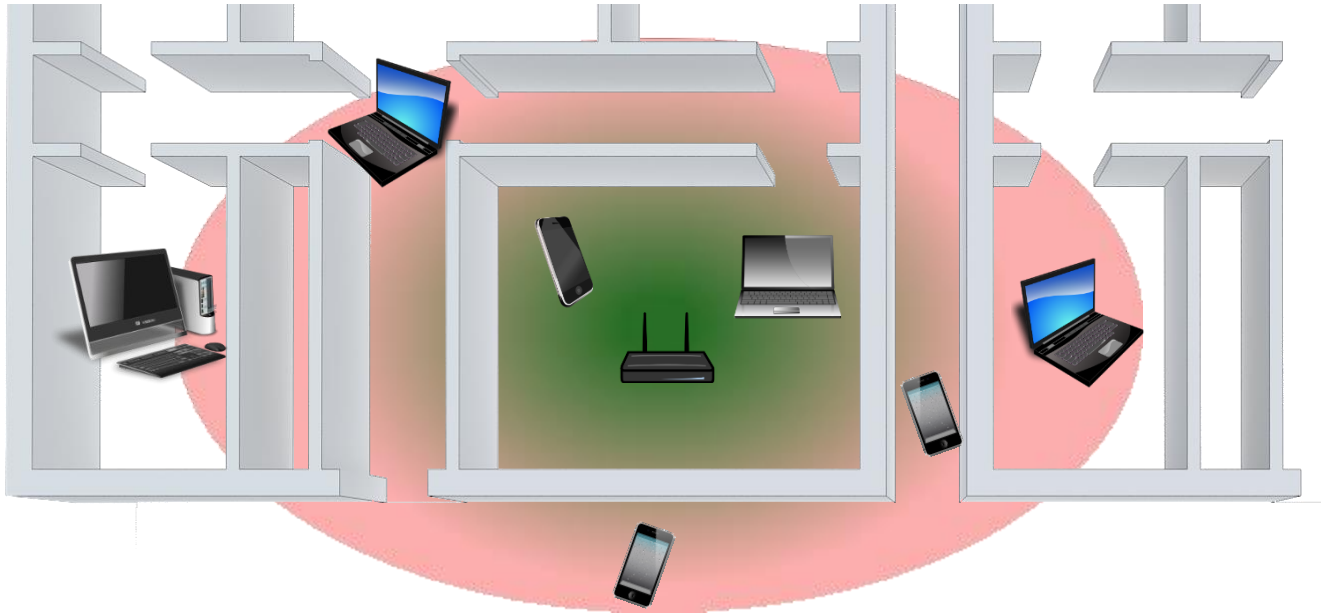
Va considerata come un supporto alla sicurezza computazionale



Scenario Applicativo



Reti wireless sicure senza **chiavi precondivise**



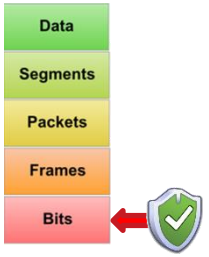
rete aperta

PHY security

Si può **generare una chiave** campionando il canale wireless

Oppure si può sfruttare la differenza di canale per realizzare un'**area sicura**

Attività @DII-UnivPM



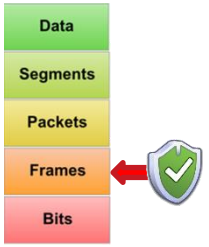
- Progetto di Ricerca **ESCAPADE** (tot. budget 426'500 €)
  (escapade.dii.univpm.it)

Presidenza del Consiglio dei Ministri
Ministero dell'Istruzione dell'Università e della Ricerca

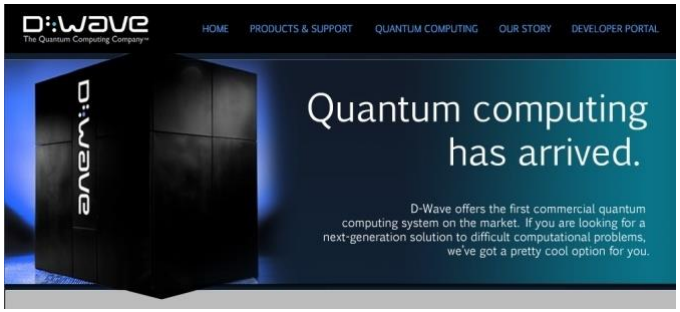
FUTURO IN RICERCA

- 15 pubblicazioni scientifiche recenti
- Organizzazione di workshop internazionali
  - Workshop on Communication Security (WCS 2014)
- Partecipazione a comitati tecnici di conferenze intern.
  - IEEE ICC 2015 Workshop on Wireless Physical Layer Security
  - Workshop on Wireless Communication Security at the Physical Layer (WiComSec-Phy 2015)

Crittografia post-quantica

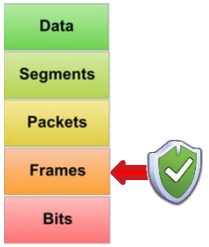


- I **computer quantistici** consentono di fattorizzare grandi numeri interi e calcolare logaritmi discreti in modo veloce
- **Romperanno** molti dei più diffusi sistemi di crittografia a chiave pubblica e firma digitale (**RSA**, **DSA**…)
- Minacceranno anche i sistemi basati su **curve ellittiche** (come **ECDSA**)



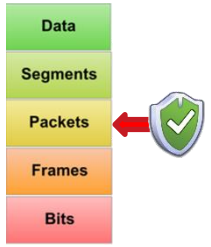
- Eventi recenti:
  - **Ottobre 2011**: primo centro accademico di quantum computing (Univ. South. California, Lockheed Martin e D-Wave Systems).
  - **Gennaio 2012**: D-Wave annuncia l'esistenza di un quantum computer a 84 qubits.
  - **2014**: alcuni documenti di Edward Snowden confermano l'esistenza del progetto "Penetrating Hard Targets" con cui NSA punta a sviluppare computer quantistici per scopi crittanalitici.

Attività @DII–UnivPM



- Definizione di **nuovi schemi crittografici** a chiave pubblica capaci di resistere ai computer quantistici
- Estensione a nuovi schemi di **firma digitale**
- 12 pubblicazioni scientifiche recenti
- 1 libro
- 2 brevetti
- Partecipazione al comitato tecnico di conferenze intern.
  - IMA Cryptography and Coding 2015
- Partecipazione ad azioni COST
  - COST Action IC1306 (Cryptography for Secure Digital Interaction)
  - COST Action IC1104 (WG3: “Crypto Aspects of Network Codes”)

Cifratura per Cloud Distribuiti



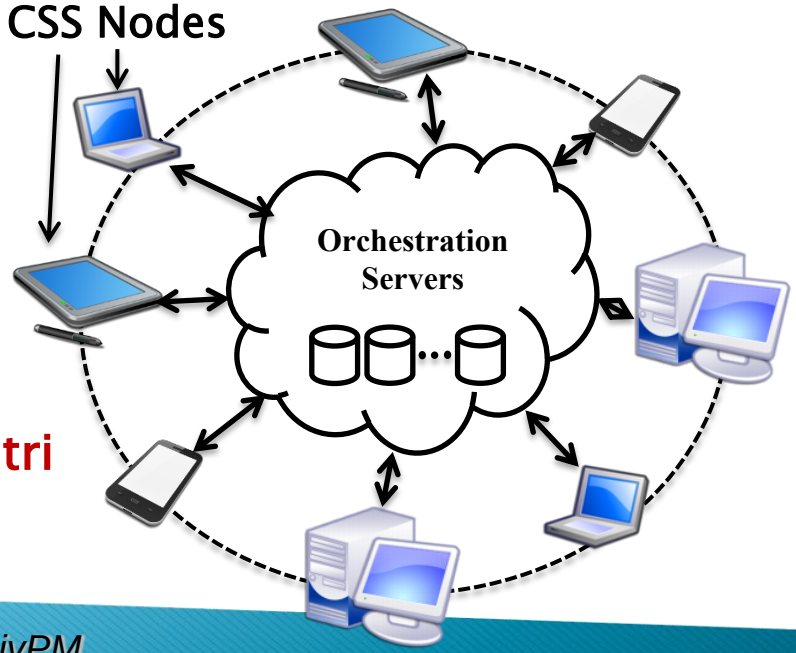
Distributed Storage Service (DSS)

- Il provider fornisce un gran numero di server
- All'aumentare del numero di utenti aumenta la necessità di server

Dropbox OneDrive iCloud

Cooperative Storage Service (CSS)

- Gli utenti **cooperano** mettendo a disposizione le proprie risorse (connettività e capacità di storage)
- Il provider fornisce soltanto **server di «orchestrazione»**, che coordinano la cooperazione



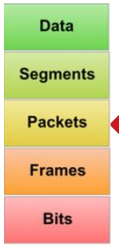
Vantaggi dei CSS

- Minori **costi** iniziali
- Infrastruttura **scalabile**
- "**Sostenibilità**" del sistema

Svantaggi dei CSS

- Ciascun utente memorizza **dati degli altri**

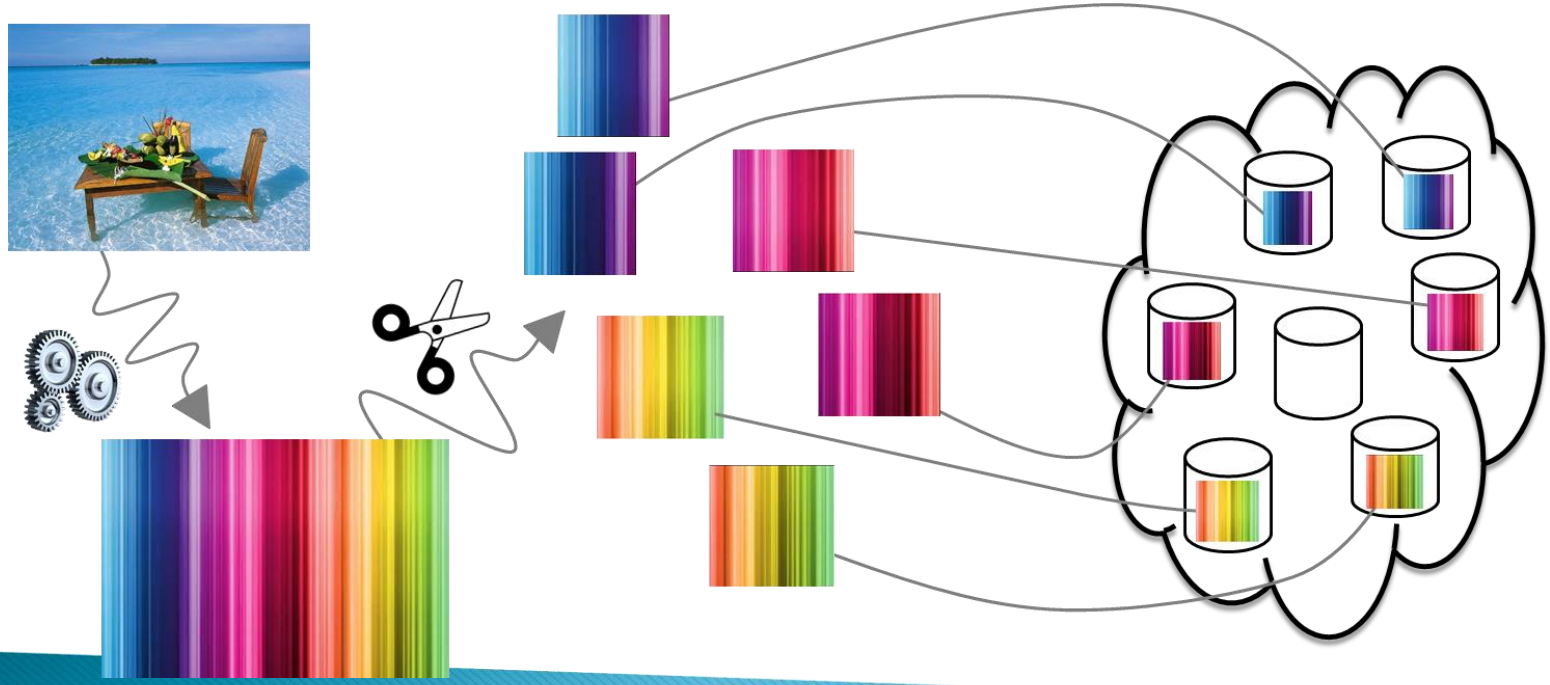
Cifratura per Cloud Distribuiti (2)



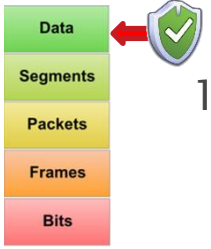
Servono due tipi di protezione:

- Protezione contro **perdite** di dati
- Protezione contro **furti** di dati

Soluzione innovativa: **codifica** + **dispersione** dei dati



Verifica Formale di Sicurezza



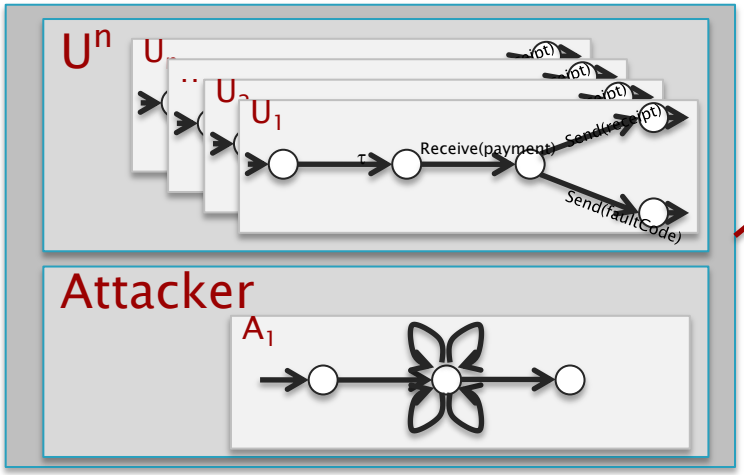
- **Difetti** di progettazione e realizzazione rendono i sistemi **vulnerabili**
- La **verifica dei requisiti** di sicurezza di un sistema favorisce la riduzione delle vulnerabilità
- Requisiti
  - Proprietà e Iperproprietà
- Modello del sistema
  - Linguaggio: BPMN o Timed Automata
  - Parametrizzato (numero arbitrario di istanze)
  - Modello dell'Attaccante

Attività @DII-UnivPM

Requisiti

$\forall\, i,j.\ \mathrm{AG}\ (x(i){:}\mathrm{searchResult}{=}\mathrm{success} \rightarrow \mathrm{AF}(y(j){:}\mathrm{Payment})$

Sistema



smc4ws

yes/no
counterexample

Risultati teorici, oltre 20 pubblicazioni scientifiche

Applicazioni

- Verificata sicurezza dei protocolli **SET** e **iKP**
- Trovati difetti ai protocolli **Kerberos** (inedito), **Lu&Smolka** (inedito) e al sistema di grid computing **Condor**

Gruppo cyber security @DII – UnivPM

Componenti

Marco Baldi
Franco Chiaraluce
Emanuele Frontoni
Luca Spalazzi
Primo Zingaretti
Francesco Spegni
Nicola Maturo
Giacomo Ricciutelli

Collaborazioni con Aziende

HTS HI-Tech Services SRL
Netcetera AG
Nautes S.p.A.
Computer Var ITT Srl
XAutomata Technology GmbH
Polizia di Stato
Fed. Ital. Medici di Medicina Generale
Federsanità ANCI
Fondazione Nuvola Sanitaria
Netmedica Italia

Collaborazioni con Università

University of Zurich
University of Padua
University of Trento
University of Rome La Sapienza
University of Dayton – Dayton, OH – USA
Wright State University – Dayton, OH – USA
Technische Universität Wien – Vienna – Austria
Alpen-Adria-Universität Klagenfurt – Klagenfurt – Austria
King's College London – UK
SRI International, Menlo Park, CA – USA
EPFL École polytechnique fédérale de Lausanne
ETH Zurich

Didattica e Sicurezza @DII-UnivPM