# Security Issues In DOSNs

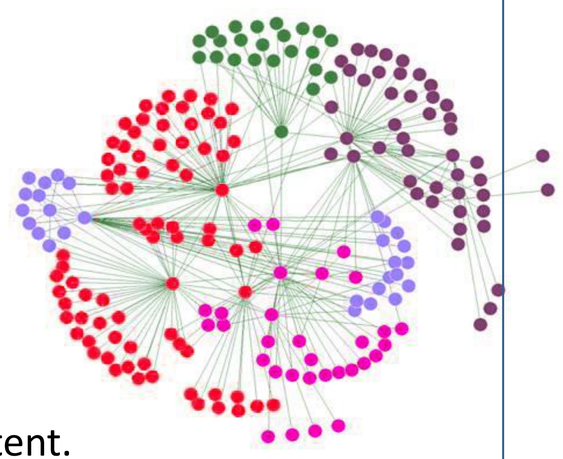
Panagiotis Ilia <e-mail:pilia@ics.forth.gr>

## Online Social Networks (OSNs)

OSNs → web-based services → *"killer applications"*

**Facebook**: Reached **1 billion** users in October 2012

Based on real-life relationships.



An OSN allows users to:

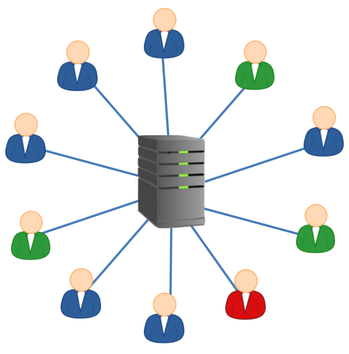
- Construct a public profile
- Create a list of connections
- View and traverse other lists.

Users **generate**, and **share** their content.

(upload and tag photos, comments, chat, messages etc.)

## Decentralised OSNs (DOSNs)

OSNs → centralised architecture → *"client - server"*

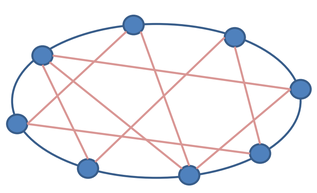


- Servers: Information silos
- Honest but curious providers
  Able to control user's data
- User's personal data is disclosed for revenue. Privacy breaches.
- User: Weak control over shared data

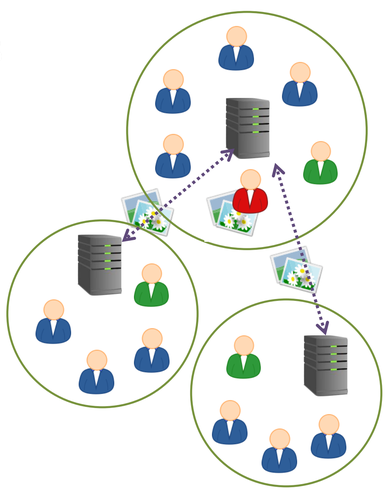
→ **A shift to Decentralised Architectures**

**Web-based or P2P overlay networks**

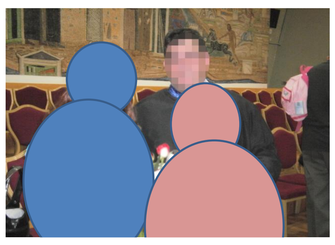
- Ownership of personal information
- Confidentiality and integrity guarantees
- Protection of privacy and IP



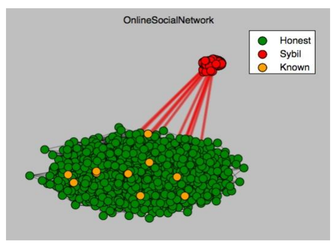
Scalability
Fault tolerance
High performance



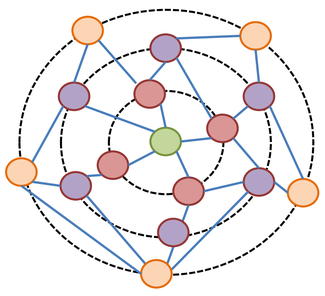
## Security Issues



- Privacy and access control.
  Especially in the case of conflicting interests.




- Sybil and Compromised nodes → Sybil attacks
- Man-In-The-Middle attacks
- Impersonation attacks



- Spam distribution
- Identification and prevention of malicious content **(malware)**
- Collaboration among the nodes

Guarantee continuous data availability

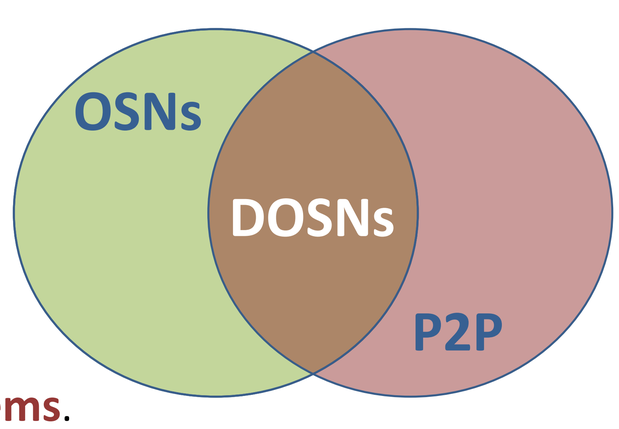
- Replication of profiles on trusted nodes
- Prevent DDoS on the centralised components
- Prevent DHT and routing poisoning

## Objectives

- Identify critical security issues in DOSN, by investigating reported security threats in non-decentralised OSNs.
- Identify security issues originating from decentralised networks. Focus on **malware and spam distribution**.
- By studying and investigating the DOSNs and the already deployed OSNs, new security threats can be detected.
- Perform real-world experiments and simulations to address the mentioned security threats.
- Analyse the experimental results, propose and adopt solutions for mitigating the threats.

## Security In DOSNs

- Suffer from most of the **security issues** of the **centralised OSNs**.
- Have the **vulnerabilities** and security problems of the **peer-to-peer systems**.




## Evaluation

- Setup controlled environments that simulates the operation and functionality of OSNs and DOSNs.
- Reproduce the OSNs' studied threats and apply them in DOSNs (or modify them to be applicable for DOSNs).
- Perform real-world experiments and simulations
  - Various setups, properties and parameters
  - Both for DOSNs and OSNs.

FORTH Foundation for Research & Technology - Hellas
MARIE CURIE ACTIONS
PEOPLE