



Security of Cloud Computing

Fabrizio Baiardi
f.baiardi@unipi.it



Syllabus

- Risk Assessment and Management
 - Cloud Computing Introduction
 - Definitions
 - Economic Reasons
 - Service Model
 - Deployment Model
 - Supporting Technologies
 - Virtualization Technology
 - Scalable Computing = Elasticity
 - Security
 - New Threat Model
 - New Attacks
 - Countermeasures
-



New threat model

- The cloud provider as a powerful attacker
- Physical security is no longer sufficient
- Service level agreement as a first countermeasure
 - Abundance of data but data must be available
 - Quantify as much as possible the SLA
 - Physical security is not your friend



New attacks

- Colocation (a new step to attack in a cloud)
- Side channel attacks
- The browser
 - Xss
 - Request forgery
 - SQL injection
- Availability also depends upon network connections
- Memory as a service : attacks and countermeasures



Countermeasures (new and old)

- Attestation
 - TPM
 - Static
 - Introspection
 - TPM
 - Dynamic
 - Bootstrap to minimize overhead
 - Encryption (to defend against the provider)
 - Omomorphic
 - Search on Encrypted data
 - Standard encryption to defend against standard attackers
-