



# Sicurezza in ambito storage

**C'è qualcosa di nuovo sotto il sole ?!**

---

Stefano Zanero  
**Ricercatore post-doc, Politecnico di  
Milano**

zanero@elet.polimi.it

**CTO & Cofounder, Secure Network  
S.r.l.**

s.zanero@securenetwork.it



## Back to basics

---

- ❑ “Tanto più complessa è la spiegazione, tanto meno funzionante è la soluzione proposta”
- ❑ Nella sicurezza informatica abbiamo un bisogno urgente di tornare alle regole fondamentali
  - ❑ Tutela della confidenzialità delle informazioni
  - ❑ Preservazione dell'integrità dei dati
  - ❑ Garanzia della disponibilità dei sistemi
- ❑ Esiste un problema di sicurezza nelle problematiche di storage ? **Certamente sì !**
- ❑ **Esiste un problema di “sicurezza dello storage” ?**

# Una visione olistica della sicurezza



- Case study: azienda di progettazione meccanica**
- Risk assessment**
  - Asset: disegni già pronti da integrare in progetti custom**
  - Risk: sottrazione dei disegni**
  - Countermeasure: controlli d'accesso ai fileserver**
- Sbagliato dalle fondamenta: il problema in questo caso è tutelarsi dal dipendente infedele!**
- Viene usato storage ?**
- Il problema è lo storage ?**
- Il problema viene risolto da una misura di sicurezza sullo storage ?**



# La sicurezza è fatta a strati...

---

- ❑ (non sarò esaustivo, ma...)
- ❑ **Sicurezza perimetrale**
  - ❑ Firewall, VPN, IDS, gateway AV etc.
- ❑ **Sicurezza degli endpoint**
  - ❑ Antivirus, patch management, policy enforcement
- ❑ **Sicurezza delle persone**
  - ❑ Identity and access management, fraud detection...
- ❑ **Sicurezza dei dati**
  - ❑ (ne parliamo dopo)
- ❑ **In cima a tutto: sistemi di security management**
- ❑ **Availability significa anche reliability; integrità significa anche resilienza ai**



# Intanto: che significa "storage"?

---

- ❑ **Si possono intendere tutti i sistemi e le architetture di salvataggio dati**
- ❑ **In genere si sottintende "tutte le tecnologie per immagazzinare dati:**
  - ❑ **In ambiente di rete**
  - ❑ **Con grandi volumi di dati**
  - ❑ **Con meccanismi di management/virtualizzazione**
- ❑ **Macroclassi di tecnologie**
  - ❑ **DAS**
  - ❑ **NAS**
  - ❑ **SAN**
- ❑ **File system distribuiti**
  - ❑ **NFS, SMB/CIFS, AFS, DFS...**

# Tecnologie di sicurezza di ieri e di oggi...



- ❑ Lock-down di sistemi usati come NAS
- ❑ Utilizzo di tecnologie di autenticazione di rete, a volte integrate con AD, RADIUS o Kerberos
  - ❑ Es. AFS ed NFSv4 supportano Kerberos
- ❑ Utilizzo di sistemi di ACL convergenti verso quelli Windows NT o verso sistemi POSIX
  - ❑ Relative problematiche di mapping
  - ❑ ... e di gestione !
- ❑ Protezione fisica dei dispositivi spesso assente, o delegata a un uso "superficiale" della crittografia
  - ❑ "Non-shared" crypto file systems, end-to-end encryption
  - ❑ Non proteggono contro "insider attacks"
- ❑ Uso della crittografia per proteggere i backup: un'arma a doppio taglio



# Sicurezza delle architetture SAN

---

## ❑ Fibre Channel

- ❑ Tipica misura di sicurezza: associa nodi a LUN accessibili
  - ❑ Peccato che i WWN dei nodi si possano spoofare...
  - ❑ Vale anche per LUN masking, purtroppo
  - ❑ Usare sia port che node WWN per identificare !
- ❑ Hijacking e man in the middle sui protocolli FC
  - ❑ Simili ad ARP spoofing e DNS poisoning
- ❑ Attacchi per superare lo zoning
  - ❑ Unico a resistere: hard zoning su port, ma restrittivo !

## ❑ Protocollo iSCSI

- ❑ Autenticazione (CHAP) e Crittografia (IPSEC) opzionali...
- ❑ Autorizzazione ... in clear text... 3S: sniff, spoof, see
- ❑ Si possono fare MITM, Hijacking, Domain Hopping...



## ... outsourcing ?!

---

- ❑ IANAIA: I am not an industry analyst...
- ❑ ... però vedo molti dei miei clienti scettici sull'outsourcing, in particolare dello storage
- ❑ Molti "storage providers" sono usciti dal mercato e/o forniscono servizi di backup a PMI e consumer
- ❑ Esisterebbero motivazioni a favore:
  - ❑ Utility computing model: provisioning rapido, condivisione di tecnologia
  - ❑ Riduzione dei costi di management (fino a 10 volte il costo del ferro, secondo Gartner)
- ❑ Alcune aziende usano dei service provider per backup/business continuity
- ❑ Qui le challenge di sicurezza non sono solo tecniche

# Tecnologie di sicurezza di domani...

---



- ❑ Anomaly detection sull'accesso ai sistemi di storage
  - ❑ Es. FABS, File and Block Surveillance System (FABS) – un tool di apprendimento che può individuare pattern di accesso non standard
- ❑ Utilizzo di honeypot nei sistemi di storage
- ❑ Strategie di Continuous Data Protection
- ❑ Utilizzo di sistemi crittografici a chiave pubblica integrati con i file system per fornire integrità e confidenzialità / controllo di uso (shared encrypted file system, “DRM”, etc.)
  - ❑ Dato cifrato in modo da poter essere acceduto solo dalle persone autorizzate... non esiste una soluzione banale!
  - ❑ Si risolvono anche problemi di shredding e di insider



## Conclusioni

---

- ❑ La sicurezza è un processo
- ❑ La sicurezza è un processo olistico
- ❑ La sicurezza dei sistemi di storage dipende solo in parte dai sistemi di storage
- ❑ Crittografia e soluzioni di autenticazione sono solo parzialmente “forti” e usabili
- ❑ La gestione della sicurezza e dell'identità su sistemi di storage è un problema aperto
- ❑ L'outsourcing non è in generale una soluzione veramente accettata dal mercato
- ❑ Domani tecnologie di sicurezza più pervasive forse ci aiuteranno ad approcciare meglio il problema



# Grazie per la vostra attenzione !

---

- ❑ Se ci sono domande sono a vostra disposizione
- ❑ Feedback e follow up: [zanero@elet.polimi.it](mailto:zanero@elet.polimi.it)
- ❑ Slide: [www.securenetwork.it](http://www.securenetwork.it) sezione "Seminari"
- ❑ Per approfondimenti: [www.sikurezza.org](http://www.sikurezza.org)
- ❑ Visitate AIPSI: [www.aipsi.org](http://www.aipsi.org)