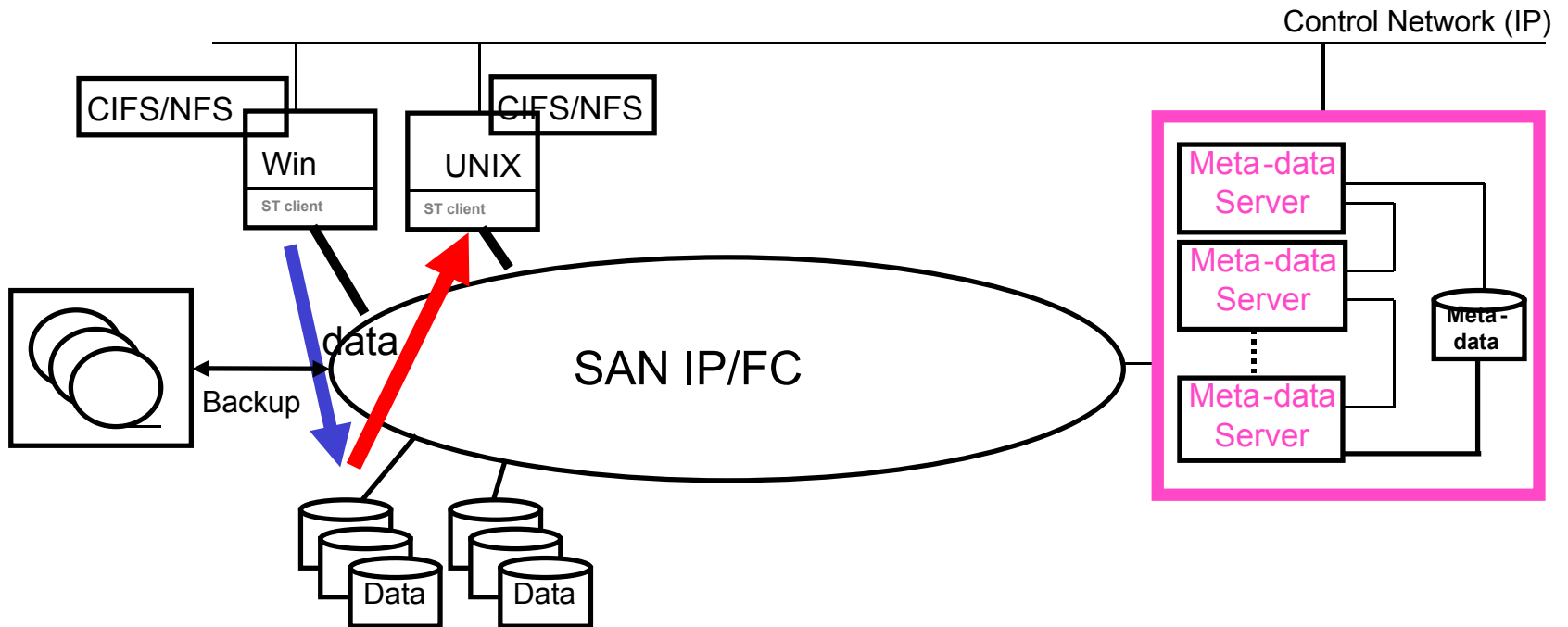# Object Storage - Panel

Julian Satran

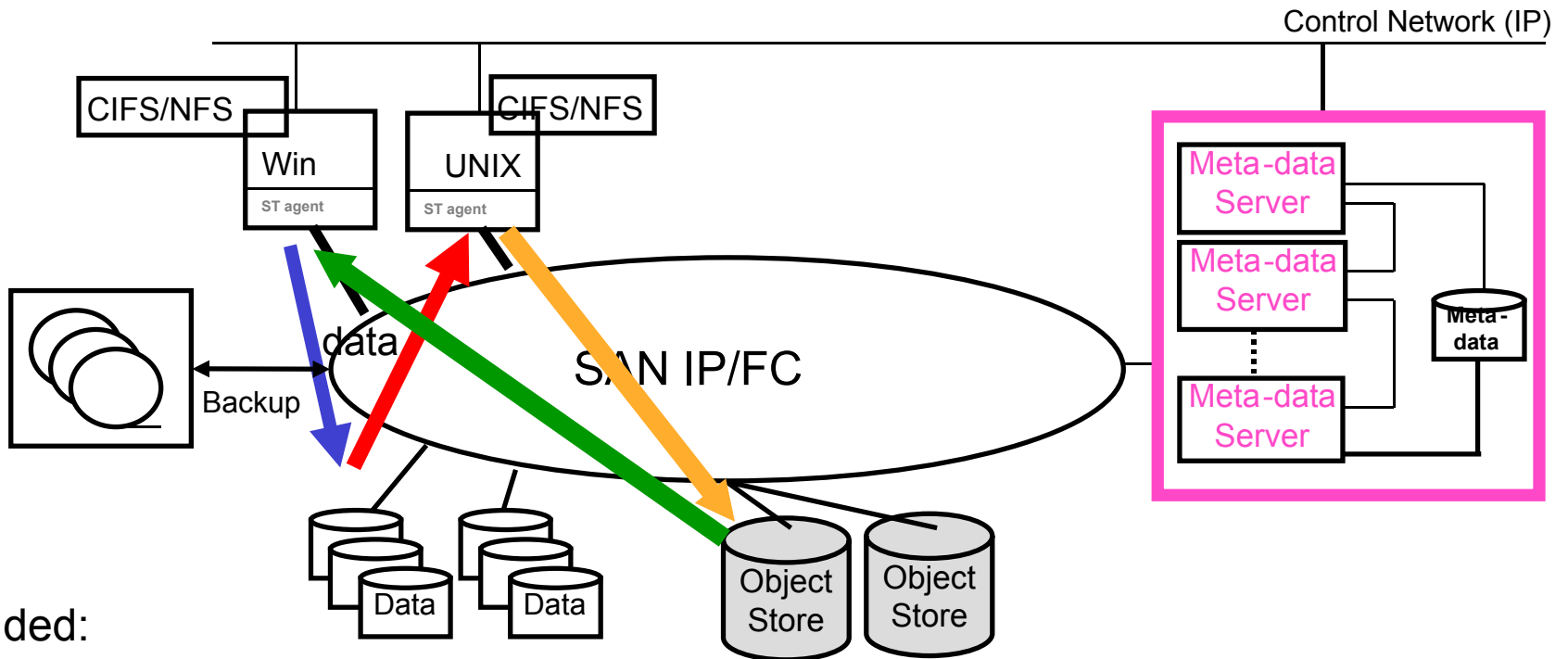# Storage Tank Background (IBM Research Almaden)

Capabilities:
- Performance and semantics similar to local file system
- Sharing like NAS
- Policy-based, centralized storage management
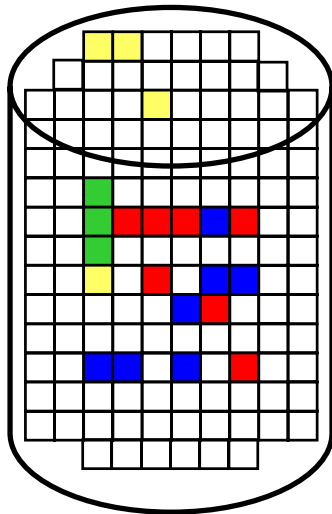
Object Store added to Storage Tank

added:
- SAN security
- Scalability
- Manageability

Object Storage

Today's Block Device

Operations
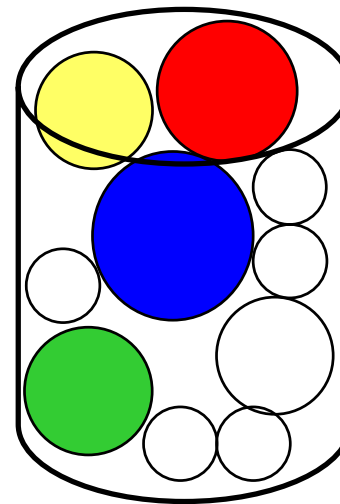   read block
   write block

Security
   Weak
   Full disk

Allocation
   External

Object Store

Operations
   read object offset
   write object offset
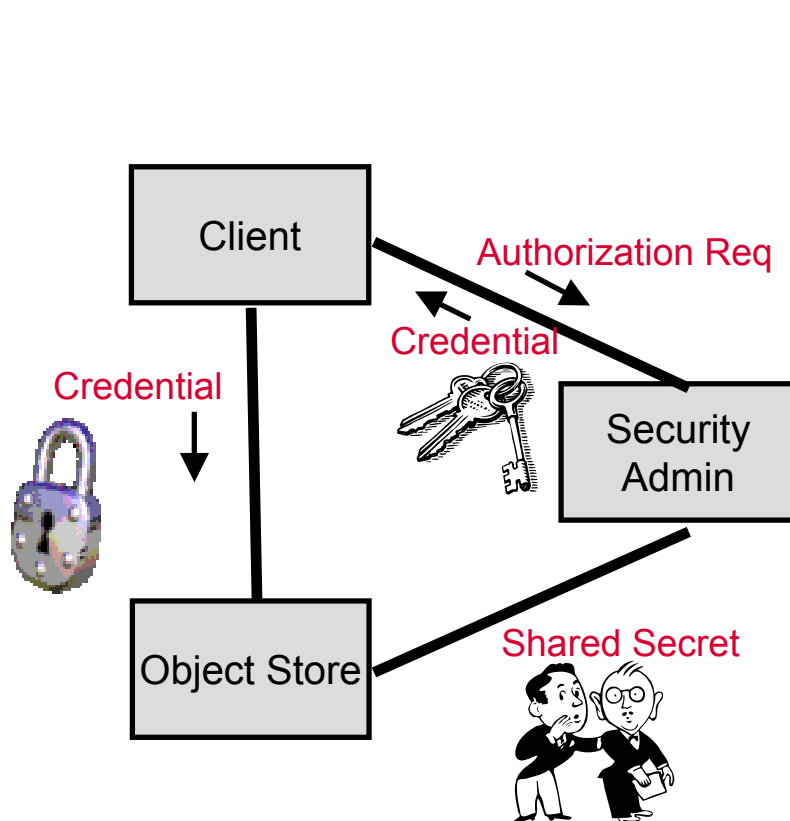   create object
   delete object

Security
   Strong
   Per Object

Allocation
   Local

Object Store Security

All operations are secured by a credential
Security achieved by cooperation of:
 Admin - authenticates, authorizes and generates credentials.
 ObS - validates credential that a host presents.
Credential is cryptographically hardened
 ObS and admin share a secret
Goals of Object Store security are:
 Increased protection/security
  At level of objects rather than whole LUs
  Hosts do not access metadata directly
Allow non-trusted clients to sit in the SAN
Allow shared access to storage without giving clients access to all data on volume

Client

Authorization Req

Credential

Credential

Security Admin

Object Store

Shared Secret

ObS vs. alternatives

- ◈ Complete segregation of the disk space (secure large entities)
  - ◈ Pros
    - ◈ No infrastructure change
  - ◈ Cons
    - ◈ No sharing
    - ◈ Requires careful synchronization
- ◈ NAS – the only complete alternative
  - ◈ Requires all application to use the FS naming structure (heavy)
  - ◈ Does not scale

What has to happen/is happening

- Standards & Prototypes
  - SNIA, T10
  - IEEE Storage Security
- Experimental Deployments
- Complete solutions including and data movement solutions
- Rich set of new applications

What next

◈ Data repositories with semantic access (next generation FS)

◈ Closer "coupling" with search and indexing engines

◈ Passive and active access models (push/pull)

◈ Richer security models (including securing data at rest)

◈ Multimodal data