invent

HP WORLD 2004
Solutions and Technology Conference & Expo

Storage Security: Considerations and Implementation

Abbott Schindler
Senior Technologist, HP

The information contained herein is subject to change without notice

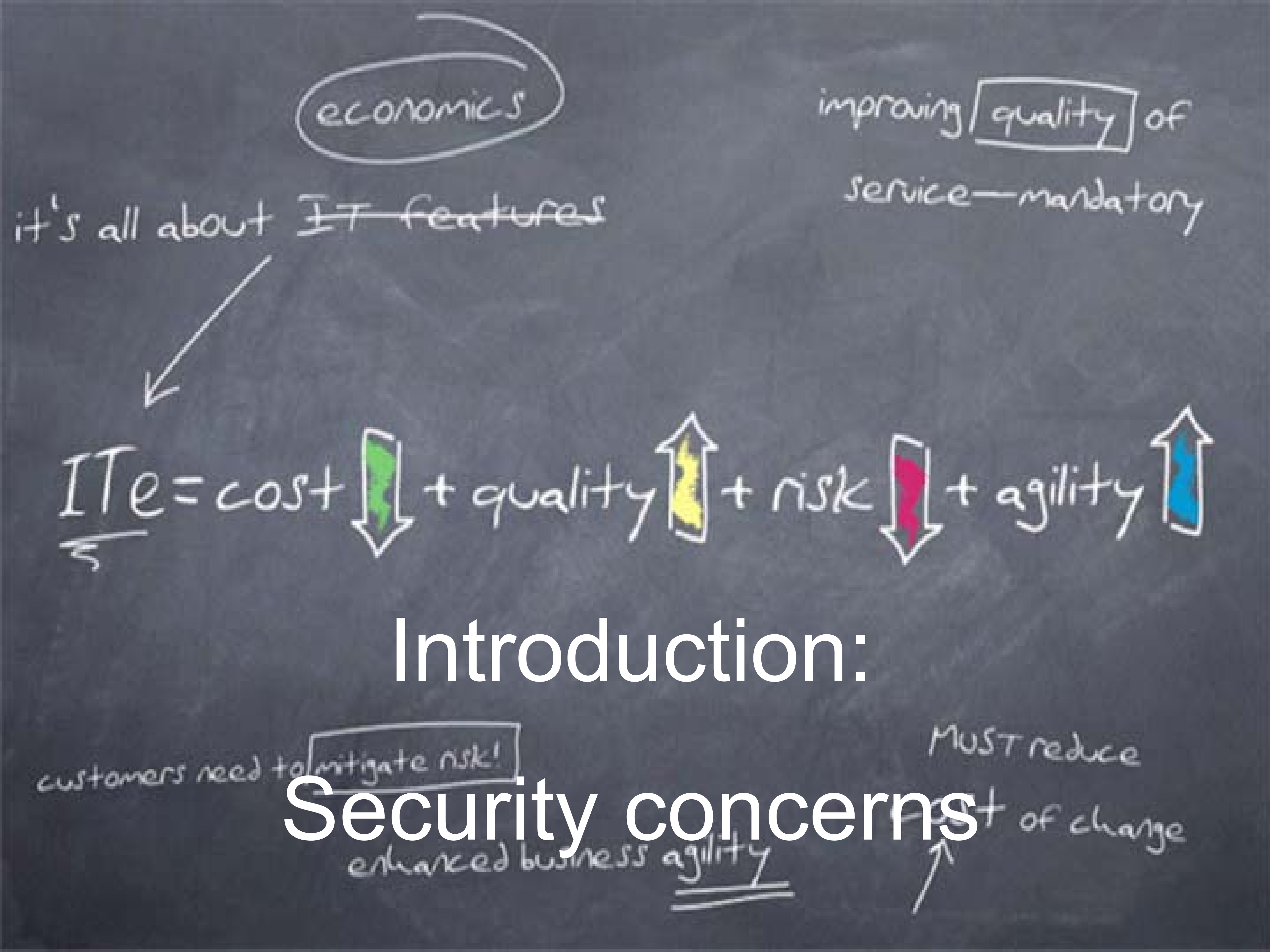
hp

Storage security…

The tip of the iceberg

Topics

- Security concerns
- A storage security model
- Implementation


economics
improving quality of
service—mandatory
it's all about ~~IT features~~
ITe = cost ⇩ + quality ⇧ + risk ⇩ + agility ⇧
customers need to mitigate risk!
MUST reduce
st of change
enhanced business agility

Introduction:
Security concerns

Storage security

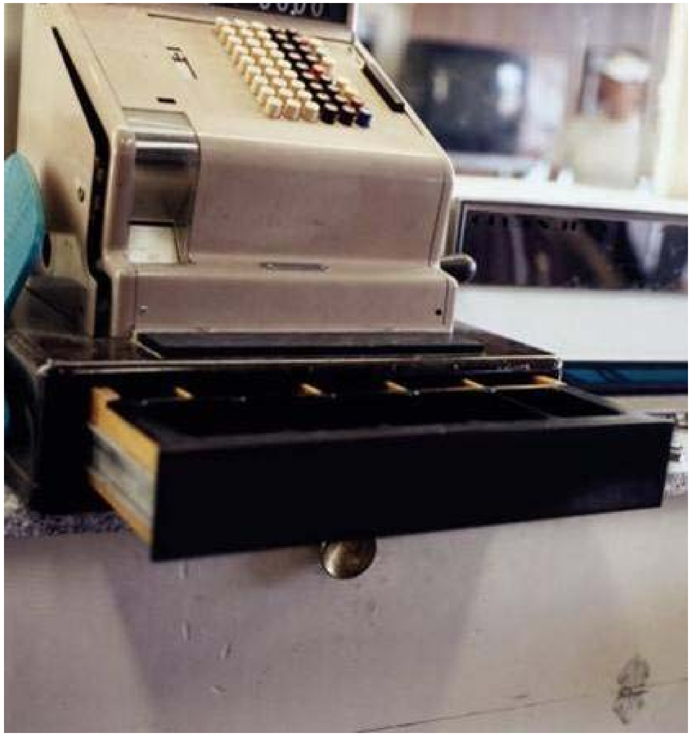
- Growing customer concern is catalyzing industry action
  - The industry is trying to wrap its collective head around the problem…toward creating working solution models
- Security products are emerging, addressing specific concerns
  - Provide and monitor access, audit trails, encryption
  - Emerging market…leading to proprietary solutions
- Storage security is a component of overall IT or enterprise security
  - Central authentication, authorization
  - Consistent view of threats, risks

Storage security drivers

- The way data is accessed
  - More data online accessible to more applications
  - Networked storage is shared by many systems
  - Sophisticated disaster recovery schemes
- Privacy concerns
  - Well publicized incidents of theft of sensitive data
  - Privacy laws
- Standards and industry organizations
  - FC-SP standard for FibreChannel
    - Expect early products within a year
  - iSCSI security standards and their use of IPsec
  - SNIA Storage Security Industry Forum (SSIF)
- Companies advertising and selling new products and features which address various aspects of storage security

Business drivers

- Economic consequences
  - Application uptime
  - Loss/corruption of data
- Compliance
  - Failure to meet regulatory compliance tests and requirements



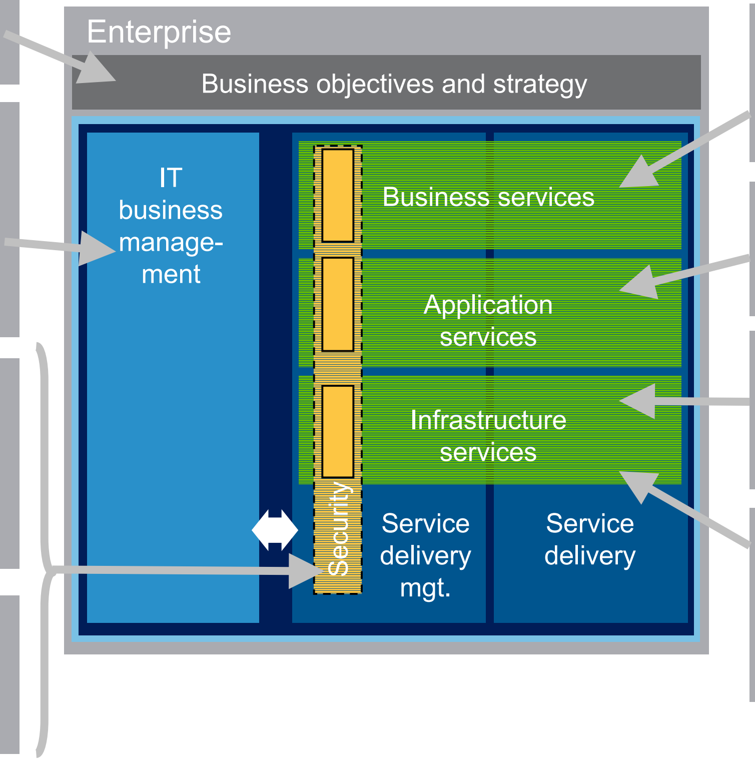
Adaptive Enterprise security model

Business Security
Business strategy and processes to define trust relationships, attitude towards risk, and security of the information

Security Governance
Organizational structure, processes, and training to create an effective enterprise information security program. Includes planning, reporting, audit, and management of threats and incidents.

Risk & Trust Management
Synchronization, assurance, fulfillment, and management of trust relationships, policies, security attributes, and security services. Includes event management.

Trustworthy Management
Effective trust and security policy and controls applied to the management and control infrastructure



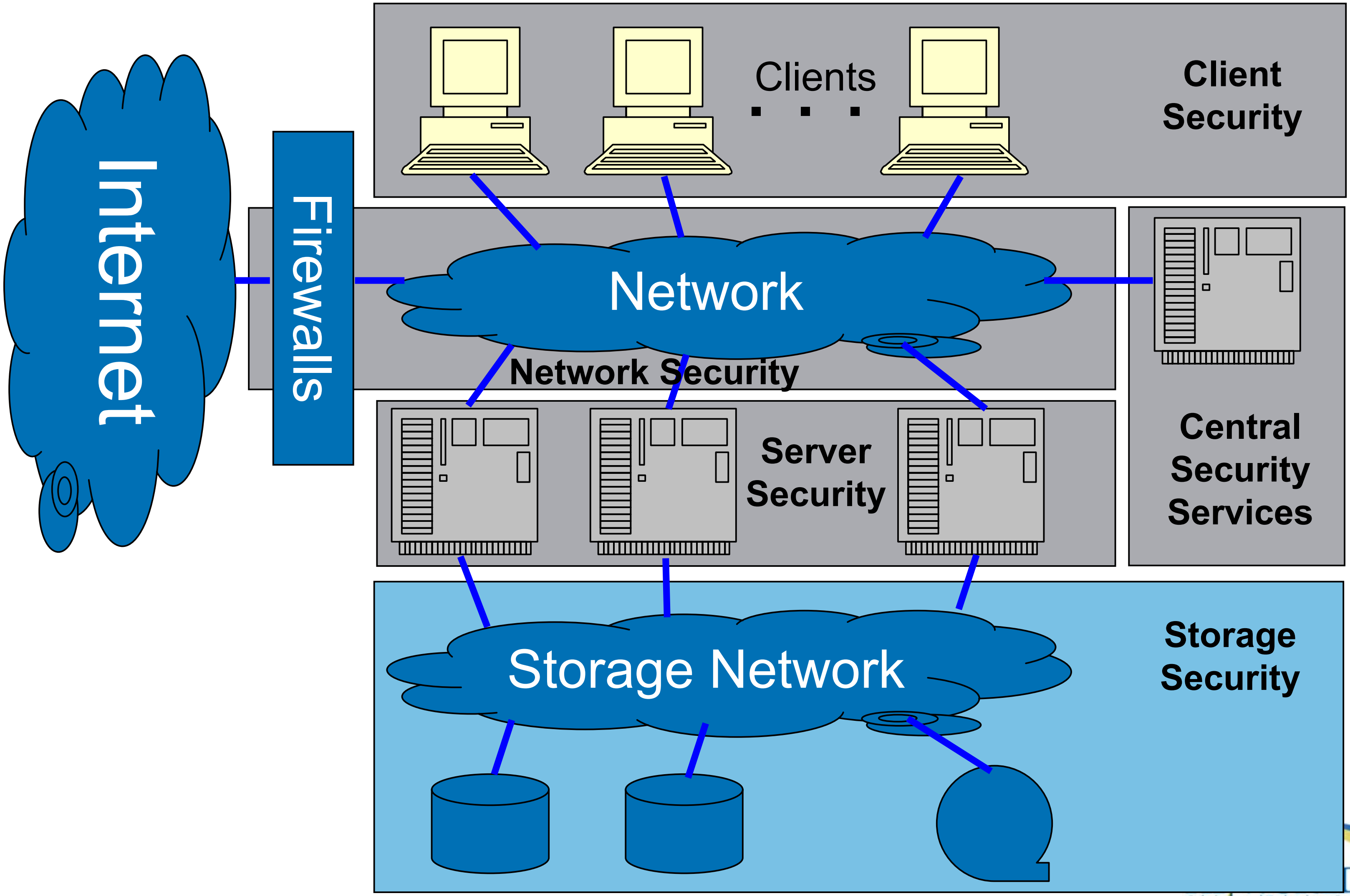
End-to-End Security
Integration and orchestration of security services and controls to implement the security policy across the value chain

Security Integration
Use of standard security services to implement security controls and functions

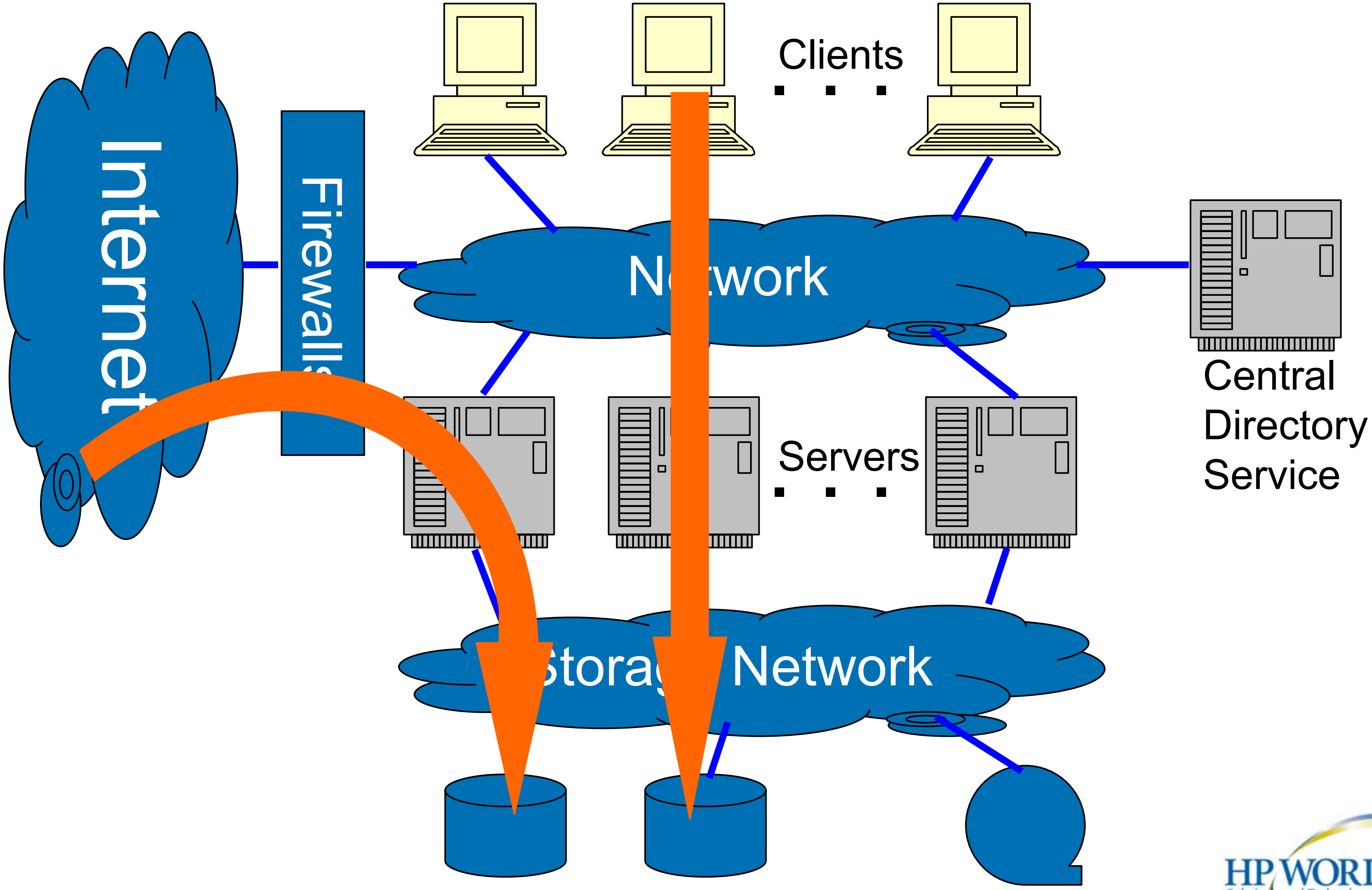
Trust & Security Services
Identification and authentication, authorization, confidentiality, integrity, non-repudiation, privacy, key management, …

Trustworthy Infrastructure
Combination of system, device, storage, and network security to protect the availability, integrity, and confidentiality of data and processes

Comprehensive data center security



Starting point: secure the IP network

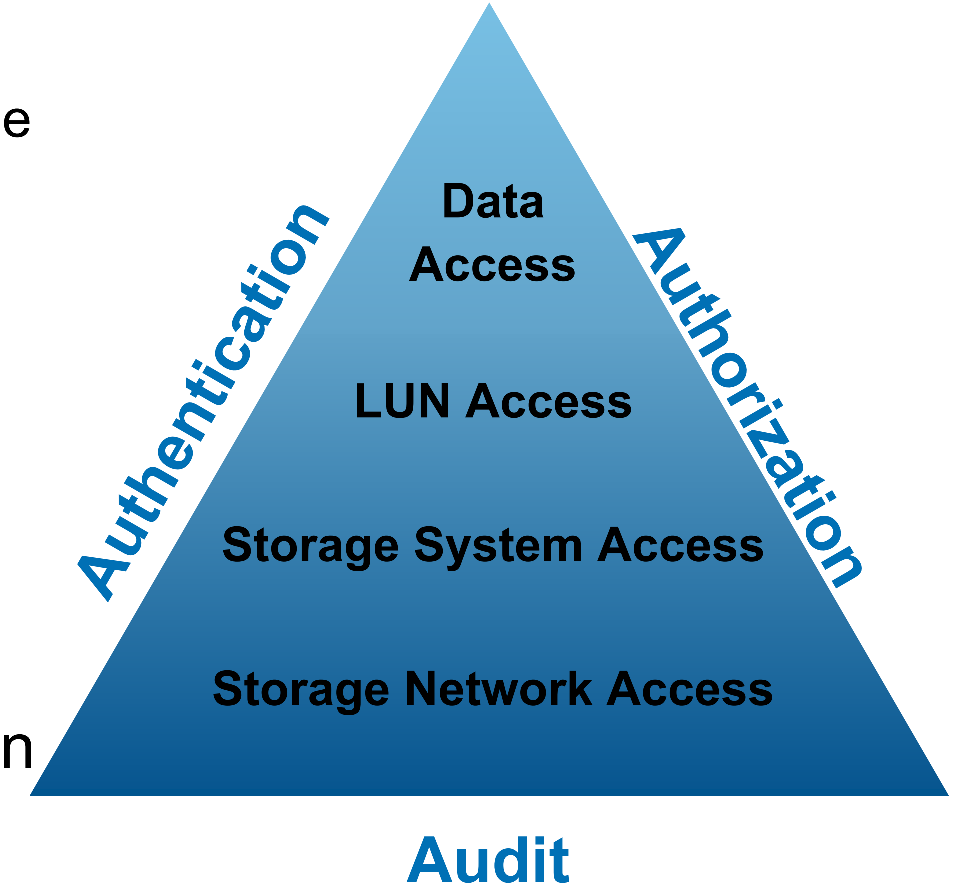


Storage security

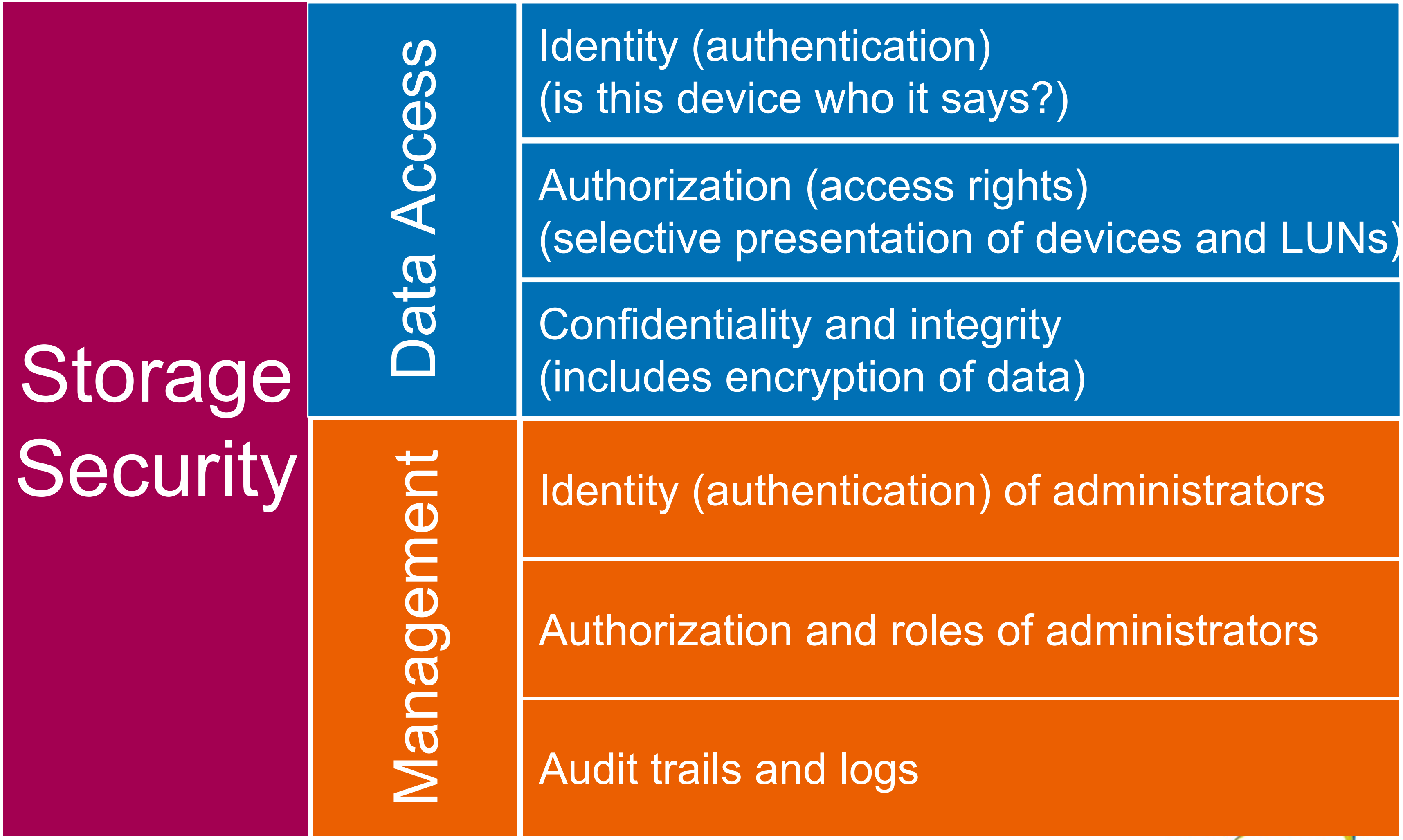
- Confidentiality
  - Prevent unauthorized reading of data
- Integrity
  - Prevent unauthorized modification of data
- Identity
  - Authentication of both administrators and devices
- Authorization
  - Administrators, to perform actions
  - Devices, to access data
- Audit and Accounting
  - Records of who did what, when
- Availability
  - Prevent denial of service attacks

NSS storage security philosophy

- Comprehensive storage-based security model
  - Component of data center-wide security
- Protects data everywhere
  - On storage
  - In flight
- Audit trails
  - For all system accesses
  - For all storage management operations that touch data
- Single administrative sign-on
  - Single way to assign roles, permissions, etc.



Storage security model



Storage Security

Data Access

Identity (authentication)
(is this device who it says?)

Authorization (access rights)
(selective presentation of devices and LUNs)

Confidentiality and integrity
(includes encryption of data)

Management

Identity (authentication) of administrators

Authorization and roles of administrators

Audit trails and logs

Data Path threat model

	Attack	Exposure	Mitigation
Data Access	Steal or copy disks	Data exposed, loss of data	Physical data centre security
	Unauthorized access to arrays	Data exposed	LUN masking, LUN level security
	Unauthorized access to tape system	Data exposed	Backup application roles and authorization Tape security in *HP Extended Tape Library Architecture*
	“Spoofing” (forged credentials)	Data exposed, loss of data	Fabric check/verify address
	Unauthorized change in array/switch permissions	Data exposed, loss of data	Strong authentication, role-based permissions

Management threat model

Management

Attack	Exposure	Mitigation
Change to disk array permissions	Data exposed, loss of data	Strong authentication, role-based permissions
Change in disk array configuration	Loss of data	Strong authentication, role-based permissions
System mounts/initializes a volume it doesn’t own Operator error Software error	Loss of data	LUN masking LUN security
Denial of service (flood of data from errant or rogue system)	Temporary loss of access to data	Manually disconnect attacking system

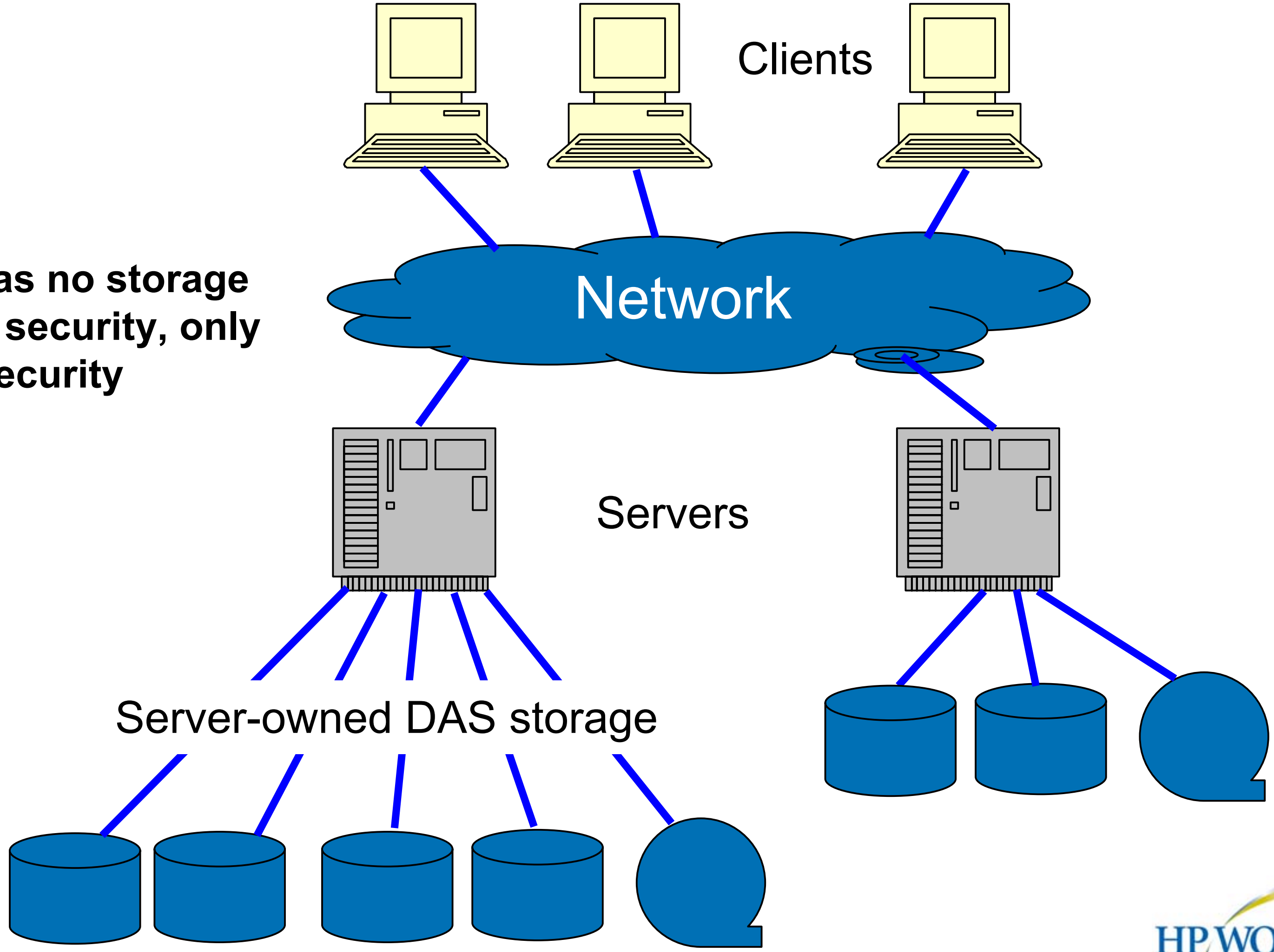
Authorization

- “Does this device have permission to perform this action?”
    - SCSI does not have an authorization mechanism
- FibreChannel SANs
    - Zoning, LUN masking
- iSCSI (Ethernet) SANs
    - Per-device and per-LUN Access Control Lists (ACLs)
- NAS
    - NFS, CIFS permissions (ACLs)

Confidentiality and Integrity

- In-flight encryption of data
  - Today: replication data between data centers
    - Requires encryption/decryption box at each end
  - Future: iSCSI encryption facilitated by IPsec
    - Can be built into future interfaces, making encryption speeds usable
  - Future: FibreChannel encryption using FC-SP
    - Encapsulated Security Payload (ESP) encryption
      - Key-based on-the-wire (“in flight”) encryption
    - Requires all elements of SAN to possess encryption and key capabilities
- On-Media encryption of data
  - Possible today, but costly and complex to administer

Storage network security (10 years ago)



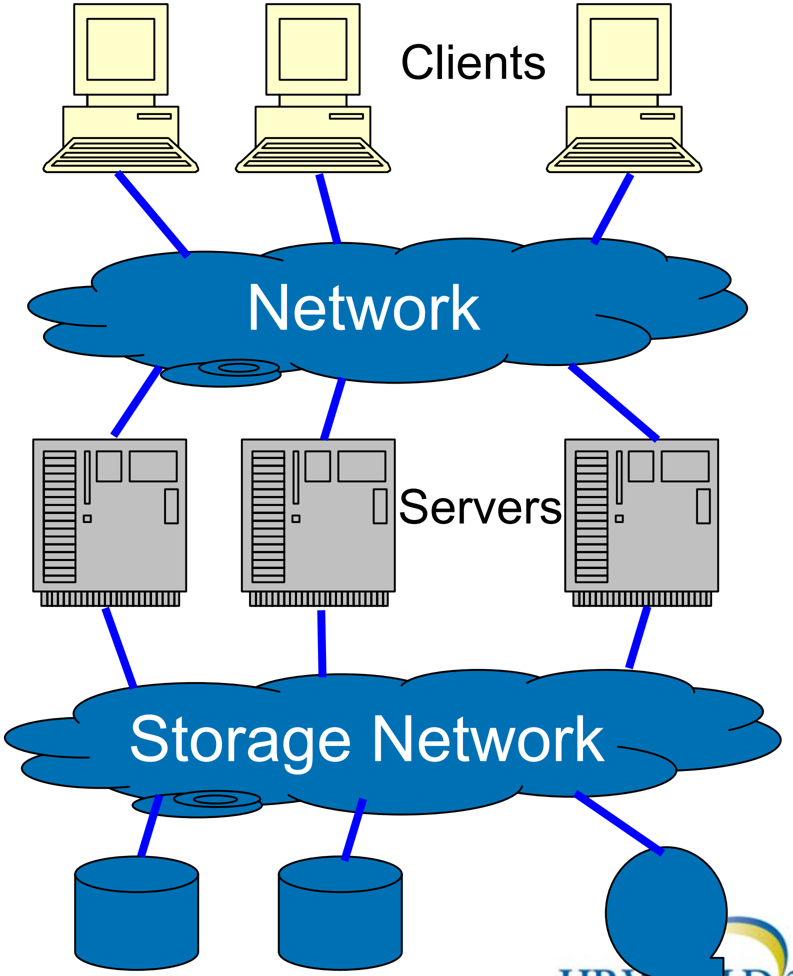
There was no storage network security, only server security

Today’s storage security toolset

- Storage for many clients (servers or networked clients) is consolidated onto networked devices
- Three tiers of data access security
  - SAN zoning allows a SAN to be divided into parts (zones) which are logically isolated
  - Selective LUN presentation, which controls access to LUNs provided by disk arrays
  - ACLs on file systems (NAS)
  - Virtualization ensures that network storage consumers “see” a dedicated storage system containing only its data
- Administrative security follows the systems model
  - Each switch or disk array has one or more roles
  - The administrator must give the appropriate password
    - Array controller, management appliance, management utility

Storage network security (today)

- WWN based LUN security
- Passwords on all storage device management functions
- Device management ports isolated from standard network
- Audit trails, logs per device
- Leading edge opportunity to prevent WWN spoofing
- Leading edge opportunity for encryption



HP WORLD 2004 Solutions and Technology Conference & Expo

Storage security standards: FC-SP

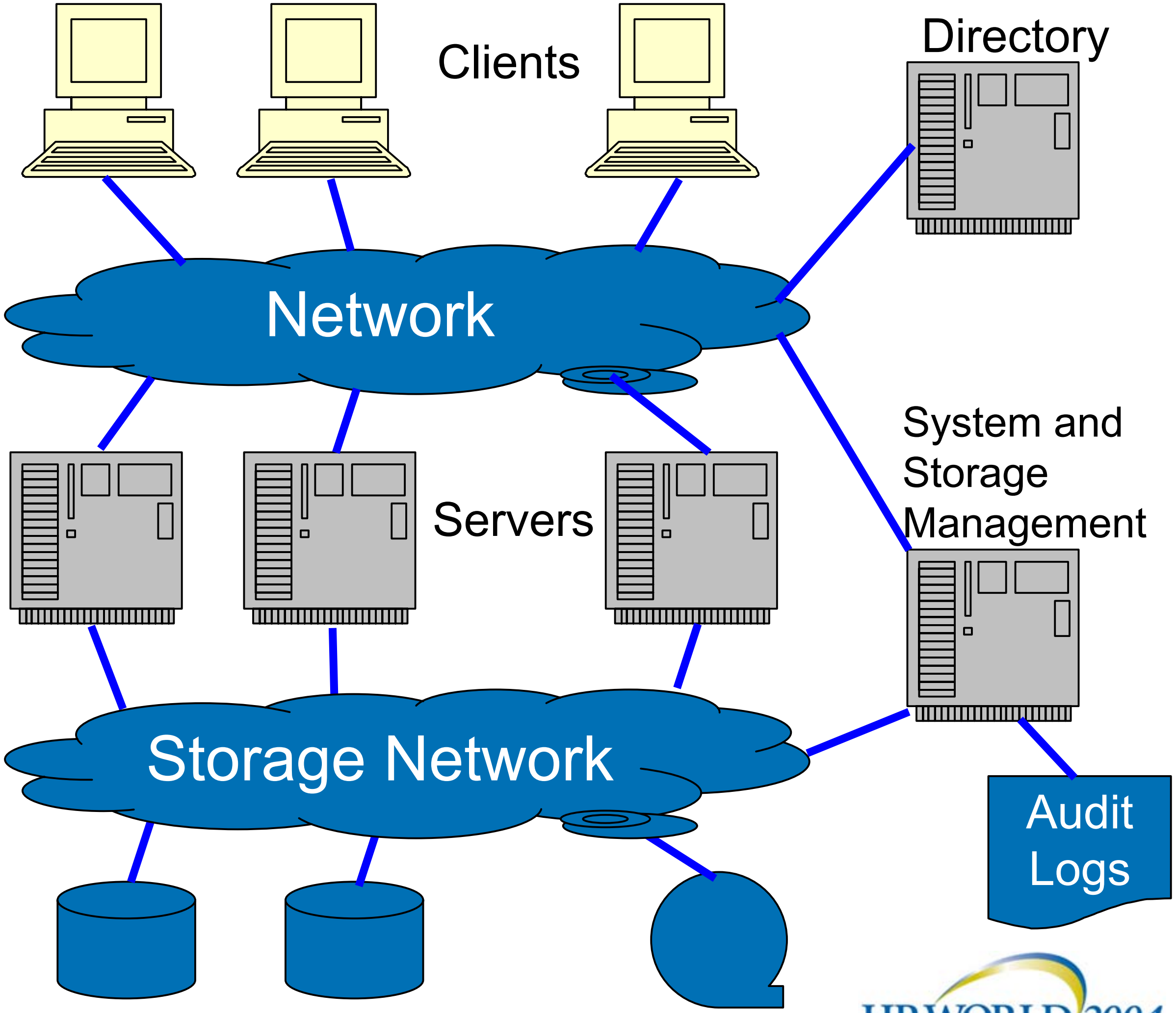
- Fibre Channel Security Protocol
  - Industry expected to deliver products in 2005
- Key capabilities
  - Authentication mechanisms
  - Device Membership lists
  - Switch Membership Lists
  - Switch Connectivity Objects
- Why it's important
  - Eliminates impersonation (spoofing)
  - Enabling technology for exchanging keys

Storage security standards: IPsec

- iSCSI
  - Risk: opens the possibility of storage connected directly to the Internet
- IPsec capabilities
  - Security design is a robust combination of product features and operating procedures
    - Includes iSCSI gateway, IPsec authentication

Storage network security (future)

- Consolidated Management of storage and servers
- Single signon for management
- Consolidated view of audit trails
- Device authentication based on a variety of standards: certificates, FC-SP for Fibre Channel, IPsec for iSCSI
- Leading edge of enterprise wide single sign on, centralized authentication



The changing definition of “identity”

- Historically, an identity was
  - A logon belonging to a user (“Abbott”) or
  - A logon belonging to a role (“superuser” or “administrator”).
- Recent trend
  - Focus identity on the person (“Abbott” again)
  - Special privileges are associated with a role
    - Role is assigned to a person
    - Eg, “Abbott” has “administrator” privileges on this server
- Separate from the identity of an individual
  - FC-SP and iSCSI both give a device its own identity
  - An application may have a role that requires special privilege in order to run.

Future of identity and authorization

- Near future
  - Authorization will depend on the appropriate one of user, device, or application identity
    - Two of these might be used separately
  - Example: a user accesses a file
    - File system checks user’s permissions
    - Disk array checks system’s permission to access the LUN
- Farther out
  - Authorization will be done based on all three
  - Example: I can remotely access the network if
    - My identity as a user is confirmed, AND
    - The PC I’m logging on with belongs to my company, AND
    - The application I’m using is authorized

“Trust” – trusted systems

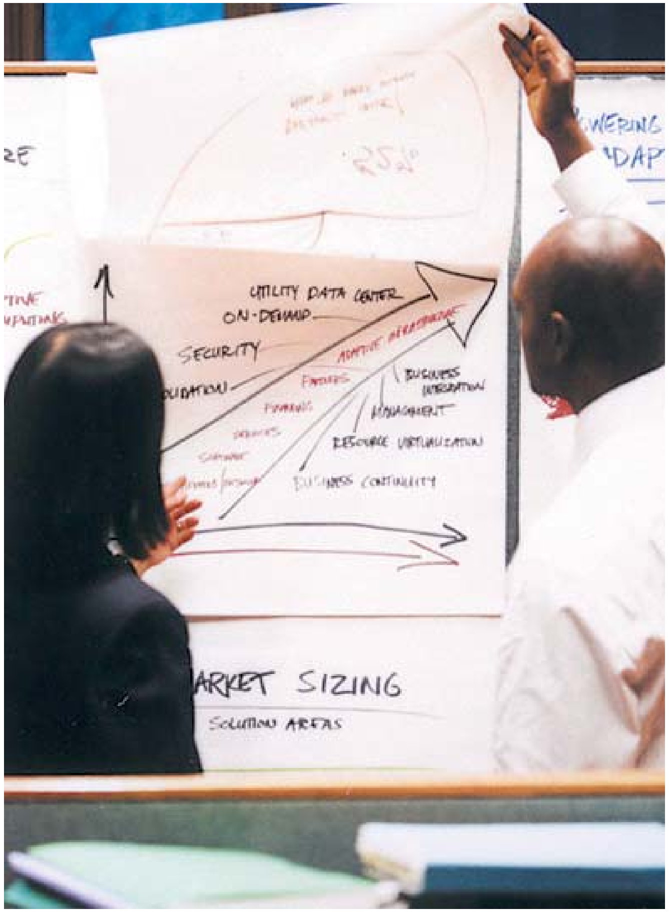
- Emerging technology, very powerful concept
- Goal: systems will refuse to run if corrupted
- Basic idea: use only known and trusted hardware and software in computers
  - Start with an incorruptible core containing the information needed to validate BIOS and hardware
  - Check each component before bringing online
  - Example:
    - Validate software digital signature against known public key
    - Check each piece of hardware against known configuration
    - If this works correctly, machine will be in a trustable state by construction at the time it attempts to join the network
    - At that time it will be asked for additional credentials such as proof that antivirus is running and current, or firewall is up

Storage in trusted systems

- Storage system itself must be trusted
  - By construction, purpose built hardware/firmware, or
  - By build-up-from-incorruptible core as systems do
- Storage system must have a verifiable identity
  - System can trust that it is not reading data from or writing data to an impostor
  - FC-SP will provide this for Fibre Channel
  - iSCSI has authentication mechanism
- Additional requirements for storage will probably emerge

Implementation guidelines

- Centralize management
  - And control access
- Implement fabric authentication wherever possible
  - iSCSI gateway (today), FC-SP (future)
- Authorize/control devices joining the fabric
  - Disable all ports not being used
- Audit, log, track, and report
  - Monitor for breaches
- IP based storage (iSCSI, NAS)
  - FC SAN in a locked data center is difficult to penetrate
  - A network reaching every desk in a company is easier
  - A device on the open Internet is easiest



Conclusions

- All of security is important, not just storage
  - Choose your level of security for the whole data center or the whole organization, not just for storage
- When securing storage today,
  - Pay attention to management paths first
    - All the passwords, all the device management ports
  - Use LUN level security
    - Zoning where appropriate
    - Prevent spoofing-of-WWN attacks (advanced topic)
  - Consider advanced security technologies if necessary