Multilevel Security in Remote Storage

KEVIN BUTLER, SHIVA CHAITANY, PATRICK MCDANIEL, ANAND SIVASUBRAMANIAM

Motivation for Multilevel Security

Separation of duties and access to information is vital for many business processes, particularly military applications. In businesses, this separation is becoming increasingly important, given the current regulatory conditions concerning compliance.

For example, the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) have stringent requirements for health providers and financial companies, respectively, concerning who has access to information. Separation of duties and functions must be enforced under threat of criminal investigation and substantial penalties. Accountability is critical, and multilevel security can enforce these operations, such as data deletion by unauthorized users.

Multilevel security can be used to enforce confidentiality (Bell-LaPadula model), integrity (Biba model), or separation of duties (Clark-Wilson model).

Security lattices define categories of security by forming a structure of lattices and compartments: levels are vertical (TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED) while compartments can be found at each level (e.g. NUC, EUR, US, null for intelligence, giving access to nuclear, European, US secrets or none).

Remote Storage

Enterprise storage has become increasingly centralized over the past ten years, due to the rise of storage area networks (SAN) and network attached storage (NAS). Many competing technologies exist, such as FibreChannel and NASD, but iSCSI is becoming the predominant protocol for allowing remote storage.

The iSCSI protocol is a mechanism for sending SCSI disk commands directly over IP.

Security Lattices

Access to all compartments

(NUC, EUR, US)

(NUC, EUR)

(NUC, US)

(EUR, US)

(NUC)

(EUR)

(US)

Access to no compartments

∅

Storage Security

Storage systems need to provide security above and beyond network security.

Firewalls alone are not the answer because of insider threats and potential existence of compromised machines. Storage threats include deletion of persistent data, a significant threat not addressed by network safeguards.

Protecting integrity, confidentiality, availability of data is of prime importance. Goal: prevent unauthorized access to, and modification of data.

MLS and Block-Addressed Storage

How do we define multilevel security in block storage? Our solution: Grant access in a distributed manner by the creator of the content, who delegates access. Use metadata proxies to avoid changing the iSCSI protocol.

A TCP connection over a UNIX pipe links the iSCSI server and client with the metadata server and client proxies, respectively. We consider Linux iptables to extract user and group information from the OS, interrupting the socket call and gathering the pertinent information, extracting & re-encapsulating the SCSI commands over the proxy connection.

For security, the links are protected with IPsec. To improve performance, we consider offloading encryption to crypto cards on the machine, and lazy decryption for received information, as well as techniques to minimize system upcalls through the network stack.

Current Experiments and Results

We are currently evaluating performance of iSCSI over IPsec in our experimental testbed, with a security evaluation to follow; this work forms the foundation for performing MLS.

Encryption algorithms used by IPsec (ESP) can dramatically affect performance (e.g., using AES vs DES and 3-DES; use of IPsec also affects scalability of clients. We are considering methods of improving performance and scalability, and techniques such as skip encryption. In addition, the use of lazy decryption can serve to greatly improve performance as data would only be decrypted when necessary, reducing computational burdens that cause performance bottlenecks.

IPsec (ESP, 3-DES) for sequential reads

IPsec (ESP, 3-DES) for random reads

RESEARCH SPONSORED BY RAYTHEON