The Need to Pass more than one Decryption Key

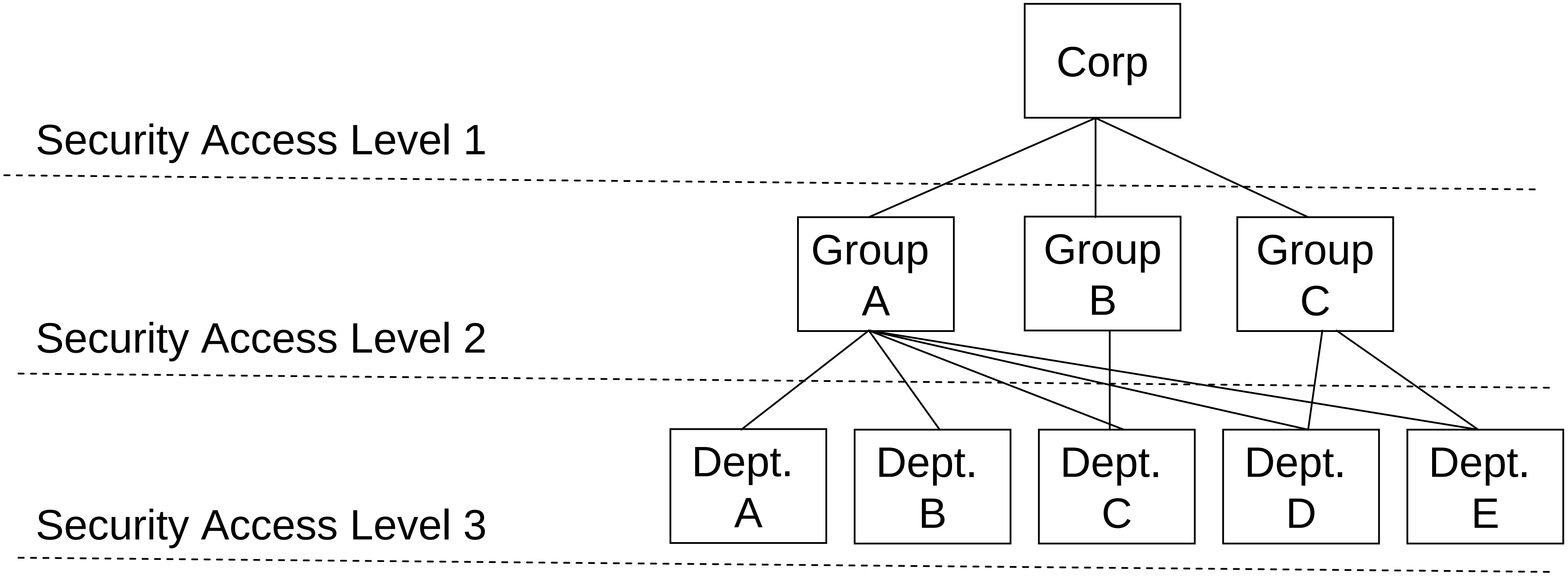
6 Jan 2006

Dwayne Edling

Sun Microsystems DMG

Proposal Number T10/06-051r0

The Requirement for More than One Decryption Key



Corp

Security Access Level 1

Group A

Group B

Group C

Security Access Level 2

Dept. A

Dept. B

Dept. C

Dept. D

Dept. E

Security Access Level 3

The Requirement for More than One Decryption Key

- In a secure data system, Keys will serve to:
  - Segregate data bases between functional departments
  - Segregate data based on level of security clearance
  - Segregate data based on ownership of data
- Corporate should have the keys to access all levels below (i.e. Groups and Dept.)
- Groups access one or more departments
  - Groups like Finance would access all departments.
  - Groups like engineering would only access engineering departments.
  - Departments would only access their own records.

The Requirement for More than One Decryption Key

- Passing only one decryption key requires that a new read decryption key must be provided at group or department file boundaries.
- This method can cause performance loss.
  - Keys would not be changed until a record was encountered that did not have the correct decryption key.
    - The decryption would have to be attempted and fail.
    - A decryption failure would have to be reported.
    - A new key would have to be provided by the client.
  - For look aside decryption systems.
    - If a small cache buffer filled while waiting for the next key a reposition would be encountered.
  - For pass through decryption systems.
    - A reposition may be required every time a new key was required, if the encryption HW is positioned before the cache memory.

The Requirement for More than One Decryption Key

- Passing more than one decryption key will provide for optimized performance in a streaming device.
  - Based on the security access level granted to a client session, all the keys required for reading during that session could be provided in one exchange.
  - There are many vendor unique methods for matching keys to records. I am not proposing that any of these be in the specification but here are a few solutions.
    - Directory entries.
      - Order dependent key maps.
    - Block meta data.
    - Tape Marks?

The Requirement for More than One Decryption Key

- Adding an option to pass more than one decryption key will allow for the single key management model currently proposed and provide for vendor unique optimizations.