CERIAS

the center for education and research in information assurance and security

JTAM: A Joint Threshold Administration Model

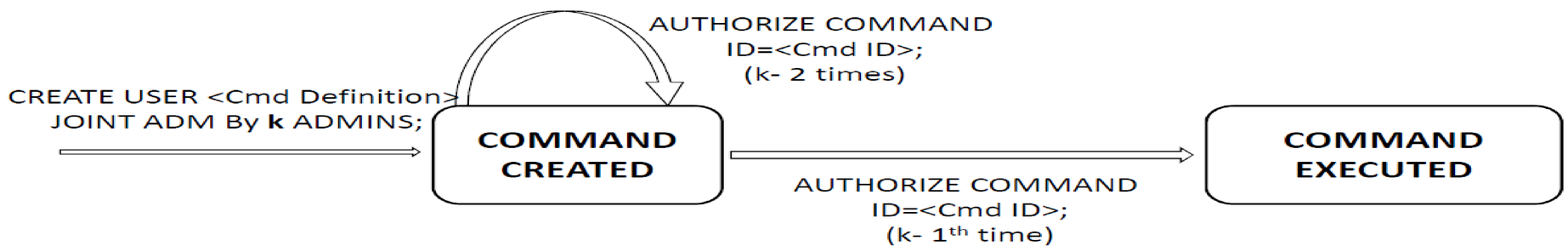
Ashish Kamra, Elisa Bertino
akamra@purdue.edu, bertino@cs.purdue.edu

OBJECTIVE: To support separation-of-duty in performing certain critical and sensitive operations (at production sites) called JTAM-ops such as user creation/deletion/modification, grant/revoke of permissions, modification of security policies, and so forth.

KEY IDEA: A JTAM-op is not executed by the system unless it has been authorized by at least k - 1 additional administrators where k must be specified when creating the JTAM-op.

HIGHLIGHTS: 1. Create a digital signature on the hash of the in-progress JTAM-op details.
2. The JTAM-op is executed by the system only when a valid digital signature can be created on the JTAM-op details.
3. Uses Victor Shoup's threshold cryptography signature scheme to create the digital signature.
4. Every administrator is assigned a secret share for signing a JTAM-op.

Lifecycle of a JTAM-op (Create user command for example)



LIFECYCLE DETAILS: 1. The system generates a signature share on the hash of the command definition using command creator's secret share.
2. It then generates a signature share for each of the administrators that authorizes the command.
3. When k - 1 administrators have authorized the command, the signature combining and verification algorithms are executed.
4. The final signature on the command is verified using the public key corresponding to the k value associated with the command.
5. The final signature is stored along with the newly created user entry.
6. A signature verification deamon periodically verifies the signature on all the user entries.
7. Any user attribute modified without using a JTAM-op will invalidate the signature on the user entry. The signature violation is detected by the signature verification daemon.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center