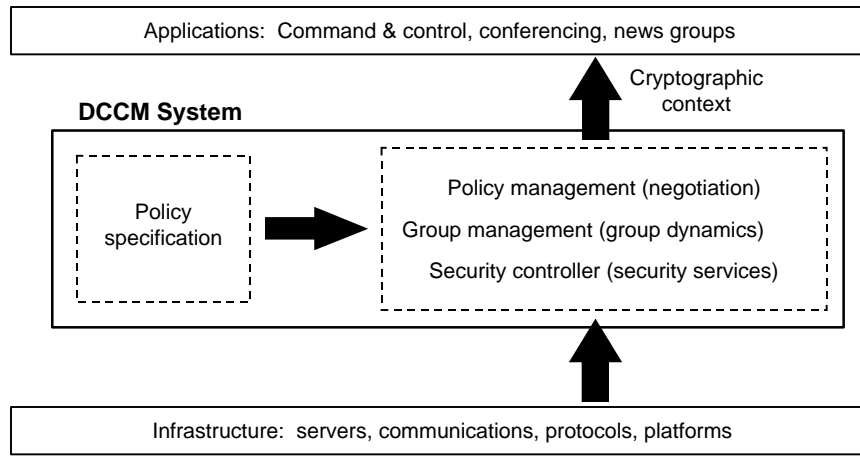


Dynamic Cryptographic Context Management (DCCM)

High-level Architecture



New Ideas

Policy-driven multi-party application security management for very large, dynamic groups (e.g., 100,000 participants)

- security policy specifies goals, services, and constraints
- policy drives cryptographic context for application
- policy / context negotiated and maintained dynamically

Security policy to cryptographic context translation

- security policy encoded in a cryptographic context
- security parameters change when policy changes

Dynamic group cryptographic keying / re-keying capability

- maximum participant list created for application
- group key changes when participant list changes
- goal is to optimize key update protocol / computation

Impact

Comprehensive security architecture / framework for very large, dynamic multi-party applications.

Policy-driven security services and mechanisms for very large, dynamic multi-party application groups.

Automated support for multi-party security policy specification, negotiation, translation, and accommodation.

Efficient, scalable group key establishment and re-key methods.

Demonstrated capability in dynamic cryptographic context management.

Schedule

