CERIAS

the center for education and research in information assurance and security

Enforcing Spatial Constraints for Mobile RBAC Systems

Michael S. Kirkpatrick and Elisa Bertino
CERIAS, Purdue University
mkirkpat@cs.purdue.edu, bertino@cs.purdue.edu

Background & Motivation

GEO-RBAC

- Augments RBAC with location information
- Supports mutual exclusion and separation of duty
- Distinguishes *enabled role* and *activated role*
- Allows for hierarchical roles and policies

Sample Policy:

< *Doctor, Hospital, Patient Records, RW* >
< *Nurse, ER, Patient Records, R* >

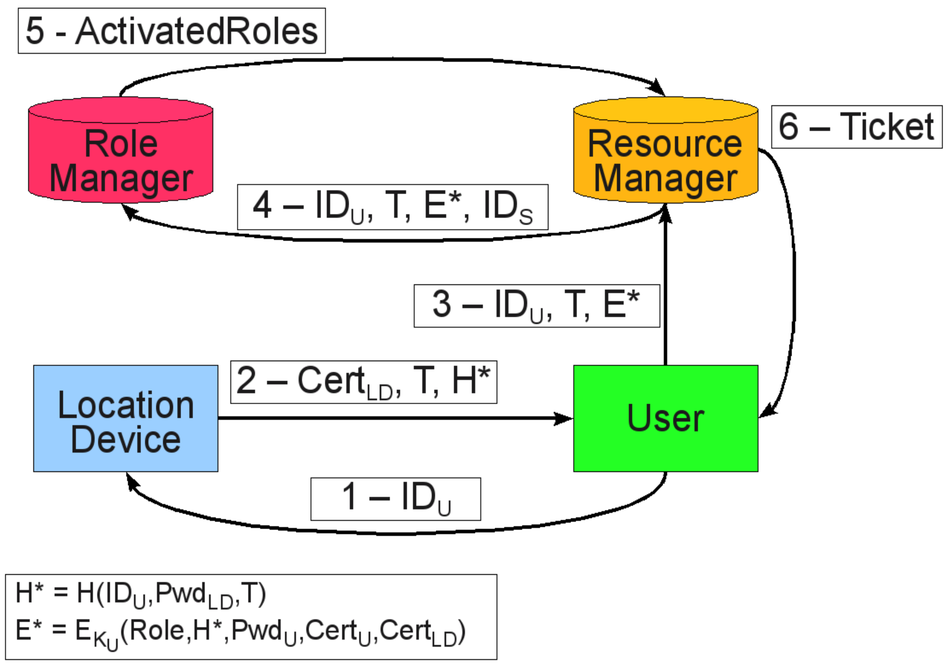
Sample Requests:

< *Surgeon, ER, John Smith's prior surgeries, read* > ✓
< *Clerk, Billing Dept., Celebrity X's ultrasounds, read* > ✗
< *Nurse, Home Office, ex-spouse's allergy list, delete* > ✗

Key Challenges:

- Integrity of claimed location
- Continuity of usage as user moves

Basic Access Request Protocol



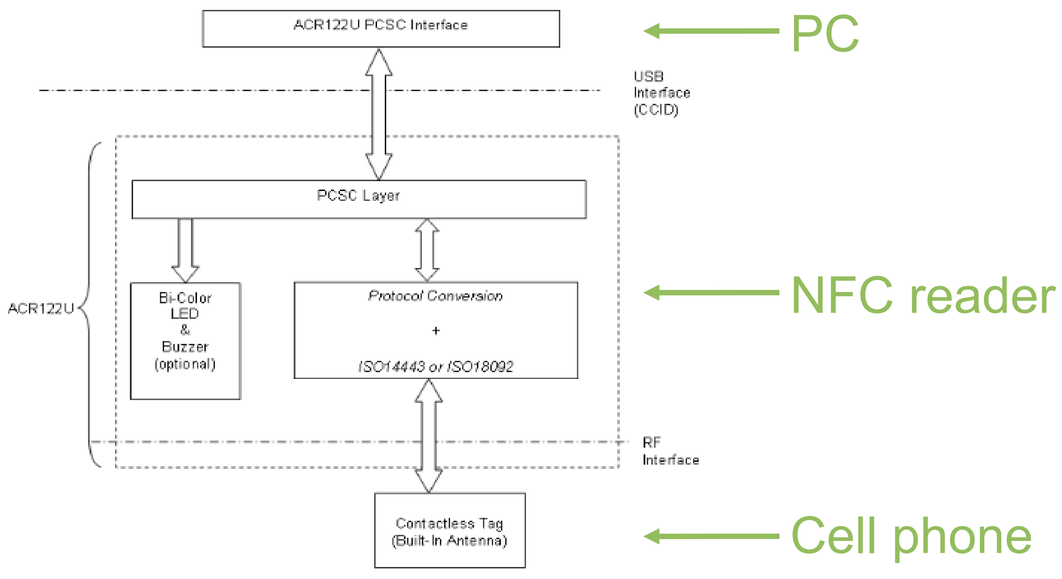
Security Guarantees:

- **Proximity** ensures location integrity
- Updating active roles enforces continuity

Near-Field Communication

RFID-based Technology:

- Limited broadcast range of **10cm**
- Allows peer-to-peer data transfer
- Widely deployed in Nokia cell phones in Europe, Japan



Coming soon to an iPhone near you!

Protocol Extensions

Mutually Exclusive Roles:

- Disable current role on activation of a conflicting role
- Broadcast *ActivatedRoles* to all resource managers

Continuity of Usage:

- Require update to location proof
- Proactive (user initiated) vs. reactive (required by resource manager)
- Granularity of updates impacts performance

Future Work:

- Distributed role manager
- Enforcement based on relative proximity
- Separation of duty

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center