

NSAC

Network Security and Applied
Cryptography Laboratory

<http://crypto.cs.stonybrook.edu>

Lab and Projects Overview

Radu Sion

sion@cs.stonybrook.edu

www.cs.stonybrook.edu/~sion

Phone: 631-632-1672

Fax: 631-632-1690



Lab Overview

NSAC

Faculty: **Radu Sion**

Established: **2006**

Active Funding: **\$360,000+**

Sponsors: **Motorola, CEWIT, NSF**

Graduate Students: **3+** (Fall 2006)

Affiliation: **Center for Cybersecurity**

Collaborators: **IBM Research, Motorola**

Selected Projects Overview

NSAC

- NS³
- Tamper-proof WORM 😊
- Personal DRM
- Sensor Nets: Location Certification
- SQi: Secure Query Interface
- SecureGates
- Enterprise DRM

NS³: “Networked Secure Searchable Storage”

NSAC

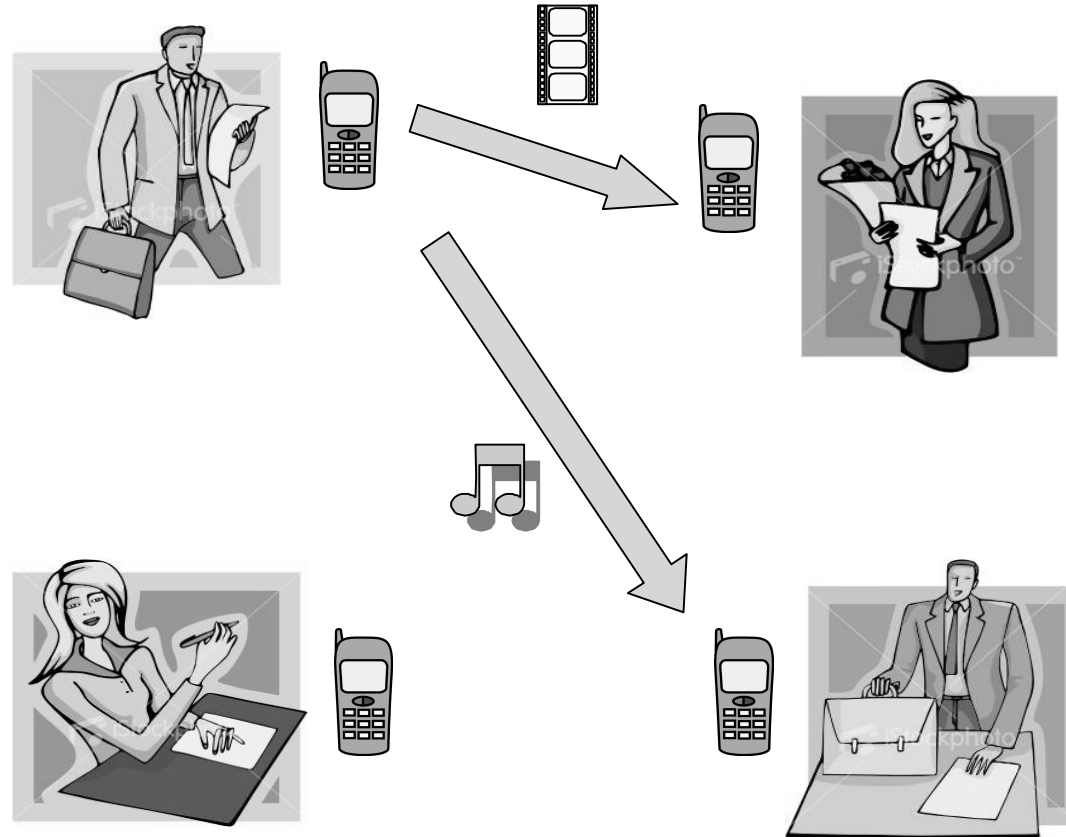
- Networked Data Storage
 - Confidentiality
 - Correctness
 - Efficient In-Storage Search
 - Access Privacy
 - Sponsor: NSF Cybertrust (with Erez Zadok)

Tamper-proof WORM **NSAC**

- Storage in Un-trusted Environments
 - Massive Data (PetaBytes)
 - Write-Once Read-Many
 - Non-Repudiation
 - Efficient Search
 - Tamper-proof
 - Think about: Enron files 😊
 - Sponsors: none yet

Personal DRM in Mobile Environments (Overview)

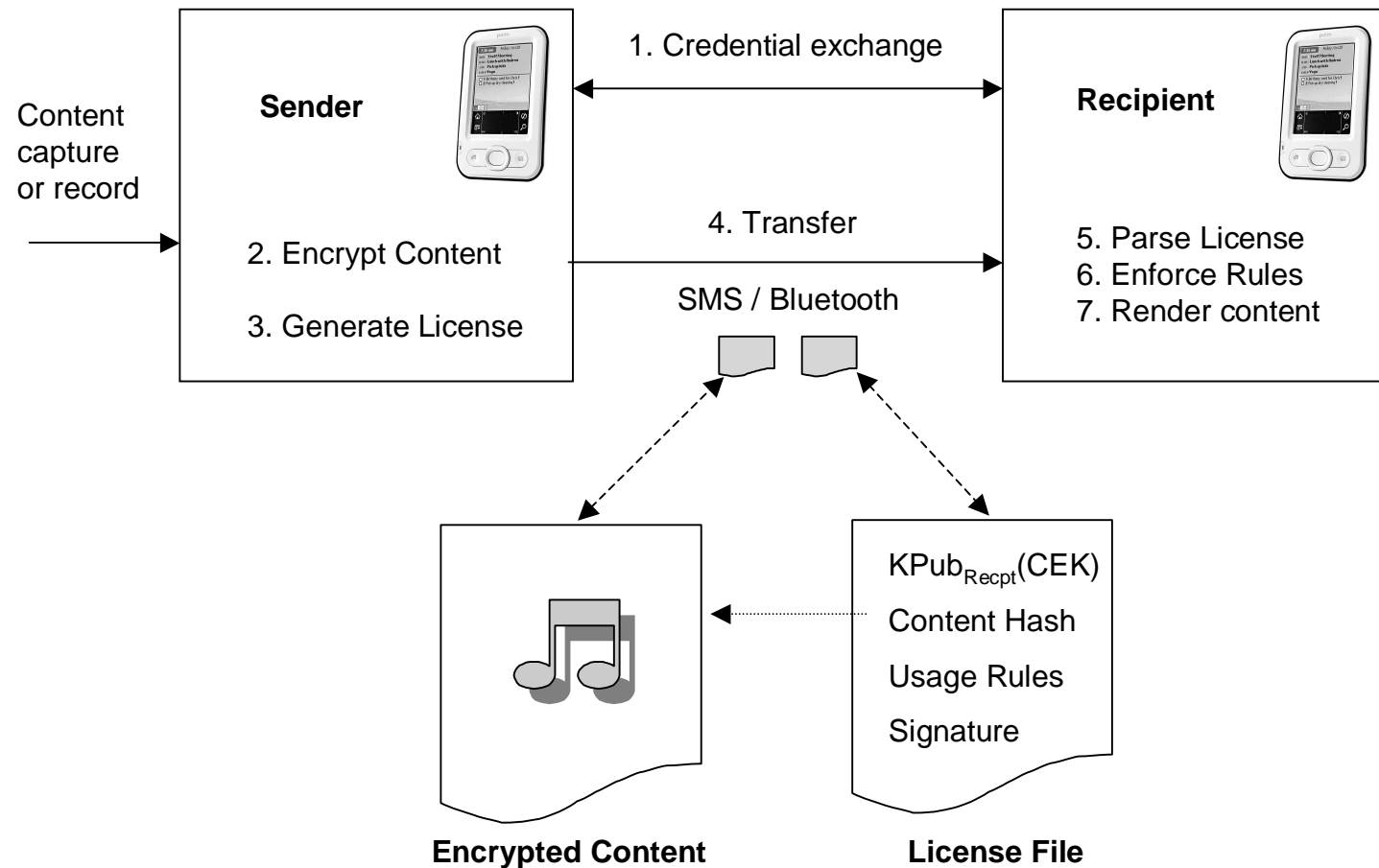
NSAC



Sponsor:
Motorola

Personal DRM in Mobile Environments (Solution)

NSAC



Location Certification for Sensor Networks

NSAC

- Securing Sensor Networks
 - Un-trusted Environments
 - Battlefield
 - Emergency Response
 - Correctness Assurances of Location Claims
 - Adversary
 - Faulty Equipment
 - Interference
 - Malicious
 - Sponsor: CEWIT (**until 12/2006**)

SQi: The Secure Query Interface

NSAC

- Outsourced Data Management
 - Clients require transparent assurances
 - Query Correctness
 - Data Confidentiality
 - Query Privacy
 - Example: Schwab allows IBM to manage its data warehouse
 - Sponsors: none yet.

SecureGates

NSAC

- Inside a government agency
 - Document flow
 - Assured accountability
 - Document creation, access, modifications
 - Concerns
 - Leaks 😊
 - Merit distribution
 - Solution: Secure tracking infrastructure with data-persisted fingerprints.
 - Sponsors: none yet.

Enterprise DRM

NSAC

- Inside a corporation
 - Controlled data flow
 - Scenario: business meeting documents should not be accessible outside the company. Upon crossing trust boundary, they should be automatically sanitized.
 - Content is augmented with DRM controls
 - Specify traditional DRM constraints
 - Extended to specify actions that happen upon crossing administrative boundaries
 - Transparent and portable mechanisms
 - Only add-on software layers
 - Specifically, no modifications required of legacy apps

Q/A

NSAC

Thanks ! 😊