

# Trust Management for Mobile Devices

Vipin Swarup

703-983-7625 • [swarup@mitre.org](mailto:swarup@mitre.org)

MITRE Sponsored Research

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

**MITRE**  
**Technology**  
**Program**

# Problem

- Access rights are often **context-sensitive** and **transient** (e.g., is soldier in friendly or hostile territory?).
- Today, access rights don't change as user's context changes (e.g., as soldier moves).
- **Can we build security mechanisms that adapt to user's current environment?**

# Background

**Dismounted warriors  
on tactical battlefield**



**Access to  
mission plan  
is restricted.**

- **Access rights depend on soldier's environment, e.g., physical location, WLAN membership, presence of trusted third party, etc.**

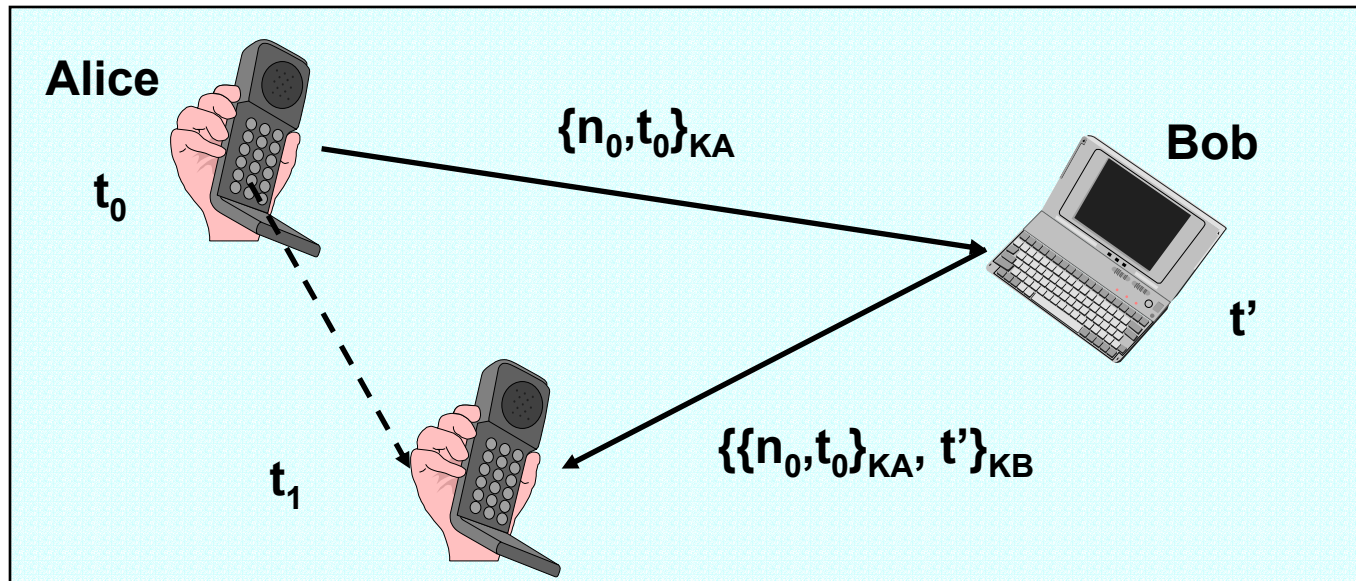
# Objective

- **To build secure applications that function seamlessly even as trust relationships change due to device mobility**
- **To simplify the development of security-aware applications**

# Activities

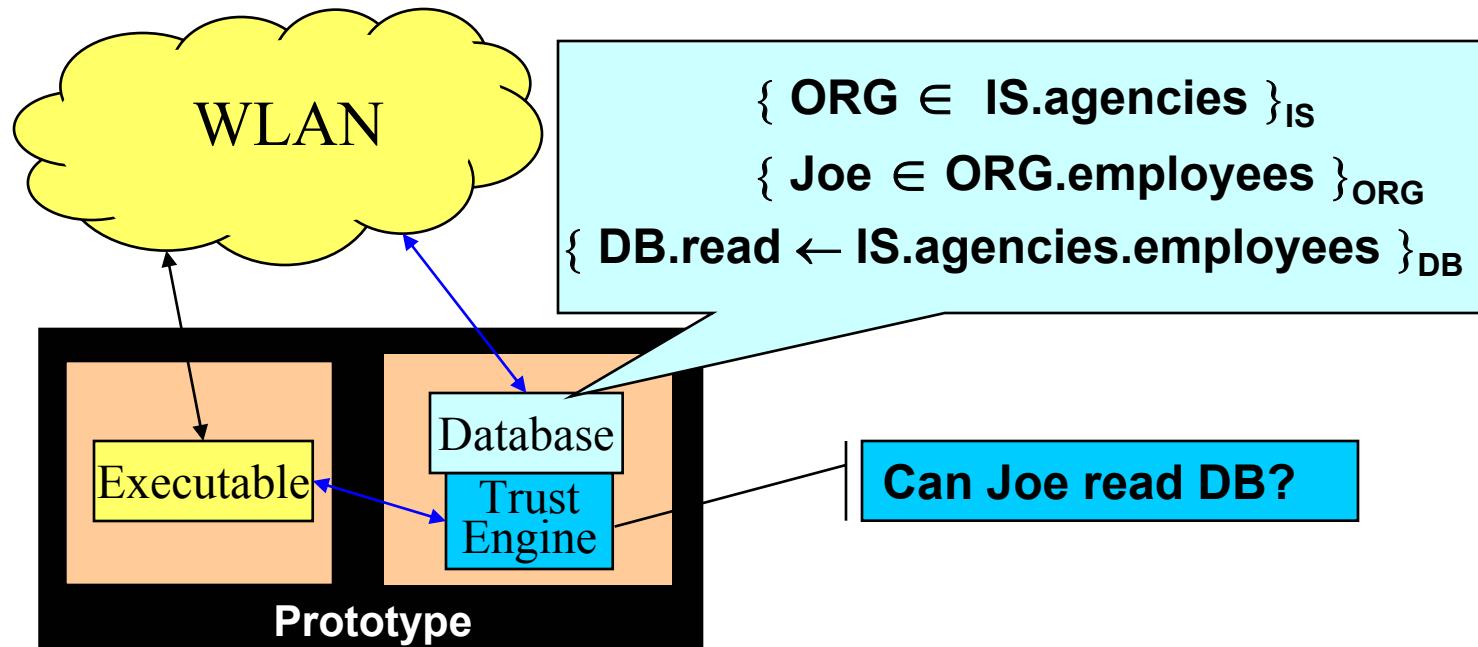
- **Establish spatial and temporal properties of mobile devices**
- **Develop a trust management engine for access control in open distributed systems**
- **Develop a context-sensitive access control mechanism that adapts to the changing environment of mobile devices**

# Highlight



- **Secure location services**
  - **Can Alice determine Bob's location?**
  - **Is the protocol secure?**

# Highlight

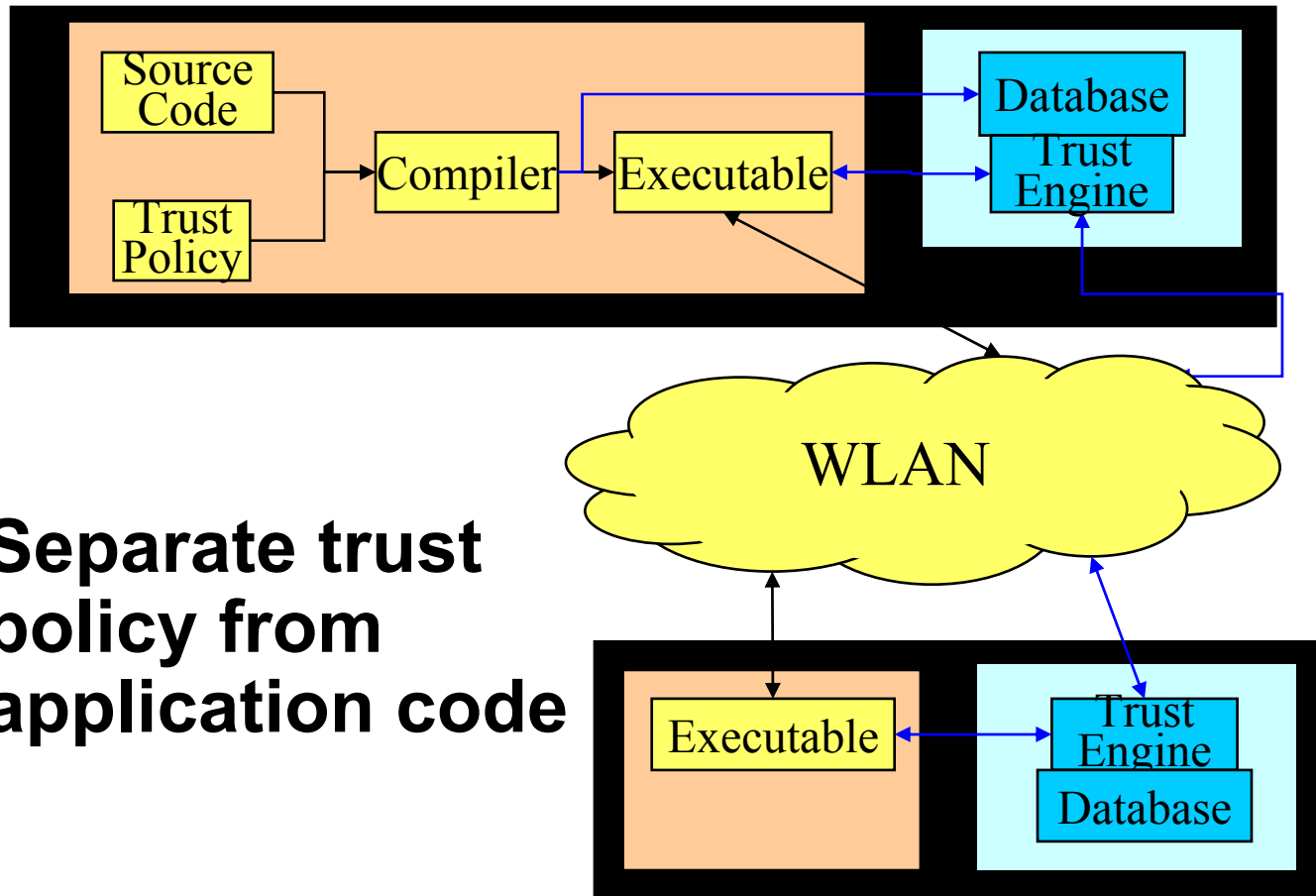


- Trust management: access control for open distributed systems

# Impacts

- **Will advance state of the art of information assurance (context-sensitive trust and separation of concerns)**
- **Will impact security architectures of next-generation mobile systems**

# Future Plans



- **Separate trust policy from application code**