Implementation of Policy-Based Encryption System for Data Sharing in the Power Grid

Aleksandr Shulman, University of Illinois at Urbana-Champaign
ADVISORS: Himanshu Khurana & Rakesh Bobba

Background

- EMERGENCY: Cascading Power Disruptions Are Spreading Due to Localized Failures
- REACTION: Correct information sharing will prevent the situation from spreading
- GOAL: Prevent disruptions through secure information sharing

Challenges: How can you guarantee uptime without revealing more sensitive data than absolutely necessary?

Solution:
- Encryption of sensitive data
- Distribution based on environment situation
- Ad hoc policy generation
- Centralized policy enforcement

Research Plan

- Leveraging the best open-source security suite: Speed, Capability, Flexibility, Ease-of-use, Open license
- Implement permission rights engine: Java's XACML implementation chosen - Reliable and well-documented - Capable of using environmental variables
- Set up attribute database - MySQL chosen due to licensing, ease of use, and development familiarity

Optimize for speed:
- Tweak various components in the system for optimal performance
- Locate bottlenecks and performance limitations

Model different entities on virtual machines:
- Multi-threaded KDC that can run multiple simultaneous queries and be generally fault-tolerant
- Gauge performance

Related work/interaction with other projects:
- Trustworthy Cyber Infrastructure for the Power Grid (TCIP), tcip.iti.uiuc.edu.