UNIVERSITY OF AGDER

User authentication in mobile cloud for crisis and emergency management

Joseph TWAYIGIRA

Supervisor: Prof. Vladimir Oleshchuk

07/05/2015

Overview

- Introduction
- Objectives
- Research question
- General system architecture
- User authentication
- User certificate issuing
- Conclusion

Introduction

- **Cloud-based solutions can be used to provide reliable bridge between government organizations and citizens in crisis situation.**

- **Reliability and security of collected and shared crisis and emergency information in mobile cloud is an issue.**

- **Strong user authentication can help to enhance the security and authorization of access to cloud-based crisis information systems and resources.**

Objectives

- **To propose user authentication model in mobile cloud by using digital certificates. It empowers security for mobile users with access control over cloud.**

- **To discuss the key security of user authentication using Certificate Authority(CA) in crisis situation.**

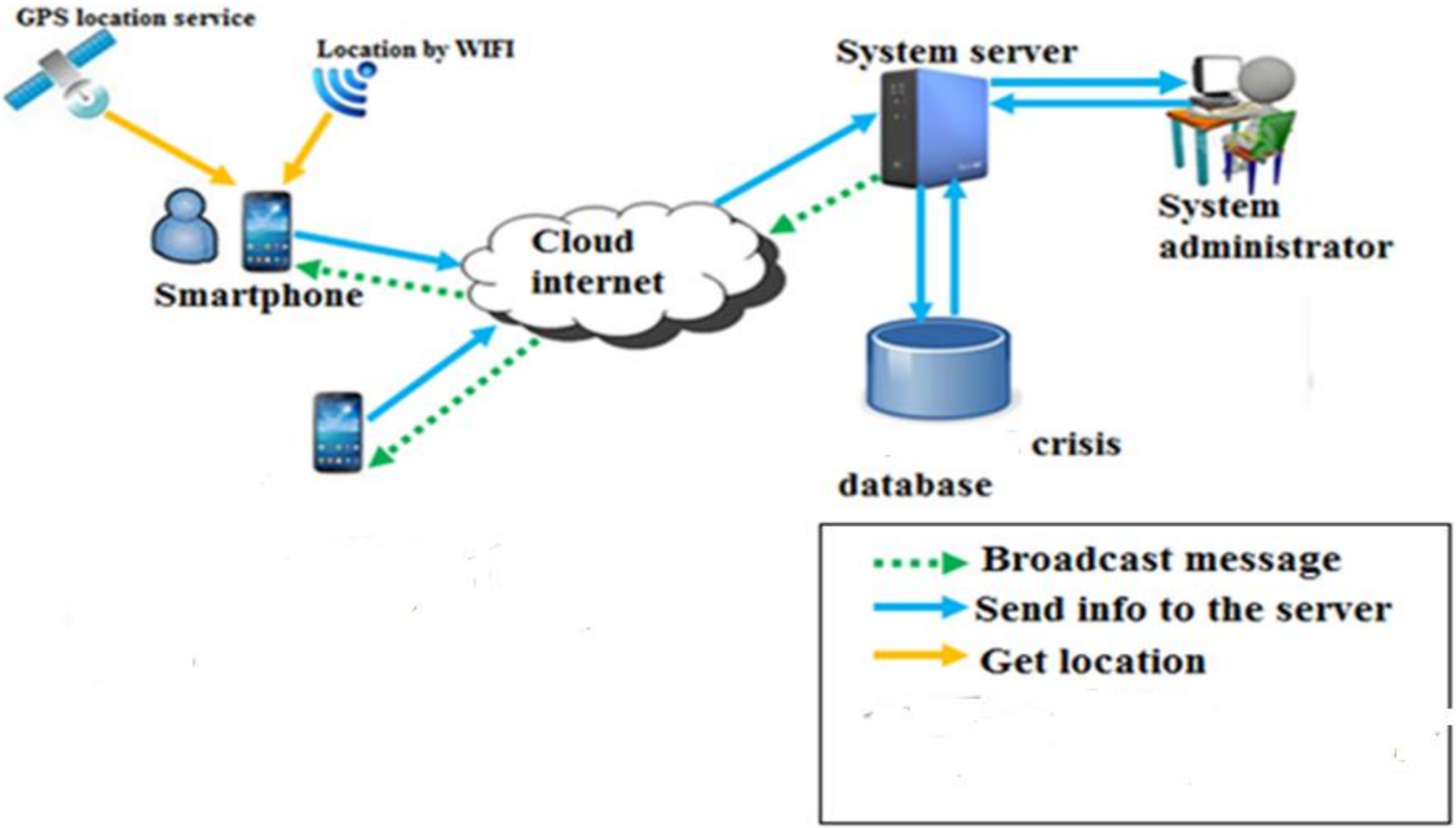
- **To design and implement a new security model for mobile user authentication to cloud. It is suitable for emergency and crisis management.**

Research question

What are user authentication scenarios?

1. **Use Certificate Authority (CA)**
2. **Provide strong security to mobile users**
3. **To access crisis and emergency application running in the cloud**

System architecture

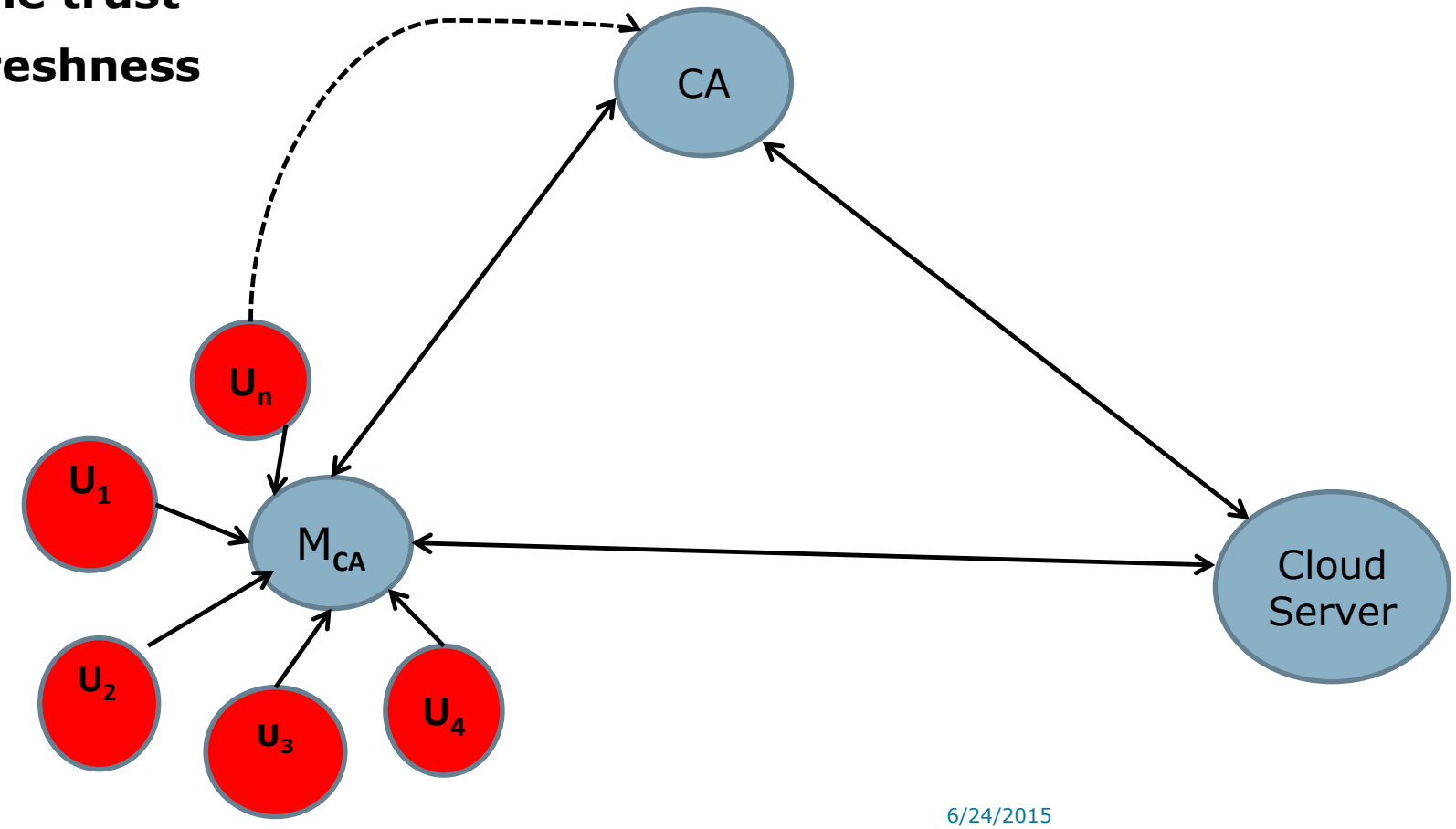


User Authentication

- Fundamental security building block
  - basic of access control & user accountability
- When communicating parties are concerned with the integrity and authenticity of messages
- The process of verifying an identity claimed by or for a system entity
  - Two steps:
    - identification: specify identifier
    - verification: verify entities' identifiers

The Key Factors in Authentication

- **Some secrets**
- **Or some trust**
- **And Freshness**



Digital Certificates

- **A digital certificate contains:**
  - **Identity details**
    - **Eg. Personal ID, web site URL**
  - **Public key of identity**
  - **Issuer (Certification Authority)**
  - **Validity period**
  - **Attributes**
- **The certificate is *signed* by the CA**

Digital Certificate

- **Certificate ≠ Signature**
  - **Certificate is *implemented using* signatures**
- **Certificate ≠ Authentication**
  - **Authentication *can* be *implemented using* certificates**
  - **Also for authorization/access control.**

Proposed Solutions for User authentication to the cloud

Authentication:
Mobile user sends a message to cloud and prove to cloud that he is the sender.

1. **Mobile users generate signatures and send them to the cloud.**
2. **Cloud verifies the signatures by users' public keys. Then the cloud send the verification result back to users.**

Authentication is ensured by signature and its verification.

Proposed Solutions for certificate issuing

- **Usability of users: make sure that users are still have access to the cloud after "M" is compromised.**
- **Reliability and security: the compromise of "M" can not lead the failure of the whole system.**
- **Solution for both issues mentioned above:**
  - **Use multiple "M"**
  - **Use threshold to generate users' certificates**
    - **Provide n-out-of-m security**

Conclusion

- **User authentication is important ingredient security service for mobile cloud system to verify if a smart phone user is legal through cloud server in emergency situation.**
- **A strong user authentication in mobile cloud contributes to efficient collection and sharing data since it increase trustworthiness of information share.**
- **The proposed user authentication scheme can be suitable for crisis and emergency application with security requirements in mobile cloud.**

THANK YOU!