

Background

- Assisted Living is a healthcare approach that benefits from transferring medical information monitored at home to clinicians over networks
- Reliability, Usability, Security, and Interoperability are required
 - Assisted persons and clinicians are technology naive

Drop-Box Architecture

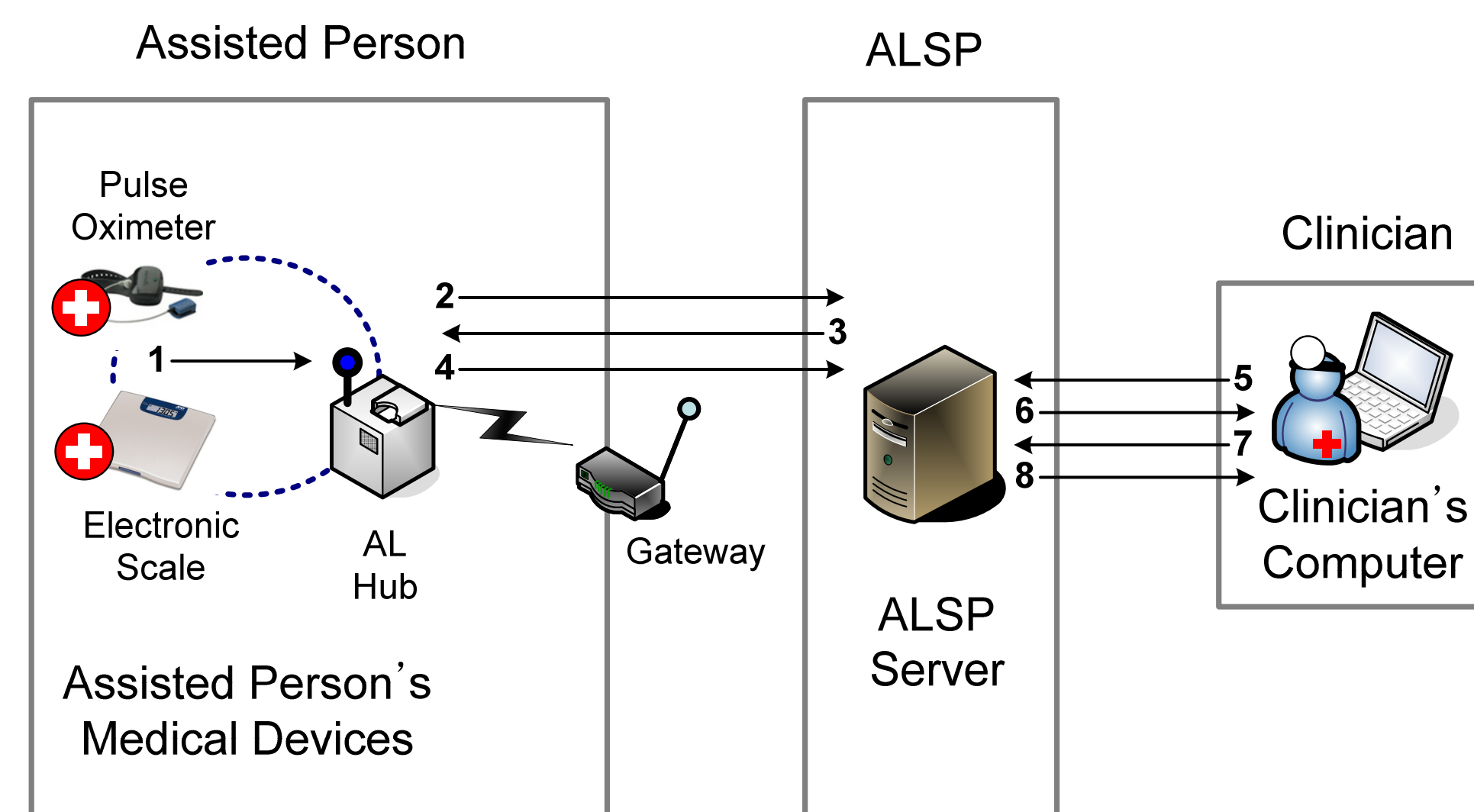
- Four types of participants: Assisted Person, ISP, Clinician, and Family or Friend
- Assisted Living Service Provider (ALSP), an intermediary between assisted person and clinicians
 - stores medical information
 - detects emergencies

- Assisted Living Hub (AL Hub) provides cryptographic functionalities for medical devices
 - Bootstrapping steps are investigated

Assumptions and Trust model

- All patients, clinicians, and family members participate honestly
- ALSP is a semi-trusted entity
 - performs authentication and encryption
 - (trusted in security aspect)
 - insider attack is possible
 - (not trusted in privacy purpose)

Architecture Diagram



Report protocol (Assisted Person <-> Clinician)

Msg1 $D \rightarrow H : n | chk(n) | t | s | m$

Msg2 $H \rightarrow G \rightarrow AS : U^{**}?$

Msg3 $AS \rightarrow G \rightarrow H : \Gamma_{AS}$

Msg4 $H \rightarrow G \rightarrow AS : \{ \{n | chk(n) | t | \delta\}_{K_{mi}} | (Family | \{K_{mi}\}_{K_P}) | (Doc | \{K_{mi}\}_{pub(\Gamma_{Doc})}) | \delta | m \}$
 $| K_{mo} \quad s:(pswd P_{PA}, r_1, t_1) enc:(K_{mo})$
 $s:(pswd P_{PA}, r_1, t_1) enc:(pub(\Gamma_{AS}))$

Msg5 $CC \rightarrow AS : V^{**}?$

Msg6 $AS \rightarrow CC : \Gamma_{AS}$

Msg7 $CC \rightarrow AS : \{from: Doc | about: Pat | get: new\} \quad s:(priv(\Gamma_{Doc}) enc:(pub(\Gamma_{AS}))$

Msg8 $AS \rightarrow CC : \{ \{n | chk(n) | t | \delta\}_{K_{mi}} | (Doc | \{K_{mi}\}_{pub(\Gamma_{Doc})}) | Pat | m \} \quad s:(priv(\Gamma_{AS}) enc:(K_o)$
 $| K_o \quad s:(priv(\Gamma_{AS}) enc:(pub(\Gamma_{Doc}))$

Protocols

- Two goals in protocols
 - For security, verify security against a Dolev-Yao style attacker (inject, intercept, or construct arbitrary messages)
 - For privacy, guarantee that an attacker cannot discover message contents and that the ALSP can not gain access to more information than it needs
- Report protocol (Pull)
- Alarm protocol (Push)

Protocol Verification

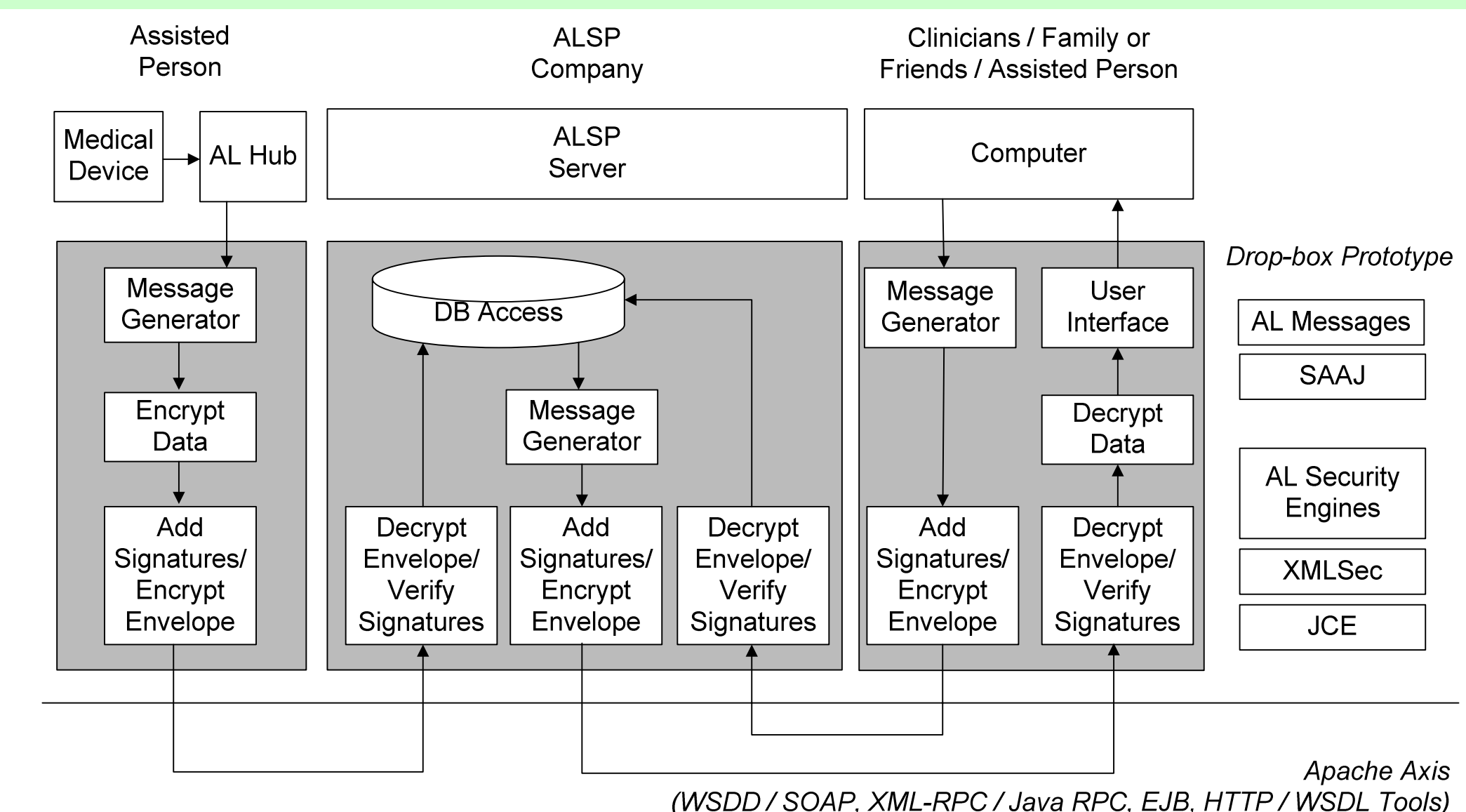
- Specified in TulaFale, Verified with ProVerif
- Proved security theorems

Theorem 3. (Secrecy) *If a patient sends a reading r encrypted for a doctor or family members, the attacker cannot discover it. This is true even the monitoring service reveals all of its secrets and intermediate information to the attacker*

Corollary 1. (Secrecy) *If a patient sends a reading r encrypted for a doctor or family members, the monitoring service cannot discover it*

Implementation

- Implemented a testbed based on Web Service standards



Contributions and Future Work

- Developed workflows and protocols
- Verified secrecy properties
- Authentication and Access Control studies are in progress

To learn more, Google "Illinois Security Lab"