Securing Smart Home Devices against Compromised Cloud Servers

Rahmadi Trimananda, Ali Younis, Thomas Kwa,
Brian Demsky, and Harry Xu

UCI UCLA

Introduction

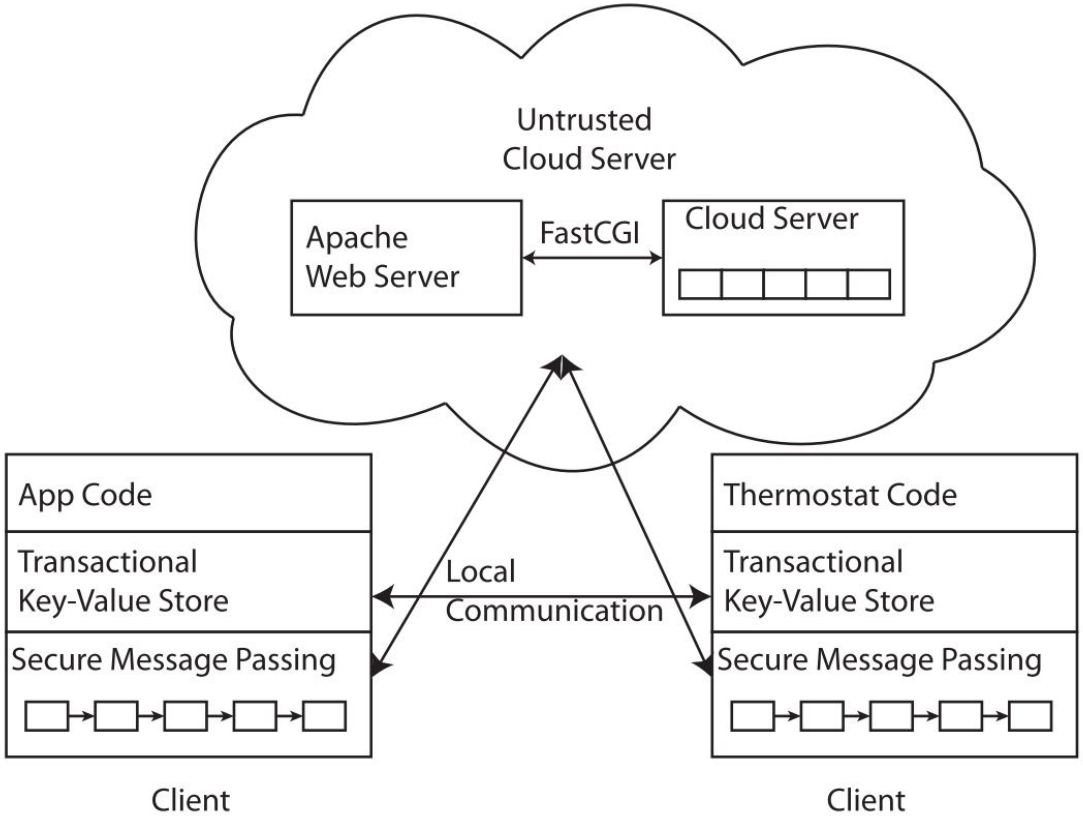
- Client-side security
  - Extensive research
- Cloud-side security
  - Less explored
  - Feasible to mount attack *at scale*

Assumptions

- Three parties
  - cloud – device – smart phone
- Assume untrusted cloud server
- Connectivity of any number of
  - smart home devices
  - smart phones

UCI UCLA

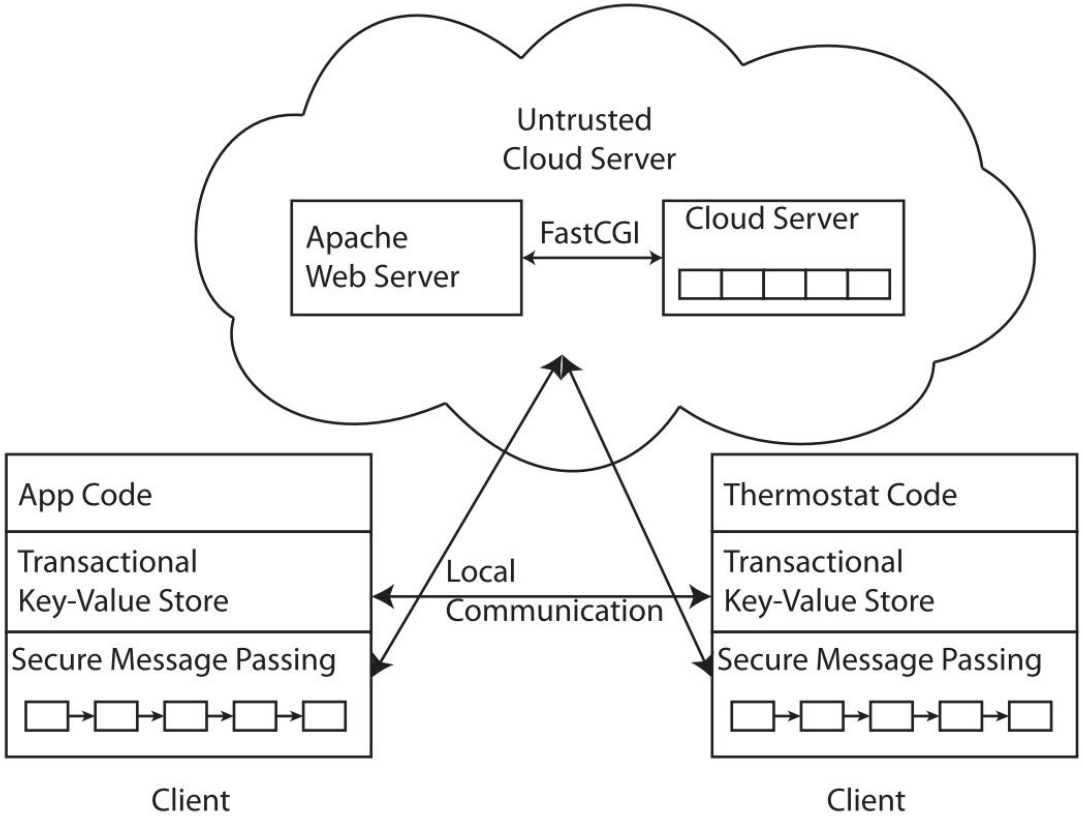
Fidelius System



- Transactional programming model
- Two layers
  - Message passing
  - Transactional Key-Value store
- Local control

UCI UCLA

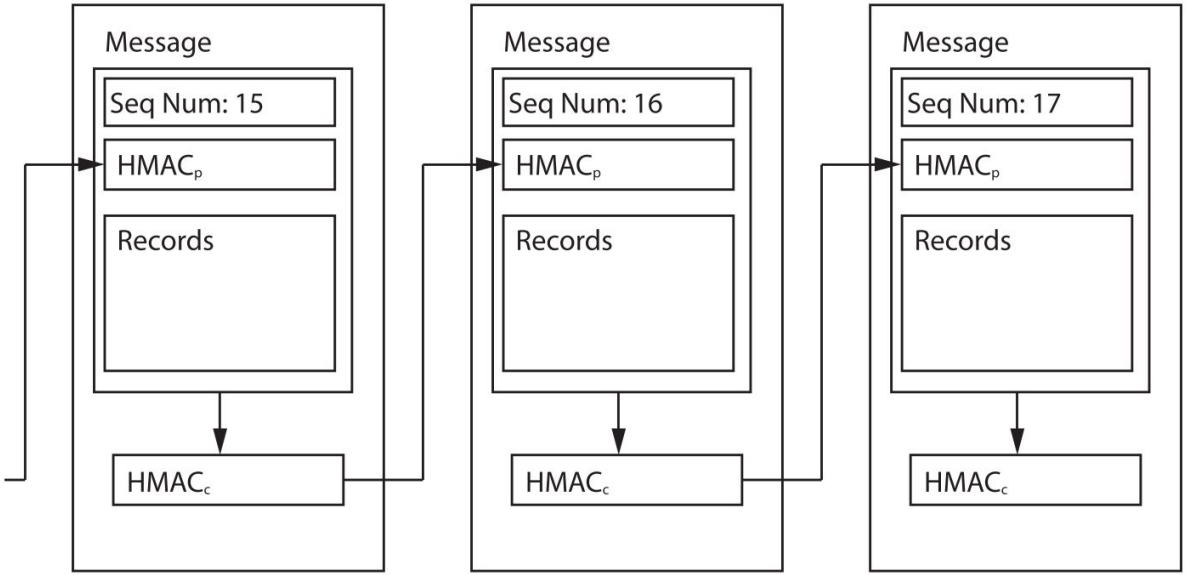
Fidelius System



- Oblivious privacy
- Integrity of the message passing layer

UCI UCLA

Message Chain



Records

- KV-store
- Last message
- Rejected message
- Queue size

UCI UCLA

Evaluation

- Acceptable overhead
- Reduces 50% communication time
- Around 2X battery life
- Comparison to PyORAM
  - 4-7X faster access
  - 25-43X less data transferred

Conclusions

- **Fidelius**: secure key-value store
- Good performance
- Low power consumption
- Resilient to attacks
- Efficient on smart home class hardware

Feedback

- Key distribution among devices
- Encryption is heavy for IoT devices
- Fidelius for current cloud trends? Analytics?
- Securing timing channels

Thank You!

Paper and software

http://plrg.ics.uci.edu/fidelius/

Rahmadi Trimananda (**rtrimana@uci.edu**)

UCI UCLA

Evaluation

- Test bed
  - 15 Particle Photons (temperature/humidity, magnetic door, and motion sensors)
  - 2 LiFX light bulbs
  - Raspberry Pi as arbitrator node

UCI UCLA