Poster: Securing Smart Home Devices against Compromised Cloud Servers

Rahmadi Trimananda, Ali Younis, Thomas Kwa, Brian Demsky
University of California, Irvine

Harry Xu
UCLA

In contrast to extensive research on client-side smart home security, the security of the cloud servers that control these client-side devices has received less attention from researchers. This is particularly concerning—e.g., recent work shows that if an attacker can control enough high-wattage IoT devices, the attacker can cause power grid failures [4]. Implementing attacks *at scale* by compromising individual smart home devices is not straightforward due to the sheer number of devices that must be hacked. Thus, compromising cloud servers can be a more practical approach. In fact, the year of 2018, alone, has seen a huge number of compromises to cloud servers, including those operated by many well-known companies (*e.g.*, Facebook [3], Sony [7], Target [5] etc.)

In addition to large-scale attacks on physical infrastructures, there are other concerns with trusting the cloud: (1) *Privacy:* Smart home devices collect a great deal of information about users [6]. Private data can be leaked if a cloud server is compromised. (2) *Traffic Analysis:* It may be possible to learn information by observing traffic patterns [1]. For example, such an analysis could reveal that when the thermostat's mode transitions (*e.g.*, from *Home* to *Away*), it always sends a packet of a specific length [2]. By watching traffic, attackers could discover whether people are home.

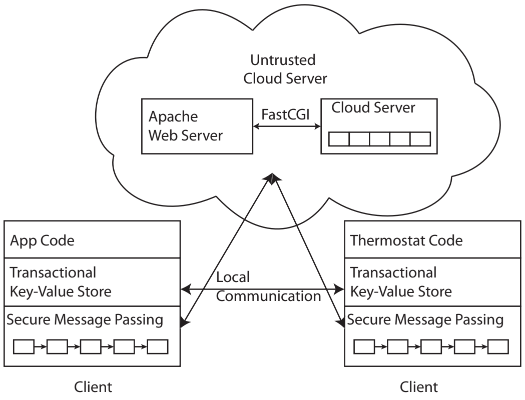

Figure 1: System Overview

Our Approach: FIDELIUS Motivated by these security and privacy concerns, this paper presents FIDELIUS. FIDELIUS provides consistency and security to smart home devices even in the presence of compromised servers in realistic smart home environments that include the presence of intermittent network accesses. Figure 1 presents an overview of the FIDELIUS system. A FIDELIUS deployment consists of (1) an untrusted cloud-based server that provides connectivity between clients, (2) any number of clients that are smart home devices, and (3) any number of clients that are smartphone apps. Our server implementation is architected as a FastCGI server that communicates with the Apache Web Server. We focus our work on providing a secure *key-value storage system* targeted at IoT applications. While existing systems use adhoc protocols for communicating data, the standard *key-value abstraction* is powerful enough to subsume a wide-range of adhoc protocols. We do not impose special requirements on server hardware; instead, the FIDELIUS enforcement runs on *each client device*. Clients communicate with the server; in the absence of Internet connectivity, they can also communicate with each other locally to maintain functionality. This design is well matched for the smart-home environment where devices are mutually connected in a local home network.

Our work makes the following contributions:[1]

- **Secure Transactional Key-Value Store:** It presents a key-value store that provides strong security and privacy guarantees even if the server is malicious.
- **Local Control:** It presents an algorithm supporting local control of smart home devices when connectivity is lost.
- **Transactional Programming Model:** It presents developers with a transactional model to abstract consistency and availability tradeoffs that arise from network partitions.
- **Evaluation:** Compared to Particle.io, FIDELIUS reduces more than **50%** of the data communication time and increases battery lifetime by **2**×. Compared to PyORAM, FIDELIUS has **4-7**× faster access times with **25-43**× less data transferred.

[1] FIDELIUS is released at http://plrg.ics.uci.edu/fidelius/.

References

[1] N. Apthorpe, D. Reisman, and N. Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. *CoRR*, abs/1705.06805, 2017.

[2] B. Copos, K. Levitt, M. Bishop, and J. Rowe. Is anybody home? Inferring activity from smart home network traffic. In *Security and Privacy Workshops (SPW), 2016 IEEE*, pages 245–251. IEEE, 2016.

[3] M. Isaac and S. Frenkel. Facebook security breach exposes accounts of 50 million users. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html, September 2018.

[4] S. Soltan, P. Mittal, and H. V. Poor. Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 15–32, Baltimore, MD, 2018. USENIX Association.

[5] G. Wallace. Target credit card hack: What you need to know. https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html, December 2013.

[6] Z. Whittaker. Smart home tech makers don't want to say if the feds come for your data. https://techcrunch.com/2018/10/19/smart-home-devices-hoard-data-government-demands/, 2018.

[7] Sony pictures hack. https://en.wikipedia.org/wiki/Sony_Pictures_hack.