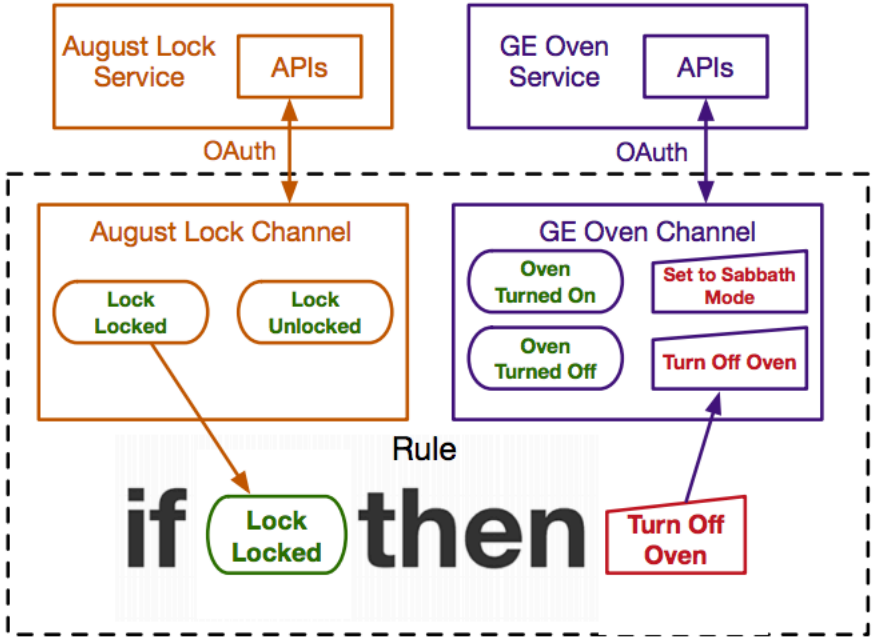
Decentralized Action Integrity for Trigger-Action IoT Platforms

Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash

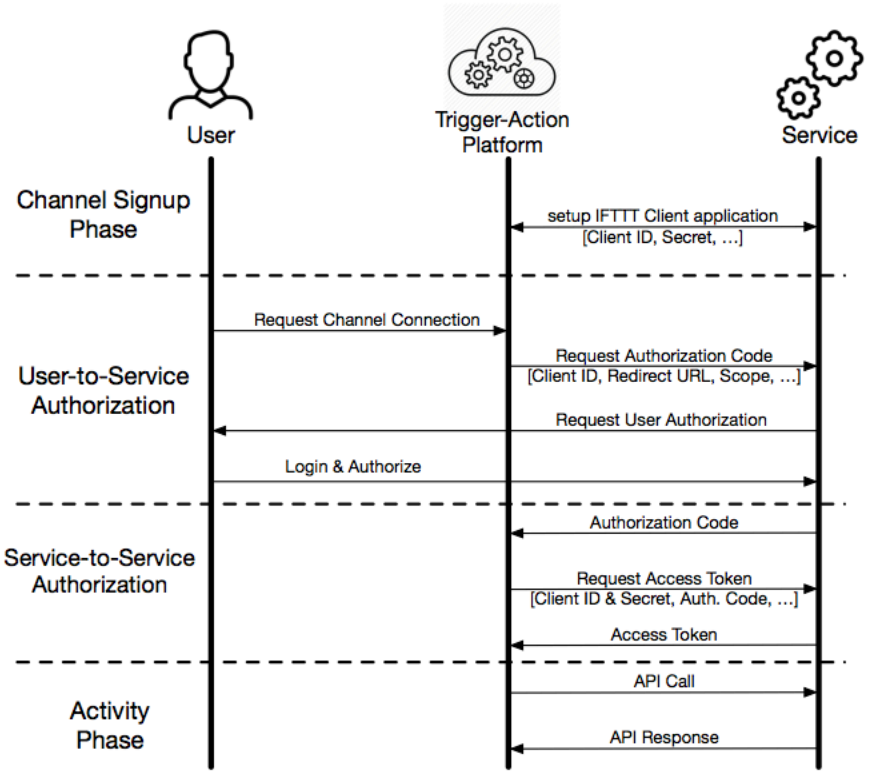
Background

- Channel
  - online service's set of APIs on the trigger-action platform
- Trigger
  - Events that occur in the associated online service
- Action
  - functions that exists in the API of the online service
- Rule
  - A rule stitches together various channels to achieve useful automation
  - If "alarm is on", then "turn off my oven"

Background


August Lock Service
APIs
GE Oven Service
APIs
OAuth
OAuth
August Lock Channel
Lock Locked
Lock Unlocked
GE Oven Channel
Oven Turned On
Set to Sabbath Mode
Oven Turned Off
Turn Off Oven
Rule
if
Lock Locked
then
Turn Off Oven

Authorization Model



Security Implications

- Platform Compromise
- OAuth Token Compromise
- Overprivilege
  - coarse-grained scopes
  - balancing usability and security

Threat Model

- Trigger-action platform is untrusted
- Attacker can leak Oauth tokens
- Attacker can manipulate triggering data
- Online services are not compromised

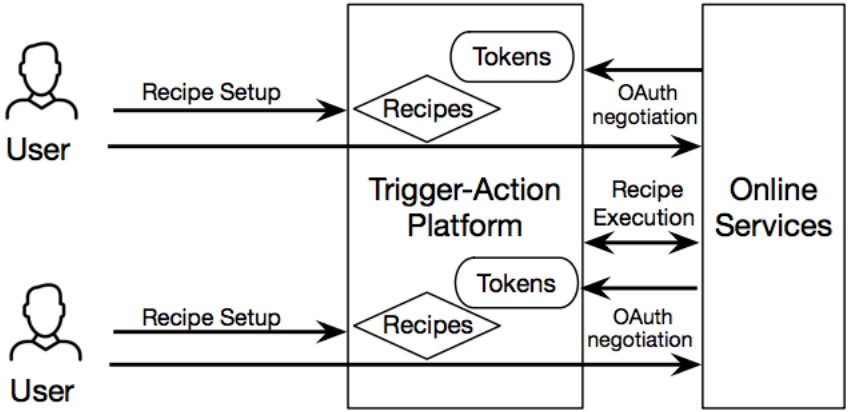
Design Space Exploration

- Short-lived Oauth Tokens
- Fine-Grained Tokens and Per-Rule Permission Prompts
- Avoiding Bearer Tokens
- Fully Decentralized Platform Construction
- Rule Analytics/Anomaly Detection

Decentralized Action Integrity

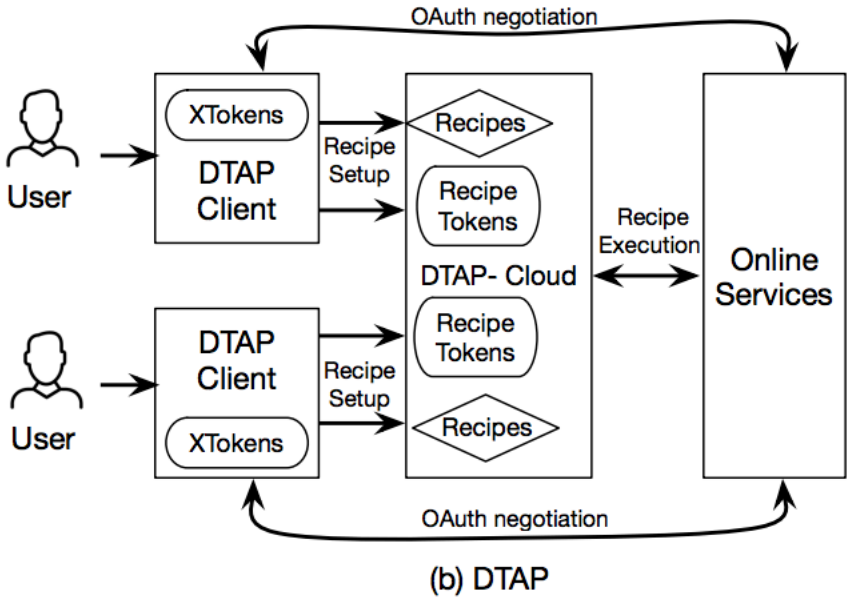
- Rule-specific Oauth tokens
- Timely and verifiable triggers
- Data integrity
- Decentralized tokens

Decentralized Action Integrity



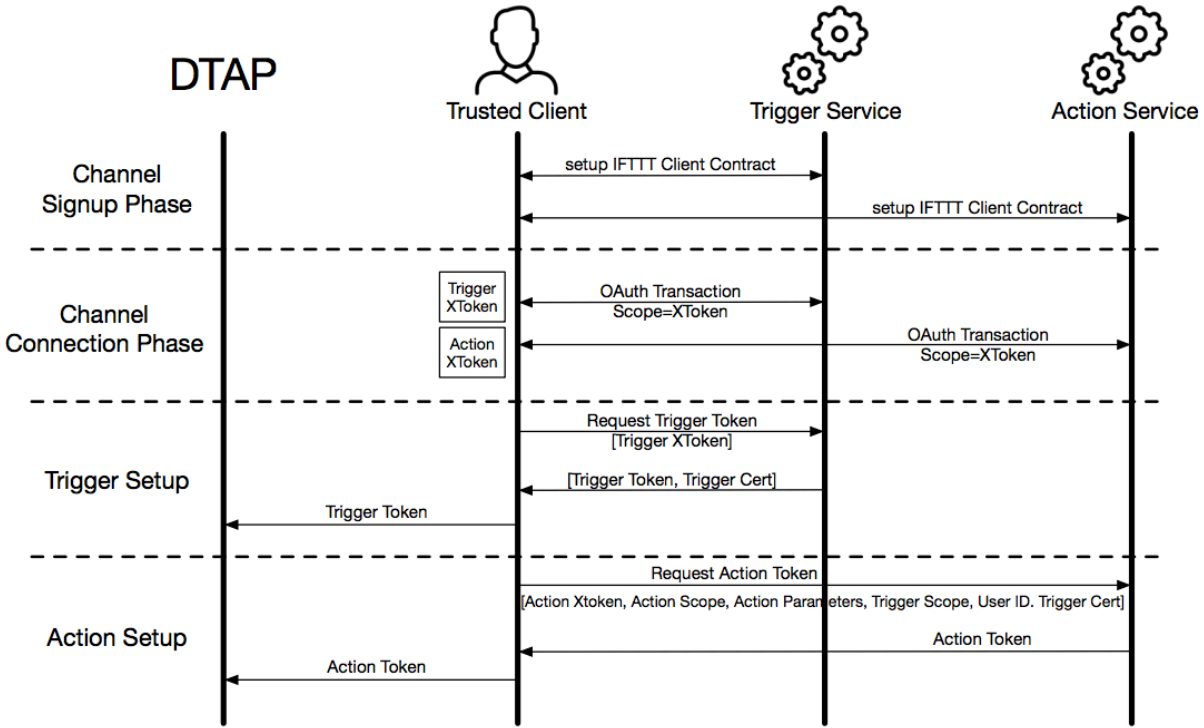
(a) Insecure Trigger-Action Platform

Decentralized Action Integrity



(b) DTAP

Decentralized Action Integrity



Security Properties of DTAP

- Action Function Misuse Prevention
- Trigger Misuse Prevention
- Trigger Data Integrity
- Recipe Deletion
- No single Point of Failure

Evaluation

- Storage Overhead
  - 3.5KB per rule
- Transmission Overhead
  - 6~11 %
- Developer Effort
  - library provided