Securing Trigger-Action Platforms

Earlence Fernandes*
Amir Rahmati*
Jaeyeon Jung
Atul Prakash

* Work started while at the University of Michigan
If Trigger-Condition Then Action

• Web-based systems that are increasingly popular in smart home/IoT settings
  • If new NASA Instagram pic, Then send me email
  • If 9PM, Then close the door
• End-user programming
IF smoke detected, THEN turn off oven

Integrates with 300+ Online Services (IoT and non-IoT)

11 Million Users, 54 Million Trigger-Action Rules
IF IFTTT is compromised, THEN ...

Attackers can use OAuth tokens to do whatever they want
How can we architect a trigger-action platform whose compromise does not permit attackers to invoke actions arbitrarily?
Decentralized Action Integrity

Assume: Trigger-Action platform is compromised

If “smoke is detected” Then “turn off my oven”

Attacker cannot create false triggers or re-use triggers from past executions

Execute: (1) ONLY this action and (2) ONLY when the corresponding trigger is true

Verifiable and Timely Triggers

Rule-Specific Tokens
Decentralized?

Trigger-Action Platforms Today

Long-Lived OAuth tokens of all users

All users must completely trust this

A user only trusts its own client

Our Proposed Platform

Rule-Specific Tokens

Users do not trust this

...
Securing Trigger-Action Platforms

Even if a trigger-action platform is compromised, an attacker can only: (1) execute existing user rules correctly or (2) prevent execution of those rules

https://iotsecurity.eecs.umich.edu

* Work started while at the University of Michigan