Published in NDSS, 2018

Decentralized Action Integrity for Trigger-Action IoT Platforms

By Fernandes et al.

January 2020

Outline

Background

Trigger-Action platforms

Problems - Mitigations

DTAP design

Limitations

Summary

Background

- Many researchers have focused on the different trigger and action channels used by IFTTT users
  - IFTTT → If-This-Then-That
- Other works tried to determine the risks that users face due to errors in rule creation
- Studies have shown that the majority of deployments of OAuth in Android apps are vulnerable
- The notion of XTokens is inspired by Kerberos's single sign-on protocol
  - "Ticket granting tickets" are used to acquire "service tickets" to prove the user's identity to services

Motivation

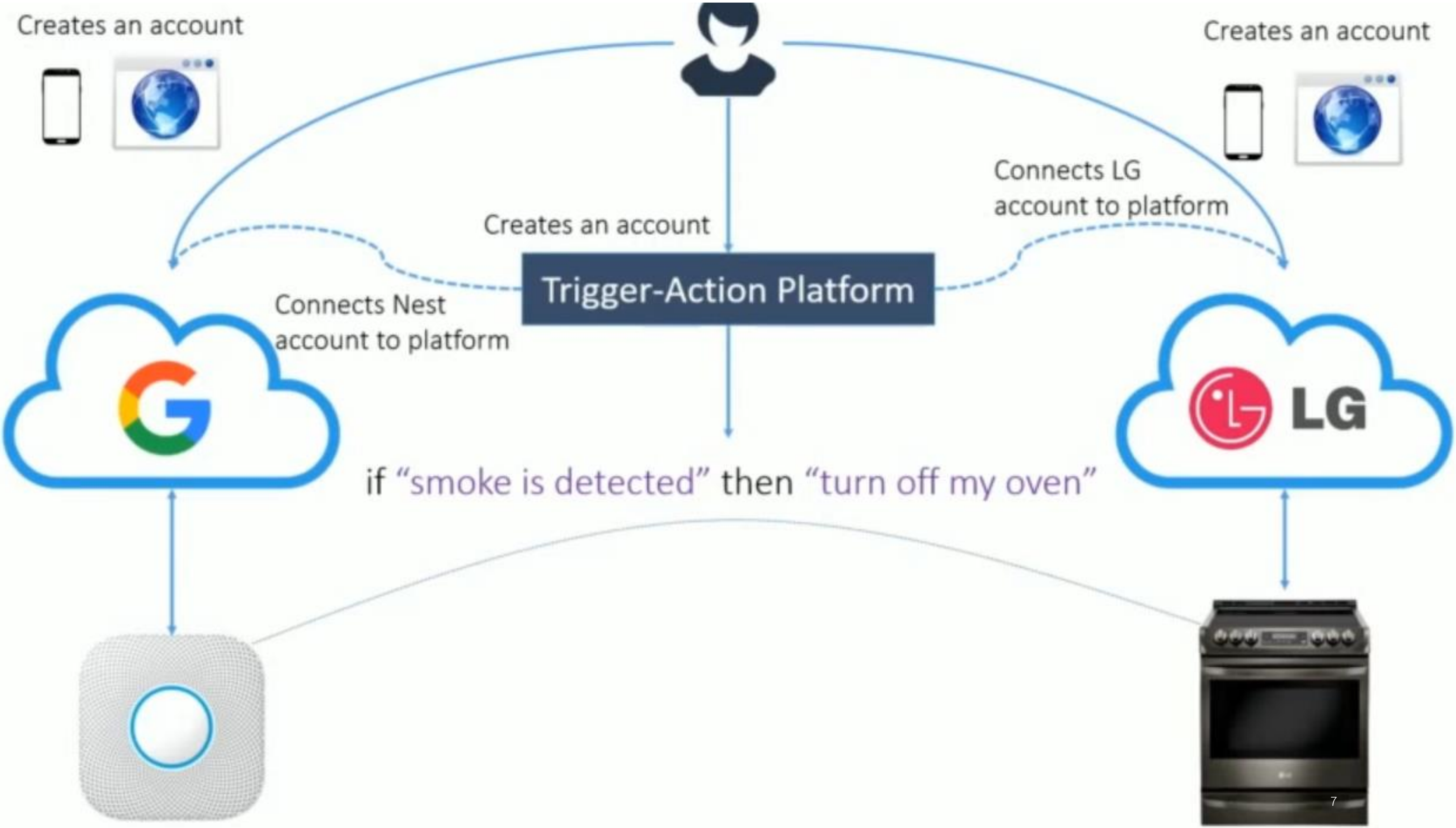
- How an incorrect deployment of OAuth protocol can affect the security properties of trigger-action platforms.
  - What will happen if these tokens are overprivileged?
- Prevent attackers from stealing OAuth tokens and executing actions at will
  - Independently of user rules

Contribution

- A security principle that prevents an untrusted trigger-action platform from misusing compromised OAuth tokens
- Designed and implemented the Decentralized Action Integrity
  - Based on rule-specific OAuth tokens with decentralized verifiable triggers
  - Uses the XToken, a way to gain the power of fine-grained tokens without losing the usability benefits of coarse-grained tokens
  - Backwards-compatible with OAuth protocol
- DTAP is the first decoupled trigger action platform supporting Decentralized Action Integrity

What is a Trigger-Action platform?

- A class of web-based systems that stitch together a number of online services
- Provide users the ability to set up automation rules
  - E.g., “If I post a picture to Facebook, save this picture to my OneDrive account”
- Such platforms have added automation support for physical devices
  - E.g., “If there is an alarm, turn on the lights



Creates an account

Creates an account

Creates an account

Trigger-Action Platform

Connects Nest account to platform

Connects LG account to platform

if “smoke is detected” then “turn off my oven”

Trigger-Action platforms are targets

- Trigger-Action platforms support a wide variety of business and IoT use-cases, using a logically monolithic design
  - If attackers compromise the platform, they will be able to leak OAuth tokens for all users

- These platforms have privileged access to users’ online services and physical devices

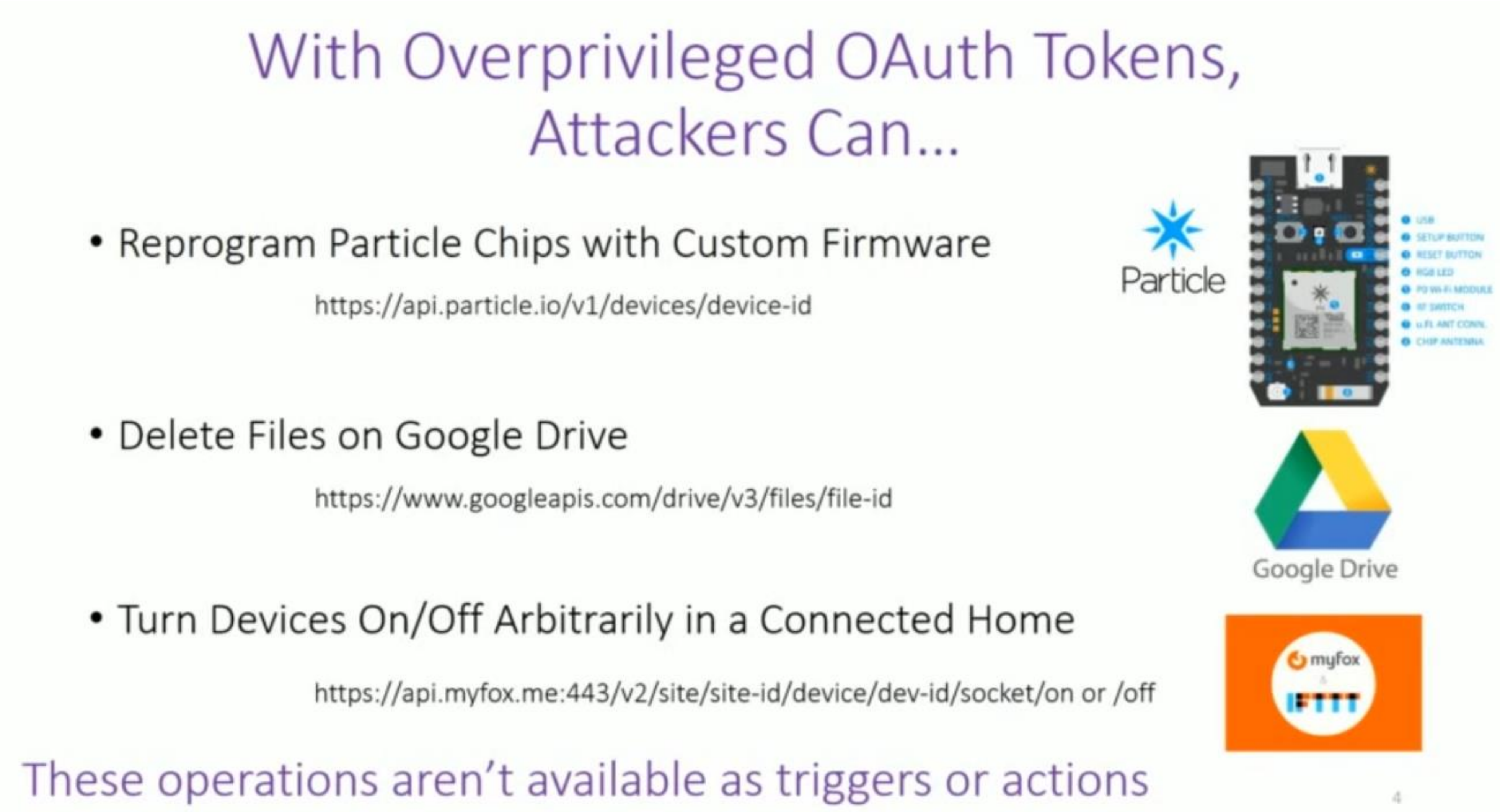
- If they get compromised, attackers can arbitrarily manipulate data and devices belonging to a lot of user

Research Question

How can we guarantee that actions are executed according to user rules in an untrusted trigger-action platform?

Initial research

- A survey of 7 trigger-action platforms with over 11 million users
- Cloud services are still not immune to persistent and sophisticated attacks
- The overprivilege in the OAuth tokens enable the attacker to invoke API calls that are outside the abilities of the trigger-action platform itself.



With Overprivileged OAuth Tokens, Attackers Can…

- Reprogram Particle Chips with Custom Firmware

  https://api.particle.io/v1/devices/device-id

- Delete Files on Google Drive

  https://www.googleapis.com/drive/v3/files/file-id

- Turn Devices On/Off Arbitrarily in a Connected Home

  https://api.myfox.me:443/v2/site/site-id/device/dev-id/socket/on or /off

These operations aren’t available as triggers or actions

Threat model

- Assume that the platform is not trusted, and can be compromised
- Assume that online services are not compromised
- An attacker can leak OAuth tokens and attempt to invoke actions arbitrarily
- An attacker can manipulate any triggering data passing through the platform

- The model DO NOT prevent:
  - DoS attacks
  - Leakage of sensitive data

They could try …

BUT non of the designs prevent a compromised platform from arbitrarily manipulating data and devices

Short – lived OAuth tokens?

- Require many refresh calls
  - Reduces the useful attack window
- Depends on the existence of a separate signaling mechanism

Rule Analytics/Anomaly Detection?

- After-the-fact, damage is done
- Does not address root cause

Fully Decentralised Platform?

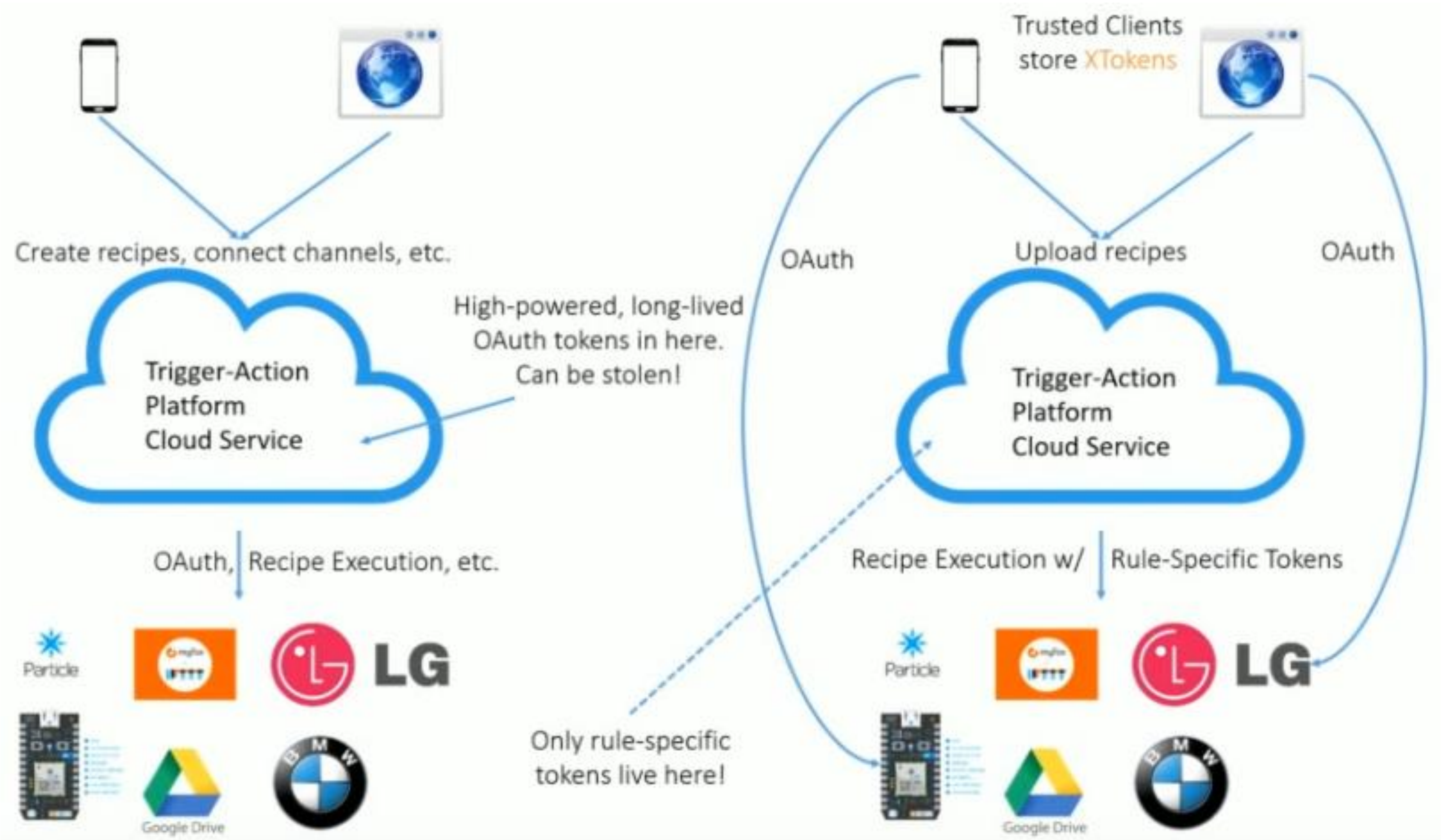
- Provides functionalities to each user through a client that executes rules on their own machine
  - Trigger-action platform is not a single valuable target anymore
  - It does not provide the benefits of a cloud services (e.g., availability, fault tolerance)

Finely – Grained Tokens?

- Platforms request tokens when users program rules
  - The platform only has the amount of privilege necessary to execute rules
- Usability problems
  - Increases the number of permissions prompts for users

Insecure Platforms vs DTAP

- Storing overprivileged tokes in the cloud,
- Each user uses a DTAP client to secure his token
- Trusted clients negotiate OAuth tokens, recipes, XTokens
- DTAP guarantees that no other action other than the specified in the recipes can be performed using the recipe-specific token
- A compromise of DTAP cloud does not affect the clients
- DTAP clients are not created/managed by the DTAP cloud

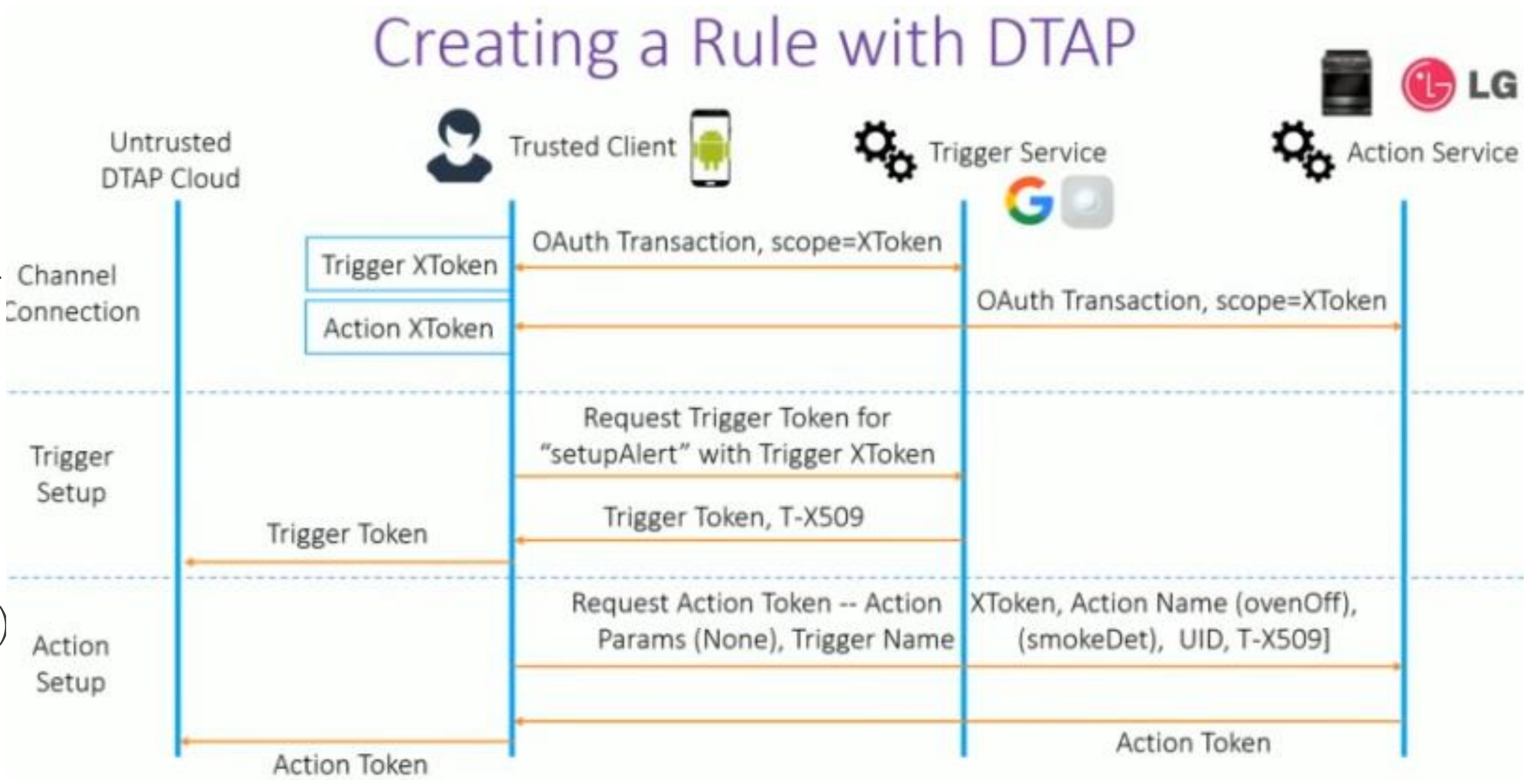

Create recipes, connect channels, etc.
Trigger-Action Platform Cloud Service
High-powered, long-lived OAuth tokens in here. Can be stolen!
OAuth, Recipe Execution, etc.
Particle
LG
Google Drive
Trusted Clients store XTokens
OAuth
Upload recipes
OAuth
Trigger-Action Platform Cloud Service
Recipe Execution w/ Rule-Specific Tokens
Only rule-specific tokens live here!
Particle
LG
Google Drive

The principle of Decentralized Action Integrity

- The concept must comply with the following elements:
  - Rule-specific OAuth tokens
    - “IF smoke is detected THEN turn off oven.
      - The platform needs two different OAuth tokens.
  - Timely and verifiably triggers
    - Execute an action function if it can prove that the corresponding triggering event was true within a reasonable time period
  - Data integrity
    - IF new NASA Instagram post, THEN save the picture to my Dropbox
      - A compromised cloud service of the platform should not be able to replace the Instagram image with malware
  - Decentralized tokens
    - The compromisation of the platform does not mean that the all the tokens are leaked

DTAP authorisation

- The client obtains scope-to-function maps for every online service
- Then they setup up triggering events (e.g. If there is smoke..)
- These tokes are used to request rule-specific tokens



Creating a Rule with DTAP

LG
Untrusted DTAP Cloud
Trusted Client
Trigger Service
Action Service
Channel Connection
Trigger XToken
Action XToken
OAuth Transaction, scope=XToken
OAuth Transaction, scope=XToken
Trigger Setup
Request Trigger Token for "setupAlert" with Trigger XToken
Trigger Token, T-X509
Trigger Token
Action Setup
Request Action Token -- Action Params (None), Trigger Name
XToken, Action Name (ovenOff), (smokeDet), UID, T-X509]
Action Token
Action Token

Decentralized Action Integrity

- Attackers who control a compromised trigger-action platform :
  - Can only invoke actions and triggers needed for the rules that users have created
    - They should prove to an action service that the corresponding triggered occurred in the past
- To provide a proof that tokens were not misused, the principle places verification checks for misuse of OAuth tokens at the endpoints (e.g., online services) of the system
- A compromise of the platform does not leak tokens of all the users

Limitations

- DTAP only allows a user to use a single trusted client at a time
  - The protocol itself does not preclude multiple clients
- XToken is a high-powered credential. A malicious client can still leak this credential
  - But this will affect only one user and not the whole system
- An attacker can gain access to sensitive data simply by passively recording rule execution
  - Data passing through the DTAP-cloud need encryption

Results

- DTAP enables fine-grained control and good descriptiveness of the permissions used
- Storage overhead:
  - Each DTAP rule creates a 3.5 KB overhead in addition to the 0.8 KB required to store the XToken
- Transmission overhead:
  - DTAP created 6 – 11% overhead (even when using 10 parameters). This overhead does not exceed 7.5 KB
- End-to-End latency:
  - Excluding the network latency, the maximum verification overhead is less than 15ms.
- DTAP protocol has not been formally verified yet

Summary

- Trigger-Action platforms work by gaining privilege to access user data and devices in the form of OAuth tokens
- DTAP, the first trigger action platform supporting Decentralized Action Integrity
  - Provides guarantee that even if the OAuth tokens of a trigger-action platform are stolen, the attack cannot misuse the tokes.
  - Only if they can prove that the triggering condition was true for a given rule
- The design introduces the notion of an XToken coupled with rule-specific tokens and a cryptographic extension to the OAauth 2.0 protocol

Thank you!

QUESTIONS?