野村総合研究所

IETF 90 OAuth WG

OAuth Symmetric Proof of Possession for Code Extension

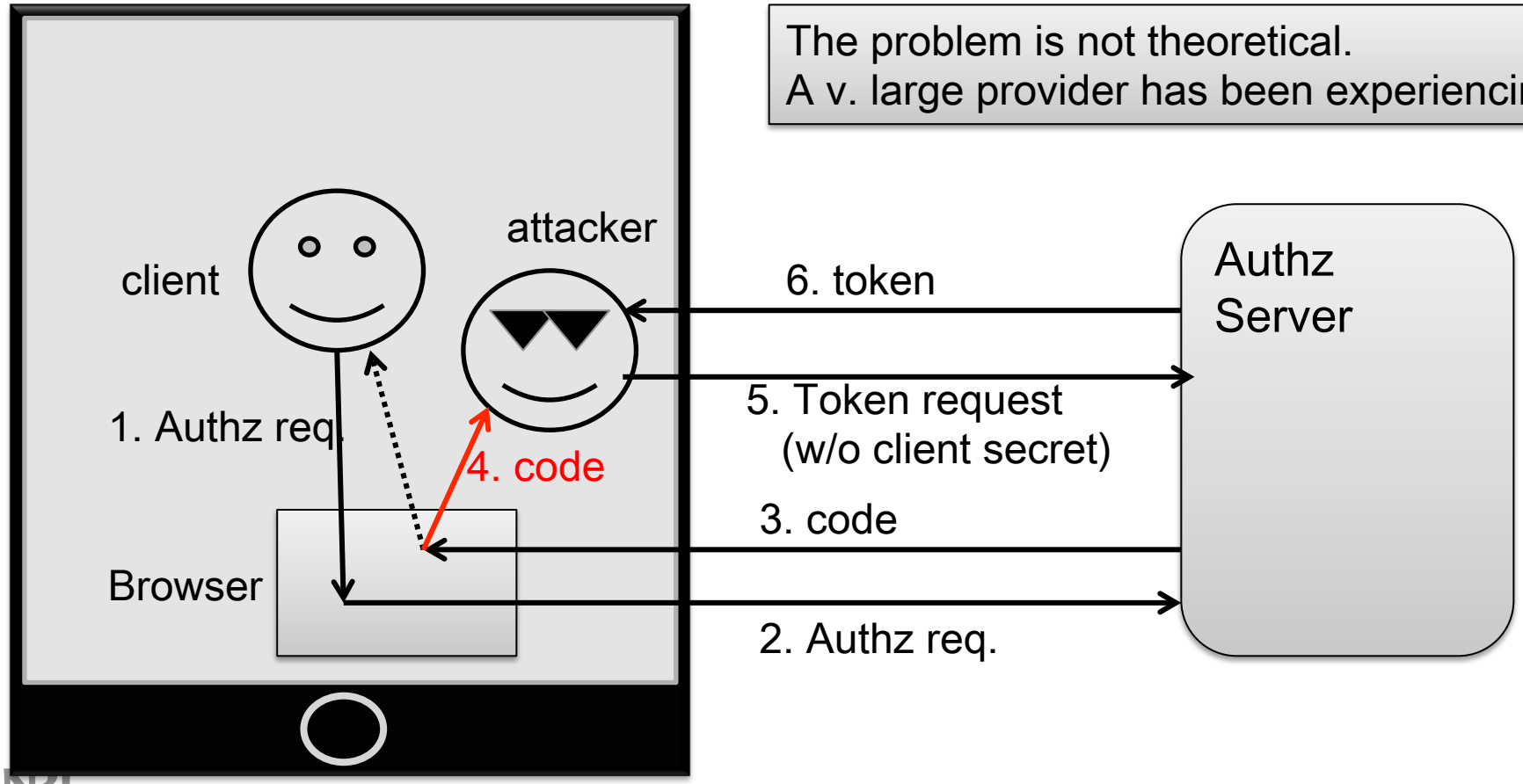
draft-sakimura-oauth-tcse-03

2014/7/24

Nat Sakimura
Nomura Research Institute, Ltd.

Problem Statement

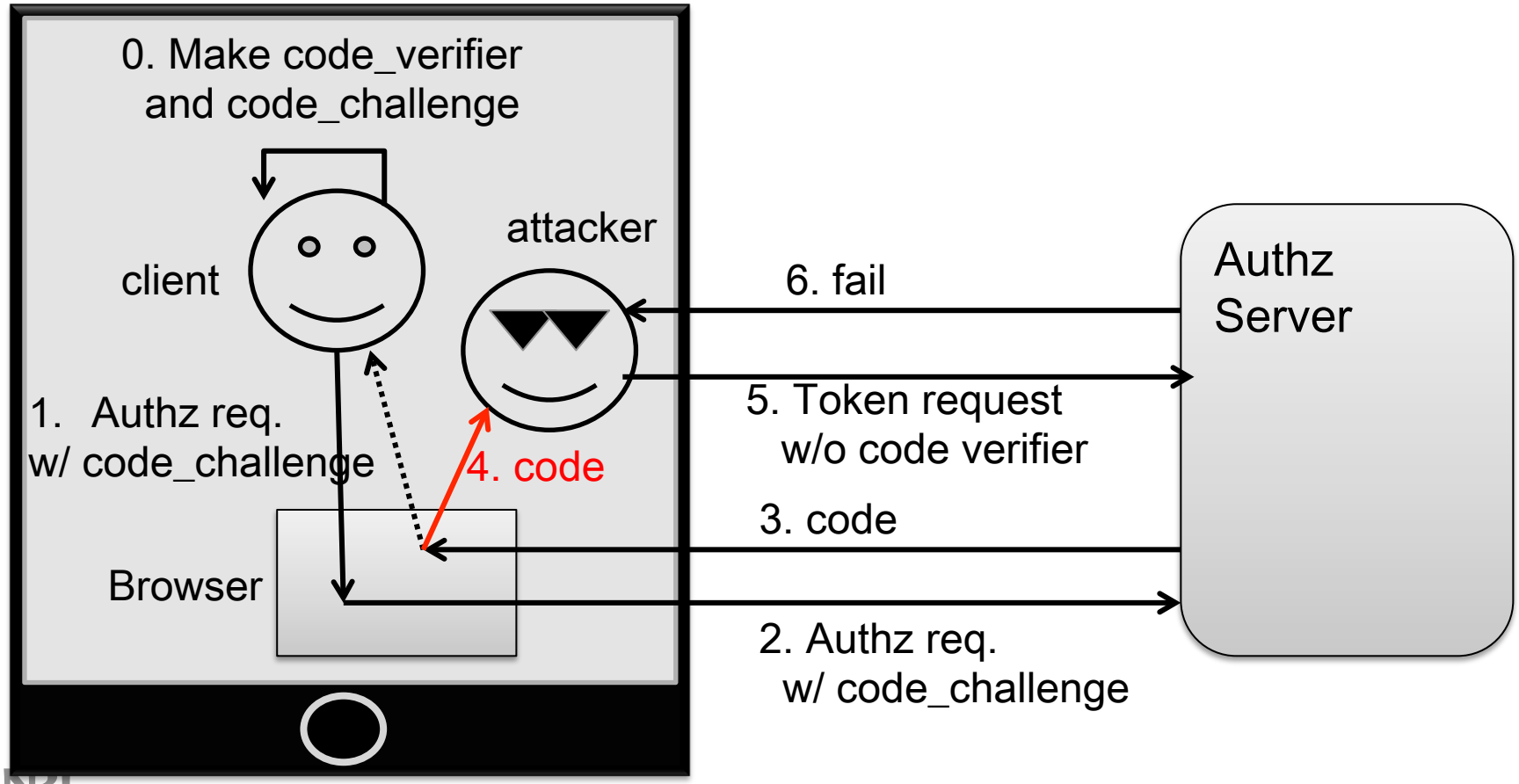
- Code interception attack (against public clients)
  - A malicious client gets the code instead of the client via registering the same scheme as the client, etc.



The problem is not theoretical.
A v. large provider has been experiencing it.

Solution

- Have the client create a one-time-credential and send it with the Authz req.
  - Based on the assumption that attacker cannot observe the request.



FAQ

- Why does it not use asymmetric crypto?
  - We first proposed it but was turned down by the developers.
- Why not require HMAC at least?
  - It is a good idea to do so in the environment in which the request can be monitored/captured by other apps.
  - We ran the idea to the app developers but it was not popular.

Draft is short and has been pretty stable

- Only 8 pages including boilerplates.
- Has been very stable.

OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: ~~April 22,~~ October 23, 2014

N. Sakimura, Ed.
Nomura Research Institute
J. Bradley
Ping Identity
N. Agarwal
Google
~~October 19, 2013~~
April 21, 2014

OAuth Symmetric Proof of Posession for Code Extension
~~draft-sakimura-oauth-tcse-02~~
draft-sakimura-oauth-tcse-03

Abstract

The OAuth 2.0 public client utilizing authorization code grant is susceptible to the code interception attack. This specification describe a mechanism that acts as a control against this threat.

- The concept has been battle tested.
- Adopt it as a WG item and finish it quickly?