Building Privacy-Preserving Cryptographic Credentials From Federated Online Identities

APR 19TH, 2016

论文下载

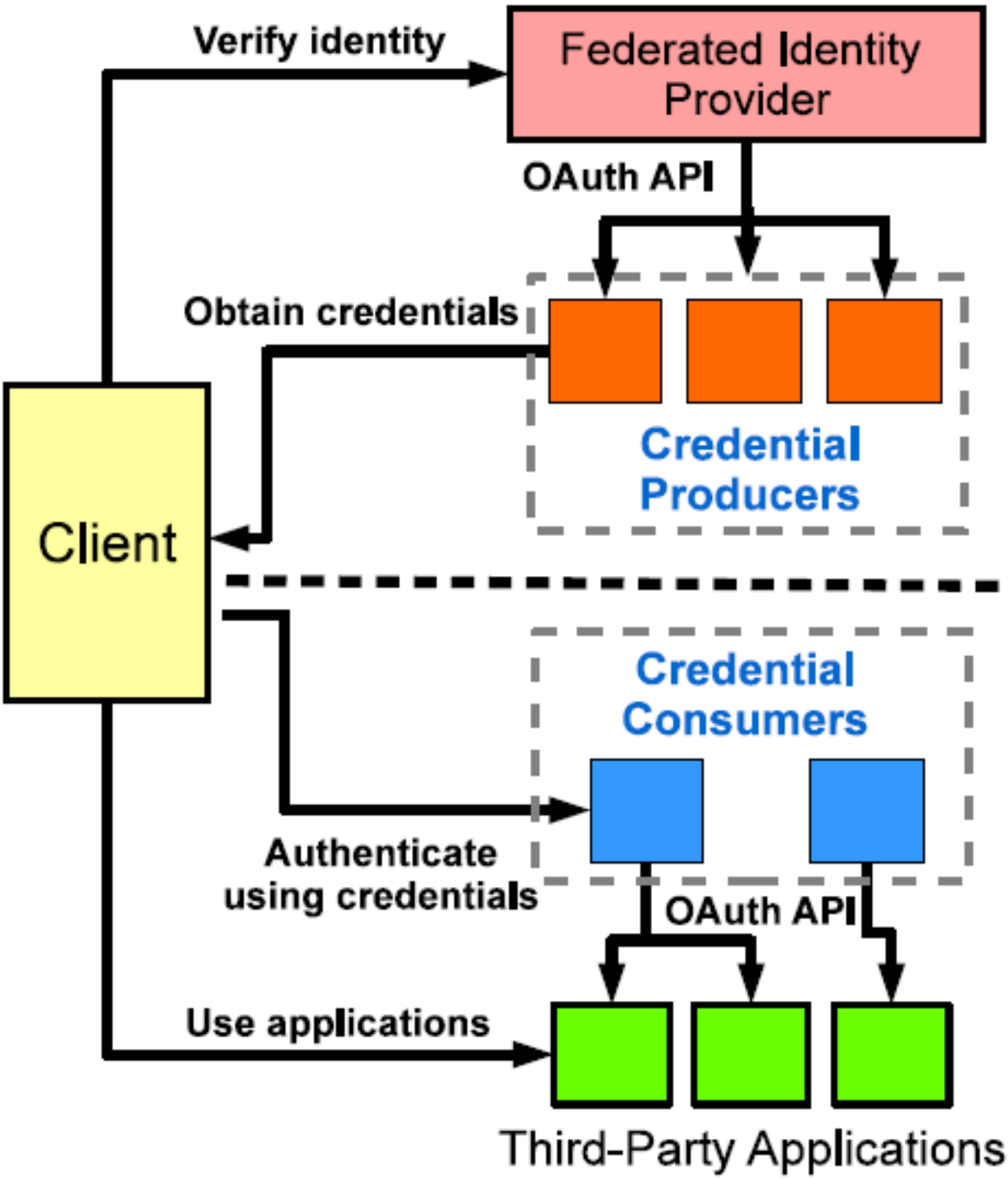
Abstract & Introduction

- 这篇文章提出了Crypto-Book方案，用于解决跨站认证过程（SSO）中的隐私泄露和追踪问题。
- 贡献主要有4点：
  - 提出了一种现实可行方案能够在SSO中提供隐私保护。
  - 提出了多种插件化的认证凭据方案可以支持不同级别的隐私和匿名性。
  - 认证凭据来自多个不同的身份提供商，避免了单个身份被攻破带来的安全问题。
  - 对本系统的现实可行性进行了充分的评估。

Privacy Concerns

- 身份提供商能够了解到用户需要登录的每个网站，以及他们登录的时间点。
- 第三方应用能够了解到用户的真实身份，包括许多重要信息如朋友列表、地理位置等。
- 第三方应用能链接用户的信息，跨应用的（？），然后出售给广告商。
- 如果用户的一个联合身份账号被攻破，攻击者能够用它登录第三方应用。

Overview & Methodology


Verify identity
Federated Identity Provider
OAuth API
Obtain credentials
Credential Producers
Client
Credential Consumers
Authenticate using credentials
OAuth API
Use applications
Third-Party Applications

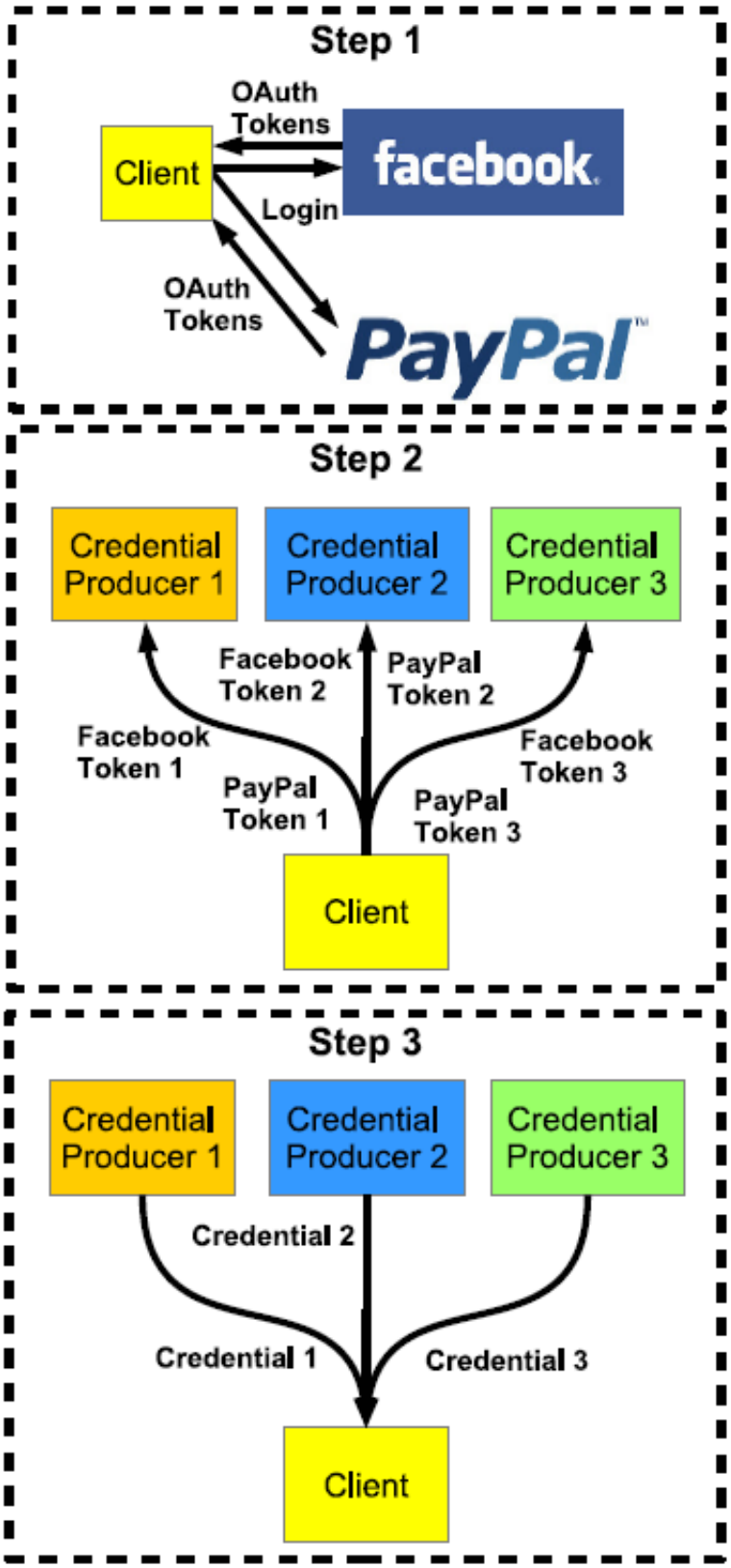


Figure 2: Client collects credentials from multiple credential producers.

- Privacy Goals: (1) Anonymity; (2) Unlinkability; (3) Accountability.

- Credential Producers：扮演传统第三方角色搜集用户信息并产生Credentials.
- Credential Consumers：把producer产生的credentials映射到化名上去用于第三方应用认证用户。
    - OAuth provider consumer：独立在第三方应用之外，通过OAuth协议流程将credentials给第三方应用。
    - Application-embedded consumer：整合在第三方应用里，不需要信任外部的提供者。
- Credential Scheme：（1）Blind Signature；（2）Ring Signature.

Evaluation

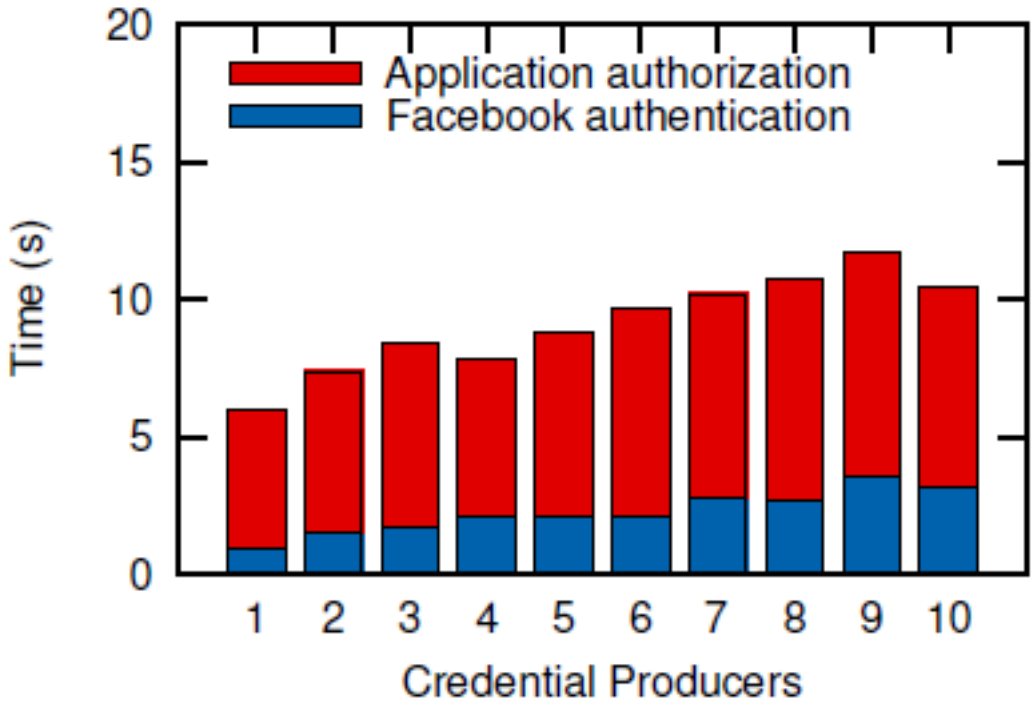


Figure 3: Facebook application authorization

Key Parameters	Signature Size (Bytes)
(1024,160)	210
(2048,224)	287
(2048,256)	325
(3072,256)	326

Table 1: Partially blind signature size

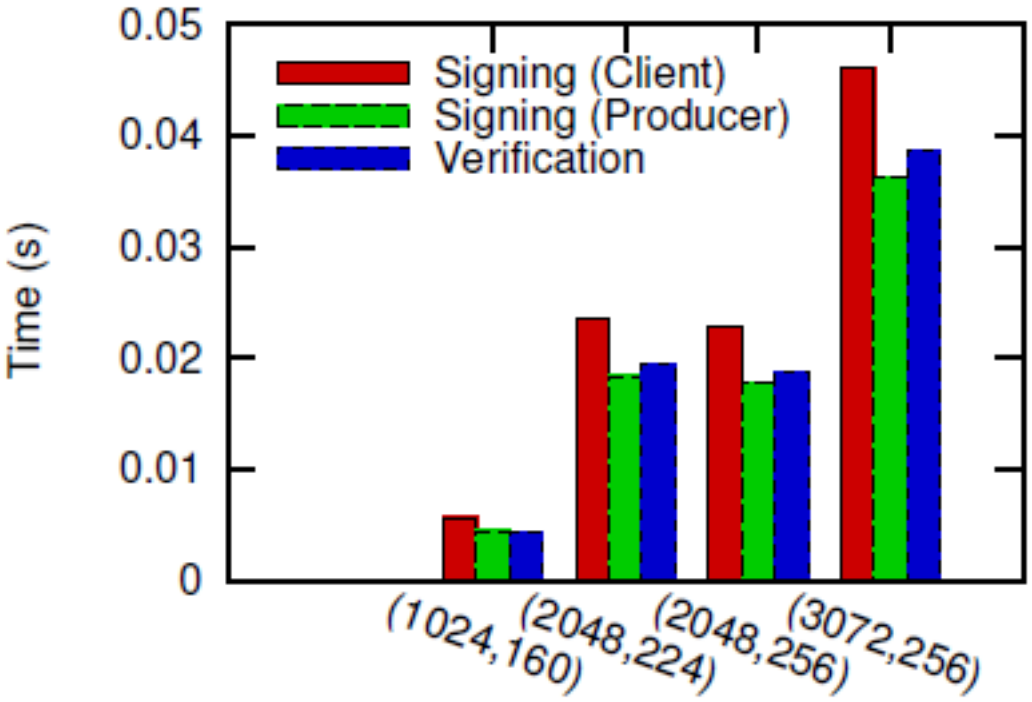


Figure 4: Partially blind signature operations

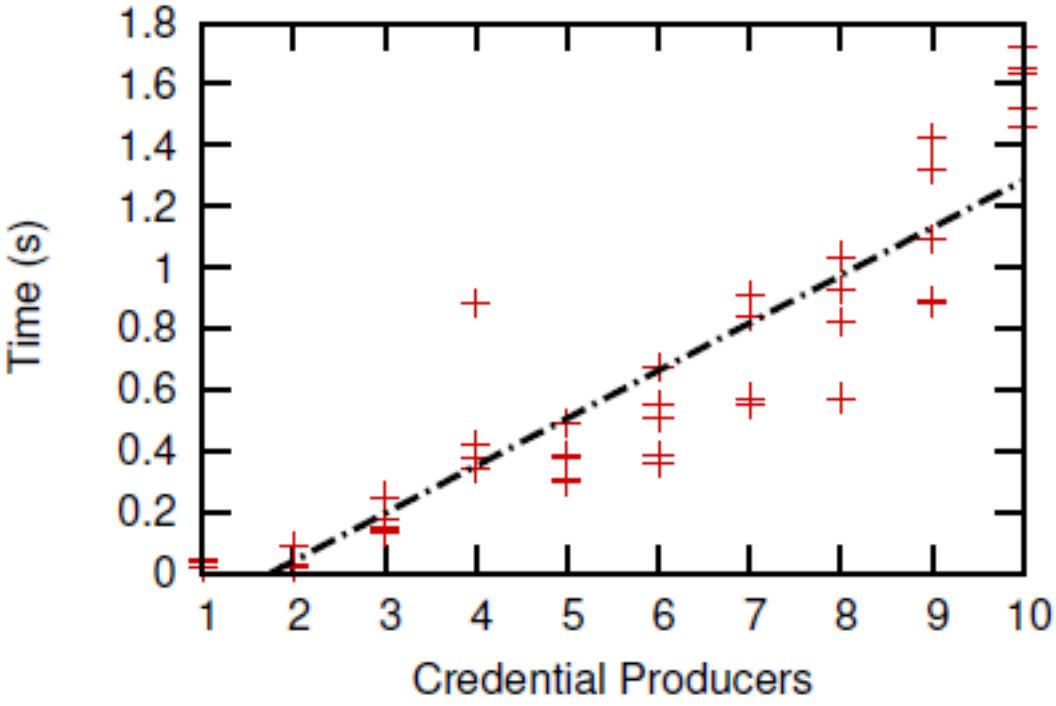


Figure 5: Distributed keypair generation

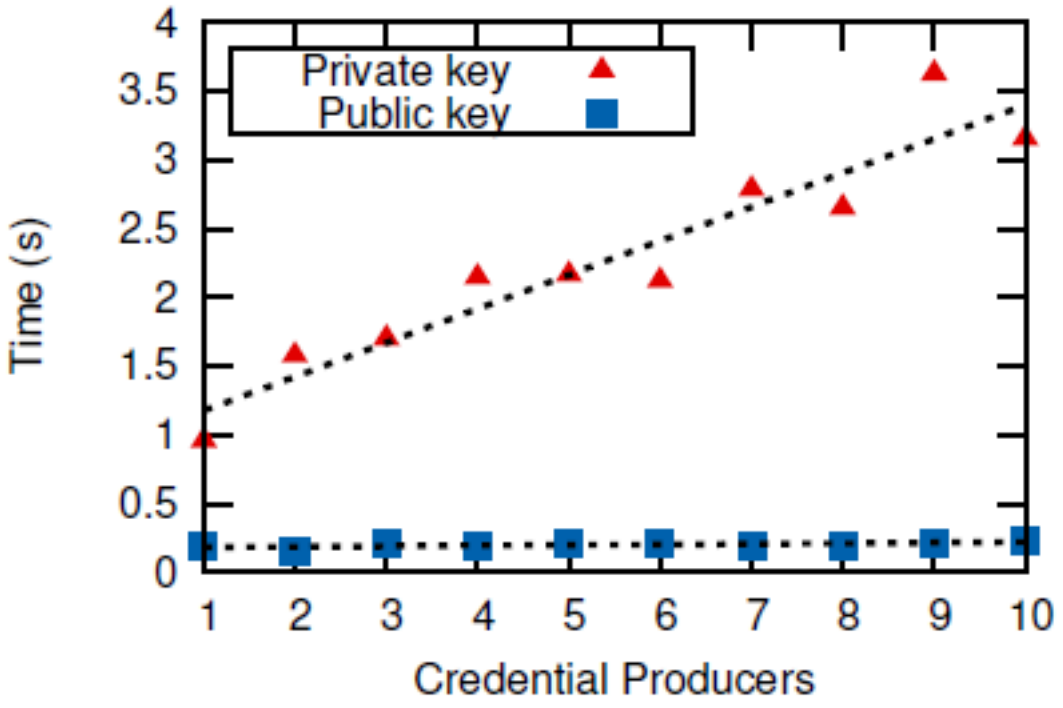


Figure 6: Retrieval of previously generated keys

Entity	Operation	Time (s)
Client	Produce LRS	0.257
Credential Consumer	Fetch Public Keys	1.011
	Verify LRS	0.035
Client-Consumer Network Latencies		0.304
	Total User-Observable	**1.607**

Table 2: End-to-end Group Authentication