Privacy Postures of Authentication Technologies

Francisco Corella and Karen Lewison

Pomcor

CHALLENGES

The development of an Identity Ecosystem requires collaboration between experts in Law, Business, Policy, Technology and Society.

But the extreme complexity of some authentication technologies makes it difficult to understand their practical implications and stands in the way of effective interdisciplinary collaboration.

Authentication technologies are evolving in separate silos, making it difficult to compare technologies across silos.

The privacy aspects of authentication technologies are not well understood because insufficient attention has been paid historically to the privacy implications of Internet technologies.

GOAL

Develop a conceptual framework that will make it possible to describe authentication technologies and their privacy implications in terms that are both accurate and comprehensible to non-specialists, by abstracting away operational concepts from the technical details.

FIRST STEPS

Survey and classify a wide range of authentication technologies.

Identify the privacy features relevant to authentication technologies and define a privacy vocabulary applicable across different classes of technologies.

Determine what privacy features are provided by each authentication technology.

Make practically relevant observations by comparing the privacy features of different technologies and classes of technologies.

FUTURE WORK

In the future we plan to extend this work to other practical aspects of authentication technologies besides privacy, including security, usability, deployability and interoperability.

CONTACT

Francisco Corella: fcorella@pomcor.com

Karen Lewison: kplewison@pomcor.com

Web site: pomcor.com

Blog: pomcor.com/blog

pomcor

pomcor.com

	Two-party authentication	Authentication by third party	Assertion of user identity	Assertion of user attributes	Closed-loop authentication	Open-loop authentication	Unobservability by identity or attribute provider	Free choice of identity or attribute provider	Anonymity	Selective disclosure	Issue-show unlinkability	Multishow unlinkability by different parties	Multishow unlinkability by same party
	1	2	3	4	5	6	7	8	9	10	11	12	13
1. User ID & password	√		√		√		N/A	N/A	√	N/A		N/A	
2. User ID & generated OTP	√		√		√		N/A	N/A	√	N/A		N/A	
3. User ID & sent OTP	√		√		√		N/A	N/A		N/A		N/A	
4. Email address & P/OTP	√		√		√		N/A	N/A		N/A		N/A	
5. Microsoft Passport		√	√	√	√					√			
6. SAML browser SSO profile		√	√	√	√			(1)		(3)			
7. Shibboleth		√	√	√	√			(1)	√	(3)		√	√
8. OpenID		√	√	√	√			√		(4)			
9. ICAM OpenID profile		√	√	√	√			(2)	√	(4)		√	
10. OAuth		√	√	√	√			(2)		(4)			
11. OpenID Connect		√	√	√	√			√		(4)			
12. Uncertified key pair	√		√		√		N/A	N/A	√	N/A		N/A	
13. Public key certificate		√	√	√		√	√	N/A	√				
14. Structured certificate		√	√	√		√	√	N/A	√	√			
15. Idemix pseudonym	√		√		√		N/A	N/A	√	N/A		N/A	
16. Idemix anon. credential		√		√		√	√	N/A	√	√	√	√	√
17. U-Prove token		√		√		√	√	N/A	√	√	√		
18. ICAM BAE		√		√	N/A	N/A							

(1) User may choose provider from list presented by fourth-party service.
(2) User may choose provider from list presented by relying-party.
(3) Attributes selected by attribute provider or relying party, user not asked for consent.
(4) Attributes selected by attribute provider or relying party, user asked for consent.

NEW CONCEPT

Closed-loop authentication: The credential authority that issues or registers a credential is later responsible for verifying possession of the credential at authentication time.

Open-loop authentication: The credential authority is out of the loop at authentication time.

CLASSIFICATION FACETS

Two-party authentication (to *a service provider*) vs. reliance on a third party (an *identity or attribute provider*, the service provider being then a *relying party*).

Assertion of user identity vs. assertion of attributes that do not necessarily identify the user.

Closed-loop vs. open-loop authentication.

How the user's identity or attributes are communicated to the service provider (the relying party in third-party authentication):

- Rows 1-4: user presents bearer credential to service provider.
- Rows 5-11: identity or attribute provider conveys bearer credential to relying party.
- Rows 12-17: user's device proves possession of cryptographic credential directly to relying party.
- Row 18: relying party obtains attributes directly from attribute provider after identifying the user.

PRIVACY FEATURES

Unobservability by identity or attribute provider: identity or attribute provider is not informed of the authentication transaction.

Free choice of identity or attribute provider (relevant if no unobservability).

Anonymity: user is not uniquely identified in a broader context than that of the service provider.

Selective disclosure: it is possible to only present partial information extracted or derived from a credential.

Issue-show unlinkability: it is not possible to determine whether a credential used in an authentication event is the same credential that was issued in a particular issuance event.

Multishow unlinkability (by same or different relying parties): it is not possible to determine whether the same credential was used in two different occasions.

OBSERVATIONS

Passwords can be replaced with uncertified key pairs for two-party closed-loop authentication without loss of privacy.

Open-loop authentication provides unobservability by identity or attribute provider.

Free choice of identity or attribute provider by the user is the exception among authentication technologies that lack unobservability by the identity or attribute provider.

Idemix anonymous credentials and U-Prove tokens have different privacy postures.