Privacy Postures of Authentication Technologies

Presentation to ID360 2013

Francisco Corella (fcorella@pomcor.com)
Karen Lewison (kplewison@pomcor.com)
Web site: pomcor.com
Blog: pomcor.com/blog

pomcor
pomcor.com

Update (May17, 2013)

- The speaker notes for this presentation can be found at

  http://pomcor.com/documents/PrivacyPosturesSpeakerNotes.pdf

- A recap of the feedback that we received on this presentation and the paper can be found at

  http://pomcor.com/2013/05/15/feedback-on-the-paper-on-privacy-postures-of-authentication-technologies/

- The paper with revisions taking into account the feedback can be found at

  http://pomcor.com/techreports/PrivacyPostures.pdf

Challenges

- Development of an Identity Ecosystem requires interdisciplinary collaboration but extreme complexity of some authentication technologies stands in the way
- It is difficult to compare authentication technologies across technology silos
- The privacy implications of authentication technologies are particularly difficult to pin down

Goal

- Develop a conceptual framework for describing authentication technologies in terms that are both accurate and comprehensible to non-specialists
- First step: provide an actionable understanding of the privacy implications of authentication technologies

Results So Far

- Survey and classification of authentication technologies
- Identification of privacy features relevant to authentication
- Matrix indicating what privacy features are provided by each technology
- A few observations derived from the matrix

	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.

Classification Facets

- How identity or attributes are delivered to service provider (4 row groups)
- Two-party authentication vs. reliance on third party (columns 1-2)
- Whether intention of technology is to identify user, to assert user attributes, or both (columns 3-4)
- Closed-loop vs. open-loop authentication (columns 5-6)

Delivery of Identity or Attributes

User presents bearer credential to service provider	User ID and password User ID and generated OTP User ID and sent OTP Email address and password/OTP
Identity or attribute provider conveys bearer credential to relying party	Microsoft passport (historical) SAML browser SSO profile Shibboleth OpenID ICAM OpenID profile OAuth OpenID Connect
User's device proves possession of cryptographic credential to relying party	Uncertified key pair Public key certificate Structured certificate Idemix pseudonym Idemix anonymous credential U-Prove token
Relying party fetches attributes	ICAM Backend Attribute Exchange

Two-party	Third-party
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
	Microsoft passport (historical)
	SAML browser SSO profile
	Shibboleth
	OpenID
	ICAM OpenID profile
	OAuth
	OpenID Connect
Uncertified key pair	
	Public key certificate
	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token
	ICAM Backend Attribute Exchange

Identity	Attributes
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token
	ICAM Backend Attribute Exchange

Closed-loop	Open-loop
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
Microsoft passport (historical)	
SAML browser SSO profile	
Shibboleth	
OpenID	
ICAM OpenID profile	
OAuth	
OpenID Connect	
Uncertified key pair	
	Public key certificate
	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token

Privacy Features

- Unobservability by identity or attribute provider
- Free choice of identity or attribute provider
- Anonymity
- Selective disclosure
- Issue-show unlinkability
- Multishow unlinkability (by same or different relying parties)

Color coding: **Green: YES** **Red: NO** **Blue: N/A**

pomcor
pomcor.com

Unobservability by id/attr provider	Free Choice of id/attr provider, by user
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

Anonymity

User ID and password
User ID and generated OTP
User ID and sent OTP
Email address and password/OTP
Microsoft passport (historical)
SAML browser SSO profile
Shibboleth
OpenID
ICAM OpenID profile
OAuth
OpenID Connect
Uncertified key pair
Public key certificate
Structured certificate
Idemix pseudonym
Idemix anonymous credential
U-Prove token
ICAM Backend Attribute Exchange

Selective Disclosure by user	Issue-Show Unlinkability
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

Multishow Unl. by different parties	Multishow Unl. by same party
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

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 the identity or attribute provider.
- Free choice of identity or attribute provider is the exception among authentication technologies that lack unobservability.
- Idemix anonymous credentials and U-Prove tokens have different privacy postures.

Questions?

Francisco Corella (fcorella@pomcor.com)

Karen Lewison (kplewison@pomcor.com)

Web site: pomcor.com

Blog: pomcor.com/blog