Outsourcing Phone-based Web Authentication while Protecting User Privacy

NordSec 2016

Martin Potthast[1] Christian Forler[2] Eik List[1] Stefan Lucks[1]

[1]Bauhaus-Universität Weimar

Bauhaus-Universität Weimar

`<firstname>.<lastname>(at)uni-weimar.de`

[2] Beuth Hochschule für Technik Berlin

BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

04 Nov 2016

Section 1

Motivation

Passwords

- Humans are bad at memorizing strong passwords
- Already 2007: Median user is registered at 25 web services
  [Florêncio and Herley, 2007]
- Passwords are unlikely to disappear in the near future

password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
jennifer
111111
2000
jordan
superman
harley
1234567
fuckme
hunter
fuckyou
trustno1
ranger
buster
thomas
tigger
robert
soccer
fuck
batman
test
pass
killer
hockey
george
charlie
andrew
michelle
love
sunshine
jessica
asshole
6969
pepper
daniel
access
123456789
654321
joshua
maggie
starwars
silver
william
dallas
yankees
123123
ashley
666666
hello
amanda
orange
biteme
freedom
computer
sexy
thunder
nicole
ginger
heather
hammer
summer
corvette
taylor
fucker
austin
1111
merlin
matthew
121212
golfer
cheese
princess
martin
chelsea
patrick
richard
diamond
yellow
bigdog
secret
asdfgh
sparky
cowboy
source: xato.net

Image: xato.net

Two-Factor Authentication

2nd Line of Defense against

- Reused passwords
- Weak credentials or lacking 1st-factor policies
- Data breaches
- Phishing attacks
- . . .

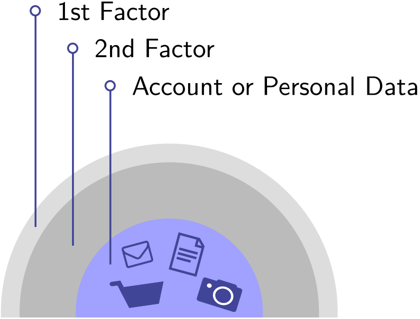


Image: https://www.google.com/landing/2step

Two-Factor Authentication

Factors

Something you know
Unique tuple of username + password

Idea: Duo Mobile 2014; Images:
http://2.bp.blogspot.com/-3wBHxiz30Do/VEU8Ba4j7BI/AAAAAAAABo4/-gs07aNu7lA/s1600/homer-idea.png,
https://frinkiac.com/caption/S06E02/42976,
http://s1.favim.com/orig/14/eye-homer-homer-simpson-simpson-simpsons-Favim.com-184669.jpg,
https://upload.wikimedia.org/wikipedia/en/0/0b/Marge_Simpson.png

Two-Factor Authentication

Factors

Something you know
Unique tuple of username + password

Something you have
Personal device or smartphone app

Idea: Duo Mobile 2014; Images:
http://2.bp.blogspot.com/-3wBHxiz30Do/VEU8Ba4j7BI/AAAAAAAABo4/-gs07aNu71A/s1600/homer-idea.png,
https://frinkiac.com/caption/S06E02/42976,
http://s1.favim.com/orig/14/eye-homer-homer-simpson-simpson-simpsons-Favim.com-184669.jpg,
https://upload.wikimedia.org/wikipedia/en/0/0b/Marge_Simpson.png

Two-Factor Authentication

Factors

Something you know
Unique tuple of username + password

Something you have
Personal device or smartphone app

Something you are
Fingerprint or retina scan

Idea: Duo Mobile 2014; Images:
http://2.bp.blogspot.com/-3wBHxiz30Do/VEU8Ba4j7BI/AAAAAAAABo4/-gs07aNu7lA/s1600/homer-idea.png,
https://frinkiac.com/caption/S06E02/42976,
http://s1.favim.com/orig/14/eye-homer-homer-simpson-simpson-simpsons-Favim.com-184669.jpg,
https://upload.wikimedia.org/wikipedia/en/0/0b/Marge_Simpson.png

Two-Factor Authentication

Factors

Something you know
Unique tuple of username + password

Something you have
Personal device or smartphone app

Something you are
Fingerprint or retina scan

Someone you know
[Brainard et al., 2006]

Idea: Duo Mobile 2014; Images:
http://2.bp.blogspot.com/-3wBHxiz30Do/VEU8Ba4j7BI/AAAAAAAABo4/-gs07aNu71A/s1600/homer-idea.png,
https://frinkiac.com/caption/S06E02/42976,
http://s1.favim.com/orig/14/eye-homer-homer-simpson-simpson-simpsons-Favim.com-184669.jpg,
https://upload.wikimedia.org/wikipedia/en/0/0b/Marge_Simpson.png

Phone-based Two-factor Authentication

Benefits:

- Omnipresent, ubiquitous
- Spares users from carrying around additional devices
- Spares service providers from shipping devices

Phone-based Two-factor Authentication

Benefits:

- Omnipresent, ubiquitous
- Spares users from carrying around additional devices
- Spares service providers from shipping devices

Disadvantage:

- Difficult to implement from scratch $\Longrightarrow$ outsourcing

Phone-based Two-factor Authentication

Benefits:

- Omnipresent, ubiquitous
- Spares users from carrying around additional devices
- Spares service providers from shipping devices

Disadvantage:

- Difficult to implement from scratch $\Longrightarrow$ outsourcing

Privacy? An honest-but-curious authentication provider potentially learns

- Usage statistics of users
- Usage statistics of service providers
- Relations of users to service providers

Phone-based Two-factor Authentication

Benefits:

- Omnipresent, ubiquitous
- Spares users from carrying around additional devices
- Spares service providers from shipping devices

Disadvantage:

- Difficult to implement from scratch $\Longrightarrow$ outsourcing

Privacy? An honest-but-curious authentication provider potentially learns

- Usage statistics of users
- Usage statistics of service providers
- Relations of users to service providers

Goal of Passphone:

- Phone-based two-factor authentication scheme
- Outsource verification of 2nd factor while preserving privacy

Existing Phone-Based Two-Factor Authentication Schemes

Time-based One-Time Passwords:

- Google 2-Step [Google, 2013], Microsoft [Meisner, 2013], Apple [Apple, 2016], Facebook [Song, 2011]
- CRONTO [VASCO, 2013], Duo Mobile [Duo Security, 2016]

Academia:

- SOUNDPROOF [Karapanos et al., 2015]: Avoided need for user interaction
- Shirvanian et al. [Shirvanian et al., 2014]: Resilience to off-line attacks
- PHONEAUTH [Czeskis et al., 2012]
- MP-AUTH [Mannan and van Oorschot, 2011]: No secret on device
- TIQR [Van Rijswijk and Van Dijk, 2011], SNAP2PASS [Dodson et al., 2010], QR-TAN [Starnberger et al., 2009]: QR-based
- PHOOLPROOF [Parno et al., 2006]: Bookmark-based

Remarks

- Privacy-unaware users may be tracked down by other means:
  - Users must avoid reuse or self-related credentials and mail addresses
  - Users should hide their identity (e. g., use services like TOR)
- Base on TLS-secured connections
- Recommendations:
  - Public-key pinning for Trusted Third Party
  - Bind TLS connections to specific channel

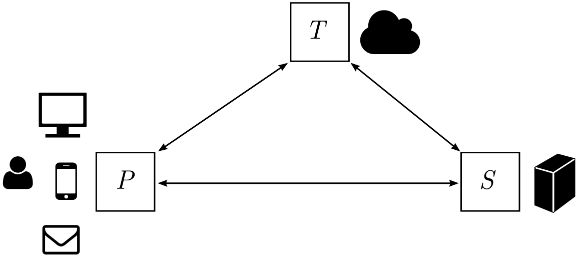
Goal:

- No additional angles for user profiling by second factor

Section 2

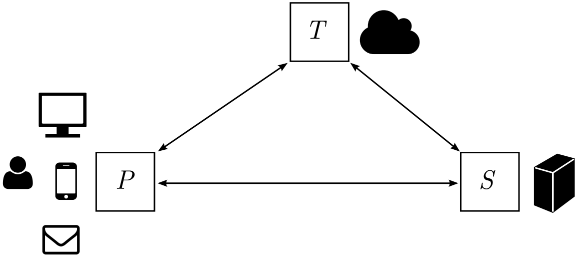
Passphone Protocols

Involved Parties



S	Service provider
T	Trusted Third Party
P	User (prover)
PT	Prover's telephone
PM	Prover's mail box

Involved Parties



S Service provider

T Trusted Third Party

P User (prover)

PT Prover's telephone

PM Prover's mail box

- Assume: User has device PT and mail box PM under control
- Assume: TTP is honest (but curious)
- Encode protocol, step, version, and sender information in all messages
- Protocols: Registration, Activation, Authentication, Revocation, Rekeying

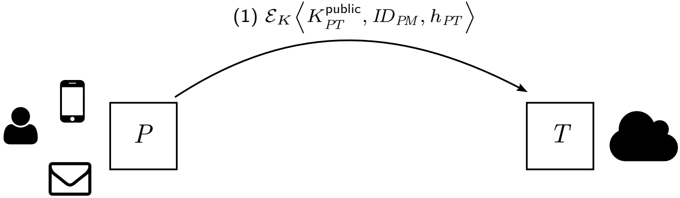
Passphone: Registration

P's device PT generates and stores a key pair $K_{PT}^{\text{public}}, K_{PT}^{\text{secret}}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Registration

P submits public key and a blinded ID $h_{PT} = \mathsf{Hash}(N_{PT})$ to T



(1) $\mathcal{E}_K \left\langle K_{PT}^{\mathsf{public}}, ID_{PM}, h_{PT} \right\rangle$

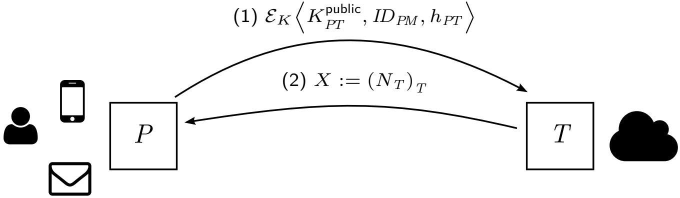
P

T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Registration

T sends challenge N_T to P's mail account

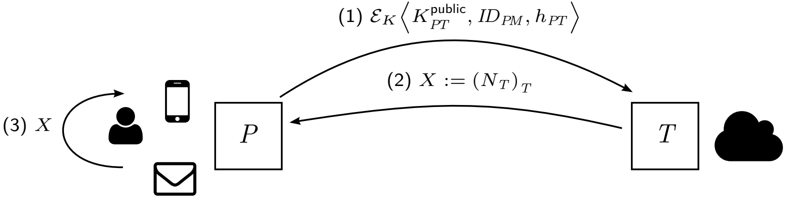


(1) $\mathcal{E}_K\left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT}\right\rangle$
(2) $X := (N_T)_T$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Registration

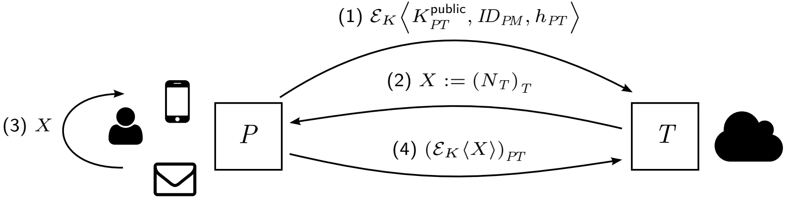
P forwards challenge to PT


(1) $\mathcal{E}_K \left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT} \right\rangle$
(2) $X := (N_T)_T$
(3) X
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Registration

Challenge is signed by PT as response

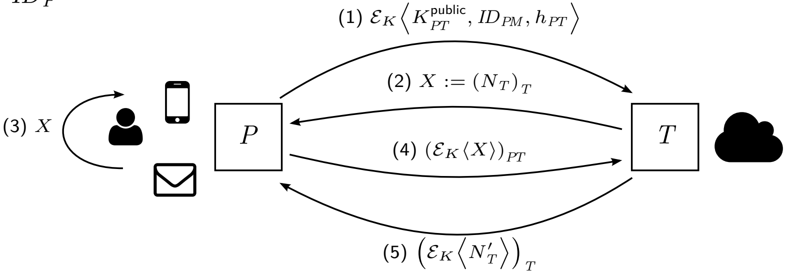


(1) $\mathcal{E}_K\left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT}\right\rangle$
(2) $X := (N_T)_T$
(3) X
(4) $(\mathcal{E}_K\langle X\rangle)_{PT}$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Registration

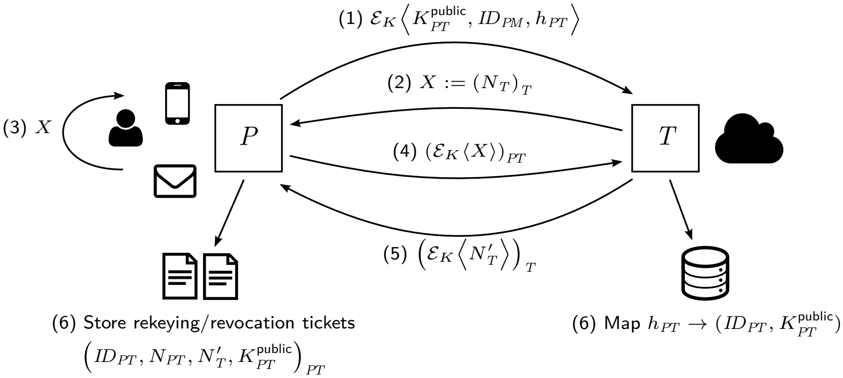
T checks response, and creates a ticket, and assigns $ID_{PT} = \text{Hash}(h_{PT}, N'_T)$ to P


(1) $\mathcal{E}_K \left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT} \right\rangle$
(2) $X := (N_T)_T$
(3) X
P
T
(4) $(\mathcal{E}_K \langle X \rangle)_{PT}$
(5) $\left(\mathcal{E}_K \left\langle N'_T \right\rangle\right)_T$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K \langle \cdot \rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Registration

P creates key-management tickets; T maps P's IDs to her key



(1) $\mathcal{E}_K\left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT}\right\rangle$

(2) $X := (N_T)_T$

(3) X

P

T

(4) $(\mathcal{E}_K\langle X\rangle)_{PT}$

(5) $\left(\mathcal{E}_K\left\langle N'_T\right\rangle\right)_T$

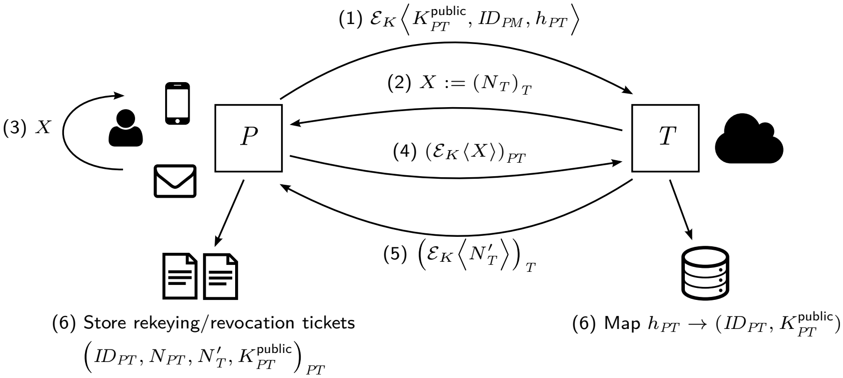
(6) Store rekeying/revocation tickets $\left(ID_{PT}, N_{PT}, N'_T, K_{PT}^{\text{public}}\right)_{PT}$

(6) Map $h_{PT} \rightarrow (ID_{PT}, K_{PT}^{\text{public}})$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Registration

Only P can create the key-management tickets (not even T)



(1) $\mathcal{E}_K\left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT}\right\rangle$

(2) $X := (N_T)_T$

(3) X

(4) $(\mathcal{E}_K\langle X\rangle)_{PT}$

(5) $\left(\mathcal{E}_K\left\langle N'_T\right\rangle\right)_T$

P

T

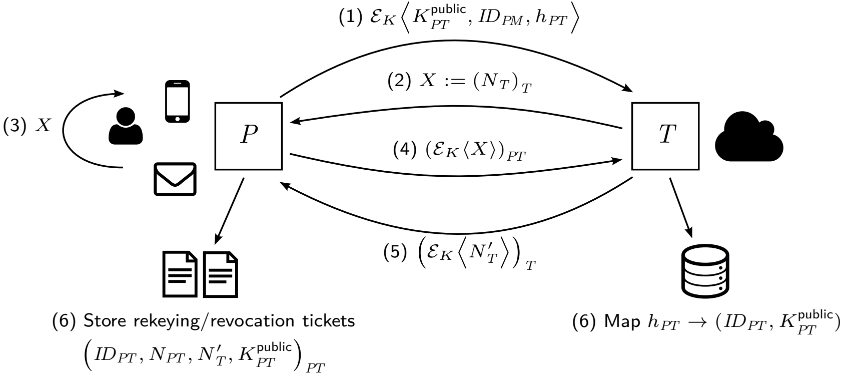
(6) Store rekeying/revocation tickets $\left(ID_{PT}, N_{PT}, N'_T, K_{PT}^{\text{public}}\right)_{PT}$

(6) Map $h_{PT} \to (ID_{PT}, K_{PT}^{\text{public}})$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Registration

T knows only public information from P

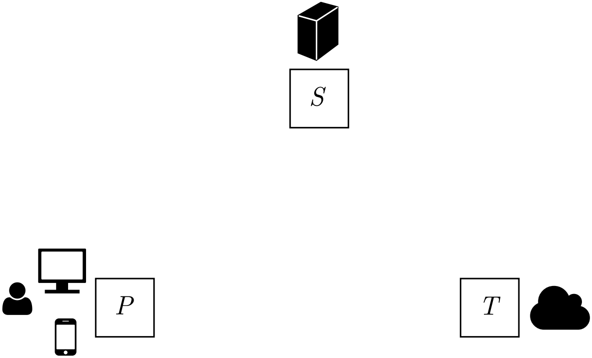


(1) $\mathcal{E}_K \left\langle K_{PT}^{\text{public}}, ID_{PM}, h_{PT} \right\rangle$
(2) $X := (N_T)_T$
(3) X
P
T
(4) $(\mathcal{E}_K \langle X \rangle)_{PT}$
(5) $\left(\mathcal{E}_K \left\langle N'_T \right\rangle\right)_T$
(6) Store rekeying/revocation tickets
$\left(ID_{PT}, N_{PT}, N'_T, K_{PT}^{\text{public}}\right)_{PT}$
(6) Map $h_{PT} \rightarrow (ID_{PT}, K_{PT}^{\text{public}})$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

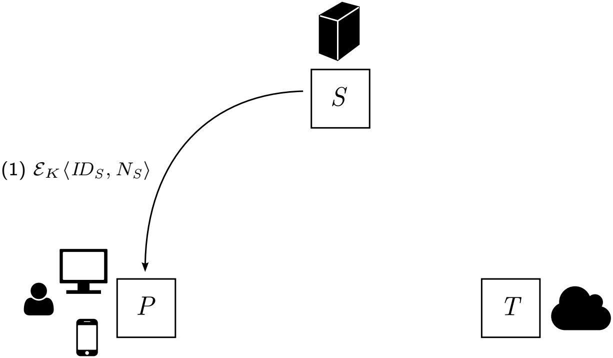
P requests activation of 2nd factor at S



S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Activation

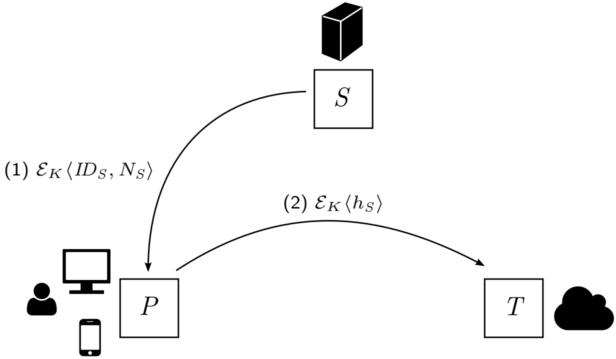
S sends its ID and challenge N_S



S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

P blinds S's ID: $h_S = \text{Hash}(ID_S, N_S)$, and sends it to T

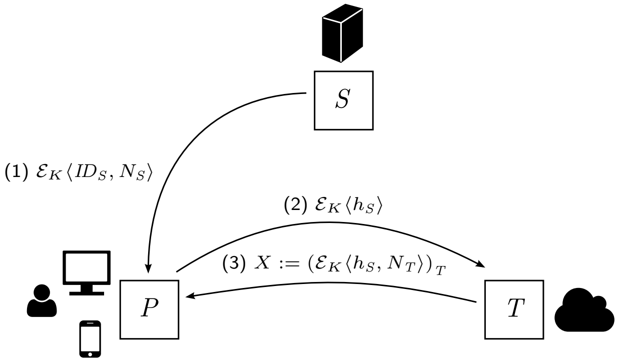


S
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Activation

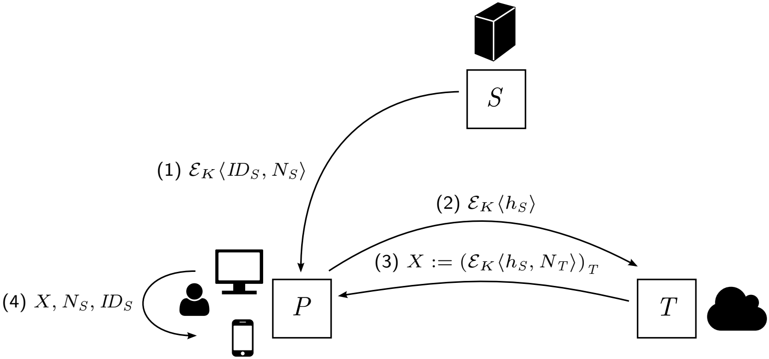
T sends challenge N_T to P


S
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

P forwards both challenges from its browser to its device



S

(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$

(2) $\mathcal{E}_K\langle h_S\rangle$

(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

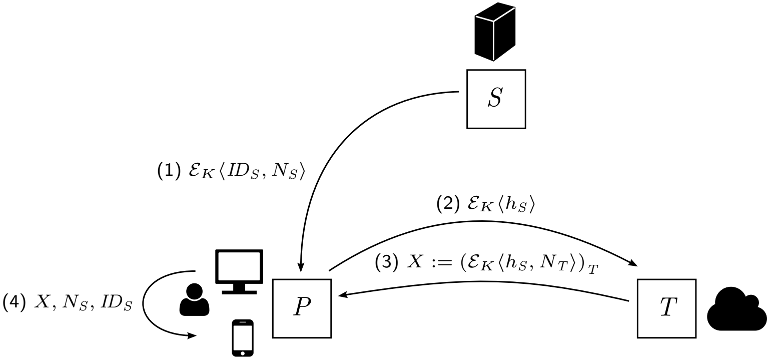
P

T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Activation

P verifies contents and ID_S



S

(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$

(2) $\mathcal{E}_K\langle h_S\rangle$

(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

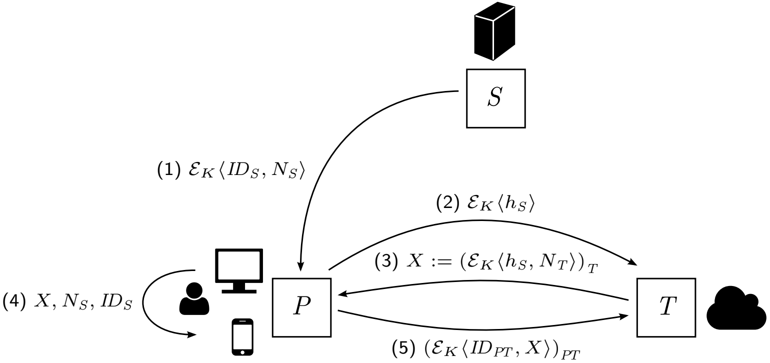
P

T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

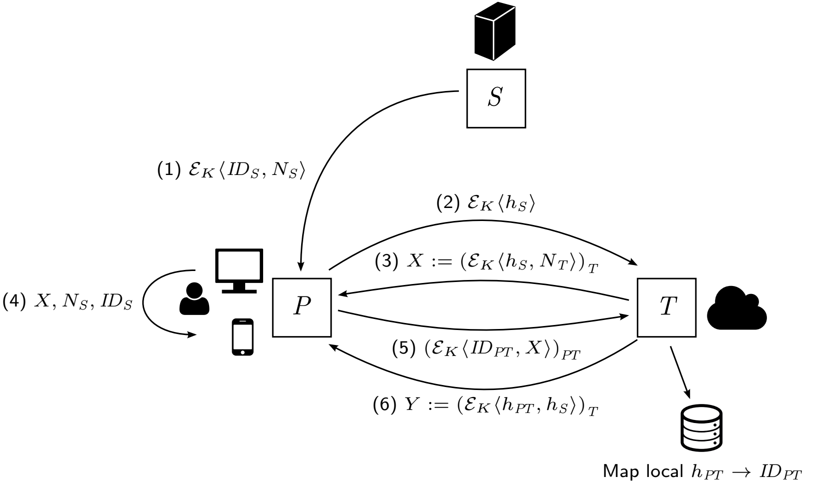
If successful, P signs challenge with its ID to T


S
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

T verifies response; if valid, T generates a local $h_{PT} = \mathsf{Hash}(ID_{PT}, N_T)$

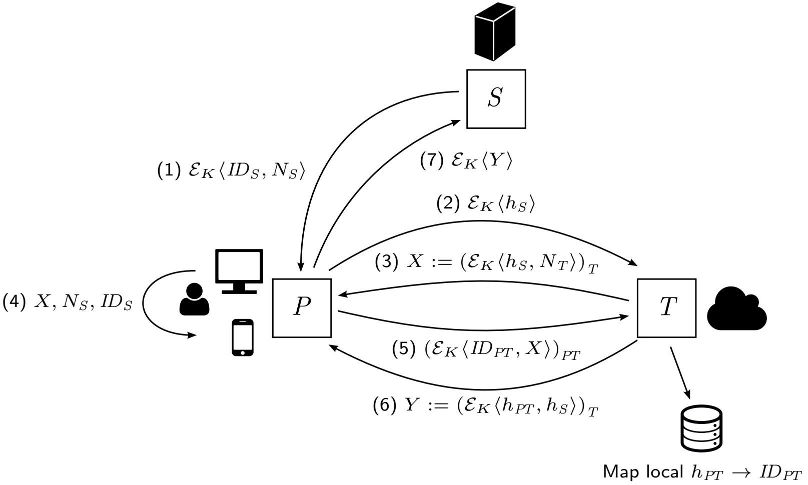


S
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$
Map local $h_{PT} \rightarrow ID_{PT}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

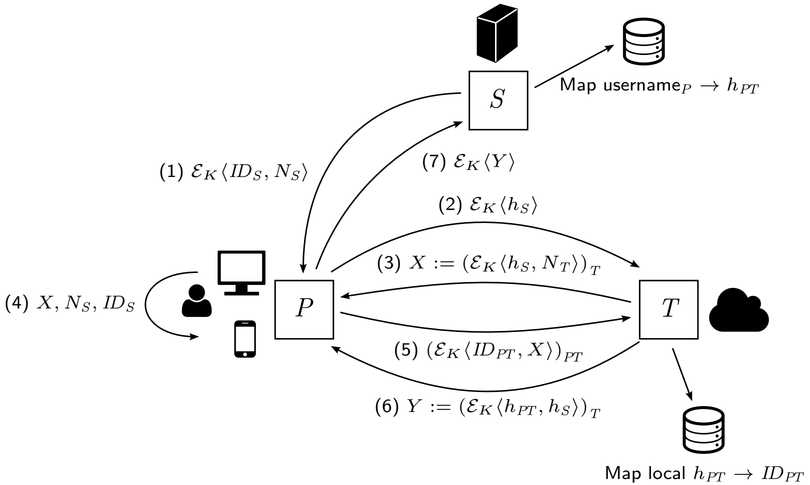
P forwards the ticket to S


S
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(7) $\mathcal{E}_K\langle Y\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$
Map local $h_{PT} \rightarrow ID_{PT}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Activation

S maps P's account to blinded ID; T maps local blinded h_{PT} to ID_{PT}



S

Map username$_P \rightarrow h_{PT}$

(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$

(7) $\mathcal{E}_K\langle Y\rangle$

(2) $\mathcal{E}_K\langle h_S\rangle$

(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

P

T

(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$

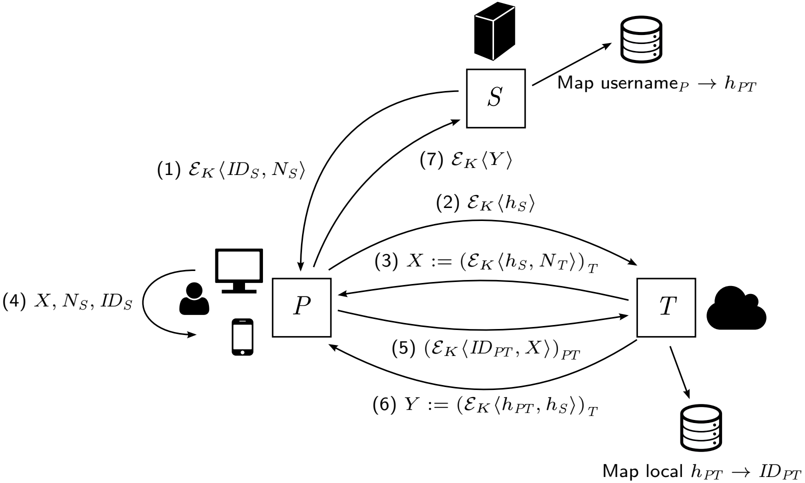
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$

Map local $h_{PT} \rightarrow ID_{PT}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Activation

S does not see ID_{PT} nor can it link it; T can not link S

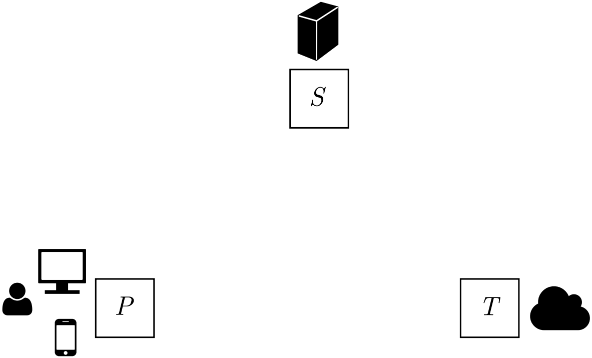


S
Map username$_P \rightarrow h_{PT}$
(1) $\mathcal{E}_K\langle ID_S, N_S\rangle$
(7) $\mathcal{E}_K\langle Y\rangle$
(2) $\mathcal{E}_K\langle h_S\rangle$
(3) $X := (\mathcal{E}_K\langle h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$
Map local $h_{PT} \rightarrow ID_{PT}$

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

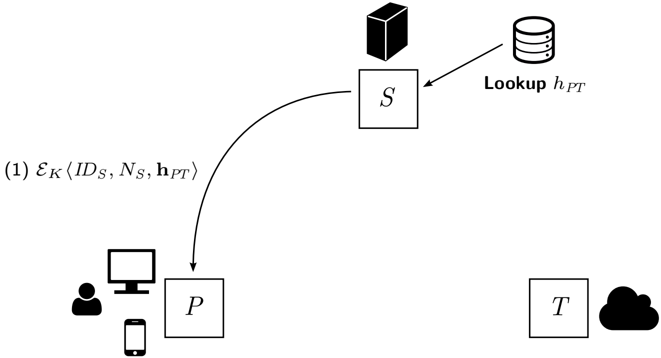
P logs in at S with 1st factor



S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

S looks up h_{PT} and sends it with a challenge N_S

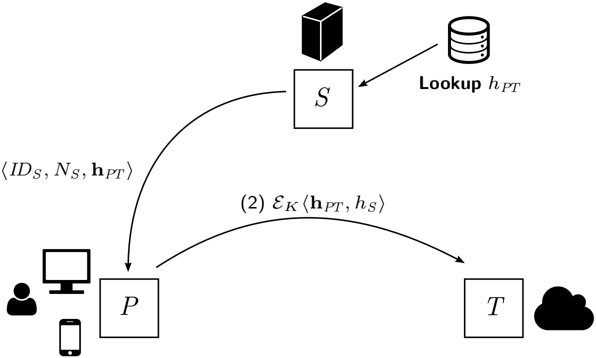


S
Lookup h_{PT}
(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

P blinds S's ID: $h_S = \mathsf{Hash}(ID_S, N_S)$; sends it to T together with h_{PT}

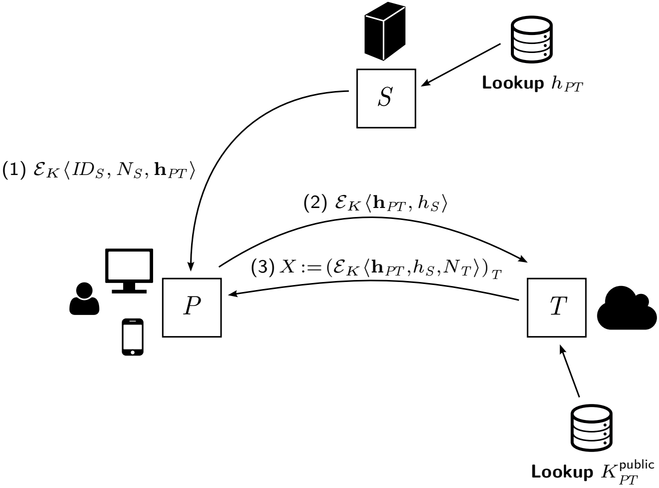


S
Lookup h_{PT}
(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$
(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$
P
T

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

T looks up key, and adds a challenge N_T

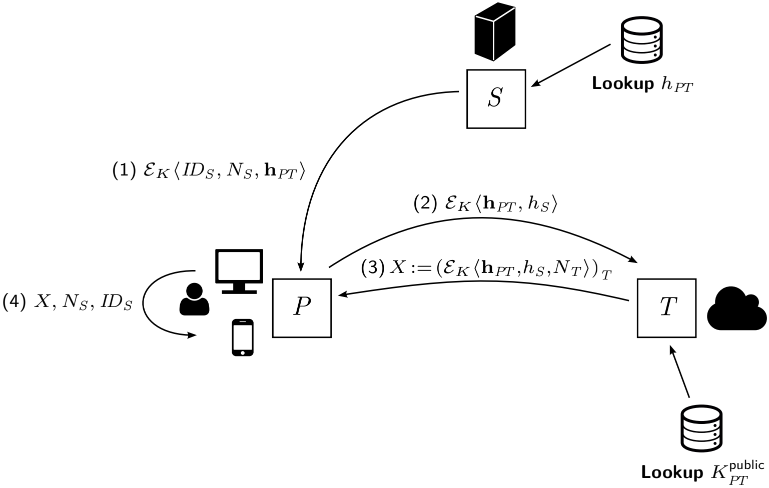


S
Lookup h_{PT}
(1) $\mathcal{E}_K \langle ID_S, N_S, \mathbf{h}_{PT} \rangle$
(2) $\mathcal{E}_K \langle \mathbf{h}_{PT}, h_S \rangle$
(3) $X := (\mathcal{E}_K \langle \mathbf{h}_{PT}, h_S, N_T \rangle)_T$
P
T
Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K \langle \cdot \rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

P forwards both challenges from its browser to its device

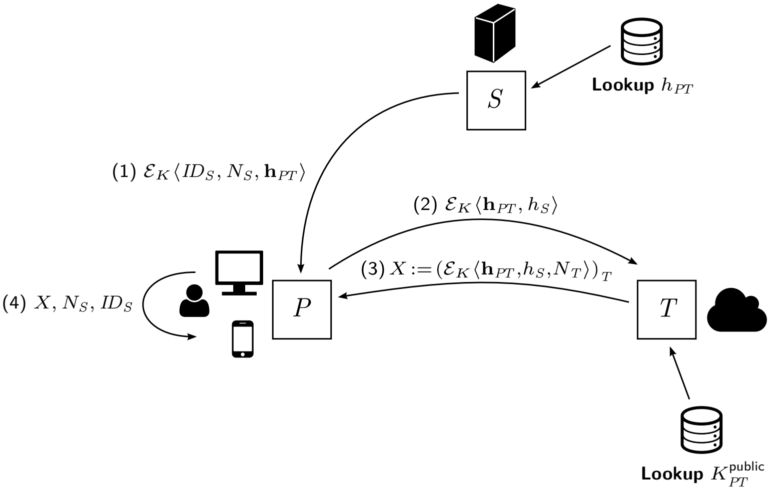


S
Lookup h_{PT}
(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$
(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$
(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

P verifies correct service provider, $h_S = \text{Hash}(ID_S, N_S)$, and signatures



S

Lookup h_{PT}

(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$

(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$

(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

P

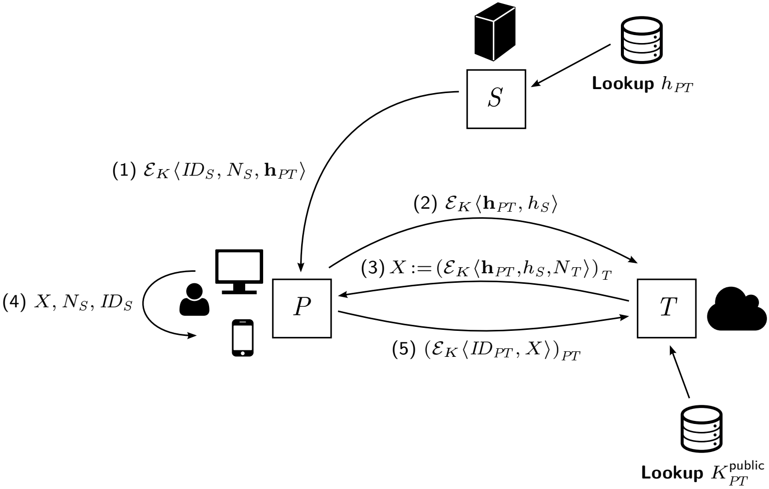
T

Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

If successful, P signs challenge, and sends it together with its ID to T

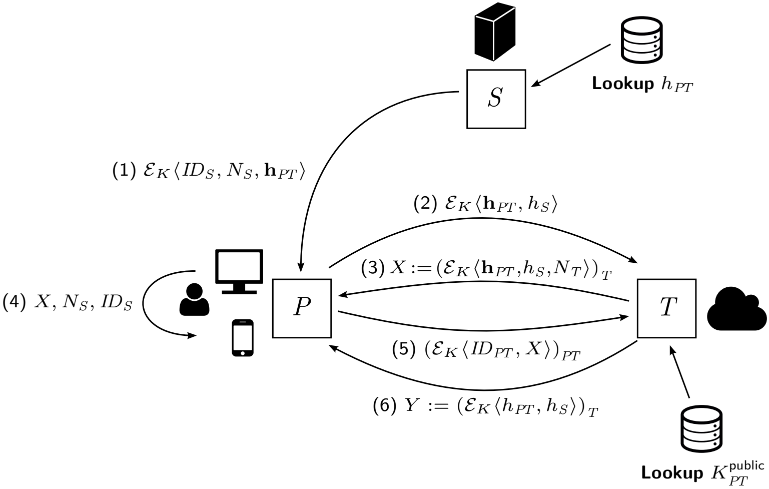


S
Lookup h_{PT}
(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$
(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$
(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$
Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

T verifies parameters and signature and issues authentication ticket



S

Lookup h_{PT}

(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$

(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$

(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

P

T

(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$

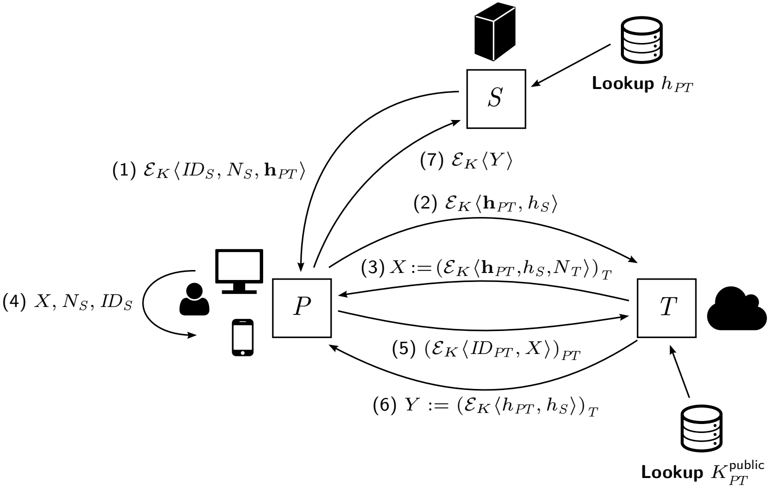
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$

Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Passphone: Authentication

P forwards the ticket to S

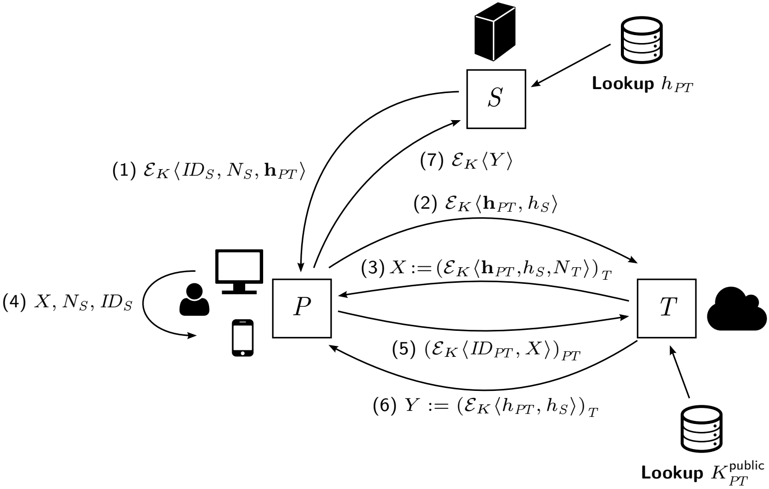


S
Lookup h_{PT}
(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$
(7) $\mathcal{E}_K\langle Y\rangle$
(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$
(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$
(4) X, N_S, ID_S
P
T
(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$
(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$
Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

PASSPHONE: Authentication

S verifies ticket, and grants P access if valid.



S

Lookup h_{PT}

(1) $\mathcal{E}_K\langle ID_S, N_S, \mathbf{h}_{PT}\rangle$

(7) $\mathcal{E}_K\langle Y\rangle$

(2) $\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S\rangle$

(3) $X := (\mathcal{E}_K\langle \mathbf{h}_{PT}, h_S, N_T\rangle)_T$

(4) X, N_S, ID_S

P

T

(5) $(\mathcal{E}_K\langle ID_{PT}, X\rangle)_{PT}$

(6) $Y := (\mathcal{E}_K\langle h_{PT}, h_S\rangle)_T$

Lookup K_{PT}^{public}

S	Service provider	ID_X	ID of X	$(\cdot)_X$	Signed by X
T	Trusted Third Party	h_X	Blinded ID of X	$\mathcal{E}_K\langle\cdot\rangle$	TLS-protected
P	User (prover)	N_X	Challenge of X		

Section 3

Security Analysis

Security Goals

1. Authentication security
   Adversary cannot authenticate as some honest P at some honest S

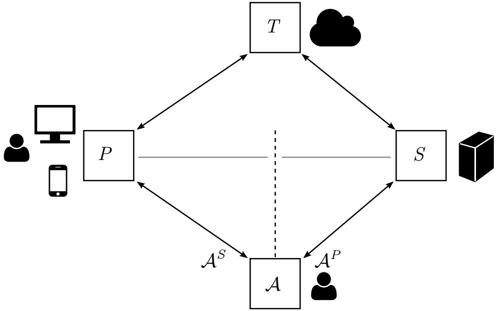
2. Preserving anonymity wrt. TTP
   An honest-but-curious TTP cannot determine which user is registered with which service provider

3. Preserving unlinkability
   Colluding service providers cannot link users registered at multiple of their services

Authentication Security

Assumptions: $\mathcal{A}$ can...

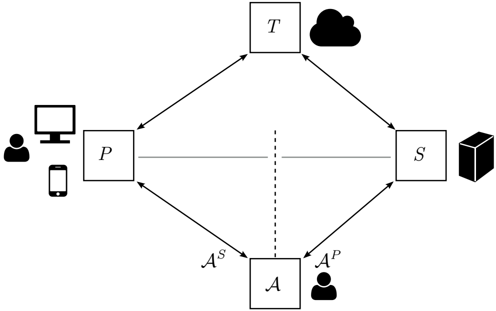
- ... generate, intercept, manipulate, or replay messages.



Authentication Security

Assumptions: $\mathcal{A}$ can...

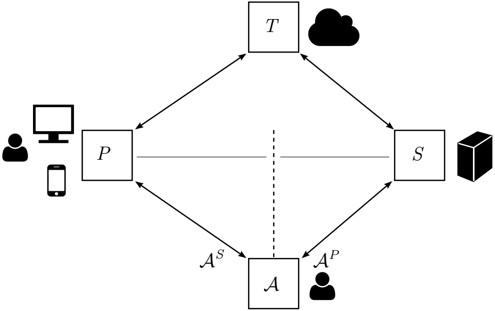
- ...generate, intercept, manipulate, or replay messages.
- ...**not** feasibly break the underlying crypto or guess challenges (τ-bit effective key lengths, independent keys, 2τ-bit random independent challenges, signatures, and hashes)



Authentication Security

Assumptions: $\mathcal{A}$ can...

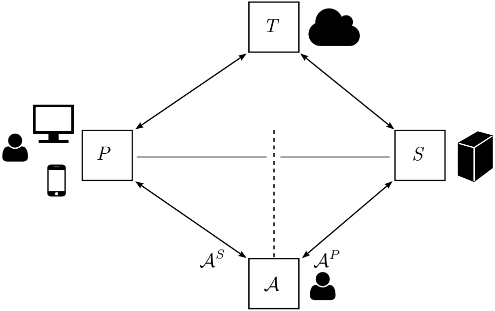
- ...generate, intercept, manipulate, or replay messages.
- ...**not** feasibly break the underlying crypto or guess challenges (τ-bit effective key lengths, independent keys, 2τ-bit random independent challenges, signatures, and hashes)
- ...**not** feasibly produce collisions/preimages for Hash$(\cdot)$ (random oracle).



Authentication Security

Assumptions: $\mathcal{A}$ can…

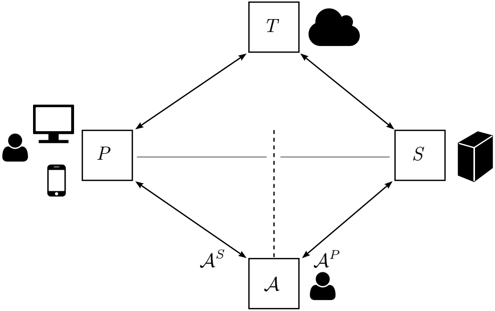
- …generate, intercept, manipulate, or replay messages.
- …**not** feasibly break the underlying crypto or guess challenges (τ-bit effective key lengths, independent keys, 2τ-bit random independent challenges, signatures, and hashes)
- …**not** feasibly produce collisions/preimages for Hash$(\cdot)$ (random oracle).
- …control other user(s) $\mathcal{A}^P$ registered at S.



Authentication Security

Assumptions: $\mathcal{A}$ can...

- ...generate, intercept, manipulate, or replay messages.
- ...**not** feasibly break the underlying crypto or guess challenges (τ-bit effective key lengths, independent keys, 2τ-bit random independent challenges, signatures, and hashes)
- ...**not** feasibly produce collisions/preimages for Hash$(\cdot)$ (random oracle).
- ...control other user(s) $\mathcal{A}^P$ registered at S.
- ...control other service provider(s) $\mathcal{A}^S$ where P is registered with.



Authentication Security – Proof Ideas

Use framework by Bellare et al.

- $\mathcal{A}$ can ask Execute (passive), Send (active), Corrupt (1st factor of P), and Test (final) queries

To win, $\mathcal{A}$ must achieve at least one of the following:

1. Forge (the signature of) a valid authentication ticket
    - Infeasible by assumption
2. Replay an old accepted ticket
    - N_S is fresh and uniformly random chosen by S
    - Must find collision or preimage Hash$(ID_S, N_S) \implies$ infeasible
3. Obtain a fresh valid ticket for a different (parallel) session

Authentication Security – Proof Ideas (Cont'd)

3. Obtain a fresh valid ticket for a different session

- Successfully pretend S in the view of P
  $\implies$ infeasible ($\mathcal{A}$ cannot forge/decrypt TLS)

Authentication Security – Proof Ideas (Cont'd)

3. Obtain a fresh valid ticket for a different session

- Successfully pretend S in the view of P
  $\Longrightarrow$ infeasible ($\mathcal{A}$ cannot forge/decrypt TLS)
- Forge signature of P for a message to T
  $\Longrightarrow$ infeasible

Authentication Security – Proof Ideas (Cont'd)

3. Obtain a fresh valid ticket for a different session

- Successfully pretend S in the view of P
  $\Longrightarrow$ infeasible ($\mathcal{A}$ cannot forge/decrypt TLS)
- Forge signature of P for a message to T
  $\Longrightarrow$ infeasible
- Replace ID_S, N_S, or N_T in $((\mathcal{E}_K\langle ID_T, h_{PT}, h_S, N_T\rangle)_T, N_S, ID_S)$, and still make P sign the challenge
  - Replace $ID_S \Longrightarrow PT$ will notice
  - Find collision/preimage to $h_S = \mathsf{Hash}(ID_S, N_S) \Longrightarrow$ infeasible
  - Forge signature by $T \Longrightarrow$ infeasible
  - Replace $h_S \Longrightarrow$ wrong signature
  - Replace N_T from some parallel session $\mathcal{A} \leftrightarrow T \Longrightarrow$ wrong signature

Authentication Security – Proof Ideas (Cont'd)

3. Obtain a fresh valid ticket for a different session

- Successfully pretend S in the view of P $\Longrightarrow$ infeasible ($\mathcal{A}$ cannot forge/decrypt TLS)
- Forge signature of P for a message to T $\Longrightarrow$ infeasible
- Replace ID_S, N_S, or N_T in $((\mathcal{E}_K\langle ID_T, h_{PT}, h_S, N_T\rangle)_T, N_S, ID_S)$, and still make P sign the challenge
  - Replace $ID_S \Longrightarrow PT$ will notice
  - Find collision/preimage to $h_S = \text{Hash}(ID_S, N_S) \Longrightarrow$ infeasible
  - Forge signature by $T \Longrightarrow$ infeasible
  - Replace $h_S \Longrightarrow$ wrong signature
  - Replace N_T from some parallel session $\mathcal{A} \leftrightarrow T \Longrightarrow$ wrong signature

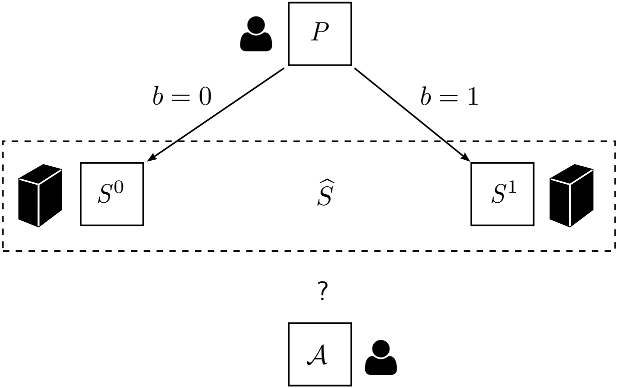
Theorem 1 (Authentication Security)

Given our assumptions and let Hash be a random oracle. Then, any PPT adversary $\mathcal{A}$ asking at most q queries has, for a random execution of $\mathcal{G}^{\mathsf{Auth}}$ on our protocol $\mathbb{P}$, a success probability of at most $4q/2^\tau$.

Anonymity

Modelled as a Real-or-Random Game

- **Setup:** Challenger registers P with either S^0 or S^1
- Whenever P interacts with either S^0 or S^1, the game uses $\widehat{S}$ as compound service provider in view of $\mathcal{A}$
- **Goal of $\mathcal{A}$:** Determine which service provider P has registered with



Anonymity

Proof Ideas

$\mathcal{A}$ can learn from a run of the...

- Registration protocol: $ID_{PT}, K_{PT}^{\text{public}}, ID_{PM}$
- Activation protocol: Mapping $h_S \rightarrow (ID_{PT}, h_{PT})$
- Authentication protocol: $ID_{PT} \leftrightarrow h_{PT}$ to $h'_S \leftarrow H(ID_S, N'_S)$

- h_S blinds ID_S, fresh and random for every session
- h_{PT} blinds ID of P across service providers
- $\mathcal{A}$ must predict challenges $N_S \implies$ infeasible

Anonymity

Proof Ideas

$\mathcal{A}$ can learn from a run of the...

- Registration protocol: $ID_{PT}, K_{PT}^{\text{public}}, ID_{PM}$
- Activation protocol: Mapping $h_S \rightarrow (ID_{PT}, h_{PT})$
- Authentication protocol: $ID_{PT} \leftrightarrow h_{PT}$ to $h'_S \leftarrow H(ID_S, N'_S)$

- h_S blinds ID_S, fresh and random for every session
- h_{PT} blinds ID of P across service providers
- $\mathcal{A}$ must predict challenges $N_S \implies$ infeasible

Anonymity Result:

$$\mathbf{Adv}_{\mathbb{P}}^{\mathsf{Anon}}(\mathcal{A}) \leq (q_{\mathsf{exe}} + q_{\mathsf{send}}) \cdot 1/2^{2\tau}.$$

Section 4

Prototype

Prototypical Implementation

Device:

- Android App
- QR codes for transmitting challenges from browser to device

Prototypical Implementation

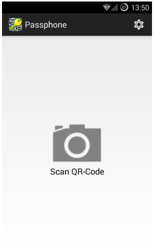
Device:

- Android App
- QR codes for transmitting challenges from browser to device

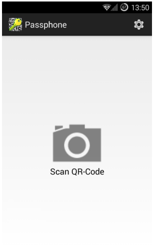
Trusted Third Party + Test Service Provider:

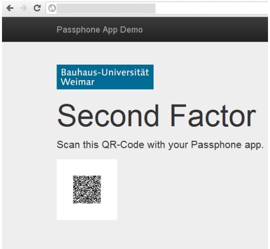
- Java Web Services for component sharing
- SHA256 for Hash$(\cdot)$; EC-DSA signatures

Prototype – Authentication



Prototype – Authentication

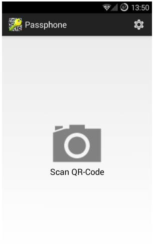


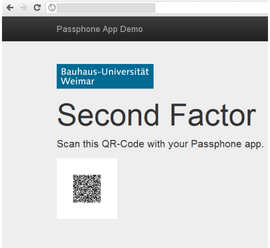


Second Factor

Scan this QR-Code with your Passphone app.

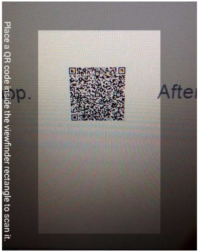
Prototype – Authentication



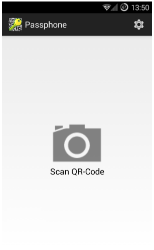


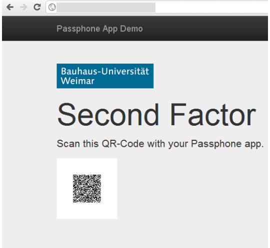
Second Factor

Scan this QR-Code with your Passphone app.


Place a QR code inside the viewfinder rectangle to scan it.

Prototype – Authentication

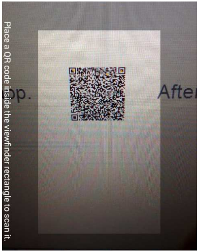


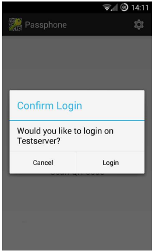

Passphone App Demo

Bauhaus-Universität Weimar

Second Factor

Scan this QR-Code with your Passphone app.


Place a QR code inside the viewfinder rectangle to scan it.



Confirm Login

Would you like to login on Testserver?

Section 5

Evaluation

Criteria of Authentication Schemes

Framework by [Bonneau et al., 2012]:

- 25 features and quasi-features
- Concerning

Security

Usability

Deployability

Comparison

Using the Framework by [Bonneau et al., 2012]

Authentication scheme	Usability								Deployability						Security (*Res.* = Resilient)											Summary	
	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable	#●	#○
Cronto [VASCO, 2013]	–	–	○	–	●	○	○	–	–	○	–	●	●	–	●	●	●	●	○	●	●	●	●	●	●	13	5
FBD-BT-BT/WF-WF [Shirvanian et al., 2014]	–	○	○	–	●	●	●	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	–	●	13	4
FBD-QR-BT/WF [Shirvanian et al., 2014]	–	○	○	–	●	●	○	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	●	●	13	5
Google 2-step [Google, 2013]	–	–	○	–	●	○	○	○	○	–	–	●	●	–	–	○	●	–	–	●	●	●	●	●	●	10	6
MBD-QR-QR [Shirvanian et al., 2014]	–	○	○	–	○	○	–	–	○	○	–	○	–	●	–	●	●	●	–	●	–	●	●	●	●	9	7
MP-Auth [Mannan and van Oorschot, 2011]	–	–	○	–	●	○	–	○	○	○	–	–	–	●	–	○	–	–	–	–	●	●	●	●	●	7	6
PhoneAuth (opportunistic) [Czeskis et al., 2012]	–	○	○	–	●	●	○	●	●	●	○	–	○	●	○	○	○	○	○	○	○	●	●	●	○	9	13
PhoolProof [Parno et al., 2006]	–	–	○	–	●	○	○	–	○	○	○	–	–	●	●	●	●	●	○	●	●	●	●	●	●	12	7
SoundProof [Karapanos et al., 2015]	–	–	○	–	●	●	○	○	●	●	–	●	–	●	○	–	●	●	–	●	●	●	●	●	–	13	4
Tiqr [Van Rijswijk and Van Dijk, 2011]	–	–	○	–	●	○	○	–	○	○	○	●	●	●	–	●	–	–	○	●	○	●	●	●	●	10	8
Passphone (this paper)	–	○	○	–	●	○	○	●	○	○	○	●	–	●	●	●	●	●	–	●	●	●	–	●	●	**13**	**7**

Comparison

Using the Framework by [Bonneau et al., 2012]

Authentication scheme	**Usability**								**Deployability**						**Security** (*Res.* = Resilient)											**Summary**	
	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable	#●	#○
Cronto [VASCO, 2013]	–	–	○	–	●	○	○	–	–	○	–	●	●	–	●	●	●	●	○	●	●	●	●	●	●	13	5
FBD-BT-BT/WF-WF [Shirvanian et al., 2014]	–	○	○	–	●	●	●	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	–	●	13	4
FBD-QR-BT/WF [Shirvanian et al., 2014]	–	○	○	–	●	●	○	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	●	●	13	5
Google 2-step [Google, 2013]	–	–	○	–	●	○	○	○	○	–	–	●	●	–	–	○	●	–	–	●	●	●	●	●	●	10	6
MBD-QR-QR [Shirvanian et al., 2014]	–	○	○	–	○	○	–	–	○	○	–	○	–	●	–	●	●	●	–	●	–	●	●	●	●	9	7
MP-Auth [Mannan and van Oorschot, 2011]	–	–	○	–	●	○	–	○	○	○	–	–	–	●	–	○	–	–	–	–	●	●	●	●	●	7	6
PhoneAuth (opportunistic) [Czeskis et al., 2012]	–	○	○	–	●	●	○	●	●	●	○	–	○	●	○	○	○	○	○	○	○	●	●	●	○	9	13
PhoolProof [Parno et al., 2006]	–	–	○	–	●	○	○	–	○	○	○	–	–	●	●	●	●	●	○	●	●	●	●	●	●	12	7
SoundProof [Karapanos et al., 2015]	–	–	○	–	●	●	○	○	●	●	–	●	–	●	○	–	●	●	–	●	●	●	●	●	–	13	4
Tiqr [Van Rijswijk and Van Dijk, 2011]	–	–	○	–	●	○	○	–	○	○	○	●	●	●	–	●	–	–	○	●	○	●	●	●	●	10	8
Passphone (this paper)	–	○	○	–	●	○	○	●	○	○	○	●	–	●	●	●	●	●	–	●	●	●	–	●	●	**13**	**7**

Comparison

Using the Framework by [Bonneau et al., 2012]

Authentication scheme		Usability								Deployability						Security (*Res.* = Resilient)											Summary	
		Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable	#●	#○
Cronto	[VASCO, 2013]	–	–	○	–	●	○	○	–	–	○	–	●	●	–	●	●	●	●	○	●	●	●	●	●	●	13	5
FBD-BT-BT/WF-WF	[Shirvanian et al., 2014]	–	○	○	–	●	●	●	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	–	●	13	4
FBD-QR-BT/WF	[Shirvanian et al., 2014]	–	○	○	–	●	●	○	–	○	○	–	–	–	●	●	●	●	●	●	●	–	●	●	●	●	13	5
Google 2-step	[Google, 2013]	–	–	○	–	●	○	○	○	○	–	–	●	●	–	–	○	●	–	–	●	●	●	●	●	●	10	6
MBD-QR-QR	[Shirvanian et al., 2014]	–	○	○	–	○	○	–	–	○	○	–	○	–	●	–	●	●	●	–	●	–	●	●	●	●	9	7
MP-Auth	[Mannan and van Oorschot, 2011]	–	–	○	–	●	○	–	○	○	○	–	–	–	●	–	○	–	–	–	–	●	●	●	●	●	7	6
PhoneAuth (opportunistic)	[Czeskis et al., 2012]	–	○	○	–	●	●	○	●	●	●	○	–	○	●	○	○	○	○	○	○	○	●	●	●	○	9	13
PhoolProof	[Parno et al., 2006]	–	–	○	–	●	○	○	–	○	○	○	–	–	●	●	●	●	●	○	●	●	●	●	●	●	12	7
SoundProof	[Karapanos et al., 2015]	–	–	○	–	●	●	○	○	●	●	–	●	–	●	○	–	●	●	–	●	●	●	●	●	–	13	4
Tiqr	[Van Rijswijk and Van Dijk, 2011]	–	–	○	–	●	○	○	–	○	○	○	●	●	●	–	●	–	–	○	●	○	●	●	●	●	10	8
Passphone	(this paper)	–	○	○	–	●	○	○	●	○	○	○	●	–	●	●	●	●	●	–	●	●	●	–	●	●	**13**	**7**

Conclusion and Summary

Key Message:

- Privacy-preserving phone-based two-factor authentication protocol
- Outsources verification of 2nd factor to TTP for increasing integration for small and medium-sized services
- Users still have to be privacy-aware on the web

Conclusion and Summary

Key Message:

- Privacy-preserving phone-based two-factor authentication protocol
- Outsources verification of 2nd factor to TTP for increasing integration for small and medium-sized services
- Users still have to be privacy-aware on the web

Summary:

- Independent from first factor
- Conducted security analysis and prototype evaluation
- Automated security analysis using AVISPA: [Armando et al., 2005]
  HLSPL code will be published online
  `https://github.com/passphone`

Conclusion and Summary

Key Message:

- Privacy-preserving phone-based two-factor authentication protocol
- Outsources verification of 2nd factor to TTP for increasing integration for small and medium-sized services
- Users still have to be privacy-aware on the web

Summary:

- Independent from first factor
- Conducted security analysis and prototype evaluation
- Automated security analysis using AVISPA: [Armando et al., 2005]
  HLSPL code will be published online
  `https://github.com/passphone`

Questions?

References I

Apple (2016).
Two-factor authentication for Apple ID.

Armando, A., Basin, D. A., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., Drielsma, P. H., Héam, P., Kouchnarenko, O., Mantovani, J., Mödersheim, S., von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L., and Vigneron, L. (2005).
The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications.
In Etessami, K. and Rajamani, S. K., editors, *CAV*, volume 3576 of *LNCS*, pages 281–285. Springer.

Bonneau, J., Herley, C., van Oorschot, P. C., and Stajano, F. (2012).
The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.
In *IEEE Symposium on Security and Privacy*, pages 553–567.

Brainard, J. G., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006).
Fourth-Factor Authentication: Somebody You Know.
In *ACM Conference on Computer and Communications Security*, pages 168–178. ACM.

Czeskis, A., Dietz, M., Kohno, T., Wallach, D. S., and Balfanz, D. (2012).
Strengthening User Authentication Through Opportunistic Cryptographic Identity Assertions.
In Yu, T., Danezis, G., and Gligor, V. D., editors, *ACM CCS*, pages 404–414.

Dey, A. and Weis, S. (2010).
PseudoID: Enhancing Privacy in Federated Login.
In Serjantov, A. and Troncoso, C., editors, *Hot Topics in PETS*, pages 95–107.

Dodson, B., Sengupta, D., Boneh, D., and Lam, M. (2010).
Snap2Pass: Consumer-Friendly Challenge-Response Authentication with a Phone.
http://prpl.stanford.edu/papers/soups10j.pdf.

Duo Security, I. (2016).
Two Factor Authentication: Duo Security.

References II

Florêncio, D. A. F. and Herley, C. (2007).
A Large-Scale Study of Web Password Habits.
In *WWW*, pages 657–666. ACM.

Google (2013).
2-step Authentication.

Karapanos, N., Marforio, C., Soriente, C., and Capkun, S. (2015).
Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound.
In *USENIX Security*, pages 483–498.

Mannan, M. and van Oorschot, P. (2011).
Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers.
J. Comput. Secur., 19(4):703–750.

Meisner, J. (2013).
The Official Microsoft Blog: Microsoft Account Gets More Secure.

Nuñez, D. and Agudo, I. (2014).
BlindIdM: A privacy-preserving approach for identity management as a service.
International Journal of Information Security, 13(2):199–215.

Nunez, D., Agudo, I., and Lopez, J. (2012).
Integrating OpenID with Proxy Re-encryption to Enhance Privacy in Cloud-based Identity Services.
In *CloudCom*, pages 241–248.

OpenID (2015).
Certification program of openid connect.
Founded be Google, Microsoft, Ping Identity, ForgeRock, Nomura Research Institute, and PayPal.

References III

Parno, B., Kuo, C., and Perrig, A. (2006).
Phoolproof Phishing Prevention.
In Crescenzo, G. D. and Rubin, A. D., editors, *FC*, volume 4107 of *LNCS*, pages 1–19.

Riesch, P. J. and Du, X. (2012).
Audit Based Privacy Preservation for the OpenID Authentication Protocol.
In *2012 IEEE Conference on Technologies for Homeland Security*, pages 348–352. IEEE.

Shirvanian, M., Jarecki, S., Saxena, N., and Nathan, N. (2014).
Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices.
In *NDSS*. The Internet Society.

Song, A. (2011).
Introducing Login Approvals.

Starnberger, G., Froihofer, L., and Göschka, K. M. (2009).
QR-TAN: Secure Mobile Transaction Authentication.
In *ARES*, pages 578–583. IEEE Computer Society.

Urueña, M., Muñoz, A., and Larrabeiti, D. (2014).
Analysis of Privacy Vulnerabilities in Single Sign-On Mechanisms for Multimedia Websites.
Multimedia Tools and Applications, 68(1):159–176.

Van Rijswijk, R. and Van Dijk, J. (2011).
Tiqr: A Novel Take on Two-factor Authentication.
In Limoncelli, T. A. and Hughes, D., editors, *LISA*. USENIX Association.

VASCO, D. S. I. (2013).
Cronto.

Section 6

Supporting Slides

Outsourcing Authentication

- **OpenID Connect** [OpenID, 2015]: Merge of
  - OpenID (Google, Yahoo!, Wordpress, etc)
  - OAuth 2.0 (Twitter, Facebook, PayPal)
- Privacy problems in OpenID and Facebook Connect [Urueña et al., 2014]
  - Linkability of users, non-resilient to phishing [Bonneau et al., 2012]
- Some attempts to solve them [Dey and Weis, 2010, Nunez et al., 2012, Nuñez and Agudo, 2014, Riesch and Du, 2012]

OATH Standards

- 2005: HOTP (Hash-based One-Time Passwords)
  - HMAC-based one-time passwords
- 2011: TOTP (Time-based One-Time Passwords)
  - Based on HOTP
  - Passwords only work for a small time slot (30-60 seconds)
- Ongoing: FIDO (Fast IDentity Online) Allicance promotes U2F (Universal 2nd Factor, public-key-based)
  - Computer + USB device

Consistent Messaging Format

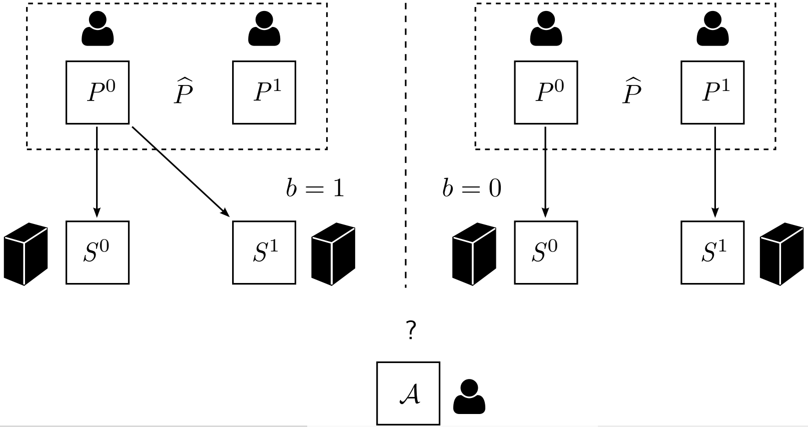
- Add consistent protocol, step, version, and sender information to every message

$$\begin{aligned}\langle\text{message}\rangle &::= E_K(\langle\text{header}\rangle, \langle\text{payload}\rangle)_{\langle\text{signature}\rangle}\\ \langle\text{header}\rangle &::= [\langle\text{domain}\rangle, \langle\text{step}\rangle, \langle\text{version}\rangle, \langle\text{sender}\rangle]\end{aligned}$$

Unlinkability

Modelled as a Real-or-Random Game

- **Setup:** Challenger registers either P^0 with both S^0 or S^1; or P^0 with S^0 and P^1 with S^1
- Game uses $\widehat{P}$ as compound user in view of $\mathcal{A}$
- **Goal of $\mathcal{A}$:** Determine who interacts with S^1



Unlinkability

$\mathcal{A}$ can learn from a run of...

- ...the registration protocol: Nothing about relations
- ...the activation protocol:
  Mapping $h_{PT^i} \rightarrow h_{S^j}$, where $h_{S^j} = \mathsf{Hash}(ID_{S^j}, N_{S^j})$
- ...the authentication protocol: $h^j_{PT^i}$

- Only $h^j_{\widehat{P}} = \mathsf{Hash}(ID_{PT^b}, N_T)$ visible
- $\mathcal{A}$ must find a preimage ID_{PT^b}, N_T for $h^j_{\widehat{P}}$

Unlinkability

$\mathcal{A}$ can learn from a run of…

- …the registration protocol: Nothing about relations
- …the activation protocol:
  Mapping $h_{PT^i} \to h_{S^j}$, where $h_{S^j} = \mathsf{Hash}(ID_{S^j}, N_{S^j})$
- …the authentication protocol: $h^j_{PT^i}$

- Only $h^j_{\widehat{P}} = \mathsf{Hash}(ID_{PT^b}, N_T)$ visible
- $\mathcal{A}$ must find a preimage ID_{PT^b}, N_T for $h^j_{\widehat{P}}$

Theorem 2 (Unlinkability)

Let the employed public-key signature scheme be EUF-CMA-secure and H be a random oracle. Then, for any PPT adversary $\mathcal{A}$ whose run time is bounded by t and which asks at most q_{exe} execute and q_{send} send queries, It holds for a random execution of $\mathcal{G}^{Unlink}$ on our protocol $\mathbb{P}$:

$$\boldsymbol{Adv}^{Unlink}_{\mathbb{P}}(\mathcal{A}) \le (q_{exe} + q_{send}) \cdot 1/2^{2\tau}.$$

Authentication Security

Proof Ideas (Cont'd)

Framework by Bellare et al. **Queries:**

Execute(P^i, S^j, T) Passive $\mathcal{A}$ that eavesdrop on connection between P^i, S^j, and T.

Send(U, U', m) Active attack, sending a message m between users $U \xrightarrow{m} U'$

Corrupt(P^i, S^j) Leaks first factor of P^i at S^j

Test(P^i, S^j) Models authenticaton request of $\mathcal{A}$ as P^i at S^j