UNIVERSITY OF CAMBRIDGE

Explicit Delegation using Configurable Cookies

SPW 2016

David Llewellyn-Jones, Graeme Jenkinson, Frank Stajano

{David.Llewellyn-Jones, Graeme.Jenkinson, Frank.Stajano}@cl.cam.ac.uk

Pico Project, University of Cambridge

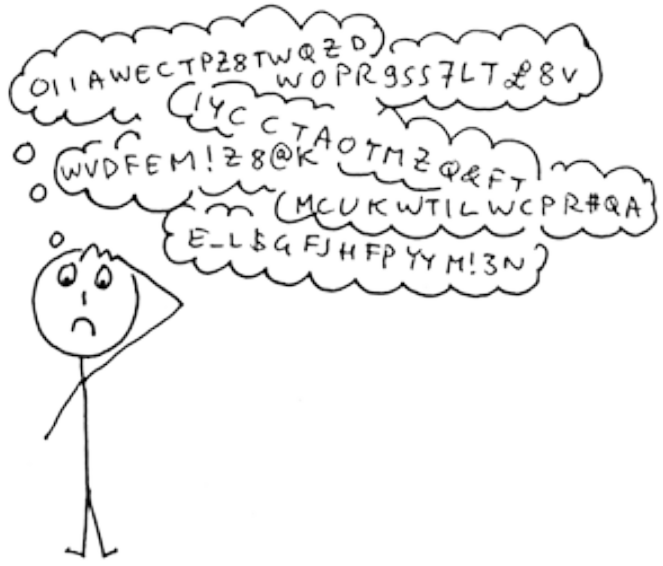
8th April 2016

Overview

Preliminary research around delegation.

Undertaken as part of the Pico project.

Our starting point is password delegation and the question of how to replace this functionality with something ‘better’.



People Share Passwords

Yes, they do!

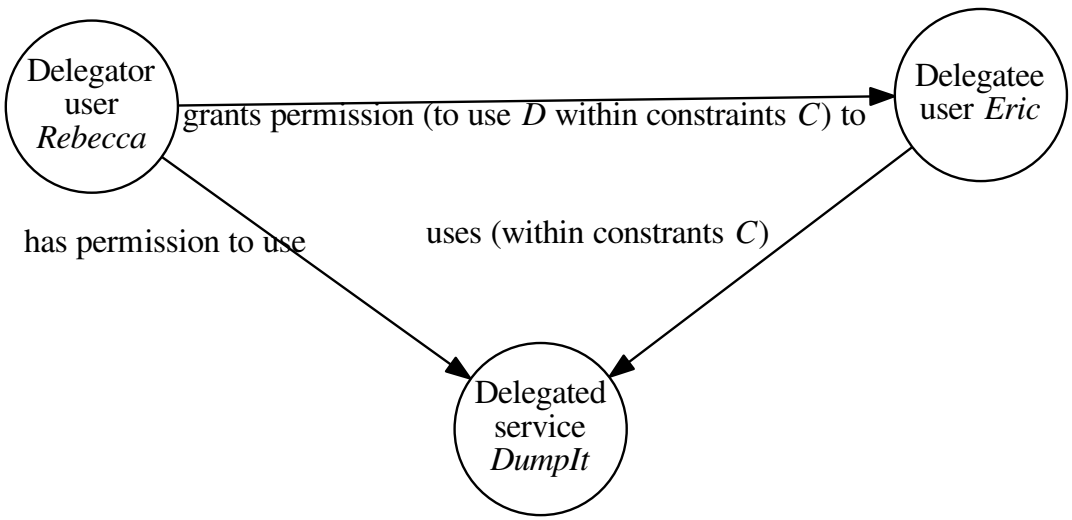
http://uk.pcmag.com/password-managers-products/35518/feature/tips-for-sharing-passwords

Common Practice

Rebecca gives Eric her password (PIN, token, phone) for DumpIt to Eric, so that he can perform some action.

Eric then forgets Rebecca's password (or doesn't).

1. Delegato**r** **R**ebecca
2. Delegate**e** **E**ric
3. Delegate**d** **D**umpIt



It's not secure, but is useful, simple and intuitive functionality.

Implicit Requirement

Rebecca needs to trust Eric

CNN Regions » British police tricked terror suspect into handing over phone, source says

Police officers posed a company managers

Khan was arrested in mid-July 2015. Undercover police officers posing as company managers arrived at his workplace and asked to check his driver and work records, according to the source. When they disputed where he was on a particular day, he got out his iPhone and showed them the record of his work.

Junead Khan, left, and Shazib Kahn plotted to join ISIS, prosecutors say.

The undercover officers asked to see his iPhone and Khan handed it over. After that, he was arrested. British police had 30 seconds to change the password settings to keep the phone open.

"It was very important we actually took possession of that phone ... a lot of evidence presented at court was held on that phone," Dean Haydon, the head of Counter Terrorism Command of the British Metropolitan Police, told CNN.

Haydon told CNN Khan had used his phone to keep in contact with ISIS fighters.

http://edition.cnn.com/2016/04/01/europe/uk-isis-terror-convictions/

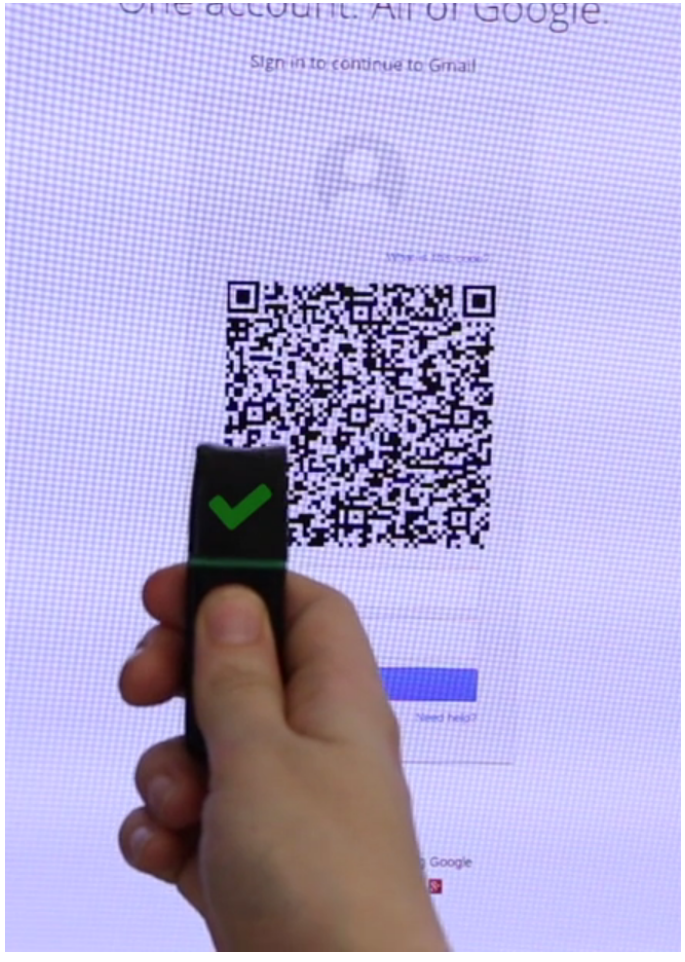
Pico Project

Pico: No more passwords!

Can Pico provide a better alternative approach to delegation?

So we thought: "How would we extend Pico to support delegation?"

It turned out, Pico was doing it already.



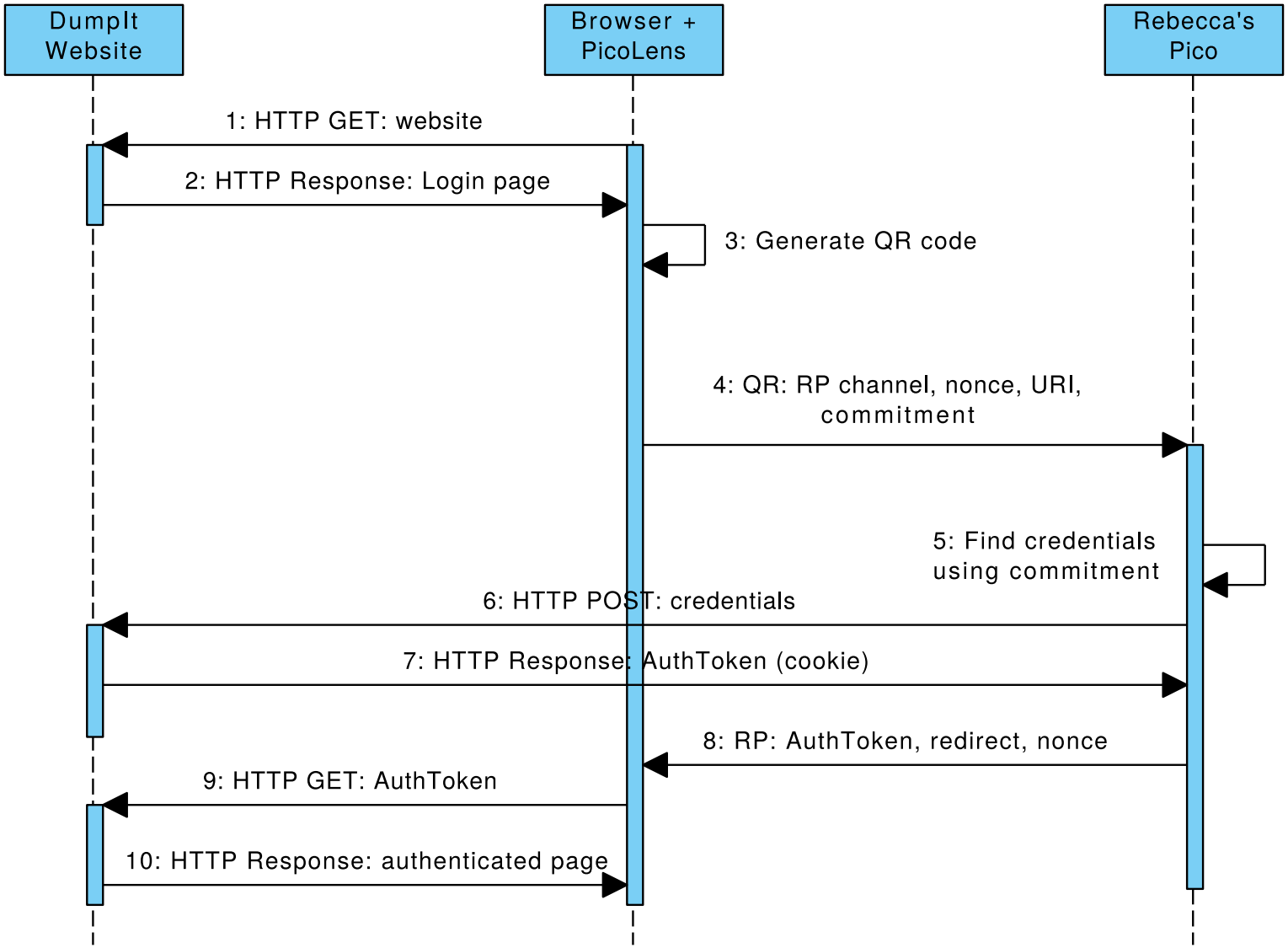
http://mypico.org

Contributions

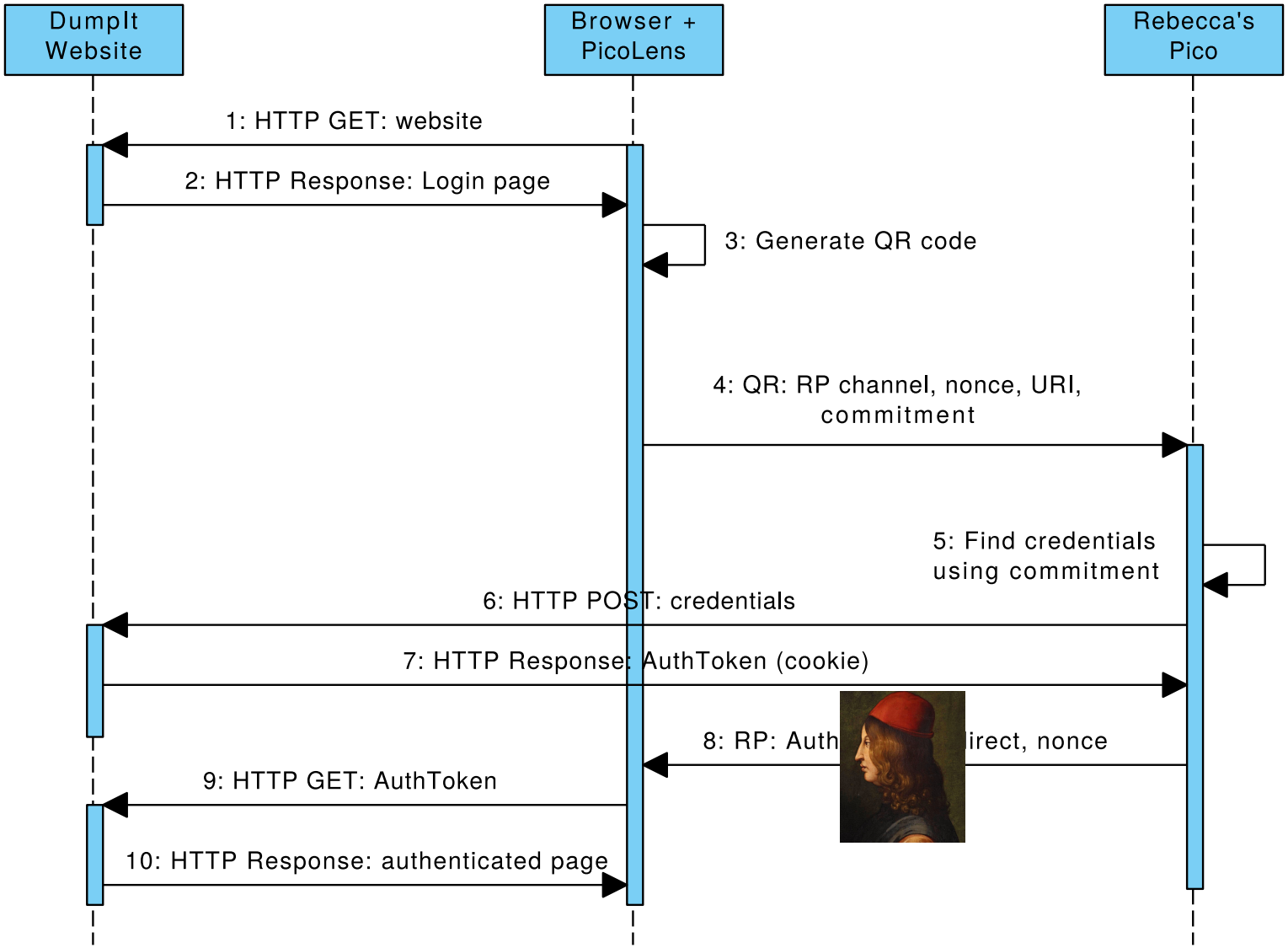
1. A solution offering security, reducing reliance on goodwill and using existing Web technologies.
2. A taxonomy to explore the space of possible delegation solutions.
3. A theorem that you cannot delegate securely and revocably without introducing technical changes to the verifier.
4. Open questions.

We want a *practical* solution.

Standard Non-Delegated Authentication

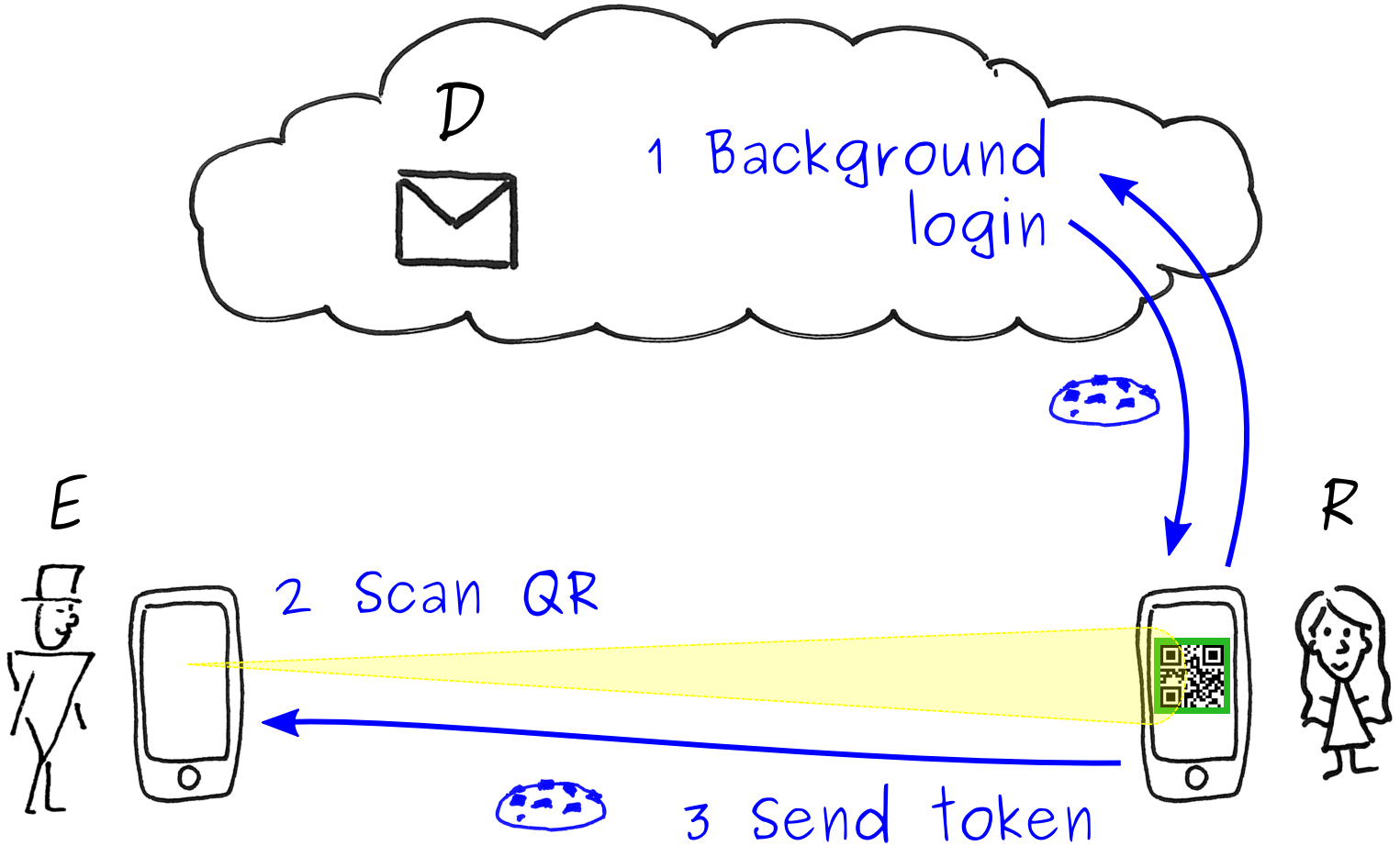


Standard Non-Delegated Authentication



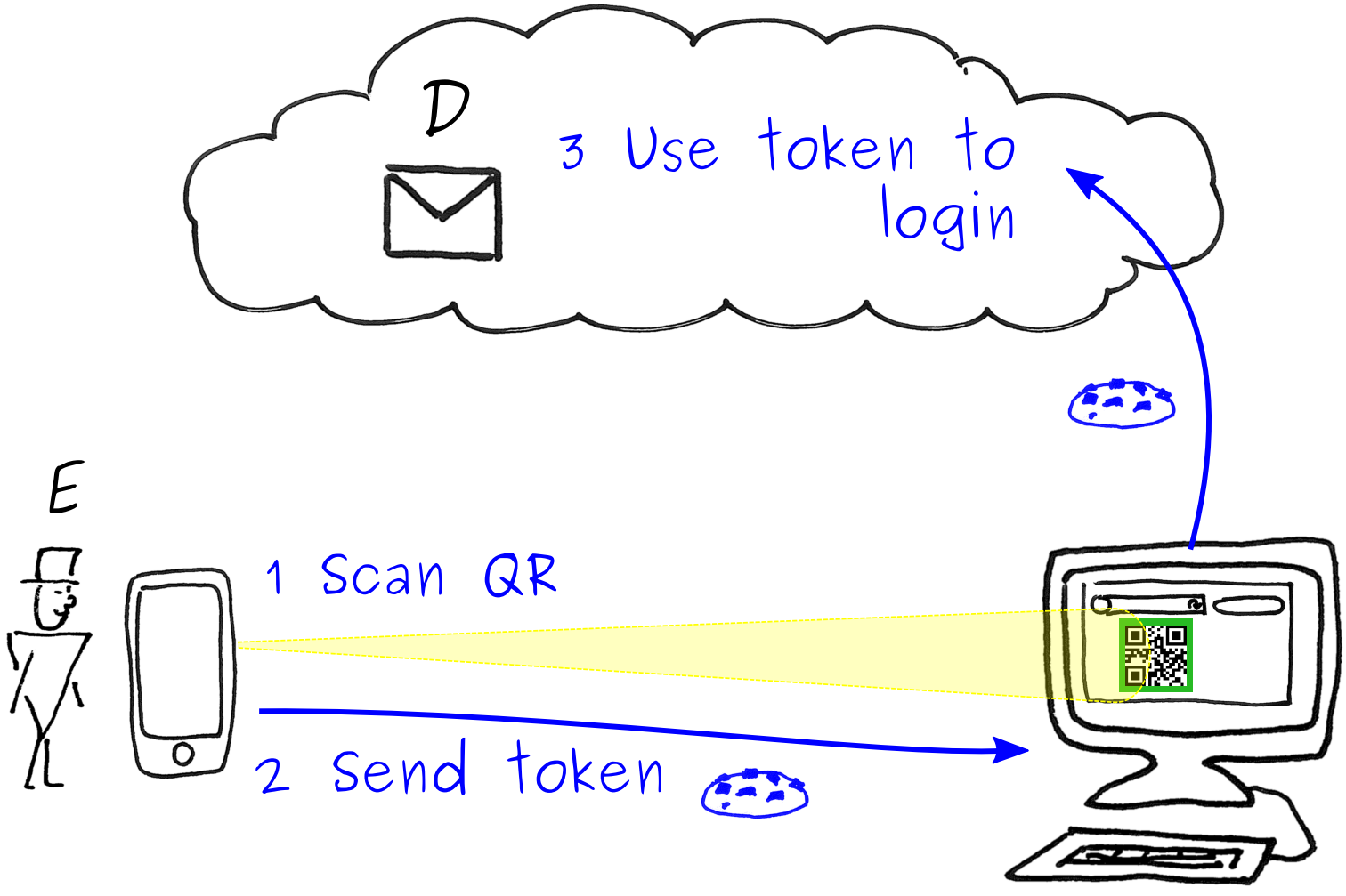
Delegation of Token

From Rebecca to Eric

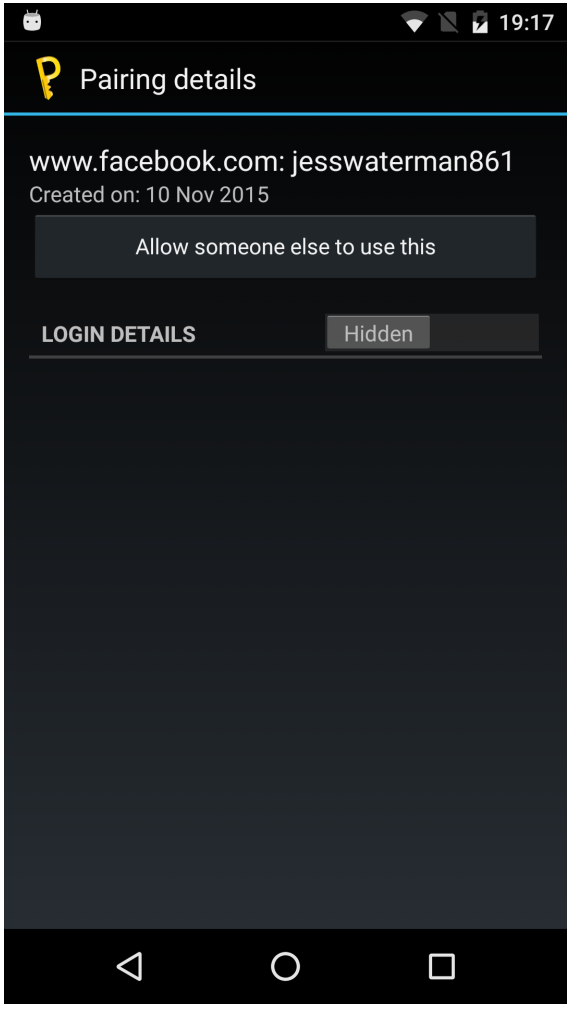


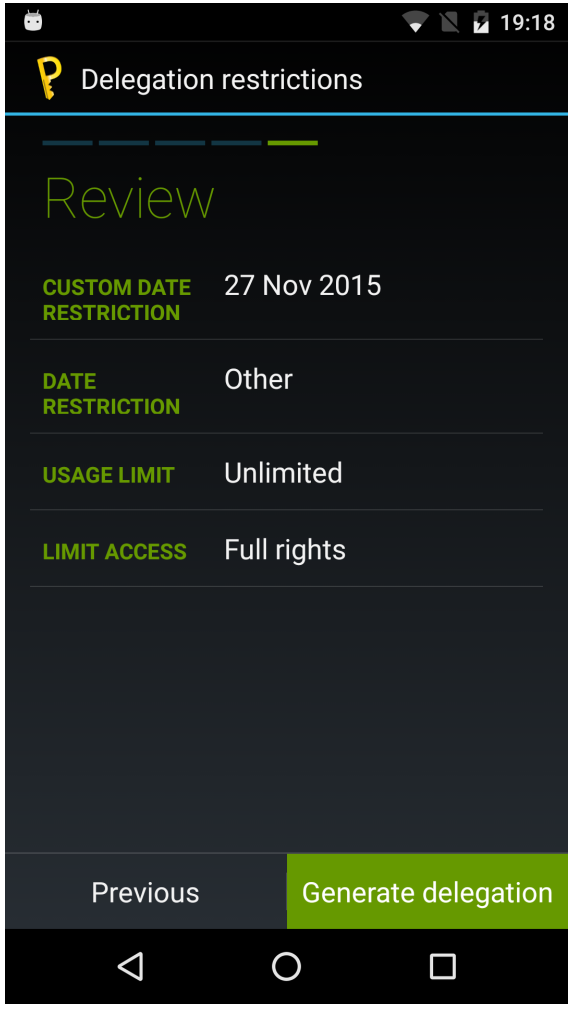
Use of Delegated Token

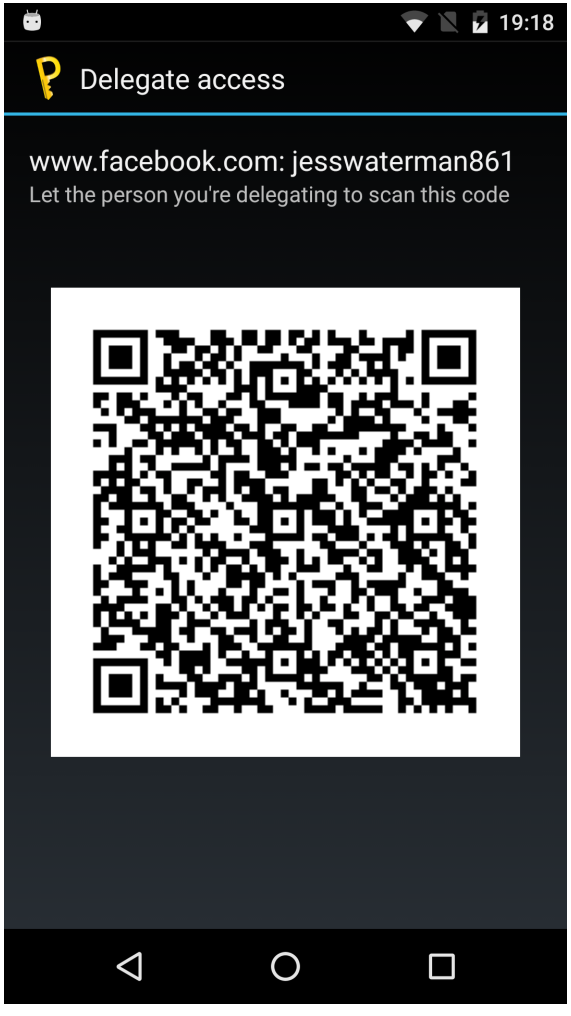
Between Eric and DumpIt



Pico Interface







Implementation

Demonstrates it as practically achievable.

But compared to password delegation:

1. Is it more secure?
2. Is it as usable?
3. Is it as flexible?

We've tried to break down delegation into its constituent features.

???

Bauer, L., Cranor, L.F., Reiter, M.K., Vaniea, K., "Lessons learned from the deployment of a smartphone-based access-control system" SOUPS 07.

Question

Would real people actually use the functionality? Will users take the time to learn about and apply tight delegation rules?

Palfrey, J., Sacco, D.T., boyd, d., DeBonis, L., Tatlock, J., "Enhancing Child Safety and Online Technologies" ISTTF 2008.

Question

Is there a way to avoid formal delegation processes becoming a mark of distrust?

Delegation Features

Variable	Type	Values
Usability	cont	low – high
Expressiveness/flexibility	cont	low – high
Security	cont	low – high
Trust required	cont	low – high (of E by R)
Accountability of E	discrete	$\emptyset$, E, R, D, ER, ED, RD, all
Plausible deniability of E	discrete	full, RD, ED, ER, D, R, E, $\emptyset$
Involvement at creation	discrete	$\widehat{ER}$, ER, ED, $\widehat{ERD}$, ERD
Involvement at operation	discrete	ED, EDR
Revocable by	discrete	$\emptyset$, R, D, RD

Example: Passwords

$$
\begin{array}{rclrcl}
\mathit{usability} & = & \mathsf{high}, & \mathit{flexibility} & = & \mathsf{min}, \\
\mathit{security} & = & \mathsf{min}, & \mathit{trust} & = & \mathsf{max}, \\
\mathit{accountability} & = & \emptyset, & \mathit{deniability} & = & \mathsf{full}, \\
\mathit{creation} & = & \widehat{ER}, & \mathit{operation} & = & \mathit{ED}, \\
\mathit{revocable} & = & \emptyset. & & &
\end{array}
$$

Example: Pico

Relies on the content of the cookie.

Is a cookie more or less powerful than a password?

1. Can't be more powerful.
2. Can sometimes be less powerful.

WordPress Cookie

$$cookie = username \mid expiration \mid token \mid hash.$$
$$hash = SHA256(username \mid expiration \mid token,$$
$$MD5(username \mid passfrag \mid expiration \mid token)).$$

Example: Pico

Pico using cookies:

$$
\begin{array}{rcl@{\qquad}rcl}
\mathit{usability} & = & \text{medium}, & \mathit{flexibility} & = & \text{medium}, \\
\mathit{security} & = & \text{medium}, & \mathit{trust} & = & \text{medium}, \\
\mathit{accountability} & = & RD, & \mathit{deniability} & = & R, D \\
\mathit{creation} & = & \widehat{ER}, & \mathit{operation} & = & ED, \\
\mathit{revocable} & = & D. & & &
\end{array}
$$

Passwords (for reference):

$$
\begin{array}{rcl@{\qquad}rcl}
\mathit{usability} & = & \text{high}, & \mathit{flexibility} & = & \text{min}, \\
\mathit{security} & = & \text{min}, & \mathit{trust} & = & \text{max}, \\
\mathit{accountability} & = & \emptyset, & \mathit{deniability} & = & \text{full}, \\
\mathit{creation} & = & \widehat{ER}, & \mathit{operation} & = & ED, \\
\mathit{revocable} & = & \emptyset. & & &
\end{array}
$$

Relationships

Claim (1)

The following relationships are intrinsic to the nature of delegation.

1. *There is an inverse relationship between expressiveness and usability.*
2. *There is a direct relationship between expressiveness and security.*
3. *There is an inverse relationship between security and trust.*
4. *Accountability is the precise inverse of plausible deniability.*
5. *Revocation implies accountability.*

Expressiveness

We can identify expressiveness as a key lever for controlling security and trust.

Claim (2)

For Rebecca to minimise her exposure she must restrict the permissions entrusted to Eric to just those needed for him to carry out his task.

Verifier Involvement

Who can control the expresiveness and its enforcement? Only the service provider.

Claim (3)

The security-trust balance of delegation can only be achieved if the verifier offers a means of expressing fine-grained permissions.

???

Question

Is it appropriate to make this functionality available, or better to wait until sites offer the security of configurable cookies?

Experiences

The situation can be improved using cookies as an authorisation token.

This can provide a path for the evolution of delegation.

1. From passwords to cookies.
2. From cookies to expressive cookies.

Not perfect in many ways.

1. Can't prevent someone passing the cookie on.
2. Buy-in needed from end users and verifier.

Open Questions

1. Is it appropriate to make this functionality available, or better to wait until sites offer the security of configurable cookies?
2. Would real people actually use the functionality? Will uses take the time to learn about and apply tight delegation rules?
3. Is there a way to avoid formal delegation processes becoming a mark of distrust?
4. Can we enforce non-transitive delegation without Eric having an account, and without conflicting with plausible deniability?
5. Many sites offer REST-ful APIs for delegated access by trusted apps using OAuth. Do these provide a better starting point?