DelegaTEE: Brokered Delegation using Trusted Execution Environments

**Sinisa Matetic (ETH Zurich)**, Moritz Schneider (ETH Zurich), Andrew Miller (UIUC), Ari Juels (Cornell Tech), Srdjan Capkun (ETH Zurich)

27th Usenix Security Symposium, August 12-17, 2018, Baltimore, MD, USA
Motivation – Account sharing with restrictions
Motivation – Account sharing with restrictions

PayPal Student Account
- Effective April 25, 2018, PayPal Student accounts are no longer be able to make purchases online. The send money feature to transfer funds from the Student Account to the parent’s PayPal account will be available until April 25, 2018.

Are there other PayPal products I can use to send money to my student?
At this time, we aren’t introducing a replacement for PayPal Student Accounts and PayPal Student Debit MasterCards. We will continue to explore ways to serve our younger population in the future. If
Motivation – Account sharing with restrictions

- Bob really wants to make Alice happy…
- Bob is fine sharing his account…
- But, he doesn’t really want to reveal his login credentials to Alice and also give her unlimited spending capabilities…

- (since Bob is very security aware and uses the same password in all web service that he has… :D)
Motivation – Account sharing with restrictions

- If only the service would support such a scheme...
- Applicable to all types of online services and action performed on the web
  - Delegation is only possible if directly supported by the service provider

Authorize Tweetgif.com to use your account?

This application will be able to:
- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

Authorize app  No, thanks

This application will not be able to:
- Access your direct messages.
- See your Twitter password.

Request for permission

Test Feed Test is requesting permission to do the following:
- Access my basic information
- Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.
- Post to my Wall
- Test Feed Test may post status messages, notes, photos and videos to my Wall
- Access posts in my News Feed
- I will not be able to access my data when I'm not using the application.
- Access my photos and videos
- Photos uploaded by me

Report application

Logged in as Russell Says (Not you?)

Allow  Don't allow
Solution – Brokered Delegation

Bob

OR

Service

Alice
- DelegaTEE: Brokered Delegation using Trusted Execution Environments
**Trusted Execution Environments**

- Enable isolated execution within a user’s system
  - ARM Trustzone, Intel SGX, …
- Intel SGX – secure enclaves
  - Runtime isolation, ecall/ocall interfaces, sealing, attestation
  - Memory content encrypted

- NOTE: Recent work shows successful compromise of such environments
  - Side-channel attacks, Spectre, Meltdown, Foreshadow (see talks from yesterday)
  - Patches on the way
Our contribution: Brokered Delegation with enclaves

- A new concept that seems very familiar
- Flexibly, securely and selectively share and delegate access (credentials and rights)
- No explicit support (or even knowledge) of the service providers
- Fine-grained delegation without trust between the credential owner and other users
- Supported with the usage of TEEs
- Credential Owners (give access) and Delegatees (receive restricted access)
DelegaTEE - Challenges and desired properties

- The Owner’s credentials remain confidential.
- The Owner can restrict access to his account, e.g., in terms of time, duration of access, no. of reads/writes etc. - with rich contextual policies
- The system logs the actions of Owners and Delegatees so that post-hoc attribution of their behaviour is possible (as a means of resolving disputes)
- The system minimizes the ability of a service to distinguish between access by the Delegatee and that of the legitimate Owner

- Owner does not have to always be online
DelegaTEE – two system designs

- Peer-to-peer system model
- Centrally brokered system model
Owners A₁...n → agreement on credential delegation any informal communication channel → Delegatee B₁...n

1. owner registration
   - login information acquired
   - establish secure communication

2. store credentials for Services G₁...n

3. any informal communication channel

4. Owner Aᵢ exchange unique identifiers for the system Delegatee Bⱼ

5. Owner Aᵢ: delegate credentials Cₓ to Bⱼ for service Gₖ with access control policy Pᵢⱼₓₖ

6. ok

7. * enforced and constrained under specified access control policy in the central system

8. establish secure communication available delegated credentials

9. service access*
   - check access control policy
   - if expired, terminate access

* Centrally Brokered system

Siniša Matetić | 17.8.2018 | 12
Trust assumptions and security

- Intel SGX enclaves are trusted for confidentiality and attestation
  - The Owner is to be fully protected
- Server and the operator *per se* do not need to be trusted

- System works as trusted a proxy, a man-in-the-middle
  - End-to-end TLS from enclave-to-delegatee and enclave-to-service
Case Study Implementation 1: PayPal

1. Owner
   - Username
   - Password

Policy:
- To whom
- Restrictions

2. Delegatee

3. Centrally Brokered system

4. API enclave

5. PayPal enclave

6. Confirmation

7. Confirmation

Merchant

PayPal

Demo Case Study Implementation 1: PayPal

Confirmation
3. Payment

PayPal
PayPal is an international payment service allowing transactions to be made directly between vendors and buyers. PayPal processes your payment before forwarding it to us. Further information about this service is available on www.paypal.com.

4. Delivery options

Without delivery note or receipt
Saturday delivery permitted
Preferred delivery date: None (as soon as possible)

5. Order overview

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Price</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taco Powerband Montagband Ultra</td>
<td>1</td>
<td>10.70</td>
<td>10.70</td>
</tr>
<tr>
<td>Strong (Thick, 3rd)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 items</td>
<td></td>
<td>ready for delivery from our warehouse</td>
<td></td>
</tr>
</tbody>
</table>

Total Products: 10.70
Payment fee: 0.55
Minimum order value (before VAT): 0.00
Total excl. VAT: 26.15
Total incl. VAT: 28.25

If not stated otherwise, all prices are including VAT and in CHF.

By placing your order you accept the terms and conditions. If your order contains tobacco products or alcoholic beverages, you hereby confirm to be 18 years or older.

[Pay]
Demo

Select PayPal Credentials

<table>
<thead>
<tr>
<th>Delegator</th>
<th>Name</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>andrew</td>
<td>personal+paypal</td>
<td></td>
</tr>
<tr>
<td>srdjan</td>
<td>personal_paypal</td>
<td></td>
</tr>
</tbody>
</table>

Execute payment

Close
Demo

DelegaTEE PayPal Captcha

Submit
Close

8Z6cNRVb
Thank you for your order

You will receive an order confirmation e-mail shortly.

Order: 16320090

Payment:
Your PayPal payment of CHF 28.25 incl. tax confirmed.

Order overview and delivery status of the ordered products

Monitor the order status, expected delivery time and payment status in your customer account. Please keep in mind that an order confirmed more than one time will only be dispatched when all products are available. Exceptions are direct deliveries made by some of our suppliers. There is no option of triggering a partial delivery in your customer account. Simply go to delivery details in the order overview. Should you have any questions regarding the delivery, please do not hesitate to contact our customer service.

Back to start page  |  Show order

Demo

360 Eye: Dyson’s first robot vacuum cleaner

Galaxy Deal of the day
Go to all current offers

109.- instead of 145.
1 Turmix Soupmaker

Galaxy Live

Customer feedback

Very friendly and competent service.
A. from Zurich per 03.10.2017
Case Study Implementation 2: Credit Card - Demo

Credit card number

CVV

Expiry month

Expiry year

Pay with Credit Card

Pay with DelegaTEE

Select Credit Card

Delegator | Name | Select
---|---|---
srdjan | institute_credit_card | 

Execute payment

Close
Case Study Implementation 3: Email - Demo

DelegaTEE Mail Client

Inbox

From | Subject | Received
--- | --- | ---
anonymised | Test mail | Fri, 16 Jun 2017 11:09:42 +0200
anonymised | next test | Fri, 16 Jun 2017 14:42:24 +0200
anonymised | Sending mails using Intel SGX and DelegaTEE | Mon, 30 Oct 2017 09:24:18 -0700 (PDT)
anonymised | from my inf ethz to mail enclaves | Wed, 4 Oct 2017 14:12:18 +0000
anonymised | from my gmail to test gmail | Mon, 2 Oct 2017 17:45:51 +0200

DelegaTEE Mail Client

New Mail!

**To:**

bob@mail.com

**Subject:**

Hi

**Text:**

Hi Bob,

...
Case Study Implementation 4: General website browsing - Demo

Login form with username and password fields.

SGX HTTPS Proxy:
- www.google.com
- Go button

Secure HTTPS connection indicated.
**Performance**

- In line with the original performance of the use case scenario
- P2P system
  - Minimal and negligible overhead
  - Functions as a local proxy
  - Supports all provided use-cases

- Centrally Brokered System
  - Serves all delegation request through a central system
  - All use cases except video streaming handled almost instantaneously
  - No. of concurrent users depends on the server hardware
Brokering Delegation may undermine service’s policy enforcement

- MAC-to-DAC
  - Similar to the setuid in Unix systems

- Building secondary markets for any service
  - Netflix, and any other video streaming service
  - Paid subscription services, such as news portals, etc.
  - …

- Services expect the difficulty of broadly sharing credentials
Discussion, Challenges and Limitations

- Identity-based model
- Anonymous model

Policy creation and enforcement
- Easy for standardized protocols and messages
- More difficult for a general use-case example
- Curated "policy app store" for different use cases?

For more details please see the paper!
Discussion, Challenges and Limitations

- Authentication challenges
  - Two-step authentication
  - CAPTCHA
- Authentication Collisions
- Usability
- Deployment
- Service Prevention
- Scalability

For more details please see the paper!
Summary & Conclusion

- Secure and flexible delegation of user access rights and credentials
- Applicable for online transactions with password-based authentication
  - Can be developed to support brick-and-mortar transactions
- No changes needed on the service side
- Compatibility with wide range of services
- Rise of new sharing economies and business models
- A potential game changer? Market disruptor?
Thank you for your attention! Questions?

Sinisa Matetic

ETH Zurich
System Security Group
Institute of Information Security
Department of Computer Science

www.syssec.ethz.ch

sinisa.matetic@inf.ethz.ch

© ETH Zurich, August 2018