DELEGA TEE: Brokered Delegation Using Trusted Execution Environments

Sinisa Matetic and Moritz Schneider, ETH Zurich; Andrew Miller, UIUC; Ari Juels, Cornell Tech; Srdjan Capkun, ETH Zurich
Overview

• Background
• Introduction
• Problem Statement

• DELEGATEE
  • Security Analysis
  • Implementation
  • Performance Analysis
  • Limitations

• Conclusion
Background

• **Brokered Delegation** – allows user’s to flexibly share and delegate access, without requiring explicit support from service providers
  • New type of delegation restricted under policy enforcements by a TEE enclave

• **Trusted Execution Environments (TEEs)** - a secure area inside a main processor
  • Emergence of TEEs, such as Intel SGX, enables an alternative way to achieve delegation without trust between the Owner and Delegatee
Introduction

• Many online services either have limited support or no support for delegation
  • Delegation – the ability to share a portion of one’s authority with another
• Delegation allows user’s to safely and selectively secure online accounts and services
• Researcher’s created DELEGATEE
  • Provides brokered delegation for many existing web services
Problem Statement

• Two major motivations:
  • To demonstrate the many settings in which brokered delegation gives rise to new functionality
  • To demonstrate how trusted hardware TEEs can transform any mandatory access control policy within online services into a discretionary one

• DELEGATEE allows users to delegate authority

• Challenge: Without backend support two possible strategies
  • Owner remains online and mediate requests
  • Owner provides Delegatee with a resource for unmediated access
DELEGATEE

Owner’s Credentials → TEEs / Intel SGX → Delegation Policy → Web Service
DELEGATEE

• Decentralized Peer-to-Peer System
  • A system in which a Delegatee uses brokered credentials to execute secure enclaves

Figure 1: DELEGATEE’s P2P system architecture
DELEGATEE

- Centralized Broker System
  - A system which operates through a third party
DELEGATEE System Design Details

• DELEGATEE supports both identity-based (non-anonymous) and anonymous use models
  • Identity-based model
  • Anonymous model

• Policy Creations and Enforcement
  • Aim to prevent attackers from modifying the policies or changing the enforcement
  • Burden remains on the Owner to choose an appropriate access control policy
Security Analysis

• Main security proprieties that DELEGATEE will ensure
  • Owner’s access credentials remain confidential
  • The use of the delegated credentials is defined by the access control policy which will not be violated.
  • Use of the credentials should only be granted to the intended Delegatee, as authorized by the Owner

• DELEGATEE system is designed in a way that breaking the SGX protection mechanism on an arbitrary enclave will not weaken the system

• Attacker will need to break the exact enclave running DELEGATEE
Implementation

• DELEGATEE was implemented on four service specific enclaves
  • Mail
  • PayPal
  • Credit card/e-banking
  • Full website access
• An additional enclave was implemented to authenticate users and store credentials
• A browser extension was implemented to communicate with the Centrally Brokered system and Delegatee
Implementation - Mail

- DELEGATEE implemented in the mail enclave
Implementation - PayPal

• DELEGATEE was implemented using the no javascript fallback mechanism from PayPal
• Tested using PayPal’s sandbox and real-world environment
• Browser extension allows the user to choose DELEGATEE at checkout
Implementation – Credit Card/E-Banking

- Similar to the implementation of the PayPal enclave
- Upon checkout the browser extension is triggered if a payment form is available
Implementation – Full Website Access

• Implemented a HTTPS proxy enclave using cookies to set the correct host name and parse through requests
Performance Analysis

• Conducted on two i7-7700 machines with 16 GB RAM, connected via the internet and local network
• Can serve up to 100 users
• Mail, PayPal, Credit Card, and Full Website Access performed well
• Testing conducted on streaming websites, such as Netflix, was the same to normal streaming
Limitations

• Development of a generic module to support a variety of services
• Authentication challenges
  • Two-Step Authentication
  • IP Address changes
  • Simultaneous login attempts
• Bandwidth to support video streaming
• Secondary markets
Conclusion

• Proposed a new concept called Broker Delegation, which uses TEEs to enable flexible delegation
• Implementation and experiments show that DELEGATEE can be applied to real-world applications
• DELEGATEE runs with minimal overhead and preserves security against a strong attacker