先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	サイバーレジリエンス構成学 （門林　雄基　（教授））		
学籍番号	2211316	提出日	令和 6年 1月 19日
学生氏名	湯浅　潤樹		
論文題目	アクセス制御とプログラム記述可能なテストを通じたOpenID Connect利用時の安全性強化についての研究		

要旨

近年，webサービスにおけるユーザのアカウント管理の負担を削減するためにシングルサインオン(SSO)の導入が進んでいる．主要なSSOプロトコルであるOpenID Connectを利用する際には，認証フローをどのようにサービスに組み込むかについてのユースケース設計を行い，ユースケースに基づく具体的なプログラム実装を行う．OpenID Connectの安全な利用のために，ユースケース設計ではユーザの真正性の保証が求められ，実装では認証・認可目的で使用されるトークンの漏洩を防ぐための事前の脆弱性検証が求められる．しかし，一般的に利用されるユースケースではユーザ真正性が侵害される可能性があり，既存のテストツールは存在しうる脆弱性を網羅することができない．本論文では，一般的に使用されるユースケースにおける問題と既存のテストツールにおける問題を定義する．(1)ユースケースにおける問題．OpenID Connectを利用するwebサービスにおいては，ユーザ認証を行うIDプロバイダから発行されるIDトークンを，ユーザのブラウザ経由で受け取ってユーザを認証し，認証後にはユーザのセッション識別のためのトークン（セッショントークン）を用いて認可を行うことが一般的である．しかし，IDトークンやセッショントークンを不正取得・利用ができる場合に，攻撃者は正規ユーザになりすますことができ，ユーザ真正性が侵害される．(2)テストツールにおける問題．OpenID Connectでは仕様から乖離した実装による脆弱性（仕様違反の脆弱性）だけではなく，仕様で定義されていない部分が原因で脆弱性（実装に起因する脆弱性）が生じる．実際に起こりうる様々な認証フローを模擬するために，シナリオベースのテストツールが存在しているが，既存テストツールはシナリオのカスタマイズ性が乏しく，仕様違反によって生じる脆弱性しか検出できない．

本論文では，アクセス制御とプログラム記述可能なテストにより，これらの問題を解決する．第一に，ユースケースにおける問題を解決するために，ID/セッショントークンを用いたなりすましを防ぐ新たなアクセス制御機構を提案する．このアクセス制御機構では，認証時にIDトークンを用いたなりすましを防ぐために，ユーザ登録の際に一度だけ生成される秘密鍵・公開鍵を用いた署名の作成と検証を行う．また，認証後にセッショントークンを用いたなりすましを防ぐために，認証完了時に生成される秘密情報を用いたハッシュ値の作成と検証を行う．そして，認証後の機密性の高い操作においては，パスワードレス認証技術であるFIDOを用いた認証を併用することで正しいユーザであることを確認する．第二に，テストツールにおける問題を解決するために，テストカバレッジとシナリオのカスタマイズ性の担保を両立する新たなテストツールを提案する．このテストツールは，シナリオをプログラム記述可能にすることでシナリオのカスタマイズ性を確保している．また，脆弱性分析に基づくシナリオ記述機能の設計により，仕様違反の脆弱性だけでなく，実装に起因する脆弱性を検証するテストシナリオの記述と実行が可能である．OpenID Connectの利用における2つの問題を解決することで，ユースケースと実装の両面からの安全性強化を実現する．