ActiveDirectoryへの偽アカウント登録不要な新しい欺瞞システムの提案
new deception system without registering fake accounts in Active Directory

戸渡晃輝・ネットワーク分科会・情報セキュリティ大学院大学

研究背景

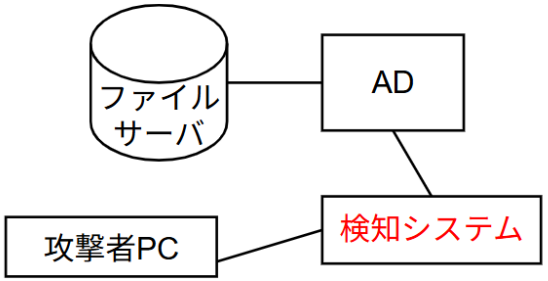
Active Directoryはネットワーク全体の認証及びアクセス制御を一元的に管理していることから，広くの企業や組織で利用されている．そのため，攻撃者にとって重要な標的となる．

目的

Active Directory環境における不正侵入の被害拡大の防止を目的とし，実在するユーザ情報の悪用を防止する．
本提案では，既存手法の課題であるハニーアカウントのAD管理やサーバ負担などを軽減する．

提案手法

ADの認証方式であるKerberos認証に焦点をあてる．
ネットワーク監視のみで偽情報に対するのAS通信から不正認証試行を検知するシステムを提案する．



今後の方針

- リアルタイムでログイン試行を検知する自動化スクリプトの作成
- 実機を通しての検証
- 既存手法の導入と提案手法との比較