情報セキュリティ研究センター
Research Center for Information Security

情報漏洩に堅牢な認証およびその応用

古原　和邦、斉藤　匡人、辛　星漢

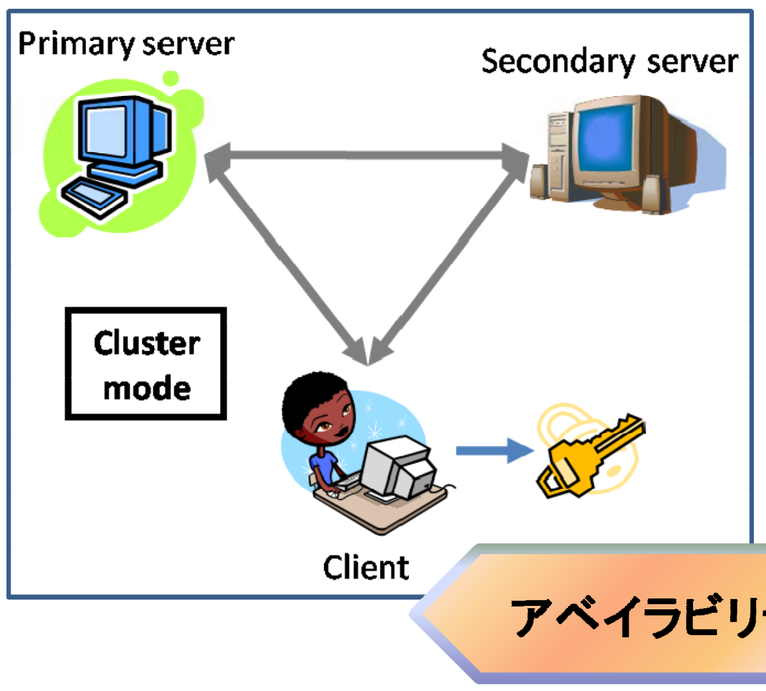
従来認証方式の問題点

- 情報漏洩で安全性が崩れてしまうケースが多い
- 情報漏洩の事件は後を絶たない
  - ユーザの不注意（紛失・盗難）、管理者の不正行為、ウイルスなど

新たな認証付きデータ管理システム

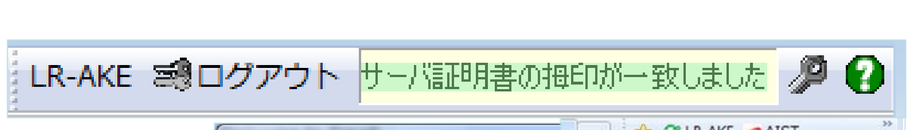
LR-AKE Leakage-Resilient AKEs & Their Applications

- 記録情報の漏洩に耐性を持たせた認証方式
- 計算量と通信量においてよりよい効率性を達成
- オンラインで安全にデータ鍵の復元が可能
- 漏洩された情報の自動無効化機能
- 攻撃者のオンラインパスワード攻撃を検知
- ユーザが覚える情報は短いパスワード一つ
- 公開鍵証明書の管理は不要
- 強前方秘匿性（将来公開鍵暗号が完全に解かれたとしても、過去の通信を復号できない）



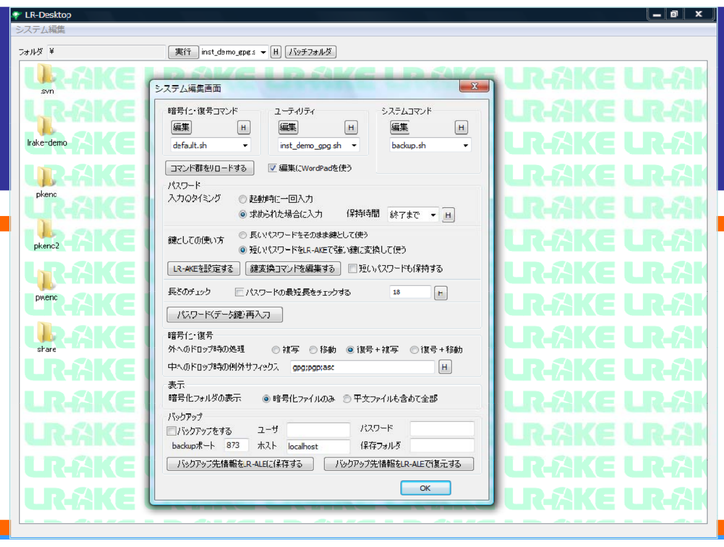
応用分野

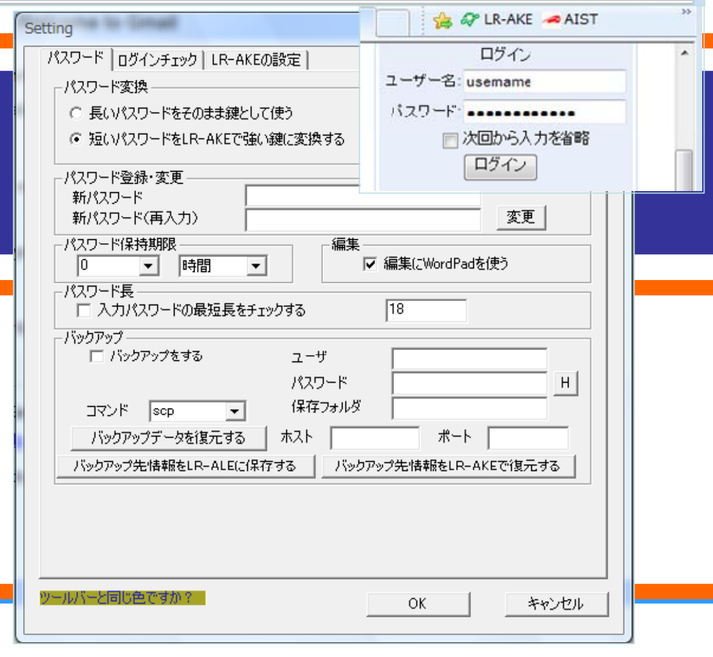
- 認証あるいはデータの保存を必要とするあらゆるサービス
  - 例）ウェブメール、ウェブショッピング、インターネットバンキング、VPNなど
- クライアント側のシングルサインオン
- クラウドストレージシステムなど



デモ

- LR-LoginChecker
- LR-Desktop
- LR-SSH





http://www.aist.go.jp
National Institute of Advanced Industrial Science and Technology AIST
独立行政法人
産業技術総合研究所

National Institute of Advanced Industrial Science and Technology
AIST

LR-AKE
Leakage-Resilient AKEs & Their Applications

RCIS
Research Center for Information Security

情報漏洩に堅牢な認証およびその応用

古原　和邦、斉藤　匡人、辛　星漢

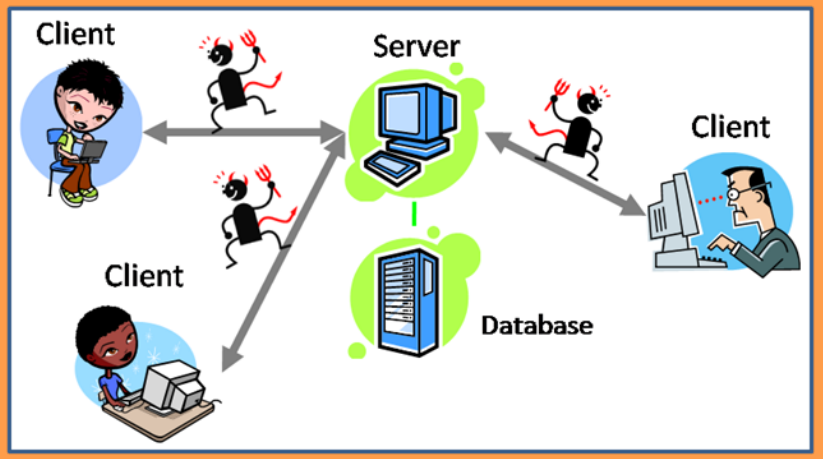
セキュリティ基盤技術研究チーム

National Institute of Advanced Industrial Science and Technology
AIST

従来認証方式の問題点

Research Center for Information Security

- 従来の認証方式は主にネットワーク攻撃者を想定した設計

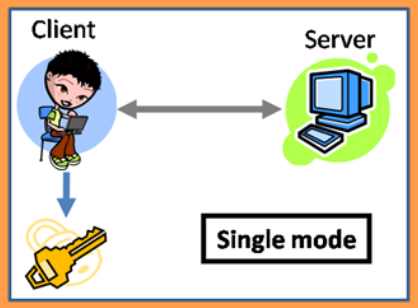


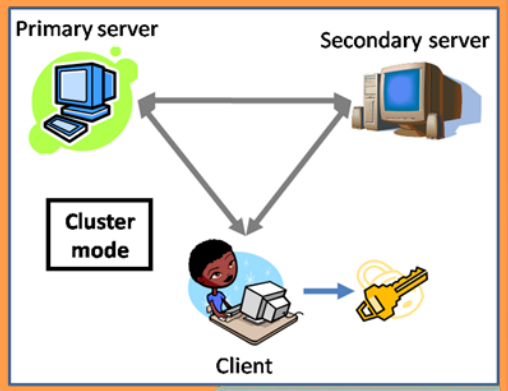
- 情報漏洩で安全性が崩れてしまうケースが多い
  - 認証情報＝アクセス権限
- 情報漏洩の事件は後を絶たない
  - ユーザの不注意、管理者の不正行為、ウイルスなど
  - 特に、紛失・置き忘れ・盗難が30.2%を占めている

（参考）「2008年上半期情報漏えいインシデント報告書（速報版Ver.1.1）」日本セキュリティ協会（2009.2.20改訂）

新たな認証付きデータ管理システム

- 記録情報の漏洩に耐性を持たせた認証方式
  - RCIS独自の技術
  - RSA/DLベース方式
- よりよい効率性を達成
  - 計算量・通信量





アベイラビリティー

- オンラインで安全にデータ鍵の復元が可能
  - 漏洩情報の自動無効化機能
  - 攻撃者のオンラインパスワード攻撃を検知
- 強前方秘匿性
  - 将来公開鍵暗号が完全に解かれたとしても、過去の通信内容を秘匿できる（但し、情報が漏洩しない場合）
- 公開鍵証明書の管理は不要

National Institute of Advanced Industrial Science and Technology AIST

従来方式との比較
（OK：耐性あり、NO：耐性なし）

Research Center for Information Security

記録された情報の漏洩

認証方式	通信路盗聴	並列オンライン攻撃	クライアントから情報漏洩	サーバから情報漏洩	時間差で両方から漏洩	フィッシング攻撃	パスワード数
CHAPなど	NO	NO	OK	NO	NO	OK	複数
PAKE	OK	NO	OK	NO	NO	OK	複数
PKI（サーバPK認証+PW）	OK	NO	OK	NO	NO	NO	複数
PKI（サーバPK認証+PW+Token）	OK	OK	OK	NO	NO	NO	複数
PKI（相互認証）	OK	OK	NO	OK	NO	NO	一つ
LR-AKE	OK	OK	OK	OK	OK	OK	一つ

クライアントから情報が漏洩しない限り、攻撃者は直列オンライン攻撃すらできない

National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

応用分野・デモ

- 認証あるいはデータの保存を必要とするあらゆるサービス
  - ウェブメール、ウェブショッピング、インターネットバンキング、VPNなど
  - ID連携、シンクライアント用認証など
  - クライアント側のシングルサインオンなど
  - クラウドストレージシステム、NASなど
- デモ（記録情報の漏洩に強いツール）
  - LR-LoginChecker
    - IDとパスワードを管理
  - LR-Desktop
    - データの暗号化・復号
  - LR-SSH
    - 安全性を強化したSSH