- 本資料は下記論文を基にして作成されたものです．文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．

- 題目：A Password-Based Authentication and Key Establishment Scheme for Mobile Environment
- 著者：Jun Liu, Jianxin Liao, Xiaomin Zhu
- 発行日：2007
- 発行所：Beijing Universityof Posts and Telecommunication

パスワードベースによる鍵確立方法

名城大学理工学部
渡邊研究室
060428262 宮崎雄介

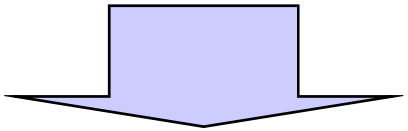
背景

- パスワード認証方法
  - 簡単な操作で、かつ簡単に実現できる
  - 費用対効果が高い
- 従来
  - サーバは平文でパスワードを管理
  - 一方向ハッシュ関数や他の暗号方法によって暗号化し管理
  - サーバにパスワードを残さない方法

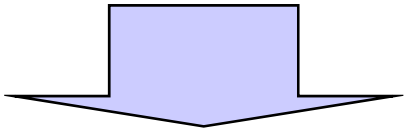
平文：暗号化されていないデータ

ICカードに関するパスワード認証方法

RSA公開鍵暗号方式に基づく方法



侵入者が傍受することが可能



改善を提案

鍵確立までのステップ

1. システム初期化
2. ユーザー個人化
3. ログイン
4. ユーザー認証
5. サーバー認証と鍵確立

Step1.システム初期化

CA…認証局
CM…central manager

CA

RSA証明書

CM

CM内部

$a = g^d \bmod n$

s_id

s_sk=h(a||s_id) mod n

用語

n = 法 (pとqの素数の積)
d = 秘密指数
g = 有理整数環（CMが選択）
|| = 連結
h(.) = ハッシュ関数

Step1.システム初期化

CA

RSA証明書

CM

$Cert_{CM}(n,e)$
h(.)
s_sk

用語

e=公開指数
CertCM(n,e)=証明書

S_j

S_j

S_j

Step2.ユーザ個人化

ボブ

u_id, u_pw

権限を確認

CM

u_id, u_pw

乱数u_rを生成

$u\_d = g^{u\_r*d} \bmod n$ ＜秘密＞

$u\_e = g^{u\_r*u\_pw} \bmod n$ ＜公開＞

u_id
n,g,a
u_d,u_e
h(.)

u_id…ユーザID

u_pw …ユーザパスワード

Step3.ログイン

s_id, u_pw入力

ボブ　カードリーダ

auth_req

S_j

ICカード内部

乱数 r を生成

時間（タイムスタンプ）t を取得

$u\_v1 = g^{r*e} \bmod n$

$u\_v2 = u\_d^{u\_pw} * g^{r*t} \bmod n$

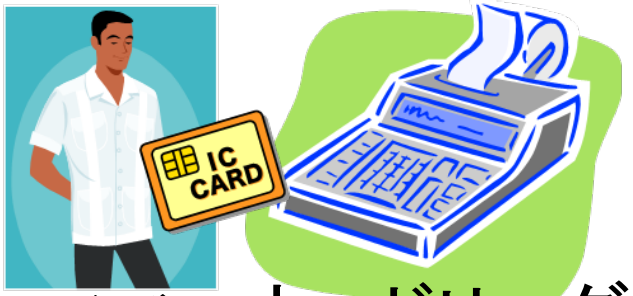
$s\_sk=(a||s\_id) \bmod n$

認証要請メッセージ

u_id, t, u_e, u_v1,
u_v2, E_{s_sk}[nounce],
hash(u_id || t || u_e ||
u_v1 || u_v2 || nounce)

※nounceは乱数，E_{s_sk}[]は暗号化

Step4.ユーザー認証



ボブ　カードリーダ

auth_resp

S_j

サーバ内部

時間（タイムスタンプ）t_{now} を取得

$t_{now} - t > \Delta t$ を判定

E_{s_sk}[nounce]を解読

ハッシュ値を計算

入力されたパスワードを判定

秘密鍵Kを生成

認証応答メッセージ

E_{s_sk}[nounce+1, K]

Step5.サーバ認証と鍵確立

ボブ　カードリーダ

auth_resp

S_j

E_{s_sk}[nounce+1，K]を復号

nounce+1，Kを取得

サーバ認証

鍵確立

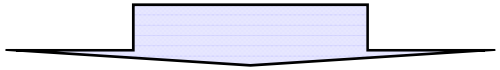
パスワードの変更

現在のパスワード u_pw ⇒ 新しいパスワード u_pwn

ユーザーはu_pwnを入力

ICカードが u_e を再計算

$u\_e = u\_d^{u\_pwn} \bmod n = g^{u\_r*d*u\_pwn} \bmod n$



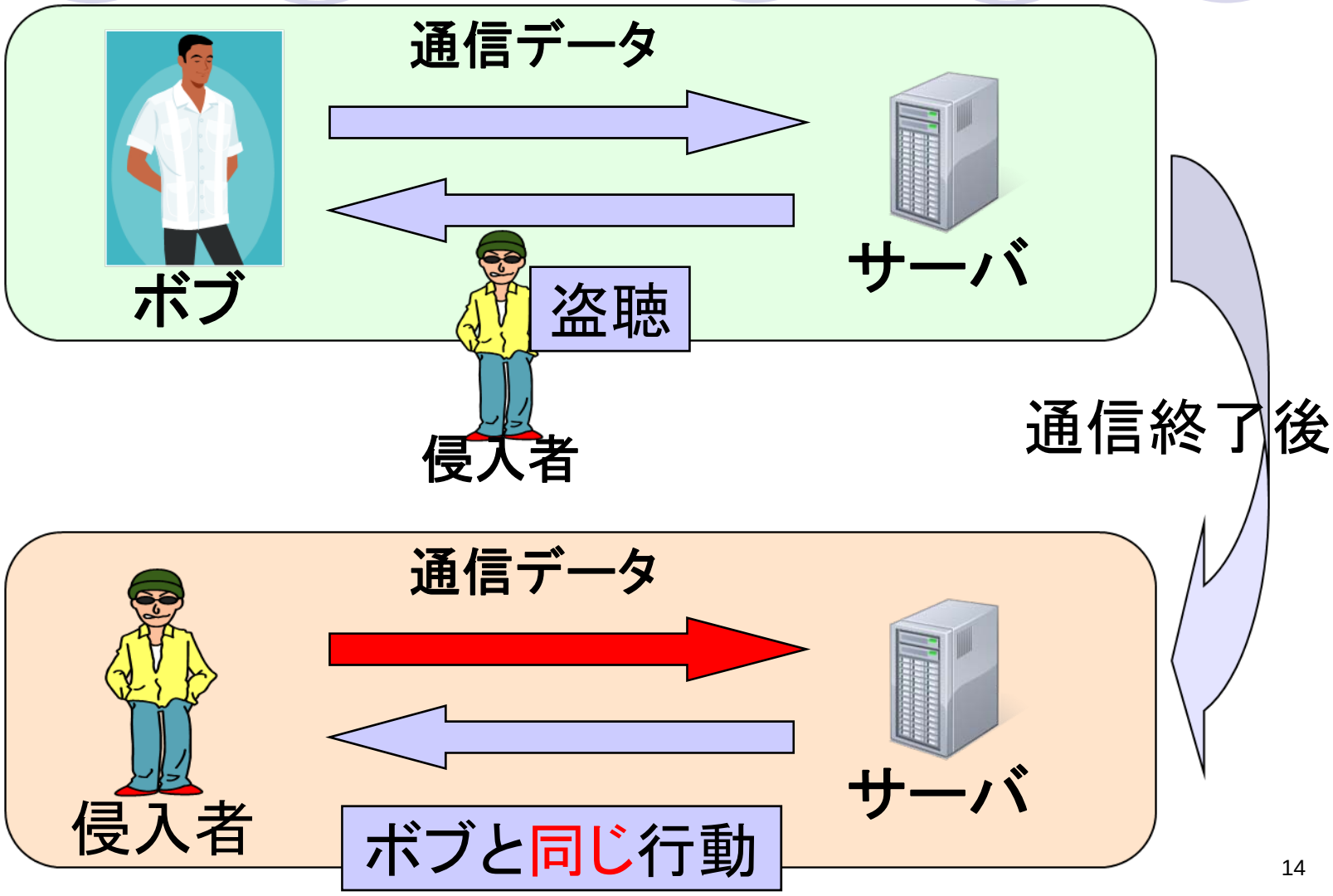
u_e を上書きする

(u_id , u_pwn) が新しいペアになる

セキュリティ

- リプレイ攻撃
- サーバのなりすまし攻撃
- オフライン攻撃
- データ保護

リプレイ攻撃（とサーバのなりすまし攻撃）



オフライン攻撃

パソコンの紛失、盗難
データの盗聴

パスワードなどを解読

セキュリティ(リプレイ攻撃)

ボブ

通信データ

サーバ

$t_{now} - t > \Delta t$ を判定

ICカード内部

時間(タイムスタンプ) t を取得

$u\_v2 = u\_d^{u\_pw * g^{r*t}} \bmod n$

$s\_sk = (a \| s\_id) \bmod n$

認証要請メッセージ

u_id, t, u_e, u_v1, u_v2,

E_{s_sk}[nounce],

hash(u_id || t || u_e || u_v1 || u_v2 || nounce)

時間 t が必要

秘密鍵不明

有効な認証要請メッセージ作成不可

セキュリティ（サーバのなりすまし攻撃）

認証要請メッセージ

u_id, t, u_e, u_v1, u_v2,
E_{s_sk}[nounce],
hash(u_id || t || u_e ||
u_v1 || u_v2 || nounce)

認証応答メッセージ

E_{s_sk}[nounce+1, K]

nounceは毎回異なる
秘密鍵不明

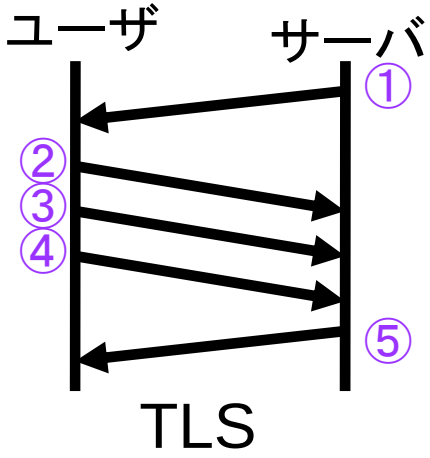
有効な認証応答メッセージ作成不可

セキュリティ(オフライン攻撃・データ保護)

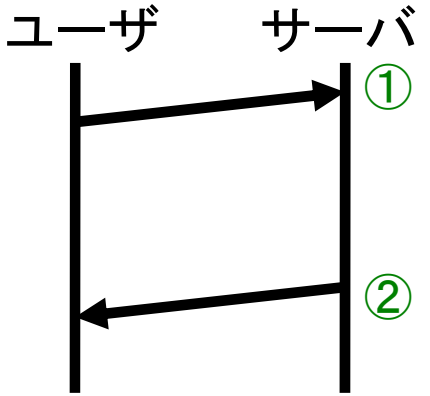
- ICカードの特性により保護される
  - ICチップによるアクセス制御
  - 内部解析には専用装置が必要
- ICカード内で完結
- 離散対数の解決が必要 $a = g^d \bmod n$ dを求めるのは難しい

攻撃に耐えられる

TLS（ Transport Layer Security ）との比較



TLS



提案方式

① サーバ証明書

② クライアントの証明書

③ プリマスタシークレットを送信

- サーバの公開鍵で暗号化

④ クライアント証明書の検証

- ハッシュ値の比較

⑤ 鍵交換・認証終了

プリマスタシークレット：
共有鍵(セッション鍵)を
生成するための情報

① 認証要請メッセージ

② 認証応答メッセージ

利点

- サーバにパスワードが保持されない
  - 漏洩の軽減
  - 管理削減
- サーバとの通信なしにパスワードの変更可能
  - ユーザーの自由
- 通信負荷の低減
- 費用対効果

欠点

- 応答時間が増える
- ほとんど性能劣化

まとめ

- パスワードをベースにした認証方式の提案
- セキュリティ対策
- メリットは費用対効果と通信負荷の低減

参考文献

- 「【図解】ICカード・ICタグ　しくみとビジネスが3分でわかる本」
  - 著：JICSAP　技術評論社
- 「企業システムのためのPKI」
  - 著：塚田孝則　日経BP社
- 「改訂　PKIハンドブック」
  - 著：小松文子　ソフト・リサーチ・センター