これからのパスワードを使った認証について

辛　星漢
セキュアシステム研究部門

独立行政法人
産業技術総合研究所（産総研）

内容

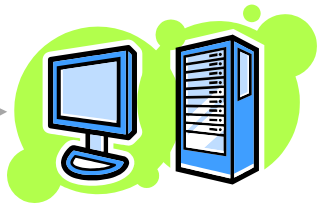
- はじめ
- パスワード認証
- パスワードを使った認証技術
  - Password-Authenticated Key Exchange (PAKE)
  - 匿名PAKE
  - Leakage-Resilient AKE (LR-AKE)
- まとめ

はじめ

情報通信社会

電子政府、
電子商取引、
電子選挙、SNSなど

メールサーバ

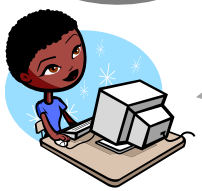


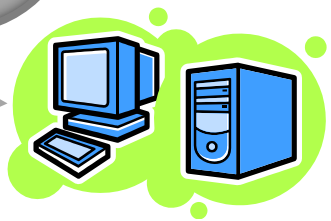
ショッピングモール

インターネット

攻撃者

銀行





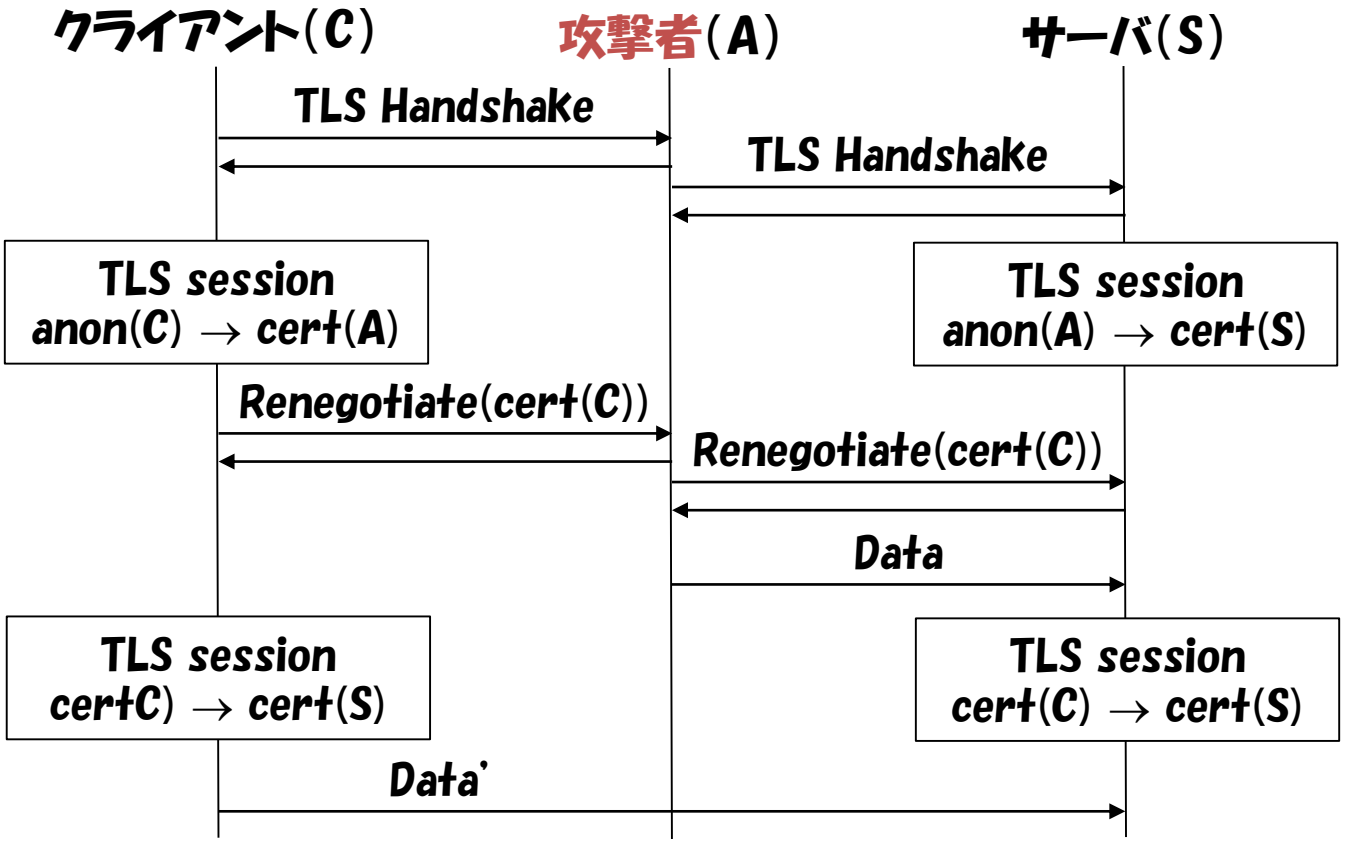
ftpサーバ

基本的なネットワーク攻撃

- 通信路盗聴 ← 受動的攻撃
  - Network Monitor
  - Wiresharkなど
- メッセージ改ざん・再送攻撃
- なりすまし攻撃 ← 能動的攻撃
- MiM (Man-in-the-Middle)攻撃

能動的攻撃の例

- TLS renegotiation攻撃(2009)
  - https://secure-resumption.com/IETF-triple-handshakes.pdf



能動的攻撃の例(つづき)

- Triple handshake攻撃(2014)
  - 詳しくは、https://secure-resumption.com/

暗号技術

- 主にデータの機密性(confidentiality)と完全性(integrity)を保障
  - 情報/ネットワークセキュリティの重大な役割を演じる
- 公開鍵/共通鍵暗号
  - 通信路盗聴、メッセージ改ざん・再送攻撃を防ぐ
- 認証
  - なりすまし攻撃、MiM攻撃を防ぐ
  - WYA (What You Are)認証
  - WYK (What You Know)認証
  - WYH (What You Have)認証

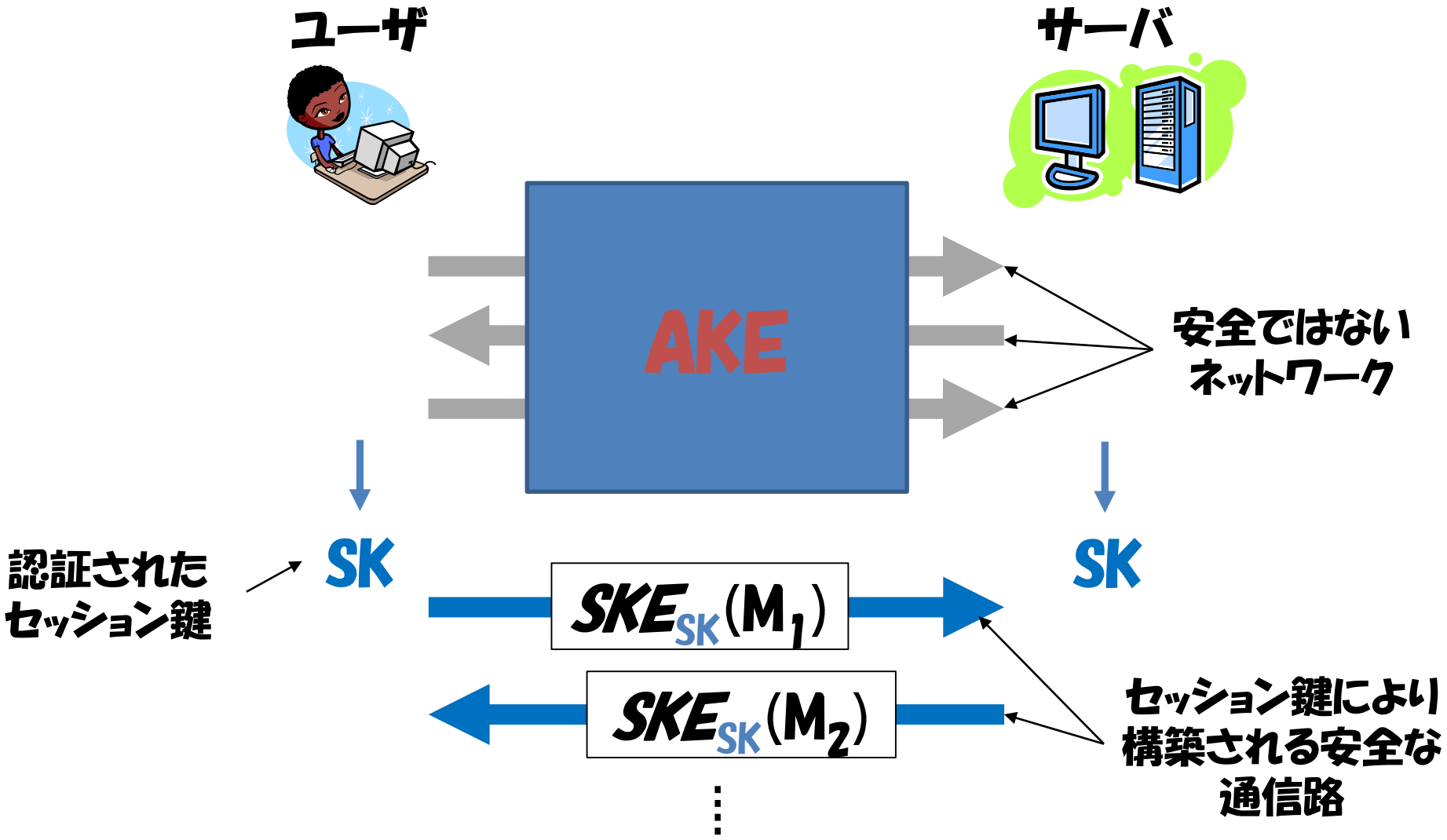
} ネットワーク認証に適切

認証付き鍵共有(AKE)

- Authenticated Key Exchange
- 重要な暗号要素技術の一つ

- 認証(通信相手のidentityを確認)+鍵共有
  - 通信entity同士に鍵共有ができれば共通鍵暗号を使ってデータの機密性と完全性を保障
  - その時に共有された共通鍵をセッション鍵と呼ぶ

認証付き鍵共有(AKE)


ユーザ
サーバ
AKE
安全ではない
ネットワーク
認証された
セッション鍵
SK
SK
$SKE_{SK}(M_1)$
$SKE_{SK}(M_2)$
セッション鍵により
構築される安全な
通信路

AKEの前提条件

- "It is not possible to establish an authenticated session key without existing secure channels already being available", C. Boyd (1993)

- Entityは既に鍵や秘密を共有している
- Off-lineサーバが使われる
  - 例、公開鍵証明書
- On-lineサーバが使われる
  - 各entityはサーバと鍵や秘密を共有している

AKEの分類

- PKIベースAKE
  - ISO/IEC IS 9798-3
  - MTI, (H)MQV
  - SSL/TLS
  - …
  - 公開鍵証明書の複雑さ
    - 公開鍵証明書の正当性はCRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol)またはSCVP (Simple Certificate Validation Protocol)を通じて確認しなければならない
    - この正当性確認を怠るとフィッシング攻撃に繋がる

フィッシング攻撃

- フィッシング用の電子メールの割合は2012年1.12%から2013年0.5%に下がったものの、よりスピア(spear)フィッシング攻撃になりつつある
  - http://community.websense.com/blogs/securitylabs/archive/2013/12/11/new-phishing-research-5-most-dangerous-email-subjects-top-10-hosting-countries.aspx
  - ソーシャルエンジニアリングなどで必要な情報を収集した後巧妙に作成された電子メールを送りつける

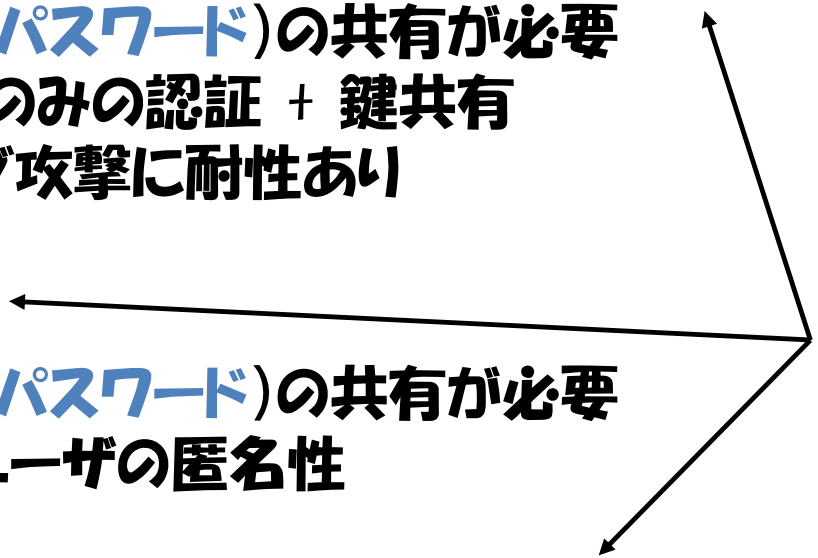
- いくつかの予防策(Wikipedia)
  - 個人情報を入力する前に、本物であることの確認
  - URLが本物であることの確認
  - 利用しようとしているサービスのセキュリティの仕組みを理解すること
  - サイトの挙動を確認する
  - http://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A3%E3%83%83%E3%82%B7%E3%83%B3%E3%82%B0_%28%E8%A9%90%E6%AC%BA%29
  - ユーザの判断に委ねる(ファーミング攻撃には？)

AKEの分類(つづき)

- 共有鍵ベースAKE
  - 共有鍵の配分が必要
  - ISO/IEC 11770-2
  - …
- On-lineサーバベースAKE
  - 共有鍵の配分が必要
  - Kerberos, 3PKD
  - …

AKEの分類(つづき)

- PAKE (Password-Authenticated Key Exchange)
  - 秘密情報(パスワード)の共有が必要
  - パスワードのみの認証 + 鍵共有
  - フィッシング攻撃に耐性あり
- 匿名PAKE
  - 秘密情報(パスワード)の共有が必要
  - PAKE + ユーザの匿名性
- LR-AKE (Leakage-Resilient AKE)
  - 認証情報の登録が必要
  - パスワードを使った新たな二要素認証 + 鍵共有
  - 受動的/能動的攻撃や情報漏えいに対しても安全性保障

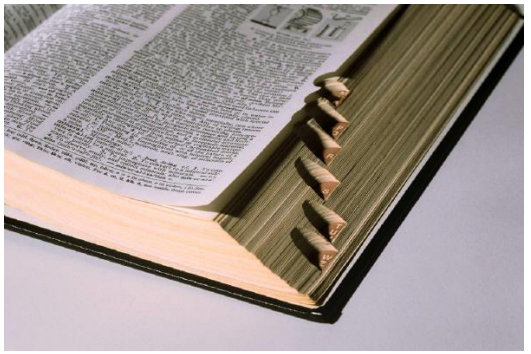


パスワードを使った
認証技術

パスワード認証？！

パスワード

- パスワードはパスワード辞書の空間から選ばれる
  - 高い利便性
  - ユーザが覚えられる長さ
    - 4桁のpin-code
    - 英数字6-8桁のパスワード



- 理想的なパスワード
  - ランダムに選ばれ、暗号鍵と同等の長さ
    - 例えば、キーボードからランダムに選んだ24桁のパスワード
  - 事実上無理！
    - 覚えられないパスワードはどこかに書いて安全ではない場所に保管してしまう(例、モニターに付けてあるパスワード)

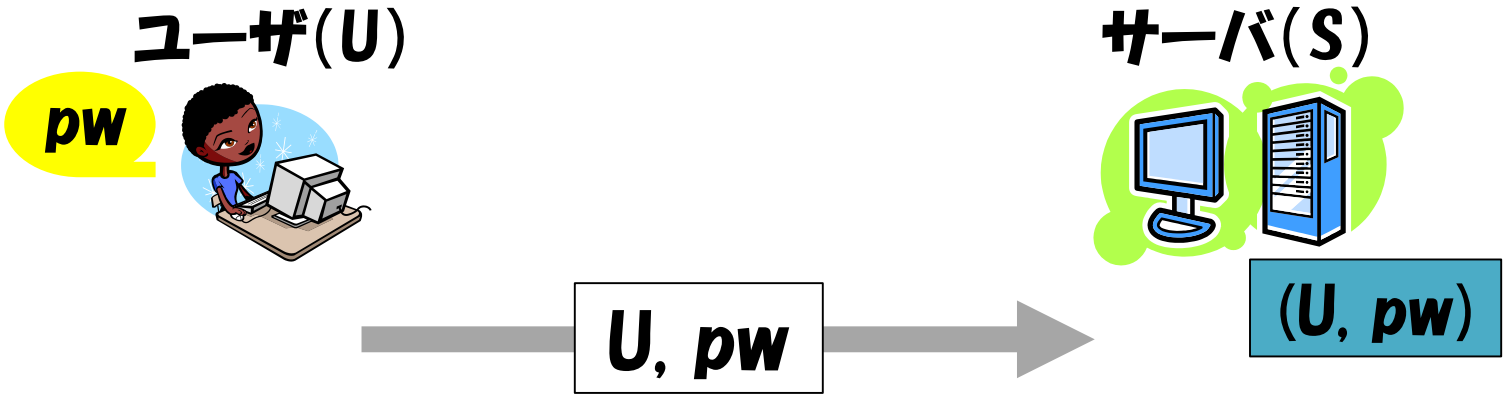
パスワード認証

- 幅広く使われている
  - 認証だけではなく暗号化の鍵としてもよく使われる（PGP, pdf/wordの暗号化など）

- パスワードに対する二つの辞書攻撃
  - オンライン辞書攻撃
    - パスワードを試すためにはユーザ或いはサーバと通信しなければならない
  - オフライン辞書攻撃
    - パスワードに関連する情報を得た後は、通信せずにオフラインですべてのパスワードを試す

安全ではないパスワード認証(その1)

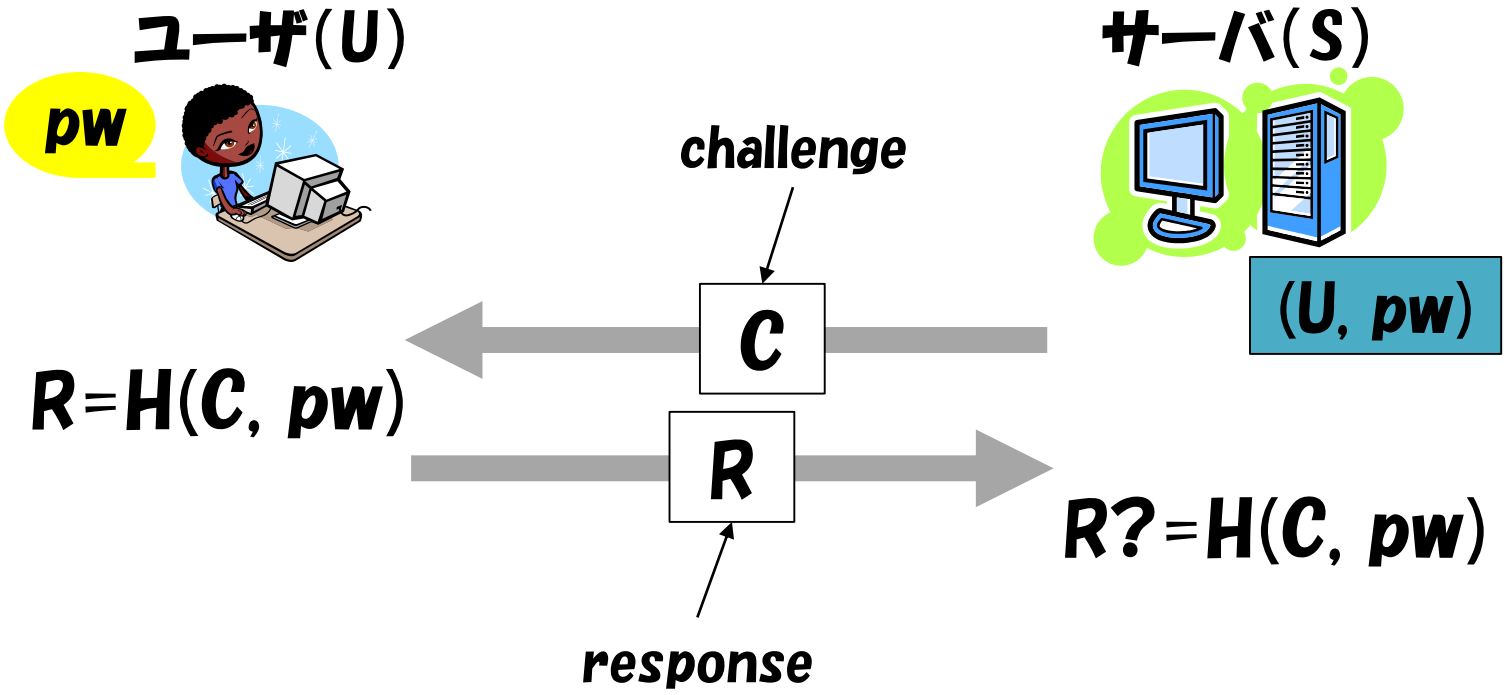
- PPP (Point-to-Point Protocol) [IETF RFC1661]



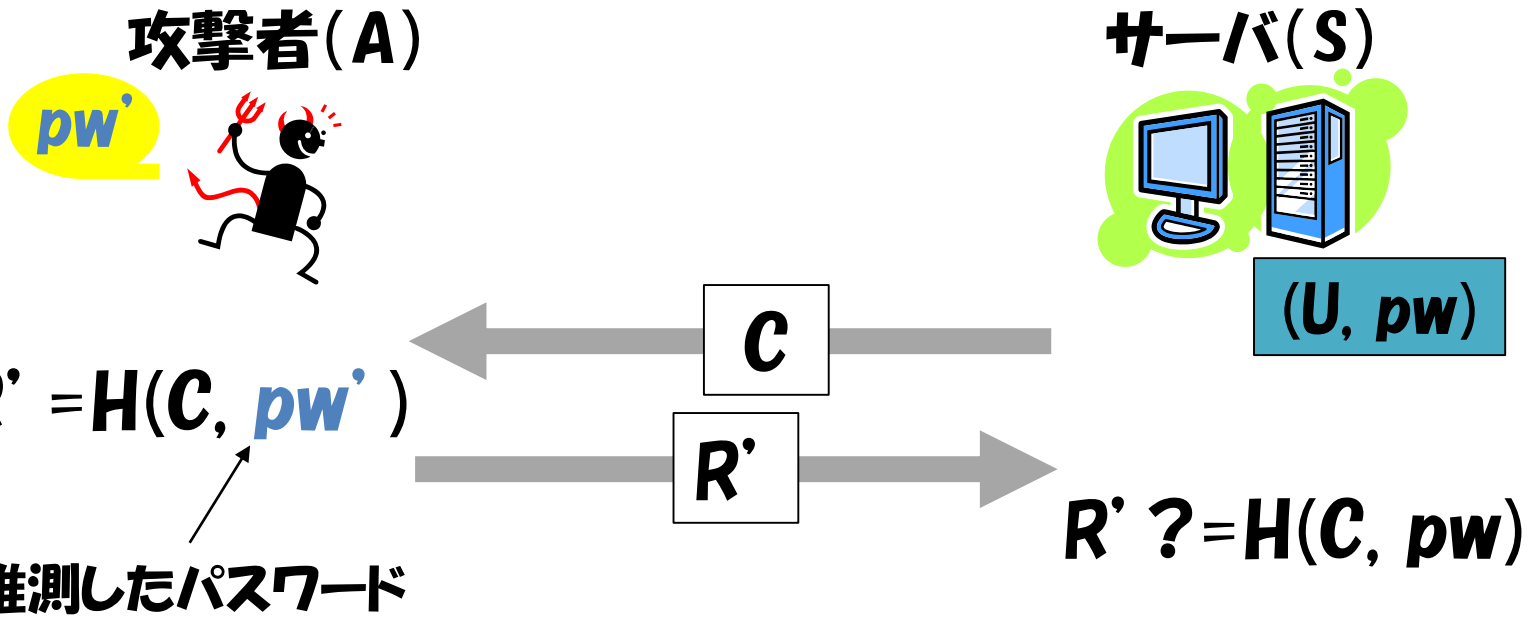
- 攻撃者は通信路を盗聴するだけでパスワードがわかる

安全ではないパスワード認証(その2)

- CHAP (Challenge Handshake Authentication Protocol) [IETF RFC1994]

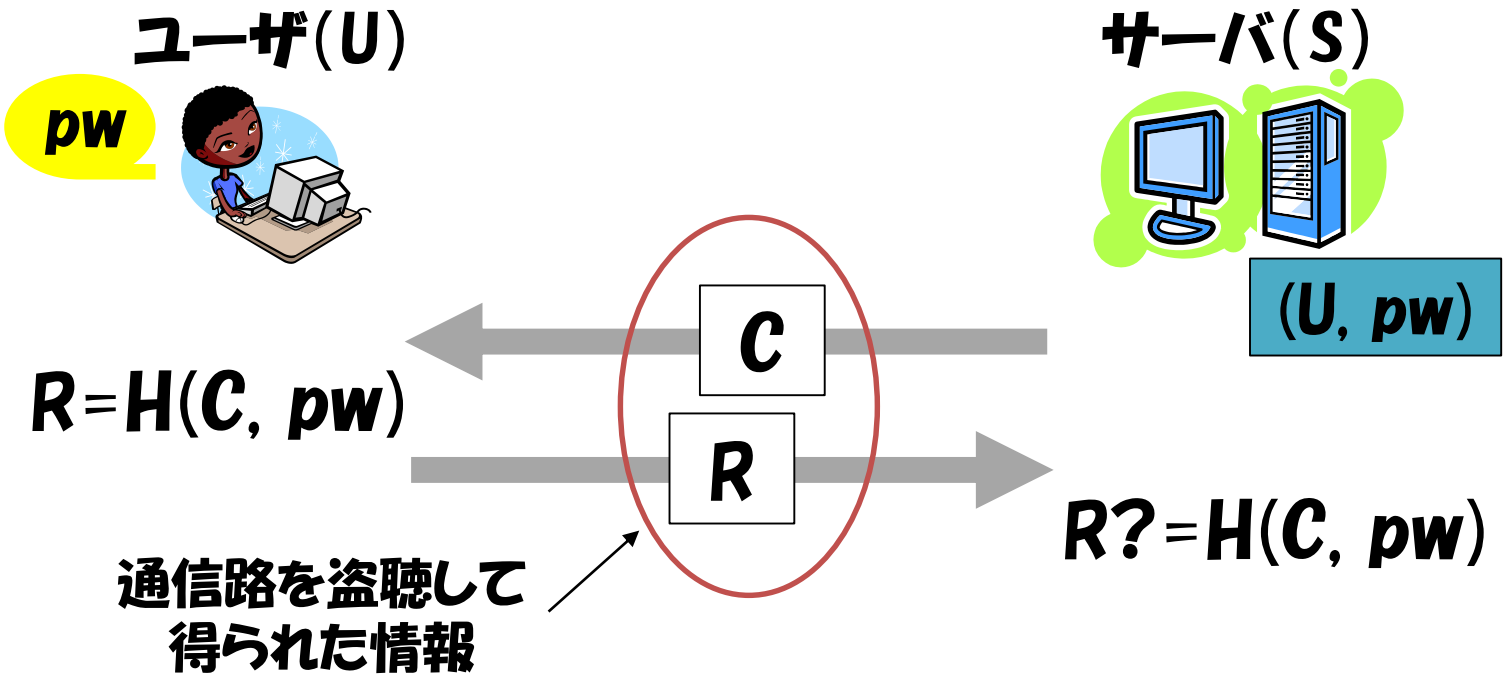


オンライン辞書攻撃



- 攻撃者はユーザのなりすましをしてサーバと通信しながら推測したパスワードを一つづつ試す

オフライン辞書攻撃



- 通信路を盗聴して得られた情報CとRを用いて、攻撃者はすべてのパスワード候補をオフラインで試す

$R? = H(C, pw')$

パスワード辞書

パスワード認証？

- パスワード認証は使うものにならない？
  - PPPもCHAPもパスワードが攻撃者にばれてしまう
- しかし、パスワード認証は実際に使われている
  - CHAPはオフライン辞書攻撃に安全ではない
  - オンライ辞書攻撃には？
  - パスワード認証でオンライン辞書攻撃は避けられないが、その反面制御できる
  - オンライン辞書攻撃への耐性を決めるにはパスワード推測エントロピー(Password Guessing Entropy)が重要

パスワード推測エントロピー(ビット)
[NIST SP 800-63-2]

パスワードの長さ

94 printable ISO characters
(キーボード)

Length Char.	User Chosen: 94 Character Alphabet: No Checks	User Chosen: 94 Character Alphabet: Dictionary Rule	User Chosen: 94 Character Alphabet: Dict. & Composition Rule	User Chosen: 10 char. alphabet 数字 (PIN)	Randomly Chosen: 10 char. alphabet 数字 (PIN)	Randomly Chosen: 94 char alphabet
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

Dictionary Rule:
一般的によく使われる単語とパスワードを除外する

Composition Rule:大小文字と特殊記号を入れる

PIN Rule:同じ数字と連続数字を除外する

パスワード強度

- なぜ6-8桁のパスワード？

- ユーザがDictionary Ruleに従って8桁のパスワードまたはDictionary RuleとComposition Ruleに従って7桁のパスワードを選び、それをパスワード認証に使っていると仮定する

- ユーザがパスワードを3回続けて間違った時、サーバは1分間ユーザアカウントにロックを掛ける場合
- 攻撃者は$2^{25.5}$個のパスワードをオンラインで試すには約90年がかかる

- サーバがオンライン辞書攻撃に対して上記のような対策を取れば十分な安全性が保障できる

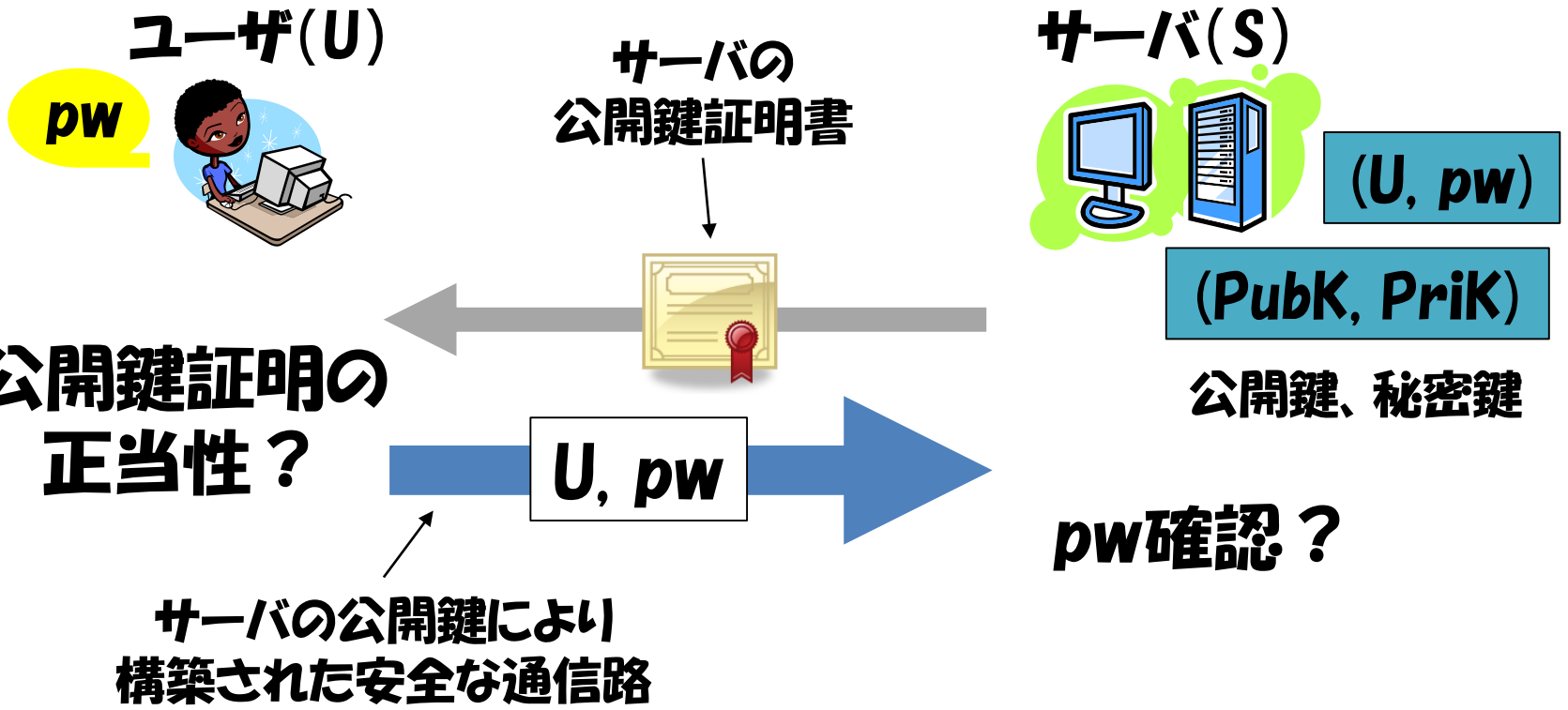
パスワード認証の安全性

- 前提条件
  - ユーザはRuleに従って適切な長さのパスワードを選ぶこと
  - サーバはオンライン辞書攻撃の対策を取ること

- パスワード認証方式に求められる安全性とは
  - （受動的/能動的攻撃を伴う）オフライン辞書攻撃に対して安全

安全なパスワード認証

- PKIベースサーバ認証 + ユーザパスワード認証
  - SSL/TLS



  - フィッシング攻撃に弱い

パスワードを使ったAKEプロトコル

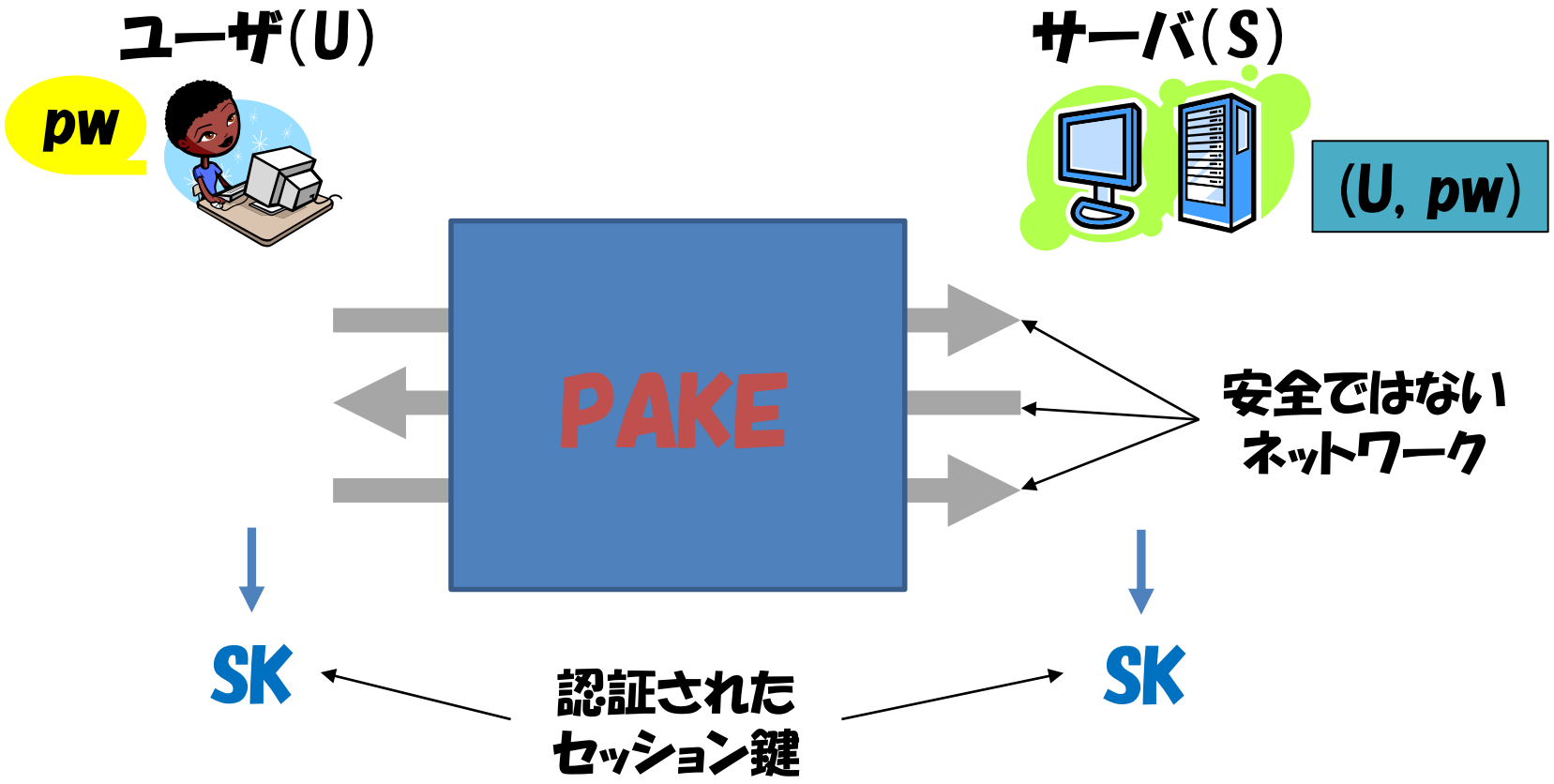
PAKE

Password-Authenticated Key Exchange (PAKE)

- パスワードのみの認証 + 鍵共有
  - PKIに依存しない
  - 高い利便性：ユーザは端末を持ち歩く必要がない
  - フィッシング攻撃に耐性あり

- しかし、安全なPAKEプロトコルを設計するのは容易ではない
  - 弱い秘密情報（パスワード）から暗号学的に安全なセッション鍵を導出しなければならない
  - オフライン辞書攻撃を防ぐための工夫が必要
  - …

PAKEプロトコル



PAKEの限界

- PAKEは利便性が高いが、

- オンライン辞書攻撃が可能
- サーバ危殆化によりオフライン辞書攻撃が可能
  - また、サーバが危殆化されるとサーバのなりすましができてしまう

- オンライン辞書攻撃に対する対策
- サーバを安全に管理

PAKEの分類

- Balanced PAKE
  - ユーザとサーバは同じパスワードを共有している
  - 受動的/能動的攻撃に対して安全
- Augmented PAKE
  - ユーザはパスワードを覚えているが、サーバはパスワード検証データ(パスワードに一方向性関数を用いて計算された値)を保持している
  - 受動的/能動的攻撃に対して安全
  - サーバ危殆化に対する安全性
    - 攻撃者がパスワード検証データを得たとしてもオフライン辞書攻撃をせずに、ユーザのなりますしができない

安全なPAKE

- IEEE 1363.2
- ISO/IEC 11770-4
- IETF RFC2945

- AugPAKE
- …

RISECでの研究開発

- PAKEに関する研究開発
  - http://www.rcis.aist.go.jp/project/PAKE-ja.html

- AugPAKE
  - Augmented PAKE
  - IETF Experimental RFC 6628として規格化
    - http://www.rfc-editor.org/rfc/rfc6628.txt
    - AugPAKEをIKEv2へ適応した内容
  - 現在、TLS WG/CFRGへI-D提出中

匿名PAKE

匿名PAKE

- PAKEはユーザの匿名性がない!
  - ユーザは自分のIDをそのまま通信路に流す

- 匿名PAKE
  - PAKE + ユーザの匿名性
  - グループ認証の概念
    - サーバはユーザがあるグループの一員であることは確認できるが、だれかは特定できない
  - 受動的/能動的攻撃者と(semi-honest)サーバに対して匿名性
  - 応用例
    - 匿名掲示板:メッセージは匿名で認証されたメンバーだけがポストできる

匿名PAKEプロトコル

グループ$U = \{U_1, U_2, U_3, \cdots\}$

ユーザ(U_2)

サーバ(S)

(U_1, pw_1)
(U_2, pw_2)
(U_3, pw_3)
:

安全ではない
ネットワーク

匿名
PAKE

SK

SK

認証された
セッション鍵

RISECでの研究開発

- 匿名PAKEとその応用に関する研究開発
  - http://www.rcis.aist.go.jp/project/PAKE-ja.html

- 現在、ISO/IEC JTC 1/SC 27/WG 2で国際標準化活動中

LR-AKE

既存のAKEプロトコルの安全性

- 既存のAKEプロトコルは保存された鍵や秘密情報(暗号鍵やパスワード検証データなど)が安全に管理されている仮定で受動的/能動的攻撃に対して安全である

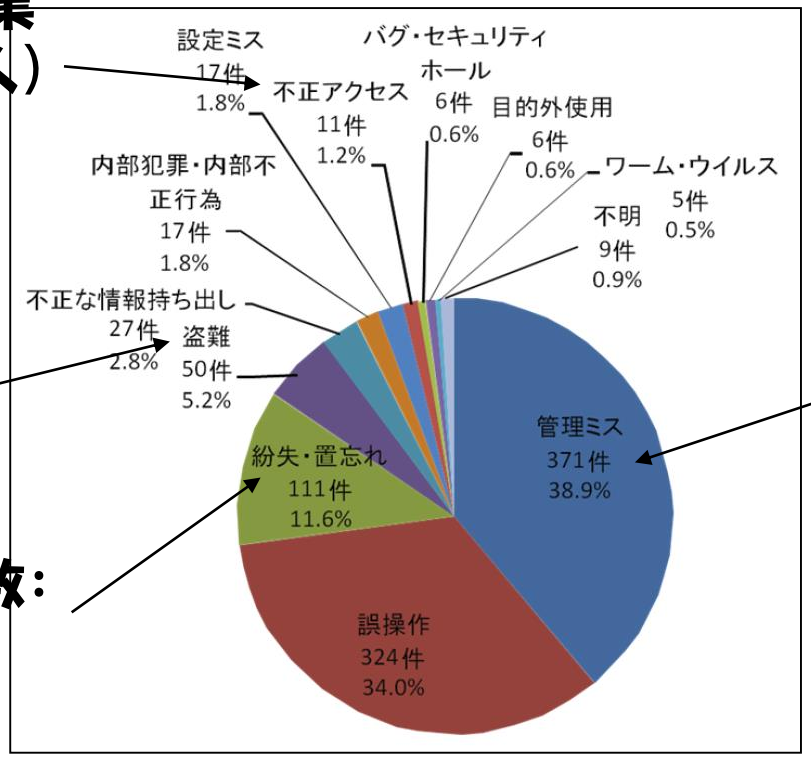
- もし、保存されている鍵や秘密情報が漏えいされてしまったら？
  - 殆どのAKEプロトコルは安全ではなくなる

情報漏えいの原因[JNSA13]

情報通信業、サービス業（漏えい人数：約28万人）など

生活関連サービス業、娯楽業（漏えい人数：約3万人）など

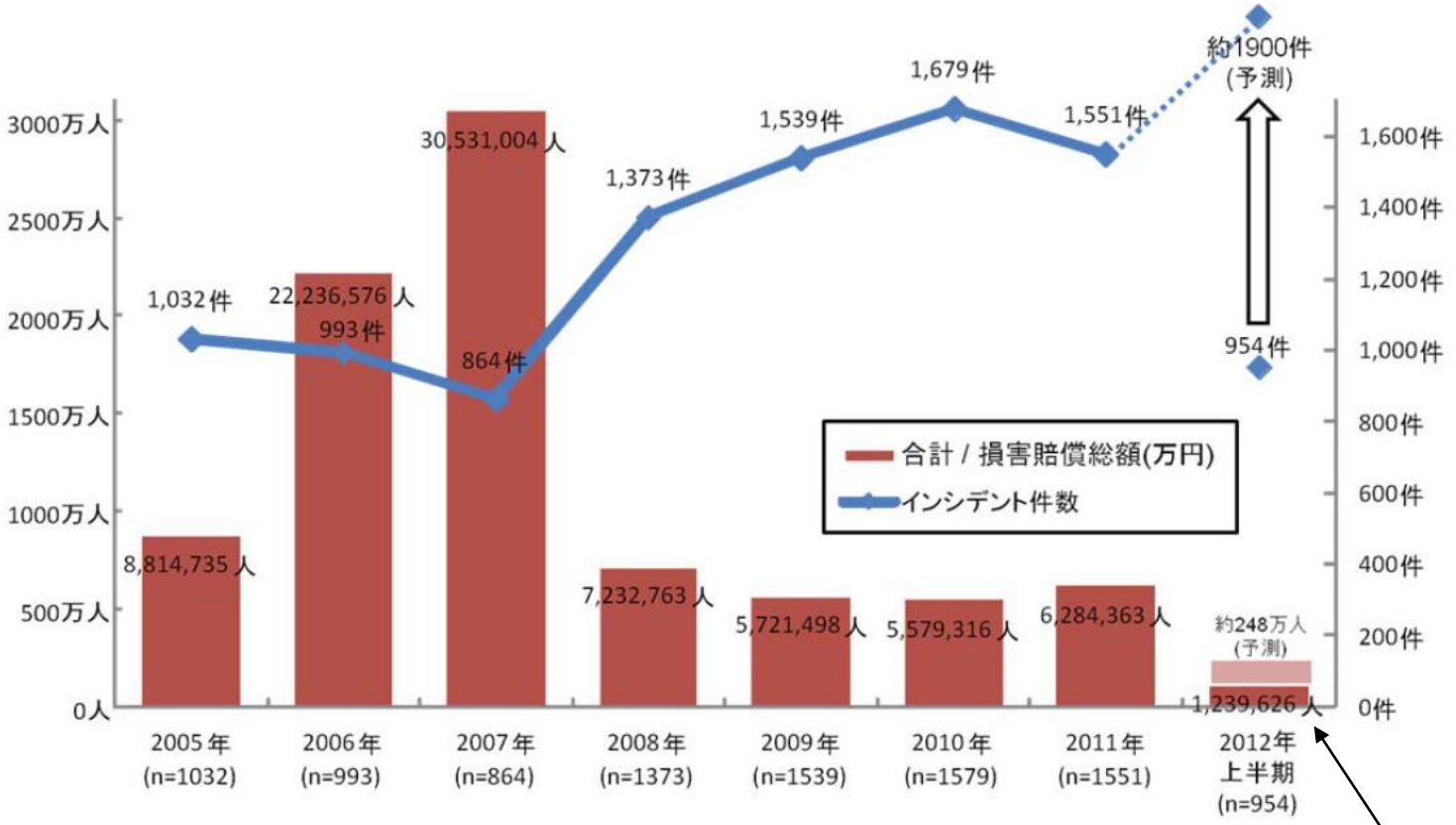
医療、福祉（漏えい人数：約3.5万人）など



金融業、保険業（漏えい人数：約55万人）など

[JNSA13] 日本ネットワークセキュリティ協会、「2012年情報セキュリティインシデントに関する調査報告書【上半期　速報版】」、2013年4月

情報漏えい人数とインシデント件数 [JNSA13]



想定損害賠償総額：約348億

韓国個人情報漏えい

- カード会社からの個人情報漏えい(2014年1月)
  - 1億4百万件
  - 情報漏えい規模では世界3位
  - 実際の情報漏えいは2012年5月から

- 2次被害
  - カード不正使用
  - 情報漏えいを利用したボイス/SMSフィッシング
  - カード再発行・解約

他の情報漏えいインシデント

- "Sony Admitted PSN's 70 Million Users Information Leakage"
  - http://tracehotnews.com/sony-admitted-psns-70-million-users-information-leakage/
- "Citigroup Cites $2.7M in Customer Losses From Hack"
  - http://www.foxbusiness.com/industries/2011/06/24/citigroup-cites-27m-in-customer-losses-from-hack/
- "DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands"
  - http://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands/?utm_source=techalert&utm_medium=email&utm_campaign=091511

パスワードの使い回し

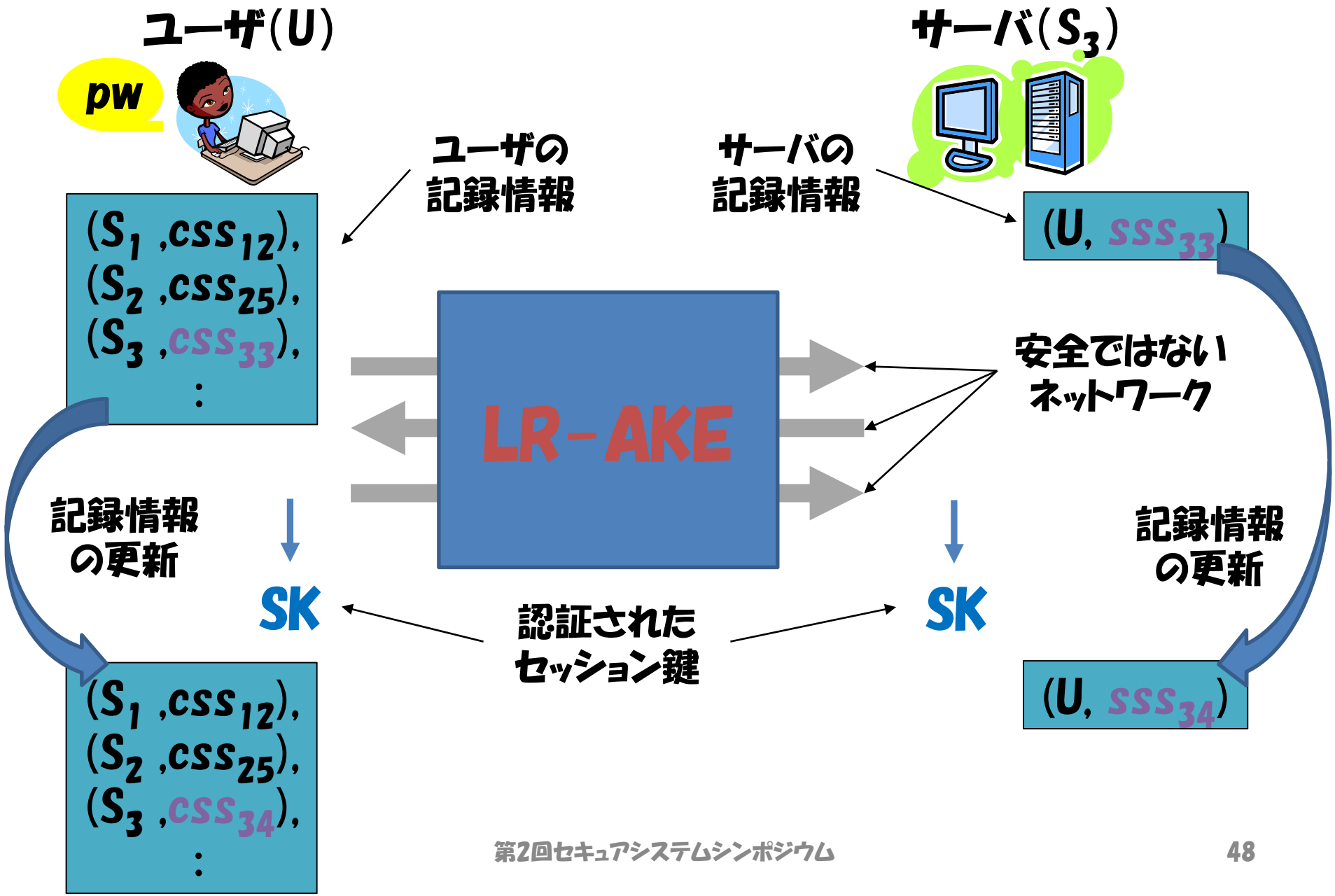
- ユーザはたくさんの異なるパスワードを覚え切れない
  - 殆どのユーザは複数のウェブサイトにパスワードを使い回している
  - http://www.pcworld.com/article/188763/too_many_people_reuse_logins_study_finds.html
  - 1/3のユーザはすべてのウェブサイトに同じパスワードを使っている
  - http://nakedsecurity.sophos.com/2009/03/10/password-website/
- パスワードの使い回しがもたらす被害
  - アカウントリスト型ハッキングによる不正ログイン
  - https://www.ipa.go.jp/security/txt/2013/08outline.html

Leakage-Resilient AKE (LR-AKE)

- ユーザは複数のサービスを利用しても覚えるパスワードはただ一つだけ
  - その代わりにユーザは端末を持つが、端末の記録情報が漏えいされても安全性を維持

- LR-AKE
  - 2要素認証 + 鍵共有
  - PKIや物理的安全性(例、TRM/TPM)に依存しない
  - 受動的/能動的攻撃及び情報漏えいに対しても最大限の安全性を保障
  - フィッシング攻撃にも耐性あり

LR-AKEプロトコル

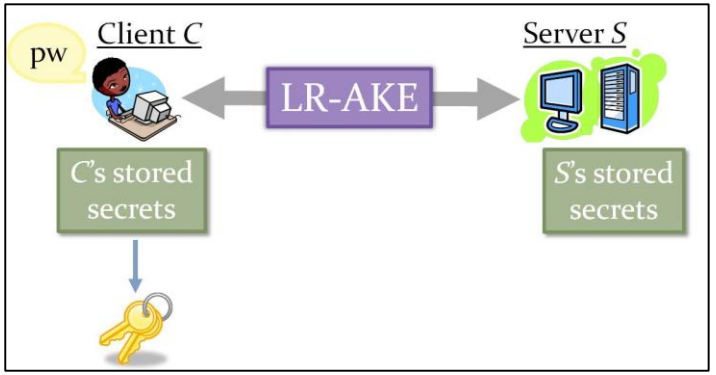

ユーザ(U)
サーバ(S_3)
pw
ユーザの
記録情報
サーバの
記録情報
(S_1 ,css_{12}),
(S_2 ,css_{25}),
(S_3 ,css_{33}),
:
(U, sss_{33})
LR-AKE
安全ではない
ネットワーク
記録情報
の更新
SK
認証された
セッション鍵
SK
記録情報
の更新
(S_1 ,css_{12}),
(S_2 ,css_{25}),
(S_3 ,css_{34}),
:
(U, sss_{34})

LR-AKEの安全性と付加機能

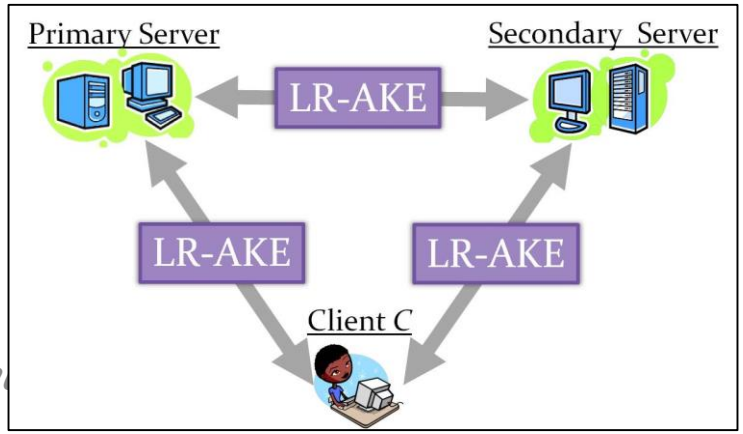
- Serialオンライン辞書攻撃ができない
  - ユーザの記録情報なしでは
  - ユーザの記録情報を得た攻撃者は、ユーザの記録情報が更新されるまで、serialオンライ辞書攻撃はできる
- 漏えいされた情報の自動無効化機能
  - 漏えいされた情報で攻撃者はserialオンライン辞書攻撃はできるが、ユーザとサーバがLR-AKEを走らせて正しく記録情報を更新すると以前の漏えいされた情報は無効になる
- オンライン辞書攻撃の検知
  - ユーザのパスワード入力間違いと攻撃者のオンライン辞書攻撃を区別

LR-AKEの応用

- データ鍵管理
  - データの暗号化よりデータ鍵の管理が重要
  - シングルモード(ユーザとサーバ)
  - クラスターモード(ユーザ、プライマリサーバ、セカンダリサーバ)
  - データ鍵の分散・復元
    - ユーザだけがデータ鍵を復元する
  - データ鍵のproactiveセキュリティ



- あらゆる認証サービスへ適用可能
- クラウドストレージサービス、SSO



RISECでの研究開発

- LR-AKEとその応用に関する研究開発
  - https://www.rcis.aist.go.jp/project/LR-AKE/

- 産総研技術移転ベンチャー
  - (株)BURSEC

まとめ

比較

AKEプロトコル	受動的攻撃(通信路盗聴)	能動的攻撃	フィッシング攻撃	記録情報が漏えいされた時のパスワードの安全性 ユーザから	サーバから	異なる時間間隔で両方から	ユーザの匿名性	パスワードの数
PPP, CHAPなど	安全ではない	安全ではない	安全ではない	安全	安全ではない	安全ではない	なし	複数
PAKE	安全	安全	安全	安全	安全ではない	安全ではない	なし	複数
匿名PAKE	安全	安全	安全	安全	安全ではない	安全ではない	あり	複数
サーバPKI認証 + ユーザパスワード(&トークン)認証	安全	安全	安全ではない	安全	安全ではない	安全ではない	あり	複数
相互PKI認証	安全	安全	安全ではない	安全ではない	安全	安全ではない	あり	一つ
LR-AKE	安全	安全	安全	安全	安全	安全	あり	一つ

ご清聴ありかとうございました