平成18年度情報セキュリティ研究センター
研究成果報告会 - RCIS2007-

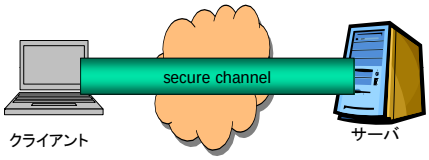
使いやすくフィッシングに対しても安全な通信路を作成する方法のご紹介
~ PAKE/LR-AKE ~

（独）産業技術総合研究所
情報セキュリティ研究センター
古原 和邦

平成19年3月29日

安全な通信路およびそれを設立するための認証鍵共有方式

- ネット上で各種サービスを安全に提供したり、アクセスポイントや遠隔サーバに安全に接続する際に欠かせない技術



例

- ネットバンキング
- オンライントレード
- 遠隔サーバ・社内LANへのログイン
- ホットスポットやネットワークへの接続
- など

IT社会を支える重要な社会基盤の一つ

PKI: Public-Key Infrastructure（公開鍵認証基盤）
CRL: Certificate Revocation List（公開鍵証明書無効化リスト）

背景

- 現在の主流：PKIを用いた方式
  - 1978年頃提案
  - 古い設計思想の元で設計された古い方式（ただし、当時としては画期的）
  - 正しく運用しようとすると以外に大変
    - 管理者や利用者に大きな負担
    - 実際、現在正しく運用されていないことが問題となっている（フィッシング詐欺など）
  - また、将来露呈すると思われる問題も控えている
    - CRLの確認
    - 情報漏えい、鍵漏洩への耐性
    - パスワード全数探索範囲の拡大
    - 公開鍵暗号の完全解読による過去の通信内容の暴露
    - など

CRL: Certificate Revocation List（公開鍵証明書無効化リスト）

古い設計思想

- 鍵は安全に管理され漏洩しない
- サーバの管理者は不正しない
- 利用者は以下のことを守れる
  - 新しい公開鍵証明書をネットワーク経由で受け取った際には、そのハッシュ値（拇印）を改ざんされない方法で受け取り比較する
  - CRLは常にチェックする
  - 本物のURLとそれに似た紛らわしいURLを注意して見分ける
  - サイト毎に個別で十分長いパスワードを覚え、一定期間毎に更新する
  - 所有物は落とさない
  - 所有物を落とした場合には、即座に連絡する

実際、ハッシュ値（拇印）を比較してみよう

SHA1, 160bits=20octetteの場合

ハッシュ値A:
f8 db 0b a5 c0 c6 bd 3f f0 f1 cd 47 1e e1 f8 74 d7 b6 40 55

ハッシュ値B:
f8 db 0b a5 c0 c6 bd 3f f0 f1 cd 47 1e e1 f8 74 d7 b6 40 55

ハッシュ値C:
79 9b 62 ec f7 0c 1c 94 1e 96 36 fb ba c0 e7 10 68 fd 26 d1

ハッシュ値D:
79 9b 62 ec f7 0c 1c 94 1e 96 86 fb ba c0 e7 10 68 fd 26 d1

現実

- 鍵は紛失・盗難・漏洩する可能性がある
  - 万が一漏れた場合、鍵の無効化は可能であるが、多大な被害を避けられない
  - 鍵は死守しなければならず管理者および利用者に大きな負担
- 魔が差したり買収されたサーバの管理者は不正を行う可能性がある
  - サーバの管理者も厳重に監視しなければならない
- 老若男女を含む全ての利用者に前述の内容を遵守させることは非常に困難
  - 教育や啓発に多大なコスト
  - また、(パスワードのチェックを除き)利用者がそれらを遵守していることをサーバ側で確認できない

近年の動向

- 2003年頃から:フィッシング被害、情報漏えい事件の増加
- 2005年:個人情報保護法完全施行
  - 情報漏えい対策の徹底
- 今後:有効期限を待たずして無効化される証明書の増加
  - CRLをチェックしないことにより生じるリスクの増大(チェックすることによる負荷の増大)

これらが物語っていること

- PKIは汎用的な技術であるが、全てをPKIで解決することの限界
- よくよく考えてみるとPKIである必要がないところでもPKIが利用されている
- PKIはPKIでなければならない場合にのみ利用すべき

PKIの良い点・悪い点

- 良い点(最初の接点の提供)
  - 互いに知らない(が認証局は知っている)2者を知り合いにさせることができる。
  - PKIはこの用途に特化すべき
- 悪い点
  - 既に知り合いになっている2者間に対しても、間に割り込んで攻撃者を紹介してくれる(フィッシング詐欺)
  - など
- 既に知り合いになっている2者間での認証鍵共有方式については見直しの時期

では、既に知り合いになっている2者間の認証鍵共有に適したプロトコルは?

LR-AKE

PAKE

- 設定が容易
  - 証明書や無効化リストなどを扱わなくてよい
- 安全かつ使いやすい
  - フィッシング被害を受けない
  - 短いパスワードを安全に使える
    - 通信路の盗聴に対して
    - オンラインでの成りすまし、サーバ管理者の不正や情報漏えいに対して
  - 複数のサーバを利用する際でも覚えるべきパスワードは一つのみ
  - 公開鍵暗号が完全解読されたとしてもそれ以前の通信内容を秘匿できる

PAKE/LR-AKE

- PAKE (Password Authenticated Key Establishment)
  - パスワードのみを用いて相互認証や鍵共有を行う方式
  - 近年盛んに研究が行われている
  - フィッシング詐欺にも耐性あり
- LR-AKE (Leakage-Resilient Authenticated Key Establishment)
  - (短い)パスワードに加えて記録情報を使うことで、サーバおよびクライアントいずれからの情報漏えいに対しても強くした方式
  - 利用者や管理者への負担を軽減しつつ安全性を強化可能
  - クライアント側の処理を軽くできるためスマートカードやユビキタスデバイスなどへの応用が期待できる
  - フィッシング詐欺にも耐性あり
  - 我々の提案方式

方式の分類

従来のパスワードベースプロトコル：
CHAP, IPsec(PSK), LEAPなど

プロトコル	ユーザの負荷		
	記憶情報の管理	記録情報の管理	
		秘密情報の管理	公開情報の検証
従来のパスワードベースプロトコル	✓		
PAKE	✓		
PKI（サーバ認証+パスワード認証）	✓		✓
LR-AKE	✓	✓	
PKI（サーバ認証+PW+OTP）	✓	✓	✓
PKI(相互認証)	✓	✓	✓

記憶情報のみを使った1要素認証

記憶情報と記録情報を使った2要素認証

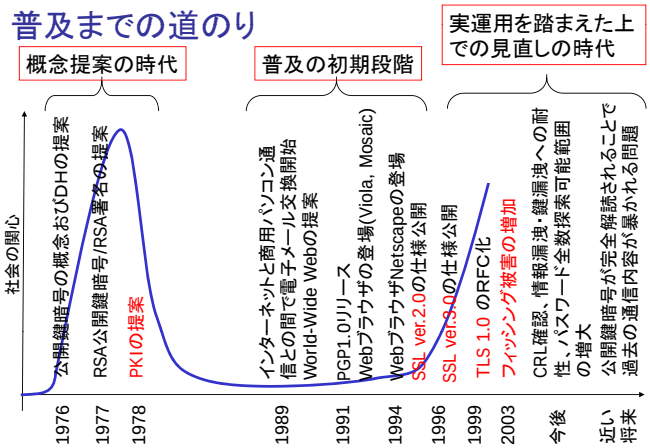
各方式を安全にするパスワードの長さと数

従来のパスワードベースプロトコル：
CHAP, IPsec(PSK), LEAPなど

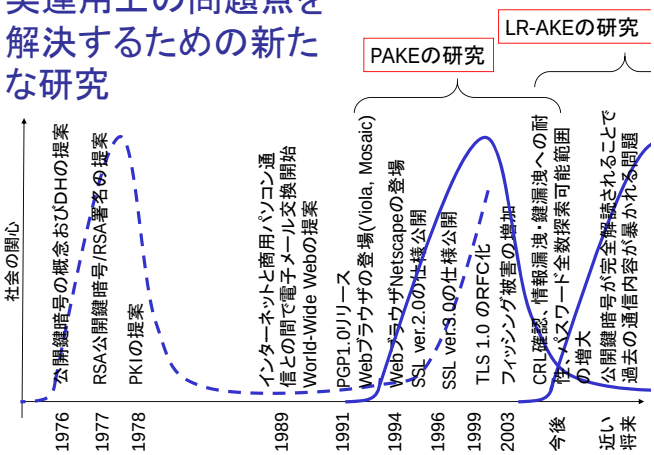
プロトコル	パスワードの長さ			パスワードの数
	記録情報が漏洩しないと仮定した場合	記録情報は漏洩するとした場合		
		クライアント側から	サーバ側から	
従来のパスワードベースプロトコル	長	N/A	長	複数
PAKE	中	N/A	長	複数
PKI（サーバ認証+PW）	中	N/A	長	複数
PKI（サーバ認証+PW+OTP）	不要	短	長	複数
PKI(相互認証)	不要	長	不要	一つ
LR-AKE	不要	短	不要	一つ

長：オフライン攻撃を防ぐ程度長くなければならない
中：パラレルオンライン攻撃を防ぐ程度長くなければならない
短：シリアルオンライン攻撃を防ぐ程度長くなければならない

PKIベース認証鍵共有方式普及までの道のり

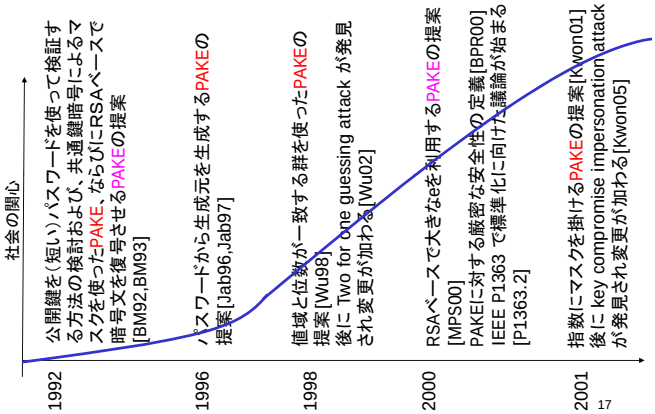


実運用上の問題点を解決するための新たな研究



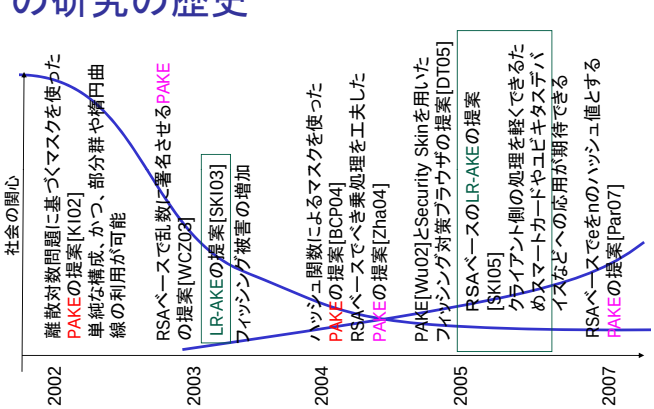
PAKEの研究の歴史

実用的な方式の抜粋



PAKEおよびLR-AKEの研究の歴史

実用的な方式の抜粋



PW: Password
OTP: One-Time Password

実運用上の問題点の比較(1/2)

比較項目 方式	1:サーバ管理者が利用者のパスワードを知りえる問題	2:偽証明書受け入れ後に入力情報が取られる問題	3:所有物が必要となる問題	4:盗難された所有物が悪用される問題
PKI(サーバ認証+PW)	X	X	△*2	○
PKI(相互認証)	○	X	X	X
PKI(サーバ認証+PW+OTP)	X	X	X	○
PAKE	X	○	○	○
LR-AKE	○	○	△*1,3	○

*1: 仕様書・実装版(現在準備中)
*2: 正しい公開鍵を所有する必要がある
*3: 初回の接続では所有物が不要

X:問題あり
△:多少問題あり
○:問題無し

PW: Password
OTP: One-Time Password

実運用上の問題点の比較(2/2)

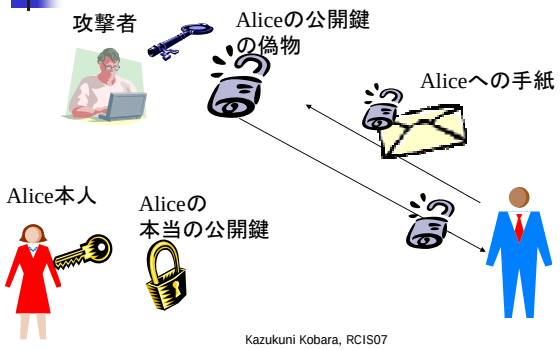
比較項目 方式	5:並列オンライン攻撃を受ける問題	6:IDが平文で流れる問題	7:送信されたごみに対してもサーバがべき剰余演算を実行しなければならない問題	8:公開鍵暗号が完全解読された場合に過去の通信内容が暴かれる問題
PKI(サーバ認証+PW)	X	○	X	X
PKI(相互認証)	○	○	X	X
PKI(サーバ認証+PW+OTP)	○	○	X	X
PAKE	X	X	X	X
LR-AKE	○	○*1	○*1	○

*1: 仕様書・実装版(現在準備中)
*2: 正しい公開鍵を所有する必要がある
*3: 初回の接続では所有物が不要

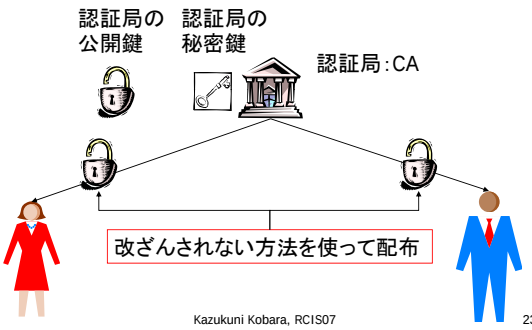
X:問題あり
△:多少問題あり
○:問題無し

PKIベース認証鍵共有

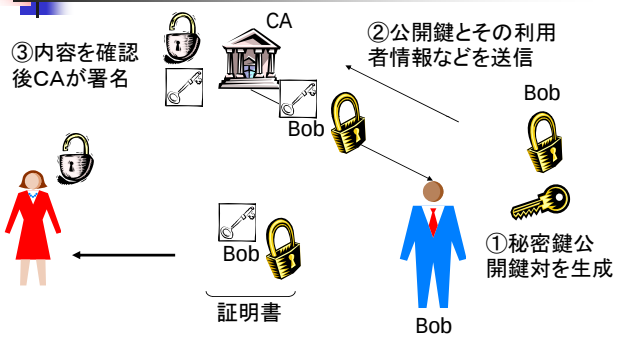
公開鍵を使う際の注意点



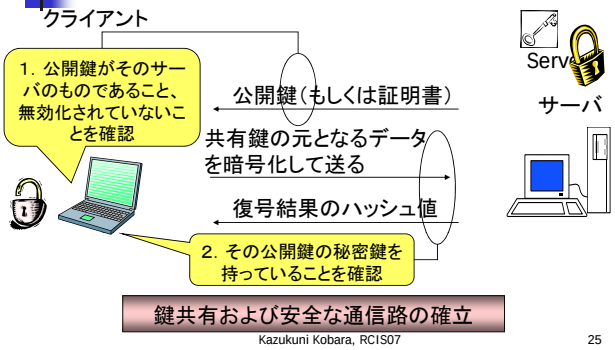
認証局(Certificate Authority)を利用する方法:PKI (1/2)



認証局(Certificate Authority)を利用する方法:PKI (2/2)

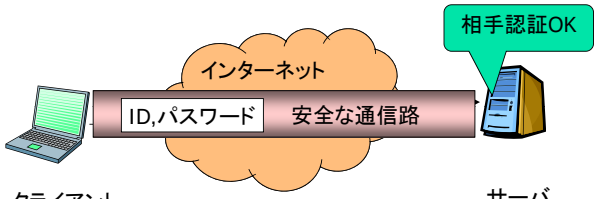


PKI:サーバ認証の例



さらにクライアントを認証する場合

ID	PW
Alice	xxx
Bob	yyy



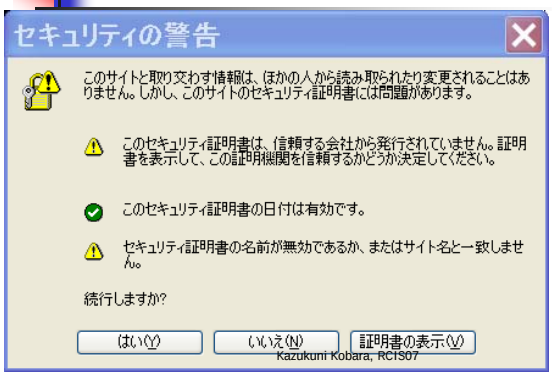
問題点1：サーバの管理者が利用者のパスワードを知りえる

- 例）
  - パスワードファイルの解析
  - 送信データの解析
  - 利用者が他のサイトのパスワードを間違えて入力
  - など
- 利用者が複数のサイトで同じパスワードを利用していた場合、被害が拡大
- 現実）魔が差したり買収されたサーバの管理者は不正を行う

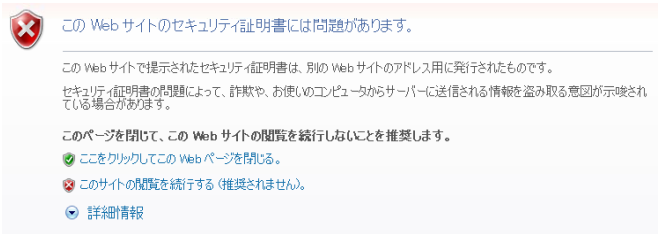
問題点2：利用者が偽証明書受け入れた場合、入力情報が取られる

- 入力情報の例）
  - クレジットカード
  - 個人情報
  - など
- 現実）多くの利用者は偽証明書受け入れてしまう

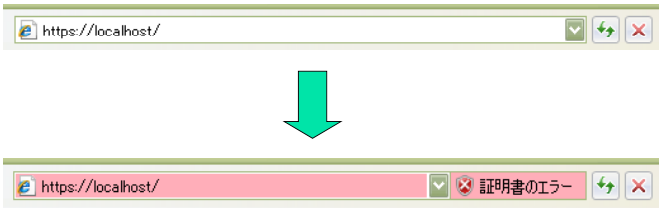
証明書検証時の警告（IE6以前の場合）



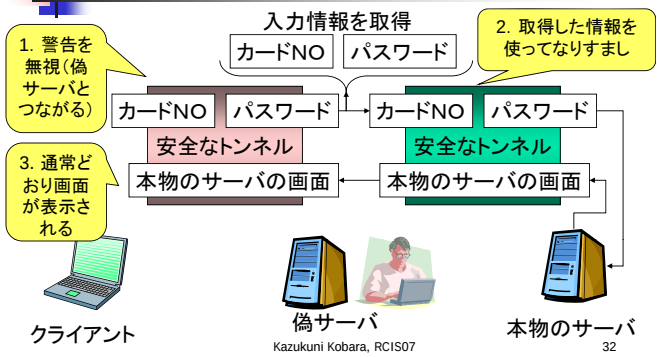
証明書検証時の警告（IE7以降の場合）(1/2)



証明書検証時の警告（IE7以降の場合）(2/2)

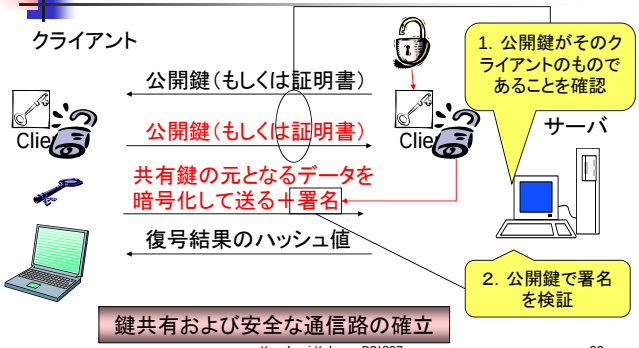


警告を無視すると：入力情報は攻撃者に盗まれる可能性あり（中間侵入攻撃）



問題点1はPKI相互認証を用いることで解決（パスワードをサーバに提示しないので）、ただし、問題点2は残る

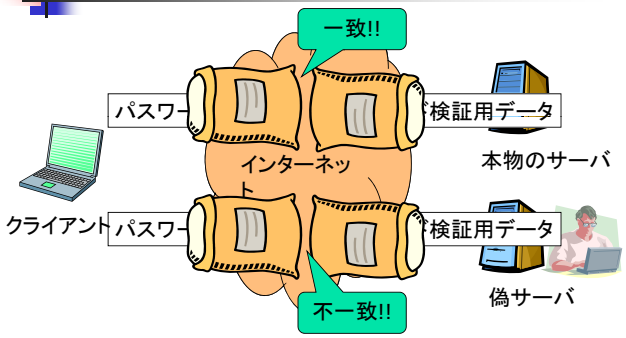
PKI:相互認証の例



PAKE/LR-AKE

•パスワードを相手に伝えることなく検証（パスワードは通信相手や盗聴者に取られない）
•検証された相手とのみ安全な通信路が作成される（認証後の入力情報も取られない）

PAKE/LR-AKE の考え方



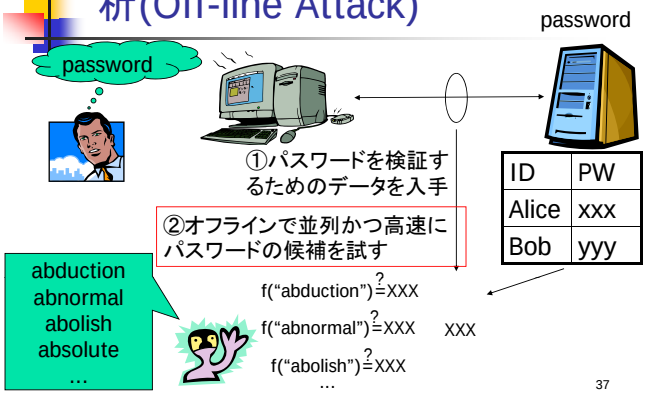
短いパスワードを使う際の注意点

- 全数探索を受ける危険性を考慮する必要がある。
- 安全に使えるパスワードの長さは適用できる全数探索の種類に応じて変わってくる。
  - オフライン攻撃
  - オンライン攻撃
    - Parallel
    - Serial

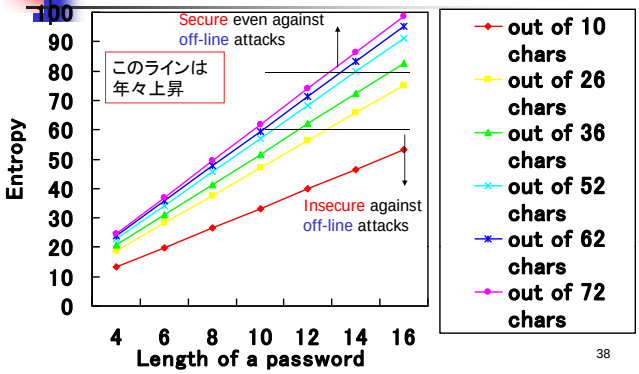
オフライン攻撃が可能な場合非常に長いパスワードが必要

直列オンライン攻撃しか適用できない場合短いパスワードを安全に利用できる

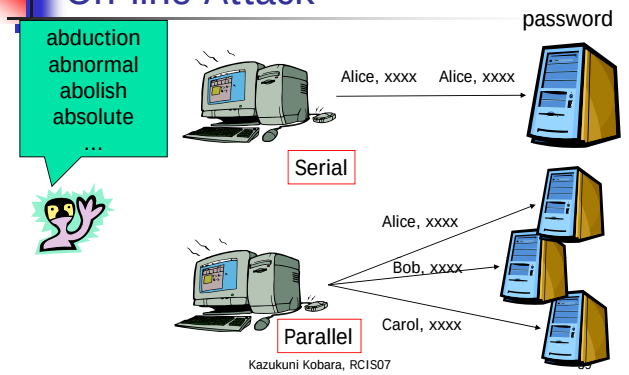
パスワードのオフラインでの解析(Off-line Attack)



Off-line Attack に耐え得るパスワードの長さ



On-line Attack



各方式を安全にするパスワードの長さと数

従来のパスワードベースプロトコル：CHAP, IPsec(PSK), LEAPなど

プロトコル	パスワードの長さ			パスワードの数
	記録情報が漏洩しないと仮定した場合	記録情報は漏洩するとした場合		
		クライアント側から	サーバ側から	
従来のパスワードベースプロトコル	長	N/A	長	複数
PAKE	中	N/A	長	複数
PKI（サーバ認証+PW）	中	N/A	長	複数
PKI（サーバ認証+PW+OTP）	不要	短	長	複数
PKI（相互認証）	不要	長	不要	一つ
LR-AKE	不要	短	不要	一つ

長：オフライン攻撃を防ぐ程度長くなければならない
中：パラレルオンライン攻撃を防ぐ程度長くなければならない
短：シリアルオンライン攻撃を防ぐ程度長くなければならない

まとめ

- 認証鍵共有方式
  - 現在のIT社会を支える上で欠かせない技術
- 現在主流のPKIベースの方式
  - 30年ほど前に提案された古い方式
  - 実際に使ってみることでさまざまな問題が露呈（フィッシング詐欺など）
  - また、将来露呈すると思われる問題も控えている
    - CRLの確認
    - 情報漏えい、鍵漏洩への耐性
    - パスワード全数探索範囲の拡大
    - 公開鍵暗号の完全解読による過去の通信内容の暴露
    - など
- 新たな潮流の紹介 PAKE/LR-AKE
  - 使い勝手を重視する場合 -> PAKE
  - 安全性を重視する場合 -> LR-AKE

参考文献(1/3)

- [BM92] S. Bellovin and M. Merritt. ``Encrypted key exchange: Password-based protocols secure against dictionary attacks''. In Proc. of IEEE Symposium on Security and Privacy, pp. 72--84, 1992.
- [BM93] S. Bellovin and M. Merritt. ``Augumented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise''. In Proc. of the First Annual ACM Conference on Computer and Communications Security (CCS '93), pp. 244--250, 1993.
- [Jab96] D. Jablon. ``Strong password only authenticated key exchange''. ACM Computer Communication Review, ACM SIGCOMM, 26(5), pp. 5--20, 1996.
- [Jab97] D. Jablon. ``Extended password key exchange protocols immune to dictionary attack''. In Proc. of WET-ICE Workshop on Enterprise Security, 1997.
- [Wu98] T. Wu, The Secure Remote Password Protocol, in Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, CA, Mar 1998, pp. 97-111.
- [MPS00] P. MacKenzie, S. Patel, and R. Swaminathan. ``Password-authenticated key exchange based on RSA''. In Proc. of ASIACRYPT 2000}, pp. 599--613. Springer--Verlag, 2000.
- [BPR00] M. Bellare, D. Pointcheval, and P. Rogaway. ``Authenticated key exchange secure against dictionary attack''. In Proc. of EUROCRYPT 2000: LNCS 1807, pp. 139--155, 2000.

参考文献(2/3)

- [P1363.2] IEEE P1363.2: Password-Based Public-Key Cryptography, http://grouper.ieee.org/groups/1363/passwdPK/
- [Kwon01] T. Kwon, “Authentication and key agreement via memorable password,“ In *ISOC Network and Distributed System Security Symposium*, February 2001.
- [Wu02] Wu, T., “SRP-6: Improvements and Refinements to the Secure Remote Password Protocol”. Submission to the IEEE P1363 Working Group 2002.
- [KI02] K. Kobara and H. Imai. ``Pretty-simple password-authenticated key-exchange protocol proven to be secure in the standard model''. IEICE Trans., E85-A(10):2229--2237, October 2002.
- [WCZ03] D. S. Wong, A. H. Chan, and F. Zhu. ``More efficient password authenticated key exchange based on RSA''. In INDOCRYPT 2003, LNCS 2904, pp. 375--387. Springer--Verlag, 2003.
- [SKI03] S. Shin, K. Kobara, and H. Imai.``Leakage-resilient authenticated key establishment protocols''. In Proc. of ASIACRYPT 2003: LNCS 2894, pp. 166--172. Springer-Verlag, 2003.

参考文献(3/3)

- [BCP04] E. Bresson, O. Chevassut, and D. Pointcheval. ``New Security Results on Encrypted Key Exchange''. In Proc. of PKC'04, LNCS 2947, pp. 145--158, 2004.
- [Zha04] M. Zhang. ``New approaches to password authenticated key exchange based on RSA''. In Advances in Cryptology - ASIACRYPT'04, LNCS 3329, pp. 230--244. Springer--Verlag, 2004.
- [Kwon05] T. Kwon, “Revision of AMP in IEEE P1363.2 and ISO/IEC 11770-4”, Submission to the IEEE P1363 Working Group, June 8, 2005.
- [SKI05] S. Shin, K. Kobara, and H. Imai, “Efficient and Leakage-Resilient Authenticated Key Transport Protocol Based on RSA”, In Proceedings of the 3rd Applied Cryptography and Network Security 2005 (ACNS2005), LNCS 3531, pages 269-284, Springer-Verlag, 2005
- [DT05] R. Dhamija and J.D. TygarJ.D. Tygar. ``The Battle Against Phishing: Dynamic Security Skins‘‘, Proc. of the 2005 ACM Symposium on Usable Security and Privacy, ACM International Conference Proceedings Series, ACM Press, pp. 77-88, July 2005.
- [Par07] S. Park. ``Efficient Password-Authenticated Key Exchange Based on RSA''. In Proc. of CT-RSA 2007, Springer--Verlag, 2007.