HITACHI
Inspire the Next

暗号プロトコルに関する評価実験

2013/09/11

株式会社 日立製作所
横浜研究所　渡辺　大

Human Dreams.
Make IT Real.

HITACHI
Inspire the Next

暗号プロトコルに関する評価実証実験結果

Contents

評価概要（全体）

背景

HITACHI
Inspire the Next

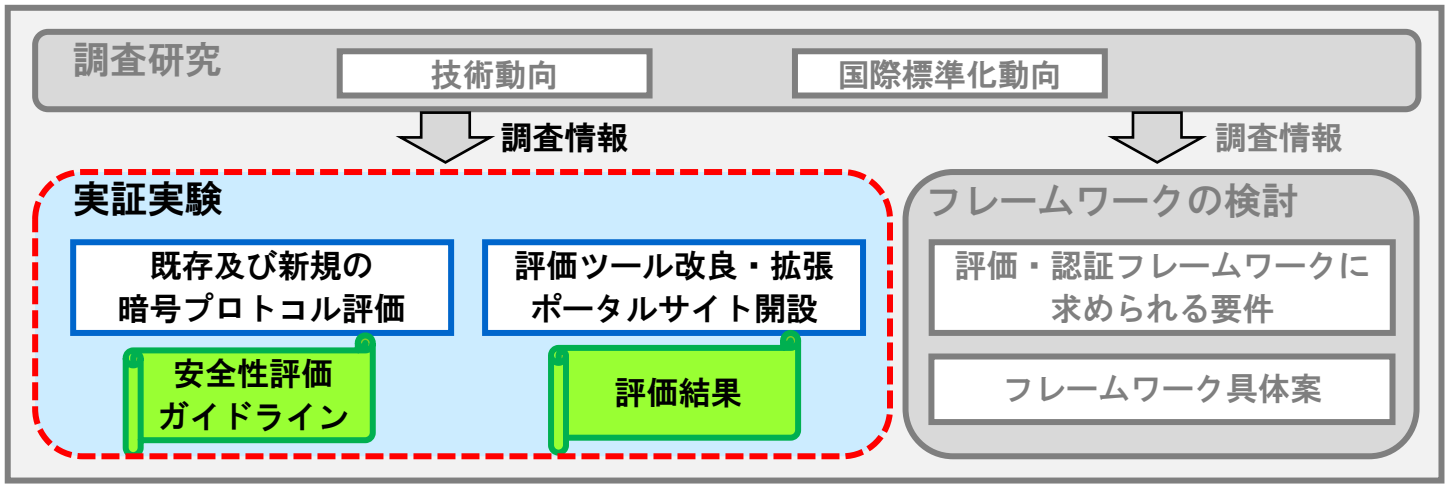
- ISO/IEC 29128 Verification of Cryptographic Protocol
  - 2007/04: SC27/WG3**でプロジェクト開始**
  - 2008/04: 1st Working Draft**提出**
  - 2011/12: International Standard**発行**
- **標準に準拠してプロトコル評価を進めるために**
  - 2012/09～2013/03:

    総務省事業「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負」

事業の概要

HITACHI
Inspire the Next

✓暗号プロトコルの安全性を確認する標準化された評価手法や
　利用に関する指針等は未整備
✓評価は個々の技術者独自の手順・品質は個々のスキルに依存



本事業の
実施内容

本事業の成果の活用や更なる検討、啓発の推進

暗号プロトコルの評価・認証に係る新しいフレームワーク

ISO/IECによる評価のクラス分け

HITACHI
Inspire the Next

ISO/IEC 29128より抜粋

Protocol Assurance Level	PAL1	PAL2	PAL3	PAL4
プロトコル仕様	**PPS_SEMIFORMAL** Semiformal description of protocol specification.	**PPS_FORMAL** Formal description of protocol specification.	**PPS_ MECHANIZED** Formal description of protocol specification in a tool-specific specification language, whose semantics is mathematically defined.	
攻撃者モデル	**PAM_INFORMAL** Informal description of adversarial model.	**PAM_ FORMAL** Formal description of adversarial model.	**PAM_ MECHANIZED** Formal description of adversarial model in a toolspecific specification language, whose semantics is mathematically defined.	
セキュリティプロパティ	**PSP_INFORMAL** Informal description of security property	**PSP_ FORMAL** Formal description of security property.	**PSP_ MECHANIZED** Formal description of security property in a toolspecific specification language, whose semantics is mathematically defined.	
自己評価	**PEV_ARGUMENT** Informal argument that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.	**PEV_HANDPROVEN** Mathematically formal paper- and-pencil proof verified by human that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.	**PEV_BOUNDED** Tool-aided bounded verification that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.	**PEV_UNBOUNDED** Tool-aided unbounded verification that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.

ツールによる評価を義務化

暗号プロトコル評価の目的

HITACHI
Inspire the Next

- 評価結果の信頼性に関する知見の蓄積
  - ツールによる結果の違い
  - 評価者による結果の違い
- 評価コストに関する知見の蓄積
  - モデル化
  - ツールの実行時間(PAL4での評価は現実的か？)
- 評価におけるポイントの洗い出し
  - プロトコル仕様
  - セキュリティプロパティ
  - 攻撃者モデル, etc.

●評価の進め方とコストを明確化し、ISO/IEC 29128に準拠した評価の実施可能性を検証
●評価報告書のあり方とフォーマットを検討

実施事項(既存及び新規の暗号プロトコル評価)

HITACHI
Inspire the Next

既存の暗号プロトコル37種111件に加え、新規に開発された暗号プロトコル1種3件の評価を実施

- 評価対象:既存プロトコル37種＋新規に開発された暗号プロトコル
  - ✓ 教科書的なプロトコル:Woo-Lam, Yahalomプロトコルなど
  - ✓ インターネットで利用されているプロトコル:IKE, EAPなど
  - ✓ その他、特定用途向けプロトコル、PAL2で評価が行われている先進的なプロトコルについても評価を実施

- 評価ツール:3種のモデル検証ツールProVerif, KDDI研独自ツール, Scyther
  - ✓ ISO/IEC 29128の区分でPAL3, PAL4に相当する評価が可能
  - ✓ UIやセキュリティプロパティの観点から、機能の異なるツールを選択

選択した評価ツールの特性

HITACHI
Inspire the Next

	Non-interactive (bounded)	(unbounded)	Interactive (unbounded)
Symbolic	NRL FDR AVISPA	Scyther ProVerif KDDI研ツール AVISPA(TA4SP)	Isabelle/HOL
Probabilistic		CryptoVerif	BPW (on Isabelle/HOL) Game-based Security Proof (on Coq)

モデル化や評価方法の多様性はあまり考慮されていない

選択した評価ツールの特性(2)

HITACHI
Inspire the Next

	GUI	テキストベース ←可読性低	可読性高→
入力	KDDI研ツール	Scyther	ProVerif
出力	Scyther	ー	ProVerif KDDI研ツール

使いやすさ(とっつきやすさ)の多様性を重視

評価ツールScytherによる評価（日立製作所）

Scytherのツール紹介

HITACHI
Inspire the Next

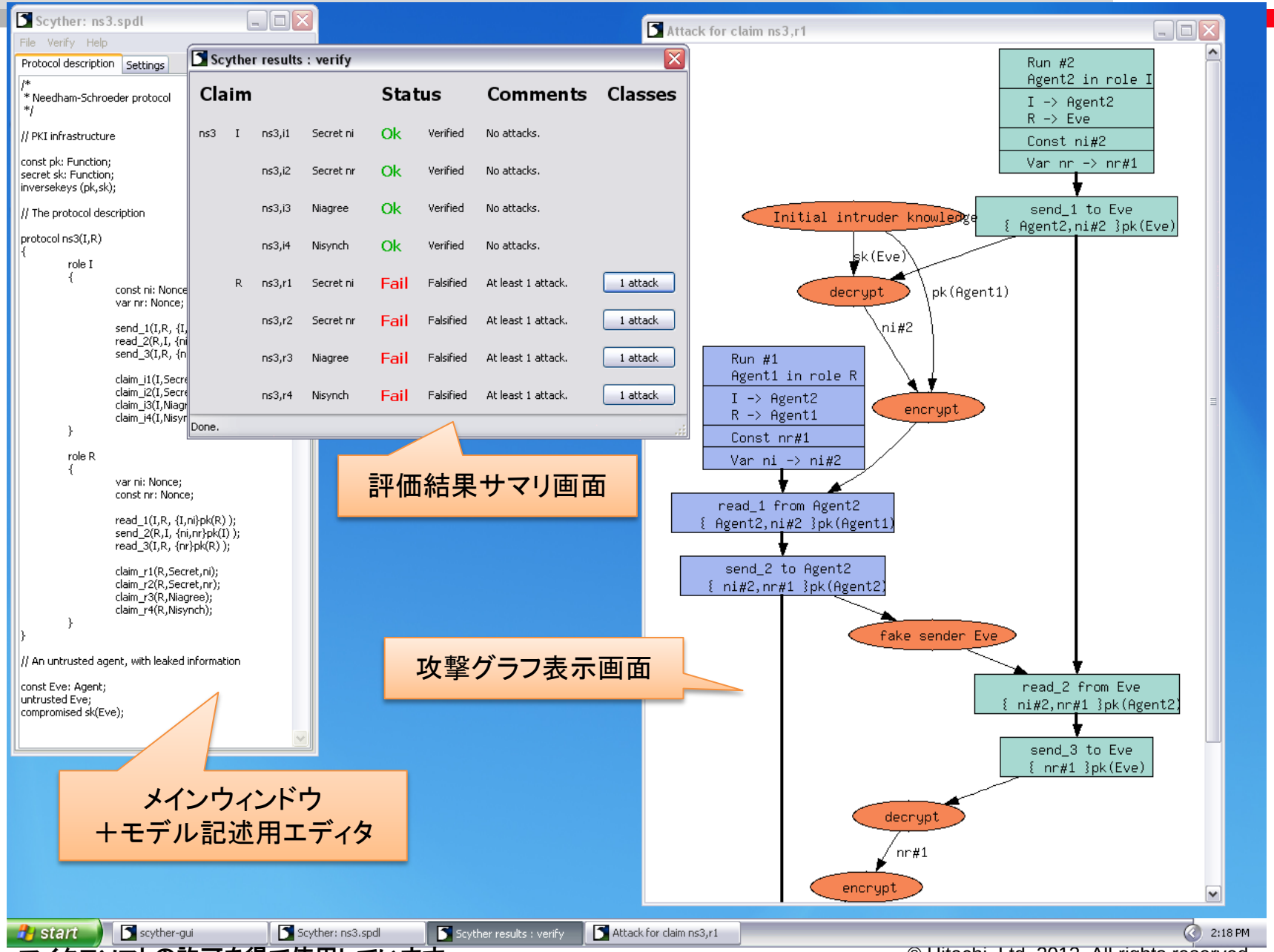
- 開発元：連邦工科大学チューリッヒ校（スイス）
- ツールタイプ：モデルチェックツール
- 動作環境：Windows/MacOS/Linux
- 参考文献：Cas Cremers and Sjouke Mauw, “Operational Semantics and Verification of Security Protocols”
- ツールの特徴
  - 評価可能なセキュリティプロパティ
    - 秘匿性
    - 認証：Loweの定義したプロパティ
    - 単射性の評価は実装されていない
      → リプレイ攻撃に対する耐性を評価することができない
  - 評価レベル
    - PAL3、PAL4いずれの評価も可能
    - PAL3については、エージェント数を指定可能
  - 2012年12月にメジャーアップデート
    - マクロ機能等が追加され、記述されたモデルの可読性が大幅に向上

Scytherのツール紹介(続き)

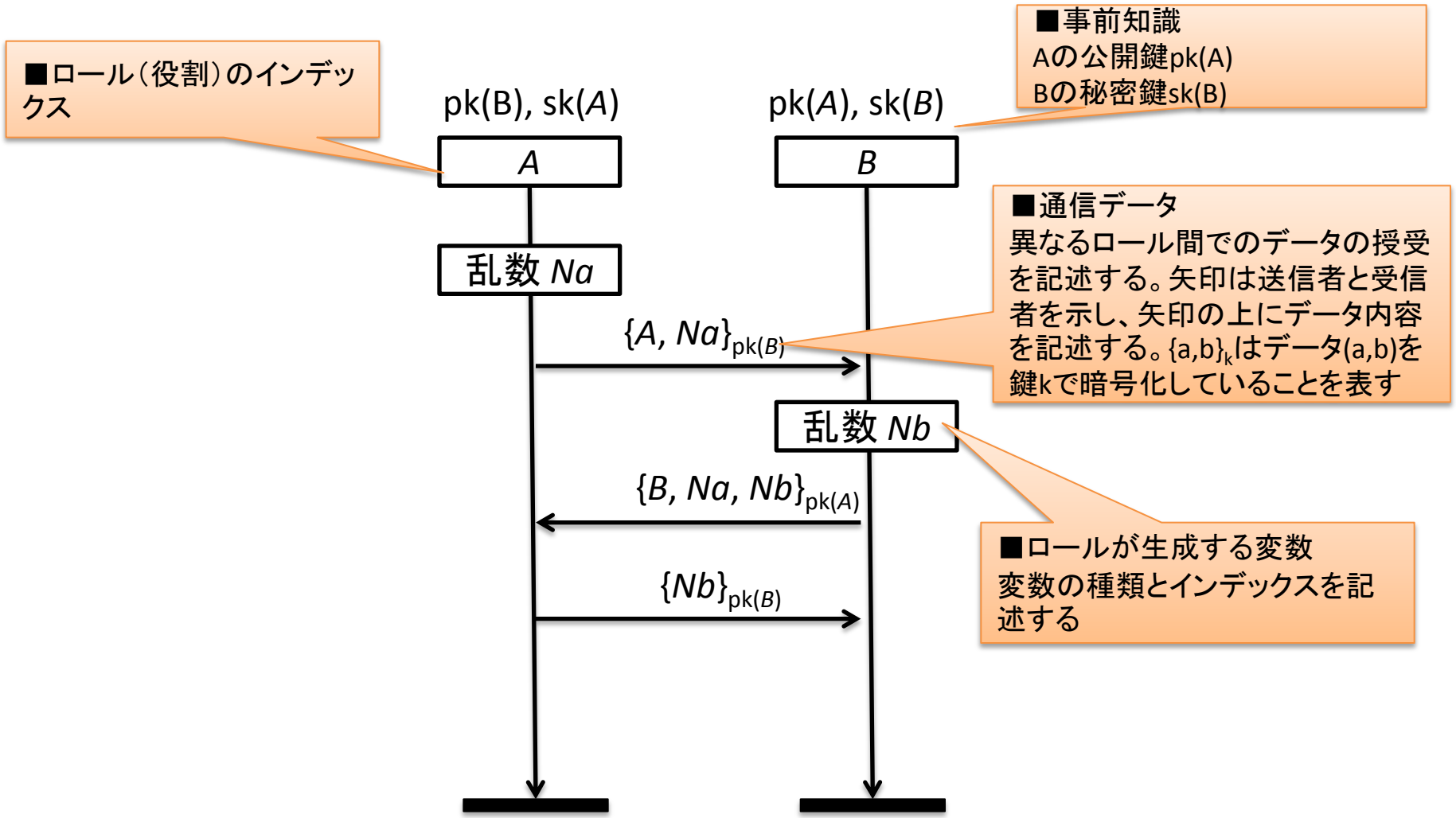
HITACHI
Inspire the Next

- **言語仕様**
  - 言語仕様は(BNF記法のレベルで)C言語に近い
    → C++プリプロセッサを用いて高度なマクロを記述可能
  - 最新版では独自にマクロ機能を実装
    - 複雑なプロトコルでも記述が容易で、記述ミスを防止
    - バリエーション評価時の書き換えコストを削減
- **ユーザーインターフェース**
  - 入力
    - モデル記述はテキストベース
  - 出力
    - サマリ:各セキュリティプロパティに関する評価結果をOK/NGで出力
    - 詳細:NGとなる場合のみ攻撃事例をメッセージシーケンスチャートに近いグラフとして生成
- **評価可能性と記述の自由度**
  - 攻撃者モデルとセキュリティプロパティがハードコーディングされているため、モデル記述の難易度が低い
  - 自由度の高い評価には向いていない
    - 攻撃者モデルはDolev-Yaoモデルのみをサポート
    - 評価可能なセキュリティプロパティはsecrecy, aliveness, weak agreement, non-injective agreement, non-injective synchronizationの5種類

Scytherの入出力インターフェース

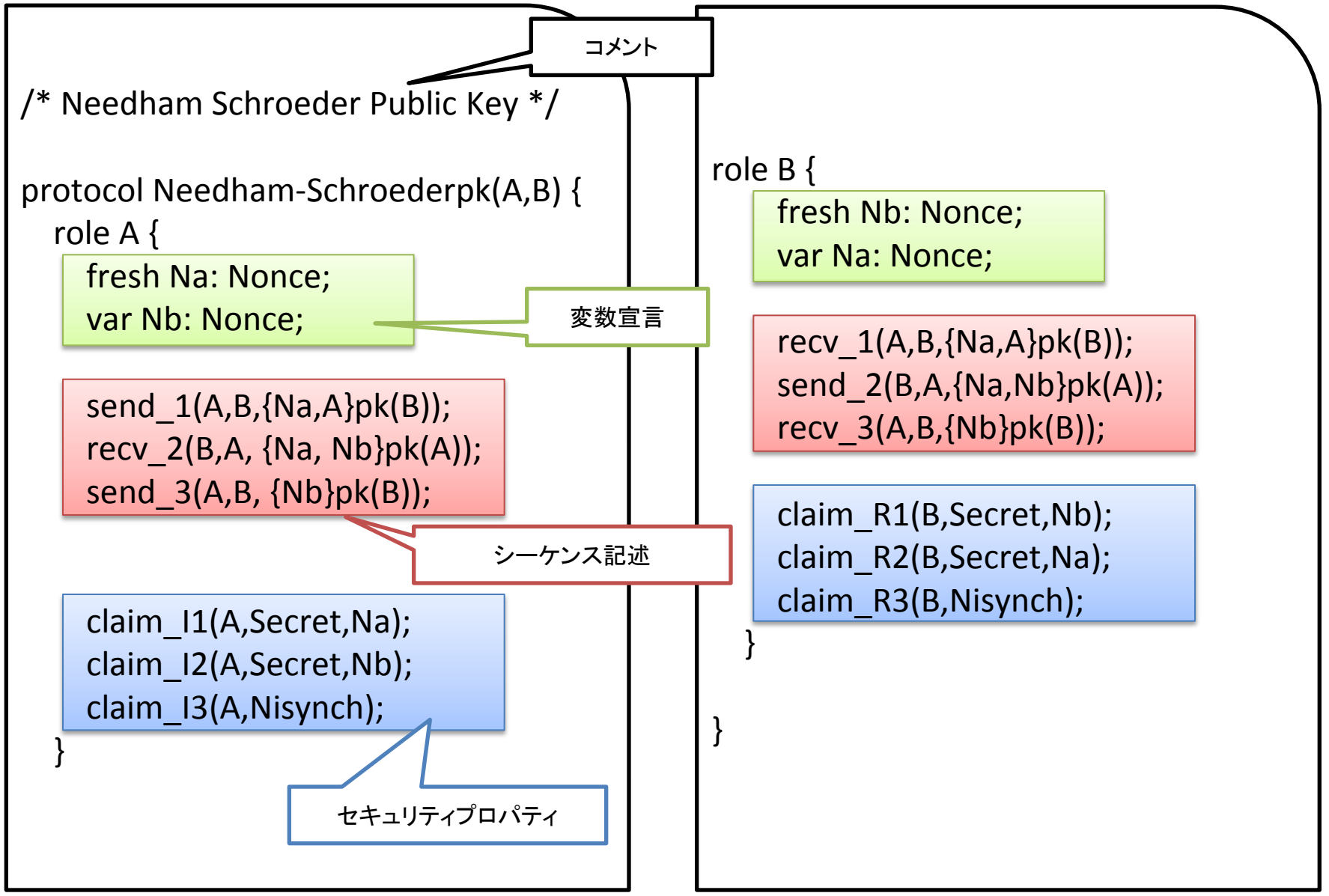


プロトコルの例(Needham-Schroeder public key(*))

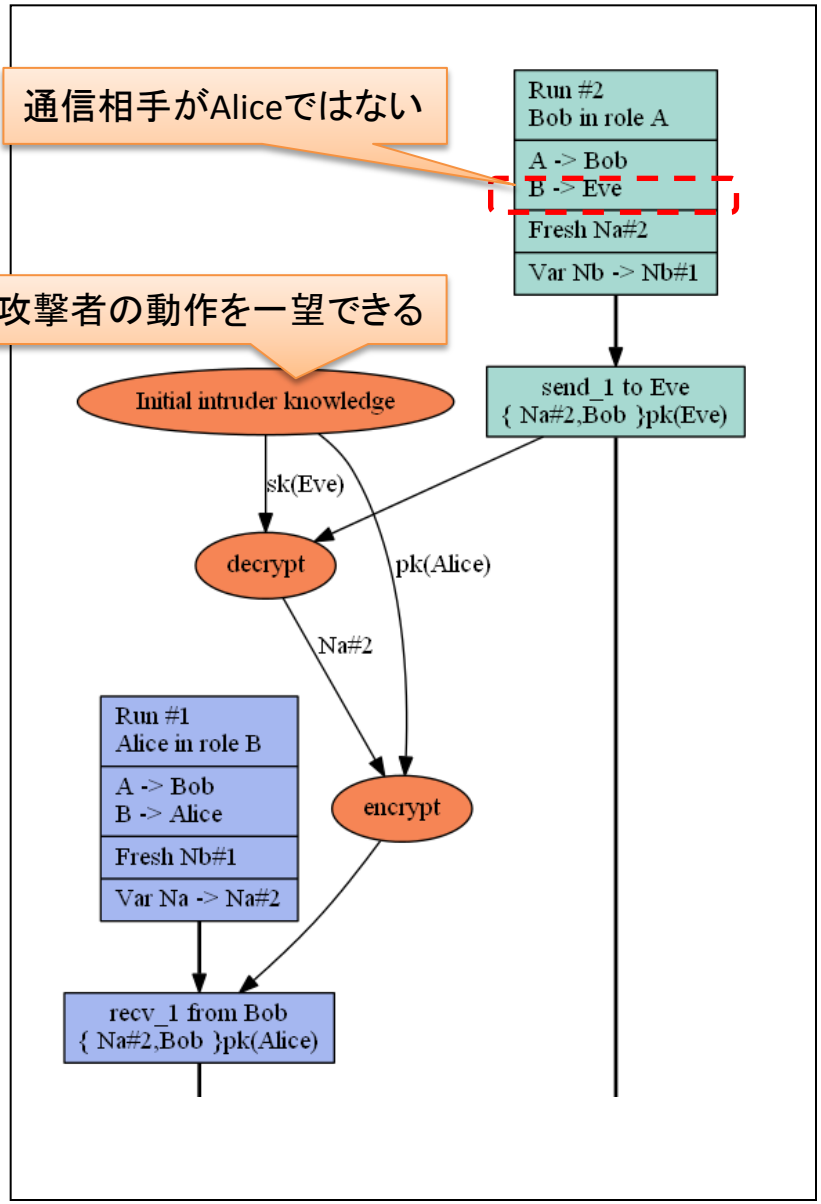


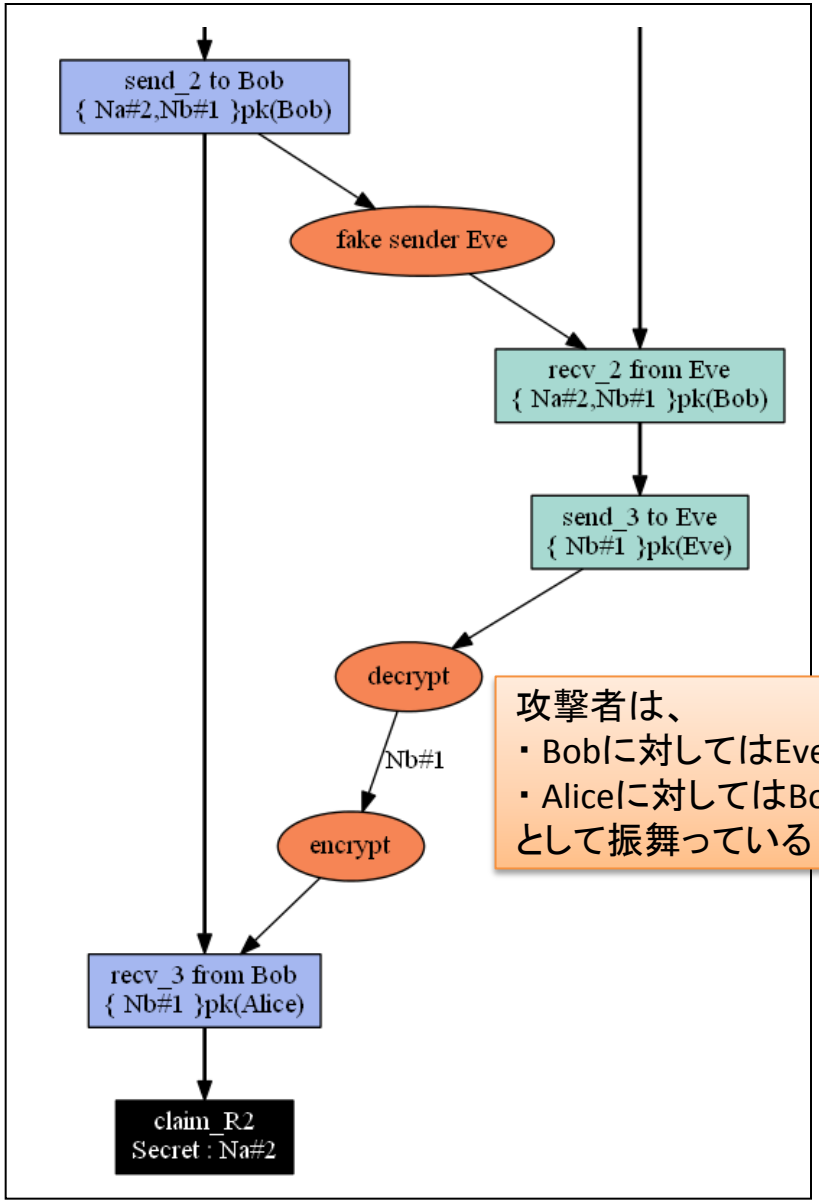
(*) 説明の簡略化のため、2者間プロトコルに変形しています。

Scytherによるモデル記述

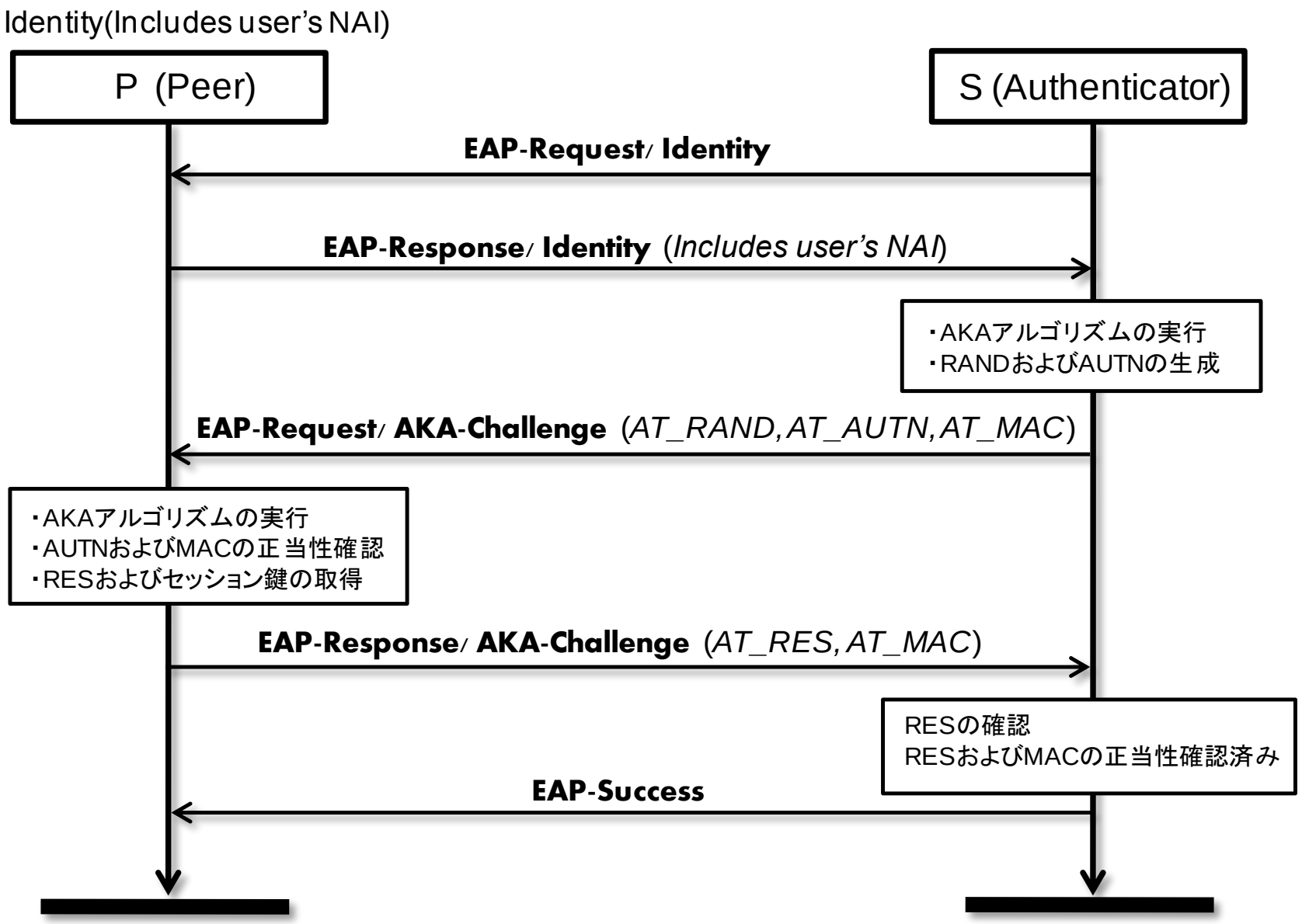


攻撃グラフ(Needham-Schroeder public key)





少し複雑なプロトコル(EAP-AKA)



Scytherによるモデル記述(EAP-AKA)

HITACHI
Inspire the Next

```
/*************************************************/
/* constants */
usertype String;
const Request, Response, Success: String;
const EAP-Identity: String;
const AKA-Challenge: String;

/*************************************************/
/* key generation function */

hashfunction f1; //used in generating AT-MAC
hashfunction f2; //used in generating AT-RES
hashfunction f3; //used in generating session key CK (encryption key)
hashfunction f4; //used in generating session key IK (integrity key)
hashfunction f5; //used in generating AK (AT-AUTN)

/*************************************************
/*
  Instead of declaration that XOR is invertible,
  a set of functions (+, -) is used.
 */
const Add: Function;
const Sub: Function; // This function is declared f      r conveniense.
inversekeys(Add, Sub);

/*************************************************     ***/
/* macros */

macro eap01 = ( Request, EAP-Identity );

macro eap02 = ( Response, EAP-Identity, P );

macro AT-RAND = ( RAND );
macro AK = f5(k(A,P), RAND);
macro AT-AUTN = ( Add( SQN, AK ) );
macro eap03-payload = ( Request, AKA-Challenge, SQN, AT-RAND, AT-AUTN );
macro AT-MAC = f1( k(A,P), eap03-payload );
macro eap03 = ( eap03-payload, AT-MAC );

macro AT-RES = ( f2(k(A,P), RAND) );
macro eap04 = ( Response, AKA-Challenge, SQN, AT-RES );

macro eap05 = ( Success );

macro CK = f3(k(A,P), RAND);
macro IK = f4(k(A,P), RAND);
```

マクロの利用により
可読性、保守性が高い

```
/*************************************************/
role P
{
  /*-----------------------------------------------*/
  //variables
  var RAND: Nonce;
  var SQN: Nonce;

  /*-----------------------------------------------*/
  //sequence

  recv_1(A,P, eap01);
  send_2(P,A, eap02);
  recv_3(A,P, eap03);

  claim_p0(P, Running, A, RAND, SQN);

  send_4(P,A, eap04);
  recv_5(A,P, eap05);


  /*-----------------------------------------------*/
  //security properties

  claim_p1(P, Secret, k(A,P));
  claim_p2(P, Weakagree);
  claim_p3(P, Niagree);
  claim_p4(P, Nisynch);
  claim_p5(P, Commit, A, RAND, SQN);

  claim_p6(P, SKR, CK );
  claim_p7(P, SKR, IK );
}

/*************************************************/
////////////////////////////////////////////////////////////////////////
/* end of file */
[EOF]
```

Scytherに関する知見

HITACHI
Inspire the Next

- プロトコル仕様
  - DH鍵交換程度の処理は抽象化によりモデル化可能
  - ただし、以下のような処理を含むプロトコルは記述できない
    - DSAなど、複雑な代数演算による復号（値の取り出し）
    - ゼロ知識証明など、確率的振る舞いを含む場合
- 攻撃者モデル
  - 盗聴、改ざんなどが可能な強い攻撃者を仮定しており、インターネット通信の評価には十分
  - 「サーバの不正を想定しない」「盗聴のみ可能」といった弱い攻撃者についてはモデルの近似が必要
- 評価結果
  - 攻撃グラフの提供により、脆弱性の確認が容易
  - （ユーザの立場からすれば）無意味な攻撃が出力されることも多い
    - 良い結果を得るためには、細かいチューニングが必要

HITACHI
Inspire the Next

KDDI研独自評価ツールによる評価
評価ツールProVerifによる評価

評価の知見とまとめ（全体）

複数ツール、複数評価者による評価結果の比較

HITACHI
Inspire the Next

#	グループ	プロトコル名	秘匿			認証		
			ProVerif	KDDI研 独自ツール	Scyther	ProVerif	KDDI研 独自ツール	Scyther
9	Yahalom	Yahalom	○			○		
10		BAN simplified version of Yahalom	○			×	△	×
13	EAP	EAP-AKA	×	○	○	×	○	○
14		EAP-Archie	○			—	○	○
15		EAP-IKEv2	○	○	—	○	○	—
17		EAP-TLS	○			○		
29	IKE	IKE signature	○			○	○	△
30		IKE public key	—	○	○	—	○	○
31		IKE pre-shared key	○			○		
32		IKEv2	○			○		

○：送信者、受信者双方ともに安全
△：送信者又は受信者の一方のみ安全
×：送信者、受信者双方ともに安全ではない
ー：評価不可

●ほとんどの暗号プロトコルをいずれかのツールで評価可能
●複数ツール、複数評価者による評価の重要性を確認

PAL3とPAL4の比較(Scyther)

HITACHI
Inspire the Next

#	グループ	暗号プロトコル	処理時間(秒)	
			PAL3	PAL4
1	Needham-Schroeder	Needham-Schroeder Public-Key Cryptographic Protocol	1620	>3600
2		Needham-Schroeder Symmetric-Key Cryptographic Protocol	0.3	0.3
3	Woo-Lam	Woo and Lam Π	0.7	>3600
4		Woo and Lam Πf	0.1	0.1
5		Woo and Lam Π1	0.1	0.1
6		Woo and Lam Π2	0.1	0.2
7		Woo and Lam Π3	0.1	0.1
8		Woo and Lam Mutual Authentication	4	8.2
13	EAP	EAP-AKA	0.3	0.1
14		EAP-Archie	0.2	0.2
15		EAP-IKEv2	63	79
16		EAP-SIM	0.3	0.3
17		EAP-TLS	13.9	>3600
19	Kerberos	Kerberos-basic	236	>3600
20		Kerberos with ticket caching	360	>3600
21		Kerberos preauth	480	>3600
31		IKEv1-preshared key	960	1086
32		IKEv2	600	789

●予想以上にPAL4でも評価が終了するケースが多かった

基礎理論・評価ツールに期待すること

HITACHI
Inspire the Next

- 最新の暗号理論への追随
  - ペアリングなど新しい演算やゼロ知識証明のような確率的振る舞いに依存する暗号プロトコル
  - プライバシやforward securityなど新しいセキュリティプロパティ
- 実装技術に関する研究
  - 現状：個々の暗号プロトコルについて、評価に要する時間を予測できない
    →評価コストを見積もれない
  - 期待
    - 暗号プロトコルの複雑度を評価する技術の確立
      （暗号プロトコルの理解を深めるためにも有効）
    - 評価アルゴリズムの高速化
- デバッグ環境の整備
  - 現状：仕様書どおりの記述になっていることをチェックするための仕組みが不足
    →複雑な暗号プロトコルの評価が困難
  - 期待：シーケンス記述の可読性を高めること

標準化に期待すること

HITACHI
Inspire the Next

- ISO/IEC 29128が提供していること
  - 暗号プロトコルの標準化における安全性評価の義務化
  - 評価のレベル感
- 評価のレベルを保証するために、さらなる標準化が必要
  - 攻撃者モデル
  - セキュリティプロパティ
    - 開発者と専門家のあいだに認識・用語のずれ
  - 評価報告書のテンプレート
  - 評価プロセス
    - 抽象レベルで暗号プロトコル仕様、達成したいセキュリティプロパティを記述
      →安全性評価を実施
      →安全性評価の前提を崩さないように仕様を詳細化
    - 安全性評価の前提条件は、実装要件としてまとめるべき
  - （評価ツール）

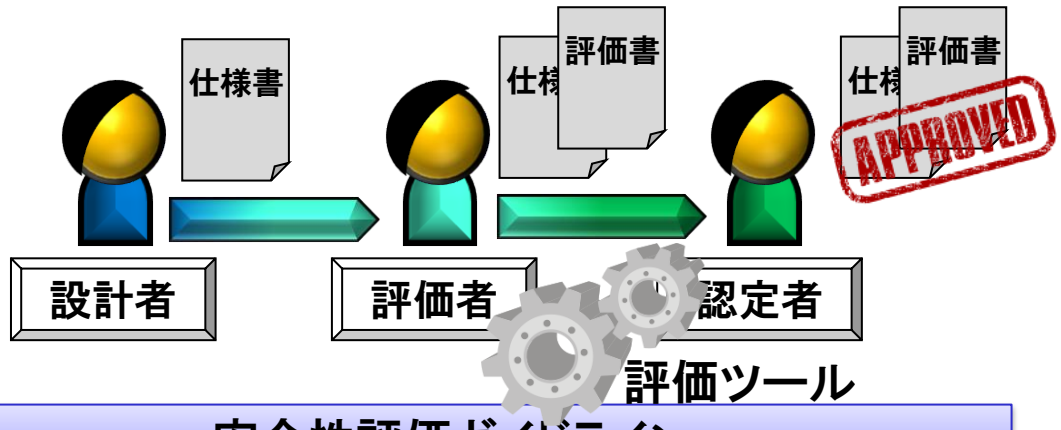
安全性評価ガイドライン

HITACHI
Inspire the Next

調査研究及び実証実験の結果を踏まえ、暗号プロトコルの安全性評価のガイドラインを策定

- ガイドライン策定の目的
  - ✓ 暗号プロトコルの開発、評価、認証を行うための基準作りの一環として、ISO/IEC 29128に準拠した評価の実施及びその報告スタイルを明確化
    - ⇒ 報告書の記載レベルの保証
    - ⇒ 報告書作成の負荷軽減

- 対象読者
  - ✓ 設計者、評価者、認定者



それぞれの項目の詳細化

用語の統一

抽象レベルでの項目

安全性評価ガイドライン

セキュリティプロパティ　攻撃者モデル　…

ISO/IEC 29128

暗号プロトコル評価から得られた知見および提言(まとめ)

HITACHI
Inspire the Next

- 仕様の記述
  - ✓ 曖昧さを排除し、解釈が一意となるようにすべき
  - ✓ 仕様に利用環境や想定する攻撃者、達成したいセキュリティプロパティ等を記載すべき
- 評価の進め方
  - ✓ ツールを用いても、評価にミスが混入する可能性が残るため、複数の評価を実施して、評価結果の信頼性を高める努力をすべき
- 標準化
  - ✓ ISO/IEC 29128に基づいた評価を実施する上で、攻撃者モデル、セキュリティプロパティの概念、用語を標準化することが望ましい

その後の展開

- 事業で実施したプロトコルの評価結果をNICTのウェブサイトで公開中
  - http://crypto-protocol.nict.go.jp/

- ISO/IEC 29128を他の標準団体に展開
  - まずはMLベースで関係者を中心に議論中

Dear all, I made a contact with chairman of ETSI SAGE,
…

This is very good news, XXXX. You deserve credit for reaching out.
…

- 積極的なご参加をお待ちしています！
  - 未評価の暗号プロトコルを評価してみる
  - 評価ツールの「使ってみた」レポート
  - 評価ツールを作ってみる
  - などなど。

HITACHI
Inspire the Next

END

暗号プロトコルに関する評価実証実験

2013/09/11

株式会社 日立製作所
横浜研究所


HITACHI
Inspire the Next