


暗号プロトコル評価フレームワークの国際標準 ISO/IEC 29128とCRYPTRECにおける適用事例

2011.9.16

日本応用数理学会 年会 FAISオーガナイズド・セッション

松尾真一郎（情報通信研究機構）
大塚玲（産業技術総合研究所）
宮崎邦彦（日立製作所）

発表の概要

- ISO/IEC 29128の標準化状況
- CRYPTRECにおけるエンティティ認証プロトコルへの形式化手法の適用


暗号プロトコル評価技術

多数の技術・ツールが研究開発されている

(1)様相論理を用いるもの

限定された認証性質についてしか推論できないため、現在ではあまり利用されていない（例：BANロジック）

(2)モデルチェッキング手法を用いるもの

自動検証可能。安全性評価に大きな効果を上げている（例：NRL、FDR、AVISPA、ProVerif、SCYTHER、CryptoVerifなど多数）

(3)定理証明を用いるもの

通常、人手による証明戦略の指示などが必要であるため、完全な自動証明は困難だが、セッション数の制限などはないため、より強い検証結果を得られる（例：Isabelle）


暗号プロトコル評価技術の分類

抽象化レベルもさまざま

- Dolev-Yaoモデル：暗号プリミティブを完全なものと仮定するモデル
- 計算量理論的なモデル：暗号プリミティブを確率的な振る舞いをする、より現実的なものと仮定するモデル

検証範囲もさまざま

- Unbounded：セッション数に制限を設けず検証
- Bounded：セッション数に制限を設けた範囲のみの探索により検証


主な暗号プロトコル検証ツール

	Model checking		Theorem proving
Symbolic	NRL FDR AVISPA	SCYTHER ProVerif AVISPA (TA4SP)	Isabelle/HOL
Cryptographic		CryptoVerif	BPW(on Isabelle/HOL) Game-based Security Proof（on Coq)

Unbounded


実用上の課題

- 各ツールが扱えるプロトコル／セキュリティ要件はそれぞれ異なり、また、検証結果の保証の程度も異なる
- 異なる手法間の関係性も必ずしも明らかではない
- その結果、暗号プロトコルを、実務的に、開発あるいは利用する立場からは、プロトコルをどのツールを使って評価すればよいのか、またどういう結果が得られれば安心できるのか、が分からない状況にある
- ➔暗号プロトコル評価に一定の基準を与えたい！

ISO/IEC 29128

- ISO/IEC 29128 “Verification of Cryptographic Protocols”
- 日本からの提案に基づきISO/IEC JTC 1/SC 27/WG 3にて2007年にプロジェクト開始
- 標準化スケジュール


ISO/IEC 29128概要

プロトコル評価を行う上で、共通的に必要となると考えられる記述事項（プロトコル仕様、攻撃者モデル、セキュリティ要件、自己評価資料）を規定し、さらに検証の度合いに応じて、以下の4つのプロトコル保証レベルを定義

- **プロトコル保証レベル１**
  プロトコル仕様は準形式的に記述され、攻撃者モデル、セキュリティ要件は非形式的に記述されていてよい。また検証は、非形式的な議論によるものでよい。
- **プロトコル保証レベル２**
  プロトコル仕様、攻撃者モデル、セキュリティ要件は**数学的に厳密な形で記述**されなければならない。検証には、**安全性証明の正しさを専門家が確認**できることが求められる。
- **プロトコル保証レベル3**
  プロトコル仕様、攻撃者モデル、セキュリティ要件は**機械的に処理可能な形で形式的に記述**されなければならない。また検証は、**ツールを用いた形式的な証明**でなければならない。ただし検証に当たっては、並行動作するセッション数には上限を設けてよい。
- **プロトコル保証レベル4**
  プロトコル保証レベル２に加えて、さらにセッション数に関する制限なしに検証されなければならない。


プロトコル保証レベル(PAL)

Protocol Assurance Level	PAL1	PAL2	PAL3	PAL4
Protocol Specification	**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.**	
Adversarial Model	**PAM_INFORMAL** Informal description of adversarial model.	**PAM_ FORMAL** **Formal description of adversarial model.**	**PAM_ MECHANIZED** **Formal description of adversarial model in a tool-specific specification language, whose semantics is mathematically defined.**	
Security Property	**PSP_INFORMAL** **Informal description of security property**	**PSP_ FORMAL** **Formal description of security property.**	**PSP_ MECHANIZED** **Formal description of security property in a tool-specific specification language, whose semantics is mathematically defined.**	
Self-assessment Evidence	**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.


標準化過程での議論（1）

特定手法・ツールに対する中立性

- 特定のツールを「標準ツール」として標準化するのではなく、各保証レベルにおいてツールに求められる性質を標準化すべき
- Model CheckingかTheorem Proverかではなく、BoundedかUnboundedか、で保証レベルを分ける
- 新たな（より高性能、高機能な）プロトコル評価ツールの活用を妨げない。


標準化過程での議論（2）

計算量モデル（暗号学的健全性）

- 多くのツールはDolev-Yaoモデルを前提としている
  - 攻撃者はネットワークを自由にコントロールできる
  - 暗号プリミティブは完全である
- 一方、暗号プリミティブを完全なものと仮定しない、より現実的なモデル（計算量モデル）に基づく、プロトコル検証技術も存在する。これらをより保証レベルの高い評価とみなすべきではないか？
- 現時点では、標準規格の中で独立した保証レベルを定義するには未成熟と判断。今後の技術の進展に期待

標準化過程での議論（３）

手証明の扱い

- 「紙と鉛筆による証明」も「非形式的な議論」もともにPAL1だったが、**PAL1とPAL2に分離**
- 手証明は誤りが混入しやすく、認定を与える機関等が証明の正しさを確認するのが困難なことから、**手証明のPAL2を、機械証明つきのPAL3、PAL4から区別**
- 優れた最新の理論的成果がツールとして利用可能なレベルにまで成熟することを期待


制度化に向けた課題

- 多くのツールはDolev-Yaoモデルを前提としている
  - 多くのツールが開発されているが、個々のツールにはそれぞれ制限事項もある(例：代数的な性質は扱えるツールと扱えないツールが存在する)
  - 有用な暗号プロトコルとそれを評価可能なツールとのギャップを埋めることが継続的に望まれる
- 熟練技術者
  - 制度として確立するためにはツールが存在するだけでは不十分であり、それらを活用して評価する能力をもった熟練技術者を十分に有した体制が必要
  - ツールの改良により熟練技術者の教育に必要なコストの削減を図ることも重要かつ有用と考えられる


CRYPTRECにおける形式化手法のエンティティ認証プロトコルへの適用

CRYPTRECの概要

- CRYPTography Research and Evaluation Committees の略
- 電子政府で利用する暗号技術について、その安全性を担保することを目的として、総務省・経済産業省の両省によって運営されている
- “電子政府推奨暗号リスト” を公開、維持管理をするとともに、リスト掲載暗号技術に関連する報告書や、リスト掲載暗号の利用方法を 示す “リストガイド” を発行
- 電子政府推奨暗号リスト
  - 国内外から暗号技術を公募し、国内外の専門家のレビューと公開の議論を経て、選考を実施
  - NISCの政府機関統一基準において参照され、電子政府システムにおける遵守事項となっている
  - FISCのガイドラインで参照され、金融機関の情報システムにおい てリスト掲載暗号以外の技術を利用している場合、金融庁検査の際 にその正当性を別途示す必要がある

エンティティ認証の評価

- 電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証
- 安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定
- 電子政府推奨暗号リストに掲載されている、あるいは 応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利 用している場合には、暗号プリミティブを理想的に安全なものとする
- その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を実施
- 提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証

今回の評価対象

- ISO/IEC 9798-2（共通鍵暗号を用いたプロトコル）
- ISO/IEC 9798-3（電子署名を用いたプロトコル）
- ISO/IEC 9798-4（検査関数（MAC）を用いたプロトコル）

例）9798-2 Mechanism 4 - Three-pass authentication

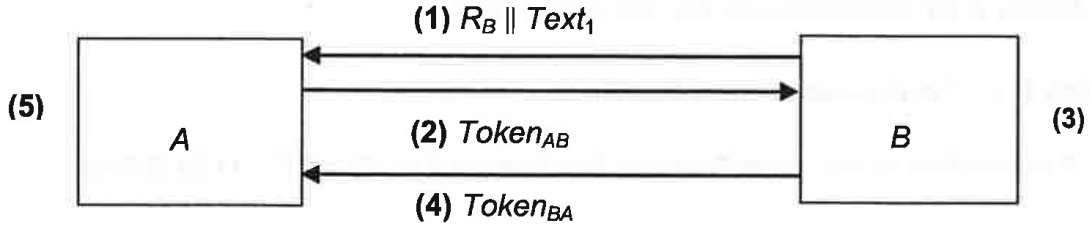


Figure 4 — Mechanism 4 — Three-pass authentication

The tokens are of the following form:

$$Token_{AB} = Text_3 \| e_{K_{AB}} (R_A \| R_B \| I_B \| Text_2)$$

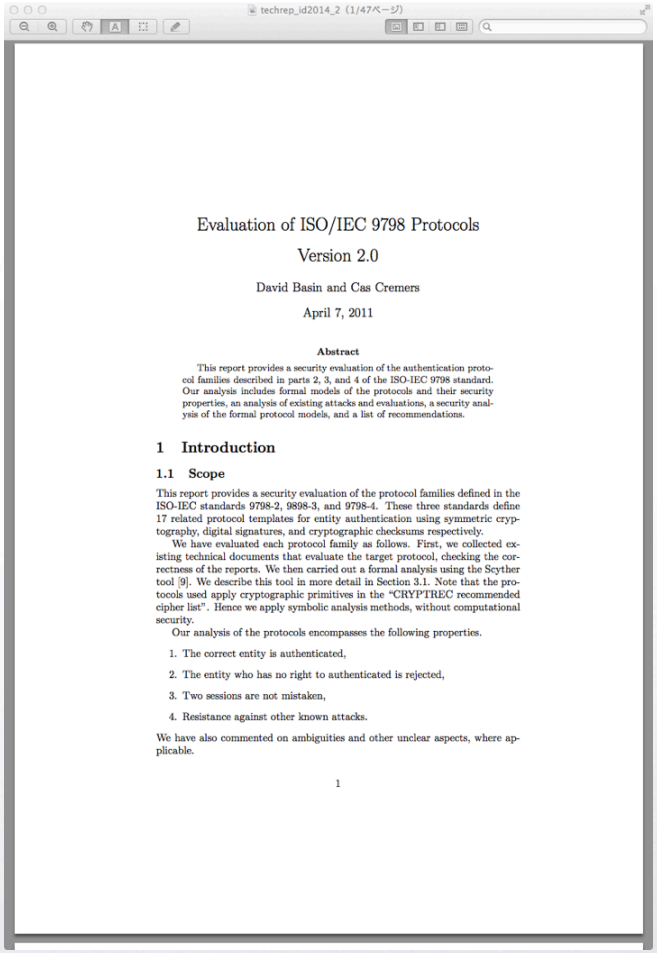
$$Token_{BA} = Text_5 \| e_{K_{AB}} (R_B \| R_A \| Text_4)$$

The inclusion of the distinguishing identifier I_B in $Token_{AB}$ is optional.

評価報告書

CRYPTRECのホームページ http://www.cryptrec.go.jp よりダウンロード可能

No.	報告書名	著者名	年度	PDF Files
2001	共通鍵ブロック暗号CLEFIAの安全性評価報告書(3月29日更新)	金子敏信	2010	PDF2001(3253KB)
2002	Evaluation of security level of CLEFIA	—	2010	PDF2002(132KB)
2003	HyRAL安全性評価報告書（3月1日更新）	岩田哲	2010	PDF2003_2(508KB)
2004	Security Analysis of HyRAL	Heung Youl YOUM, Jung Hwan Song, Sun Young Lee	2010	PDF2004(2467KB)
2005	Security Evaluation of PC-MAC-AES	Lei Wang Kazuo Sakiyama Iwamasa Nishikado Kazuo Ohta	2010	PDF2005(3471KB)
2006	CRYPTREC evaluation report on PC-MAC-AES	John P.Steinberger	2010	PDF2006(299KB)
2007	Enocoro-128v2の安全性評価	桑門秀典	2010	PDF2007(403KB)
2008	Security Evaluation of Stream Cipher Enocoro-128v2	Martin Hell and Thomas Johansson	2010	PDF2008(233KB)
2009	KCipher-2の安全性に関する評価	白石善明	2010	PDF2009(405KB)
2010	Security Evaluation of the K2 Stream Cipher（3月29日更新）	Bart Preneel	2010	PDF2010(313KB)
2011	暗号利用モードおよびメッセージ認証コードに関する安全性評価	廣瀬勝一	2010	PDF2011(522KB)
2012	Evaluation of some Blockcipher Modes of Operation(3月4日更新)	Phillip Rogaway	2010	PDF2012(1446KB)
2013	ISO/IEC 9798プロトコルの安全性評価	山村明弘	2010	PDF2013(210KB)
2014	Evaluation of ISO/IEC 9798 Protocols(4月19日更新)	David Basin and Cas Cremers	2010	PDF2014_2(217KB)



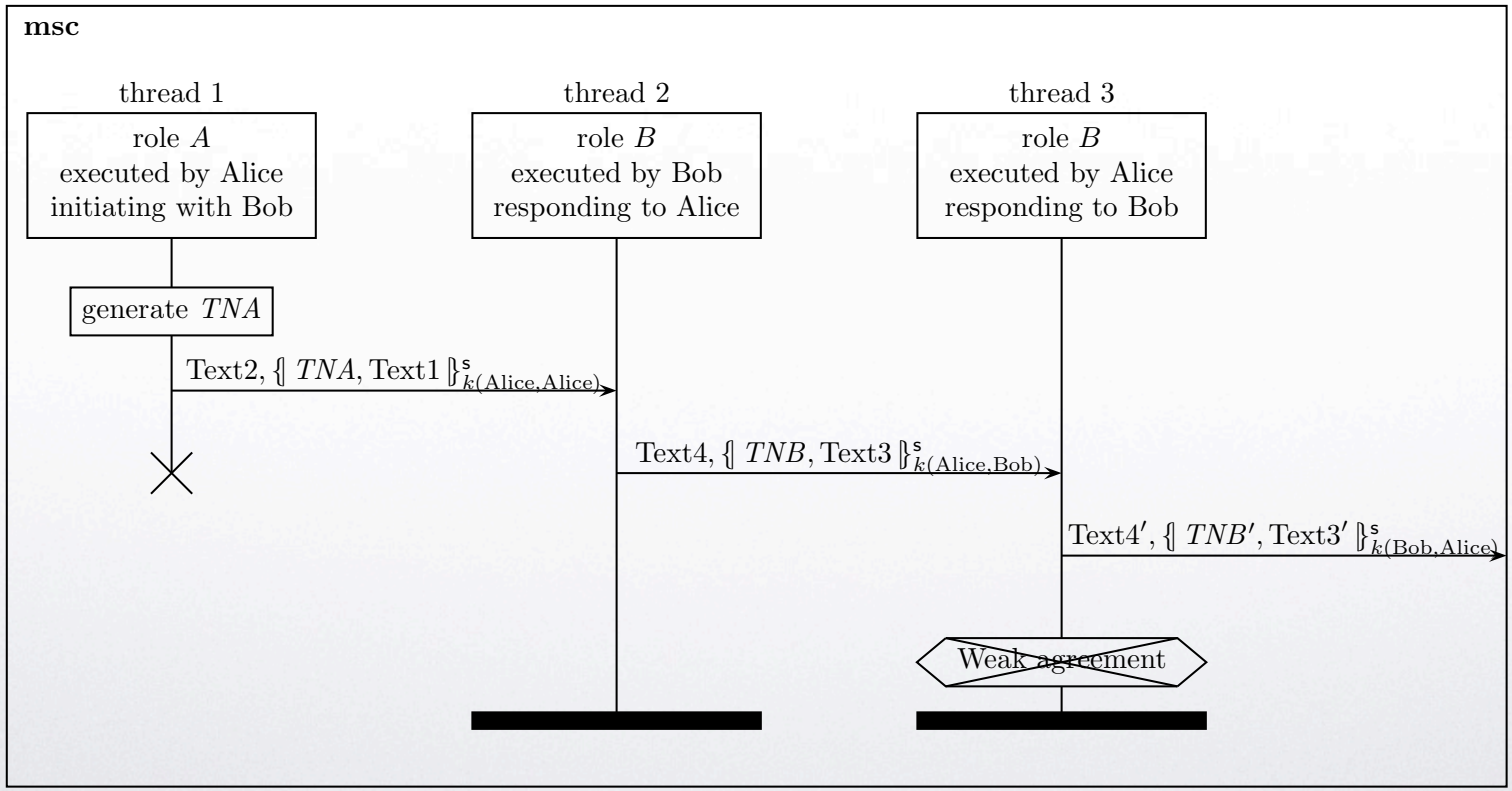
安全性評価結果

- 評価者Aは、プロトコルの脆弱性について大きな問題は発見しなかったが、数多くのタイプが存在するために、電子政府で利用する際の指針を与えることを求めている。
- 特にTime-variant Parameterとして、タイムスタンプ、シーケンス番号、乱数を用いるが、その使い分けについて推奨を示すことを求めている。

- 評価者Bは、フォーマルメソッドのツールである、Scytherを用いて安全性検証を実施。
  - Scytherはunbounded verificationをサポートしているが、本評価ではスレッド数5、1プロトコル当たりの計算機上の評価時間を10分として評価
- 5つのプロトコルの計19バリアントについて、3つの攻撃の存在を指摘
  - 各攻撃に関しては、修正方法が示されている。

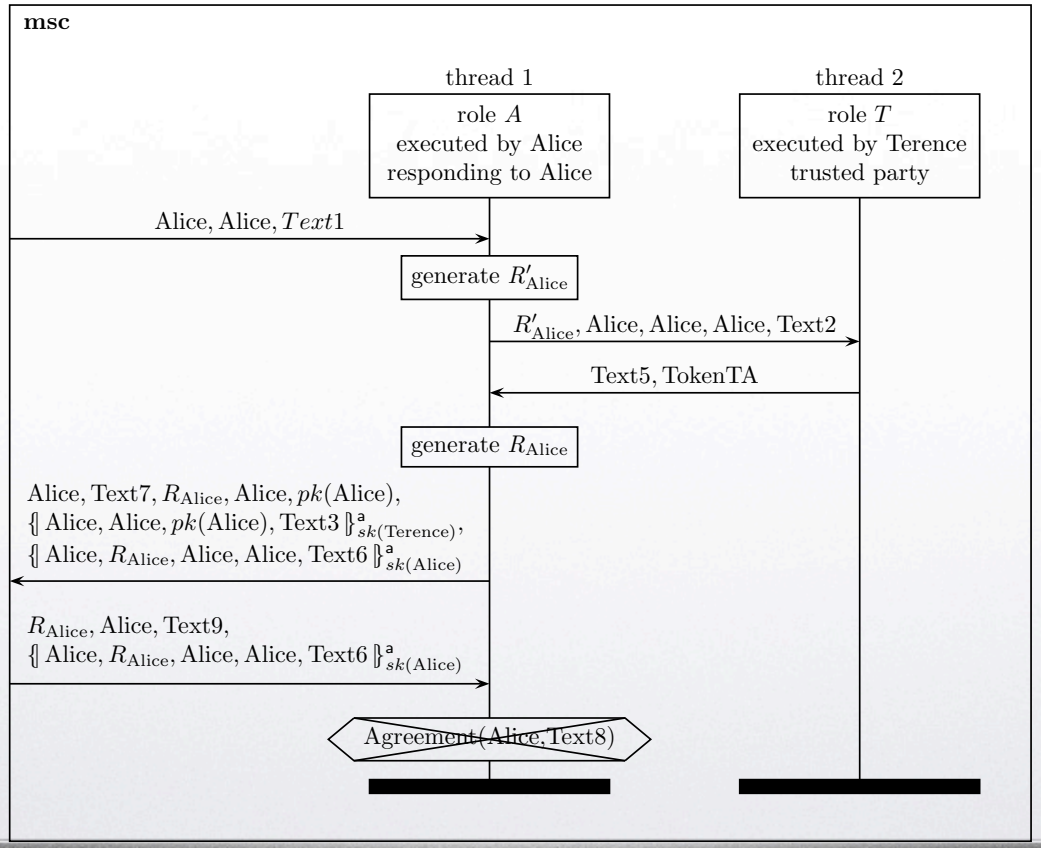
安全性評価結果(1)

- Role Mix-up Attack
  - エンティティの役割に関する確認ができなくなる攻撃
  - Matching conversationやプロトコルにおける同期の問題が発生



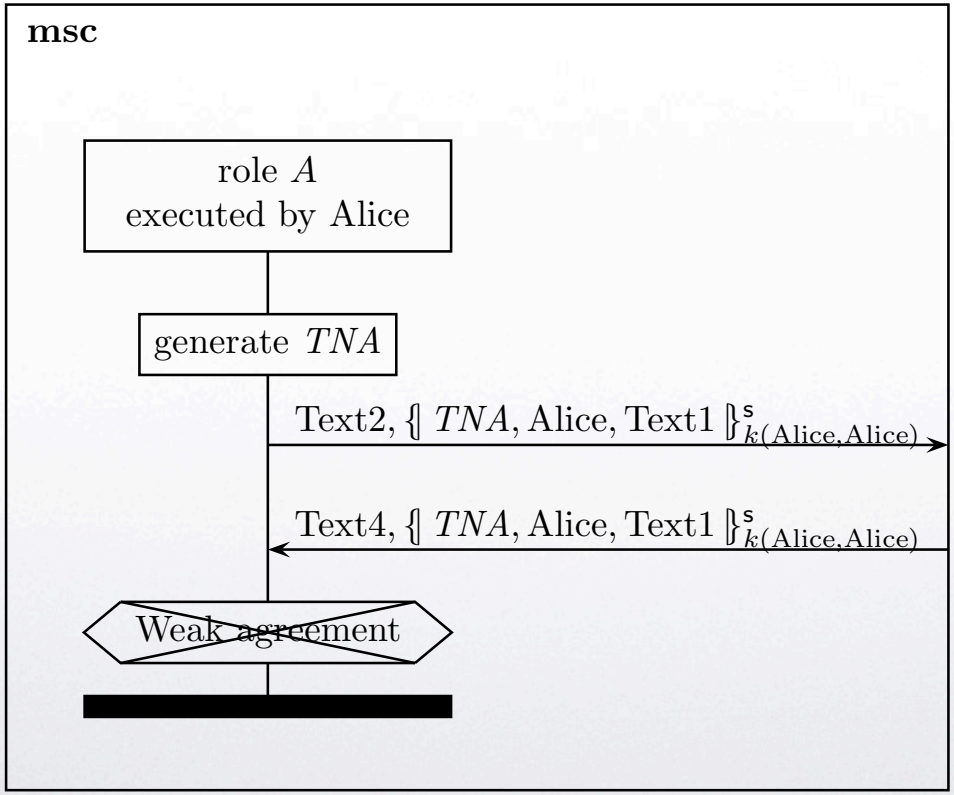
安全性評価結果(2)

- Type Flow Attack
  - エンティティの名前がnビットのビット列にエンコードされていて、プロトコル中のnonceもnビットで表現されるときに発生
  - エンティティの名前を誤ってfreshな乱数として受け取ってしまう。



安全性評価結果(3)

- Reflection Attack
  - プロトコルのInitiatorとResponderが同一の場合に起こる攻撃
  - オプションフィールドの利用目的が規定されていないため、暗号化されたデータをそのまま再利用することで攻撃が発生。



安全性評価結果

No	Protocol	Claim	No type checks Alice-talks-to-Alice initators	Type checks Alice-talks-to-Alice initators	No type checks No Alice-talks-to-Alice initators	Type checks No Alice-talks-to-Alice initators
1	isoiec-9798-2-3	A Agreement(B,TNB,Text3)	•	•	•	•
2	isoiec-9798-2-3	A Weakagree	•	•	•	•
3	isoiec-9798-2-3	B Agreement(A,TNA,Text1)	•	•	•	•
4	isoiec-9798-2-3-udkey	A Agreement(B,TNB,Text3)	•	•	•	•
5	isoiec-9798-2-3-udkey	A Weakagree	•	•	•	•
6	isoiec-9798-2-3-udkey	B Agreement(A,TNA,Text1)	•	•	•	•
7	isoiec-9798-2-5	A Alive	•	•		
8	isoiec-9798-2-5	A Agreement(B,Kab,Text5,Text7)	•	•		
9	isoiec-9798-2-5	A Weakagree	•	•		
10	isoiec-9798-2-5	B Alive	•	•	•	•
11	isoiec-9798-2-5	B Agreement(A,Kab,Text5)	•	•	•	•
12	isoiec-9798-2-6	A Alive	•	•	•	•
13	isoiec-9798-2-6	A Agreement(B,Kab,Text6,Text8)	•	•	•	•
14	isoiec-9798-2-6	B Alive	•	•	•	•
15	isoiec-9798-2-6	B Agreement(A,Kab,Text6)	•	•	•	•
16	isoiec-9798-3-3	A Agreement(B,TNB,Text3)	•	•	•	•
17	isoiec-9798-3-3	A Weakagree	•	•	•	•
18	isoiec-9798-3-3	B Agreement(A,TNA,Text1)	•	•	•	•
19	isoiec-9798-3-7-1	A Agreement(B,Ra,Rb,Text8)	•		•	
20	isoiec-9798-4-3	A Agreement(B,TNb,Text3)	•	•	•	•
21	isoiec-9798-4-3	A Weakagree	•	•	•	•
22	isoiec-9798-4-3	B Agreement(A,TNa,Text1)	•	•	•	•
23	isoiec-9798-4-3-udkey	A Agreement(B,TNb,Text3)	•	•	•	•
24	isoiec-9798-4-3-udkey	A Weakagree	•	•	•	•
25	isoiec-9798-4-3-udkey	B Agreement(A,TNa,Text1)	•	•	•	•

評価結果のまとめと対応

- ISO/IEC 9798で定義されているプロトコルの一部タイプに脆弱性を発見
- これらの脆弱性は、利用されている暗号プリミティブそのものを攻撃しなくても発生し、現実的な攻撃と考えられる
- CRYPTRECとしては、脆弱性のあるタイプについては使用しないように注釈をつけて、電子政府推奨暗号におけるエンティティ認証プロトコルとする
- 脆弱性の発見されたプロトコルについては、修正方法が存在するため、ISO/IECに対して修正を求めており、現在修正を実施中
  - 認証に利用する鍵は他の目的の鍵と区別できるようにする
  - プロトコル中の暗号化された情報がユニークに区別できるようにする

まとめ

- ISO/IEC 29128の標準化動向
  - FDIS版の概要
- CRYPTRECにおける適用事例
  - ISO/IEC 9798-2/3/4における3種類の攻撃の発見
  - ISO/IEC JTC1において修正中