事務局選出暗号の安全性評価について
エンティティ認証

CRYPTREC
Cryptography Research and Evaluation Committees

公募の目的 (公募要項P.4 第5.1節抜粋)

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証(新設)

・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

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証応募状況及び評価対象

事務局選出技術

- 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）

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-2の概要

- 共通鍵暗号を用いたエンティティ認証
  - 6つのタイプ
    - 片側認証1パス
    - 片側認証2パス
    - 相互認証2パス
    - 相互認証3パス
    - 相互認証4パス-信頼できる第三者機関あり
    - 相互認証5パス-信頼できる第三者機関あり

- 共通鍵を秘密に所有していることが前提
- 疑似乱数はISO/IEC 18031を用いる
- Time-variant Parameterとして、タイムスタンプ、シーケンス番号、乱数などを用いる

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-2の例

相互認証4パス

$$1.\ B \Longrightarrow A : R_B||Text_1$$
$$2.\ A \Longrightarrow B : Token_{AB}$$
$$3.\ B \Longrightarrow A : Token_{BA}$$
$$Token_{AB} = Text_3||e_{K_{AB}}(R_A||R_B||I_B||Text_2)$$
$$Token_{BA} = Text_5||e_{K_{AB}}(R_B||R_A||Text_4)$$

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-3の概要

- 公開鍵暗号（電子署名）を用いたエンティティ認証
  - 7つのタイプ
    - 片側認証1パス
    - 片側認証2パス
    - 相互認証2パス
    - 相互認証3パス
    - 相互認証2パス-並列実行（4パス）
    - 相互認証5パス(initiated by A)
    - 相互認証5パス(initiated by A)
- 鍵に対する証明書を保有することが前提
- 疑似乱数はISO/IEC 18031を用いる
- Time-variant Parameterとして、タイムスタンプ、シーケンス番号、乱数などを用いる

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-3の例

相互認証3パス

$$
\begin{aligned}
1.\ B &\Longrightarrow A : R_B||Text1 \\
2.\ A &\Longrightarrow B : Cert_A||Token_{AB} \\
3.\ B &\Longrightarrow A : Cert_B||Token_{BA} \\
Token_{AB} &= R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2) \\
Token_{BA} &= R_B||R_A||A||Text5||sS_B(R_B||R_A||A||Text4)
\end{aligned}
$$

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-4の概要

- 暗号検査関数を用いたエンティティ認証
  - 4つのタイプ
    - 片側認証1パス
    - 片側認証2パス
    - 相互認証2パス
    - 相互認証3パス

- 鍵を秘密に共有することが前提
- 疑似乱数はISO/IEC 18031を用いる
- Time-variant Parameterとして、タイムスタンプ、シーケンス番号、乱数などを用いる

CRYPTREC
Cryptography Research and Evaluation Committees

ISO/IEC 9798-3の例

相互認証3パス

$$1.\ B \Longrightarrow A : R_B||Text1$$
$$2.\ A \Longrightarrow B : Token_{AB}$$
$$3.\ B \Longrightarrow A : Token_{BA}$$
$$Token_{AB} = R_A||Text3||f_{K_{AB}}(R_A||R_B||B||Text2)$$
$$Token_{BA} = Text5||f_{K_{AB}}(R_B||R_A||Text4)$$

CRYPTREC
Cryptography Research and Evaluation Committees

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。

安全性評価結果

- 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

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

- 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動機の問題が発生

- 攻撃が存在するプロトコルとバリアント
  - 9798-2-3 with unidirectional key
  - 9798-2-5
  - 9798-3-3
  - 9798-4-3 with unidirectional key

安全性評価結果

- 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

- 攻撃が存在するプロトコルとバリアント
  - 9798-3-7 Option 1

安全性評価結果

- 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

- 攻撃が存在するプロトコルとバリアント
  - 9798-2-3
  - 9798-2-5

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 Agreement(B,Kab,Text5,Text7)	・	・		
8	isoiec-9798-2-5	A Weakagree	・	・		
9	isoiec-9798-2-5	B Agreement(A,Kab,Text5)	・	・	・	・
10	isoiec-9798-3-3	A Agreement(B,TNB,Text3)	・	・	・	・
11	isoiec-9798-3-3	A Weakagree	・	・	・	・
12	isoiec-9798-3-3	B Agreement(A,TNA,Text1)	・	・	・	・
13	isoiec-9798-3-7-1	A Agreement(B,Ra,Rb,Text8)	・		・	
14	isoiec-9798-4-3	A Agreement(B,TNb,Text3)	・	・		
15	isoiec-9798-4-3	A Weakagree	・	・		
16	isoiec-9798-4-3	B Agreement(A,TNa,Text1)	・	・		
17	isoiec-9798-4-3-udkey	A Agreement(B,TNb,Text3)	・	・	・	・
18	isoiec-9798-4-3-udkey	A Weakagree	・	・	・	・
19	isoiec-9798-4-3-udkey	B Agreement(A,TNa,Text1)	・	・	・	・

CRYPTREC
Cryptography Research and Evaluation Committees

まとめ

- 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、修正が完了次第注釈について再検討を行うこととする。

CRYPTREC
Cryptography Research and Evaluation Committees