5W－6

ICカード認証技術のセキュリティ向上策

市原尚久[1]　星川知之[1]　若月温[1]

Wayne Tompkin[2]　Rene Staub[2]

第1節　背景

近年,カードシステムの多機能化とセキュリティ強化を図る為にICカード化が進んでおり,様々な分野で利用されている.ところが近年,ICカードのセキュリティ(特に耐タンパ性)への警鐘が鳴らされており[1][2],その対策方法について検討が行われてきている[3].

本論文ではICカード1における耐タンパセキュリティの脆弱性に対する対策として,付加技術を搭載するICカードを提案し,その実現手段と強度について言及し,従来よりもセキュリティの高いICカードの実現例を報告する.

第2節　ICカードのセキュリティ

2.1.概要

ICカードのセキュリティにはチップ内部で暗号化処理,署名生成検証,認証プロトコルなどによって実現できるセキュリティ(能動的セキュリティ)と,ＩＣチップ自体が偽造されない事や,データが漏洩･改竄されないといった、"チップの完全性を"保証するセキュリティ(受動的セキュリティ)がある. 前者のセキュリティ強度は,暗号技術自体のセキュリティ強度によってその強度が理解できると共に,その強度の向上を図るのは比較的容易で,暗号方式の選択や鍵長の変更、鍵更新などによって実現できる.ところが後者の場合、その強度は大部分がチップ製造メーカの技術レベルに等しく,その把握が難しい.さらに,後者は前者を安全に実現するための基盤技術でもあり,現在の多くのICカードシステムにおいて,後者のセキュリティを拠り所として,機密情報(例:暗号鍵,署名鍵,電子マネー,電子証明書類等)をICチップ内のEEPROMに格納している. ところが最近ではその技術に対しても警鐘が鳴らされており[1][2],今後のICカードセキュリティにおいて注目すべき領域である.

2.2.データ機密保持性に関する脅威分析

ここで受動的セキュリティの中でも特に,**データ機密保持性**に着目して脅威分析を作成し,その脅威と対策について述べる(図１参照).図１が示すように, **データ機密保持性**を破る脅威が3つ存在し,それぞれに対策が講じられている.しかしこれらの脅威は"or**結合の脅威**"であるため,いずれか１つの対策に脆弱性が存在すれば,全体に影響しうる大きなリスクとなる.　従って,各々の脅威がどの程度のリスクであるか,または各対策がどの程度のセキュリティ強度であるかを認識する事が重要である.

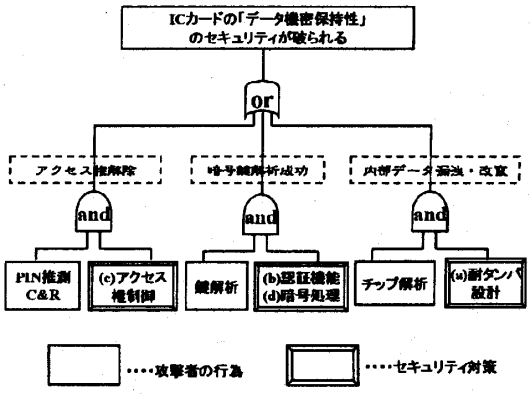

図１：脅威分析

2.3.各脅威のリスク

ここで各脅威のリスクについて述べる.

(c)**アクセス権制御**は一度 PIN が盗まれた時点で破られるレベルのセキュリティ強度であるが,通常は PIN の誤り回数許容制限を設けているので,PIN の Challenge & Repeat の攻撃に対するリスクを小さくしている.

(b)**認証機能**はカードと端末(又はセンタ）間で認証を行う機能であり(例:静的認証,動的認証), (d)**暗号処理機能**は暗号化･署名生成などを実現する処理機能である.これらに対する脅威は,プロトコル解析や,線形攻撃･差分攻撃などの鍵解読などがあるが,強力な暗号方式や長い鍵長の選択,鍵更新などによりリスクを小さくできる.

(a)**耐タンパ技術**は, ICチップの偽造,チップ解析,データ漏洩･改竄などの攻撃を困難にするための技術である.言い換えると、データの改竄やチップの偽造がされない事を「保証」するセキュリティと言える.これはICチップ製造メーカの技術力に大きく依存しており,現在はICカードのセキュリティに関して耐タンパセキュリティは安全であるという認識が世の中に浸透している.しかし,近年,RossAnderson[1]や,PaulKaucher[2]らによって信号解析,DPA,SPAなどのICチップの脆弱性が報告されており今後のチップ製造メーカの努力と共に,別な側面からの対策の必要性が言われている[3]. 従って,耐タンパ性の脆弱性をカバーする対策を"and結合"として導入する事が非常に重要である.

[1] (株)NTTデータ 技術開発本部 マルチメディア技術センタ ICカードシステム担当　担当：市原(ichihara@rd.nttdata.co.jp)

[2] OVD Kinegram Corp.,Advanced Research, Gubelstrasse 22,6301 Zug, Switzerland　tompkinw@ch.kinegaram.com

第３章　対策の検討

3.1.カード認証技術の搭載

前章で述べた耐タンパセキュリティは、暗黙に「保証」しているセキュリティであった.そこで、データの改竄やチップの偽造を能動的に「検知」する手法を取り入れる事によりセキュリティ向上が図れる。

そこで追加すべき対策方法の1つとして,偽造が容易でない事を前提としたようなカード認証用の付加技術(以後,"カード認証技術"と呼ぶ)をICカードに搭載する方法が考えられる. これらの技術では、改竄や偽造を能動的に「検査」する仕組みである.

最近のカード認証技術は様々であり、IDのタイプから分類すると、ホログラムや透かしのように存在有無で判定するもの（**singleID**）や、磁気ストライプのようにID番号の照合で判定するもの（**exclusiveID**）、また検査方法で分類すると、ホログラムのように人間の主観で判断するもの（目視確認型）や、磁気やステルスマークのように専用リーダによって偽造･変造やデータの改竄がされてないかを検査するもの（機械読取り型）がある.

3.2.検討

ここで,ICカードのセキュリティ向上策として搭載すべきカード認証技術は、「**データ改竄検知**」が実現できるという利点から、**exclusiveID**が望ましいと言える.さらに、高精度な「**偽造検知**」が実現できるという利点から**機械読取り型**のタイプ事が望ましいと言える.

但しここで重要なのは、従来の **exclusiveID＋機械読取り型**の技術の場合、チップを偽造するよりも、カード認証技術の偽造の方が容易であった点が弱点であった. つまり、図１の脅威分析図にこのような技術を追加する事が強力な対策とはならないのである.

第４章　セキュリティ向上策の提案

4.1.DiffractiveLinearCode の搭載

以上の事から我々は, セキュリティ向上策としてカードに搭載すべき技術として光学マーク技術"DiffractiveLinearCode"(以下DLCと呼ぶ)を用いる事にし、DLC搭載型ICカードを試作した(写真1参照).

DLCとは,高度な微細加工プロセスにより作られる光学マークであり,これを偽造する難しさは,現時点ではICチップの偽造困難性より高いレベルと言われている[4].またワンタイムロム型の記録媒体の為,その改竄は困難で、記録情報の読み取りは専用のリーダにより可能となる.

4.2.リスクの改善

つまりICカードにDLCを搭載する事は、脅威分析に対して"and結合"の対策を追加する事に等しく,ICカードセキュリティのリスクが改善される.

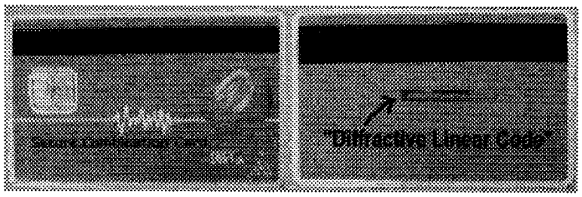

写真１：SC型ICカード

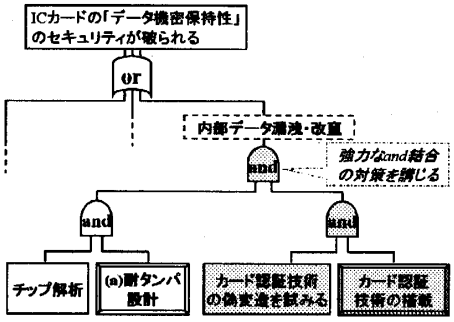

図２：脅威分析（改良版）

4.3.考察

例えば,発行の段階で,DLCとEEPROMに記録するデータに関係性を持たせ、運用の際にその関係性を検査する事で真贋判定が可能にする方式が考えられる.この場合,「**攻撃者が入手可能なDLCは,全て発行済みのものであり,思い通りの記録がされたDLCを入手する事は困難である**」という事を前提にしている.逆に言えば, 生DLCと書き込み装置は厳重に管理する必要がある.また,DLC技術自体の老朽化も当然のことながら考慮する必要があり,DLCなどの付加技術も技術的進歩が重要である.

第５節　まとめ

本論文では,ICカードのセキュリティ脅威分析により脆弱性を明示した上で,耐タンパ性への脅威対策についてのべ,DLCを利用した搭載型ICカードを実現例として示した.

参考資料

[1] "Tamper Resistance -a Cautionary Note" ,Ross Anderson.Markus Kuhn,*The Second USENIX Workshop on Electronic Commerce Proceedings*, 1996 ,pp1-11.

[2] "Differential Power Analysis",Paul Koucher,Joshua Jaffe,Benjamin Jun, http://www.cryptography.com

[3] ICカードの応用と情報セキュリティに関する調査研究報告書,(財)日本交通管理技術協会

[4]"Combination Gratings",ReneStaub,WayneR.Thompkin,Jean-Frederic Moser,pp292-299,SPIE Vo.2689