論文の内容の要旨

論文題目　A Study on Security Aspects of Mobile Communications-Authentication and End-User Security

（和訳　モバイルコミュニケーションにおける認証と利用者情報保護に関する安全性研究）

氏　名　ラーマン　モハマッド　グーラム

（本文）

ワイヤレスモバイルアプリケーションを利用するシステムでは、セキュリティはサーバにとってもクライアントにとっても非常に重要な要素である。コミュニケーションシステムがどのようなものであろうとこの問題に対する重要度は変わらないが、モバイルコミュニケーションに特有の条件や脆弱性が存在するため、特別な考慮が必要である。有線においては通信路を物理的に安全にすることも可能だが、ワイヤレスにおける通信データは潜在的な盗聴者によって容易に盗み見することができる。特にセキュリティ及びプライバシ保護はワイヤレスネットワークでは重要な問題である。しかしながら、ワイヤレスコミュニケーションにセキュリティ機能を追加する際にはいくつかの制限を考慮しなければならない。例えば、小さなパケットサイズ、狭い通信帯域、通信コストが高いこと、計算能力や記憶能力に関するリソースが限られていること、実時間に関する要求などがあげられる。

モバイル通信でセキュリティを達成するための一つの必要な機能として、システムの構成要素の認証及び権利の確認が挙げられる。ある特定の構成要素が信頼できるかはこの認証のプロセスの結果に依存する。セキュリティパラメータを定めることで、初期化手順が決定される。

これに適当な暗号アルゴリズムを適用することで要求されたセキュリティサービスを実現することができる。

最も重要なのは問題とは、認証のためのプロトコルや鍵管理方式を決めることである。この段階でのセキュリティ的に致命的な欠陥はそのセッションでのセキュリティを不確定なものにし、それに続くセッションのセキュリティに関しても不明確にする。

一方で認証やモバイルネットワーク特有の手続きにおいて、ユーザが特定できないようにすることも可能にすべきてある。このことは認証をおこなうことと矛盾しているように思えるかもしれない。我々が必要としていることとは、ユーザの匿名性を守りつつ、認証を行うことのできるメカニズムである。また、セッション鍵を交換することも一つの考慮すべき条項である。能動的及び受動的な攻撃者に対してセッション鍵を用いることによってユーザは、安全ではない通信路において通信を行うことができる。これらのすべての要求を一つのセキュリティプロトコルで満たすためにモバイルコミュニケーションにおける匿名認証鍵交換プロトコルが提案されている。本学位論文では、ユーザのローミングも考慮し、さらにドメイン内・ドメイン間両方での通信で用いるようなプロトコルを設計した。モバイルで使用されることを考慮し、本プロトコルはドメイン固有のセキュリティ及び、役割対象性も保持している。

モバイル構成要素は物理的アクセスコントロールデバイスとして、またセキュアなデータネットワークに侵入するために利用することもできる。このような点から、エンドユーザ認証も考慮すべき重要な要素である。本研究では、パスワード認証を導入することにより、エンドユーザ認証をおこなうことができるようにプロトコルが拡張されている。そして、end-to-endのユーザセキュリティとend-to-endの安全なセッションを提供するための鍵生成スキームも提案されている。

各構成要素間では、秘密鍵を共有していないため、end-to-endのセッションためのサーバベースの認証も提案されており、Deffie-Hellmanによる安全性により保証されている。
　提案された全てのプロトコルに関する安全性は、ワイヤレス環境において考えられる複数のインターリーブ攻撃に対して解析的に確認されている。