東北大学機関リポジトリ
TOUR
Tohoku University Repository
東北大学

A Monitoring Stubs-based Security Framework for Defending Against Cryptographic Threats

著者	FADLULLAH ZUBAIR M D.
号	16
学位授与機関	Tohoku University
学位授与番号	情博第513号
URL	http://hdl.handle.net/10097/59930

氏名（本籍地）	FADLULLAH ZUBAIR M D.（ファドゥルラ ズバイル モハマンド）
学位の種類	博　士（情報科学）
学位記番号	情　博　第　５１３　号
学位授与年月日	平成２３年　３月２５日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）応用情報科学専攻
学位論文題目	A Monitoring Stubs-based Security Framework for Defending Against Cryptographic Threats （暗号攻撃を防ぐためのモニタリングスタブを用いたセキュリティフレームワーク）
論文審査委員	（主査）東北大学教授　加藤　寧 東北大学教授　曽根　秀昭　　東北大学教授　木下　哲男

論文内容の要旨

近年のインターネットの発展とネットワークアプリケーションの普及に伴って顕在化してきた様々なセキュリティ脅威に対抗すべく，ここ数年で暗号技術や暗号化プロトコルの開発が急速に推し進められてきた．しかし，そのようにして新たに開発された暗号化プロトコルでさえ，しばしば攻撃の対象とされてきた．従来のMisuse-based and Anomaly-based Intrusion Detection Systems (IDSs)は，ペイロードの中身の観測と解析に過度に頼り過ぎるため，暗号化プロトコルを対象とした攻撃には効果がない．これに対し，本論文は暗号化プロトコルに対する攻撃に対抗するためのフレームワークであるDTRABに関する研究をまとめたものであり，本論文は全編7章からなる．

第1章では，暗号化プロトコルに対する攻撃に対抗するための侵入検知と防御の技術開発の重要性や，従来手法の問題点やその限界について述べている．

第2章では，SSH（Secure Shell），SSL（Secure Socket Layer），IPSec（IP Security）などの一般的に広く普及した暗号化プロトコルの機能や特徴について概観している．また，これらの暗号化プロトコルに対する様々な攻撃についても説明されており，現在のインターネットにおけるセキュリティ問題を理解する上で非常に有用である．

第3章では，提案するDTRABのアーキテクチャについて述べられている．DTRABは攻撃を検出するためのコンポーネントと攻撃を追跡するためのコンポーネントから構成される．MS（Monitoring Stub）と呼ばれるネットワーク監視モジュールをネットワーク上に分散配置することにより迅速な攻撃の検知並びに攻撃者の追跡までをも可能にする提案手法は，ネットワークに潜む脅威の元を取り除くことが可能であるという点において，その優位性が高く評価できる．

第4章では，DTRABにおける攻撃検知の方法について詳しく述べられている．MSにおいて暗号化プロトコルの異常な動作を検出する方法や，MSにおいてパケットの詳細情報を観測することなく攻撃検知に必要な特徴を抽出する方法が示されている．さらに，実験ではDTRABによって様々な暗号化プロトコルに対する様々な攻撃を比較的高速かつ高精度に検知できることが確認されており，評価に値する．

第5章では，DTRABにおける攻撃追跡の方法について詳しく述べられている．ネットワーク上に分散配置された各MSが保持する暗号化トラヒックフローに関する攻撃特徴情報が相互に関連付けられることによって追跡が可能になる．ネットワークの合流地点における提案手法の性能や，さらなる性能向上のための追跡方法の最適な拡張法などについて検討されている点は評価に値する．

第6章では，MSを利用したDTRAB技術の応用について述べられている．MSによる異常度の報告は，システムのセキュリティサービス品質の改善を促すために活用できると論じている．

第7章は結論である．

本論文は，新たなセキュリティ脅威から暗号化プロトコルを守るとともに，その脅威を取り除くために攻撃者の特定を行うことを可能にするフレームワークを与えるものであり，応用情報科学並びに情報通信技術の発展に寄与するところが少なくない．

よって，本論文は博士（情報科学）の学位論文として合格と認める．

論文審査結果の要旨

近年のインターネットの発展とネットワークアプリケーションの普及に伴って顕在化してきた様々なセキュリティ脅威に対抗すべく，ここ数年で暗号技術や暗号化プロトコルの開発が急速に推し進められてきた．しかし，そのようにして新たに開発された暗号化プロトコルでさえ，しばしば攻撃の対象とされてきた．従来の Misuse-based and Anomaly-based Intrusion Detection Systems (IDSs)は，ペイロードの中身の観測と解析に頼り過ぎるため，暗号化プロトコルを対象とした攻撃には効果がない．これに対し，本論文は暗号化プロトコルに対する攻撃に対抗するためのフレームワークである DTRAB（Detection and TRAceBack）に関する研究をまとめたものであり，本論文は全編 7 章からなる．

第 1 章では，暗号化プロトコルに対する攻撃に対抗するための侵入検知と防御の技術開発の重要性や，従来手法の問題点やその限界について述べている．

第 2 章では，SSH，SSL，IPSec などの一般的に広く普及した暗号化プロトコルの機能や特徴について概観している．また，これらの暗号化プロトコルに対する様々な攻撃についても説明されており，現在のインターネットにおけるセキュリティ問題を理解する上で非常に有用である．

第 3 章では，提案する DTRAB のアーキテクチャについて述べている．DTRAB は攻撃を検出するためのコンポーネントと攻撃を追跡するためのコンポーネントから構成される．MS（Monitoring Stub）と呼ばれるネットワーク監視モジュールをネットワーク上に分散配置することにより攻撃の検知から攻撃者の追跡まで可能にする提案手法は，ネットワークに潜む脅威の元を取り除くことが可能であるという点において，その優位性が高く評価できる．

第 4 章では，DTRAB における攻撃検知の方法について詳しく述べている．MS において暗号化プロトコルの異常な動作を検出する方法，及び MS においてパケットの詳細情報を観測することなく攻撃検知に必要な特徴を抽出する方法を示している．さらに，実験では DTRAB によって様々な暗号化プロトコルに対する攻撃を比較的高速かつ高精度に検知できることを確認しており，重要な成果である．

第 5 章では，DTRAB における攻撃追跡の方法について詳しく述べている．ネットワーク上に分散配置された各 MS が保持する暗号化トラヒックフローに関する攻撃特徴情報が相互に関連付けられることによって追跡が可能になる．ネットワークの合流地点における提案手法の性能や，さらなる性能向上のための追跡方法の最適な拡張法などについて検討している点は評価に値する．

第 6 章では，MS を利用した DTRAB 技術の応用について述べられている．MS による異常度の報告は，システムのセキュリティサービス品質の改善を促すために活用できると論じている．

第 7 章は結論である．

本論文は，新たなセキュリティ脅威から暗号化プロトコルを守るとともに，その脅威を取り除くために攻撃者の特定を行うことを可能にするフレームワークを与えるものであり，応用情報科学並びに情報通信技術の発展に寄与するところが少なくない．

よって，本論文は博士（情報科学）の学位論文として合格と認める．