発表概要

ユーザ入力の構文木解析によるSQLインジェクション攻撃防御法

金子佳樹[†] 岩崎英哉[††]

近年，データベースを用いたWebアプリケーションの増加とともに，Webアプリケーションを対象とした攻撃手法も増えている．ユーザ入力にSQLコマンドを埋め込んで，本来意図していないSQL文で問合せを行わせることにより，データベースを不正に操作するSQLインジェクションもその1つである．本研究では，期待されるユーザ入力は，SQL文法の非終端記号となっているという点に着目し，ユーザ入力をその非終端記号として構文解析し，解析に成功した入力に対してのみ，実際のデータベース操作を許すことにより，SQLインジェクション攻撃を防御する方法を提案する．さらに，本提案機構を，Webクライアントと Webアプリケーションを運用する Webサーバの間に設置して実装し，その有効性を確認した．

Protection against SQL Injection Attacks Using Syntax Tree Analysis of User's Input

Yoshiki Kaneko[†] and Hideya Iwasaki[††]

Recently, as web applications with databases increases, attacks on these web applications are increasing. SQL injection is one of such attacks, which illegally accesses databases by giving fragments of SQL commands within the user 's input and making the web application issue unexpected queries to the database. Based on the fact that an expected input corresponds to a nonterminal symbol of SQL grammar, we propose a new protection method against SQL injection which parses user's input as the nonterminal symbol and rejects such input that cannot be parsed. Experimental results demonstrates that our prototype works well in protecting well-known SQL injection attacks.

（平成18年6月1日発表）

† 電気通信大学大学院情報工学専攻
Department of Computer Science, Graduate School of Electro-Communications, The University of Electro-Communications
†† 電気通信大学情報工学科
Department of Computer Science, The University of Electro-Communications