発表概要

データベース向けアクセス制御の機能強化による SQL インジェクション対策

後藤 久美子[†] 千葉 雄司[††] 土居 範久[†]

電子商取引サイトなど，データベースと連携した Web アプリケーションを狙う攻撃手段に SQL インジェクションがある．SQL インジェクションでは，Web アプリケーションに悪意のある入力を与えることで，データベースに対して不正な問合わせを実行させる．データベースが提供する既存のアクセス制御機能は，SQL インジェクションに対する防御手段として，必ずしも有効でない．なぜなら，既存のアクセス制御がユーザによる想定外のデータの参照や破壊を防ぐものであるのに対し，SQL インジェクションの結果として生じる不正な問合わせでは，必ずしも想定外のデータを参照しないからである．そこで，本発表では，SQL インジェクション対策を目的として，データベースのアクセス制御機能を強化することを提案する．具体的には，データベース上に，個々のユーザに対して発行を許可する問合わせ文のフォーマットを準備し，フォーマットに合致する問合わせに限り実行を許可する．発表では SPECjAppServer2002 による性能評価の結果も示す．

Enhancement of the Access Control for Database against SQL Injections

Kumiko Goto,[†] Yuji Chiba[††] and Norihisa Doi[†]

SQL injection is a mean to attack web applications that execute queries to the database. The attack is issued as follows: A cracker gives malicious input to the web application, and the web application use the input to generates an invalid query statement and execute it. Then, the database may return unexpected result that makes web application do errorneous action. Access control features of the databases so far may not be good protection against SQL injections: The access control prevents users from reference of unexpected data, but the invalid query statement used in SQL injection may not refer such data. This presentation shows an enhancement on the access control against SQL injection. Our access control puts a table in the database and store formats of SQL statements that clients can execute, and when a client executes a query, it is matched against the formats to check if its execution is allowed. The presentation shows results of SPECjAppServer2002.

（平成 17 年 3 月 17 日発表）

† 中央大学理工学部情報工学科
Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University
†† 中央大学研究開発機構
Research and Development Initiative, Chuo University