≪「報告書詳細版」は巻末の付録USBメモリに収録しています≫

第10部

ウェブアプリケーションのセキュリティ技術の研究(概要版)

Gregory Blanc、宮本 大輔、門林 雄基

SWAN (Security for Web 2.0 Application) WGでは、悪意あるウェブサイトの動向を観測し検討している。ウェブを介した攻撃には、その攻撃空間が広いという特徴があり、本研究グループはその広い特性に対応した研究を行っている。

今年度も昨年度に引き続き、多くのWIDEプロジェクトメンバーが参加している日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発(NECOMA)とSWAN WGは連携した研究を行い、HTTPSを用いたフィッシングサイトにおけるX.509証明書の特徴分析、ならびに見た目分析によるフィッシングサイト検知プラグインの研究開発を実施した。

概要は以下に示す。

詳細は付録USBのmensah_badgers15_authorcr.pdfを参照していただきたい。

- X.509証明書の特徴分析: SSL/TLSハンドシェイクにおいて提示されるX.509サーバ証明書の記載事項 (Country, Organization, Organizational Unit, State) を分析することで、フィッシングサイトと正当なウェブサイトを峻別することを試みた。これは、フィッシングサイトのほうが正当なウェブサイトに対して証明書への記載事項に欠落や不正確な記載 (MyCompany, SomeState 等) が多いであろうという仮説に基づくものであったが、分析の結果、正当なウェブサイトのほうが証明書に不備が多いことが判明した。

- 見た目分析によるフィッシングサイト検知: 正当なウェブサイトに乗っ取られ、その一部にフィッシングサイトが仕掛けられた場合、フィッシングに用いられるページと他ページでは見た目が大きく異なると考えられる。本研究ではこのようなフィッシングサイト(我々の分類ではHacked Domainと呼んでいる)を検知するため、Firefoxプラグインを開発し、ウェブサイト閲覧時にnode.jsサーバにおいてperceptual hashing [54]を用いた見た目分析を行い、Hacked Domain型のフィッシングサイトを検知するシステムAJNAを開発した [55]。

SWAN WGでは引き続き悪意あるウェブサイト全般について多面的な研究を行っていく。研究成果は引き続きWIDE研究会および学会発表を通じて行い、ソフトウェアなどの成果物は必要に応じて公開を検討する。