Title	スマートフォンゲームにおける脆弱性対策機構の設計及び構築
Sub Title	Analysis and measures in security aspects for smartphone games
Author	橋本, 真太郎(Hashimoto, Shintaro) 加藤, 朗(Kato, Akira)
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2015
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2015年度メディアデザイン学 第466号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002015-0466

修士論文 2015年度（平成27年度）

スマートフォンゲームにおける
脆弱性対策機構の設計及び構築

慶應義塾大学大学院
メディアデザイン研究科

橋本　真太郎

本論文は慶應義塾大学大学院メディアデザイン研究科に
修士 (メディアデザイン学) 授与の要件として提出した修士論文である。

橋本　真太郎

審査委員：

加藤 朗 教授　　（主査）
砂原 秀樹 教授　（副査）
大川 恵子 教授　（副査）

修士論文 2015年度（平成27年度）

スマートフォンゲームにおける
脆弱性対策機構の設計及び構築

カテゴリー：サイエンス / エンジニアリング

論文要旨

近年，スマートフォンが目覚ましく普及するとともに，スマートフォンアプリケーションを狙ったサイバー攻撃の数が急増し，利用者はあまねく脅威にさらされている．主に，その攻撃対象として，SNSやオンラインバンキングなどのサービスが選ばれることが多く，ゲームが選択されることは稀である．しかし，ゲームは高い応答性を求めるあまり，セキュリティを疎かにしている可能性が高く，また，他のスマートフォンアプリケーションの中でも，ゲームは市場の占有率及び成長率が高いため，今後，サイバー攻撃の対象となる公算が大きいと考えられる．そのため，本研究では，iOSにおける市場のスマートフォンゲームに対してセキュリティ調査を行った．その結果，15本のうち14本ものゲームに，中間者攻撃を可能とする何らかの脆弱性が存在することを確認できた．また，調査を行った一部のゲームを対象に，アプリ内課金を操作する攻撃を行った結果，他者の課金を奪取できてしまうことが確認できた．この攻撃は同一Wi-Fi上に対象が存在するだけで可能なため，公共Wi-Fiの普及なども鑑み，将来的な脅威に繋がると考えられた．そこで，本研究では，この調査結果に基づき，脆弱性を効果的に対策するための3つ機構を設計し構築した．各機構には，脆弱性を対策するプログラム，脆弱性を調査するツール，脆弱性の周知を目的としたサイトなどが含まれている．

キーワード：

セキュリティ, ネットワーク, 中間者攻撃,　スマートフォンゲーム, アプリ内課金

慶應義塾大学大学院 メディアデザイン研究科

橋本　真太郎

Abstract of Master's Thesis of Academic Year 2015

Analysis and Measures in Security Aspects for Smartphone Games

Category: Science / Engineering

Summary

Smartphones become inevitable tool for everybody. A number of applications have been installed on every smartphone and they are used in daily basis. It is reported that cyber attacks targeting smartphones and their applications have been increasing rapidly. In many cases, services such as SNS and online banking are the primary, while it is rare at this moment that game applications are targeted. In order to focus on their realtime requirements, security on smartphone game applications may not be seriously considered. It is afraid that game applications will be target of cyber attacks in near future.

In this thesis, several smartphone game applications on iOS are analyzed. 14 out of 15 of them including popular titles have security vulnerabilities, which can be easily mitigated by verifying the gaming servers' certificates in SSL/TLS communications. It is demonstrated that the communication from the victim iOS devices running gaming software can be intercepted via man-in-the-middle attack method. In this context, credit to be added to the corresponding user can be stolen, and successfully added to the attacker's account. This attack can easily be implemented in public Wi-Fi environment, which becomes popular in these years.

This research also proposes a system for game programmers to detect possible vulnerabilities on the fly. A tool to investigate vulnerability is implemented based on the research result as well.

Keywords:

Security, Network, Man-In-The-Middle Attack, Smartphone game, In-App Purchase

Graduate School of Media Design, Keio University

Shintaro Hashimoto