平成２６年１月２０日

学 位 論 文 の 審 査 要 旨

学位論文申請者氏名：Ahmad Bazzi

論　文　題　目：“Advancing Intrusion Detection and Prevention Systems through the Use of Computer Virtualization”
（計算機仮想化を用いた先進的な侵入検知及び防止システム）

論文の概要及び判定理由

Ahmad Bazzi 君の研究は、コンピュータネットワークのセキュリティを向上させるため侵入検知システム及び侵入防止システムの研究開発に関するものである。特に、セキュリティ上の脆弱性をついた攻撃は、防御態勢が整わないうちに攻撃を仕掛けてくるため有効な対策をたてることが困難である。そこで、新しいタイプの攻撃でも素早く検知して防ぐことが求められている。

同君は、計算機仮想化（Computer Virtualization）を活用してゼロデイ攻撃等の新しいタイプの攻撃に対応できる仕組みを提案し評価した。本研究では、サンドボックス（Sandbox）における挙動を専門家の手に解析をゆだねるのではなく、仮想機械上でダイナミック解析を行いその解析結果を自動的に解釈し、マルウエアを検出する手法を提案し評価した点に特徴がある。次に、ファイアウォールを仮想機械上に作成し日頃使用されている動作環境の下で評価した。仮想機械を用いて実現したファイアウォールのオーバーヘッドについて、帯域幅、パケットサイズ、ＯＳを変えて評価した。適切なＣＰＵ数とメモリ容量を確保すれば十分満足できる応答速度が達成できることを示した。さらに、スマート端末のセキュリティ強化のために仮想機械を用いる手法を提案し、中間者攻撃（Man in the Middle Attack）を防ぐ手法について提案した。

以上のように、本研究で開発された侵入検知及び防止システムは、新しいタイプの攻撃でも検知して防ぐことができるため、セキュリティの向上に寄与するものであり、博士（工学）の学位に値するものと判定した。

審査年月日　平成２６年１月２０日

審査委員

主査	群馬大学理工学研究院	教　授	横尾　英俊	印
副査	群馬大学理工学研究院	准教授	河西　憲一	印
副査	群馬大学理工学研究院	准教授	山本　潮	印
副査	群馬大学理工学研究院	准教授	加藤　毅	印
副査	群馬大学理工学研究院	教　授	小野里　好邦	印

関連論文

1 著者名	Ahmad Bazzi and Yoshikuni Onozato,
論文題目	"Feasibility Study of Security Virtual Appliances for Personal Computing", （パーソナル計算用仮想セキュリティ装置の実現可能性）
雑誌名	Journal of Information Processing, Vol.19,pp.378-388, July (2011).
2 著者名	Ahmad Bazzi and Yoshikuni Onozato,
論文題目	"Automatic Detection of Malicious PDF Files Using Dynamic Analysis", （ダイナミック解析を用いた悪質な PDF ファイルの自動検出）
雑誌名	JSST 2013 International Conference on Simulation Technology, OS3:Soft Computing, Sept.11-13, Meiji University Surugadai Campus (2013).
3 著者名	Ahmad Bazzi and Yoshikuni Onozato,
論文題目	"IDS for Detecting Malicious Non-Executable Files Using Dynamic Analysis", （ダイナミック解析を用いた悪質な非実行型ファイル検出可能な IDS）
雑誌名	The 15th Asia-Pacific Network Operations and Management Symposium (APNOMS2013), Poster Session1: p1-05-116390.pdf, 25-27 September 2013, International Conference Center Hiroshima, Japan (2013).

参考論文

1 著者名	Ahmad Bazzi, Yoshikuni Onozato, Ruttikorn Varakulsiripunth and Sakchai Thipchaksurat
論文題目	"Server Consolidation and its Effect on Performance in Common Hardware" （一般のハードウエアを用いたサーバ統合とその評価）
雑誌名	International symposium on technology for Sustainability

(ISTS-2012), pp.220-223, November21-24,Swissotel Le Concorde, Bangkok, Thailand (2012).

２著者名　　Ahmad Bazzi and Yoshikuni Onozato and　Yuta Kiriyama,

論文題目　"Privacy-Aware Gateway to Prevent Privacy Leaks from Smart Devices",
（スマートデバイスからの個人情報漏洩を防ぐためのプライバシーに配慮したゲートウェイ）

雑誌名　　第 21 回 マルチメディア通信と分散処理ワークショップ(DPSWS2013), December 4-6, 2013, Kusatsu, Gunma-ken, Japan (2013).