論 文 内 容 の 要 旨

博士論文題目　Study on High Interaction Client Honeypot for Infiltrative Intrusion Detection

氏　　名　　秋山　満昭

（論文内容の要旨）

We studied a honeypot that is a decoy system to conduct infiltrative observation for malware infection in order to provide useful information for protection/mitigation scheme. According to the attack model and adversarial techniques of recent malware infection, we enumerated basic requirements for design and implementation as follows: precise detection, inspection performance, information collection, safeguarding, camouflaging, and seed URL selection. For precise detection, we proposed stepwise-detection based on three exploitation phases in order to broaden coverage of discovering various patterns of known/unknown exploitation. For collecting precise information, our honeypot coordinates network-based events and host-based events to identify complex relationship of web contents. For camouflaging, our honeypot uses high interaction system and a network environment of IP address randomization. For achieving high-inspection performance and safeguarding, we proposed two approaches: 1) multi honeypot-agent, and 2) multi browser-process. In particular, the second approach is novel sandbox mechanism for process multiplication on single honeypot OS. Our proposed sandbox enables process-level execution environment isolation. For seed URL election, we proposed URL neighborhood lookup to discover potential malicious URLs in the neighborhood of a malicious URL for blacklist candidates. Our developed client honeypot, called Marionette, enables us to conduct stable and sustainable observation for long period and gather the properties of adversarial strategy: 1) Hosting structure of malicious website, 2) Aggregated malware distribution network, and 3) Unknown malicious URLs neighboring known one. Obtained knowledge can accelerate countermeasures of malware infection.

氏　名	秋山　満昭

（論文審査結果の要旨）

本博士論文では、プログラムの脆弱性に起因する Web 経由でのマルウェア感染（ドライブバイダウンロード攻撃）に対して、攻撃検知と情報収集を目的として能動的に動作する「おとりシステム」であるクライアントハニーポットの研究を行っている。ドライブバイダウンロードの攻撃モデルおよび用いられる耐解析手法を列挙し、これらに基づいてクライアントハニーポットに求められる要求条件である“検知性能”、“情報収集性能”、“巡回性能”、“安全性”、“偽装性”、“検査対象選定”を明らかにしている。攻撃を検知するには、Web 空間の中から検査対象（URL）を選定し、その対象を検査することで悪性かどうかを判別する。検査対象の選定は、悪性 URL の近隣性に基づいて既知の悪性 URL から未知の悪性 URL を検査対象候補として列挙する近隣探索手法を提案しており、悪性 URL の発見効率の向上に寄与している。検査対象が悪性かどうかを判別するための提案手法は、攻撃を段階的に検知することで、従来手法における偽陰性であった攻撃の失敗についても検知可能にしている。これにより偽陽性を排除しつつ偽陰性の減少に貢献し、また未知の攻撃にも追従可能にしている。OS 上で複数のプロセスを仮想的に隔離して動作させる提案手法であるプロセスサンドボックスは、同一 OS 上で複数のハニーポットインスタンスの立ち上げに成功し、飛躍的な巡回性能向上を達成した。本手法はプロセスレベルの動作制御が可能なため、攻撃を受けた後のマルウェア起動時に動作を停止させることで、攻撃情報の収集を阻害することなく安全性を確保している。ハニーポット環境の偽装性については、実被害端末と同等のホスト環境を用いることと、動作する IP アドレス空間のランダム化を行うことでハニーポット環境の特定を困難にさせる方法を用いている。これらの手法を統合的に実装したクライアントハニーポットは、Web 空間における悪性サイトの観測において有効に動作することを長期間の実験により証明している。これらの提案手法と実験結果は３件の国際会議論文と３件の論文誌論文でまとめられており、理論的な面でも有効性は認められている。以上により、本博士論文は研究内容について新規性並びに有効性があることが認められ、博士（工学）の学位を授与するにあたって十分な内容であると認められる。

氏　名	秋山　満昭

（最終試験結果の要旨）

本博士論文では、プログラムの脆弱性に起因するWeb経由でのマルウェア感染（ドライブバイダウンロード攻撃）に対して、攻撃検知と情報収集を目的として能動的に動作する「おとりシステム」であるクライアントハニーポットの研究を行っている。ドライブバイダウンロードの攻撃モデルおよび用いられる耐解析手法を列挙し、これらに基づいてクライアントハニーポットに求められる要求条件である“検知性能”、“情報収集性能”、“巡回性能”、“安全性”、“偽装性”、“検査対象選定”を明らかにした上で、手法の提案と有効性の評価を行っている。本年１月に行われた公聴会では、博士論文草稿に対して下記の４点について指摘が有った。審査提出された博士論文では全ての項目について改善が見られた。以下に最終審査の結果概要を示す。（１）攻撃検知手法の説明が不足しているとの指摘については、脆弱性が存在する関数に対して処理を一時的に迂回するための手順と、脆弱性発症条件を判別した後に本来の処理に復帰させることで攻撃を停止することなく透過的に検知する手順に関する記述が論文で明記された。（２）攻撃の観測空間と判別に関する説明が不明瞭であり、また誤検知・見逃しに関する説明が不足しているとの指摘があった。これについて、攻撃を検知するにはWeb空間から検査対象を選定し、選定した検査対象が悪性であることを判別する手順からなることが論文中で明記された。また、攻撃の各段階における攻撃検知手法は誤検知を含まない方法であり、またこれらを組み合わせることで見逃しの低減に貢献しているという説明が追記されている。（３）プラットフォームと実装に関する指摘については、まず最新のプラットフォームにおいてもドライブバイダウンロード攻撃が成功することから本研究が対象とする攻撃モデルの継続性を説明し、次に最新のプラットフォームへの本手法の適用に関する実現可能性についての説明が追加された。（４）本手法の活用方法に関する説明が不足しているとの指摘については、本手法を取り巻くステークホルダと本手法の取得情報に基づいた対策について列挙し論文に明記した。また、ハニーポットで得られる信頼性の高い一連の侵入の根拠情報は、OpenIOCやCybOXなどのセキュリティ情報表現形式との親和性が高いことを論文に明記した。以上により、主要な指摘項目の４点について充分な改善が見られ、本博士論文は博士（工学）の学位を授与するのに充分な内容であり、独立した研究者として研究開発を継続するに充分な素養を備えていると判断できる。

なお、2013年2月20日、全審査委員により、学位申請者に対して論文内容及び関連事項についての試問を行い、充分な知識を持つ者と認められたので合格と判定した。