卒業論文 2018 年度 (平成 30 年)

低対話型 Honeypot のコマンド拡張による収集ログの変化の計測

慶應義塾大学 総合政策学部
菅藤 佑太

卒業論文要旨 - 2018 年度 (平成 30 年度)

低対話型 Honeypot のコマンド拡張による 収集ログの変化の計測

PC の普及や IoT デバイスのシステム高度化により，高度な処理系を組むことが可能になった．これによりデバイス上に Linux 系などの OS が搭載された機器が広く人々に使われるようになった．また，Linux 系 OS にリモートログインする手法として SSH がある．これを用いて不正に侵入する攻撃が行われている．侵入された際に侵入者がどのような挙動をしているのかを知る手段として，Honeypot がある．Honeypot は SSH で侵入しやすいような環境を作ることで，侵入者にログイン試行に成功したと検知させ，その際に実行したコマンドのログを収集するものである．また現在では Shell の挙動をエミュレートした Honeypot が広く使用されており，この Honeypot は実行できるコマンドが少ない実装になっている．そのため Honeypot への侵入者に侵入先が Honeypot であると検知されてしまう．そこで事前実験では Honeypot のコマンドを拡張し，拡張をしていない Honeypot とコマンドの拡張をした Honeypot で侵入ログを収集した．収集したログを確率的な算出方法を使用することで比較した結果，より多くの侵入者のコマンド実行ログのパターンを取得できることを示した．本研究ではコマンドを拡張した Honeypot の侵入ログがどれほど実際の OS に不正な SSH の侵入をされた際の侵入ログの近似を試みた．評価として，拡張をしていない Honeypot とコマンドの拡張をした Honeypot と，さらに実際の OS を使用した Honeypot で侵入ログを収集し，比較を行なった．この 3 つの侵入ログを自然言語処理の意味解析を用い，一セッションにおけるコマンドログの意味をベクトル空間上に表現することで，拡張した Honeypot で収集した侵入ログが，拡張をしていない Honeypot で収集した侵入ログよりも，一般的な UNIX ユーザーの実行するコマンドログから離れることが明らかとなった．

キーワード:
1. 自然言語処理，2. 意味解析，3. Honeypot，4. SSH

慶應義塾大学 総合政策学部
菅藤 佑太