総合理工学研究科 Graduate School of Science and Technology 情報理工学コース Information Science and Technology



統計解析による攻撃検知に関する研究 トラフィック解析の攻撃検知への適用

Attack detection based on statistical analysis

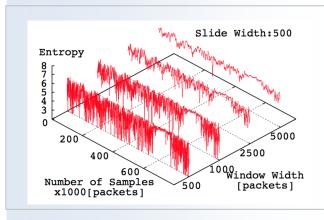
Application of the traffic analysis to attack detection

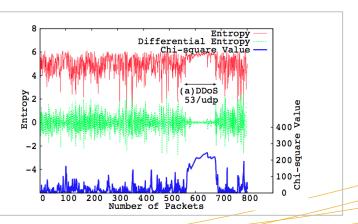
教授 中嶋 卓雄 Prof. Takuo Nakashima

Keyword : 攻撃検知・トラフィック解析・統計解析 Attack detection・Traffic analysis・Statistical analysis

近年、個人のみならず企業や国家機関にたいし ても DoS/DDosS 攻撃などのサイバー攻撃が頻繁に 行われています。ウィルスなどの固有な特徴を検 出する研究は従来から行われていますが、新しい ウィルスに瞬時に対応できないのが現状です。本 研究では、特定の組織に対して、その前兆となる 動作を監視し、その組織への全トラフィックを統 計的に解析することにより、攻撃トラフィックを 検知するシステムを開発しています。統計量とし ては、エントロピーおよび χ²値検定を利用してい ます。エントロピーによる検出では、エントロピ ーがバラツキの度合いを計測する指標であること から、エントロピーが通常より小さく、または大 きく変動することにより、DoS または DDoS として 検出することができます。統計量の計算は、パタ ーンマッチング手法と比較して計算時間が非常に 短く, 早期に組織内のすべての攻撃を発見できる メリットがあります。

In recent years, DoS/DDoS attacks widely servers. companies occurred to and government sites. Researches detection comparing the specified features are conducted in these days. New viruses, however, are hardly detected within short period. In this research, we observe the pre-attacking behavior and analyze incoming traffic using statistical methods for the specified organization. These methods adopt the entropy method and chi-square method. Variation of entropy values is utilized in entropy method. If entropy value is lower than normal value, attacks seem to be DoS attacks. On the other hand, if entropy value is higher than the normal value, attacks seem to be DDoS attacks. The calculation times of these statistical methods is very short compared to the pattern matching method leading to the quick detection. These methods have the merit to find all incoming attacks of local organization.





◆リンクページ(Link): http://www.u-tokai.ac.jp/graduate/science_and_technology/academic/index.html

◆電子メール (address): taku@ktmail.tokai-u.jp

