時間管理による SYN cookies の改良提案

Modified SYN cookies Using Time Management

情報セキュリティ大学院大学

武藤　展敬

要旨

近年，ネットワークは急速に普及し必要不可欠なインフラになってきている．DoS 攻撃は，そのインフラに対して多大な影響を与える攻撃である．DoS 攻撃の中でも SYN Flood 攻撃は，多数攻撃事例が報告されている DoS 攻撃の一種類である．この攻撃に対して効果がある対策として，SYN cookies がある．SYN cookies はキャッシュレスで相手が特定できるという利点があるが，いきなり ACK パケットを送信されコネクションが確立してしまう危険性がある．本研究では，攻撃者がネットワーク上を流れる SYN-ACK パケットを観測し，サーバを攻撃する想定を元に考え，ACK パケットを大量に受けいれる問題の検出・対処に関して改良する理論検討を実施した。改良したことにより ACK パケットの返答が多くなってきた段階で SYN cookies の振る舞いを変更し、SYN-ACK パケットの回答量を抑える提案が有効であるという見通しを得た．

Abstract

The communication for file transfer has increased rapidly in recent years on the telecommunication networks and become an indispensable application service for businesses. DoS attack is one of the network security attacks that give a serious influence on the file transfer communication. Among the DoS attacks, the SYN Flood is the attack observed most frequently. To counter the SYN Flood, the use of SYN cookies was proposed. The proposed scheme on the SYN cookies can determine sources of the clients without cash data of the concerned SYN cookies. However, it has the risk that the SYN cookies as the sudden ACK would be sent to establish a packet connection. In this study, attackers monitor the SYN-ACK packets through the network. Attackers execute the attack that sends the server a large amount of observed ACK packets. The improvement was examined about the detection of correspondence and the problem to a large amount of ACK packet. The prospect with an effective proposal to compare the improvements of SYN cookies, and to suppress the amount of the answer of the SYN-ACK packet was obtained.