シンボリック実行やプログラム解析を用いたSSRF検出

SSRF detection using symbolic execution and program analysis

坂本圭・大久保研究室・情報セキュリティ大学院大学

背景：
SSRFはクラウドサービスへの脅威度の高いな脆弱性であるが、攻撃手法の多様性により検出及び防御が困難である。したがって、SSRF脆弱性の体系的な分析及び効果的な検出方法が求められている。

手法：
SSRF脆弱性を発動させるシンク関数へのパスをシンボリック実行により経路を探索し、ファジング、実際にペイロードを流して脆弱性の発見を試みる

課題：
シンボリック実行によるパス爆発への対処