検索エンジンによる Covert Channel の検出

木下研究室　　久保直也　(200602824)

1　はじめに

近年、ネットワークの巨大化によりアクセス権限も複雑に絡み合っている。ネットワーク内では不正な情報経路が発生し、情報流出の危険性が増大してしまっている。このような情報流出経路の解析法として Covert Channel 解析がある。従来のように把握したコミュニティの ACL(Access Control List) のみを用いた Covert Channel の解析だけでは検出できないアクセス権の矛盾が存在する場合がある。そこで検索エンジンで得られた情報にオントロジーを用いたセマンティックな解析手法を適用することで ACL の矛盾や経路を効率よく見つけることを目的とする。

2　基礎知識

2.1　Covert Channel

Cvert Channel とは，ある object に権限がないのにも関わらず意図しない経路から情報が流出してしまう現象の事を言う。図 1 の場合、object とはアクセスされる客体（データなど）の事をいい、subject とは object にアクセスする主体（ユーザーなど）である。R は read 権、W は write 権、φは権限なしの事である。矢印の流れで Subject3 が本来読めないはずの Object1 を読めてしまう。まず内的な ACL では S3 は O1 を読むことができない。しかし外的要因を考慮した場合 O1 を読み書きできる S2 が O8 にコピペしてしまうことで Sothers に読まれてしまう。S それをクローラが収集しそれをサーチすることでもしくは 08 から直接 S3 は O1 を読むことができるようになってしまう。

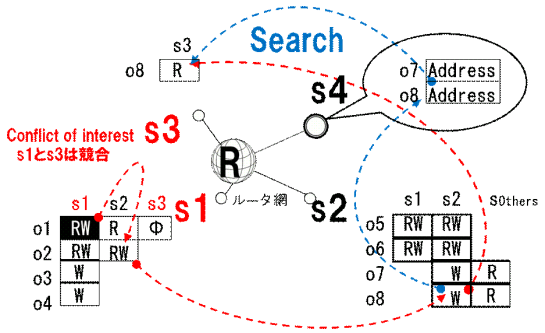

図 1: Covert Channel

クローラで収集した情報は形態素解析・構文解析を行う。形態素解析構文解析を行うことで検索の精度を上げることができる。オントロジーを用いたセマンティックな解析を行うために RDF 化する。RDF 化することで意味まで考慮したマッチングを行うことができる。

2.2　形態素解析　構文解析

形態素解析では単語分割、品詞タグ付けを行う。単語分割とは、文中の単語を同定する作業である。例えば子供｜の｜体力｜低下と単語分割される。品詞タグ付けとは各単語の品詞を同定する作業である。

構文解析では主に係り受けを解析する。先程の例では子供→体力　体力→低下と表される。

3　Covert Channel の検出

検索エンジンを用いた Covert Channel の検出手順を以下に示す。

1. クローラで収集された情報を形態素解析・構文解析を行う

2. 形態素解析・構文解析された情報を述語論理化、RDF 化する。

3.RDF で検索された処理結果とオントロジー DB から、外的要因を考慮した ACL を解析エンジンを用い導く

以上により、内的な ACL では読めないことになっている情報が Web 検索の結果を解析して得られた外的要因まで考慮した実質的な ACL では読めると言ったような矛盾を見つけることができる。その矛盾と経路の例を図 2 に示す。

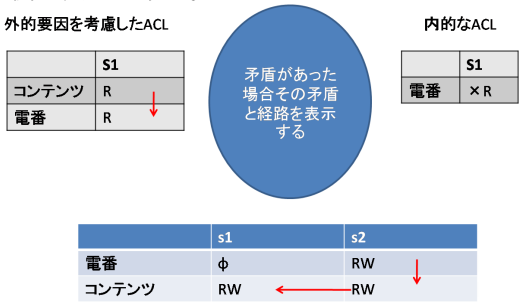

図 2: Covert Channel の検出

4　まとめ

本稿では検索エンジンを用いた Covert Channel の検出方法を提案した。これにより従来のように把握したコミュニティの ACL のみを用いた Covert Channel の解析だけでは検出できないアクセス権の矛盾を見つけることが可能になった。