推移閉包アルゴリズムを用いたCovert Channel検出

木下研究室　　中村 峻生 (200803007)

1　はじめに

近年，ネットワーク上の情報リソースにアクセスできる者を設定する，アクセス制御（Access Control）技術が発展してきた．これによってネットワーク上の情報リソースは，権限を持たない者による盗聴などの脅威から保護されている．しかし，covert channelと呼ばれるアクセス制御の脆弱性によって情報漏洩が起きる可能性がある．セキュリティの観点から，covert channelの検出技術の発展が望まれている．本稿では，covert channel検出問題を効率的に解くアルゴリズムを提案をする．

2　covert channel検出

アクセスされる対象となる情報リソースをobject(客体)と呼び，その集合をOで表す．objectにアクセスする者をsubject(主体)と呼び，その集合をSで表す．あるsubject $y \in S$があるobject $x \in O$にread権限を持つときxRyと書き，write権限を持つとき，yWxと書く．全てのアクセス権限を書いたものをACL(access control list)と呼ぶ．ACLの例を図1(a)に示す．

ここで，頂点集合$V := O \cup S$，辺集合$E := \{(x,y) \in V \times V | xRy \vee xWy\}$とすれば，あるACLに対してアクセスグラフ$G_A = (V, E)$が定義できる．図1(a)のACLに対する，アクセスグラフは図1(b)となる．

グラフ$G = (V, E)$の推移閉包$G^+ = (V, E^+)$とは，ある$x, y \in V$で，xから辺を辿ってyに到達できるとき，$(x, y) \in E^+$となるグラフである．図1(b)のG_Aに対する，推移閉包は図1(c)となる．例えば，$s_1 \to o_1 \to s_2$の経路でs_1からs_2へ到達できるので，$(s_1, s_2) \in E^+$となっている．

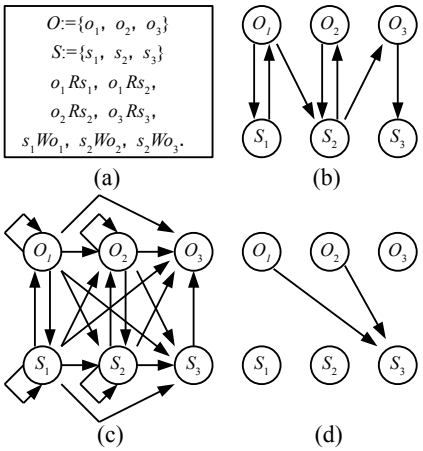

図 1: (a) An example access control list, (b) The access graph G_A of ACL of (a), (c) The transitive closure G_A^+ of graph G_A of (b), and (d) The covert channel detection of ACL of (a).

G_Aの辺はACLで許可された情報の流れを表す．一方，その推移閉包G_A^+の辺はACLで直接的･間接的に許可された情報の流れを表す．図1において$(o_1, s_3) \notin E$であるが，$(o_1, s_3) \in E^+$となっている．これは，ACLで直接許可されていないread権限が間接的に許可された矛盾した状態である．この状態を，o_1, s_3間にcovert channelが存在すると言う．アクセスグラフ$G_A = (V, E)$のcovert channel検出$G_A^{\#} = (V, E^{\#})$とは，$E^{\#} := \{(x,y) \in O \times S | (x,y) \in E^+ - E\}$となるグラフである．図1(b)の$G_A$に対する，covert channel検出は図1(d)となる．

3　提案アルゴリズム

次の検出アルゴリズムを提案する．

1. ACLからアクセスグラフG_Aを構築する．
2. G_Aから凝縮グラフ$\bar{G}_A$の推移閉包$\bar{G}_A^+$を計算する．
3. G_Aと$\bar{G}_A^+$からcovert channel検出$G_A^{\#}$を計算する．

隣接リスト形式でグラフを表現する場合，step1の計算量は$\mathcal{O}(|E|)$である．STACK_TC[1]を用いた場合，step2の最悪計算量は$\mathcal{O}(|V||\bar{E}_r| + |V||\bar{V}| + |\mu|)$である．step3は$\mathcal{O}(|V|^2)$で求まる．$|E| \le |V|^2, |\mu| \le |V||\bar{V}| \le |V|^2$より，提案アルゴリズムの最悪計算量は$\mathcal{O}(|V|^2 + |V||\bar{E}_r|)$である．この最悪計算量は従来のcovert channel検出アルゴリズム[2]の最悪計算量$\mathcal{O}(|V|^2 + |V||E|)$より優れている．ただし，$|\bar{E}_r|$は$G_A$の凝縮グラフ$\bar{G}_A$の推移還元$\bar{G}_{Ar}$の辺数を表し，$|\bar{E}_r| \le |\bar{E}| \le |E|$が成り立つ．

4　まとめ

推移閉包アルゴリズムを用いることでcovert channel検出アルゴリズムの計算量を改善できることを示せた．

参考文献

[1] Esko Nuutila, "Efficient Transitive Closure Computation in Large Digraphs.",ISBN 951-666-451-2, ISSN 1237-2404, 1995.

[2] 戸田　瑛人, クラウドの情報漏洩解析を高速に行うためのMapReduceの適用, 平成21年度修士論文