MapReduce を前提とした covert channel 解析

木下研究室　　吉澤　孝寛 (200702979)

1　はじめに

クラウドに於いて，情報流を制御し，covert channel による情報の漏洩・改竄が生じない様にする事は，大きな懸案事項である．ところが N × N アクセス行列における covert channel 分析にかかる計算量は，$O(N^3 logN)$ となり，仮にインターネットの中の局所的な community を分析ターゲットとし，分析のために全てのリソースを知る必要は無いと言う前提を設けても，膨大な計算量になる．そこで、covert channel 分析問題を分割統治法の導入によって部分問題に分割し，そのアクセス行列を reduce して部分問題自体を縮減する．更に、reduce 規則を導入し分析の効率化をするようなアルゴリズムを提案する．

2　covert channel 分析計算の方針

covert channel 分析問題を各 object 毎の部分問題に分割し分散処理させる事で，リアルタイム処理時間を短縮する．まず各 object 毎に並列で subejct の reduce をする．終了次第 reduce された各 object の reduce をする．その reduce を元に各 object 事のΦ を解析対象として分析する．

2.1　covert channel 分析

covert channel 分析のアルゴリズムの幅優先探索アルゴリズムを使う．アクセス行列はグラフとしての表現が可能であり、アクセス行列をノードとエッジにて表現し幅優先探索アルゴリズムを使う．

2.2　アクセス行列の縮減

計算量を減らすために, アクセス行列のサイズを小さくする. その為に, 行や列を合成する. その際に効率的に分析できるような,reduce を規則を提案する. reduce 規則により, アクセス権限集合体 (コミュニティ) の擬似的作成やアクセス権限不確定の権限の推論をする.

1. アクセス権限の追加
   権限の推論をするので, 新たに権限を追加する. アクセス権限不確定を E とし, 推論されたものを E-？とする. 推論されないものは単純に E とする
   RW,R,W, Φ ,E,E-RW,E-R,E-W,E-Φ
2. **subject の reduce 規則**
   各 object 毎に subject の reduce する.RW グループ,R グループ,W グループで reduce し, 最終的にグループ毎も reduce する. Φ は解析対象の為にリスト化し、アクセス権限不確定はコミュニティ作成の為にリスト化する. Φ リストと E リストと呼ぶ事にする. 具体的には図 1 のの流れとなる. 図 1 では,(a) のような object 行が存在していて, その subject の権限をグループ毎に reduce し, 更にすべて reduce しているという例である.
3. **object の reduce 規則**
   Φ リストと E リストから, コミュニティ (権限の集合体) を作成する為に, リスト同士の同一, 類似したものから reduce する. 図 2 のように同一, 類似を reduce する. 図 2 において, 同一, 類似のΦ リストと E リストをから図 2 のような object 同士を reduce する.

	s2	s4	s9	s8	s1	s7	s3	s5	s6
o1	RW	RW	RW	RW	R	R	R	W	W

(a)

	s2,s4s9,s8	s1,s7,s3	s5,s6
o1	RW-4	R-3	W-2

(b)

	s2,s4,s9,s8,s1,s7,s3,s5,s6
o1	RW-4-3-2

(c)

図 1: subject の reduce 規則

	E	RW	Φ
o1	S 1 ,S 6 ,S7	RW-12-5-2	S 3 ,S 5
o3	S 1 ,S 6 ,S7	RW-8-7-4	S 3 ,S 5
o5	S 1 ,S 6	RW-10-5-5	S 3 ,S 5 ,S7
o10	S 6 ,S7	RW-6-7-2	S 1 ,S 3 ,S 5

図 2: 始点と終点の解析

4. アクセス権限不確定の推論 **reduce 規則**
   コミュニティ外部と内部に存在する E を分類し, 内部の E の権限を推論する,E リストとΦ リストと reduce 対象の E リストとΦ リストの E リストの差分をコミュニティの内部と判定し, 判定されたものはグループ分けした際の reduce 情報を元にアクセス権限の推論をする.

2.3　始点と終点の解析

リスト化されたΦ をその行の object 毎に解析する. 始点は対応する object であり, 終点はリスト化されたΦ である. 幅優先探索を使い解析が可能である. 図 3 のような解析をすることとなる. 図 3 では S'm は subject の reduce,O'm は object の reduce とし, Φ リストから S1 と S2 を分析して,S2 に covert channel があるという例である

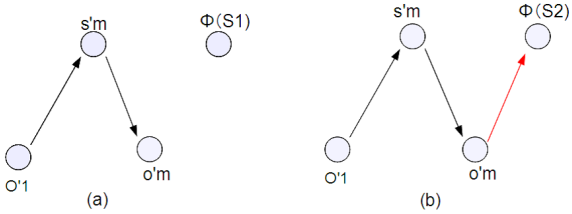

図 3: 始点と終点の解析

2.4　reduce 規則を利用した分析

始点と終点を元に経路の解析をする. その際に, 解析対象のノードを始点と終点からおこない解析する. 更に,reduce 規則を元にその規則とは逆の展開をする. これにより規則を持った展開が可能であり, コミュニティ毎の展開, 同一, 類似権限の展開しながらの解析が可能である

3　まとめ

subject，object の covert channel 分析の組合せアルゴリズムは，大規模クラウドの膨大なリソースを情報流制御の視点で大雑把に，かつ情報漏洩・改竄の脅威を漏らさない様に表示する上で効果的に結びつく