УДК 004.[021+023]

Восстановление состояния Linux-процесса оптимальными последовательностями системных вызовов на основе Марковских преобразователей.

Н.Н.Ефанов[1]

[1]Московский физико-технический институт (государственный университет)

Рассмотрена задача восстановления состояния пользовательского процесса Линукс. Решение данной задачи имеет важнейшее значение в построении систем заморозки/восстановления и миграции процессов[1].

Структуре задачи сопоставляется орграф, ветвям которого соответствуют системные вызовы, а в узлах расположены сигнатуры состояния процесса после соответствующего вызова. В вышеуказанной терминологии задача представляется как задача восстановления орграфа из некоторого начального состояния в конечное. Такой орграф:

а)изоморфен графу системных вызовов процесса.

б)имеет ассоциированный неориентированный граф, восстанавливаемый за O(M^4), где M — количество вершин[2].

Ввиду практической сложности сбора и хранения сигнатур состояний, в работе предлагается альтернативный вышеописанному механизм:

а)ввести строчное описание состояния. К примеру, любой процесс записывается как подстрока |pid pgid sid ;[children].

б)сопоставить системным вызовам выводящие правила. К примеру, системный вызов «setsid» имеет правило: |* * * ;* , |p p * ;* → |\1 \1\ 1 ;\4 , |p p \3 ;\4 . Данный шаг задаёт формальную грамматику системных вызовов, предоставляя механизмы разбора и поиска перехода из начального в конечное состояние. В общем случае грамматика имеет тип 0, однако имеет место цель сведения грамматик к неукорачивающим с помощью ряда ограничений.

Для анализ цепочек, порождаемых введённой выше грамматикой, в простейшем случае строится граф полного перебора. В графе могут быть простые циклы, ввиду приведения некоторыми цепочками системных вызовов к эквивалентным состояниям. Далее выполняется редуцирование графа с сохранением оптимальных цепочек. Работа рассматривает восстановление таких цепочек Марковскими преобразователями (восстановление системного вызова N по цепочке из N-1 произошедших). Марковские

преобразователи реализуются разложениями на соответствующих суффиксных деревьях с подсчетом условной вероятности данного системного вызова при некотором наборе произошедших[3]. Далее к рёбрам переборного графа применяется поиск характерных цепочек, вообще говоря, содержащих контекстно-зависимые участки. К примеру, подцепочки open -> write -> close и open -> read -> close кластеризуются в "контекстно-зависимую" подцепочку open -> * -> close, где * - вызов , зависящий от контекста[3]. Работа рассматривает цепочки переменной длины и затрагивает вопрос оптимального диапазона длин для любых цепочек.

Литература

1. Проект “CRIU”. Электронный источник: https://criu.org

2. *Сапунов С. В.* Восстановление графа с помеченными вершинами перемещающимся по нему мобильным агентом // Изв. Сарат. ун-та Нов. сер. Сер. Математика. Механика. Информатика; Izv. Saratov Univ. (N.S.), Ser. Math. Mech. Inform.. 2015. №2 С.228-238.

3. *Eskin E.*, *Lee W.*, *Stolfo S.* Modeling system calls for intrusion detection with dynamic window sizes. In Proc. DISCEX, 2001.