Гамаюнов Денис Юрьевич, к.ф.-м.н., м.н.с.
лаборатория Вычислительных комплексов, факультет ВМК МГУ имени М. В. Ломоносова
e-mail: gamajun@lvk.cs.msu.su
тел: +7 (909) 913-51-15

Критерий Поппера и исследования в области сетевой безопасности

Аннотация

В статье поднят вопрос о применимости критерия Поппера к исследованиям в области защиты информации, в частности, рассматривается направление сетевой безопасности и борьбы с компьютерными атаками и вредоносным программным обеспечением. Констатируется отсутствие необходимых условий фальсифицируемости теорий и гипотез, в частности, отсутствие практики опубликования экспериментальных данных. Существующие открытые наборы данных по компьютерным атакам (KDD Cup'99 dataset, VX Heavens dataset) значительно устарели, а новые и активно обновляющиеся банки данных являются де-факто закрытыми. Предложено создание и поддержка сообществом исследователей открытого банка данных с актуальными наборами как вредоносного программного обеспечения, так и частично обработанных результатов его анализа.

Ключевые слова: обнаружение атак, методология

Dennis Gamayunov, PhD, researcher
Computer Systems Lab, Lomonosov Moscow State University, CS Dept.
e-mail: gamajun@lvk.cs.msu.su
тел: +7 (909) 913-51-15

Popper's criterion vs. information security research

Abstract

Popper's falsifiability criterion helps us to distinguish between scientific and non-scientific theories. In this paper we try to discuss whether this criterion is applicable to the information security research, especially to the intrusion detection and malware research field. In fact, the designated research field seems to fail to satisfy the falsifiability criterion, because it lacks practice of publishing raw experimental data which is used to prove the theories. Existing public datasets like KDD Cup'99 dataset and VX Heavens virus dataset are outdated. At the same time new malware analysis projects tend to keep their datasets private. The conclusion is scientific community should pay more attention to creating and maintaining public open datasets of malware and any kinds of computer attacks related data.

Keywords: intrusion detection, methodology

В 1935 году Карл Поппер предложил критерий научности эмпирической теории, который определяет научность, исходя из принципа фальсифицируемости. Согласно данному принципу, научная теория не может быть принципиально неопровержимой [1], всегда должна существовать методологическая возможность экспериментального опровержения этой теории. На уровне отдельного исследования следование критерию фальсифицируемости превращается в практику опубликования исходных экспериментальных данных вместе с результатами их анализа.

Область информационной безопасности является частью намного более крупной области Computer Science, если следовать принятой на Западе классификации. И если в части направлений данной области дела с фальсифицируемостью обстоят вполне неплохо – а именно в криптографии и криптоанализе, то в области обнаружения компьютерных атак и анализа вредоносного программного обеспечения ситуация сложилась несколько иная: в настоящее время практика такова, что даже на самых высокоранговых конференциях публикуются только конечные численные результаты, а исходные экспериментальные данные не публикуются почти никогда. При этом область сетевой безопасности часто имеет дело с явлениями реального мира, воспроизвести которые в лабораторных условиях зачастую невозможно. Примером такого явления является эпидемия сетевого червя, использующего для распространения уязвимость типа «0-day» в популярном прикладном программном обеспечении или операционной системе. Эпидемии сравнительно редки, в «лучшем» случае они происходят несколько раз в год – это зависит от количества и характера публикуемых уязвимостей в соответствующем году. Типичной практикой постановки эксперимента для анализа сетевого червя является установка сети компьютеров-ловушек, и последующий мониторинг сетевой активности в течение значительного времени. Если исследовательской группе «повезло», и за период наблюдения их сеть ловушек действительно пронаблюдала какую-то эпидемию сетевого червя, то они проводят анализ этой эпидемии и публикуют результат – например, предлагают новый алгоритм обнаружения сетевых червей. Но при этом практически никогда не публикуются исходные данные, собранные исследователями за период наблюдения. В результате, у стороннего исследователя нет возможности воспроизвести заявленные в работе результаты, и остаётся лишь верить результатам на слово, либо пытаться получить похожие результаты на собственных данных.

Другой пример – исследование эффективности систем обнаружения или предупреждения компьютерных атак. В настоящее время не существует общепринятой методики оценки эффективности методов и алгоритмов обнаружения компьютерных атак, несмотря на то, что как направление исследований обнаружение атак существует уже

более тридцати лет. Существуют специальные коммерческие лаборатории, которые занимаются разработкой методик и тестированием готовых коммерческих систем обеспечения сетевой безопасности. Например, компания NSS Labs уже несколько лет проводит независимое тестирование систем обеспечения безопасности в сетях, и публикует отчёты о результатах у себя на веб-сайте [2]. Но коммерческие лаборатории не публикуют собственно тестовые наборы, которые используются в этих испытаниях. И их можно понять – ведь до сих пор подавляющее большинство систем обнаружения атак до сих пор используют сигнатурные методы обнаружения, и они могут быть с лёгкостью «адаптированы» к конкретному тестовому набору с целью повышения показателей эффективности, что может дать не совсем честно полученные конкурентные преимущества одним производителям перед другими. Хотя при корректном научном подходе к разработке методов обнаружения атак актуальные наборы данных были бы очень полезны. Таким образом, можно утверждать, что критерий Поппера в области сетевой безопасности в настоящее время не выполняется.

Теоретически, данную проблему могли бы решить общедоступные наборы данных, которые большинство исследователей считали бы достаточно доверенными, чтобы их можно было использовать для сравнения результатов исследований. За последние пятнадцать лет несколько раз предпринимались попытки создания подобных наборов данных. В качестве примеров можно привести KDD Cup'99 Dataset [3] – набор, сформированный на основе дампов трафика в реальной сети, в которой тестировались несколько систем обнаружения атак в 1999-м году – и набор вирусов и вредоносного программного обеспечения VX Heavens [5]. К сожалению, к настоящему моменту первый из них устарел настолько, что его использование в исследовании не просто бесполезно, но более того, гарантирует негативную оценку исследования в научном сообществе с вероятностью, близкой к единице [4]. Использование набора VX Heavens ещё возможно в работах студенческого уровня, то также не может считаться хорошей постановкой эксперимента.

В настоящее время существует несколько исследовательских проектов, которые осуществляют сбор экземпляров вредоносного программного обеспечения, как бинарных исполнимых файлов, так и сценариев JavaScript – это проекты CWSandbox [6], Anubis [7], Wepawet [8]. По каким-то причинам, ни один из них не предоставляет свободный доступ исследователей к собранным данным – авторами проектов публикуются лишь результаты анализа. В случае CWSandbox такое поведение вполне понятно, т.к. проект стал основой для бизнеса компании Sunbelt Software, и накопленная коллекция вредоносных файлов составляет немалую часть её активов. Возможно, аналогичные соображения движут и

авторами проектов Anubis и Wepawet. Но в результате научное сообщество получает лишь набор исследовательских работ, которые не удовлетворяют попперовскому критерию научности.

Можно отметить ещё один немаловажный фактор – наличие публичного и общепризнанного набора экспериментальных данных стимулирует исследовательскую активность само по себе. Сравним количество упоминаний упомянутых выше коллекций данных в научных работах, вычисленное по соответствующим запросам в Google Scholar:

Таблица 1. Цитируемость коллекций данных по Google Scholar

Название коллекции	**Число упоминаний в научных статьях**	**Год публикации**	**Нормированное по годам число упоминаний**
KDD Cup 99 dataset	2,850	1999	237
Vx heavens	9,530	1999	794
Anubis	115	2007	28
CWSandbox	243	2006	48
Wepawet	25	2008	8

Приведённые в таблице числа показывают, что количество работ, сделанных с использованием открытых наборов данных, по меньшей мере на порядок превышает количество работ с закрытыми данными, включая цитирования.

Существуют исследовательские работы, где основой полученных экспериментальных результатов является альтернативная реализация известного метода (к примеру, портированная на CUDA API версия известной библиотеки), либо реализация, иллюстрирующая основную идею работы. Т.е. когда реализация является существенным условием фальсифицируемости результата. Для таких работ также нередки случаи, когда единственным ответом на запрос о предоставлении исходных данных, даже под соглашение о неразглашении, единственным ответом будет:

«Thanks for writing. We won't be releasing the implementation. Sorry that I can't be more helpful»

Представляется целесообразным создание и поддержка сообществом исследователей, работающих в области сетевой безопасности, открытого банка данных с актуальными наборами как вредоносного программного обеспечения, так и частично обработанных результатов его анализа. И что особенно важно – необходимо восстановить практику опубликования тех экспериментальных данных, на которых базируются публикуемые результаты. Накопленный опыт в нашей области и в смежных областях

естественных наук показывает, что открытость подобного рода всегда способствует как количественному, так и качественному росту исследований.

Ссылки

1. К. Поппер. Логика и рост научного знания. М.:Прогрес, 1983.
2. Отчёты NSS Labs по системам обнаружения атак. [WWW] http://www.nsslabs.com/research/network-security/network-ips/
3. KDD Cup 1999 Data. [WWW] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
4. Terry Brugger, KDD Cup'99 dataset considered harmful. UC Davis, 2007. [WWW] http://www.bruggerink.com/~zow/GradSchool/KDDCup99Harmful.html
5. VX Heavens. Computer virus collection. [WWW] http://vx.netlux.org/vl.php
6. CWSandbox. Malware analysis system. [WWW] http://mwanalysis.org/
7. Anubis: Analyzing Unknown Binaries [WWW] http://anubis.iseclab.org/
8. Wepawet [WWW] http://wepawet.cs.ucsb.edu/