A.V. Fedorchenko, I.V. Kotenko, A.A. Chechulin

Development of Information Access and Management Services for Integrated Vulnerability Database

Keywords: vulnerability databases, security evaluation, security monitoring systems.
The paper is devoted to the investigation of open vulnerability databases and methods of their integration for construction of an integrated security information repository. The novelty of the present work lies in the proposed process model of repository construction and filing optimized for the task of network security evaluation. As a practical implementation the set of security information management services are presented. The main distinguishing feature of proposed integrated repository is its adaptation for use as a service in the network security evaluation systems and aggregation of security information from multiple open databases in one repository.

А.В. Федорченко, И.В. Котенко, А.А. Чечулин

РАЗРАБОТКА СЕРВИСА ДОСТУПА И УПРАВЛЕНИЯ ИНТЕГРИРОВАННОЙ БАЗОЙ УЯЗВИМОСТЕЙ

Введение

Одним из способов повышения защищённости компьютерных сетей является периодическая проверка используемых программно-аппаратных средств на наличие в них уязвимостей, нарушающих безопасность компьютерных систем. На данных момент существует ряд организаций, занимающихся мониторингом, классификацией и накоплением данных об уязвимостях. Данные организации предоставляют открытый доступ к своим базам уязвимостей, однако каждая такая база заполняется независимо от других и, что более важно, имеет свой формат представления данных. Кроме того, существующие базы данных уязвимостей ориентированы именно на хранение данных, но не на их использование, что приводит к значительным временным затратам при поиске уязвимостей, характерных для некоторых программно-аппаратных конфигураций.

Одной из областей применения баз уязвимостей являются средства оценки защищенности компьютерных систем и инфраструктур [1, 4]. Списки уязвимостей в решениях данного класса используются как одни из основных источников информации для оценки защищённости, так как описания уязвимостей содержат как предусловия, так и оценки, характеризующие результат реализации атак, эксплуатирующих эти уязвимости. Кроме того, в описания уязвимостей входят списки конкретных программно-аппаратных продуктов, содержащих данные уязвимости. Предполагается, что объединение открытых баз данных уязвимостей приведёт к ряду преимуществ, а именно: 1) интеграции самих записей уязвимостей, что обеспечит более систематизированный доступ к информации об уязвимостях; 2) расширению списка продуктов, в которых уязвимости могут иметь успешную реализацию, что позволит повысить вероятность обнаружения уязвимых программно-аппаратных средств, используемых в анализируемых системах, и, как следствие, улучшит точность оценки защищенности этих систем. Кроме того, использование структуры базы данных, адаптированной для поиска записей уязвимостей посредством удаленного сервиса, позволит применять эту базу в системах оценки защищённости, работающих при эксплуатации исследуемых инфраструктур, то есть проводящих анализ безопасности в режиме, близком к реальному.

Основными задачами, решаемыми в данной работе, являются: 1) создание модели процесса формирования интегрированной базы данных уязвимостей для повышения точности оценки защищённости компьютерных сетей; 2) разработка реляционной модели формируемой базы для обеспечения необходимой оперативности при функционировании в составе системы оценки защищённости компьютерных сетей. Основное отличие интегрированной базы данных – ее адаптация к использованию как сервиса в системах оценки защищенности и совмещение в одной базе информации из разнородных открытых источников описаний уязвимостей. В работе основное внимание уделено модели процесса формирования и структуре интегрированной базы данных уязвимостей, а также их обоснованности на основе анализа открытых баз данных уязвимостей.

Модель процесса формирования интегрированной базы данных уязвимостей и проектирование её структуры

В настоящее время базы данных уязвимостей широко применяются при решении задач обеспечения безопасности компьютерных систем. Они используются в сканерах уязвимостей, сканерах безопасности, системах обнаружения и предотвращения атак и т.д. [2] Основной проблемой существующих баз данных уязвимостей является неспособность автоматизированного открытого и беспрепятственного доступа для формирования результата поиска уязвимого программно-аппаратного обеспечения. Задача формирования такого результата усложняется наличием сложной зависимости между элементами программно-аппаратного обеспечения, необходимыми для реализации некоторой уязвимости. Учитывая тот факт, что базы данных уязвимостей наполняются преимущественно отдельно друг от друга и имеют различные форматы описания уязвимостей и продуктов, их применение в системе оценки защищённости компьютерных инфраструктур затруднено.

Для полноценного применения разрабатываемой интегрированной базы данных уязвимостей в средствах оценки защищённости компьютерных систем, она должна содержать в себе: 1) список уязвимостей; 2) список продуктов (платформ, операционных систем и приложений); 3) показатели, характеризующие уязвимости [3]. В связи с тем, что данные в базу добавляются из разных источников, записи уязвимостей были помещены в интегрированный список уязвимостей, а записи продуктов – в интегрированный словарь продуктов.

Процесс интеграции уязвимостей был разделен на два этапа: 1) установление соответствия по прямым ссылкам и идентификаторам на уязвимости объединяемых баз; (2) установление соответствия по ссылкам на неиспользуемые источники (например, другие базы данных уязвимостей) с условием, что данные ссылки уникальны для всех объединяемых баз. Таким образом, формирование интегрированного списка уязвимостей можно представить, как показано на рис. 1.

Стоит отметить: если идентификаторы в пределах одной базы ссылались на собственные записи уязвимостей, то такие уязвимости объединялись в одну запись интегрированного списка уязвимостей.

Рис.1. Модель процесса формирования интегрированного списка уязвимостей

Процесс формирования интегрированного словаря продуктов заключается в объединении записей продуктов используемых баз данных уязвимостей с исключением дублирования. На начальном этапе данный словарь составляется путем добавления записей Общего перечисления платформ (Common Platform Enumeration, CPE). CPE – это структурированная схема именования для компьютерных систем и платформ, основанная на синтаксисе Универсальных идентификаторов ресурсов (Uniform Resource Identifiers – URI). Данный словарь взят в качестве основного источника записей продуктов, так как он содержит большее количество записей продуктов по сравнению со списками продуктов используемых баз уязвимостей, а реализация его записей имеет наилучшую на сегодня форму представления продуктов. Несмотря на данный факт, формат самих записей был приведен к следующему виду:

{тип}:{производитель}:{продукт}:{версия}:{модифи-кация}:{ редакция}.

Также следует отметить, что в качестве показателей, характеризующих уязвимости, была выбрана Общая система оценки уязвимостей (Common Vulnerability Scoring System, CVSS), которая, по мнению экспертов, является одной из наиболее востребованных для проведения оценки защищенности.

В рамках интегрированного хранилища информации безопасности, в качестве связывающего элемента между записями уязвимостями и вышедшими эксплойтами (например, из базы Exploit Database), а также для связывания со списком слабостей (Common Weakness Emumeration, CWE) и списком конфигураций (Common Configuration Enumeration) предлагается применение идентификаторов, используемых баз уязвимостей и имен продуктов. Данный подход обеспечит оптимизированный доступ к информации безопасности при использовании поиска лишь по параметрам одной записи из используемых источников. Особенностью данного хранилища является то, что его применение полностью адаптировано для работы с сервисом доступа и управления, который используется при моделировании атак и оценке рисков системы оценки защищенности компьютерных систем [5, 6].

Проектирование структуры интегрированной базы данных уязвимостей производилось в соответствии с разработанной моделью процесса формирования. Конечные

данные были распределены по следующим реляционным таблицам: 1) производители (Vendors); 2) продукты (Products, содержит внешний ключ табл. 1); 3) параметры продуктов (Units, включает поля «тип», «версия», «модификация», «редакция» и внешний ключ табл. 2); 4) уязвимости (Vulns); 5) ссылки на источники описания уязвимостей (Refs); (6) уязвимые конфигурации (Vuln_units, включает внешние ключи записей табл. 4 и 3, а также параметр зависимости); 7) таблица связи ссылок и уязвимостей (Vuln_refs, включает внешние ключи табл. 4 и 5).

Параметр зависимости в реляционной табл. (6) – необходимый и единственный признак, определяющий связь между уязвимым программно-аппаратным обеспечением и продуктами, при которой данная зависимость может быть реализована. Таким образом, если указанный в качестве ключа продукт имеет уязвимость без такой зависимости, то поле «параметр зависимости» этой записи будет иметь значение 0. Если же данная уязвимость для данного продукта реализуется только в случае наличия другого продукта, то такая зависимость будет описана следующим образом: 1) пусть группа продуктов, имеющих положительную реализацию уязвимости в зависимости от наличия в системе любого из продуктов другой группы, является группой A; 2) тогда группа продуктов, влияющих на положительную реализацию уязвимости продуктов группы A, является группой B; 3) значение поля «параметр зависимости» записи таблицы связывания для продуктов группы A будет нечетным, начиная со значения 1; 4) значение поля «параметр зависимости» записи таблицы связывания для продуктов группы B будет четным, начиная со значения 2.

Описанная структура позволяет с помощью одного SQL-запроса к интегрированной базе данных уязвимостей осуществлять поиск уязвимостей, присущих некоторому комплексу программно-аппаратных продуктов (т.е. списку установленного программно-аппаратного обеспечения на отдельном устройстве исследуемой системы).

В общем виде, для двух проверяемых продуктов, представленных в виде записей:
продукт 1 - {тип_1}:{производитель_1}:{продукт_1}:{версия_1}:{модификация_1}:{редакция_1} и
продукт 2 - {тип_2}:{производитель_2}:{продукт_2}: {версия_2}:{модификация_2}:{редакция_2}
такой запрос выглядит, как представлено на рис. 2, где выделенные символом '~' участки кода QUERY определены на рис. 3.

```
SELECT * FROM Vulns WHERE [ключ записи уязвимости] LIKE IN
(SELECT [ключ записи уязвимости] FROM Vuln_units WHERE (
( ~QUERY_1~ = ~QEURY_2~ ) = ( ~QUERY_1~ = ~QEURY_4~ ) AND
( ~QUERY_3~ = ~QEURY_2~ ) = ( ~QUERY_3~ = ~QEURY_4~ )) OR
( ~QUERY_1~ = ~QEURY_2~ ) = 0 OR (~QUERY_1~ = ~QEURY_4~ ) = 0)
```

Рис. 2. Общий вид запроса к интегрированной базе уязвимостей

```
~QUERY_1~ == SELECT [параметр зависимости] FROM Vuln_units
             WHERE [ключ конечной записи продукта]

~QUERY_2~ == SELECT Units.[ключ конечной записи продукта]
             FROM Vendors INNER JOIN Products
             USING ([ключ производителя])
             INNER JOIN Units USING ([ключ продукта])
             WHERE Vendors.[имя производителя]={производитель_1}
             AND Products.[имя продукта]={продукт_1}
             AND Units.[тип]={тип_1}
             AND Units.[версия]={версия_1}
             AND Units.[модификация]={модификация_1}
             AND Units.[редакция]={редакция_1}

~QUERY_3~ == SELECT [ключ записи уязвимости] FROM Vuln_units
             WHERE [ключ конечной записи продукта]
```

Рис. 3. Обозначение участков запроса к интегрированной базе уязвимостей

Стоит отметить, что участок кода QUERY_4 – аналогия участка QUERY_2 для обозначения запроса поиска ключа конечной записи второго продукта.

Такая особенность разработанной базы позволяет значительно снизить время, необходимое для поиска подходящих уязвимостей и, как следствие, подтверждает применимость предлагаемой базы данных уязвимостей в средствах оценки защищённости компьютерных систем, работающих в условиях, приближенных к реальному времени.

Анализ открытых баз данных уязвимостей

Для формирования интегрированной базы данных уязвимостей был проведён анализ ряда открытых баз данных уязвимостей, в том числе следующих баз: 1) Общие уязвимости и воздействия (Common Vulnerabilities and Exposures, CVE); 2) Национальная база данных уязвимостей (National Vulnerabilities Database, NVD); 3) Открытая база данных уязвимостей (Open Source Vulnerabilities DataBase, OSVDB); 4) База уязвимостей X-Force [7].

Анализ базы данных уязвимостей CVE показал, что она обладает высокой степенью связывания с другими источниками описания уязвимостей. Однако более подробное описание уязвимостей, содержащихся в CVE, представлено в базе данных NVD. Эта база включает в себя описание уязвимостей с указанием подверженных им программно-аппаратных продуктов в формате CPE. Кроме того, данная база содержит показатели, характеризующие уязвимости в формате CVSS. Однако количество ссылок на другие базы данных уязвимостей, по которым производится интеграция записей уязвимостей, в базе NVD меньше, чем в базе CVE. Анализ базы NVD показал, что из всех уязвимостей, зависимости включают только 10,63 % записей.

При анализе базы данных уязвимостей OSVDB было выявлено множество ссылок на сторонние источники, причем наилучшими показателями по количеству и уникальности обладают ссылки на базы CVE и NVD.

В завершение обзора используемых источников стоит отметить: база уязвимостей X-Force – единственная в своем классе, имеющая описание уязвимостей с временными показателями системы CVSS, что вносит дополнительное преимущество при её применении.

Исходя из полученных результатов, именно данные базы стали основными источниками информации об уязвимостях для формирования интегрированной базы данных уязвимостей.

Описание сервиса доступа и управления интегрированной базой уязвимостью

В качестве практической реализации был разработан сервис доступа и управления интегрированной базой данных уязвимостей, который обеспечивает, в том числе, формирование самой базы. В результате полученная интегрированная база содержит данные из следующих источников описания уязвимостей и продуктов: 1) база CVE; 2) база NVD; 3) база OSVDB; 4) база X-Force; 5) словарь CPE. В результате формирования интегрированной базы общее число уникальных записей уязвимостей составило примерно 90 тысяч (для сравнения, число загруженных записей уязвимостей из базы CVE составило ~67 тыс., из базы OSVDB ~100 тыс., а из базы X-Force ~65,5 тыс.). В свою очередь, общей размер интегрированного словаря продуктов составил 192 тыс. оригинальных записей (из них 99,5 тыс. из словаря CPE). Также показатели обосновывают преимущество данной базы перед применяемыми источниками описания уязвимостей и продуктов, а также теоретическое повышение точности при использовании разработанного сервиса в средствах оценки защищенности компьютерных инфраструктур для решении задачи моделирования атак в режиме, близком к реальному.

При сравнении разработанного сервиса с аналогами, а именно: с online-сервисом «CVE Details», были выявлены следующие преимущества интегрированной базы уязвимостей: 1) превосходство по количеству обрабатываемых производителей, продуктов и их версий; 2) наличие соответствия записей уязвимостей базы CVE с базами OSVDB и X-Force, а также между собой; 3) предоставление возможности как автоматизированного, так и ручного (для администраторов безопасности посредством web-интерфейса) доступа к возможностям поиска уязвимостей в интегрированной базе.

Дополнительное качество сервиса доступа и управления интегрированной базой данных уязвимостей – наличие возможности автоматизированного обновления, как из сети Интернет, так и с локальных ресурсов (жесткий диск, FTP-ресурсы), что позволяет поддерживать актуальность информации об уязвимостях на должном уровне для обеспечения высокой точности оценки защищенности исследуемых инфраструктур.

Для проверки эффективности функционирования сервиса доступа и управления интегрированной базой уязвимостей была проведена серия экспериментов для моделирования различных сценариев атак, которая показала, что при росте числа проверяемых в рамках одного запроса конфигураций и, соответственно, увеличении количества проверяемых программно-аппаратных средств, среднее время формирования результата для одной конфигурации изменяется по экспоненциальному закону за счет многократного вхождения имен производителей, продуктов и версий в список проверяемого программно-аппаратного обеспечения.

Заключение

В работе предложена модель процесса формирования и структура интегрированной базы данных уязвимостей, а также реализованный сервис доступа и управления её прототипом. Данный сервис в настоящее время применяется в составе системы оценки защищённости компьютерных инфраструктур, предназначенной для функционирования в условиях, приближенных к реальному времени. Разработанная интегрированная база данных уязвимостей обеспечивает повышение точности обнаружения уязвимого

программно-аппаратного обеспечения, что позволяет средствам оценки защищённости улучшить эффективность выполнения поставленных перед ней задач.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451) и программы фундаментальных исследований ОНИТ РАН (контракт №1.5).

СПИСОК ЛИТЕРАТУРЫ:

1. Котенко И.В, Степашкин М.В., Дойникова Е.В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3. С.40-57.
2. Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности, Т.8, № 2, 2012. С.100-108.
3. Kotenko I., Polubelova O., Saenko I. Data Repository for Security Information and Event Management in Service Infrastructures // SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography. Rome, Italy. 24-27 July 2012. P.308-313.
4. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН, Вып.1 (20), СПб.: Наука, 2012. С. 27-56.
5. Kotenko I., Chechulin A. A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict 2013 (CyCon 2013). Proceedings. IEEE and NATO COE Publications. Tallinn, Estonia. 4-7 June 2013. P. 119-142.
6. Котенко И.В., Дойникова Е.В., Чечулин А.А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд, № 4, 2012. С.54-66.
7. X-Force. http://xforce.iss.net/, 07.02.15.

REFERENCES:

1. Kotenko I.V., Stepashkin M.V., Dojnikova E.V. Analiz zashchishchennosti avtomatizirovannyh sistem s uchetom socio-inzhenernyh atak // Problemy informacionnoj bezopasnosti. Kompyuternye sistemy. 2011. № 3, P.40-57.
2. Kotenko I.V., Polubelova O.V., Saenko I.B., Chechulin A.A. Primenenie ontologij i logicheskogo vyvoda dlya upravleniya informaciej i sobytiyami bezopasnosti // Sistemy vysokoj dostupnosti, T.8, № 2, 2012. P.100-108.
3. Kotenko I., Polubelova O., Saenko I. Data Repository for Security Information and Event Management in Service Infrastructures // SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography. Rome, Italy. 24-27 July 2012. P. 308-313.
4. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Primenenie tekhnologii upravleniya informaciej i sobytiyami bezopasnosti dlya zashchity informacii v kriticheski vazhnyh infrastrukturah // Trudy SPIIRAN Vyp.1 (20), SPb.:Nauka, 2012. P.2 7-56.
5. Kotenko I., Chechulin A. A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict 2013 (CyCon 2013). Proceedings. IEEE and NATO COE Publications. Tallinn, Estonia. 4-7 June 2013. P.119-142.
6. Kotenko I.V., Dojnikova E.V., Chechulin A.A. Obshchee perechislenie i klassifikaciya shablonov atak (CAPEC): opisanie i primery primeneniya // Zashchita informacii. Insajd, № 4, 2012. P.54-66.
7. X-Force. http://xforce.iss.net/, 07.02.15.