8 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

МОДЕЛЬ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МАТЕРИАЛОВ ХАКЕРСКИХ КОНФЕРЕНЦИЙ

Э.Р. Хусаинова

Проблема создания модели угроз является мало разработанной и актуальной. Модели угроз должны стать отправными точками для проектирования будущих систем защиты компьютерных и информационных систем. Построение модели угроз на основе материалов хакерских конференций позволит повысить надежность и защищенность информационных систем и программных продуктов.
Ключевые слова: хакерские конференции, модель угроз, защита информации, прогнозирование атак.

Введение

Предотвращение компьютерных атак со стороны злоумышленников – очень актуальная задача для специалистов, работающих в сфере информационных технологий. Согласно данным исследования специалистов из университета Мериленда (США), в Сети каждые 39 секунд происходит новая компьютерная атака [1]. Поэтому очень важно быть в курсе самых последних новостей, касающихся взлома и различного рода атак со стороны хакеров. Получить такую информацию можно из конференций и съездов, организуемых бывшими хакерами, ныне экспертами в области безопасности компьютерных систем и главами соответствующих ИТ-компаний. Попытаемся построить структурную модель оценки угроз информационной безопасности (ИБ) на основе материалов хакерских форумов и съездов.

Цели и задачи конференций хакеров

В литературе моделирование процессов нарушения информационной безопасности предлагается осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации – уязвимость – последствия». Требуется, чтобы в ходе анализа все возможные источники угроз были идентифицированы, все возможные уязвимости сопоставлены с идентифицированными источниками угроз, всем источникам угроз и уязвимостям (факторам) сопоставлены методы реализации [2]. На наш взгляд, такая модель в рамках хакерских конференций будет неполной, поскольку не учитываются мотивы и цели субъектов угроз, а также их количественные и качественные характеристики, потоки информации, циркулирующие между источниками угроз и объектами исследований (т.е. уязвимостями).

Рассмотрим, что представляют собой хакерские конференции, каковы цели, задачи, масштабы подобных съездов, набирающих все большую популярность и значимость в области защиты ИБ.

Хакерские конференции – одни из важнейших мероприятий в области ИБ, значительно способствующие повышению уровня защиты информации и квалификации специалистов, а также демонстрирующие новые угрозы и атаки, методы реализации взлома и нападения на компьютерные и информационные системы. География проведения подобных мероприятий достаточно обширна. Функционирует ежегодная конференция Defcon в Лас-Вегасе, где собираются несколько тысяч участников из многих стран мира

– от США до Австралии [3]. С 1989 г. раз в четыре года проходит представительный хакерский форум в Голландии «Hackers At Large». Ежегодно в Германии проходит Всемирный конгресс хакеров под эгидой «Chaos Computer Club». Аналогичные конференции проходят также в таких странах, как Канада, Израиль, Южная Корея, Япония, Малайзия, Саудовская Аравия, Англия и т.д.

На международных съездах хакеров отчетливо прослеживается тенденция взаимодействия хакерского движения с государственными и коммерческими структурами. В них принимают участие представители государственных органов безопасности, администраторы крупнейших фирм. Более того, некоторые из известных хакеров активно участвуют в государственных и международных организациях по информационной безопасности. Так, например, президент и основатель «Chaos Computer Club» (Клуб компьютерного хаоса) Энди Мюллер-Мэган входит в состав всемирной организации «ICANN» (Internet Corporation for Assigned Names and Numbers) [4].

С каждым годом количество и состав участников растет и меняется: от хакеров до профессионалов в компьютерной безопасности, представителей крупнейших корпораций, правительственных организаций и федеральных спецслужб.

Цели, задачи и программа конференций становятся все более серьезными и глобальными, от развлечений до совместной борьбы с кибертерроризмом:

- привлечение внимания к информационной безопасности;
- сбор информации, обмен опытом борьбы с «кибертерроризмом»;
- реализация предупреждающих стратегий;
- демонстрация новейших решений в области управления информационной безопасностью;
- разработка инструментов для защиты системы от возможных угроз;
- обсуждение проблем социальных аспектов хакерства и др.

В программе хакерских конференций обсуждаются не только вопросы защиты ИБ, но и нападения со стороны нарушителей. В частности, в программу прошедших конференций были включены такие темы, как электронное голосование (поиск недостатков и выявление возможных угроз), беспроводные сети (Bluetooth – возможная утечка информации, атака с расстояния, уязвимости), DNS (сетевые атаки через DNS), социальные и технические аспекты (совесть хакера, злоупотребление властью), хакинг (методы против защиты в нецифровом мире), сетевая безопасность (IIS защита баз данных и трояны) и т.д.

Роль конференций в прогнозировании перспективных угроз

Еще одним важным достижением участников конференций является новое программное обеспечение, которое вполне можно использовать в повседневной жизни. Например, хакерская конференция ShmooCon 2008 порадовала целым арсеналом необычных устройств, которые можно было проверить в действии прямо на посетителях. Особую отметку получила оболочка Silica на базе Nokia N800, которая автоматически сканирует все окружающие Windows-компьютеры через WiFi, выявляет уязвимые ПК и позволяет сделать скриншоты с любого из них за пару щелчков мыши [5].

Результаты и подведение итогов конференций носят ценный характер с точки зрения привлечения всеобщего внимания к проблемам компьютерной безопасности и укрепления защиты важных инфраструктур от кибератак. Так, на конференции Defcon 17, прошедшей в июле 2009 года, правительство США открыто приглашало на работу «этичных хакеров». Это связано с тем, что в последние годы атакам подвергаются ключевые компьютерные сети, включая электроэнергетические системы. Специалист по безопасности и пилот Райтер Кункель (Righter Kunkel) продемонстрировал собравшим-

ся, как легко можно проникнуть в управляющую систему движения воздушного транспорта Федерального управления гражданской авиации США. При желании атакующий может, среди прочего, мешать обмену данными с диспетчерской вышкой, блокировать радар, ввести в систему поддельный план полета самолета, выдать себя за пилота, таковым не являясь, или же запретить самолетам вылет из аэропорта. Возможно, именно с этим связано множество авиационных крушений, произошедших в последнее время по всему миру [6].

Как видно, анализ негативных последствий реализации угроз на конференциях предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации, т.е. классификацию (рис.)

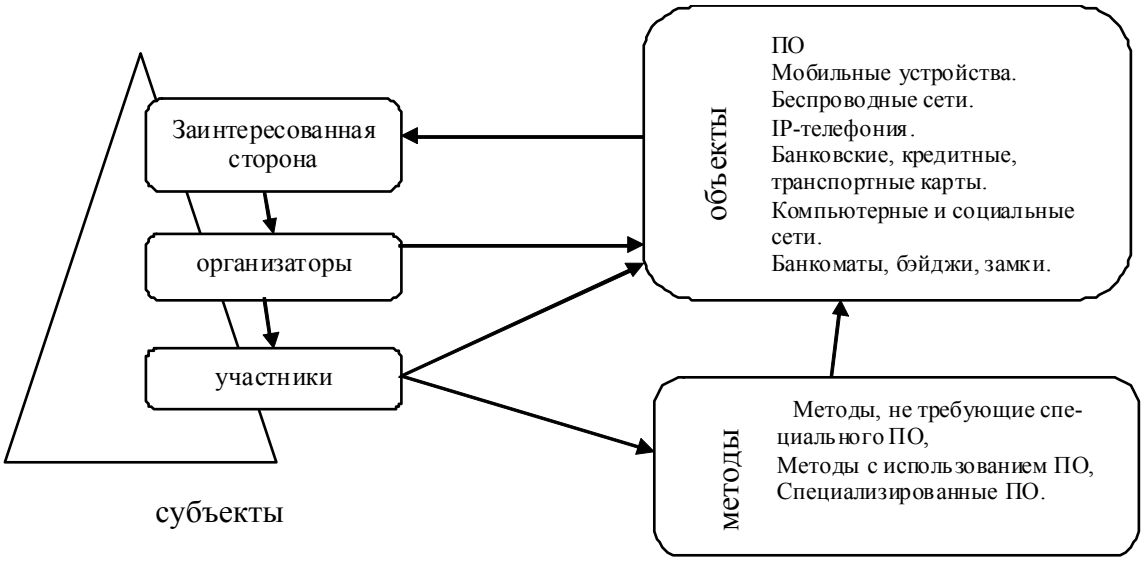

Рис. Структурная модель взаимодействия в среде хакерских конференций

К группе заинтересованной стороны относят представителей государственных структур, спецслужб, корпораций, компаний, банков, ИТ-специалистов, хакеров и агентов, для каждого из которых интерес представляет свой объект исследования. Например, для госструктур такими объектами являются программные устройства, системы контроля доступа, протоколы и т.д.

Заинтересованная сторона выбирает объект исследования, предоставляет полный или ограниченный доступ к ресурсу, ставит цели и задачи перед организаторами и сроки выполнения поставленных задач. Так, например, компания Microsoft предлагает исследовать на предмет безопасности, простоты использования, визуализации новую операционную систему (ОС), допустим, Windows Vista (объект исследования), и ставит перед организаторами следующие задачи: выявить основные области ОС, которые требуют дальнейшей доработки и модернизации, предложить возможные решения выявленных проблем. Организаторам было выделено 100 бета-версий ОС. Организаторы же, в свою очередь, выбирают группу хакеров, определяют информационные и технические ресурсы, подлежащие защите либо атаке. Участники исследуют объект, проводят анализ характеристик угроз и уязвимых мест для информации, оценивают и измеряют риски, подбирают и используют методы и способы защиты или взлома.

Вернемся к нашему примеру. Группа американских исследователей выделила такие объекты: безопасность доступа к ОС, уязвимости с точки зрений Интернет-угроз, защищенность от вирусных атак и т.п. Также были предложены соответствующие методы: интеграция в систему нескольких вирусов и исследование поведения ОС, использование программы генерации пароля для аутентификации. Подобные действия были проведены и другими группами.

Далее участники приступают к практической части конференции. На этом этапе производятся весь анализ и составление будущего выступления, презентации своих достижений на конференции:

– проверка методов и способов защиты или взлома на объектах;
– анализ и подведение итогов исследования;
– подготовка к презентации полученных результатов;
– демонстрация и апробация новых утилит и устройств.

Таким образом, модель оценки угроз информационной безопасности – непрерывный цикл информационных потоков между субъектами и объектами съездов. Это совокупность внешних и внутренних факторов и их влияния на состояние информационной безопасности и на сохранение материальных и информационных ресурсов. Модель угроз должна впоследствии использоваться в проектировании будущих систем защиты информационной безопасности от возможных уязвимостей.

Мотивация субъектов конференций

Определив источники угроз и уязвимости для анализа причин и последствий реализации угроз, необходимо выяснить, какими же мотивами и целями руководствовались нарушители. Представители компаний и банков действуют в целях получения личной выгоды, новой информации об уязвимостях, протоколах; государственные и спецслужбы – в целях национальной безопасности, раскрытия конфиденциальной информации, предотвращения утечек баз данных и другой важной информации; хакеры – ради получения порции адреналина от осуществления незаконных действий, а также, чтобы проверить свои возможности и способности в области хакинга и защиты.

В продолжение примера отметим следующее. Американские, русские и французские ученые достигли конкретных результатов и выступили с докладами на конференции. Компания Microsoft, таким образом, получила интересующие ее сведения об ОС Windows Vista и определила для себя дальнейшие пути исследований и модернизации своего продукта. Все субъекты получили свою выгоду: организаторы – денежный чек, участники – премии, вакансии в компании заказчика, известность и способность доказать значимость своих исследований, а Microsoft – новые цели, ценные кадры и рекламу ОС.

В целом такой вид получения информации касательно интересующего заказчика объекта имеет как свои плюсы, так и минусы. Непосредственно сами результаты конференции и конкретных исследований, довольно быстрое достижение результата можно отнести к положительным аспектам, а риск, на который идет заказчик, предлагая участникам изучить сам объект, в силу своей непредсказуемости, безусловно, является отрицательной стороной. Ведь публичное выступление на хакерской конференции коренным образом влияет на общественное мнение, что может как прибавить, так и уменьшить спрос на объект. Несмотря на это, подобные съезды приобретают все большую популярность и охватывают все новые и новые горизонты информационных технологий.

Заключение

Таким образом, исследование материалов хакерских конференций напрямую способствует выявлению уязвимостей программного обеспечения и оборудования, а также предотвращению Интернет-атак. Вышеперечисленные примеры доказывают эффективность подобных мероприятий и вполне адекватную реакцию на это со стороны представителей государственных и коммерческих предприятий. К наиболее важным результатам конференций следует относить последующие изменения в программном и техническом оборудовании, а также глобальное информирование пользователей ПК о возможных путях преодоления защиты и доступа к их персональным данным.

Необходимо проводить хакерские конференции в России для защиты национальных интересов страны, уделять должное внимание вопросам информационной безопасности, каковые и обсуждаются на подобных конференциях.

Результатами проведения подобной конференции в России могут стать:

- привлечение внимания общественности к проблемам защиты информации;
- повышение мирового статуса России в области информационной безопасности;
- привлечение дополнительных государственных и зарубежных инвестиций в область защиты информации.

Это качественно повысит уровень информационной безопасности и даст возможность более интенсивно развивать данную область.

Литература

1. Сайт Интернет-журнала Hackzone [Электронный ресурс] / 2009. – Режим доступа: http://www.hackzone.ru/news/view/id/5204/, свободный. – Яз. рус.
2. Вихорев С., Кобцев Р. Как определить источники угроз? [Электронный ресурс] / 2003. – Режим доступа: http://www.citforum.ru/security/articles/threats/, свободный. – Яз. рус.
3. Сайт конференции DefCon [Электронный ресурс] / 2009. – Режим доступа: www.defcon.org, свободный. – Яз. англ.
4. Сайт конференции Chaos Communication Congress [Электронный ресурс] / 2009. – Режим доступа: www.ccc.de, свободный. – Яз. англ., нем.
5. Хакерские гаджеты на конференции ShmooCon [Электронный ресурс] / 2008. – Режим доступа: http://habrahabr.ru/blogs/infosecurity/5893/, свободный. – Яз. рус.
6. Сайт Интернет-журнала securitylab [Электронный ресурс] / 2009. – Режим доступа: http://www.securitylab.ru/, свободный. – Яз. рус.

Хусаинова Эльвира Робертовна – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, elechka.de@gmail.com

ёё