Международный некоммерческий образовательный интернет-проект Supercourse [1] представляет собой инициативу по созданию библиотеки бесплатных лекций в области здравоохранения. На сегодняшний день участниками проекта являются более 55000 ученых и врачей из 174 стран, разместившие уже более 3500 презентаций в формате PowerPoint на 26 языках мира. Многие лекции посвящены проблемам терроризма, биотерроризма, биологической, информационной и общей безопасности. В данном исследовании Supercourse рассматривался как сложная эволюционирующая структура, которая дополняет сеть традиционного соавторства. Аналогично [2] в качестве узлов рассматривались авторы лекций, которые также имеют связи — соавторство в традиционных изданиях. Изучались такие параметры, как плотность распределения числа связей участников проекта, диаметр, коэффициент кластеризации, размер максимального кластера. Установлено, что средний диаметр сети авторов без учета объединяющей базы Supercourse характеризуется достаточно малой величиной ~ 6, что объясняется не спецификой предметной области, но склонностью авторов данного интернет-проекта к сотрудничеству. Оценка уязвимости сети к случайным и целенаправленным (направленным на кластеры) (за исключением SUPERCOURSE-концентратора) атакам указывает на безусловную ее стойкость.

СПИСОК ЛИТЕРАТУРЫ:

1. http://www.pitt.edu/~super1/.
2. *Barabási A. L., Jeong H., Neda Z., Ravasz E., Schubert A., Vicsek T.* Evolution of the social network of scientific collaborations. Physica A 311. 2002. P. 590–614.

А. А. Долгин
Московский энергетический институт (технический университет)

ПРОЦЕСС АНАЛИЗА ЗАЩИЩЕННОСТИ КАК ЧАСТЬ МОДЕЛИ АДАПТИВНОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

В докладе рассмотрены модель адаптивной безопасности компьютерных систем и процесс анализа защищенности как ее часть. Практическим аспектом работы стало создание сканера уязвимостей системного уровня — DAScanner.

Снижение проблем в информационной безопасности требует адаптивного, высокочувствительного к изменениям, работающего в реальном режиме времени механизма. Модель адаптивной безопасности — именно такой подход, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Обеспечение безопасности в соответствии с данной моделью описывается как процесс, содержащий:

- технологию анализа защищенности (security assessment) или поиска уязвимостей (vulnerabilities assessment);
- технологию обнаружения атак (intrusion detection);
- адаптивный компонент, который включает в себя и расширяет две первые технологии.

Среди средств защиты сетей сканеры безопасности (системы анализа защищенности) занимают особое место. Во-первых, потому, что они могут быть как средством обеспечения безопасности, так и средством нападения. Во-вторых, далеко не во всех случаях очевидна польза от применения сканеров безопасности. Речь идет лишь о потенциальной возможности атаки, а не о свершившемся факте реализации угрозы. И, в-третьих, сканеры безопасности могут оказывать нежелательное влияние на объекты защиты.

Практическим результатом изучения систем анализа защищенности является сканер системного уровня DAScanner.

Достоинства сканирования на уровне операционной системы (системного сканирования) кроются в прямом доступе к низкоуровневым возможностям ОС хоста, конкретным сервисам и деталям конфигурации.

Отличительные особенности системного сканирования делятся на 3 категории:

- идентификация рисков деятельности пользователя;
- идентификация хакера и обнаружение атаки (внутренние и внешние хакеры);
- возможность осуществления проверок, которые являются невозможными или трудновыполнимыми сетевым сканером.

DAScanner — это сканер безопасности системного уровня, имеющий распределенную архитектуру клиент—сервер. Серверная часть устанавливается на сканируемые узлы сети и отвечает за сбор параметров безопасности. Она представляет собой системную службу операционной системы Windows. Клиентская часть отвечает за инициализацию сканирования, сбор результатов, их анализ и т. д. Клиентская часть представляет собой оконное приложение Windows.

Клиентская часть сканера собирает информацию с узлов и, сравнив ее с эталоном безопасности, делает вывод о защищенности системы. Эталон формируется пользователем и хранит информацию об условной «важности» тех или иных параметров безопасности, что позволяет получать количественную оценку защищенности.

Созданный сканер отвечает многим требованиям, которые предъявляются к коммерческим разработкам подобного рода, и имеет большой потенциал в качестве учебного пособия.

Как возможные пути развития сканера можно отметить:

- развитие системы отчетов;
- автоматическое устранение уязвимостей (система реагирования);
- расширение функционала для возможности проверок на соответствие какому-либо международному стандарту. Например, ISO 15408 (Общие критерии оценки безопасности информационных технологий).

СПИСОК ЛИТЕРАТУРЫ:

1. *Долгин А. А.* Новый сканер безопасности системного уровня для компьютерных систем на основе защищенных версий ОС Windows // Труды международной научно-технической конференции «Информационные средства и технологии». М., 2006. Том 3. С. 84–87.
2. *Хорев П. Б.* Методы и средства защиты информации в компьютерных системах. М.: Издательский центр «Академия», 2005. – 256 с.
3. *Бармен С.* Разработка правил информационной безопасности. М.: Вильямс, 2002. – 208 с.
4. *Лукацкий А. В.* Адаптивная безопасность сети // КомпьютерПресс. 1999. № 8.