системы RSA и родственных ей систем, основанных на сложности задачи факторизации, это не усиливает схему. В то же время для схем, основанных на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые позволяет существенно увеличить стойкость. Обусловлено это тем, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля. По указанной причине в настоящее время происходит массовый перевод асимметричных криптосистем, основанных на сложности задачи логарифмирования в дискретных полях, на эллиптические кривые.

КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОКОММУНИКАЦИЙ ОТ КИБЕР-УГРОЗ

А.Ю. Зинченко, В.Ю. Цветков, Алби Гарби Хушам Абдулхусейен Худайр

Спектр современных угроз информационной безопасности и время их проведения изменчив. Атаки осуществляются за минуты, в то время как обнаружение занимает недели и месяцы. Для противодействия угрозам разработана концепция, которая реализуется на всех элементах (сеть, мобильные устройства, виртуальны машины, облака и др.). Концепция состоит из следующих частей: действия до атаки (контроль, усиление), во время атаки (обнаружение, блокирование) и после (устранение). На каждом участке необходимо применять соответствующие технологии. Так, на участке до атаки необходимо применять такие технологии как: Firewall, App Control, VPN, IAM/NAC. Во время — IPS, Anti-Virus, Email/Web Security. После атаки — IDS, FPC, Forensics, SIEM. Важными составляющими данной концепции являются: корреляция угрозы с устройством в сети, и необходимость агрегирования многих источников данных для определения угрозы (определения атакующего и его цели). Данная возможность реализована посредством протокола NetFlow. В рамках данной концепции, защита сетевой среды должна состоять из трёх частей: глубокого просмотра в точках анализа (идентификация/блокировка приложений и файлов, траектория файлов), защита доступа к сети и инфраструктуре (видимость пользователей и устройств, авторизация), а также широкий обзор на всех сетевых уровнях (сбор данных по всему трафику, обнаружение подозрительной и аномальной активности). Поскольку все объекты соединяются друг с другом различными взаимоотношениями, образуя единый граф, концепция подразумевает изменение тактики защитника, в частности, переход от анализа списков, к анализу графов.

МЕТОДЫ И ПРОГРАММНЫЕ СРЕДСТВА ИНТЕРАКТИВНОЙ ВИЗУАЛИЗАЦИИ МЕХАТРОННЫХ СИСТЕМ

Г.А. Зубов, В.В. Поляковский

Целью исследования является анализ существующих средств и методов интерактивной визуализации трехмерных сцен, подходов к взаимодействию между объектами трехмерной сцены. В ходе работы были рассмотрены популярные программные системы моделирования, использующиеся в различных областях промышленности, а также применяемые в них подходы. Такой анализ позволит уточнить требования для разработки специализированной системы интерактивной визуализации, а также на раннем этапе выявить ошибки в реализации. Объектами исследования являются программные продукты, используемые на различных уровнях разработки трехмерных интерактивных сцен. Это, с одной стороны, и готовы продукты, различные CAD/CAM системы, так и программные библиотеки для разработки трехмерных графических приложений. Их недостатком является достаточно низкие возможности по модифицированию используемых трехмерных моделей. Среди наиболее популярных в конструировании графического программного обеспечения были рассмотрены такие программные библиотеки, как OpenGL, DirectX, XNA Framework. Все они достаточно функциональны для конструирования трехмерных сцен, но наибольшим удобством именно для интерактивных систем обладает XNA Framework.