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.

Таким образом, для проработки концепции будущей системы интерактивной визуализации было разработано приложение-прототип, которое моделирует мультипланарную систему на одном статоре, которое включает в себя интерактивную составляющую — пользовательский интерфейс, позволяющий задать траекторию движения для каждого позиционера в трехмерном пространстве и обрабатывающий коллизии позиционеров между собой.

Литература

1. *Samuel R. Buss.* 3D Computer Graphics: A Mathematical Introduction with OpenGL. Cambridge University Press, 2003.

СРЕДСТВА И АЛГОРИТМЫ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ

А.Д. Зайков, А.М. Кадан

В докладе представлен опыт работы с современным специализированным программным обеспечением для проведения компьютерно-технических экспертиз (КТЭ) при решении задач поиска и закрепления доказательств в сфере мультимедийного контента и графической информации.

Рассмотрены задачи КТЭ, включающие изучение следующих вопросов: о наличии на исследуемых объектах информации, относящейся к делу (в том числе, в неявном, удалённом, скрытом или зашифрованном виде); о возможности (пригодности) использования исследуемых объектов для определённых целей; о действиях, совершённых с использованием объектов; об идентификации найденных документов, мультимедийной информации, программ.

Выполнен сравнительный анализ возможностей и применения современных специализированных программных систем эксперта, поддерживающих всю технологическую цепочку проведения КТЭ: EnCase, AsccessData Forensic Toolkit, Defacto AccessData, Password Recovery Toolkit, Adroit Photo Forensics, Amped Authenticate. Инструментами Image Error Level Analysis выполнена экспертная оценка графической информации. В результате работы выявлено и доказано наличие «дорисованных» областей на анализируемой базе изображений, а также отмечены документы с редактированием злоумышленником и вставленными новыми областями в ряд доказательных фотографий. Программное обеспечение позволило эффективно определить даже самые мелкие неоригинальные детали в графической информации, которые практически невозможно увидеть невооруженным глазом.

Определен класс задач, которые требуют разработки специальных алгоритмов, не реализованных существующими программными средствами и пути их решения.

МУЛЬТИАРБИТРАЛЬНАЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ДЛЯ ПЛИС

В.П. Клыбик, А.А. Иванюк

ФНФ (от англ. PUF — Physically Unclonable Function) эффективны для неклонируемой идентификации и аутентификации цифровых устройств на ПЛИС — программируемых логических интегральных схемах. Цифровые ФНФ основаны на отклонениях в задержках распространения сигналов по путям, обусловленных незначительными девиациями в физической структуре при изготовлении ПЛИС. Для измерения отклонений в задержках распространения сигналов применяется множество типов ФНФ, в частности ФНФ типа арбитр (АФНФ).

Проблемами реализации АФНФ на ПЛИС являются обеспечение симметричности путей распространения сигнала и стабильности ответов, обусловленные заведомой асимметрией конфигурируемых ресурсов ПЛИС. Для решения описанных проблем используются следующие подходы: пространственная локализация критичных доменов в одном структурном блоке ПЛИС; введение в схемы путей сигналов элементов конфигурируемой задержки; использование состояния метастабильности арбитра в качестве