ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ ДАННЫХ. СОВРЕМЕННЫЕ ПРОБЛЕМЫ РОБОТОТЕХНИКИ

УДК 004.021

МЕТОДЫ ГЕНЕРИРОВАНИЯ ДОВЕРЕННОЙ ЦИФРОВОЙ ПОДПИСИ

Бурич А.Ю.
УО «Белорусский государственный университет информатики и радиоэлектроники», г. Минск
Научный руководитель – Ярмолик С.В., к.т.н.

Введение

Доверенная цифровая подпись является модификацией цифровой подписи, которая отвечает специфичным требованиям. В схемах доверенной подписи один пользователь, называемый оригинальным подписывающим лицом, может делегировать права и возможности подписи документа другому пользователю, называемому доверенным подписывающим.

В данной работе приведены ключевые понятия, использующиеся в схемах доверенной подписи для последующей реализации и сравнения результатов, полученных теоретически и практически.

Основная часть

При реализации схемы доверенной подписи необходимо обеспечить следующие характеристики:

- различимость. Любой желающий проверить подпись должен иметь возможность определить, что подпись сделана доверенным лицом, а не оригинальным подписывающим;
- невозможность подделывания. Возможность генерирования действительной цифровой подписи должна быть только у пользователя, делегировавшего полномочия, и у его доверенного лица;
- проверяемость. Проверяющее лицо по доверенной подписи может убедиться, что подписывающий ознакомлен и согласен с содержанием документа;
- идентифицируемость. Возможность определения подписавшее лицо по подписи;
- неотрицаемость. Доверенное лицо, подписавшее документ, не может оспорить факта подписи документа.

Однако при реализации определенной схемы доверенной подписи допускается некоторое отхождение от описанных характеристик, в зависимости от того, какой тип делегирования был выбран. Для различных схем используются следующие типы делегирования:

- Полное делегирование. Оригинальный подписывающий передает доверенному лицу свой секретный ключ. В таком случае различия между доверенным и оригинальным подписывающими не возникает.
- Частичное делегирование. Оригинальный подписывающий не передает доверенному лицу секретный ключ. Вместо этого, он из секретного ключа получает доверенный ключ и передает доверенному лицу. Доверенное лицо на основании доверенного ключа генерирует подпись.
- Делегирование по доверенности. Доверенному лицу выдается доверенность, содержащая некоторую информацию о доверенном подписывающем, на основании которой доверенное лицо генерирует ключ и подписывает документ.

- Частичное делегирование по доверенности. Доверенному лицу выдается ключ, сгенерированный на основании секретного ключа оригинального подписывающего и доверенности.

Процесс подписи документа с использованием схем доверенной подписи зачастую состоит из четырех этапов:

- настройка системы. Данный этап заключается в установке публичных или приватных параметров пользователей;

- генерирование подписи. На данном этапе генерируется подпись для подписи документа;

- подпись документа. Непосредственно встраивание сгенерированной подписи в документ;

- проверка. На данном этапе происходит проверка подлинности подписи, подтверждение доверенности подписи и пр.

Заключение

В настоящее время существует достаточное количество реализаций схем доверенной подписи, которые отличаются типами делегирования, алгоритмами генерирования и подписи документов. Каждая реализация может использоваться в зависимости конкретных потребностей пользователей в быстродействии или криптографической стойкости, а также могут быть предложены новые модификации.

Список цитированных источников

1. Proxy signatures: Delegation of the power to sign messages/M.Mambo, K.Usuda, E.Okamoto. IEICE Transactions Fundamentals. – Vol. E79A, 1997.

2. Designated-Verifier Proxy Signature Schemes / G. Wang. Security and Privacy in the Age of Ubiquitous Computing (IFIP/SEC 2005). – Springer, 2005.

УДК 004.8.032.26

СИСТЕМА УПРАВЛЕНИЯ ТРАНСПОРТОМ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Войцехович О.Ю.

УО «Брестский государственный технический университет», г. Брест

Научный руководитель – Шуть В.Н., доцент, к.т.н.

1. Постановка задачи

Задача состоит в разработке адаптивной системы управления транспортом, работающей в режиме реального времени вдоль городской магистрали, способной координировать светофоры для улучшения дорожной ситуации в целом. Еще одна задача состоит в моделировании, тестировании и оценке разработанной системы.

Для решения поставленной задачи предложен подход, координирующий время горения сигналов светофоров путем распознания и предсказания движения групп транспортных средств (пачек) на магистрали и прилегающих к ней улицах с помощью полученных с детекторов и отфильтрованных данных. Для тестирования разработанного подхода в управлении транспортом была реализована имитационная модель.

2. Описание системы

Адаптивная система управления состоит из 3 частей: предсказание прибытий и очередей (обрабатывает данные с детектора и осуществляет предсказание); система принятия