Universitatea Tehnică a Moldovei

PROIECTAREA SISTEMULUI INFORMAȚIONAL PENTRU ASIGURAREA SERVICIULUI ELECTRONIC "TIMESTAMP"

Student:

Boișteanu Vladimir

Conducător:

conf.univ.dr. Pușneac Iurie

Chişinău - 2019

Ministerul Educaţiei al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat „Securitatea informației în sisteme și rețele de comunicații”

Admis la susţinere
Şef departament: dr. P. Nicolaev

„_” ___________ 2020

PROIECTAREA SISTEMULUI INFORMAŢIONAL PENTRU ASIGURAREA SERVICIULUI ELECTRONIC “TIMESTAMP”

Teză de master

Masterand: ___________ (Boișteanu Vladimir)
Conducător: ___________ (Pușneac Iurie)
Colaborator: ___________ (Tatiana Șestacova)

Chişinău – 2019

REZUMAT

Lucrarea este dedicată proiectării unui sistem informațional pentru furnizarea de servicii electronice „timestamp”.

A fost efectuata analiza componentelor sistemelor informatice moderne pentru furnizarea serviciului „timestamp”. Sunt prezentată schema generală a sistemului informațional și principalele sale componente. A fost analizată actualitatea serviciului „timestamp” și utilizarea acestuia în tehnologia informației (notar electronic, licitație, ofertă electronică etc.).

A fost dezvoltat un set de scripturi pentru instalarea și verificarea timbrelor de timp folosind biblioteca OpenSSL. A fost executat un exemplu care ilustrează instalarea și verificarea cronometrului.

SUMMARY

The master thesis is dedicated to the elaboration of an information system for the provision of electronic services "timestamp".

The analysis of the components of modern information systems for the provision of the service "timestamp" is carried out. The general scheme of the information system and its main components are presented. The relevance of the "timestamp" service and its use in information technology (electronic notary, tender, auction, etc.) is analyzed.

A set of scripts has been developed for the installation and verification of time stamps using the OpenSSL library. An example is executed for illustrating the installation and verification of the timestamp.

Р Е З Ю М Е

Работа посвящена проектированию информационной системы предоставления электронной услуги “метка времени”.

Проведён анализ компонентов современных информационных систем предоставления услуги ”метка времени”. Представлена общая схема информационной системы и ее основные компоненты. Проанализирована актуальность услуги “метка времени” и ее использование в информационных технологиях (электронный нотариус, тендер, аукцион и др.)

Разработан набор скриптов для осуществления установки и верификации метки времени используя библиотеку OpenSSL. Выполнен пример, иллюстрирующий установку и верификацию метки времени.

СОДЕРЖАНИЕ

Введение

В данной работе описаны принципы и этапы разработки информационной системы для предоставления электронной услуги ”метка времени”.

Актуальность темы.

Цифровая экономика стремительно вытесняет старый уклад во всех сферах деятельности современного общества. Трансформируется частная жизнь и рабочие места, появляются новые профессии и инструменты взаимодействия. В эпоху столь масштабных преобразований всё большую актуальность принимает проблема информационной безопасности в организациях.

Интернет – есть уязвимая среда, поскольку он представляет собой систему(сеть) общего доступа. И наше сообщение может попасть в зону влияния злоумышленника.

Существуют следующие угрозы:

- Чтение чужого сообщения;
- Редактирование чужого сообщения;
- Подмена сообщения;
- Фабрикация сообщения от другого лица;
- Отказ от факта отправки сообщения;
- Отказ от факта получения сообщения;
- Наблюдения за трафиком чужих сообщений;
- Перенаправление сообщения другому адресату;
- Угрозы связанные со временем (задержка, повторное использование);
- Уничтожение сообщения;

Любое сообщение, отправляемое по сети должно рассматриваться либо как неизбежно проходящее через злоумышленника, либо как посланное им.

Безопасность – полное отсутствие опасности. В реальной жизни такого не бывает, поэтому мы можем говорить о мерах минимизации ущерба от угроз.

Для предотвращения угроз используются сервисы информационной безопасности.

Существуют следующие элементы/сервисы:

- Конфиденциальность – с помощью этого сервиса сообщение становится непонятным/нечитаемым для посторонних;

- Достоверность – с помощью этого сервиса мы показываем то, что сообщение пришло из нужного/достоверного источника;
- Целостность - с помощью этого сервиса мы показываем то, что сообщение не изменялось при передаче;
- Неотрекаемость при отправке - с помощью этого сервиса мы не даём источнику сообщения возможность отказаться от факта отправки сообщения;
- Неотрекаемость при получении - с помощью этого сервиса мы не даём получателю сообщения возможность отказаться от факта получения сообщения;
- Анонимность - с помощью этого сервиса мы даем отправителю/получателю сообщения возможность скрыть свою сущность/личность;
- Своевременность - с помощью этого сервиса мы можем проверить пришло ли сообщение вовремя;
- Доступность - с помощью этого сервиса мы обеспечиваем невозможность уничтожения сообщения;

Всего этого нам позволят достичь следующие криптографические механизмы/инструменты защиты:

- Шифрование;
- Цифровая подпись;
- Хэширование;
- Метка времени;

Временная метка - это последовательность символов или закодированной информации, показывающей, когда произошло определённое событие. Обычно показывает дату и время (иногда с точностью до долей секунд).

Термин пришёл от сургучных печатей, используемых в офисах / на почте, чтобы отпечатать текущую дату (иногда и время) в подписи бумажных документов или записать, когда документ был принят. Типичные примеры метки времени — штемпель на письме.

Сейчас использование термина расширилось на цифровую информацию. Например, компьютерные файлы содержат метки, показывающие, когда последний раз меняли файл; цифровые камеры добавляют временные метки к изображениям.

Электронная отметка — это способ достоверно следить за временем создания и модификации документа. "Достоверно" здесь значит, что никто, даже владелец этого документа, не в состоянии изменить однажды созданную информацию так, чтоб её целостность не нарушилась. Административная сторона включает прозрачную сборку управления отметками времени, их создание и обновление.

Защищённая отметка времени — это отметка, выданная при свидетелях. Trusted third party (TTP) ведёт себя как timestamping authority (TSA). Это используется для подтверждения существования определённых данных до определённого момента времени (контракты, данные исследования, медицинские записи и т. п.) без возможности дописывания задним числом. Сложные TSA могут использоваться для повышения надёжности и уменьшения уязвимости.

Ориентирование на создание собственной такой системы, которая позволит обеспечить достоверность электронного документа на определённый момент времени и определяет **актуальность** данной разработки.

Целью данного проекта является разработка информационной системы предоставляющей электронную услугу ”метка времени” на основе библиотеки OpenSSL.

Для достижения поставленной цели необходимо решить следующие ***задачи***:

1. Провести анализ информационных систем и сервисов, предоставляющих электронную услугу ”метка времени”;
2. Разработать общую схему информационной системы предоставления электронной услуги ”метка времени”;
3. Определить набор требований и выбрать сервер времени;
4. Изучить протокол раздачи точного времени в локальной сети и протокол штампа времени;
5. Разработать набор скриптов, для реализации примера установки и верификации метки времени используя библиотеку OpenSSL;

Библиография

1. https://ru.wikipedia.org/wiki/Временная_метка - ***Метка времени***
2. https://www.freetsa.org/index_en.php - ***Provider of a free Time Stamp Authority***
3. http://xgu.ru/wiki/OpenSSL - ***Универсальный криптографический инструмент***
4. http://citforum.ru/security/cryptography/openssl/ - ***Основы работы с OpenSSL***
5. https://hightech.fm/2019/01/17/atomic-hour - ***Как работает самый точный и малопонятный прибор для измерения времени***
6. https://hi-news.ru/technology/kak-rabotayut-atomnye-chasy.html - ***Как работают атомные часы***
7. https://www.ntp-servers.net - ***Серверы точного времени***
8. https://tools.ietf.org/html/rfc3161 - ***Time stamp protocol***
9. https://www.ntp-servers.net/ntp.html - ***Network time protocol***
10. https://www.mobatime.ru/index.php?option=com_content&task=view&id=239&Itemid=26 - ***Точное время в интернете***
11. https://it.wikireading.ru/60103 - ***Защищенное предоставление меток времени***
12. https://it.wikireading.ru/60104 - ***Нотариус PKI***