Информационная безопасность

Контрольные суммы

Солдатов А. Е.

Содержание

Список иллюстраций

Список таблиц

1 Цели и задачи

Целью данной презентации является разобраться в понятии контрольных сумм и узнать для чего они нужны.

1.1 Что такое контрольная сумма?

Контрольные суммы представляют собой метод проверки целостности данных, который используется для обнаружения ошибок, возникающих при передаче или хранении информации. Это простая, но мощная техника, обеспечивающая высокую надежность передачи данных. Контрольные суммы рассчитываются с использованием различных алгоритмов, которые генерируют небольшое значение, зависящее от всех битов исходных данных. При передаче или хранении это значение сохраняется вместе с данными. При получении данных контрольная сумма пересчитывается и сравнивается с переданной, что позволяет выявить возможные ошибки.

1.2 Жизненная ситуация

Представьте ситуацию: вы приходите в магазин за наушниками. Находите нужные на витрине, пробуете их, вам всё нравится. Вы просите продавца принести такие же со склада, в упаковке.

Продавец приносит коробку, и вы понимаете, что вас хотят обмануть. Упаковку явно до этого вскрывали, в комплекте не все провода и накладки, плёночки сняты.

Этими наушниками явно пользовались до вас.

Сотрудник говорит, что это ошибка в списке комплектности, а товар на самом деле новый, просто такой пришёл с завода. Вы ему не верите, отказываетесь от покупки и идёте в другой магазин. Там вы находите такие же наушники, проверяете и радуетесь, что купили нужную вещь.

В мире информации происходит почти то же самое: товар на складе — это какие-то данные, а список комплектности товара — это контрольная сумма, которая показывает, изменялись эти данные или нет. Если понимать, что это такое и как этим пользоваться, можно проверить подлинность файла и обезопасить себя от подделок, вирусов и шпионов.

1.3 Checksum (контрольная сумма)

Описание: Простая контрольная сумма представляет собой сумму всех байтов данных, часто ограниченную определенной длиной (например, 8 или 16 бит). Этот метод широко применяется благодаря своей простоте и скорости.

Применение: Контрольные суммы используются в простых протоколах передачи данных, таких как XMODEM, а также в базовых системах контроля целостности данных, например, в микроконтроллерах и других встроенных системах.

1.4 LRC (Longitudinal Redundancy Check)

Описание: LRC представляет собой побитную или побайтную контрольную сумму, которая рассчитывается по каждому столбцу блока данных. Этот метод используется для улучшения обнаружения ошибок в многобайтовых данных.

Применение: LRC применяется в телекоммуникациях и различных протоколах передачи данных, таких как последовательные интерфейсы и системы сжатия данных, для обеспечения надежности и целостности передаваемой информации.

1.5 CRC-16-CCITT

Описание: CRC-16-CCITT — это 16-битная контрольная сумма, широко применяемая в телекоммуникациях и мобильных системах.

Применение: Используется в протоколах HDLC, Bluetooth, и в GSM-сетях для обеспечения целостности передачи данных.

1.6 CRC-32

Описание: CRC-32 — это 32-битная контрольная сумма, которая используется в различных цифровых системах для обеспечения надежности данных.

Применение: Широко используется в Ethernet, ZIP-архивах, файловых системах и других приложениях, требующих высокой надежности передачи данных.

1.7 CRC-64-ISO

Описание: CRC-64-ISO — это 64-битная контрольная сумма, использующаяся для высоконадежной проверки целостности данных. CRC (Cyclic Redundancy Check) алгоритмы являются одними из самых надежных и часто применяемых.

Применение: CRC-64-ISO применяется в системах хранения данных и телекоммуникационных стандартах, таких как сети высокой надежности и системы архивирования данных, где требуется высокая степень защиты от ошибок.

2 Итоги

1. Зачем нужны контрольные суммы?

Контрольные суммы необходимы для обнаружения и исправления ошибок, возникающих при передаче или хранении данных. Они обеспечивают целостность данных и минимизируют вероятность ошибок.

2. Какой тип контрольной суммы выбрать?

Выбор типа контрольной суммы зависит от конкретных требований приложения: от простых и быстрых методов, таких как Parity bit и LRC, до более сложных и надежных, как CRC, в зависимости от размера данных и уровня требуемой защиты.

3. Могут ли использоваться несколько типов контрольных сумм одновременно?

Да, в некоторых системах используются комбинированные методы для повышения надежности обнаружения ошибок. Например, LRC может применяться вместе с более простыми методами, такими как Parity bit, для обеспечения дополнительной защиты данных.

4. В каких областях применяются контрольные суммы?

Контрольные суммы широко используются в сетевых протоколах, базах данных, файловых системах, телекоммуникационных сетях и других областях, где критична надежность передачи данных.

3 Выводы

Разобрались в понятии контрольных сумм и узнали для чего они нужны.