Криптографические протоколы

Протоколы WEP, WPA, WPA2, WPA3

Деркач Максим Юрьевич

December 11, 2019

Ссылки

https://www.cs.jhu.edu/~Eastubble/dss/ae.pdf
http://cseweb.ucsd.edu/~mihir/papers/oem.pdf
https://habr.com/en/post/425637/

Введение

WEP (Wired Equivalent Privacy) - один из старейших протоколов безопасности, который может использовать WiFi-маршрутизатор, и он не очень безопасный. Он был использован в 1990-х годах, но с тех пор были разработаны другие протоколы безопасности.

WPA (Wi-Fi Protected Access) - это протокол, который первоначально заменило WEP как более безопасный способ хранения данных. В то время он был не идеален, но он лучше, чем WEP. Весь смысл разработки этого протокола состоял в том, чтобы преодолеть некоторые из основных недостатков WEP.

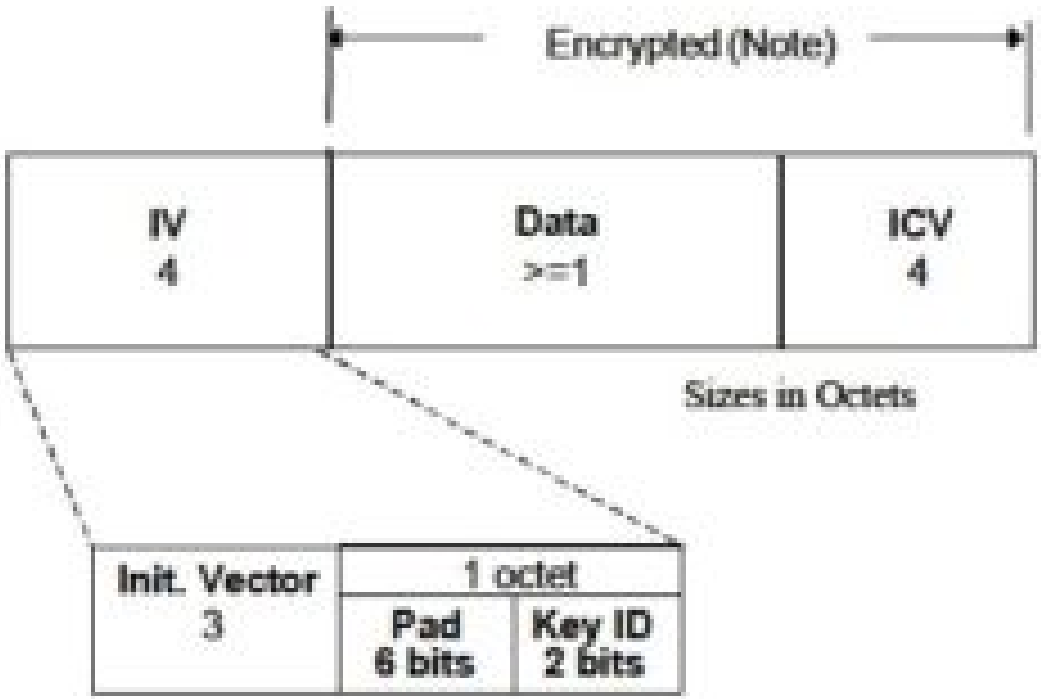
WEP

В основе WEP лежит поточный шифр **RC4**, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется **CRC32**.

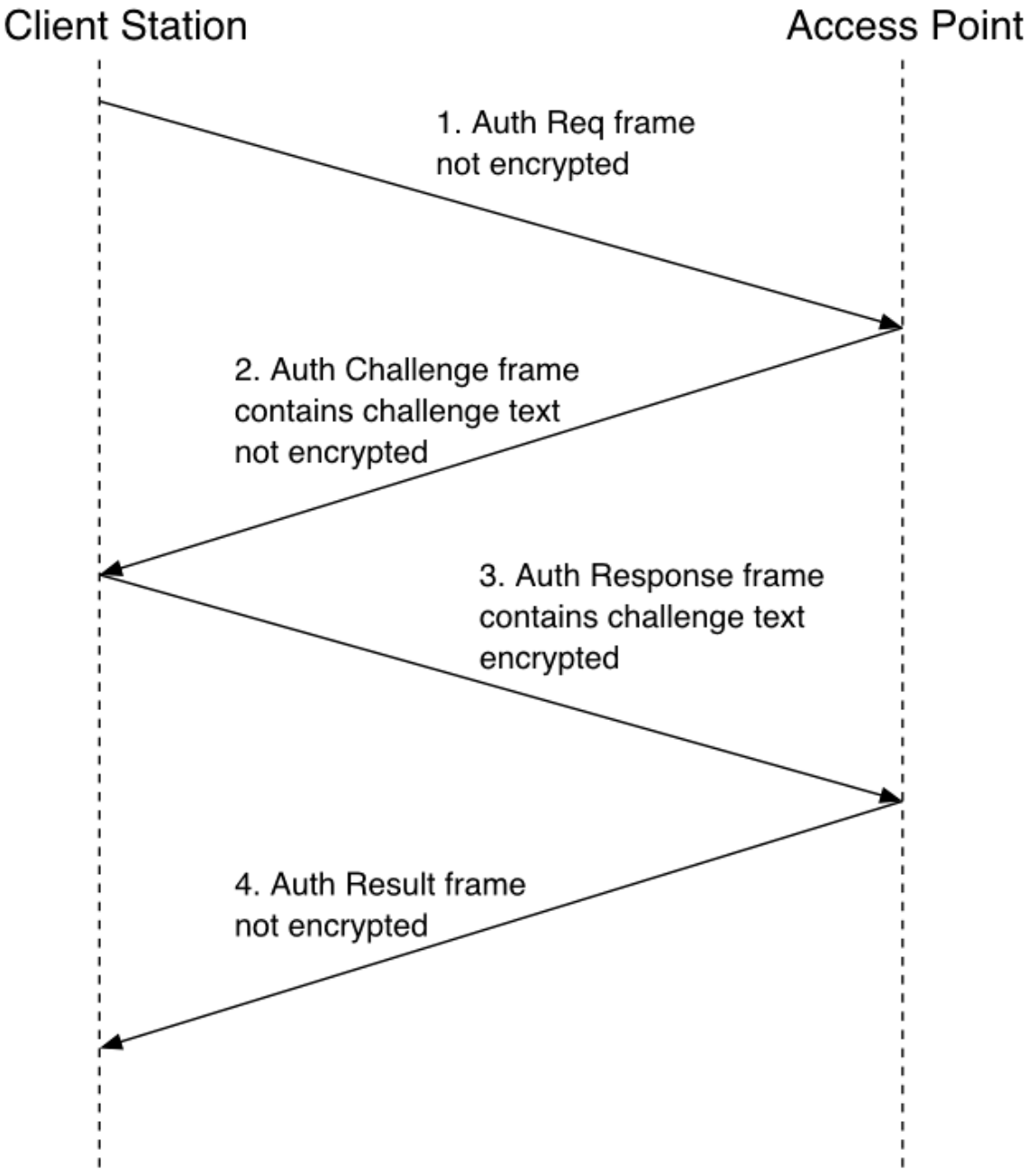
WEP

Пакет WEP протокола состоит из 2 частей:

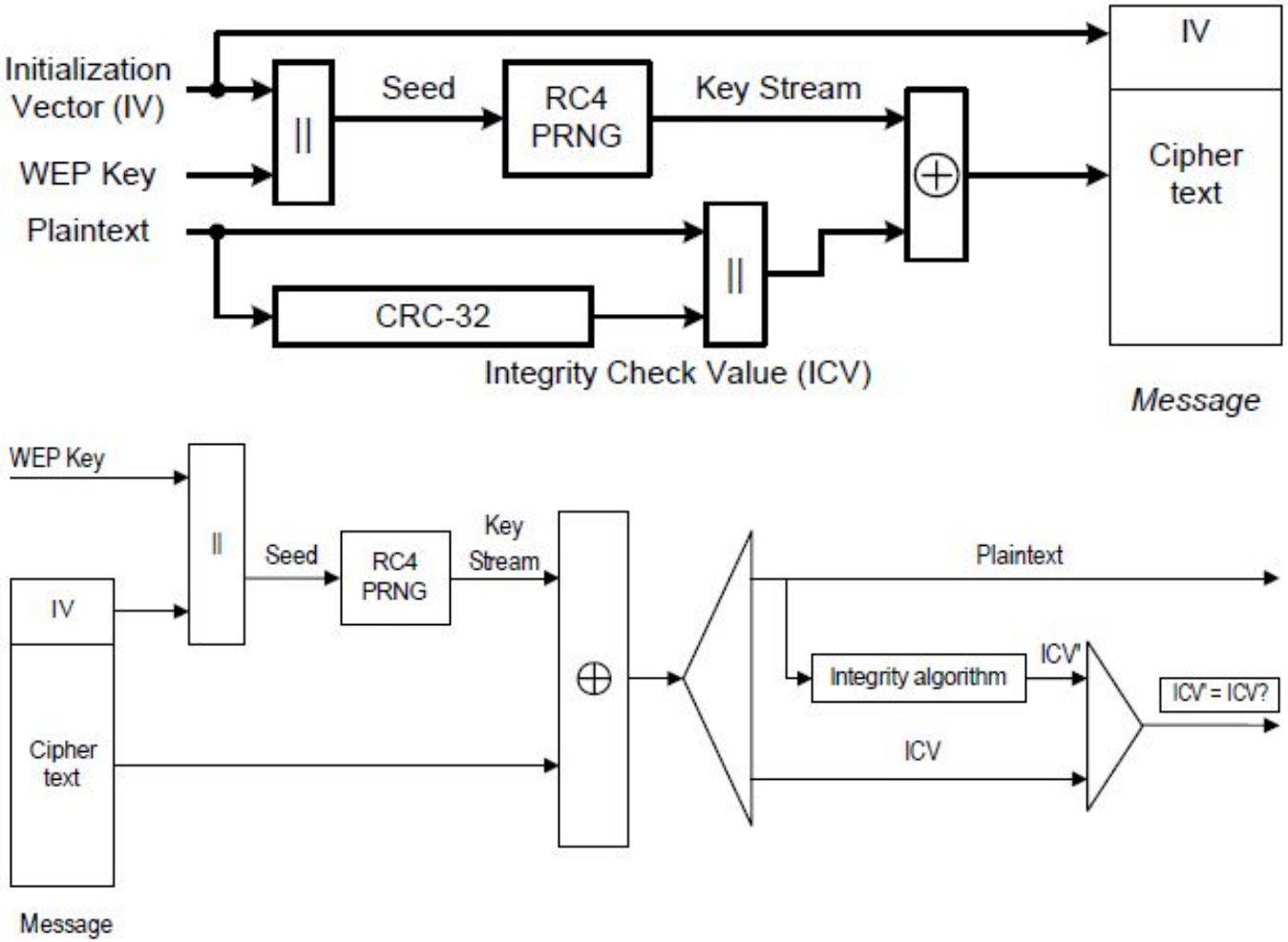
1. Открытые данные:
   - 1.1 Синхропосылка (IV) - 3 байта;
   - 1.2 Пустое место (Padding) - 6 бит;
   - 1.3 Идентификатор ключа (Key ID) - 2 бит;
2. Зашифрованные данные:
   - 2.1 Данные
   - 2.2 Контрольная сумма



WEP Auth Protocol



WEP Encryption and Decryption



WEP Security

В протоколе WEP есть множество слабых мест:

1. механизмы обмена ключами и проверки целостности данных:
   - В качестве MAC функции в WEP используется некриптографический алгоритм CRC.
2. малая разрядность ключа и вектора инициализации:
   - Повторное использование IV создает идентичные ключевые потоки, и поскольку длина IV мала, это гарантирует, что IV повторится через относительно короткое время (5-7 часов) в загруженной сети.
   - Стандарт 802.11 не описывал ограничения и правила на генерацию IV. Поэтому некоторые производители беспроводных адаптеров генерировали одинаковые последовательности IV, постоянное IV. В результате хакеры могли записывать сетевой трафик, определять поток ключей и использовать его для расшифровки зашифрованного текста.
3. способ аутентификации;
4. алгоритм шифрования.