Улучшение безопасности sources.list в дистрибутивах, использующих APT

Опция "signed-by" привязывает доверенный публичный ключ к репозиторию, что блокирует установку ПО в случае, если InRelease подписан другим ключом. Опция может быть установлена как в fingerprint ключа, так и в форме пути к файлу.

Это позволяет защититься от некоторых атак в следующей модели угроз:

1. допустим, что есть репозиторий, доступный по скомпрометированному каналу, чей приватный ключ не может быть скомпрометирован;

2. допустим, что есть репозиторий, доступный по безопасному каналу, чей приватный ключ был скомпромитирован;

3. оба репозитория прописаны в sources.list и оба ключа добавлены в доверенные.

Тогда, если нет привязки, злоумышленник может использовать скомпрометированный ключ второго репозитория для подписи поддельного InRelease для первого репозитория, получая RCE.

Поэтому в https://wiki.debian.org/DebianRepository/UseThirdParty рекомендуется прописывать всем сторонним репозиториям "signed-by", при этом указано использовать путь к ключу вместо fingerprint-а.

По моему мнению, имеет смысл прописывать signed-by вообще всем репозиториям.

В дистрибутивах, использующих APT, почему-то по умолчанию не используется опция signed-by. В инструкциях по подключению других репозиториев тоже почти никогда не встречаются указания её использовать.

Так как ручная идентификация ключей для каждого репозитория - дело трудоёмкое, был подготовлен скрипт, разбирающий sources.list, автоматически идентифицирующий fingerprint-ы и файлы ключей для каждого репозитория и выдающий модифицированный sources.list для сравнения с оригинальным.

В скрипте используется собственная библиотека для парсинга и сериализации sources.list на основе грамматики для parglare.