SecureShare

Team Ninja
Harshal Mahangare and Douglas Choi

Introduction

This an Android WifiDirect peer-to-peer file transfer application.

This app will be able to host a secure peer group for file transfer, allow other devices to connect, and securely transfer files within the peer group.

Setup

Language: Java

IDE: Android Studio

Cryptography Library: Bouncy Castle

Adversary

CCA in presence of eavesdropper - cannot view the files that are transferred.

Man-in-the-middle attack

Implementation - WifiDirect

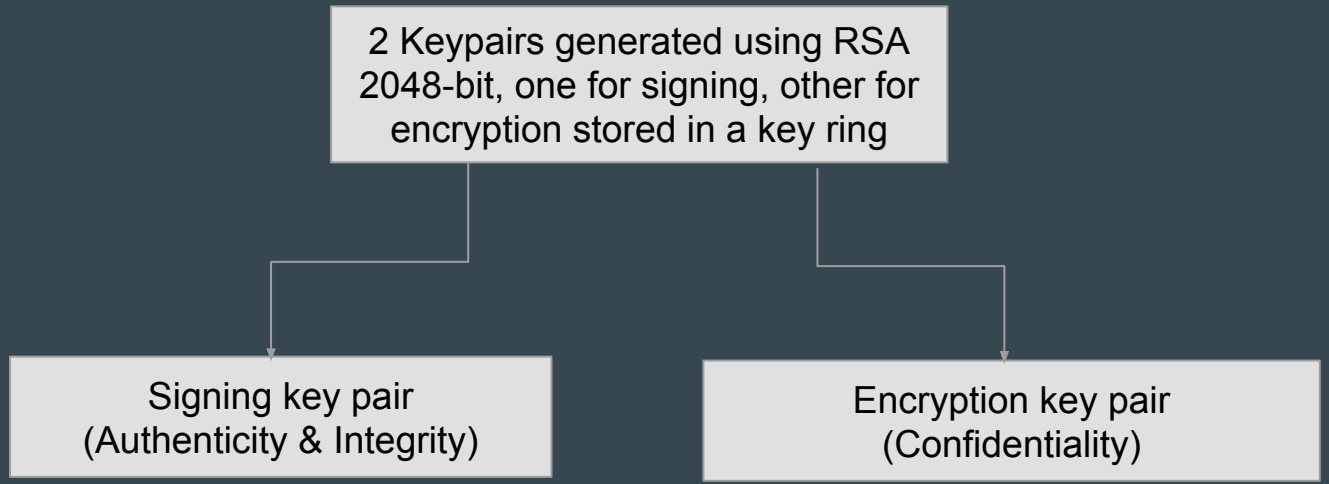
- Host creates group, makes himself WifiDirect discoverable
- Peer discovers WifiDirect host
- Peer attempts to connect to host via WifiDirect
- Host can accept connection and creates open socket on a new thread
- Host and peer exchange public key
- Now, host and peer can send files through the open socket
- Within the group, the host manages multiple threads - one for each client

Security Implementation

Pretty Good Privacy (PGP) is a hybrid encryption standard to support message confidentiality, message authentication, and integrity checking.

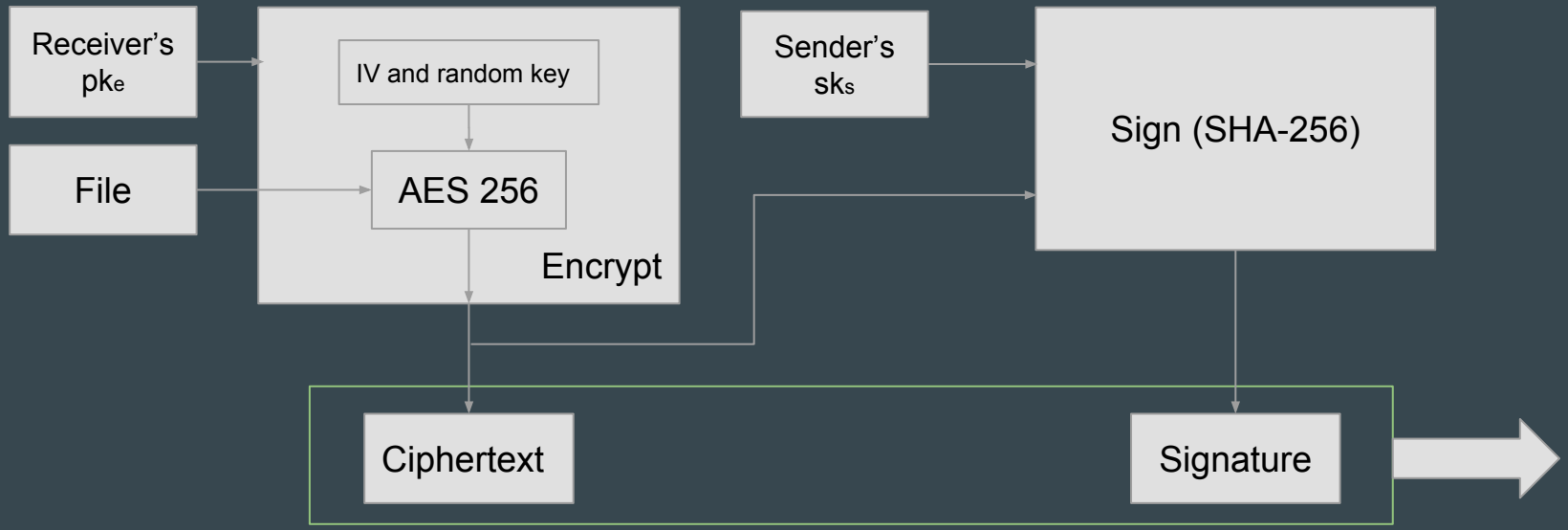
Used the OpenPGP implementation in Bouncycastle

Key Generation



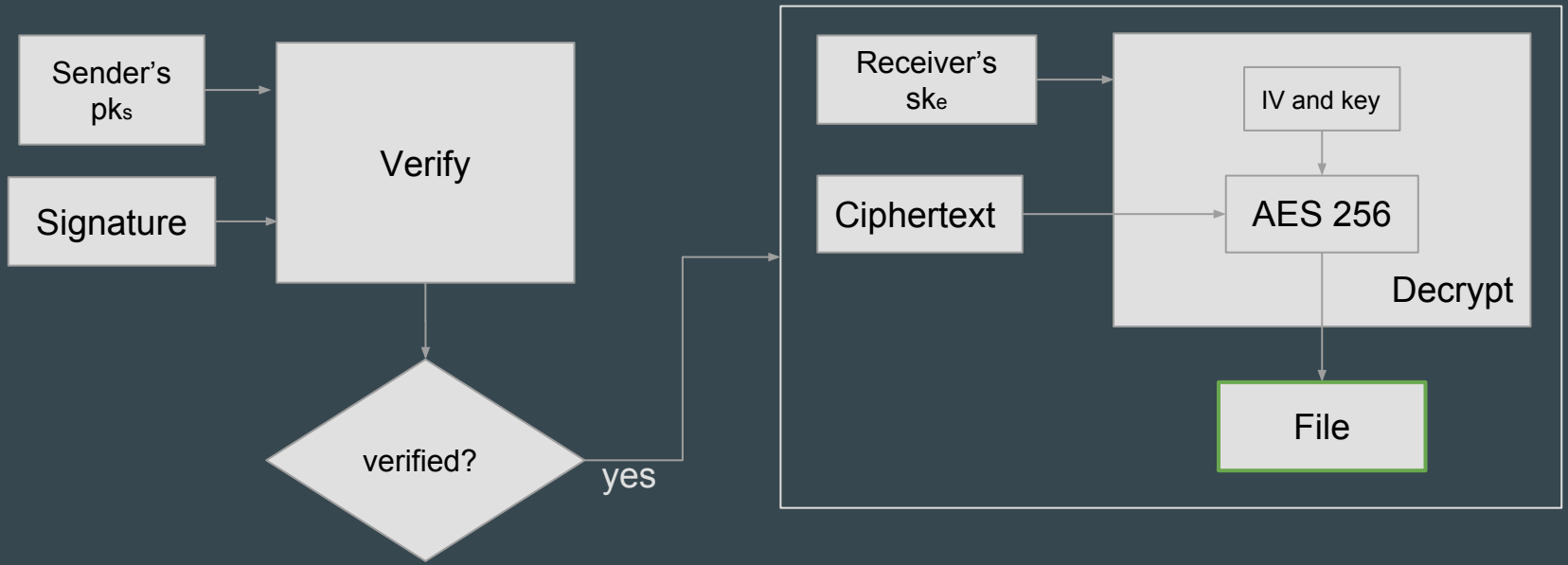
How we use PGP

1. Encryption and signing

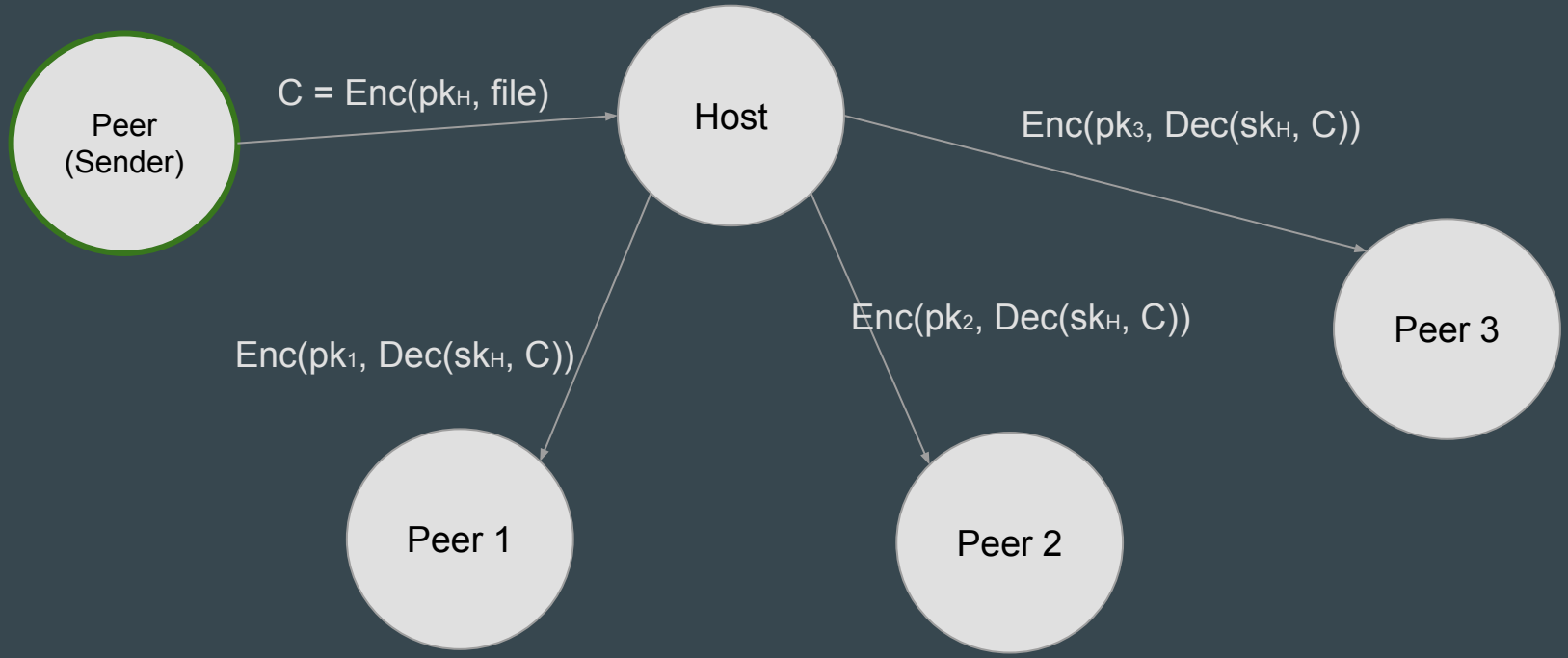


How we use PGP

2. Verification and decryption



Group Management



Demo

Future Improvements

Join peers and transfer public keys using NFC

Securely store files within the app on the devices.

Questions?

Backup

Attacks

Chosen-Ciphertext Attack against (less successful if data is compressed before encryption) [1]

The attacker may attempt to compromise a user's pass-phrase, gain access to the location of a user's private key or may deceive others by distributing fake or compromised public keys, etc.

- should not store the private key file on any machine that they do not have complete physical control over

Users must be able to trust that a public key really belongs to whom it appears

- A trusted centralized key server or Certificate Authority (CA)

When a file is deleted only the file allocation information changes and the file contents still reside on the disk until that space is overwritten by another file