Security & Privacy for Mobile Phones

Carybé, Lucas Helfstein

July 4, 2017

Instituto de Matemática e Estatística - USP

What is security?

Security is ... a System!

- That assures you the integrity and authenticity of an information as well as its authors;

Security is ... a System!

- That assures you the integrity and authenticity of an information as well as its authors;
- That grants the information you provide the assurances above;

Security is ... a System!

- That assures you the integrity and authenticity of an information as well as its authors;
- That grants the information you provide the assurances above;
- That ensures that every individual in this system knows each other;

Security is ... a System!

- That assures you the integrity and authenticity of an information as well as its authors;
- That grants the information you provide the assurances above;
- That ensures that every individual in this system knows each other;
- That tries to keep the above promises forever.

Security is ... a System!

Security is ... Cryptography!

Security is ... Impossible!

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.

Gene Spafford

What is privacy?

Privacy is ...

Privacy is ...

A too-broad-to-handle-in-this-presentation concept

Can I achieve anything close to this?

Threat Modeling

There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government.

Bruce Schneier

Threat Modeling

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;
5. It must be portable, and should not require several persons to handle or operate;

Kerckhoffs' Principles (1883)

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;
5. It must be portable, and should not require several persons to handle or operate;
6. (...) the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Linus Law

Given enough eyeballs, all bugs are shallow

Linus Law

Given enough eyeballs, all bugs are shallow

Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone.

Linus Law

Given enough eyeballs, all bugs are shallow

Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone.

Code audit = more security!

Linus Law

Given enough eyeballs, all bugs are shallow

Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone.

Code audit = more security!

Open Source Software

Apps

FLOSS

It would be cool if there was a way to make sure that most of my softwares are Open Source.

FLOSS

It would be cool if there was a way to make sure that most of my softwares are Open Source.

Better yet would be if they where FLOSS (Free Libre Open Source Software), since I'm a curious broke CS student.

FLOSS

It would be cool if there was a way to make sure that most of my softwares are Open Source.

Better yet would be if they where FLOSS (Free Libre Open Source Software), since I'm a curious broke CS student.

F-Droid is a FLOSS apk store!

Guardian Project

- FLOSS;
- Response to NSA revelations;
- anonymity through Orbot (Tor) + Orfox (Firefox proxied), ObscuraCam;
- security through Pixelknot (encrypted stenography), Chatsecure (XMPP + OTR) *(see Communication Subsection next)*;

Permissions

I don’t expect an overnight change of all desktops to what the US Military used to call B3 level security. And even that would not stop users from shooting themselves into the foot.

Wietse Venema

Permissions

- Hacker’s Keyboard;
- AppOps;
- Intent Intercept;
- Open Street Map based GPS.

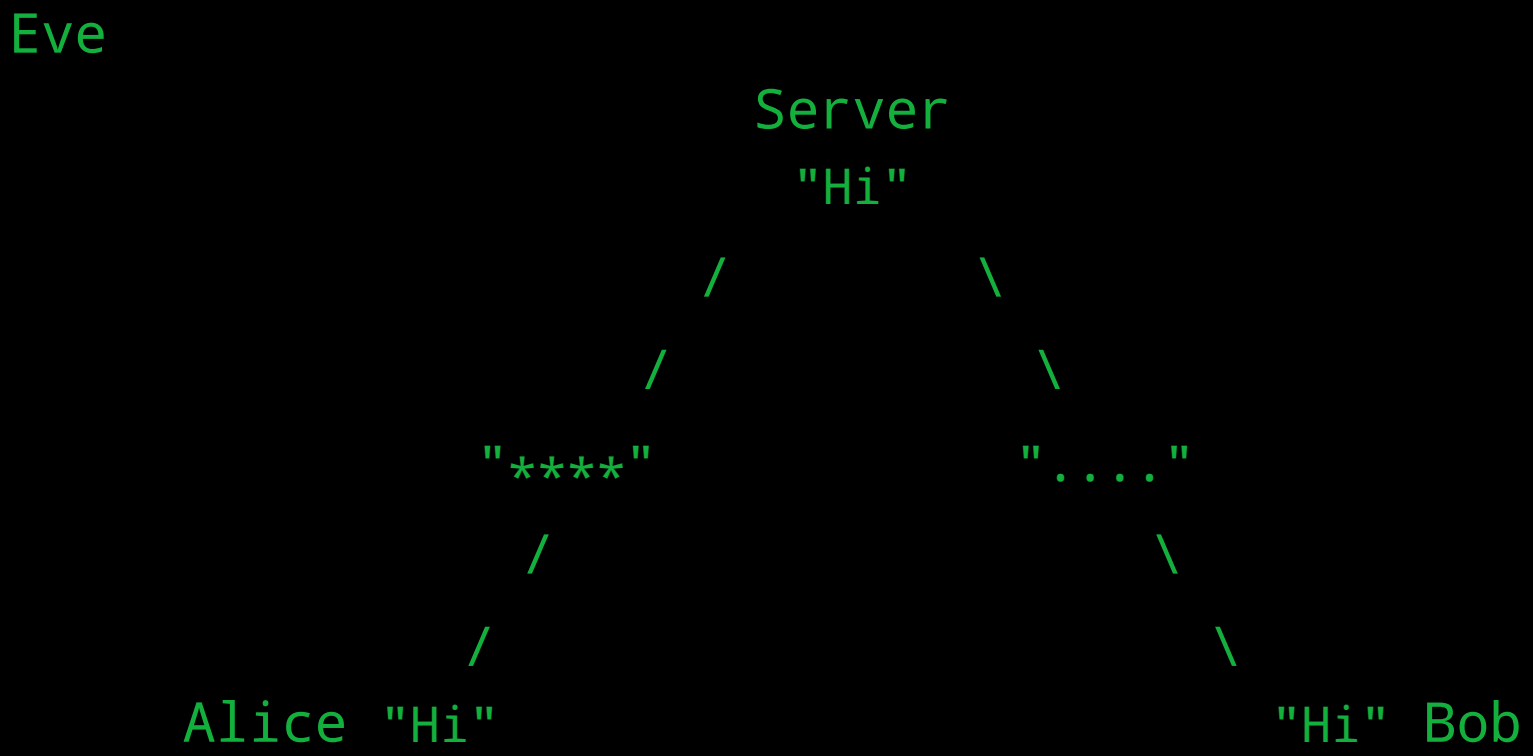
Anonymity

- Orbot (Tor) + Orfox (Proxied Firefox)
  - if root: AFWall+ (firewall)
- ObscuraCam;
- I2P

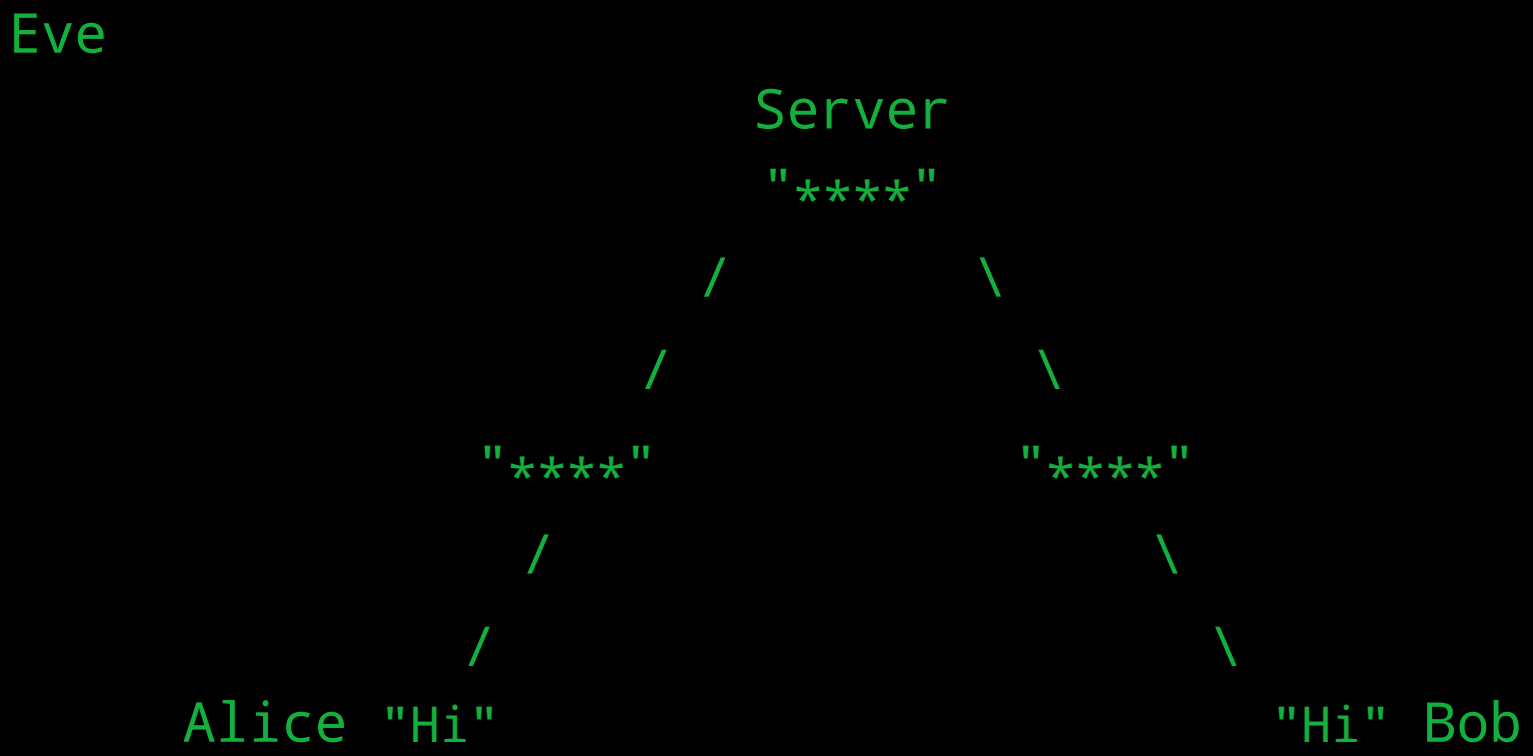
Other

- Default Device Encryption + Cryptfs Password;
- AIMSICD (counter StingRay towers, as soon as their db gets fixed)
- Goblin (for *nudes* ;))
- Local encryption:
  - PGP through OpenKeyChain
  - AES256 file encryption through Secrecy (although it hasn't been updated lately)
  - Note encryption (because, *why not?*) Note Crypt Pro, NoteBuddy, SealNote
- Password Store (UNIX pass compatible password manager)
- CryptoPass (password generation from hashes)

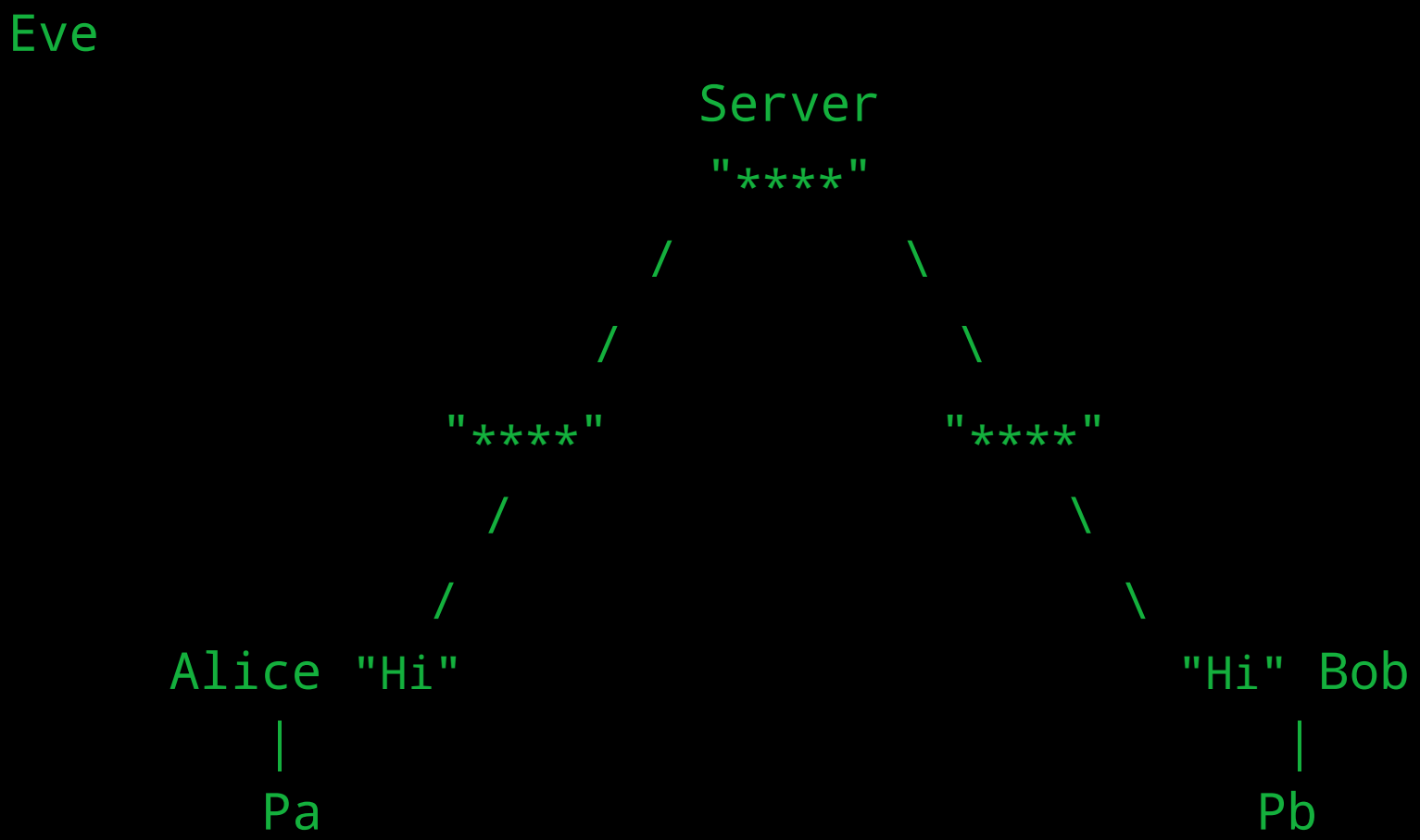
In transit encryption



End-to-end encryption



Public key encryption



Communication Apps

EFF Scorecard

1. Encrypted in transit?
2. Encrypted so the provider cant read it? (end-to-end encryption)
3. Can you verify contacts identities?
4. Are past messages secure if your keys are stolen? (forward secrecy)
5. Is the code open to independent review?
6. Is security design properly documented?
7. Has there been any recent code audit?

Pretty Good Privacy protocol - PGP

Developed in 1991

Features public key encryption with signing and fingerprinting for authentication.

Web of Trust dependent.

RSA-based.

PGP-based

- K-9 Mail, only full-feature email client, compatible with OpenKeychain;
- Pretty Easy Privacy, QuickMSG are basically email client disguised as IM apps;
- Kontalk XMPP-based app.

Off-the-Record protocol - OTR

Provides everything that PGP features, plus:

- Metadata Protection
- Forward Secrecy (if the key is ever compromised, it can only be used to decrypt future messages)
- Malleable encryption -> plausible deniablity (everyone that has access to the message could have written it)

XMPP-based

Extensible Messaging and Presence Protocol (XMPP) is a federated open communication protocol

- Xabber and Zom (formerly Chatsecure), features OTR and PGP encryption;
- Conversations, features OTR, PGP and OMEMO encryption.

Double Ratchet Algorithm - DRA

Grants everything OTR does, plus:

- Asynchronous communication;
- Multi-user group chat;
- Future Secrecy (self-heals compromised keys).

Signal Protocol

Combines the Double Ratchet Algorithm (formerly Axolotl), prekeys, and a triple Diffie-Hellman handshake, uses Curve25519, AES-256 and HMAC-SHA256 as primitives.
Used by:

- FLOSS:
  - Signal
- Proprietary and Closed-Source Software:
  - WhatsApp
  - Facebook Messenger ("secret conversations")
  - Google's Allo ("incognito mode")

Even though its server code is FLOSS, considering it is very server dependent there's no other options to servers.

Why not Telegram?

There’s absolute no reason to use:

- SHA1 (old, weak)
- Vulnerability to a Chosen-Ciphertext Attack (CCA)
- Non-standard padding algorithm ("append whatever")
- MAC-then-encrypt (Does not provide any integrity on the ciphertext and it may be possible to alter the message to appear valid and have a valid MAC code)

OMEMO

XMPP extension

The next big thing

Implements Signal's Double Ratchet Algorithm

OMEMO

XMPP extension

The next big thing

Implements Signal's Double Ratchet Algorithm

Asynchronous!

OMEMO

XMPP extension

The next big thing

Implements Signal's Double Ratchet Algorithm

Asynchronous!

Multi-user AND multi-device capable.

Others

- Silence, DRA through SMS
- Riot, DRA to an IRC-like platform
- ServalMesh, AES-256
- Briar, beta app that supports bluetooth, tor, and wifi
- Ring, (currently in beta2) uses blockchain and Distributed Hash Table
- Cyphor, encrypts messages before sending them to servers, not well explained

Systems

BlackPhone

- Proprietary, *pero no mucho*
- Suite Silent Circle (Silent Phone, silentOS, Silent World, ...)
- Privacy by design (builtin Tor)
- Big sale

BlackPhone

- Proprietary, *pero no mucho*
- Suite Silent Circle (Silent Phone, silentOS, Silent World, ...)
- Privacy by design (builtin Tor)
- Big sale flop!

Android-based

- Replicant
  - FLOSS focused
- CyanogenMod -> LineageOS
  - "Ubuntu-like"
- CopperheadOS
  - Only (serious) security focused
  - Based on SELinux technology

Just a bunch of links

http://polr.me/oalf
http://polr.me/redo
http://polr.me/goldm
http://polr.me/aneh
http://polr.me/umpro
http://polr.me/fess
http://polr.me/orom
http://polr.me/aior
http://polr.me/legal

http://polr.me/espe
http://polr.me/roqu
http://polr.me/elem
http://polr.me/edeu
http://polr.me/maboa
http://polr.me/notan
http://polr.me/essese
http://polr.me/minario