Cryptoparty for Journalists

Dipl.-Ing. Florian Wilde

partially based on "Digital Security for Journalists" by Pranesh Prakash and "Cryptoparty an der LMU" by Michael Weiner

1. July 2015

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

General Risk

Digital Miranda Warning

"Anything ~~you say or do~~ *recorded about you* can and will be used against you in ~~a court of law~~ *any way deemed appropriate to corrupt you now or decades into the future*."

Journalistic Essentials

Even if do not fear for your own (you should!),
think about the life and wellbeing of your sources!

Asking the right questions

Instead of

How am I secure?

Be More Precise

- What do I want to protect?
- With regard to what?
  - Disclosure
  - Alteration
  - Destruction
- Against whom with which capabilities?

At Stake

- Identities
  - Job
  - Reputation
  - Freedom
  - Physical integrity
  - Life
- Communicated information
- Stored data
- Secondary Research

Threats

Adversary

- Individuals
- Companies
- States
  - Police
  - Some agency
  - NSA / GCHQ

Capabilities

- Budget
- IT-Knowledge
  or contact to experts
- Access
  - to your devices
  - to your network
  - to intermediaries

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication
- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Security is More Than Secrecy

Authenticity

The information, e.g. message, truly originates from the individual claimed to be the author.

Integrity

The information has not been modified, e.g. shortened, changed or extended, since it was originally created.

Confidentiality

No one but the intended individuals knows the information.

Symmetric Crypto

Keys

- One single key for encryption and decryption (private)
- Size currently 128 to 256 bit, equals around

  116 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 possible keys

Examples

- DES (old & broken)
- 3DES (old & weak)
- AES

Usage

- Good for stored data, e.g. disk encryption, because
  - Faster than asymmetric crypto
  - No need to share (private) key, which would be difficult

Asymmetric Crypto

Keys

- A key pair consisting of a private and a public key.
- Both are mathematically connected, but it is infeasible (though possible) to calculate one from the other.
- Based on mathematical problems
  not efficiently solveable for large numbers

Examples

- DSA
  - Discrete logarithm, keys only 1024 bit
- RSA
  - Prime numbers, keys currently 2048 to 4096 bit
- ECC
  - Elliptic curves, keys currently 163 to 256 bit

larger for equal computational complexity than symmetric crypto because of the prime number stuff

Asymmetric Crypto 2

Usage

- Good for communicated data,
  because public key can be disclosed
- Encrypting messages
  - Anyone can encrypt messages with public key of receiver
  - Only the owner of the corresponding private key
    can decrypt these messages
- Signing messages
  - Only the owner of the private key
    can create valid signatures
  - Anyone can verify the signature with the public key

Caveat

Be sure to use the public key that really belongs
to the intended receiver or assumed author!

Fom Theory to Real World Products

Edward Snowden, June 2013:

> "Properly implemented strong crypto systems are one of the few things that you can rely on."

- Don't use "military grade crypto"
  - Those often have no idea of the math behind
  - Yet publish the first somehow working piece of code
- Don't use "whistleblower proof crypto"
  - Honest crypto guys will be very cautious with recommendations for such high-risk activities
- Open & closed source programs both contain bugs – or even backdoors
  - But in open source products we can find them and alert
  - Only use well established, audited open source tools
- You have to decide on your own who to trust

Trust In Devices

- If your en-/decrypting device is bugged, you are done
- While there may be civil rights within your country, most of them are vanished at the border
  - The German “Staatstrojaner” was usually installed at border controls
  - Run a zero data policy while travelling abroad
- They say it takes less than 5 minutes to compromise an Android device with physical access
- Putting sticky tape on the camera assumes the device can be remotely controlled
  - In this case all information on the machine must be assumed tainted
  - Audio is even more important than video, yet you don’t put sticky tape on your microphone

Trust In Devices 2

- Trojans can also be deeply embedded into your hardware
- Those cannot be removed by reinstalling OS
  or booting from removable media
- Don't buy hardware online
  but solely in stock parts from local shops
  - Thereby you at least avoid trojans customised for you

Airgapped Device

Definition

- A device which is not connected to the internet,
  i.e. separated by an “airgap” from the rest of the world

Purpose

- Attack surface to compromise device is minimised
- Even when compromised,
  the device cannot send information anywhere
- Well suited to protect long living private keys

Airgapped Device 2

How to create

1. Buy cheap netbook
   (minimises loss if physically destroyed)
2. Install necessary software using full disk encryption
3. Physically destroy all wireless capabilities and LAN
4. Add sensitive information

- Data into the device: Via any removable media
- Any media ever attached to the airgapped device has to be destroyed immediately thereafter
- Data out of the device:
  Solely via manually typing off the screen

Crypto Economics

- The more valuable some information is,
  the more effort will be put into
  - Getting to know it
  - Keeping you from publishing it
- The measures you take,
  must set the barrier higher than that
- Currently, most people
  - Leave their house open for anybody
  - Publish their CV on their front door
  - Write to their spouse – or lawyer – via post cards shipped in transparent vehicles

5 Minute Break

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Corporate Networks & Devices

- Are virtually always heavily monitored
- Never use them for whistleblowing

- Companies don't need proof, indication suffices
- Agencies too, by the way

Metadata

What is it?

- Who contacts whom, by
  - Phone number
  - Email address
  - Username
  - IP address
- When
- For how long (or how large is the message)
- Subject (for emails)

For mobile phones additionally:

- Where have you been when, all the time

Is it crucial?

Michael Hayden (former NSA and CIA director), 10.05.14:
"We kill people based on metadata"

When Metadata Matters

Not So Much

- Contacting your colleagues, boss, spouse, etc.

Pretty Much

- Researching backgrounds to new story

Like Hell

- Contacting sources

Different Levels of Encryption

Content / Metadata	Eavesdropper	Intermediaries	Recipients
No security (default)	Full / Full	Full / Full	Full / Full
Transport Layer Security (TLS, SSL)	No / Some	Full / Full	Full / Full
End-to-End Encryption (GPG, S/MIME)	No / Full	No / Full	Full / Full

Eavesdropper: A passive 3rd party,
e.g. someone sniffing your internet connection

Intermediaries: E.g. your mail provider (has to share data with agencies, may be hacked by others)

Your Mobile Phone

- Is a surveillance device!
- Reports wherever you go with it
- Can be easily turned into a hidden microphone without you noticing at all
- Can be easily turned into a hidden camera without you noticting at all
- Phone number, IMEI, IMSI, MAC, IP are all directly connected to your full name
- Put out of the room while sensitive talks. Seriously!
  - Putting into fridge or removing battery would show when sensitive talks happen: Metadata
- Never carry with you when meeting sources
- Do not use to contact sources

SMS

Metadata

- Always leaks, no way to secure

Content

can be encrypted, e.g. using

- Android
  - SMSSecure
  - TextSecure (uses data connection)
- iPhone
  - Signal (uses data connection)

Mobile & Landline Calls

Metadata

- Phone number, time, duration are always there
- Phone number might be hard to trace back to you by using public phone box
- Caveat: Combination with other metadata, e.g. position of mobile phone in your pocket
- In case you are really a high-value target: Fingerprints & DNA traces at the phone box

Content

- No practical way to secure

VoIP Calls

Metadata

- Phone number, time, duration are always there
- Phone number might be hard to trace back to you (depends on VoIP provider)
- IP address of caller and callee are hard to obfuscate
  - Advanced users may do so by using TOR

Content

can be encrypted, e.g. using

- Android
  - RedPhone
- iPhone
  - Signal
- SIP Provider

VoIP Calls – SIP

SIP Provider

- Dozens, recommendation from Prakesh: Ostel.co
- Downside: USA roundtripping

SIP App

- Android
  - CSipSimple
- iPhone
  - Linphone
- Blackberry
  - PrivateGSM
- Windows / Mac / Linux
  - Jitsi

Video Calls

Do *not* use

- Skype

Do use

- SIP
  - Jitsi
- WebRTC
  - Firefox Hello
  - Jitsi Meet

Email

Metadata

- Can be obfuscated to some extend by using a provider who does not keep logs
  - Riseup.net (allegedly Snowden used this)
  - Lavabit (busted)
- Email addresses can be obfuscated by
  - Throw away recipient address, e.g. from mailinator.com
  - Caveat: Inboxes are public, use with GPG
    so only intended recipient can decrypt and read content
  - Fake address in "From" field
  - Requires both parties to know
    which inbox to check and to whom to reply
- IP address in header data still identifies you
  - Advanced users may obfuscate by sending via TOR

Email 2

Content

can be encrypted with GPG

- Android
  - OpenKeychain
- iPhone
  - Proprietary: ~~iPGMail~~
- Windows
  - GPG4Win
- Mac
  - GPGTools
- Linux
  - built-in

use with proper client

- Thunderbird, with plugin Enigmail
- Claws, with plugin Claws GPG plugin

Email 3

Is that key truly from Edward Snowden?

- PGP
  - You decide yourself
  - "Web of Trust": Keys can be signed by others, you know someone who knows someone who has meet the recipient in person and checked his key.
- S/MIME
  - One of a dozen certificate authorities (CAs) decides and your mail client accepts it without warning
  - Compromising one of them to generate false certificates: easy (at least for state level adversaries)

Letter

Metadata

- Addressee – and possibly sender – is logged
- Sender can be obfuscated by not writing on envelope
- Personal delivery to inbox of recipient: none
  - Except you carried your mobile with you
  - Except there is CCTV
  - Except you are subject to physical observation
- In case you are really a high-value target:
  Fingerprints & DNA traces if the recipient gets raided

Content

- Due to workload, letters are opened only selectively
- Classical cryptography is too easy to break
  - Encrypted flash drive or CD-ROM or floppy
  - Destroy after copying data to remove old-style traces

Chat

Metadata

- Username, IP addresses,
  timestamps and size for each message
- Username might be hard to trace back to you
- But as with all internet based communication,
  IP address identifies you
  - Advanced users may obfuscate using TOR
- Username and chatroom need to be exchanged priorly

Content

can be encrypted, e.g. by

- Crypto.cat (Plugin for Firefox, Chromium, iPhone)
  - If you use the fallback on facebook chat
    you vanish anonymity even with TOR
- Peerio (Chrome, Windows, Mac)

Instant Messenger

Metadata

- Same as chat, but username is often more telling

Content

- XMPP does already transport level encryption
- Additional end-to-end encryption with OTR (Off-the-record messaging)

Instant Messenger 2

Provider

- XMPP
  - Riseup.net
  - Yax.im
  - DuckDuckGo
  - jabber.ccc.de

Clients

- Android
  - Conversations
- iPhone
  - ChatSecure
- Windows, Linux
  - Pidgin (OTR plugin available)
- Mac
  - Adium

5 Minute Break

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Why bother?

- Devices can get lost
- Devices can get stolen
- State level adversaries raid also editorial offices (even if its illegal)
- In case your device gets compromised, encrypted containers not mounted since then stay secure

How to Encrypt?

- Most OS' collect lots of metadata
  - Thumbnails
  - Recently used files
  - etc.
- Full disk encryption
  - TrueCrypt 7.1a
- In case you might be forced to reveal passwords
  - TrueCrypt Hidden Volumes
  - One password shows sensitive looking, but unimportant content
  - The other password shows the real details

Backups

- Security also means secure from data loss
- Backups have to be encrypted
  - Full disk encryption is worthless
    if someone can steel your plaintext backup
- Backups have to be physically separated
  - Physical incidents like fire must not be able
    to destroy working copy and backup(s) at the same time
- Backups must not be online longer than necessary
  - If your device gets compromised,
    backup must stay unaffected

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Search Engines

Do *not* use

- Google
  - Apart from recording your search history, Google filters the results according to your preferences
  - I.e. you get only biased information

Do use

- Ixquick
- Startpage
- DuckDuckGo

Tracking

- Can be done through cookies
  - Global disable,
    allow only for certain sites you know they need it
  - Delete them on browser shutdown
- Even without cookies,
  your browser is often uniquely identifiable
  - EFF's Panopticlick "Browser fingerprinting"
- All sites with "Like" button get your ID
  if you surf them while being logged into facebook
- "Private mode" of your browser only avoids local traces,
  the sites you visit and eavesdroppers can still track you

HTTPS

- HTTPS not only hides content from eavesdroppers but also ensures their integrity
- HTTPS Everywhere automatically uses HTTPS for all sites known to support it

TOR

- Enables strong anonymity
- By routing your connection through several proxy nodes
- Peeling off one layer of encryption at each node
- Route changes every 10 minutes

How to use

- Tor Browser Bundle
  - Ready to use Firefox with TOR preconfigured
- Tails
  - Ready to use OS with TOR preconfigured
  - Runs as live OS from any removable media
  - Breaking out of Firefox
    does not immediately compromises device
    (except deep trojan gets installed)
- Change your browsing habbits when using TOR

Agenda

Risk Assessment

Crypto Basics

BREAK

Communication

- General
- Mobile Phones
- Calls
- Mail
- Chat

BREAK

Data Storage

Research

Tutorial Session

Tutorial Session

Supporters

- Please make yourself visible!

Questions

- You may ask questions to any supporter,
  they will pass them in case they don't know ;)

Tutorials

- Most measures mentioned are just a few clicks away!
- Grab one of the supporters and ask him if you got stuck.