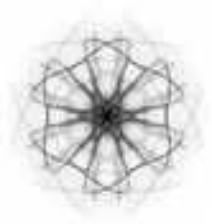




Zero-Information-System

- × Algorithm using
- × How key exchange works
- × Planned features



ZIS Algorithm using > Risk Analysis

Since BarsWF became popular many things changed. Currently there are some Bruteforcer which are using OpenCL to crack Passwords. If you want to know more search for “Passwords^12” on Google or Youtube.

I'm looking forward to use Elliptic Curve Cryptography (ECC). Of course I just could use RSA but this would lead me to use 4096 bit keys – which are way to heavy to handle for my purpose. I'm currently looking at 512 bit keys for ECC and also using Keccak (NIST selected it as SHA-3) with 512 bit.

What problem are we **focusing** at?

- Man-in-the-middle
- Weak password (Bruteforce & Wordlists and Time-Memory Tradeoff attacks)
- Wrong implementation (See WEP causing to be broken in less then 5 minutes)



ZIS Algorithm using > Risk Solutions

man-in-the-middle

You can prevent MITM attacks basically with verified public keys. How to verify the public key later on...

Weak password

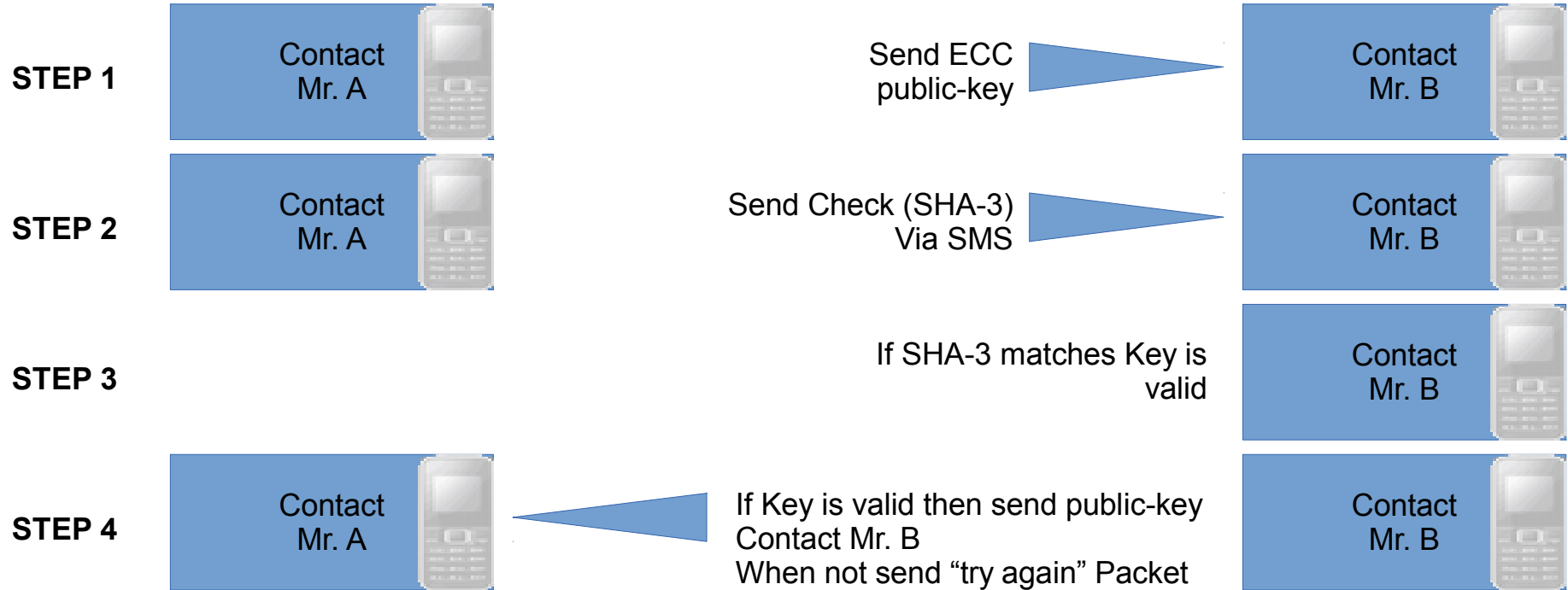
The key will be stored into a keyfile so you don't have to remember a password. It will be stored in the program path. As long as you use a trust able environment you're good. When not you've already lost the power from preventing that another just simply take screenshots etc.... See XCP rootkit (Sony CD-Rootkit) as an example of this bad situation.

Wrong implementation

Because it will be GPL which means opensource everybody can look into the sourcecode and mail me – so I can correct it.

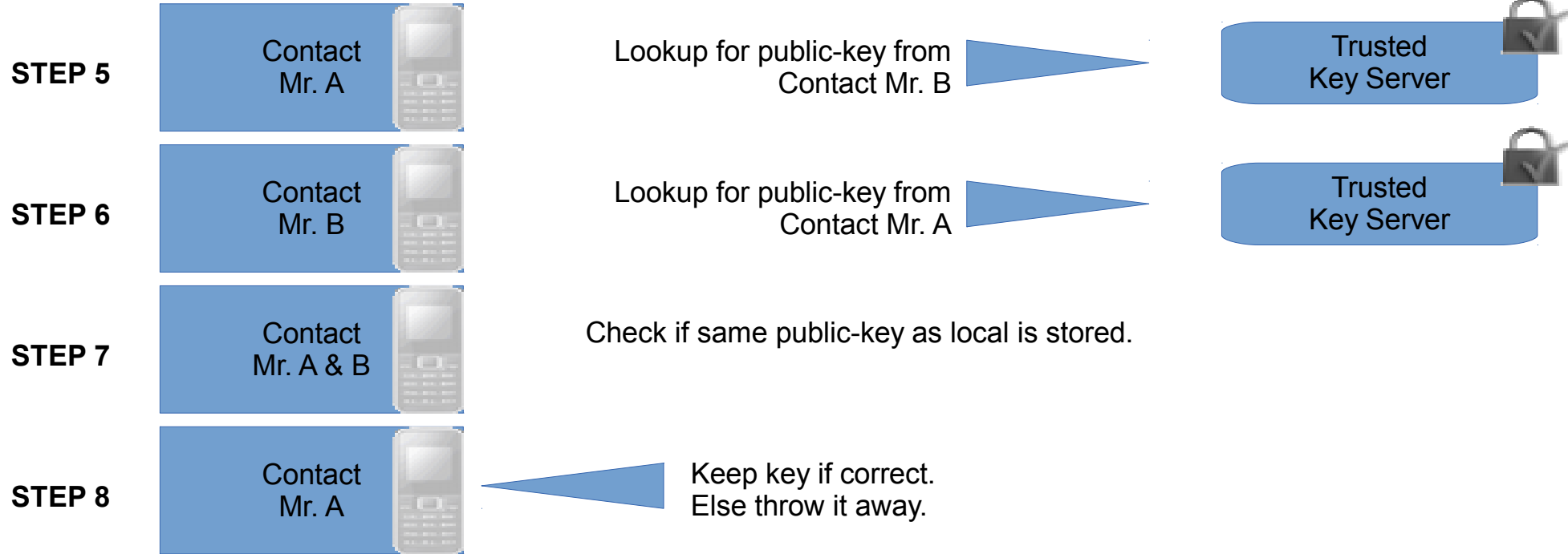


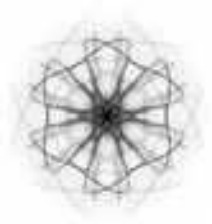
ZIS How key exchange works > Verifying Part 1





ZIS How key exchange works > Verifying Part 2





ZIS How key exchange works > Verifying Part 3

Of course you should also check the public-key manually by calling them personally or meet them local and check via QR-Code... But this are features which are planned but not first priority.

ZIS can only communicate with a verified key. The reason is simple. Everyone just thinks “Oh for what should I use encrypted communications”. Instead of informing themselves why, they don't care a second. To prevent this behaviour I push them to use encryption.



ZIS Planned features

There are so many ideas in my head... But for now I would like to collect YOUR ideas too!

Please contact me via Mail for more.

ADMIN@TROSTBROT.CH

