CRYPT-CLIP: MOBILE ENCRYPTION DEVICE

Joshua Alexander Kettlewell, Intake: January 2014, EPD, Supervisor: Joe Fitzsimons, PhD Student.

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

Abstract

We propose a device, Crypt-Clip, that allows two parties to exchange information with unconditional security against eavesdroppers. This allows use of comprised phones or computers to be used for secure communication. Crypt-clip is secure against all known attacks and there is no central server - so businesses can trust to equip their employees with our technology, being confident that no external entity is snooping on their activities.

The Problem

Everyone has secrets. Everyone would like to keep them secret.

Every time we exchange information, we make implicit assumptions about the security of the technology in our hands:

1. Telecoms communication is not monitored.
2. Apps that claim to do encryption are doing encryption properly.
3. The apps we are using have no backdoors.
4. The device, mobile phone or computer, we are using has not been infected with malware that is snooping on your activities.
5. Our phone, computer or operating system is not backdoored.
6. More generally, that the crypto-schemes used to protect information cannot be broken (for instance, we accept that numbers cannot be decomposed into their prime factors efficiently, the underlying assumption of RSA).

Solution

Our approach to the problem allows for a *burn after reading* architecture.Crypt-clip can generate large keys, take in a file and encrypt it by applying a one time pad [AppCrypt] using one of the generated keys. To our knowledge, no such portable device exists. Unlike existing cryptographic protocols we don't need to make computational assumptions about the difficulty of certain calculations. There is no central server - so businesses can trust to equip their employees with our technology, being confident that no external entity is snooping on their activities.

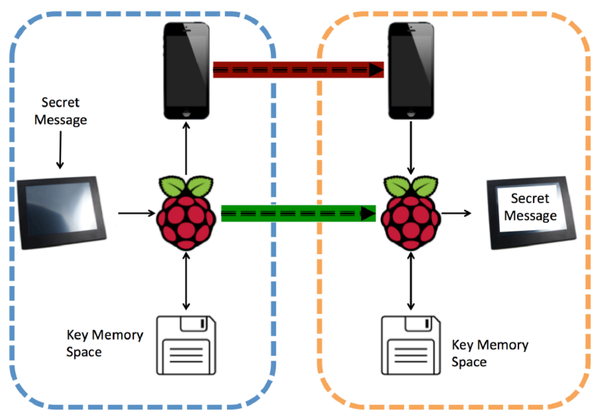


Figure 1: **Basic schematic of communication**. Blue box identifies the devices of message sender (Alice), orange box identifies the devices of receiver (Bob). Red arrows shows insecure communication (cyphertext only), Green arrow shows the transmission of secret keys (this is done in advance and it is secure). Raspberry indicates raspberry pi computer.

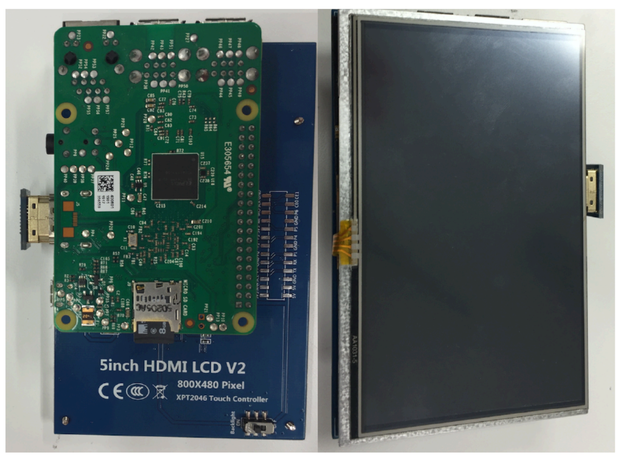


Figure 2: Front/Back of current *CryptClip* prototype, not including battery.

Protocols and Abilities

- Wegman-Carter autentication to prevent message tampering
- Large key (one time pad) encryption.
- Optional hashing of small keys using $SNOW - 3G$ key exchange protocol
- Able to encrypt all file types

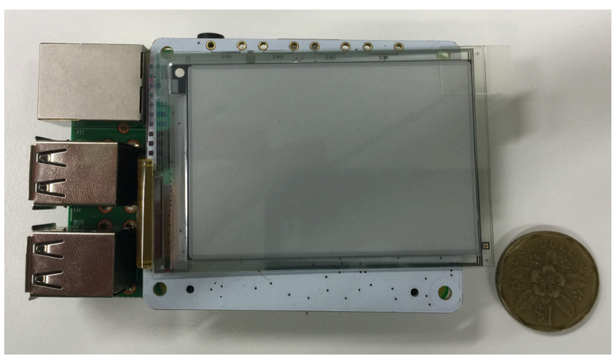


Figure 3: second *CryptClip* prototype, not including battery. An eink screen is used to save power.

Infographic:

93 *Respondents*

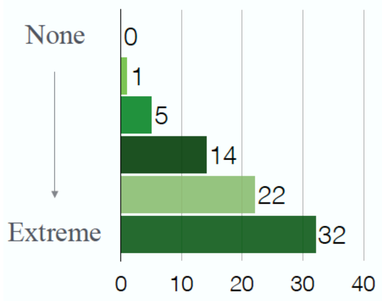
Main age group: 26 - 35 (60%)

Mostly not students (90%)

Industries most represented

- IT industry (20%)
- Research and development (20%)
- Media and Arts (13%)

Level of distress if personal data were compromised (74 responses)



Most important kind of information to exchange securely (69 responses)

Email, instant messages — 62%

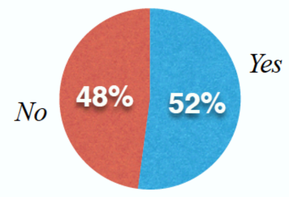
PDF, word documents — 16%

Key questions:

Do you believe *secure communication* is an issue for either your work life and/or personal life? (93 responses)

- Both personal and work life (45%)
- Personal life only (20%)
- Work Life only (10%)
- I do not believe it is an issue (25%)

Do you use software of physical devices to protect the privacy of your communication? (71 responses)



How much are you willing to pay for a device like CryptClip that can keep your communications (calls, messages, file sharing, etc.) secure (72 responses):

- More than 50$ (25%)
- Between 20$ and 50$ (30%)
- Less than 20$ (30%)
- Would not buy it (15%)

Market Evaluation

Competitive Landscape

Company Name	Product Type	Key Security Features	Security Rating	Price	Usability
Telegram	Instant messenger	Optional end-to-end encrypted messaging with self-destruct timers	Low	Free	High
WhatsApp	Instant messenger	end-to-end encrypted	Low	Free	High
BlackBerry	Smart phones	Option of a secure workspace	High	Around US$600	Moderate
SpiderOak	Online backup and file hosting service	encrypted cloud storage and client-side encryption key creation	Moderate	Free	High
Crypt-Clip	Encryption device	Encrypted communication with secret key distribution	High	Around US$100	High

Table 1: *When looking at sales to the general public our main competitors would be* ***Telegram Messenger***, ***WhatsApp***, *and similar secure messaging apps based on 256-bit symmetric AES encryption, RSA 2048 encryption and DiffieHellman key exchange. [telecry]. These do not provide thorough security solutions and are susceptible to many attacks.*

References

[QCrypt] N. Gisin et al., *Quantum cryptography*, Rev. Mod. Phys. 74, 1, 2002.

[AppCrypt] B. Schneier, *Applied Cryptography: Protocols, Algorithms*, John Wiley & Sons, Inc. 1993

[telecry] "FAQ for the Technically Inclined" Telegram. Retrieved 9 January 2016.

[MAS] http://www.mas.gov.sg/

[Trad] http://www.iesingapore.gov.sg/

[QuesLink] http://goo.gl/forms/gbspejiKUA Security device feedback

Figure 4: Team members:

Joshua Kettlewell, SUTD | Ewan Munro , NUS | Wei Pan, SUTD | Dr. Tommaso Demarie, SUTD | Ada Altybayeva, SUTD | Zhikuan Zhao, SUTD

Acknowledgements

Kettlewell acknoledges the support of the *'Big-D project'* funding via Singapore University and Technology and Design.