VE475
Introduction to Cryptography

Project 2

Manuel — UM-JI (Summer 2022)

Goals of this project

- Improve research efficiency
- Develop teamwork and collaboration skills
- Organise and write clear documents
- Improve understanding by confronting acquired knowledge to new information

Discuss with your teammate which subjects you desire to investigate. If you all agree on a topic not listed below please inform us of your choice.

For each topic some references or simple guidelines are provided together with a goal to achieve. Thoroughly investigate the chosen subject from a cryptographic perspective.

This project should take more time than project 1. Therefore **do not wait the last minute** to start up. Writing a good project requires several days of work, so make sure you start early enough.

Any source of information can be used (internet, textbooks, OS documentation...). However, in any case, **do not recopy the materials** and quote your sources.

When reading new information, understand it, process it, consider how it relates to what you already know, and how you can reach conclusions beyond the ones offered in your source.

Available topics:

1. Side channel attacks
   - Articles:
     - Mobile Device Security: The case for side channel resistance (G. Kenworthy and P. Rohatgi)
     - Physical Key Extraction Attacks on PCs (D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer)
   - Goal: as much as possible reproduce the experiments and recover a secret key
2. Breaking WEP encryption
   - How is WEP encryption working, and how to break it?
   - Goal: implement an attack to recover the secret key
     Note: the implementation must be yours, the goal is not to learn how to run `aircrack-ng`, but to implement the attack yourself
3. Tor, an anonymity network
   - Official Tor website: `https://www.torproject.org/`
   - Goal: understand “onion routing”, study the code and present at least two attacks, taken from research articles, on the Tor network
4. Hash functions
   - Website on sponge functions and SHA-3: `http://sponge.noekeon.org/`
   - Goal: understand the sponge construction and implement Keccak

5. TrueCrypt is dead
    - Website with much documentation: `http://andryou.com/truecrypt/index.php`
    - Goal: carefully read all the documentation and understand all the possible attacks and how to prevent them. How secure was TrueCrypt and why is it dead?
      Note: the official reason is very unlikely to be the right one...
6. OpenSSL
    - Website: `https://www.openssl.org/news/vulnerabilities.html`
    - Goal: study the code and understand the many recent security issues
7. GnuPG
    - Website: `https://www.gnupg.org/`
    - Goal: study the code and understand the various attacks that lead to the "important security fixes" mentioned on their website
8. Multiple polynomials quadratic sieve*
    - Simple presentation: `http://www.cs.virginia.edu/crab/QFS_Simple.pdf`
    - Goal: fully understand the mathematics behind the MPQS and implement it
9. Shor algorithm*
    - Article: `http://epubs.siam.org/doi/pdf/10.1137/S0036144598347011`
    - Goal: understand the basics of quantum computing and explain how RSA can be broken using a quantum computer
10. Bitcoin*
    - Website: `https://en.bitcoin.it/`
    - Goal: understand how the bitcoin currency works and how it makes use of more advanced cryptography and mathematics
11. TUF
    - Website: `https://theupdateframework.io/`
    - Goal: understand why TUF was developed, i.e. how updates were developed before, and study how TUF is used in git
12. LRNG
    - Websites: `https://github.com/smuellerDD/lrng` and `http://www.chronox.de/lrng/doc/lrng.pdf`
    - Goal: in recent Linux kernels random numbers are generated following a new strategy. Study the limitations of the previous one and why LRNG is suitable from a cryptographic point of view.

*Those slightly more advanced projects will benefit from a softer grading policy.