VE475
Introduction to Cryptography

Project 2 (09/08/2017)

Manuel — UM-JI (Summer 2017)

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
   - Article: `http://mostconf.org/2012/papers/21.pdf`
   - 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

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

Groups

Hong Jingzhou 洪劲舟 and Huang Jingwen 黄静文
Hao Yuxuan and Xu Kejia 徐可嘉

Geng Yajie 耿亚捷 and Zhu Wenyang 朱文扬
Bao Shuci 包书慈 and Wang Wenhao 汪文浩

Zhai Yifan 翟逸凡 and Zhang Yongyin 张永银
Hu Xuefeng 胡雪峰 and Pan Shengjie 潘圣杰

Han Zhuoran 韩卓然 and Mou Yipeng 牟一鹏
Wang _fu 王塬夫 and Wang Jie 王捷

Zhou You 周游 and Zhao Li 赵力
Wang Xiangyu 王翔宇 and Xu Zilin 徐子临

Xu Haining 徐海宁 and Yu Chengyun 于承运
Feng Yu 丰羽 and Song Jieming 宋杰铭

Gu Yichen 顾宜宸 and Liu Yihao 刘逸灏
Peng Junda 彭俊 and Wang Dayi 王达一

Tang Shenghao 汤晟皓 and Wang Zilu 王子路
Yin Leyi 殷乐宜 and Zhang Chi 张弛

He Zhiyuan 何知远 and Ni Yanchao 倪彦超
Li Siying 李思颖 and Wu Xinyi 吴欣怡

Wang Zhiyuan 王智远 and Wei Chuxi 魏楚希
Tan Lunte 谭伦特 and Wang Jingyuan 王靖元

Cai Zhibo 蔡志波 and Chen yudong 陈煜东
Diao Zihuan 刁梓桓 and Yang Yunlu 杨云路

Wenyang 文仰 and Wu Jiaxi 吴嘉熙
Gao Jiecheng 高杰诚 and Lu Yilong 陆翼龙

Zhenwei Yang 杨振玮 and Li Xiang 李响
Diao Zhuoran 刁卓然 and Gu Ronghao 顾荣豪

Cui Shuoyang 崔朔杨 and Qian Xiangru 钱相如
Liu Qiyang 刘齐阳 and Sun Siqi 孙思齐

Sato Muneyuki and Wu Yuzhou 吴禹洲
Li Guohao 李国豪 and Wu Yichen 吴奕辰

Feng Zhengyang 冯正扬 and Zuo Jiaqi 左嘉琦
Zeng Zhi 曾挚 and Zhu Chen 朱宸

Silva Rui and Wu Wenyi
Chen Zhiqing 陈志卿 and Wu Jiachen 吴佳晨

Liu Xu 刘旭 and Zhang Kai 张开
Qian Shengyi 钱圣轶 and Song Qun 宋

Song Yue 宋越 and Zhu Wenyao 朱文耀
Wang Zesen 王泽森 and Xue Leyang 薛乐阳

Lu Chengzhe 陆成哲 and Zhang Jian 张简
Shi Yucheng 史玉成 and Xu Rishang 徐日上

Ding Kaili 丁恺笠 and Wu Chenggang 吴承刚
Hu Qiaoyu 胡乔予 and Wei Chen 卫晨

Duan Yijian 段益坚 and Hang Wei 杭卫
Vagne Lars and Zhu Yifan 朱一凡

Lan Tianmu 兰天牧 and Wang Yuchen 王宇辰
Wu Yuexiao 吴越箫 and Zheng Xuan 郑璇