Intro to Cybersecurity – Spring 2024

Homework/Lab #1

Due: Monday, April 1th 2024

Highlights

- Expected contribution towards the final score: 10%.
- You should work on this homework/Lab individually or in a team of up to 5 members (highly recommended). One submission per team.
- For experiments (e.g., running openssl commands), **give step-by-step screenshots**
- **Submit your work as a pdf** through the USTC Blackboard
  - If you work as a team, clearly state the contribution of individual members
  - If you work as a team, submit as a Blackboard team

1) **(5 points)** What are the risks of having the US government select a cryptosystem for widespread commercial use (both inside and outside the United States). How could users from outside the United States overcome some or all of these risks

2) **(5 points)** Why do we need modes of operation for block ciphers? Also, Give a direct comparison between CBC and CTR.

3) **(20 points)** Explain why hash collisions occur. That is, why must there always be two different plaintexts that have the same hash value? What property of a hash function means that collisions are not a security problem. That is, why can an attacker not capitalize on collisions and change the underlying plaintext to another form whose value collides with the hash value of the original plaintext?

4) **(20 points)**
   a) (10 points) Identify the CAs (including the intermediate and root ones) that have issued the TLS certificate for https://ustc.edu.cn/. Then, identify the certificate expiration date. Besides, export the TLS certificate into a PEM file (e.g., through openssl), and calculate its md5 hash and SHA256 hash.
   b) (10 points) Similarly, redo the above experiments for www.12306.cn and www.bing.com

5) **(30 points) Encrypt/Decrypt/Sign through openssl**
   a) Generate an AES-128 key with the cipher mode of CBC through openssl
   b) encrypt a message m = "introduction to cybersecurity 2024" and decrypt it back using the above AES-128-cbc secrets.
   c) Generate a public and private key pair
   d) generate a sha256 hash of the message m, and generate a signature by encrypting the hash with your private key
   e) Verify the digital signature, with your public key
   f) Take screenshots of step a-e, and embed them in the submission pdf.

6) **(20 points)** Select and read one of the following papers, summarize its ideas, and give your critical reviews (e.g., pros and cons of this paper):
   a) Diffie, Whitfield, and Martin E. Hellman. "**New directions in cryptography**." In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman
   b) ElGamal, Taher. "**A public key cryptosystem and a signature scheme based on discrete logarithms**." IEEE transactions on information theory 31, no. 4 (1985)

c) Troncoso, Carmela, et al. "Decentralized privacy-preserving proximity tracing." arXiv preprint arXiv:2005.12273 (2020).

d) Albrecht, Martin R., et al. "Practically-exploitable cryptographic vulnerabilities in matrix." 2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023.

Your review should contain the following elements

- A good summary of the paper with one or two paragraphs.
- Key contributions of the paper in terms of identifying new questions, proposing new methodologies, and distilling insightful understandings, etc.
- Limitations and future works