Security of Distributed Software

SS 2019 – 5. Tutorial

Valentin Siegert M.Sc.

Dang Vu

*VSR.Informatik.*TU-Chemnitz.*de*

Task 1

Where to use one-way hash functions?

Transmit error detection

Fast data access

Identification/Comparison of secrets

Criteria of a good one-way hash function:

Pre-image resistance, irreversibility

Second pre-image resistance, collision resistance

Efficient calculable

High dispersion $\leftrightarrow$ order preservation

1. A message “VSR” is given. Using the ASCII table and the hash function $f(s) = (\sum_{i=1}^{length(s)} s_i)\ mod\ 7$ *compute the hash value of the message.*

81	0x51	121	Q
82	0x52	122	R
83	0x53	123	S
84	0x54	124	T
85	0x55	125	U
86	0x56	126	V

$$f("VSR") = (86 + 83 + 82)\ mod\ 7 = 251 \bmod 7 = 6$$

1. A message “VSR” is given. Using the ASCII table and the hash function $f(s) = (\sum_{i=1}^{length(s)} s_i)\ mod\ 7$ *compute the hash value of the message.*
2. *Get acquainted with the tool GnuPG.*
   a. Create a MD5 hash of the message “VSR”.
   b. Check if the copy of the file *bankdaten.txt* in OPAL was not manipulated. (md5: 8C E8 26 9E 53 F8 47 57 27 F0 63 41 04 64 DC 3C)
   c. Let your neighbor choose one of “fry”, “lila” or “bender”. Tell him/her a random number.
      He/she builds: “Number:Secret” and tells you the md5.
      Find out which secret your neighbor has chosen.

Task 2

1. Read about the Ceaser cipher.
   Using the key “4” decrypt the message “WSQQIV”.

2. Which security risks are imposed by the Ceaser cipher?

Advantages

Fast Algorithms

Easy Hardware implemenation

Disadvantages

Requies secure channel

Requires Keyadministration

Security Risks

Frequency analysis

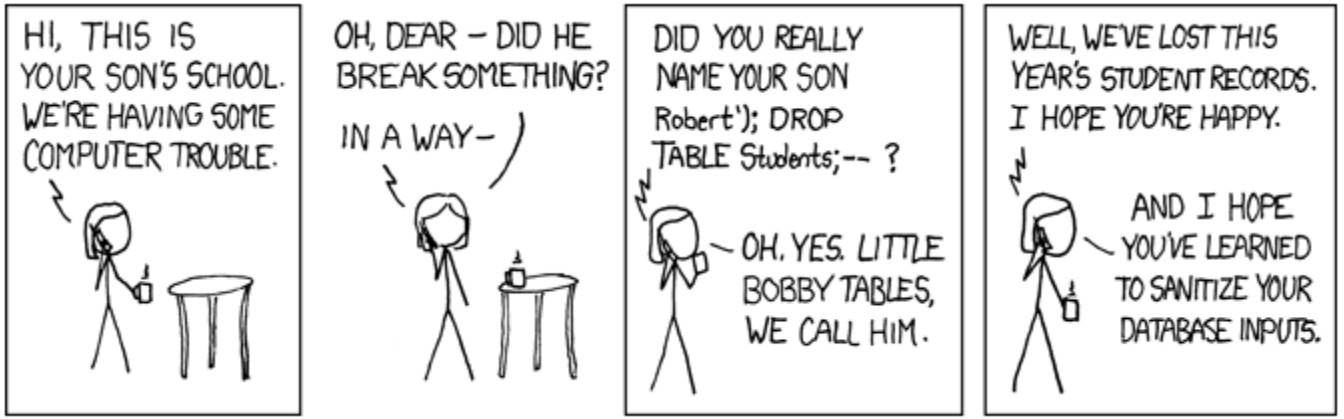
Brute-Force

Concealment of approach not key

1. Read about the Ceaser cipher.
   Using the key “4” decrypt the message “WSQQIV”.

2. Which security risks are imposed by the Ceaser cipher?

3. Using GnuPG decrypt *image.png.gpg*
   (Cipher: AES, Password: tu-chemnitz)


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Task 3

1. Consider the RSA encryption and decryption.
   a. Your partner passed you a public key (e=7, N=77).
      Encrypt the message “DE” using this key.
      Use positions of letters in alphabet as codes.
   b. Decrypt the message from subtask a using the privat key (d= 43, N=77).

2. Using the GnuPG tool create a RSA key pair. Exchange public keys with your neighbor:
    a. Create a folder with your URZ username in the “Schlüsseldatenbank” folder of OPAL.
    b. Upload your public key to the folder of your neighbor.
3. Create a message, encrypt it using your partner’s public key and upload it to his folder in OPAL.
4. Decrypt the message using your private key.

4 Task 4

1. Inform yourself about building signatures using RSA.
   a. Sign the message “DE” using your private key ($d^*=27$, $N^*=55$).
   b. Your partner knows your public key ($e^*=3$, $N^*=55$). How can he verify your signature?
2. Sign the message from task 3.3.
   If you want you can change the message.
   Upload both message and signature into your partner’s OPAL folder.
   Let him/her check if the message corresponds to the signature.

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*