CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Hash Functions – Part 2

Video Summary

- What is Hashing?
- Message Authentication Code (MAC) ✓
- Hash Functions ✓
- Hash Algorithms ✓
- Applications of Hashing →
- Hash Implementation using OpenSSL →

To be useful for message authentication, a hash function H must have the following properties:

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant ✓
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x) ✓
- Collision resistant or strong collision resistance ✓
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Security and Applications of Hash Functions

There are two approaches to attacking a secure hash function:

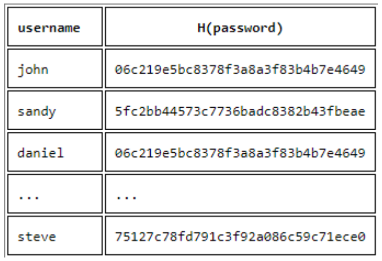
Cryptanalysis

- Exploit logical weaknesses in the algorithm

Brute-force attack

- Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm



username	H(password)
john	06c219e5bc8378f3a8a3f83b4b7e4649
sandy	5fc2bb44573c7736badc8382b43fbeae
daniel	06c219e5bc8378f3a8a3f83b4b7e4649
...	...
steve	75127c78fd791c3f92a086c59c71ece0

Additional secure hash function applications:

Passwords

- Hash of a password is stored by an operating system

Intrusion detection

- Store H(F) for each file on a system and secure the hash values

Hash Functions with Open SSL

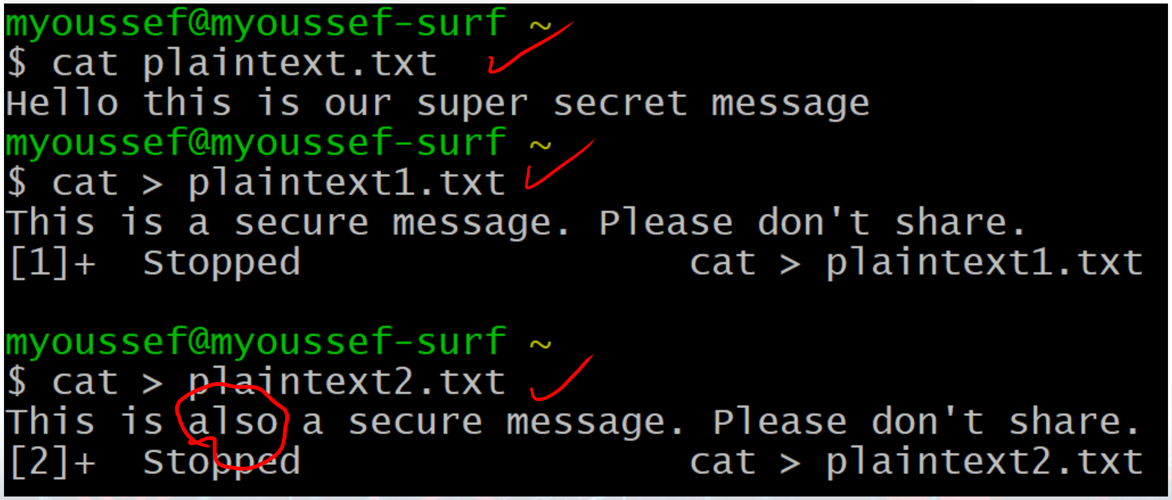
```
$ openssl list-message-digest-algorithms

$md5sum plaintext.txt

$sha1sum plaintext.txt

$openssl dgst –sha256 plaintext.txt
```

MD5 SHA1
SHA256
SHA512



```
myoussef@myoussef-surf ~
$ cat plaintext.txt
Hello this is our super secret message
myoussef@myoussef-surf ~
$ cat > plaintext1.txt
This is a secure message. Please don't share.
[1]+  Stopped                 cat > plaintext1.txt

myoussef@myoussef-surf ~
$ cat > plaintext2.txt
This is also a secure message. Please don't share.
[2]+  Stopped                 cat > plaintext2.txt
```

Video Summary

- What is Hashing?
- Message Authentication Code (MAC)
- Hash Functions
- Hash Algorithms
- Applications of Hashing
- Hash Implementation using OpenSSL