One-Way Hash Functions

One-Way Hash Commands

Linux utility programs

- Example: md5sum, sha224sum, sha256sum, sha384sum and sha512sum

```
$ md5sum file.c
919302e20d3885da126e06ca4cec8e8b   file.c

$ sha256sum file.c
0b2a06a29688...(omitted)...1f04ed41d1   file.c
```

One-Way Hash Commands (Contd.)

Using openssl command to calculate hash

```
$ openssl dgst -sha256 file.c
SHA256(file.c)= 0b2a06a29688...(omitted)...1f04ed41d1

$ openssl sha256 file.c
SHA256(file.c)= 0b2a06a29688...(omitted)...1f04ed41d1

$ openssl md5 file.c
MD5(file.c)= 919302e20d3885da126e06ca4cec8e8b

$ openssl dgst -md5 file.c
MD5(file.c)= 919302e20d3885da126e06ca4cec8e8b
```

Integrity Verification

- Changing one bit of the original data changes hash value

```
$ echo -n "Hello World" | sha256sum
a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

$ echo -n "Hallo World" | sha256sum
d87774ec4a1052afb269355d6151cbd39946d3fe16716ff5bec4a7a631c6a7a8
```

- Usage examples:
  - Detect change in system files
  - Detect if file downloaded from website is corrupted

Keyed-Hash MAC (HMAC)

- Uses hash function H (compression function block size B) and a secret key K
- ipad = 0x36 (B times), opad = 0x5c (B times)
- Can be used with any one-way hash function