Computer Security (COM-301)

Authentication – Passwords & Biometrics

Interactive Exercises

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Authentication aboard the Enterprise

Consider the following authentication exchange in which Spock uses his password 'LongAndProsper' to prove his identity to Kirk:

```
Spock ---- (Spock, 'I want to login') ----> Kirk
Spock <--- Hash(Spock) ----- Kirk
Spock ---- Enc('LongAndProsper', Hash(Spock)) ----> Kirk
```

Which of the following statements is correct?

(a) Hash(Spock) is not a good challenge because it will be used every time
(b) Hash(Spock) is not a good challenge because anyone can compute it
(c) The protocol is bad because the login is sent on the first message
(d) Hash(Spock) is a good challenge because hashes output random numbers

Facebook password onion

```
$cur  = 'password'
$cur  = md5($cur)
$salt = randbytes(20)
$cur  = hmac_sha1($cur, $salt)
$cur  = remote_hmac_sha256($cur, $secret)
$cur  = scrypt($cur, $salt)
$cur  = hmac_sha256($cur, $salt)
```

Why does Facebook use this onion?

Source: Tom Ristenpart

Knock, knock, knocking

Cersei and Jaime meet secretly every week in the crypt. To make sure that they are each other, before opening the door they have a protocol in which:

1) Jaime knocks a particular sequence (toc, toc, toctoc)

2) Cersei replies with another sequence (toctoc, toc, toctoc)

3) Jaime replies with just (toc).

Is this safe against an eavesdropping Tyrion hidden behind the bushes? If yes, justify. If not, explain how to fix it.

Securing grades

Agree or disagree with the following statement and justify your answer:

“When configuring biometrics to be used as an authentication function to secure access to students’ exams grades, it is important that the system has a low false negative rate even if the system finds many false positives”

Good Biometrics

These are common attributes for an authentication mechanism

(a) Universality: everyone has them

(b) Uniqueness: everyone has a different biometric

(c) Permanence: they do not change over time

(d) Secret: they are only known to the user

(e) Unpredictable: given a biometric trait, other trait cannot be predicted

Which ones are desired for biometric authentication? Of the desirable ones, do they have any downside?