University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 5-1

Topic: Authentication

Presenter: Matt Niemiec

Announcements

- Project 2 is going up soon
- Moodle backend is... a work in progress
  - Talk to us if you have any concerns about your grades!

Homework 3

Question **1**

Not yet answered

Points out of 5.00

Consider the following scenario: Two parties want to perform a key exchange using the Diffie-Hellman Key Exchange algorithm. They agree on a prime number p=37, a base number g=7. The first party generates a key x_1=22, and the second party generates a random key x_2=13.

1. What is y_1, the number generated by the first party to send to the second party?

2. What is y_2, the number generated by the second party to send to the first party?

3. What is z, the key that resulted from their transaction of keys?

4. What can we say about the intermediary keys, y_1 and y_2?

- The keys were different, but mathematically they could have been the same
- The keys were the same because the Diffie Hellman Key Exchange is extremely insecure and vulnerable to such errors
- The keys were different. It is necessary for the keys to be different if the initial secrets x_1 and x_2 are different
- The keys were the same. This possibility is important since we lose information and we're transmitting a secret over an insecure channel

Question **1**

Not yet answered

Points out of 2.00

1. Bob decides to send Alice a message. Using his private key and the DSA, he appends a digital signature. What aspects of the CIA triad does this provide for Alice?

- [ ] Confidentiality
- [ ] Integrity
- [ ] Availability

2. Alice decides to send Bob a message. Using Bob's public key, she generates a digital envelope with the secret inside. Which of the CIA triad is provided by this?

- [ ] Integrity
- [ ] Confidentiality
- [ ] Availability

Question **1**

Not yet answered

Points out of 1.00

A perfect hashing algorithm will have no collisions

Select one:

- True
- False

Question **1**

Not yet answered

Points out of 1.00

We roll a die 3 times. What is the probability that all three rolls yield distinct values (i.e. there are NO collisions). Enter as a probability 0<=p<=1 with an error of <=0.01

Answer:

Question **1**

Not yet answered

Points out of 2.00

Earth is gone! We didn't learn to recycle or use renewable energy sources, so Elon Musk had to take us all to live on Mars, where there are 687 days in a year. Now, everybody up there has a Martian birthday. You wonder if anybody in the room shares a birthday, so you use your knowledge of probability and calculate. To answer the questions below, you can assume equal distribution, an exact 687 days in a year, and anything else that isn't actually true to have the math we did in class.

1. What's the fewest number of people will you need in a room to have a >0.5 probability of two or more people sharing a birthday?

2. What's the fewest number of people you'd need in a room to have a > 0.65 probability of having two or more people with the same birthday?

Question **1**

Not yet answered

Points out of 2.00

Assume we have a hash function that is perfectly random, and has a mediocre 40-bit output. How many different inputs will we need before we have a >0.01 probability of having a collision?

Answer:

Authentication

What is Authentication?

- Prove a user is who they say they are
- Different than authorization
- Verify your identity
  - Whatever that is!

Four Means of Authenticating a User

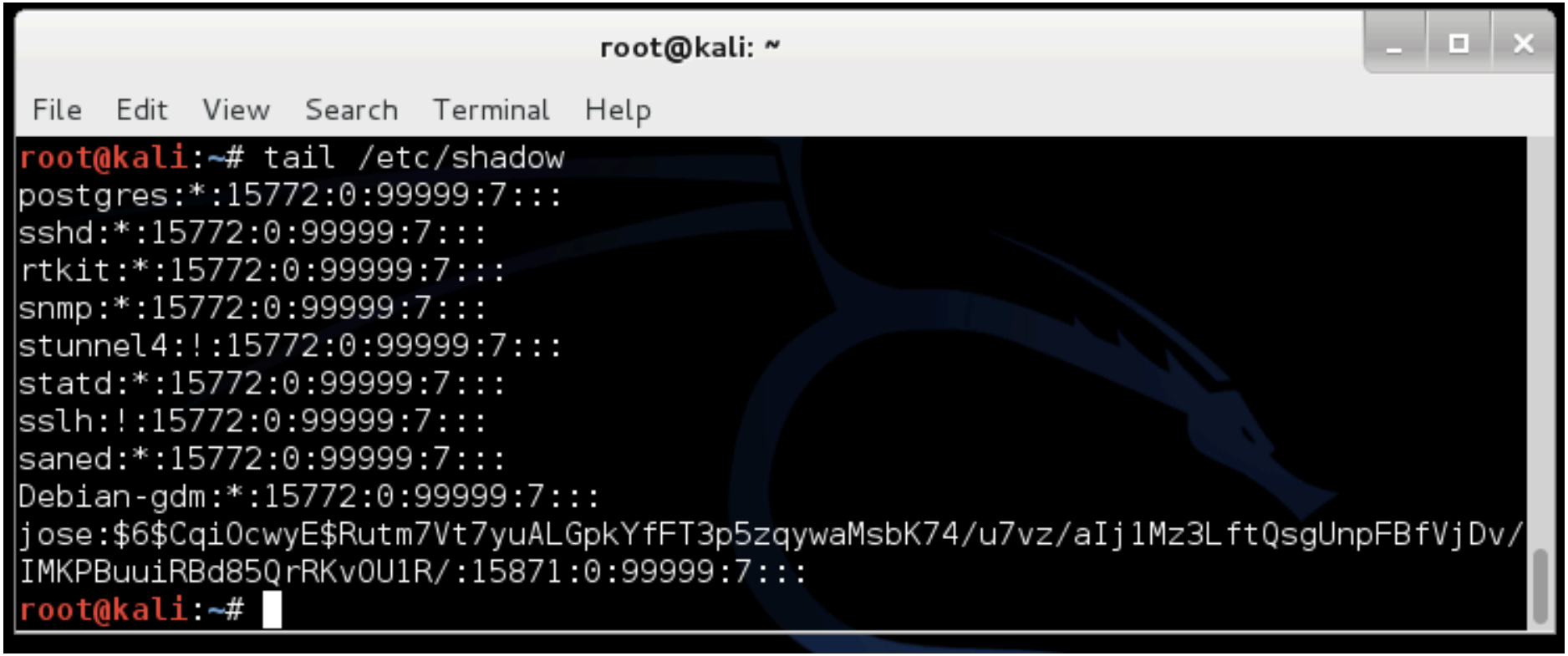
- Something you have
  - Credit card, badge, smart card, key, etc.
- Something you know
  - PIN, password, security questions, etc.
- Something you are
  - Fingerprint, retinal scan, facial recognition, etc.
- Something you do
  - Voice pattern, typing rhythm, gait analysis, etc.

Something You Know

Passwords

- Easy to verify
- Choose between
  - Easy to remember
  - Difficult to guess
- Should be hashed in case of a breach


https://www.troyhunt.com/the-773-million-record-collection-1-data-
HOME
WORKSHOPS
SPEAKING
MEDIA
ABOUT
CONTACT
SPONSOR
The 773 Million Record "Collection #1" Data Breach
17 JANUARY 2019
ny people will land on this page after learning that their email address has appeared in a data
ach I've called "Collection #1". Most of them won't have a tech background or be familiar with


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tail /etc/shadow
postgres:*:15772:0:99999:7:::
sshd:*:15772:0:99999:7:::
rtkit:*:15772:0:99999:7:::
snmp:*:15772:0:99999:7:::
stunnel4:!:15772:0:99999:7:::
statd:*:15772:0:99999:7:::
sslh:!:15772:0:99999:7:::
saned:*:15772:0:99999:7:::
Debian-gdm:*:15772:0:99999:7:::
jose:6CqiOcwyE$Rutm7Vt7yuALGpkYfFT3p5zqywaMsbK74/u7vz/aIj1Mz3LftQsgUnpFBfVjDv/
IMKPBuuiRBd85QrRKvOU1R/:15871:0:99999:7:::
root@kali:~#

Password Vulnerabilities

- Offline dictionary attack
  - Or brute force
- Online/specific account attack
- Workstation hijacking
- Exploiting user mistakes
- Exploiting password reuse
- Electronic monitoring/sniffing

Rainbow tables

- Pre-compute common hashes (>30GB worth!)
- Useful for offline or online?

Salting

- Append a random value to the password before hashing
- How does this help?

Salting

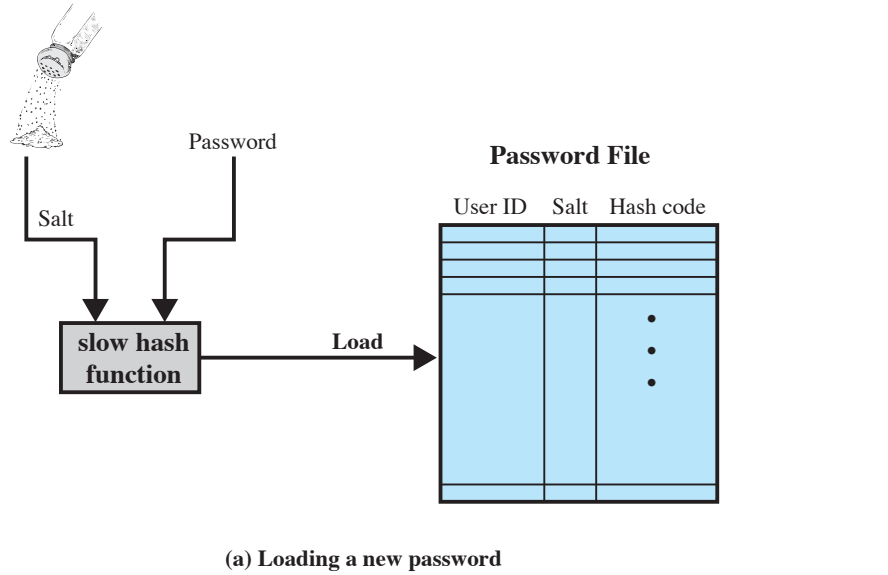
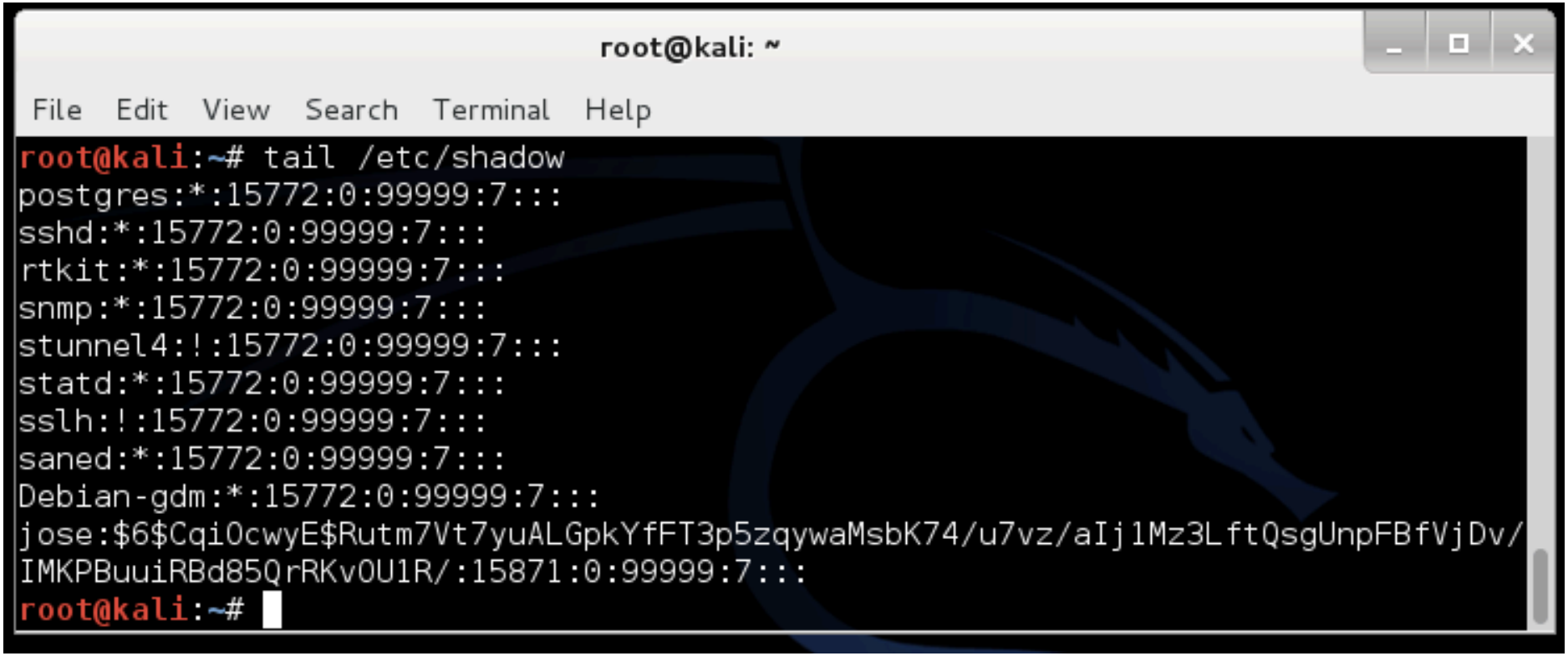


Figure 3.3 UNIX Password Scheme


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tail /etc/shadow
postgres:*:15772:0:99999:7:::
sshd:*:15772:0:99999:7:::
rtkit:*:15772:0:99999:7:::
snmp:*:15772:0:99999:7:::
stunnel4:!:15772:0:99999:7:::
statd:*:15772:0:99999:7:::
sslh:!:15772:0:99999:7:::
saned:*:15772:0:99999:7:::
Debian-gdm:*:15772:0:99999:7:::
jose:6CqiOcwyE$Rutm7Vt7yuALGpkYfFT3p5zqywaMsbK74/u7vz/aIj1Mz3LftQsgUnpFBfVjDv/
IMKPBuuiRBd85QrRKvOU1R/:15871:0:99999:7:::
root@kali:~#

Salting

- Remember: salts are stored in plaintext!
- There are four main reasons for hashing:
  - Avoid same hashes within the same file
  - Avoid same hashes between different systems
  - Prevent rainbow tables
  - Attackers must target one user at a time
- Online vs. offline attacks

Salts Shortcomings

- Don’t help in targeting a single user
- Don’t help in online attacks
  - Do you know your salt?

Password Complexity

- Dictionary attacks
- Complexity is $size\_of\_char\_set^{\#characters}$
- On average, it takes *n/2* tries to crack a password in a set of size *n*

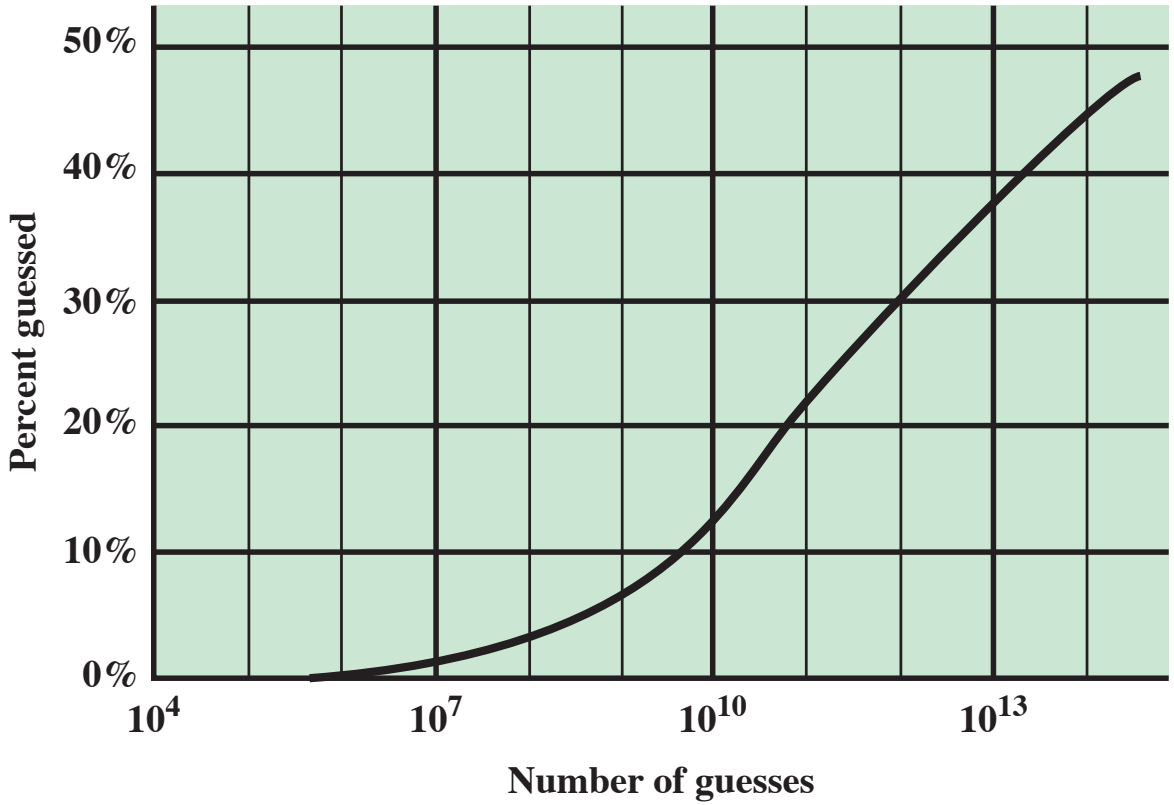


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses


John
the
Ripper