Processes and authentication

UNIX process hierarchy

ssh b146-*

pstree -p | less -S

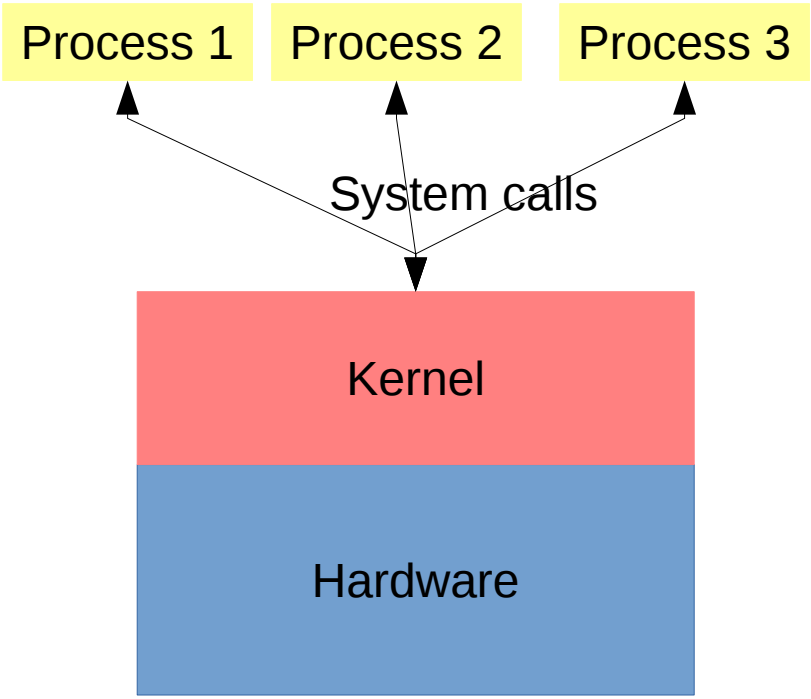
pstree -pu crandall

lsof -p31009

nc -l 20202 &

lsof -p31626

kill -9 31626



Authentication in general

- Bishop: “Authentication is the binding of an identity to a principal. Network-based authentication mechanisms require a principal to authenticate to a single system, either local or remote. The authentication is then propagated.”

Authentication in general (continued)

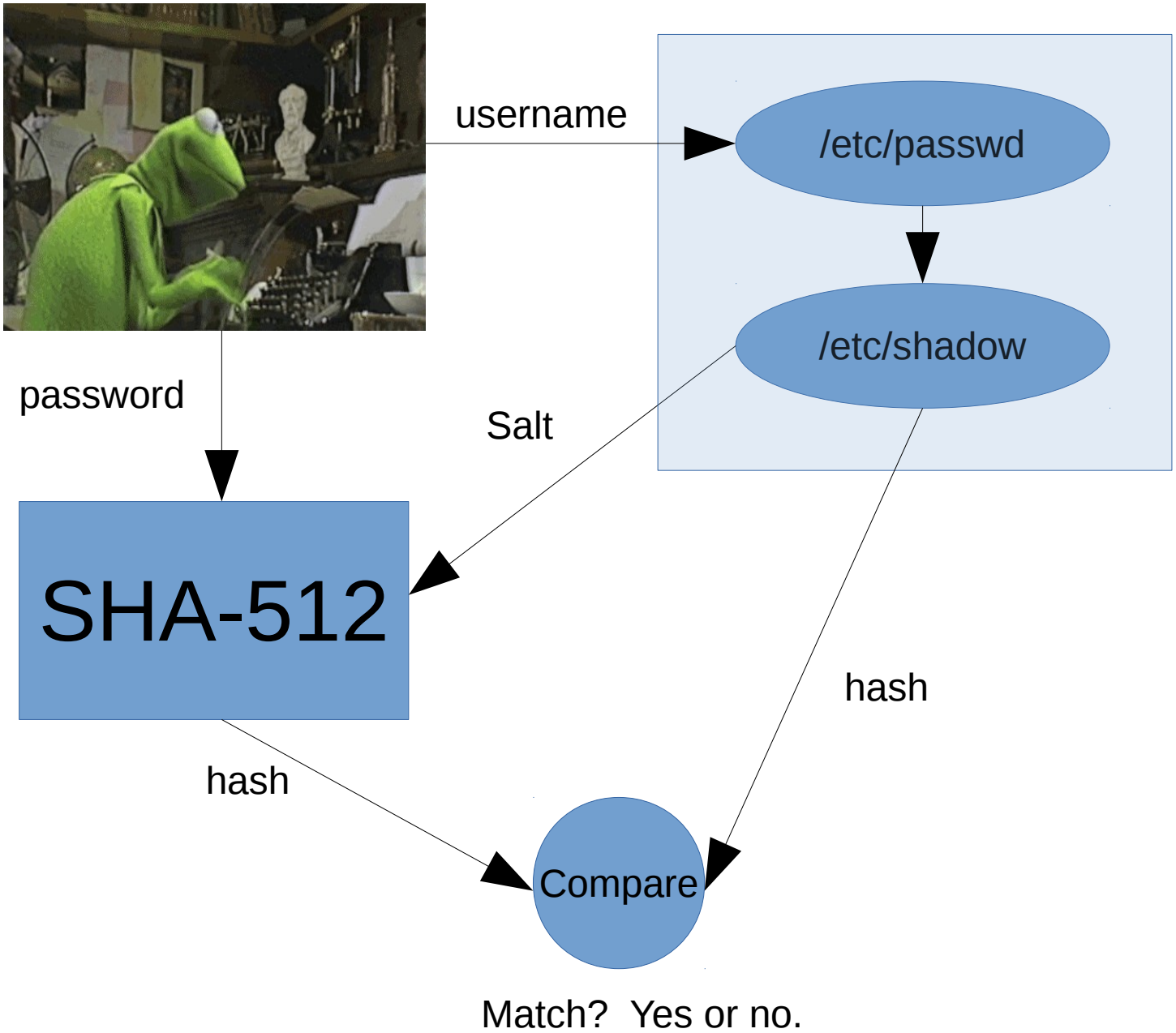
- Bishop: “Authentication consists of an entity, the *user*, trying to convince a different entity, the *verifier*, of the user's identity. The user does so by claiming to know some information, to possess something, to have some particular set of physical characteristics, or to be in a specific location.”
- Informally: something you know, something you have, something you are

2FA = 2-Factor Authentication

- Two of these:
  - Something you know
  - Something you have
  - Something you are
- *E.g.*, bank card plus PIN
- For Internet services, typically the first two
- Helps protect against phishing, for example

Basic Linux authentication

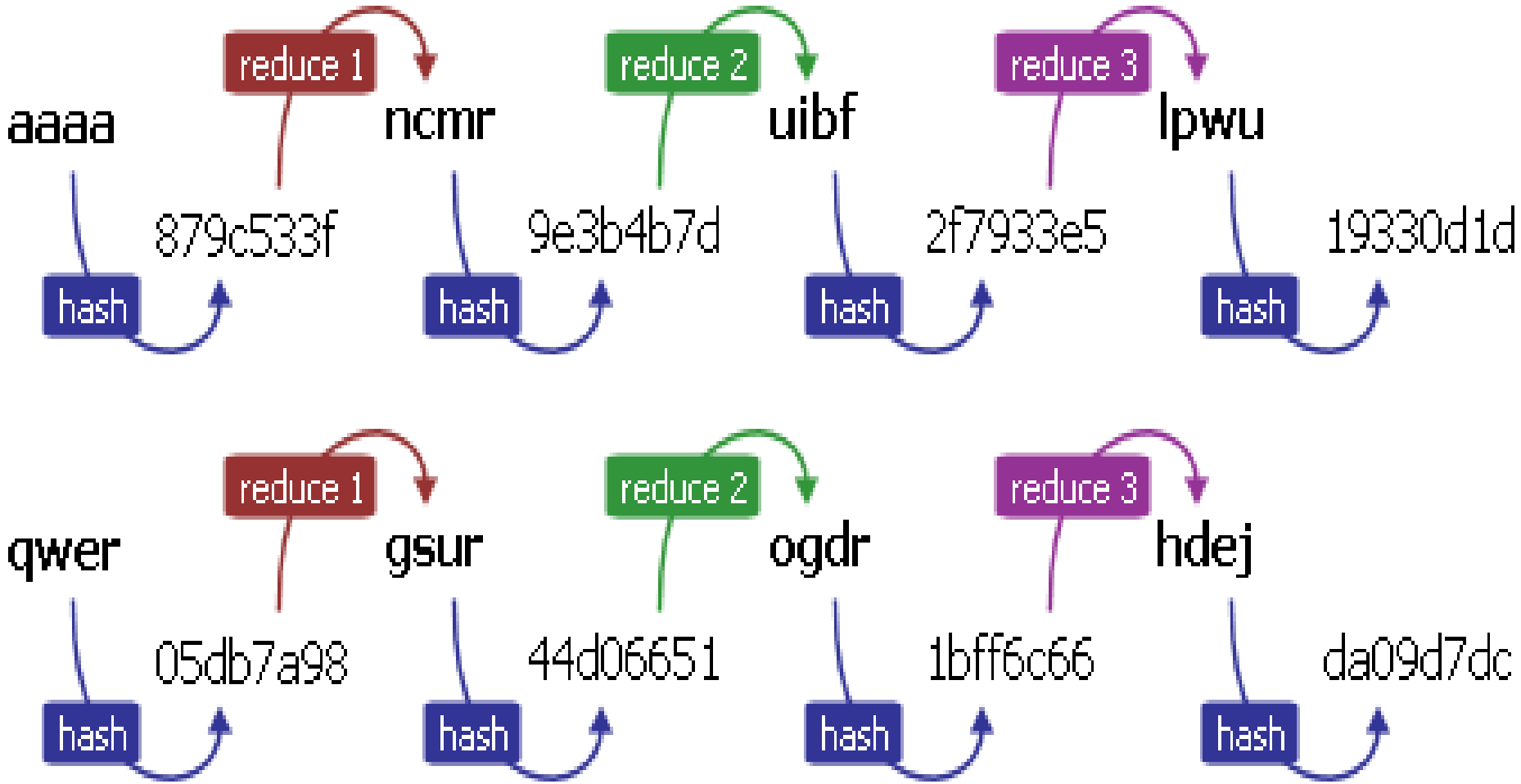
- Ties you (the identity) to your user ID (the principal), which is in turn tied to subjects (*e.g.*, processes) and objects (*e.g.*, files)
- Based on hashing
  - Also salting
  - Also shadowed password hashes


username
/etc/passwd
/etc/shadow
password
Salt
SHA-512
hash
hash
Compare
Match? Yes or no.

Passwords

- Should be high ~~entropy,~~ algorithmic complexity
- Should be easy to remember

These requirements are in
conflict with each other!
Password managers help.



Rainbow Table

aaaa	19330d1d
qwer	da09d7dc

Plagiarized from https://i.imgsafe.org/2bf87cbfe2.png

Time-memory tradeoff

- Rainbow tables can store lots of hash results compactly (precomputation)
- Just check if a user's hash might be in a hash chain, only recalculate it if so
- As a fall-back, just try every possible password (brute force)

Salting helps against precomputation.

Good passwords, system-imposed delays, shadowing help against brute force.

Shadowing the password file

```
crandall@hannibal: ~
crandall@rubicon ~ $ sudo grep "hal" /etc/passwd
hal:x:1003:1003:Hal,,,:/home/hal:/bin/bash
crandall@rubicon ~ $ sudo grep "hal" /etc/shadow
hal:$6$4asLz5vU$l5FDnfwLtlXQf/EESsxI3f3YbjM3fzTtw9EwKy8vsnEU4e8uKIvoy0ST99nquwH5
QrHwt3SvGsciQk2D98OQ9.:17259:0:99999:7:::
crandall@rubicon ~ $ ls -l /etc/passwd
-rw-r--r-- 1 root root 2021 Apr  2 22:49 /etc/passwd
crandall@rubicon ~ $ ls -l /etc/shadow
-rw-r----- 1 root shadow 1532 Apr  2 22:49 /etc/shadow
crandall@rubicon ~ $
```

Phishing

From: "Dropbox Notification" <dropbox.noreplay@gmail.com>
Date: Dec 7, 2016 [redacted]
Subject: You have 1 new file in your inbox
To: [redacted]
Cc:

Hi [redacted]

You have received a new document in your inbox, view the file "مذكرة القبض على عزة سليمان.**pdf**" on Dropbox.

View file

Image plagiarized from https://citizenlab.org/wp-content/uploads/2017/02/Ponytail-Figure-1.png

Phishing

- Wide range of sophistication in terms of the social engineering aspect
  - One end of the spectrum: “Plez logg in and changer you password, maam!”
  - Other end of the spectrum: “The attached PDF is my notes from the meeting yesterday, it was nice to see you again!” (from someone you saw at a conference the day before)

2FA helps protect against phishing
(but state actors can easily spoof your
cell phone and get SMS messages)

File permissions

```
crandall@hannibal: ~
crandall@rubicon ~ $ sudo grep "hal" /etc/passwd
hal:x:1003:1003:Hal,,,:/home/hal:/bin/bash
crandall@rubicon ~ $ sudo grep "hal" /etc/shadow
hal:$6$4asLz5vU$l5FDnfwLtlXQf/EESsxI3f3YbjM3fzTtw9EwKy8vsnEU4e8uKIvoy0ST99nquwH5
QrHwt3SvGsciQk2D98OQ9.:17259:0:99999:7:::
crandall@rubicon ~ $ ls -l /etc/passwd
-rw-r--r-- 1 root root 2021 Apr  2 22:49 /etc/passwd
crandall@rubicon ~ $ ls -l /etc/shadow
-rw-r----- 1 root shadow 1532 Apr  2 22:49 /etc/shadow
crandall@rubicon ~ $
```

-rwxr-x---

- First is special designations (symlink, directory)
- Next triplet is user (u)
- Triplet after is group (g)
- Last triplet is others (o)
- r = read, w = write, x = execute
- Sometimes you'll see other things, like s for Set UID

Preview...

- Processes (subjects) act on files (objects)
- Processes are tied to principles (users)
- File permissions are checked when the file is opened (and added to the file descriptor table of the process), not with every access!

man ...

- ls (ls -l is a useful flag), cd, pwd, chown, chgrp, chmod, stat, id, w, who, last, kill, ps, pstree, netstat, cat, less, sudo, watch, screen, fuser

Some more things to read up on

- FIFO pipes (can be unnamed or named)
- The /proc/ filesystem
- Character devices (*e.g.*, PTY, PTS, TTY)

Resources

- http://www.cs.unm.edu/~crandall/linuxcommandcheatsheet.txt
- Matt Bishop's *Computer Security: Art and Practice*, Chapter 12
- https://citizenlab.org/