CSCI 331:
Introduction to Computer Security

Lecture 6: Passwords

Instructor: Dan Barowy

Williams

Topics

Lab 1

C bugs

Password systems

Crypto primer

Lab 1

1. Labs should make you stretch, not be **hard**.
2. Calibration—**everyone** now gets an **extra late day**. Bank it or use it on lab 2.
3. Feeling confused? This is **not bad**. Get in touch.
4. Feeling discouraged? This is **not good**. Get in touch.
5. Nobody who hands in **something** will do poorly in this class, because…
6. **Resubmissions**.

Your to-dos

1. Read *Why Stolen Password Databases Are a Problem* **for Thu, 9/28**.
   i. Please take notes.
2. Project part 1 due **Sunday, 10/1**.

Spot the C bug

Four major security concerns

- Confidentiality
- Integrity
- Authenticity
- Availability

Confidentiality

Confidentiality is the property that information is **not made available** or disclosed to **unauthorized** individuals, entities, or processes.

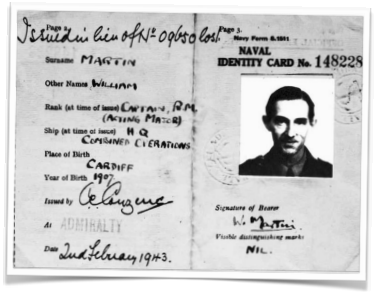
Integrity

Integrity is the property that information is **accurate**, **complete**, and **consistent** over its entire lifecycle. Importantly, information **should not be modifiable** by an **unauthorized party** or in an **undetected manner**.

Ferris changes his grade in "Ferris Bueller's Day Off."

Authenticity

Authenticity is the property that a **fact** or **identity** is **true** or **genuine**.



"Operation Mincemeat"

Operation Mincemeat

- Successful British intelligence operation (1943)
- Fooled Nazi military into believing that allied troops would invade Italy via Sardinia instead of Sicily.
- Body of deceased sailor ("Capt. William Martin") set afloat from submarine HMS Seraph with forged identity documents.
- Body was actually Glyndwr Michael, a homeless Welsh man who died after eating rat poison.
- Spanish fishermen found body; passed on to Nazi intelligence.
- Nazis redirected troops to Sardinia; allies invaded via Sicily.

Non-Repudiation

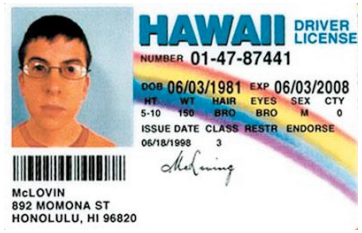
Non-repudiation is the property that an **action** can be associated with a **unique actor** (e.g., an individual or process). Such actors **cannot dispute the association**.

Non-Repudiation

Non-repudiation is the property that an **action** can be associated with a **unique actor** (e.g., an individual or process). Such actors **cannot dispute the association**.

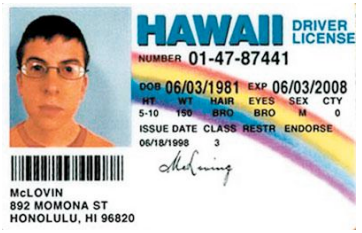
Non-Repudiation

Non-repudiation is the property that an **action** can be associated with a **unique actor** (e.g., an individual or process). Such actors **cannot dispute the association**.



Non-Repudiation

Non-repudiation is the property that an **action** can be associated with a **unique actor** (e.g., an individual or process). Such actors **cannot dispute the association**.

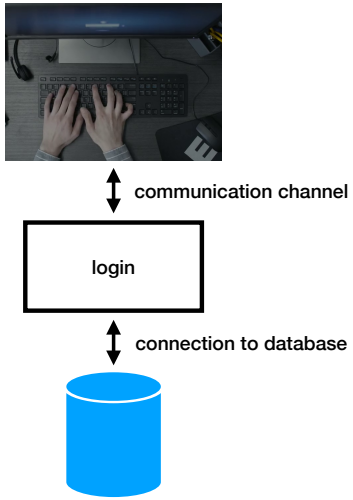


Availability

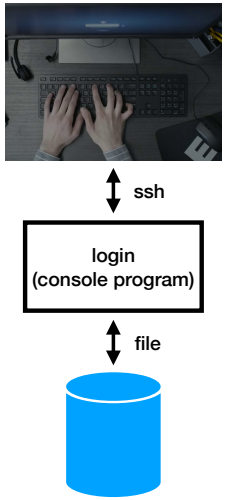
Availability is the **proportion of time** that a resource is in **functioning condition**.

Password Databases

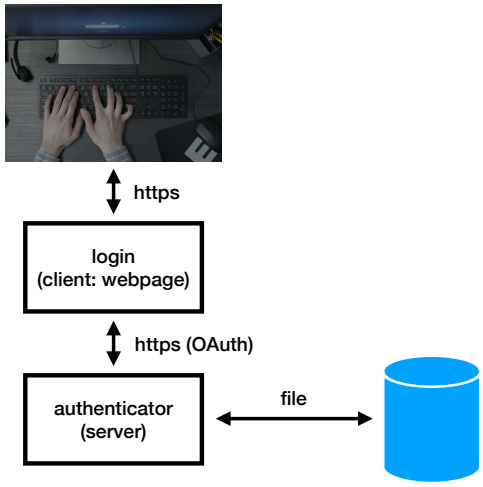
How a Password Database Works



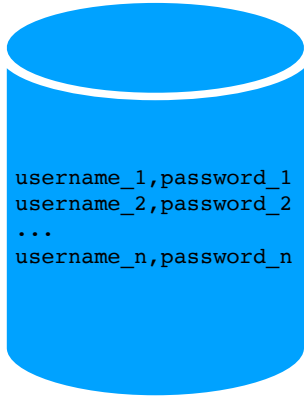
Example



Example



Form of a password database



Kept in sorted order by username (allows fast lookups).

Class Activity

Work with a partner to think of **at least one** potential **vulnerability** for a password system.

- Be sure to consider all of the password system's parts.
- Is your potential vulnerability a threat to confidentiality, integrity, authenticity, or availability?
- How realistically do you think your vulnerability can be exploited?

Class Activity

- **Confidentiality** is the property that information is **not made available** or disclosed to **unauthorized** individuals, entities, or processes.
- **Integrity** is the property that information is **accurate**, **complete**, and **consistent** over its entire lifecycle. Importantly, information **should not be modifiable** by an **unauthorized party** or in an **undetected manner**.
- **Authenticity** is the property that a **fact** or **identity** is **true** or **genuine**.
  - **Non-repudiation** means that actors **cannot dispute the association**.
- **Availability** is the **proportion of time** that a resource is in **functioning condition**.

Recap & Next Class

Today we learned:

CIAA

Password systems

Next class:

Password system attacks