Accounting

Introduction to IT Security

Otago Polytechnic
Dunedin, New Zealand

Review

AAA

- Authentication: who you are
- Authorisation: what you can do
- **Accounting: tracking what you have done**

Two parts to accounting

1. Logging events
2. Reviewing logs

Logging events

Any application of any importance should write logs.

- Log any problems or exceptions that could indicate a bug.
- Log events that could represent a security issue like a failed login.
- You may want to log apparent user errors.
- You may want to log routine events if your application has security-sensitive function.
- Be wary of over-logging. You will train users to ignore your logs if they contain useless information.

How to log

- Usually we write to a log file.
  - This is simple to do.
  - Operating systems already include this capability. (e.g., Windows event viewer, Unix/Linux syslog)
  - It's easy to set up other programs to monitor and process logs.
- Occasionally, an application may log events in a database in order to support more complex built in event reporting.

Remote logging

For large or security-intensive applications, consider logging to a remote server.

- Logs are preserved even if the system running the application is compromised.
- It's easier to check and manage centralised logs.

Log levels

- Logging services usually support a number of logging levels, e.g. informational, warning, error.
- Application configuration should include selection of log level.
- This helps avoid over-logging.

Monitoring logs

- We can, and do, view logs manually.
- If we have a large volume of logs, we may use software to process and summarise the logged data.
- We may use monitoring programs to checked logs in near real time to alert us to problems.
- Seperating responsibility for writing logs from the responsibility for monitoring logs
  - means that application programmers don't have to anticipate user security demands;
  - gives users the flexibility to design and implement their own log monitoring protocol.

Log handling and retention

Now that we are producing and reviewing lots of logs, we need a plan for retention.

- This is a policy decision balancing security needs with storage and handling capacity.
- In some areas there may be legal or regulatory concerns.
- Consider storing logs on secured write-only media.

Today's lab

We will take the password checking program we wrote last week and add logging to it.