Determining What Applications Should and Shouldn’t Log

Peter Mosmans
LEAD PENETRATION TESTER
@onwebsecurity https://www.onwebsecurity.com

Module Overview

The Dangers of Logging Too Much

The Purposes of Logging

Events to Log and Monitor

Who Decides, and When to Decide

The Dangers of Logging Too Much

Why Not Log and Monitor Everything?

Legislation

Confidentiality

Information Overload

Cost of Processing Information

Why Not Log and Monitor Everything?

Legislation

Confidentiality

Information Overload

Cost of Processing Information

Legislation

EU: General Data Protection Regulation

US: Federal Trade Commission Act

Confidentiality

Credentials

Payment details

Detailed (system) information

Sensitive information

CWE-209: Information exposure through an error message

The dangers of showing users, or non privileged accounts error messages

A6
:2017

Security Misconfiguration

CWE-779: Logging of excessive data

Software logs too much information, making log files hard to process and possibly hindering recovery efforts, or forensic analysis after an attack.

Information Overload

Too much can hinder detection

Right balance

Cost of Processing Information

More (human) resources necessary to

- configure logging
- determine baselines
- tweak monitoring

How to Decide What Not to Log

Consult your legal team before logging

Check whether the data needs to be kept confidential

Make sure the log data is proportionate to its value

The Purposes of Logging

Logging and Monitoring Is Necessary For

Situational awareness and timely discovery

Escalation prevention

Forensics

Detective Controls

Security incidents

- Access control violations
  - Incorrect logins

Compliancy purposes

- Policy violations
  - Off-business hours
  - Excessive use of service

Auditing purposes

Compliancy

Auditing

Security policy should be leading

Logging and monitoring for security purposes

Events to Log and Monitor

Access Control Events

Authentication events

- Success
- Failure

Authorization events

- Success
- Failure

Use of Privileges

- Success
- Failure

Application Specific Events

Application errors

Startup and shutdown

Configuration changes

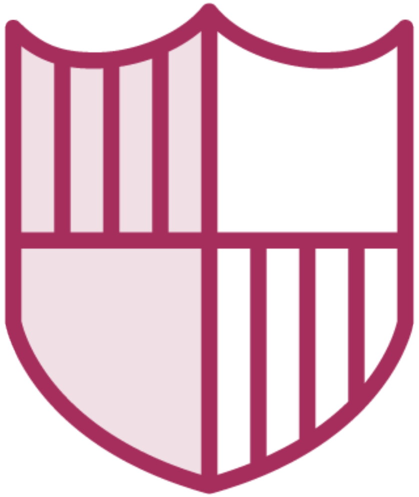
Application state information

Input and output validation

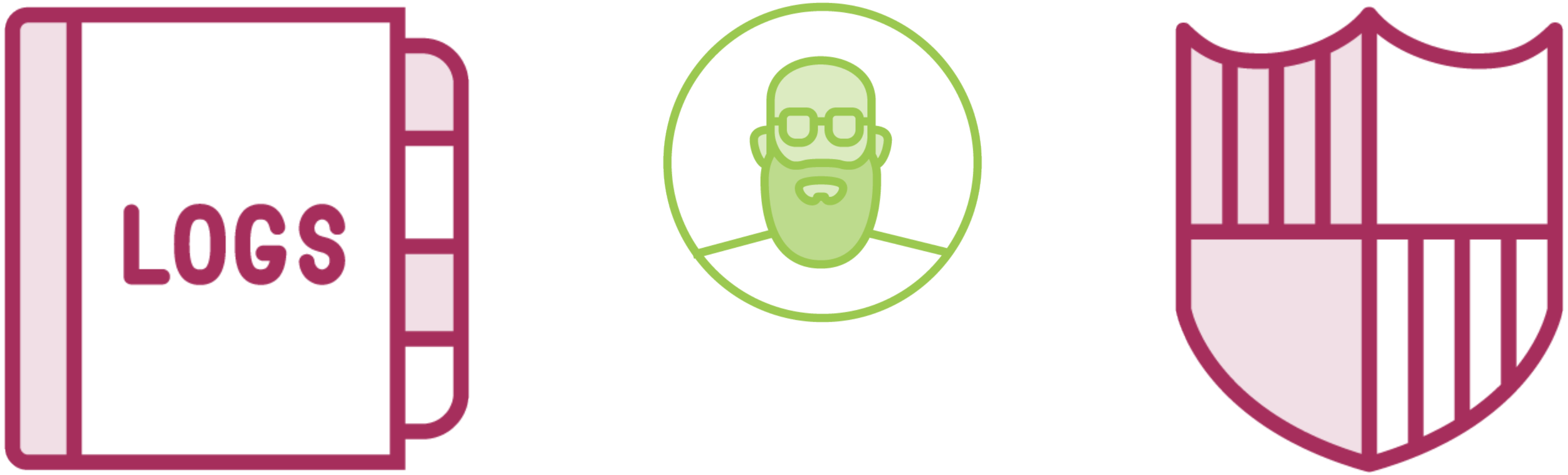
- Application is expected to handle errors

Log all security related events

Security Is a Trade Off



Security Is a Trade Off



Who Decides, and When to Decide

Who Decides What to Log and Monitor?

Software Developers

Legal Department

Security Professionals

Team

Shared Responsibility

The whole team

Software Development Life Cycle

Planning

Defining Requirements

Designing

Building

Testing

Deployment

Important Phases

Requirements and Design

Specify log as well as monitoring parameters

Define sensors

Deployment and Operation

Enable monitoring

Configure logging based on environment

Determine baselines

Tweak monitoring

Add or remove sensors

Summary

Don’t log everything:

- Legislation
- Confidentiality
- Information overload
- Cost of processing information

Use common sense

- Balanced and proportionate

Start with a minimal set

Shared responsibility

Decide early on

- Don’t forget operational phase

Next Up

Ensuring and Improving the Quality of Log Files