

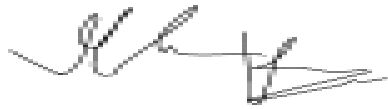
Name: Ilhan Raja

CSCE 489/689: Software Security

UIN: 22600562

On my honor, as an Aggie, I have neither given nor received unauthorized aid on this academic

work, nor shall I. e-Signature:



Use Case 1

Title - Build System

Stakeholder

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

System Administrator

Preconditions

Build system is properly cloned from the official repository. All the appropriate directories and source files are in place and ready to be used as part of the build process.

Trigger 1 System Administrator invokes make

Trigger 2 System Administrator invokes make [...] with extra parameters

Postconditions 1 logappend and logread are produced in the build directories

Postconditions 2 logappend and log read are produced in the build directories with special build

Main Success Scenario 1 make succeeds without error

Main Success Scenario 2 make with extra parameters for special build succeeds without error

Exceptions

- source files are not present in the build system
- make fails due to compilation or linkage error
- make with [...] extra parameters fails
- library dependencies are not satisfied
- logappend and logread files are not present in the build directory

Use Case 2

Title - Staff entering hospital

Stakeholders

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Logging System

Preconditions

Staff member should not already be in the hospital

The log is in a valid and ready to append state

Trigger

A staff member enters the hospital and utilizes the mechanism that triggers the logging system to record the entry into the hospital

Postconditions

The staff member's entry into the hospital is recorded by the logging system. The log is in a valid state after. Details such as the staff member being a doctor or nurse, the timestamp, and their name are included in the record.

Main Success Scenario

Doctor James Harden enters the hospital through the main entrance on 2/02/2020 at 2:02 am. The log is successfully able to verify the integrity of the log. The log recording this event contains this information so that when queried, it can take this event into account.

Exceptions

- log file does not exist, so attempt creation
if cannot be created, then exit with error condition
- log event cannot be verified. if so, exit with error condition

- the most recent timestamp of a logged event is more or as recent as the current one, if so exit with error condition
- the doctor or nurse is already in the hospital. exit with error condition

Use Case 3

Title - Staff exiting hospital

Stakeholders

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Logging System

Preconditions

Staff member be in the hospital

The log is in a valid and ready to append state

Trigger

A staff member exits the hospital and utilizes the mechanism that triggers the logging system to record the entry into the hospital

Postconditions

The staff member's exit from the hospital is recorded by the logging system. The log is in a valid state after. Details such as the staff member being a doctor or nurse, the timestamp, and their name are included in the record.

Main Success Scenario

Doctor James Harden exits the hospital through the main entrance on 2/02/2020 at 2:02 am. The log is successfully able to verify the integrity of the log. The log recording this event contains this information so that when queried, it can take this event into account.

Exceptions

- log file does not exist, so attempt creation

if cannot be created, then exit with error condition

- log event cannot be verified. if so, exit with error condition
- the most recent timestamp of a logged event is more or as recent as the current one, if so exit with error condition
- the doctor or nurse is currently in a room, if so exit with error condition
- the doctor or nurse is not in the hospital, if so exit with error condition

Use Case 4

Title - Staff entering a room

Stakeholders

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Logging System

Preconditions

Staff member must be in the hospital

Staff member must not be in a room somewhere

The log is currently in a valid and ready to log state

Trigger

A staff member enters a room.

Postconditions

The staff member's entry into a room is recorded by the logging system. The log is in a valid state after. Details such as the staff member being a doctor or nurse, the timestamp, and their name are included in the record.

Main Success Scenario

Doctor James Harden enters Room 420 on 2/02/2020 at 5 am. The log is successfully able to verify the integrity of the log. The log recording this event contains this information so that when queried, it can take this event into account.

Exceptions

- log file does not exist, so attempt creation
if cannot be created, then exit with error condition
- log event cannot be verified. if so, exit with error condition
- the most recent timestamp of a logged event is more or as recent as the current one, if so exit with error condition
- the doctor or nurse is not in the hospital
- the doctor or nurse is currently in a room already

Use Case 5

Title - Staff exiting a room

Stakeholders

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Logging System

Preconditions

Staff member must be in the hospital

Staff member must be in a room somewhere

The log is currently in a valid and ready to log state

Trigger

A staff member exits a room.

Postconditions

The staff member's exit from a room is recorded by the logging system. The log is in a valid state after. Details such as the staff member being a doctor or nurse, the timestamp, and their name are included in the record.

Main Success Scenario

Doctor James Harden exits Room 420 on 2/02/2020 at 12 pm. The log is successfully able to verify the integrity of the log. The log recording this event contains this information so that when queried, it can take this event into account.

Exceptions

- log file does not exist, so attempt creation
if cannot be created, then exit with error condition
- log event cannot be verified. if so, exit with error condition
- the most recent timestamp of a logged event is more or as recent as the current one, if so exit with error condition
- the doctor or nurse is not in the hospital
- the doctor or nurse is not currently in a room

Use Case 6

Title - Using logappend in batch mode

Stakeholders

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Logging System

Preconditions

The log is in a valid and ready to append state.

The batch log file exists.

The batch file is valid and only contains the arguments to logappend in batches

Trigger

System Administrator issues a command to append logs in batch mode

Postconditions

The batch commands are appended to the log. For each logging event appended in batch mode, details such as the staff member being a doctor or nurse, the timestamp, and their name are included in the record.

Main Success Scenario

Doctor James Harden exits Room 420 on 2/02/2020 at 12 pm. The log is successfully able to verify the integrity of the log. The log recording this event contains this information so that when queried, it can take this event into account.

Exceptions

- log file does not exist, so attempt creation
if cannot be created, then exit with error condition
- log event cannot be verified. if so, exit with error condition
- the most recent timestamp of a logged event is more or as recent as the current one, if so exit with error condition
- the doctor or nurse is not in the hospital
- the doctor or nurse is not currently in a room

Abuse Case 1

Title - Attacker spoofs log events

Stakeholders

Attacker

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Attacker

Preconditions

Attacker has the capability to invoke logappend at will

The log before invoking logappend is in a valid and ready to append state

Attacker does not know the authentication token to create the log

Trigger

Attacker invokes logappend arbitrarily

Postconditions

The log contains records of staff members moving to or leaving from places where they haven't. The log is incorrect but in a valid state.

Main Success Scenario

Attacker appends to the log that Doctor James Harden has left the hospital at 2/03/2020 for a basketball game. The log will attempt verification of this log. With malicious input or a specially crafted argument list, we can cause logappend to verify against this log event query and successfully log the event. The end goal is to successfully log an event that did not happen in real life

Mitigations

Carefully and correctly validate input

Abuse Case 2

Title - Malicious log file input could lead to buffer overflow

Stakeholders

Attacker

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Attacker

Preconditions

Attacker has the capability to invoke logappend/read at will

Attacker does not know the authentication token to create the log

Trigger

Specially crafted input payload will cause buffer flow

Postconditions

If logappend/read is run as root, you can gain code execution in the shell or environment that it was running in. This could lead to a plethora of new security violations.

Main Success Scenario

Attackers use fuzzing to find an input argument list or log file that causes a crash. After analyzing the nature of the crash, attackers craft specially made input to take control of the machine using a buffer overflow, rop/jop, etc. This opens up the machine to a new class of security violations if a shell with elevated privileges is the outcome.

Mitigations

Fuzz yourself to find these bugs before they do!

Abuse Case 3

Title - Broken Crypto and Signatures

Stakeholders

Attacker

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Attacker

Preconditions

Attacker has the capability to invoke logappend/read at will

Attacker does not know the authentication token to create the log

Trigger

None, this could happen at any time

Postconditions

Attackers can break crypto by using a technique to find the key, and break signatures on the log files. Depending on the technique used, the difficulty varies, but with weaker crypto and signature validation, this is possible. With broken crypto, you can produce plaintext or a digital signature on log files a lot more easily.

Main Success Scenario

Attackers use a technique to resolve keys and tokens for a given log file set. Once you know this, you can produce a plaintext log file, tamper with it, and then encrypt and sign it to produce a log file that represents a false reality. The log file tampered with should be in a valid state with a correct key and appropriate modifications.

Mitigations

Don't roll your own crypto and make your crypto hard to beat!

Abuse Case 4

Title - Racing timestamps

Stakeholders

Attacker

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Attacker

Preconditions

Attacker can invoke logappend at will

Attacker does not know the authentication token

Trigger

Attacker can cause racing logappends in batch or in single to known doctors and nurses in the hospital.

Postcondition

If log append is raced with, events with timestamps that appear the same to a raced event can cause the real events to be rejected by the logappend program.

Main Success Scenario

Attackers send many logappend queries for known doctors and nurses in the hospital with timestamps in real time so that when real events come in, they will race with faked events and the true events will be rejected in real time. The adversary may become aware of the rejections, but it won't matter because they will be indistinguishable from faked queries.

Mitigations

Limit the amount of resources that can invoke logappend and perform locking on resources if needed

Abuse Case 5

Title - No failure log

Stakeholders

- Attacker
- Logging System
- Hospital Staff
- System Administrator
- Hospital Administration

Primary Actor

- Attacker

Preconditions

- None

Trigger

- None

Postconditions

No capability for the system admin to distinguish between attacks and real representations of hospital activity.

Main Success Scenario

All the logappend and logread programs do if an error condition is met is write an invalid to stdout and nothing else to the actual log file. If none of this is kept track of, we won't be able to distinguish between attempts to fake events and real events.

Mitigations

Start a failure log?

Abuse Case 6

Title - Modify binary of logappend

Stakeholders

Attacker

Logging System

Hospital Staff

System Administrator

Hospital Administration

Primary Actor

Attacker

Preconditions

Attacker can modify filesystem

Trigger

Binary patch logappend and logread's bytes to do the opposite or jump somewhere else in memory when performing operations.

Postconditions

The logic of logappend will be changed to fit the needs of the attacker.

Main Success Scenario

Patch binary to do whatever you want it to do instead. For example, if there are checks against the original token, patch those out with your own inline assembly jmps, nops, etc. Or you can do much more. Might need to resign it if we are on Mac, etc. Finally, you'll be able to write

your own logs and represent the state of the hospital much differently than in real life. Thus, you can do something bad in person.

Mitigations

N/A, protect filesystem better

Requirements

Software

1. logappend shall append the correct log information to the log file provided that the parameters to the program are given correctly as stated by the specification such as the timestamp, token, name of the doctor or nurse, the kind of event, the room id, the log file path, and the batch file path.
2. logappend shall exit gracefully when the following error conditions occur. It shall print out “invalid” to stdout and return error codes when such a condition occurs.
 - the provided path to the log file does not exist
 - the provided path to the batch file does not exist and batch mode is specified
 - the timestamp is greater or equal to the most recent timestamp
 - the event provided is an arrival/departure to a room and the doctor/nurse is either not in the hospital or the room is equal to the one they are currently in
 - required arguments to the logappend command are not provided
3. logread reads a log file constructed by logappend and displays information about the state of the hospital if the user passes the authentication token and a valid path to the log file. logread shall display all the doctors and nurses in the hospital and the rooms they are in, and the rooms they have occupied previously.
4. logread shall exit gracefully when the following error conditions occur. It shall print out “invalid” to stdout and return error codes when such a condition occurs.
 - the provide path to the log file to read does not exist or any I/O error occurs when attempting to read from the file
 - arguments passed to logread are incomplete or invalid
 - a member of the hospital is both labeled as a doctor and nurse

5. logread shall display no information when given a doctor or nurse that does not exist in the hospital for a logappend log file(s)

Security

1. logappend and logread must use authentication tokens to verify integrity of the files
2. logappend and logread must exit when integrity checks fail. This will occur in cases when the authentication token is invalid, an entry in a log file cannot be verified to be created with the provided authentication token, or the log file has been corrupted.
3. ensure that data used within the program is safely using the correct bounds dedicated for it to reduce the potential for buffer overflow or denial of service attacks.
4. the build system for the passage or failure of tests against logappend or logread cannot be invoked using Internet Access or require Internet Access to execute
5. the logging system must utilize some sort of crypto technology to ensure safe storage of the logging data to ensure that attackers cannot read the data in plaintext
6. the logging system should use the original authentication token as the initialization vector as part of some encryption scheme to protect the logging data
7. the log files shall use some sort of digital signature to verify against tampering.
8. containerization must be used so that the logappend executable cannot be invoked if access to the target system is achieved
9. directories must be read only to normal users of the system
10. correct permissions must be applied to files, directories of the executables, logging data, and source files so that users cannot tamper with them undesirably
11. the logging must always be active. if inactive, unrecorded events will occur and thus can cause physical insecurity of the hospital