Name: MINIMUM REQUIREMENTS UIN: 000000000

CSCE 489/689: Software Security

On my honor, as an Aggie, I have neither given nor received unauthorized aid on this academic work, nor shall I.
e-Signature: MINIMUM REQUIREMENTS Date: September 9, 2018

Use Cases

UC 1

Title	Make
Stakeholders	1) Logger (subject that runs `logappend` and `logread`, "the logging system") 2) System Administrator
Primary Actor	System Administrator
Preconditions	1) all C/C++ source code for `logappend` and `logread` exists in `build/` directory. 2) `Makefile` exists in `build/` directory. 3) System Administrator's working directory is `build/` on `compute.cse.tamu.edu`.
Trigger 1	System Administrator invokes `make`
Trigger 2	System Administrator invokes `make coverage`
Postconditions 1	1) `logappend` and `logread` executables exist in `build/` directory.
Postconditions 2	1) `logappend` and `logread` are compiled with coverage flags. 2) `logappend` and `logread` executables exist in `build/` directory.
Main Success Scenario 1	1) `make` completes without error.
Main Success Scenario 2	1) `make coverage` completes without error.
Exceptions	1) any source code is not in `build/`. *Response: grade = 0.* 2) `make` fails. *Response: grade = 0.* 3) `make coverage` fails. *Response: grade = 0.* 4) `logappend` and `logread` executables do not exist in `build/` directory. *Response: grade = 0.* 5) source code for `logappend` and `logread` are not written in C/C++. *Response: grade = 0.* 6) any part of the source code for `logappend` and `logread` is plagiarized. *Response: violation filed with AHSO, penalty = F*.*

UC 2

Title	Log staff entering hospital
Stakeholders	1) Logger (subject that runs `logappend` and `logread`, "the logging system") 2) Hospital Staff (Doctors and Nurses) 3) System Administrator 4) Hospital Administration
Primary Actor	Logger
Preconditions	1) Staff member must not already be in the hospital. 2) The specified log is in a valid state.
Trigger	Staff member enters the hospital.
Postconditions	1) A record of the staff member entering the hospital is in the log. The record should include that the person who entered was a doctor or nurse, their name, and the time they entered. 2) The specified log is in a valid state.
Main Success Scenario	1) Doctor Ritchey enters the hospital through the main entrance at 7:53:04 AM on 9 September 2018.

2) Logger verifies the authenticity of the log.
3) Logger appends the event "Doctor Ritchey arrived at the hospital at 7:53:04 AM on 9 September 2018" to the log.

Exceptions
1) Log file does not exist. *Response: create log file.*
   i) Log file cannot be created. *Response: exit with an error condition.*
2) Log file authenticity cannot be verified. *Response: do not log the event; exit with an error condition.*
3) The most recent event in the log has a timestamp after 7:53:04 AM on 9 September 2018. *Response: do not log the event; exit with an error condition.*
4) Doctor "Ritchey" is already in the hospital. *Response: do not log the event; exit with an error condition.*

UC 3

Title Log staff entering a room

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")
2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) Staff member must be in the hospital.
2) Staff member must not be in any room.
3) The specified log is in a valid state.

Trigger Staff member enters the hospital.

Postconditions
1) A record of the staff member entering the room is in the log. The record should include the room the person entered, that the person who entered was a doctor or nurse, their name, and the time they entered.
2) The specified log is in a valid state.

Main Success Scenario
1) Nurse Bregger enters room 489 at 12:39:18 PM on 9 September 2018.
2) Logger verifies the authenticity of the log.
3) Logger appends the event "Nurse Bregger entered toom 489 at 12:39:18 AM on 9 September 2018" to the log.

Exceptions
1) Log file does not exist. *Response: exit with an error condition.* This should not happen due to precondition of already being in the hospital.
2) Log file authenticity cannot be verified. *Response: do not log the event; exit with an error condition.*
3) The most recent event in the log has a timestamp after 12:39:18 AM on 9 September 2018. *Response: do not log the event; exit with an error condition.*
4) Nurse "Bregger" is in a room already. *Response: do not log the event; exit with an error condition.*
5) Nurse "Bregger" is not in the hospital. *Response: do not log the event; exit with an error condition.*

UC 4

Title Log staff exiting hospital

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")
2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) Staff member must be in the hospital.
2) Staff member must not be in any room.
3) The specified log is in a valid state.

Trigger Staff member exits the hospital.

Postconditions
1) A record of the staff member exiting the hospital is in the log. The record should include that the person who exited was a doctor or nurse, their name, and the time they exited.
2) The specified log is in a valid state.

Main Success Scenario
1) Doctor Spock exits the hospital through the north fire escape at 12:45:09 PM on 9 September 2018.
2) Logger verifies the authenticity of the log.
3) Logger appends the event "Doctor Spock exited the hospital at 12:45:09 PM on 9 September 2018" to the log.

Exceptions
1) Log file does not exist. *Response: exit with an error condition.* This should not happen due to precondition of already being in the hospital.
2) Log file authenticity cannot be verified. *Response: do not log the event; exit with an error condition.*
3) The most recent event in the log has a timestamp after 12:45:09 PM on 9 September 2018. *Response: do not log the event; exit with an error condition.*
4) Doctor Spock is in a room. *Response: do not log the event; exit with an error condition.*
5) Doctor Spock is not in the hospital. *Response: do not log the event; exit with an error condition.*

UC 5

Title Log staff exiting a room

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")
2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) Staff member must be in the hospital.
2) Staff member must be in a room.
3) The specified log is in a valid state.

Trigger Staff member exits a room.

Postconditions
1) A record of the staff member exiting the room is in the log. The record should include that person exited a room (maybe which room), that the person who exited was a doctor or nurse, their name, and the time they exited.
2) The specified log is in a valid state.

Main Success Scenario
1) Nurse Florence exits room 2007 at 12:45:09 PM on 9 September 2018.
2) Logger verifies the authenticity of the log.
3) Logger appends the event "Nurse Florence exited room 2007 at 12:45:09 PM on 9 September 2018" to the log.

Exceptions
1) Log file does not exist. *Response: exit with an error condition.* This should not happen due to precondition of already being in the hospital.
2) Log file authenticity cannot be verified. *Response: do not log the event; exit with an error condition.*
3) The most recent event in the log has a timestamp after 12:45:09 PM on 9 September 2018. *Response: do not log the event; exit with an error condition.*
4) Nurse Florence is not in room 2007. *Response: do not log the event; exit with an error condition.*

UC 6

Title Append events to log in batch mode

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")

2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) The specified log is in a valid state.
2) The specified batch file exists.
3) The batch file contains `logappend` commands with only the arguments.

Trigger System Administrator issues the command to append events in batch mode

Postconditions
1) The events in the batch file have been added to the log.
2) The specified log is in a valid state.

Main Success Scenario
1) `logappend` is invoked to in batch mode and given a batch file.
2) Logger verifies the authenticity of the log.
3) Logger reads events from batch file and appends each valid event to the specified log.

Exceptions
1) Batch file does not exist. *Response: do not append anything to the log; exit with an error condition.*
2) For a command in the batch file, the log file authenticity cannot be verified. *Response: do not log the event; note the error condition and continue with the next command.*
3) For a command in the batch file, the log file does not exist. *Response: if command and event is valid, create log file.*
   i) Log file cannot be created. *Response: exit with an error condition.*
4) For a command in the batch file, the event is inconsistent with log file. *Response: do not log the event. note the error condition and continue with the next command.*
5) For a command in the batch file, the command invokes batch mode. *Response: do not enter batch mode. note the error condition and continue with the next command.*

UC 7

Title Get status of hospital

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")
2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) The specified log file exists.
2) The specified log is in a valid state.

Trigger System Administrator or Hospital Administrator issues the command to view hospital status

Postconditions
1) The names of staff members in the hospital are displayed.
2) The names of staff member in each occupied room are displayed.
3) The specified log file exists.
4) The specified log is in a valid state.
5) The specified log file has not been modified.

Main Success Scenario
1) `logread` is invoked to get the status of the hospital
2) Logger verifies the authenticity of the log.
3) Logger reads the log data.
4) Logger displays the names of doctors and nurses in the hospital in alphabetical order.
5) Logger displays room-by-room information indicating which doctor or nurse is in which room. Rooms are listed in numerical ascending order, names are listed

in alphabetical order.

Exceptions
1) Log file does not exist. *Response: exit with an error condition.*
2) Log file authenticity cannot be verified. *Response: exit with an integrity violation.*
3) No doctors in hospital. *Response: display empty list of doctors.*
4) No nurses in hospital. *Response: display empty list of nurse.*
5) No staff in room N. *Response: omit room N from room info display.*

UC 8

Title Get room list (path) of staff member

Stakeholders
1) Logger (subject that runs `logappend` and `logread`, "the logging system")
2) Hospital Staff (Doctors and Nurses)
3) System Administrator
4) Hospital Administration

Primary Actor Logger

Preconditions
1) The specified log file exists.
2) The specified log is in a valid state.

Trigger System Administrator or Hospital Administrator issues the command to view path of staff member by name

Postconditions
1) The list of rooms entered by the specified staff member is displayed in chronological order.
2) The specified log file exists.
3) The specified log is in a valid state.
4) The specified log file has not been modified.

Main Success Scenario
1) `logread` is invoked to get the path of a staff member by name
2) Logger verifies the authenticity of the log.
3) Logger reads the log data.
4) Logger displays the list of rooms entered by the specified staff member in chronological order.

Exceptions
1) Log file does not exist. *Response: exit with an error condition.*
2) Log file authenticity cannot be verified. *Response: exit with an integrity violation.*
3) Staff member has not entered any rooms. *Response: display empty list of rooms*

Abuse Cases

AC 1

Title Spoof staff movement using `logappend`

Stakeholders
1) Attacker
2) Logger (subject that runs `logappend` and `logread`, "the logging system")
3) Hospital Staff (Doctors and Nurses)
4) System Administrator
5) Hospital Administration

Primary Actor Attacker

Preconditions
1) Attacker has direct access to `logappend`
2) The log is in a valid state.
3) Attacker does not know the authentication token used to create the log.

Trigger None. Can happen at any time.

Postconditions
1) A record of the staff member moving in the log.
2) The log is in a valid state.
3) The log is incorrect: the staff member is not where the log says they are.

Main Success Scenario
1) Attacker invokes `logappend` to record that "Doctor Evil arrived at the hospital at 11:39:16 AM on 9 September 2018"
2) Logger verifies the authenticity of the log. This should fail, but doesn't due to a defect and/or malicious input.
3) Logger appends the event "Doctor Evil arrived at the hospital at 11:39:16 AM on 9 September 2018" to the log.

Mitigations Left as an excercise for the students.

Enumerating additional abuse cases left as an excercise for the students.

Requirements

Functional

REQ 1 `logappend` shall append staff movement records to a log file when given the relative path to the log file, the authentication token used to create the log (or to use to create the log), the time of the event, the staff affiliation (doctor or nurse) of the staff member, the name of the staff member, the type of event (arrival or departure) and the room ID (if entering or exiting a room).

REQ 2 `logappend` shall exit with an error condition when any of the following conditions occur:

(a) the specified log file does not exist and cannot be created due to an invalid path or any other I/O error.
(b) the specified timestamp is equal to or greater than the most recent timestamp in the specified log.
(c) the event is an arrival to the hospital and the specified staff member (name,type) is already in the hospital.
(d) the event is an arrival to a room and the specified staff member (name,type) is already in a room.
(e) the event is an arrival to a room and the specified staff member (name,type) is not in the hospital.
(f) the event is a departure from the hospital and the specified staff member (name,type) is not in the hospital.
(g) the event is a departure from the hospital and the specified staff member (name,type) is in a room.
(h) the event is a departure from a room and the specified staff member (name,type) is not in the specified room.
(i) batch mode is specified and the specified batch file does not exist.
(j) batch mode is specified in a batch mode command.
(k) any argument to `logappend` is invalid (e.g. a name containing numbers).
(l) any required argument to `logappend` is missing (e.g.missing path to log file).
(m) the arguments to `logappend` are inconsistent (e.g. staff member specified as being both doctor and nurse).

REQ 3 `logappend` in batch mode shall print "invalid" to `stdout` for each line in the specified batch file that results in an error condition and continue processing the rest of the batch file.

REQ 4 `logappend` in batch mode shall exit without an error condition when the specified batch file exists and has a valid path.

REQ 5 When `logappend` exits with an error condition, it shall do the following:

(a) leave the log file unmodified.
(b) print "invalid" to `stdout`.
(c) return code 255.

REQ 6 When `logappend` exits with an integrity violation, it shall do the following:

(a) leave the log file unmodified.
(b) print "integrity violation" to `stdout`.
(c) return code 255.

REQ 7 When `logappend` exits without an error condition, it shall do the following:

(a) update the log file according to the specified event(s).
(b) return code 0.

REQ 8 `logread` shall query a log file and display information about the state of the hospital when given the relative path to the log file, the authentication token used to create the log file, and a query to run against the log (either status or path).

REQ 9 `logread` shall support a status query which displays the names of staff members in the hospital and room-by-room information indicating which staff member is in which room.

(a) Names are listed in alphabetical order.
(b) Rooms are listed in numerical ascending order.

REQ 10 `logread` shall support a path query which displays the rooms that a specified staff member entered while in the hospital.

(a) Rooms are listed in ascending chronological order of entry.

REQ 11 `logread` shall display no information when given a doctor or nurse name that does not exist in the specified log.

REQ 12 `logread` shall exit with an error condition when any of the following conditions occur:

(a) the specified log file does not exist.
(b) the specified log file cannot be read due to an invalid path or any other I/O error.
(c) any argument to `logread` is invalid (e.g. a name containing numbers).
(d) any required argument to `logread` is missing (e.g.missing path to log file).
(e) the arguments to `logappend` are inconsistent (e.g. staff member specified as being both doctor and nurse).

REQ 13 When `logread` exits with an error condition, it shall do the following:

(a) print "invalid" to `stdout`.
(b) return code 255.

REQ 14 When `logread` exits with an integrity violation, it shall do the following:

(a) print "integrity violation" to `stdout`.
(b) return code 255.

REQ 15 When `logread` exits without an error condition, it shall do the following:

(a) return code 0.

SEC 16 `logappend` and `logread` shall use an authentication token to verify the authenticity of log files.

SEC 17 `logappend` and `logread` shall exit with an integrity violation when any of the following occur:

(a) the specified authentication token is incorrect for the specified log file.
(b) an entry in the log cannot be verified as having been created with an invocation of `logappend` using the correct token.
(c) the log file has been corrupted.

Non-functional

REQ 18 `make` must return within 5 minutes.

REQ 19 `logappend` and `logread` shall use at most 1GB of memory during operation.

REQ 20 `logappend` in non-batch mode shall have an average throughput of at least 1 record per second.

REQ 21 `logread` shall display hospital status information within 30 seconds of invocation.

REQ 22 `logread` shall display staff member path information within 30 seconds of invocation.

SEC 23 `make` must function without Internet access.

Enumerating additional requirements left as an excercise for the students.