Surgeon App Threat Model

Owner:
Reviewer:
Contributors:
Date Generated: Tue Sep 26 2023

Executive Summary

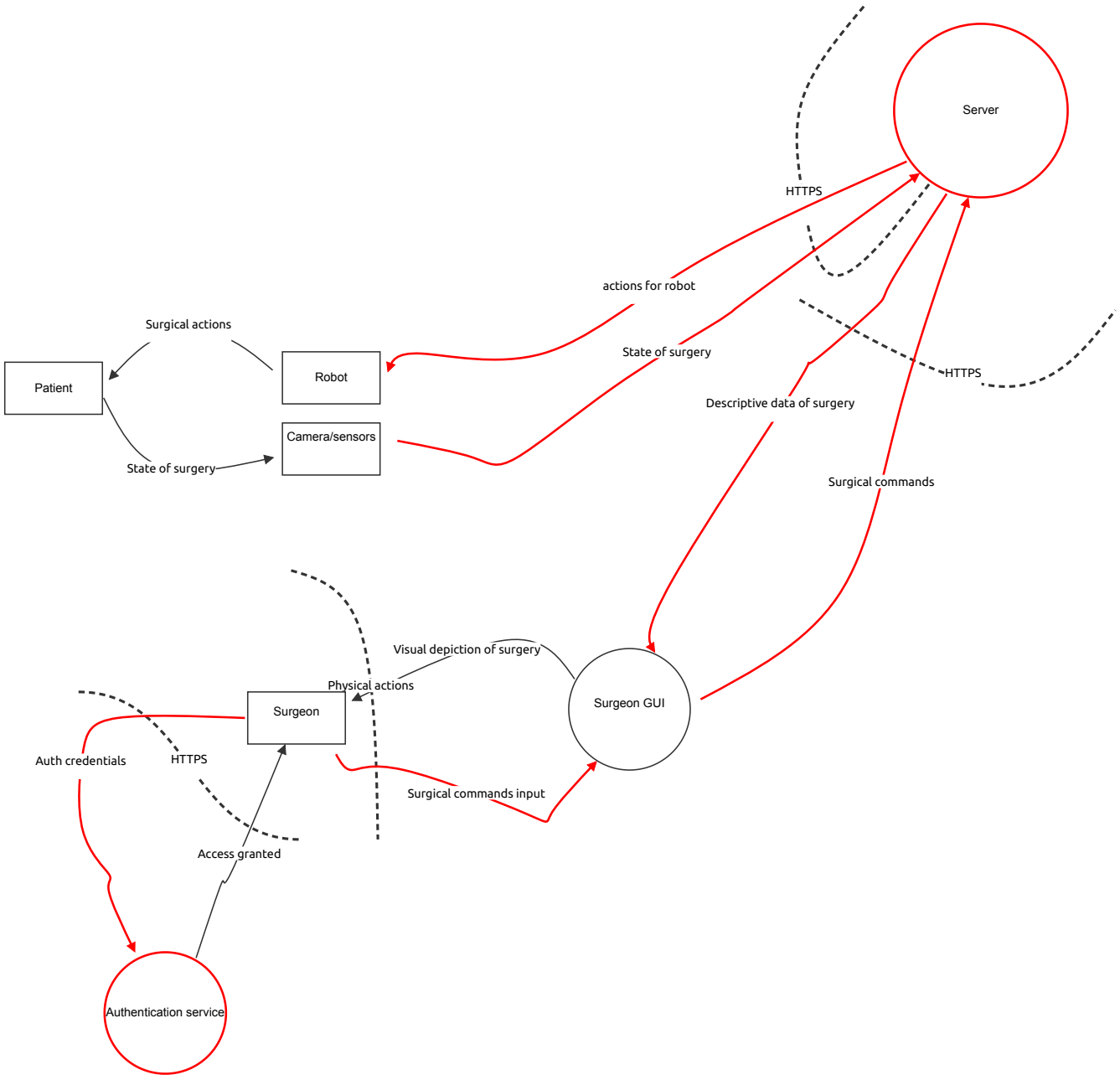
High level system description

This system allows a surgeon in one city to assist a surgeon in another city with an operation, via internet connection.

Summary

Total Threats	14
Total Mitigated	4
Not Mitigated	10
Open / High Priority	6
Open / Medium Priority	4
Open / Low Priority	0
Open / Unknown Priority	0

Surgeon App Threat Modeling



Surgeon App Threat Modeling

Visual depiction of surgery (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

State of surgery (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Surgical actions (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Access granted (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

State of surgery (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Bad actor modifies state of surgery data	Tampering	High	Open		A bad actor could modify data about the state of a surgery, leading the surgeon to believe the patient is in a different state than they actually are in.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. Although this doesn't prevent tampering altogether, it does mean that if data is tampered with, the surgeon's GUI client can detect tampering and not display tampered data. We can try to increase the security of channels that data is traveling through to decrease the risk of data being tampered with in the first place.
8	Bad actor discovers state of surgery	Information disclosure	Medium	Mitigated		By intercepting this data flow, a bad actor could learn what the state of the surgery is.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. This means that the SSL encryption protocol is used.

actions for robot (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Bad actor modifies actions for robot	Tampering	High	Open		If a bad actor has access to this data flow, they can modify or introduce their own actions for the surgical robot to take. For obvious reasons, this is dangerous.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. Although this doesn't prevent tampering altogether, it does mean that if data is tampered with, the robot end of our system can detect tampering and not act on tampered instructions. We can try to increase the security of channels that data is traveling through to decrease the risk of data being tampered with in the first place.
6	Bad actor intercepts future actions of robot	Information disclosure	Medium	Mitigated		If a bad actor has access to this data flow, they can see what actions the robot will perform next.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. This means that the SSL encryption protocol is used.

Surgical commands (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Bad actor modifies commands	Tampering	Medium	Open		If a bad actor has access to this data flow, they can modify the commands sent by the surgeon to the robot.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. Although this doesn't prevent tampering altogether, it does mean that if data is tampered with, the robot end of our system can detect tampering and not act on tampered instructions. We can try to increase the security of channels that data is traveling through to decrease the risk of data being tampered with in the first place.
15	Bad actor intercepts commands	Information disclosure	Medium	Mitigated		If a bad actor intercepts this data flow, they can tell what commands the surgeon is sending to the robot.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. This means that the SSL encryption protocol is used.

Descriptive data of surgery (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Bad actor modifies surgery data	Tampering	High	Open		A bad actor could modify data about the state of a surgery.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. Although this doesn't prevent tampering altogether, it does mean that if data is tampered with, the surgeon's GUI client can detect tampering and not act on tampered data. We can try to increase the security of channels that data is traveling through to decrease the risk of data being tampered with in the first place.
13	Bad actor intercepts surgery data	Information disclosure	Medium	Mitigated		A bad actor could glean information about the state of the surgery.	Mitigated to the extent we can by introducing HTTPS, as opposed to HTTP. This means that the SSL encryption protocol is used.

Auth credentials

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Bad actor gets real surgeon login credentials	Information disclosure	High	Open		If the transmission of login credentials is insecure, a bad actor could intercept them here. Then, the bad actor could impersonate a surgeon, which could have catastrophic consequences.	Transmit login credentials in an encrypted manner (using HTTPS, assuming an internet-based login), and only through secure channels. Even with this mitigation measure, things like a keylogger or looking over someone's shoulder could allow login credentials to get into the wrong hands. Thus, we cannot mark this threat as fully mitigated.

Surgical commands input (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Physical tampering	Tampering	Medium	Open		If a bad actor gains access to the surgeon's keyboard (or whatever hardware the surgeon is using), they can carry out malicious actions.	Physical security protocols, like locking doors and using a badge-in/badge-out system, are best here.

Surgeon (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Server (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	DOS attack	Denial of service	Medium	Open		If a bad actor can attack the server (via DDOS or some other attack), they can shut this service down.	Use a firewall to secure the server. Increase automated security protocols, such as detecting abnormal traffic and shutting it down. Diligently implement monitoring solutions for the server. Use a load balancer to distribute traffic across several servers.
10	Bad actor modifies data	Tampering	High	Open		If a bad actor has access to the server, they can modify any of the data in the application as it passes through.	Ensure the server is extremely secure, which is most easily done by using up-to-date security software, implementing a firewall, and having strong monitoring and alerting systems.

Surgeon GUI (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Camera/sensors

(Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Patient (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Robot (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication service (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Malicious actor authentication	Spoofing	High	Open		If a malicious actor tampers with authentication, they can pretend to be the real surgeon and cause major problems.	Make the authentication as secure as possible, using at least two-facor auth and protecting the service with strong firewalls, cybersecurity software, and monitoring tools. Some sort of biometric authentication could also be a good idea. Even with these measures, however, we cannot be completely sure that our system won't be infiltrated. Thus, we mark this issue as open.
16	Bad actor gives themselves admin priviledges	Elevation of privilege	Medium	Open		If a bad actor gains access to the authentication service, they can give themselves admin priviledges, allowing them to make undesired changes to the system.	Use firewalls, cybersecurity software, and monitoring tools to be aware of (and hopefully stop) potential breaches. Nonetheless, breaches are still possible, so this threat is "open".