



DREAD analysis and mitigation

for a medical mannequin
as described by Glisson et
al (2015)

	Damage	Reproducibility	Exploitability	Affected users	Discoverability
week authentication / bruteforce	1	2	2	1	3
denial of service	1	2	2	1	1
man in the middle	1	3	3	1	3

0 = no risk

1= some risk

2= elevated risk

3 = maximum risk.

Mitigations

- Two factor authentication (2FA)
- use state of the art wireless protocols (WPA-2, Bluetooth) instead of outdated and unsecure protocols (WPA)
- Deploy VPN
- Deploy firewall / limit logins to a specified IP address or range
- Monitor the network for intrusion via Intrusion Detection System (IDS)
- Deactivate vulnerable features (WPS) of the network
- Use wired connection only (e.g., cross-link cable), if feasible
- Add authentication and encryption in the application layer of the system software
- Limit failed login attempt
- Do not use default port, edit the port line in sshd_config file
- Use Captcha
- unique login URLs