
STRIDE and DREAD

CHAN KEI YIU YVONE

HUNG WEI LIN

THIEN LIU

YUSUF FAHRY



STRIDE

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Vulnerabilities identified:

1. Network security solutions - Brute force attack against router PIN
2. Network protocol - Denial of service attack

DREAD Rating Level

DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5



Brute Force Attack

Category	Score
Damage	2
Reproducibility	3
Exploitability	2
Affected Users	2
Discoverability	3
DREAD Risk: 2.4	

Denial of Service

Category	Score
Damage	3
Reproducibility	3
Exploitability	3
Affected Users	3
Discoverability	3
DREAD Risk: 3.0	

Assumptions

- Denial of service has a higher risk (DREAD risk 3.0) than brute force attack (DREAD risk 2.4) based on the following assumptions:
 - Access point configuration can be reset and changed quickly
 - Information inside iStan is not real patient data
 - The system does not contain personal information about users
 - All staff members are well-trained to perform training without iStan
 - Troubleshooting guidelines are available

References

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. and Murukan, A.
(2003). *Threat Modelling*