Seminar 2

DREAD Threat Analysis

May 12, 2021

Kalina, Marzio, Sebastian, Shoumik

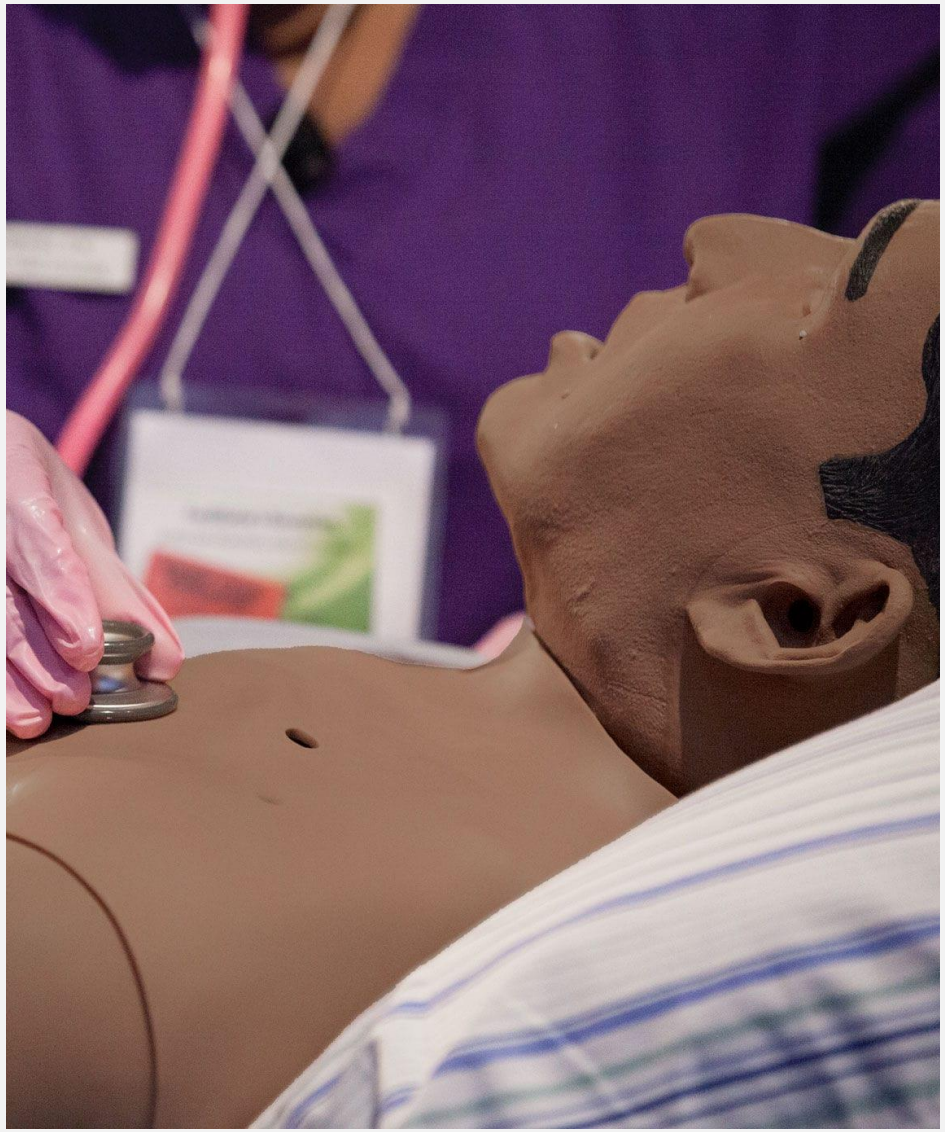
Background

Case Study: iStan medical mannequin

Vulnerabilities:

- **Network Security Solution:** breached via brute force attack using Reaver against the Router's Personal Identification Number (PIN)
- **Network Protocol:** non-availability through a denial of service (DoS) attack
- **Confidentiality and Integrity of Data:** Unencrypted connections may be at risk of sniffing and tampering attacks leaving critical data exposed

	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	
	D	R	E	A	D	
Network Security Solution	3	3	3	2	3	**2.80**
Network Protocol	1	3	3	2	3	**2.40**
C+I of Data	3	2	2	2	2	**2.20**



Source: Compromising a Medical Mannequin (2015)

Potential Mitigations

The medical mannequin relies on two types of dependencies: **direct** and **indirect**

Direct:

- Properly configured access point and secure network configuration (e.g. WPA-2)
- Disabling Static and enabling dynamic cypher for TLS
- Use of TLS 1.2 or above
- IDS + Active Network Monitoring mitigate the risk of DoS attacks
- Prevention of Spoofing to ensure legitimate traffic

Indirect:

- Properly trained nursing students and faculty staff can help prevent mentioned ripple effects
- Security regulations may help enforce strict(er) security standards for the manufacturing of such medical equipment

Reference List

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth).