Compromising a Medical Mannequin

DREAD Analysis

Group 5

By

1. Czeska Stanley
2. Dario De Giorgi
3. David Luvaha
4. Yibeltal Mengesha
5. Kin Wong
6. Aimalohi Odia

Scope

- Top three vulnerabilities
- DREAD analysis

Top three vulnerabilities

1. **Brute Force Attacks**

Kaspersky Lab (2021) defines brute force attacks as the use of extreme force to get access to private account by predicting authentication information, cipher keys or hidden content through trial and error method.

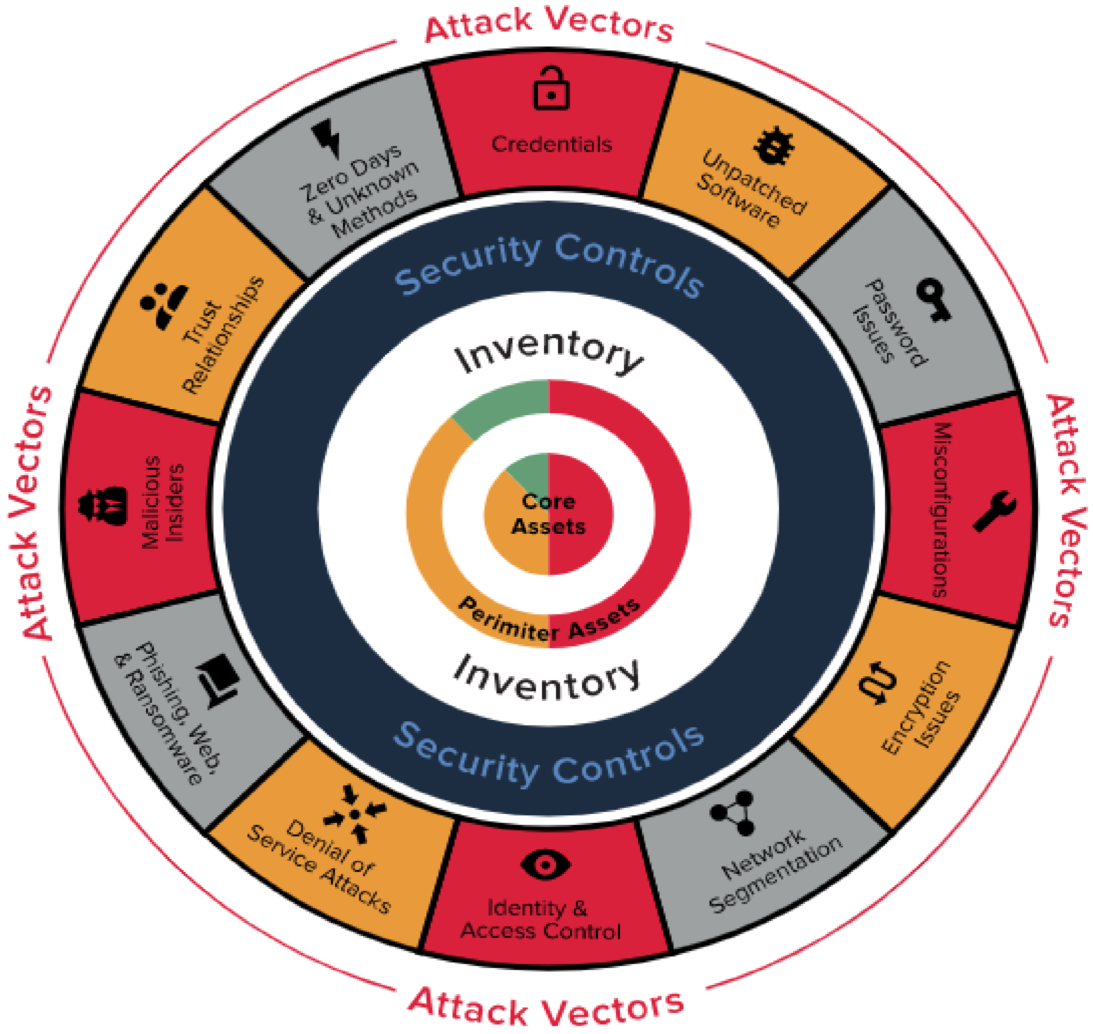
2. Denial of Service (DoS) Attack

Norton life lock & Steve (Weisman 2021) defines DoS attack as holding website's resources at ransom to prevent users' access to the same.

3. Security Control Attack

A security control often consists of management security, operation security and physical security. A security control attack would be an attack on one of these 3 measure

Security Control Attack cont’



Adopted from https://www.balbix.com/insights/what-is-cyber-security-posture/

DREAD analysis

According to Ben-Tzur(2007) DREAD is a methodology for risk rating. Every vulnerability is graded as follows:

1. **D**amage potential(**0-Low, 5- Sensitive, 10- very Sensitive**)
2. **R**eproducibility(**0- Very difficult to reproduce, 5-Easy, 10- Very Easy**)
3. **E**xploitability(**0-Very skilled, 5- skilled, 10-not skilled**)
4. **A**ffected Users(**0-few users, 5 – some users, 10 –all users**)
5. **D**iscoverability(**0- unlikely, 5- accessible to few users, 10 published**)

Rating = (D+R+E+A+D)/5

DREAD Ratings for Medical Mannequin

THREAT	D	R	E	A	D	RATING	REMARKS
Brute Force Attacks	5	10	10	10	10	9	HIGH
Denial of Service (DoS) Attack	7	9	10	10	10	9.2	HIGH
Security Control Attack	5	9	10	10	10	8.8	HIGH

Which is the risk with the highest rating? What assumptions have you made? Denial of Service (DoS) Attack

References

Ben-Tzur , C.(2007) *Threat modelling with SRIDE and Dread* slide Toronto Area Security Klatch Available from: https://www.slideshare.net/chuckbt/stride-and-dread?qid=6421019f-f9f1-4c13-a267-11fe70a294d7&v=&b=&from_search=2 [Accessed 9 May 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015), Compromising a Medical Mannequin. Available from: https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf [Accessed 9 May 2021].

Kaspersky Lab.(2021) Brute Force Attack: Definition and Examples. Available from: https://www.kaspersky.com/resource-center/definitions/brute-force-attack [Accessed 9 May 2021].

Norton life lock& Steve,W. (2021) What are Denial of Service (DoS) attacks? DoS attacks explained. Available from: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html [Accessed 9 May 2021].

Compromising a Medical Mannequin Potential Mitigation

Group 5

By

1. Czeska Stanley
2. Dario De Giorgi
3. David Luvaha
4. Yibeltal Mengesha
5. Kin Wong
6. Aimalohi Odia

Scope

- Potential Mitigation
- Why hospitals use wireless enabled pace maker
- Does this type of application make any difference to your DREAD analysis and mitigations?

Potential Mitigation

- Kaspersky Lab (2021) suggests Salt the hash, Two-factor authentication, Password sensitization, High encryption rates and Account shut down after excessive login attempts as some of the solutions to mitigate brute force attack
- Halperin et al (2015) suggest cooperation between device manufacturers, cyber security experts and medical specialists to create better guidelines and hardware.
- Gollakota et. al., (2011) suggest the development of non- intrusive medical hardware that safeguard the hardware from outgoing and incoming signals
- Diallo et. Al (2014) support creation of wireless solutions that have quicker query processing times.
- Norton life lock& Steve (Weisman 2021) suggests using hardware that scans packets and blocks malicious packets and employing anti- distributed denial-of-service (DDoS) technology as a shield.

Why do hospitals use wireless enabled pace maker?

According to Clery(2015) Medical devices like insulin pumps, glucose monitors, and pacemakers or defibrillators are linked with hand-held controller using Bluetooth. The controller or the device is connected to the Internet by means of Wi-Fi so that data can be sent directly to clinicians.

Any difference to your DREAD analysis and mitigations?

NO

References

Clery, d. (2015) Could a wireless pacemaker let hackers take control of your heart?.
Available from:
https://www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart
[Accessed 9 May 2021].

Diallo, O., Rodrigues, C., Sene, M., and Niu, J.(2014) Real-Time Query Processing Optimization for Cloud-Based Wireless Body Area Networks," Information Sciences:0).
Available from:
http://www.caehealthcare.com/eng/patient-simulators/istan
[Accessed 9 May 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015), Compromising a Medical Mannequin. Available from: https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf [Accessed 9 May 2021].

Gollakota, S., Hassanieh, H., Katabi,D & Fu, K (2011) They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices.
Available from:
https://groups.csail.mit.edu/netmit/IMDShield/paper.pdf
[Accessed 9 May 2021].

Halperin, D., Heydt-Benjamin, T., Ransford, B., Clark, S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W.(2008) Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. Proceedings of the 2008 IEEE Symposium on Security and Privacy. pp. 129-142.
Available from:
https://www.secure-medicine.org/hubfs/public/publications/icd-study.pdf [Accessed 9 May 2021].

Kaspersky Lab.(2021) Brute Force Attack: Definition and Examples.
Available from:
https://www.kaspersky.com/resource-center/definitions/brute-force-attack [Accessed 9 May 2021].

Norton life lock& Steve,W. (2021) What are Denial of Service (DoS) attacks? DoS attacks explained.
Available from:
https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html
[Accessed 9 May 2021].

Thanks