Unit 4 Seminar Preparation

Threat Modelling Exercises

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Read Shostack (2018) chapters 3 – 5 (that cover STRIDE and DREAD, Attack Trees and Attack libraries) as well as Spring et al (2021) (that discusses the history and some failings with CVSS) and then create a threat model based on one of the following scenarios:

1. A large international airport based in the United States of America.
2. A large international bank based in the UK.
3. A large nuclear power station in France.

You should use the Threat modelling Manifesto, the OWASP Threat modelling Cookbook and the ATT&CK libraries to inform your model design. Be prepared to share and discuss your designs at the seminar session this week.

You should also add your individual designs to your e-portfolio.

---

2. A large international bank based in the UK

Threat modelling is an essential apect of the risk assessment process as these allow developers and security personnel to “pinpoint design and implementation issues that require mitigation, whether it is early in or throughout the lifetime of the system” (Braiterman et al., n.d). The treat models below were created using data from the first ten attacks of CAPEC Mitre’s “OWASP related attack list” (2021, see appendix I) as these attacks are often leveraged against financial institutions.

The first threat model is a STRIDE attack table outlining the type of breaches that can occur if an attack is successfully exploited. STRIDE is a mneumonic diagram that consists of six attack types: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (Shostack, 2014). *Table 1* illustrates the STRIDE taxonomy for our sample data. This type of table describes the category of an attack, but not the severity or possible attack path.

Table 1: STRIDE Taxonomy of Sample Data

Attack Vulnerability	S	T	R	I	D	E
Blind SQL Injection		X		X		
Buffer Overflow via Environmental Variables		X		X		X

Embedding NULL Bytes	X	X	X
Session Credential Falsification through Prediction			X
Session Fixation			X
Cross-site Request Forgery	X	X	X
Cross-site Scripting (XSS)	X	X	
SQL Injection	X	X	X
Using Unicode Encoding to Bypass Validation Logic	X		
Xpath Injection		X	X

The second threat model is a threat profile, as these display the severity of a given attack according to a rating system which spans from ‘very high’ to ‘very low’ (T*able 2*). Mitre uses CVSS to rate their attack vulnerabilities, and while this method has been criticised as unreliability mathmatically CVSS continues to be the standard against which attack ratings are compared (Spring et al., 2021). Though threat profiles describe the severity of a given attack, they do not describe the category or attack path.

Table 2: Threat Profile of Sample Data

Attack Vulnerability	Attack Likelihood	Attack Severity	Skill Required
Blind SQL Injection	high	high	medium
Buffer Overflow via Environmental Variables	high	high	low
Embedding NULL Bytes	high	high	medium
Session Credential Falsification through Prediction	high	high	low
Session Fixation	medium	high	low
Cross-site Request Forgery	high	very high	medium
Cross-site Scripting (XSS)	high	very high	low
SQL Injection	high	high	low
Using Unicode Encoding to Bypass Validation Logic	medium	high	medium
Xpath Injection	high	high	low

The last threat model is an attack tree, which essentially “depict[s] attacks on a system in tree form. The tree root is the goal for the attack, and the leaves are ways to achieve that goal”

(Chick et al., 2018:8). Attack trees provide a possible attack path, but do not explicitly decribe the severity or category of an attack. An example threat tree can be seen in *Figure 1*.

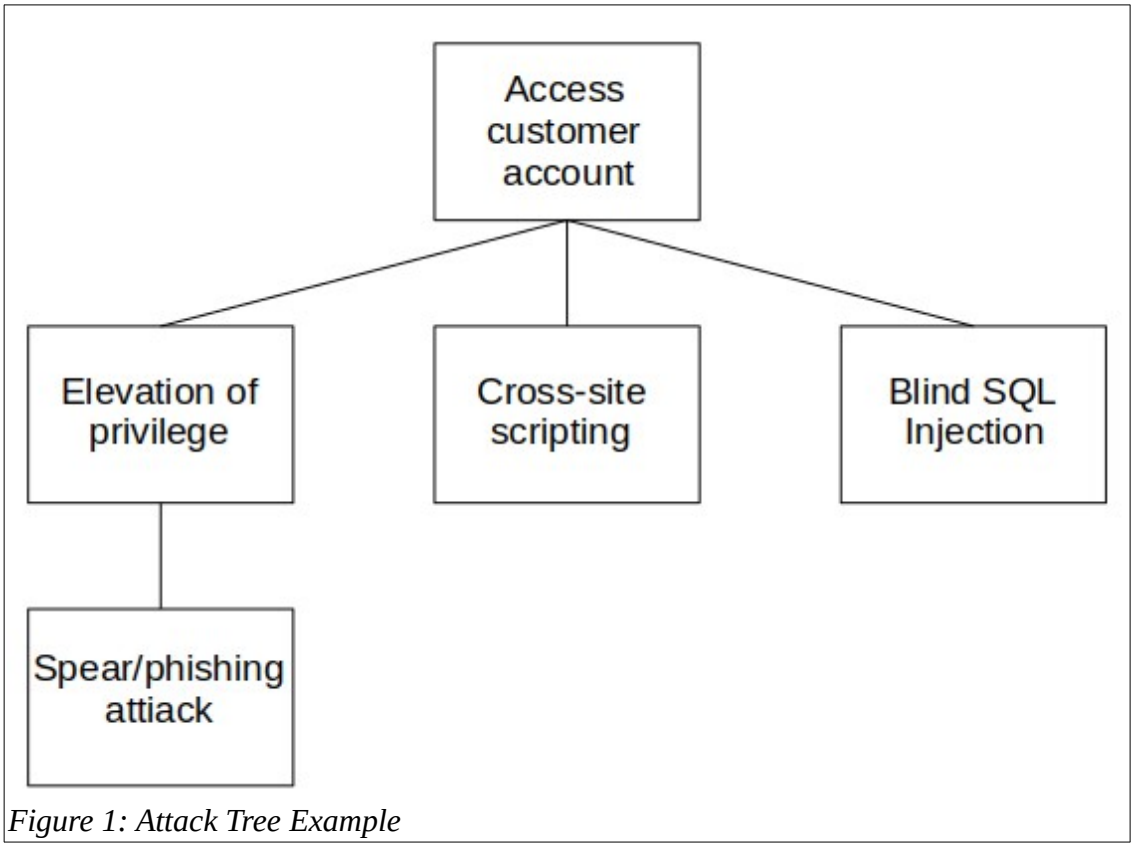

Figure 1: Attack Tree Example

Appendix I

	A	B	C	D	E	F	G
1	Rating: Very high = VH, High = H, Medium = M, Low = L, Very low = VL, no data = n/a						
2	CAPEC URL: https://capec.mitre.org/data/definitions/659.html						
3							
4	Group	Attack	Likelihood of Attack	Typical Severity	Skill Level Required	STRIDE	
5	OSWAP-Related Attacks	7. Blind SQL Injection	high	high	medium	T, I	
6		10. Buffer Overflow via Environmental Variables	high	high	low / high	T, I, E	
7		52. Embedding NULL Bytes	high	high	medium / high	T, I, E	
8		59. Session Credential Falsification through Prediction	high	high	low / medium	E	
9		61. Session Fixation	medium	high	low	E	
10		62. Cross-site Request Forgery	high	very high	medium	T, I, E	
11		63. Cross-site Scripting (XSS)	high	very high	low / high	T, I	
12		66. SQL Injection	high	high	low	T, I, E	
13		71. Using Unicode Encoding to Bypass Validation Logic	medium	high	medium	T	
14		83. Xpath Injection	high	high	low	I, E	
15							

References

Braiterman, Z. et al. (no date) *Threat modeling manifesto*, *Threat Modeling Manifesto*. Available at: https://www.threatmodelingmanifesto.org/ (Accessed: November 27, 2022).

Chick, T. A., N., O'Riordan, Scanlon, T. P., Shevchenko, P., & Woody, C. (2018) *Threat modeling: a summary of available methods*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Mitre. *Common attack pattern enumeration and classification* (2021) *CAPEC*. Available at: https://capec.mitre.org/data/definitions/658.html

Shostack, A. (2014) *Threat modeling : designing for security*. Wiley & sons ltd.

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS? *IEEE Security & Privacy*, 19(2), pp.74–78.