Key SDEV Week 1 Summary

CIA Security Objectives:

Security Objectives for information and information systems include Confidentiality, Integrity and Availability (CIA). This triad is critical and the foundation of cybersecurity today. Each objective is defined as:

- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability - Ensuring timely and reliable access to and use of information.

Not meeting any of these objectives may result in the following:

- A loss of confidentiality is the unauthorized disclosure of information.
- A loss of integrity is the unauthorized modification or destruction of information.
- A loss of availability is the disruption of access to or use of information or an information system.

Additional key concepts of cybersecurity include the risk and potential impact of not fulfilling these fundamental security objectives. Often the impact is categorized as low, medium or high and generally defined as:

- Low impact – limited adverse effects on organizational operations, organizational assets, or individuals.
- Medium impact – serious adverse effects on organizational operations, organizational assets, or individuals.
- High impact – severe or catastrophic effects on organizational operations, organizational assets, or individuals.

From the definitions, there is room for additional clarification and details. For example, some organizations may label certain data sets as high impact if there is any loss of confidentiality, integrity or availability. Each organization uses the above broad definitions to further categorize their data and systems to help understand, prioritize and mitigate risk and organization impact.

Web Applications and the OWASP Top 10:

Web applications are used today in practically every business and organization to provide products, services and information to their customers. Making sure the technology, code and infrastructure related to the web applications is critical to the mission of an organization. This course takes a look at the process and some tools used to secure web applications.

As shown in the OWASP Top 10 Web application security risks document reading this week, the number of attacks and success of those attacks on Web applications is concerning. Every few years, the OWASP group prepares a list of the top 10 security threats for Web applications. The interesting result is many of the same threats are present even after years of attempting to mitigate them. Clearly, we have much work to do here.

Be aware, there are much more than 10 security threats. The OWASP document just provides the most significant and potentially most impactful or damaging. As a developer, tester, designer or security engineer, it is critical to be constantly aware of the threats, the changes in the threats, and the trends.

We will continue to prepare for and mitigate SQL injection as Injections remain the top security threat. However; new threats such as XML External Entities (XXE), Insecure Deserialization, and Insufficient logging and monitoring have made the top ten for this iteration.

OWASP adds additional criteria for evaluating risk including exploitability, weakness prevalence, weakness detectability, and technical impacts. Each of these include points for computing the overall risk in three different categories. For example, 1 point is assigned if the exploitability of the threat is difficult, 2 points if the exploitability is average, and 3 points if the exploitability is easy. The higher the number in the category the higher the risk and the closer to the top the threat will appear.

Weakness detectability includes the same categories and points for difficulty, average and easy. If the threat can easily detect a weakness, the impact could be larger. Weakness prevalence attempts to categorize how common the weakness is. If the weakness is uncommon, 1 point is assigned. Two points are assigned for common weaknesses, and 3 points are assigned to widespread prevalence. For the technical impacts, minor, moderate and severe are assigned 1, 2 and 3 points respectively.

Each of the top 10 web security threats are defined in the OWASP document along with example attack scenarios, mitigation steps and how to determine if your application is vulnerability. During this semester we will cover several of these attack scenarios and use tools to attempt to detect the vulnerabilities and provide steps to mitigate the issues.