Week 2 Playbook Entry: Cryptographic Concepts

* The Principles of Cryptography

Cryptography in Greek translates to hidden writing. The goal of Cryptography is to hide the meaning, rather than hiding the message itself. We can apply the idea of encrypting a message to information security. Messages can be decrypted with a key, allowing for those who need the data to access it while making it impossible for those who don’t have the key to access it.

* Cryptographic algorithms

The oldest methods of encryption used physical cypher disks, you would receive an encrypted message, you would look at the letter written on the page, and then write down the letter corresponding on the wheel. A far more advanced version of this concept was used by the Nazis during World War II, the Enigma machine not only automated the process, but was far more sophisticated. Symmetrical algorithms have the same key on both ends, meaning that both sides have the exact same key. This has the issue of requiring both sides to share the exact same key. Unlike asymmetric cryptography, which the sender uses a public key, and the receiver uses their own private key to decrypt the message.

* Hashing Algorithms

Hash algorithms are designed to output a unique mathematical output unless you input the exact same set of data. You can not decrypt from a hash, instead the point of the data is to provide a unique identifier on data as a way of making sure that no changes were made to it. While not the same as creating a checksum, the processes are very similar.

Key Takeaways

* Encryption is one of the most important tools in information security.
* Hardware encryption becomes more important the more sensitive the data is.
* Some forms of encryption can be cracked, so it’s important to keep in mind what encryption algorithms are in use.

Real World applications

Protecting information using cryptography happens every day, encrypting sensitive data is very important, such as payment information and private communication.

Future Goals