Cryptography and Network Security

Suprajit Sardar

11th September 2020

1 Introduction

There is a proverb that " Prevention is better than cure".So, to prevent successful attacks on a system we need a good security system as well as a well build design. Here are some principles discussed below to build such systems.

2 Some Secure System Design Principles

- Make Defaults Safe : Normally users never change defaults that's mean a initial setting of a system must be secured enough. example - Use https instead of http.
- Make the Design Open : More eyeballs , often better security. It means that when a system is open to all , there are more possibilities to know the faults. However , this is not always true. example - Microsoft's Bug Bounty Program.
- Principle of least privilege : Putting some kinds of bound that who can use the most critical resources of the system. example - Provide limited resources, Occurrence of time out after a certain period of time.
- Least Surprise : User should not be surprised or confused by the interface of the system. So if we have to implement some useful things which may surprise the user , try to make them default. example - Provide what interface a user want.
- Never Trust the Input : Always verify the security properties like Integrity , Authentication etc.
- Isolation : Always maintain a copy of useful data like use hard-disk drive or disk partition. So that anything happen to the main file , we can retrieve data later on.Not only that but also to ensure security we need isolation of a large system like an aircraft, submarine. In this large systems if you use isolation or separation techniques it will be lot more easier to use and access.

- KISS(Keep-It-Simple-Stupid) : keep designs as simple and small as possible . That will make the user happy and easy to detect the faults in the system . However, this is not always true.

3 Conclusion

No system is totally safe.Here are some principles discussed above which may prevent some successful attack to a system. Along with we have to regularly check a systems security and find out the weakest spots and improve them. So, I can say from the whole discussion that security is a continuous process.