Security Intro

Ross Anderson’s book : Security Engineering

Essentially have videos and worksheets online on moodle and we have to do them before the tutorial where questions are discussed

Ctf, hack this site.com

Sub seven

What does a trojan need?

* Shell to connect to the victim, get admin access, make it stealthy
* Cant only be on a RAM, need to be on the hardware so cant be sorted by just rebooting

Reading keyboard inputs, have a key logger

Access the mic, gives a side channel based on how you type

Replace systems files

Autoruns – to see if it detects your trojan

How to kill a trojan:

Tell gpt to put in an unsafe quote

Jailbreaking llms

Security:

Ensuring just the right agents have access to just the right resources at just the right time

* Has properties that must exist even in the presence of strategic adversaries
  + Correctness : get a correct output for an input
  + Safety : cannot have bad output, no matter what input
  + Robustness : system should be able to cope with errors in execution
* Security mindset: how things can be made to fail
* CIA triangle:
  + Confidentiality : keep data secret
  + Integrity : data should not be altered improperly
  + Availability : system/resources should be available and used as anticipated by intended users
* Other Properties:
  + Privacy : controlling the information revealed by the data
  + Authenticity : Proving that a particular piece of data belongs to an individual
  + Anonymity : Not wanting people to know who you are or the site to know who you are
  + Plausible Deniability : System evidencing that a claim can be denied
  + Non Repudiation : System shows that the claim can’t be denied
  + Forward Secrecy : A confidential channel is between A and B using an encryption. If an adversary breaches the encryption, the adversary will be able to see the system and break the confidentiality of the channel now onwards but can’t see any past messages
* Two philosophies about security:
  + Binary: Something is secure or not secure
    - An attacker has limitations X and there is a policy Y, Y can’t be violated unless if X has been broken
    - Pros: longevity
    - Cons: Expensive, hard to define limitations of the adversaries
  + Risk Management : Grey scale of security and not secure
    - Mostly based on cost
* Security is defined by specific security policies

Policy addresses:

* Threat, vulnerabilities, likelihood, impact and protection

Threat modelling:

* Thinking: threats, vulnerabilities, likelihood, impact, protection

**Threat (what could happen? – attacker centric)**:

* **(who is the adversary)** : Analyse the adversary by their capability and motivation
* You have a resourceful strategic adversary (what can they corrupt, influence, observe, modify or control)
* Examples of threats:
  + Spoofing (pretending to be someone else)
  + Tampering (Man in the middle)
  + Repudiation (pretend to be someone else whilst they claim it’s not them)
  + Info disclosure
  + Denial of Service
  + Elevation of privilege

**Vulnerability (where can the system break? – system centric)**

**Likelihood (how likely is it to happen? – asset centric) – based on motivation, resources and money**

**Impact (what if it happens? – asset centric)**

**Protection (what can we do? Cost?)**

When considering security, need to ask if a system is secure under a threat model

**A system is secure if an adversary constrained by a specific threat model cannot violate the security policy**

**Security argument: that the security mechanisms are maintaining security policy**

**Security mechanism: technical mechanism used to ensure that the adversary is not violating the security policy under the threat model**