Define Confidentiality

the property of non-public information remaining accessible only to authorized parties, whether stored or in transit

Define Data Integrity

the property of data, software, or hardware remaining unaltered except by authorized parties

Define Authentication

assurance that a principal, data, or software is genuine relative to expectations

Define Authorization

the property of computing resources being accessible only to authorized entities

Define Availability

the property of information, services, and computing resources remaining accessible for authorized use

Define Accountability

the ability to identify principals responsible for past actions

The 6 high level security goals:

1. Confidentiality
2. Integrity
3. Authorization
4. Availability
5. Authentication
6. Accountability

Define Trustworthy

is an actor that doesn't have our trust but is deserving of it

Define Trusted

is an actor that has our trust whether it deserves it or not

Define Principals

The agents representing users, communicating entities or system processes
Have associated privileges specifying the resources they are allowed to access

Define Privacy

information protection to prevent unauthorized disclosure

Define Anonymity

a persons actions are not linkable to the their public identity

Define Assets

(includes) information software, hardware, and computing and communication services

Define Policy

The design intent of a system's rules and practices, includes what is and what is not allowed. It may specify assets that need to be protected, specific users allowed to access and allowed means of access

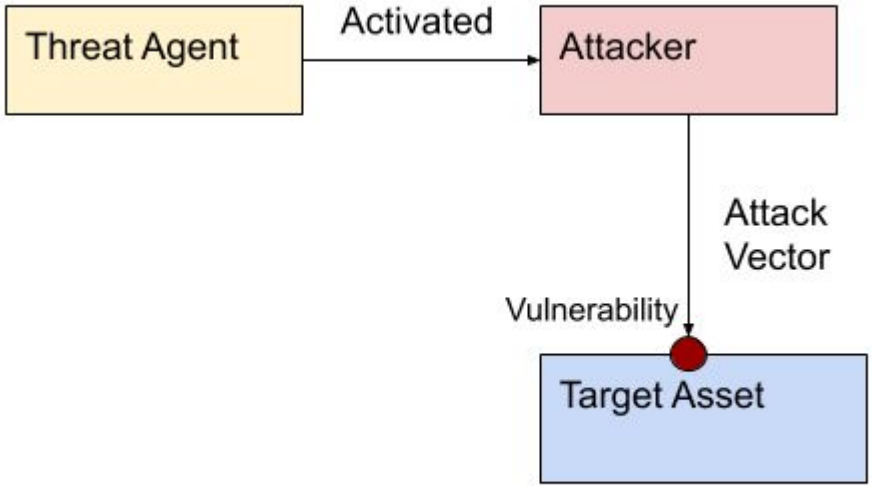
Define Repudiation

The ability to credibly deny previous commitments or actions

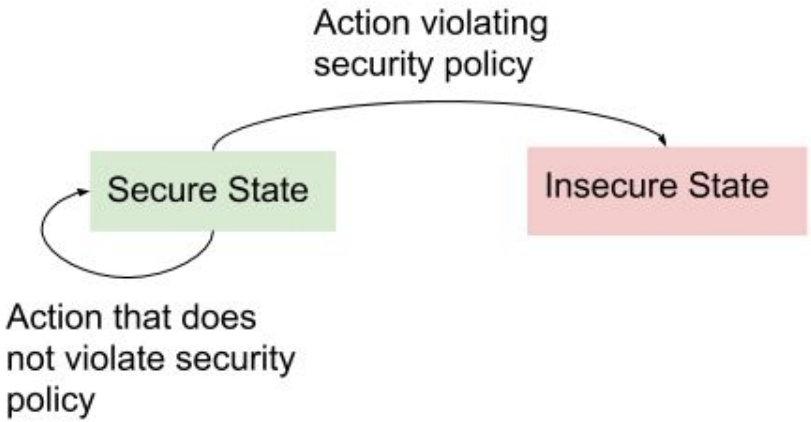
Repudiation vs Accountability

If repudiation is possible then accountability has not been achieved. If transaction evidence or logs are implemented properly then there are records and repudiation is not possible

Attack Diagram (Threat Agent, Attacker, Target)


Threat Agent
Activated
Attacker
Attack
Vector
Vulnerability
Target Asset

Security Policies and States


Action violating
security policy
Secure State
Insecure State
Action that does
not violate security
policy

Qualitative Risk Assessment

- Compares risks relative to each other and ranks them
- Advantages: having a rank of each asset can help prioritize which areas need improvement
- Disadvantages: It is an estimation and could be wrong

Quantitative Risk Assessment

- Estimate rarely possible in practice
- Numerical estimation of risk
- Advantages: A numerical value for risk could be valuable for shareholders, and for calculating the minimum risk
- Disadvantages: Can not be achieved/calculated accurately in practice

The Risk Equation

R = T x V x C

The risk equation - the expected loss due to harmful future events relative to an implied set of assets and over a fixed period of time

- T - threat information (the probability that particular threats are initiated by actors in a given period
- V - the existence of vulnerabilities
- C - asset value, and the cost or impact of an attack

The Simplified Risk Equation

P = (T x V)

- P - the probability that a threat agent takes an action and successfully exploits a vulnerability

What are some examples of adversary capabilities?

Computing resources (CPU, storage, bandwidth), skills, knowledge, personnel, opportunity

Define Adversary Methods

The anticipated attack techniques, or types of attack

Define Adversary Objective

Potential attack target or goal

Suggest target assets requiring special protection

Define Risk Management

Estimating and identifying threats and managing the risk

Example Risk Management Strategies

(a) Mitigating risk by technical or procedural countermeasures

(b) Transferring the risk to third parties

(c) Accepting the risk in hope that doing so is less costly

(d) Eliminating risk by decommissioning the system

Risk Assessment Challenges

- Incomplete knowledge of vulnerabilities
- Difficulty of quantifying the value of intangible assets (strategic information, corporate reputation)
- Incomplete knowledge of threat agent and their adversary classes

Annual Loss Expectancy

For a given asset:

$ALE = \Sigma Fi.Ci$

- Sum over all security events modeled by index i
- Fi = estimated frequency of events of type i
- Ci = the average loss expected per occurrence of event of type i

Define Risk Assessment

- Involves analyzing different factors (probability of attack expected loss) in order to estimate risk

Define Risk

The expected loss due to harmful future events, relative to an implied set of assets over a fixed period of time

Define Controls and Countermeasures

- Measures put in place to prevent security policy violations
- Ie. software monitors

Define Attack Vector

Specific methods, or a sequence of steps, by which attacks are carried out

Define Threat

- Any combination of circumstances and entities that might harm security assets ie. cause security violations

Define Credible Threat

- Capable means and intentions

Threat Agent vs Adversary vs Attacker

- Source or threat agent behind a potential attack = adversary
- Once threat is activated into an actual attack = attacker

Define Attack

The deliberate execution of one or more steps intended to cause a security violation

Define Security Violation

When a system moves into an unauthorized state

Security Policies in Practice

Informal documents including guidelines and expectations related to known security issues

Define Vulnerability Assessment

Identifying weaknesses in deployed systems

What is security in theory?

A formal security policy precisely defines each possible system state as either authorized (secure) or unauthorized (non-secure). System should start in a secure state. System actions can cause transitions. If a security policy is violated a system moves into an unauthorized state.

What are schemas in threat modelling?

Used for modelling adversaries

- Categorical Schema - classifies adversaries into named groups (ie. foreign intelligence, cyber-terrorists, organized crime, ..)
- Capability Schema - groups generic adversaries based on a combination of capability and intent, ie. weakest to strongest

Targeted vs Opportunistic Attack

Targeted: specific individuals or organizations
Opportunistic or general: arbitrary victims

User Workflow in Threat Modelling

- Trace through users actions from the time a task begins to the time it ends

Adversary: Insider vs Outsider

Outsider: an attack launched without prior access to the target network
Insider: parties having a starting advantage (ie. legitimate credentials)

Threat Modelling: Data Flow Diagrams

Trace the flow of data through the system for a simple task, transaction or service

Trust Domains

- System gateways where system controls restrict and filter communications - (safe domains)

Define Threat Model

Identifies threats, threat agents, and attack vectors that the target system considers in scope to defend against

Define Security Model

- Relates system components to parts of a security policy to be enforced, the model may then be explored to increase confidence that the system requirements are met

Define Attack Tree

- Tree starting with root node at top - overall attack goal
- Lower nodes break out into alternative ways to reach the root node (attack vectors)

Black vs White Box Testing

- White box: proceeds with the use of insights from design documents or source code
- Black box: proceeds without the use of insights from design documents or source code

Threat Modelling: Lifecycles

- Of data, software, accounts
- Locations of data
- Where it flows

Threat Modelling: Attack/Threat Checklists

Checklist of attacks

- Make sure none of them are feasible/possible
- Go through each item one by one and check them off

Threat Modelling: STRIDE

Memory Aid for recalling 6 categories of threats:

S - spoofing - attempt to impersonate an entity

T - tampering - unauthorized altering

R - repudiation - denying responsibility for past actions

I - Information Disclosure - unauthorized release of data

D - Denial Of Service - impacting availability of service or quality of service, through actions that consume resources

E - Escalation - obtaining of privileges to access resources typically referring to malware that gains a base level of access as a foothold and exploits vulnerabilities to extend this to gain greater access

Observability in Security

- Testing would ideally confirm the absence of vulnerabilities - Negative Goal
- we not only want ro confirm that the functionality works as planned but that the exploits are also absent
- not observing had outcomes does not mean that they do not exist

Penetration Testing

- self-assessments
- involve customers or hired consultants
- finding vulnerabilities in deployed systems by demonstrating exploits

Formal Security Evaluation

- Third-party lab review
- Considerable cost and time
- done on the final form of the product or system
- recertification required when the smallest changes are made