Vulnerability Assessment and Risk Management

Chapter 2 of the textbook and supplementary material

Stages of a Vulnerability Assessment

Planning

Assessing

Reporting

Risk Management

- Avoidance
- Reduction
- Spreading
- Transfer
- Elimination
- Acceptance

Risk Assessment Questions

- ✗ What can go wrong
- What is the likelihood of that occurring
- ? What are the consequences

Risk Management Questions

- ✓ What can be done
- ? What options are available to do it
- What are the costs and benefits

Consider

- Cyber
- Executive
- Transportation

Conduct

- Threat Analysis
- Consequence Analysis
- Event and Fault Tree Analysis
- Vulnerability Analysis
- In Summary: Security requires knowing What is the likelihood of an event and What are the consequences.

Risk Formula

Use both Quantitative and Qualitative measures to calculate: **R= Pa X (1-Pe) X C**

Where:

R is Risk measured between 0.0 and 1.0

Pa is the probability of an attack

Pe represents the vulnerability of the protection system and is calculated as:

Pe=Pi X Pn where **Pi** is the probability of interruption and **Pn** is the probability of neutralization.

C is the consequence value of the event; 0 – 1 and represents the severity of the event

Note: If you can't detect and interrupt and attack **(Pi=0)** and you can't stop it even if you interrupt it **(Pn=0)** then **Pe =(0 X 0)=0**.

Therefore 1-Pe = 1 and R = Pa X 1 X C or Risk is equal to the probability of an attack times the consequence.

If, on the other hand Pi is 50% and Pn is 50% then Pe = 25% =.25 and **Risk = Pa X 0.75 X C**

Likelihood in security is often based on subjective measures (intuition, expertise). Be careful because subjective measures may cause a reduction in credibility.

Example 1

- It has been determined that for event 1, Pa=.9, Pi=.5, Pn=.6, C=.9
- And for event 2, Pa=1, Pi=1, Pn=1, C=.5

On which event should you focus the greater amount of your resources and why?

Example 1

- It has been determined that for event 1, Pa=.9, Pi=.5, Pn=.6, C=.9
- And for event 2, Pa=1, Pi=1, Pn=1, C=.5
- On which event should you focus the greater amount of your resources?
- Event 1: R = .9 X (1 - (.5 X .6)) X .9 = .9 X (1 –(.3)) X .9 = .9 X .7 X .9 = 0.567
- Event 2: R = 1 X (1 – (1X1)) X .5 = 0

Event 2 is guaranteed to happen but we can both interrupt it and neutralize it every time so there is no risk.

Example 2

- It has been determined that for event 1, Pa=1, Pi=.0, Pn=.0, C=.1
- And for event 2, Pa=.5, Pi=0, Pn=0, C=.8

On which event should you focus the greater amount of your resources and why?

Example 1

- It has been determined that for event 1, Pa=1, Pi=0, Pn=0, C=.1
- And for event 2, Pa=.5, Pi=0, Pn=0, C=.8
- On which event should you focus the greater amount of your resources?
- Event 1: R = 1 X (1 - (0X0)) X .1 = 1 X (1 –(0)) X .1 = 1 X 1 X .1 = 0.1
- Event 2: R = .5 X (1 – (0X0)) X .8 = .4

Even though event 1 is more likely to occur, the consequence is low.

Event 2 is less likely but the consequence is higher therefore the Risk is greater.

The Incident has Three Phases

- Pre-attack: How certain are we that an attack is likely
- Attack: The bad guy is here
- Post Attack: Suffering the consequences

Qualitative measures could be used :

Pa = Not Likely, Likely, Very Likely

C = Minimal, Severe, Critical

Explain why this is the worst possible circumstance in english

- Pa = 1
- Pe = 0
- C = 1

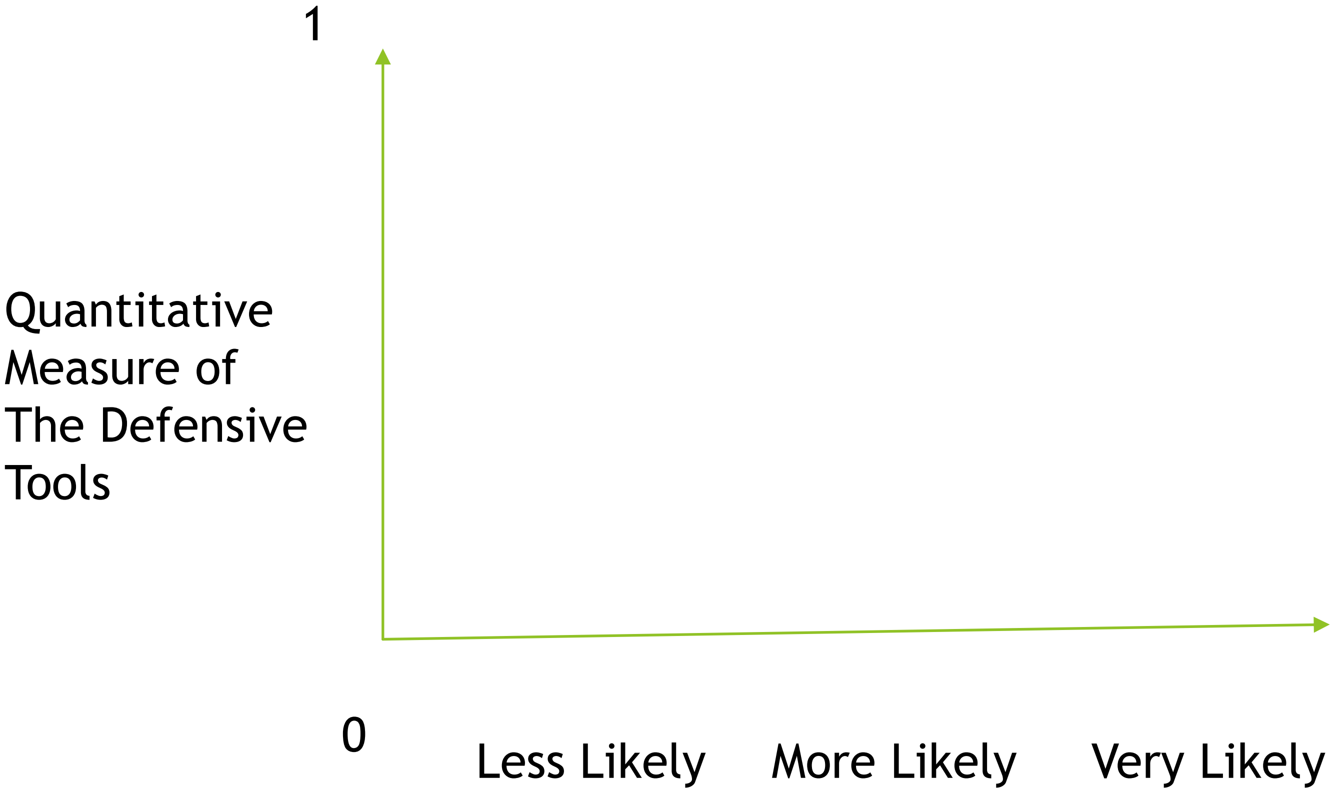
Explain why this is the worst possible circumstance in english

- $Pa = 1$
- $Pe = 0$
- $C = 1$

An attack is guaranteed. We can’t interrupt it and/or we can’t neutralize it and the Consequences are at their highest level.

Note that attacks which result in greater consequence may attract more capable and motivated attackers.

You can combine qualitative and quantitative measures



1

Quantitative Measure of The Defensive Tools

0

Less Likely

More Likely

Very Likely

Annualized Rate of Occurrence (ARO)

The likelihood of an event in any given year.

i.e. We have a break in every 2 years. There the ARO is ½ or 0.5.

Asset Value (AV)

The value of the Asset to be protected. Never limited to just the cost of the item.

Exposure Factor (EV)

The percentage of the Asset value you lose with each occurrence. 0 -1

An Exposure factor of 0.5 means that with each event we lose half the value of the asset.

Single Loss Expectancy (SLE)

The loss ($) incurred for each event.

SLE = AV x EF

An Asset has a Value of $10,000 and an Exposure Factor of 20% or 0.2.

SLE = 10,000 X 0.2 = 2,000

With every occurrence of the event we lose $2,000.

Annualized Loss Expectancy (ALE)

The loss ($) we should budget for each year.

ALE = SLE x ARO

Our SLE is $2,000

Our ARO is 0.5

We should budget to cover a loss of $1,000 each year.

Does this mean that we can ACTUALY expect to lose $1,000/year to this event?   No.

Example 1

Our on-line e-commerce site produces on average $1,000,000/year. We have a robust fault tolerant system but a single DDOS attack will negatively impact this by 10%.

On average we experience a DDOS attack every two years.

What is the maximum that we can request be added to our security budget each year to deal with DDOS attacks?

Example 1

Our on-line e-commerce sight produces on average $1,000,000/year. We have a robust fault tolerant system but a single DDOS attack will impact this by 10%.

On average we experience a DDOS attack every two years.

What is the maximum we should request be added to our security budget each year to deal with DDOS attacks?

AV = 1,000,000

EF = 0.1

SLE = 100,000

ARO = ½ =0.5

ALE = 100,000 * .5 = $50,000.

We can request up to $50,000 per year to deal with DDOS attacks.

Example 2

Kids keep breaking windows in our building.

Each window costs $500 to replace.

No part of the broken window can be saved.

On average, they break three windows a year.

On average, once every year the broken window leads to $1,000 in water damage.

What is the maximum we can request be added to our annual budget to deal with broken windows and the water damage?

Example 2

Kids keep breaking windows in our building.

Each window costs $500 to replace.

No part of the broken window can be saved.

On average, a window is broken three times a year.

On average, once every year window breakage leads to $1,000 in water damage.

What is the maximum we can request be added to our annual budget to deal with broken windows and the water damage?

Window ALE is $1,500

Water Damage ALE is $1,000

We should request an annual budget allocation of $2,500.

Do we have any other alternatives?

Example 2 – Alternatives.

- 1. Status quo (acceptance of Risk).
- 2. We could buy Window and water damage insurance for $1,000 per year. (transference).
- 3. We could brick in the windows for a one-time cost of $10,000. (avoidance).
- 4. We could put metal screens over the windows for a one-time cost of $3,000 (Reduce/Mitigate).
- 5. Arrest the kids and make an example of them. (elimination)

Statistics and Quantitative Analysis

- Quantitative analysis is used when there is a high consequence loss of assets.
- Qualitative analysis is used when there is no quantitative data available or the consequence loss is small.

Describe the outcomes to determine success

When a security event occurs an the security component receives an input (stimulus), the component must perform its intended task.

Example: A sensor detects and intrusion and triggers an alarm.

In each of these events there are four possible outcomes

1. True Positive – The event is detected. Used to determine the **Detection Rate.**
2. **False Positive** (false reject) – The security component indicates that the event has occurred when it has not.
3. False Negative (false accept)- The event occurs but is not detected by the security component.
4. True Negative – The event does not occur and there is no response from the security component.

Discrimination and Noise

A security component may be unable to distinguish between a True Positive and False Positive because it has insufficient Discrimination ability. (*i.e. can’t tell the difference between a racoon or a person*)

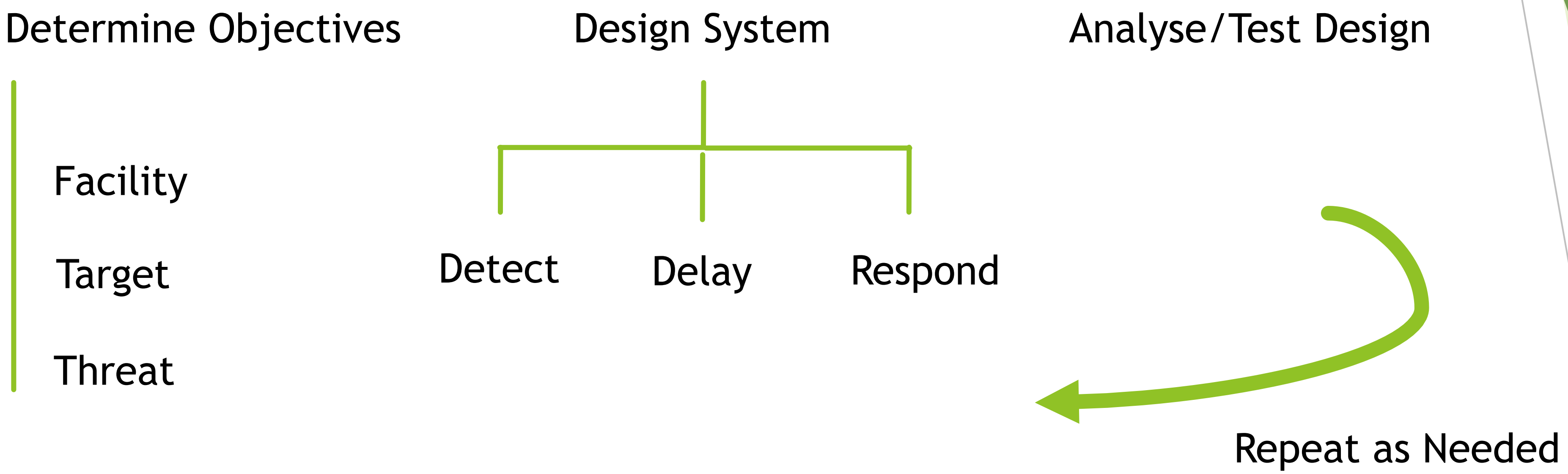
Such a lack of Discrimination ability can lead to Nuisance Alarms. The number of times this happens in a given series of security events is referred to as the **Nuisance Alarm Rate** (NAR).

False Alarms occur when there is no underlying event but the security component raises and alarm. (i.e. a fire alarm that is set off by dust or steam).

False alarms may be caused by “noise” in the environment. Such noise might take the form of EM Interference or Ambient Sound for example.

Both Nuisance Alarms and False alarms are False Positives.

Design and Testing of Security Sytem



Determine Objectives

- Facility
- Target
- Threat

Design System

- Detect
- Delay
- Respond

Analyse/Test Design

Repeat as Needed

Each security component is first described by its validated performance (i.e. detection rate) and then its performance is degraded based on how it is installed, maintained, tested and integrated into the overall system.

Planning the Vulnerability Assessment

A good plan ensures that you work is focused on the tasks required and the customer understands and agrees on the assessment they will receive.

Have a known start and finish date.

Begin with customer meetings. Understand their concerns. Determine their constraints (i.e. budget, rules, availability)

Define scope, roles and responsibilities.

Make sure the customer understands what they will receive in terms of the product.

The result is a requirements document, statement of work, contract.

This should contain all the acceptance criteria (usually measured with respect to some pre-defined tests.)

Participation by Cross-disciplinary team is Critical to Success.

You will need un-interrupted access to members of the customer team and one inside team member with authority, access and knowledge of the subject matter. This is usually a senior technical person; typically, a CTO. This person must be available to you on-demand throughout the assessment; or with minimal delay.

You also need a senior management single point of contact. For negotiations, meetings, budget and contract approvals, communications and contingencies. There will be a need for real-time decision making so this person must be accessible within an acceptable time frame (usually some time within a day and never on leave).

Project Kickoff Meeting

Every person associated with the project must be in attendance.

The project lead (possibly you) will present the plan to the group. There is usually no need to discuss budget at this meeting unless agreed by the customer in advance of the meeting.

Items to focus on / review in the presentation:

- Objectives
- Deliverables
- Acceptance criteria
- Communications
- Time Frame – start stop report
- Roles/Responsibilities (have each person describe their role)
- Tasks Involved.
- Rules

Allow plenty of time for discussion and be prepared to receive amendments.

If possible, lower level staff and other personnel should be invited into meeting and be given and introduction and overview summary of the project by the most senior customer representative present.

Customer Archive and Security

Every VA is a confidential engagement. Nothing should ever be discussed outside the VA team, even to members in your own organization. You will have many interactions with staff. Make sure all questions are directed the appropriate customer staff member. Never answer the questions yourself (but be nice).

No information should ever be transported or store outside a secure environment. This includes, but not limited to contracts and supporting documents, customer data, communications and test results and partial results.

All such digital information must be encrypted and placed in secure storage during the project; and either destroyed or returned to the customer at the end of the project.

Information in other forms (i.e. paper blueprints) must be kept inside a secure facility/container; and either destroyed or returned to the customer at the end of the project.