Adversary Modeling to Develop Forensic Observables

By John Lowry, Rico Valdez, Brad Wood

Presented by: Ignacio Marin-Garcia
imaringa@coe.neu.edu
http://www.coe.neu.edu/~imaringa/

Introduction

- The current models are based in an asymmetrical system in which:
  - Observables of malicious behavior in the cyberspace are derived from intuition and/or analysis of previous events
  - Observables based in previous events only are use to identify and protect against intrusions while forgetting about innovation.
- This asymmetrical system need to be amended by:
  - Creating an a-priory analysis model by:
  - Getting observables that can be used in that way.

Threat Modeling

- Def: a model that explains how the threats happen.
- The threat model must contain an analysis of adversary behavior and incorporate knowledge to defend the system

Threat Model (cont.)

- In order to create a functioning threat model we need to:
  - Hypothesize potential adversaries or malicious acts
  - Identify threats and adversaries missions
  - Identify the means that would have to be used or high provability of being used
  - Develop observables for those means

Threat Model (cont.)

- Hypothesize potential adversaries or malicious acts
  - In order to create a good defense and system we first need to know which adversaries we may face in a realistic way
  - We should be able to know the possible threats that the system may suffer so we can address them.

Threat Model (cont.)

- Identify threats and adversary missions
  - When we have hypothesize (wild guest ?) the threats and missions we may realistically try to identify the ones we actually confront.
  - Different systems will be confronted by different kinds of adversaries with different kind of missions according to their expertise and resources.

Threat Model (cont.)

- Identify the means that would have to be used or have a high probability of been used
  - In other words, how are we going to be confronted
- Develop observables for those means
  - How we can see those confrontations before and while the happen.

Cyber adversaries

- The cyber adversary is the person or program (virus) that is going to confront our system
- Some considerations:
  - The cyber defense community frequently makes mistake of assuming a kind of omnipotence of the adversary, this is base in:
    - Defenders are often aware if their own inadequacies
    - Defenders are aware of the asymmetric situation
    - Security evaluations fail to represent real world situations.

Cyber Adversaries (cont.)

- We must pay attention to the adversaries constrains such as:
  - They have goals and objectives, that is the reason the defender system is under attack
  - Have limited resources. Even state sponsored adversaries may have a economic or time limitation. This constrains are out of the control of the adversary.
  - They engage in mission planning, practice , develop and testing; in other words all things are done in a kinetic world.
  - They translate their behavior into the world of computers and networks: what they do and how they do reflects their personal behavior and constrains.

Cyber Adversaries (cont.)

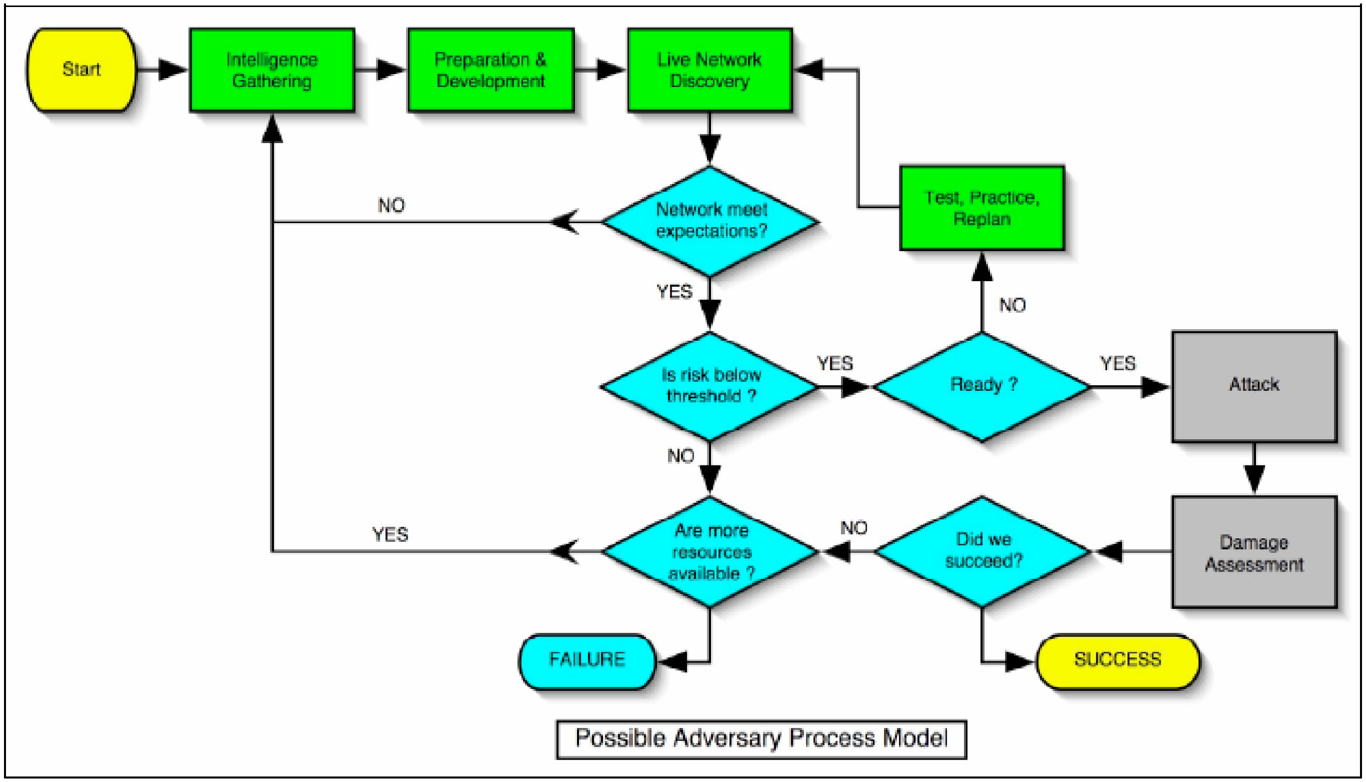


Figure 1: High-level adversary process model.

Cyber Adversaries (cont.)

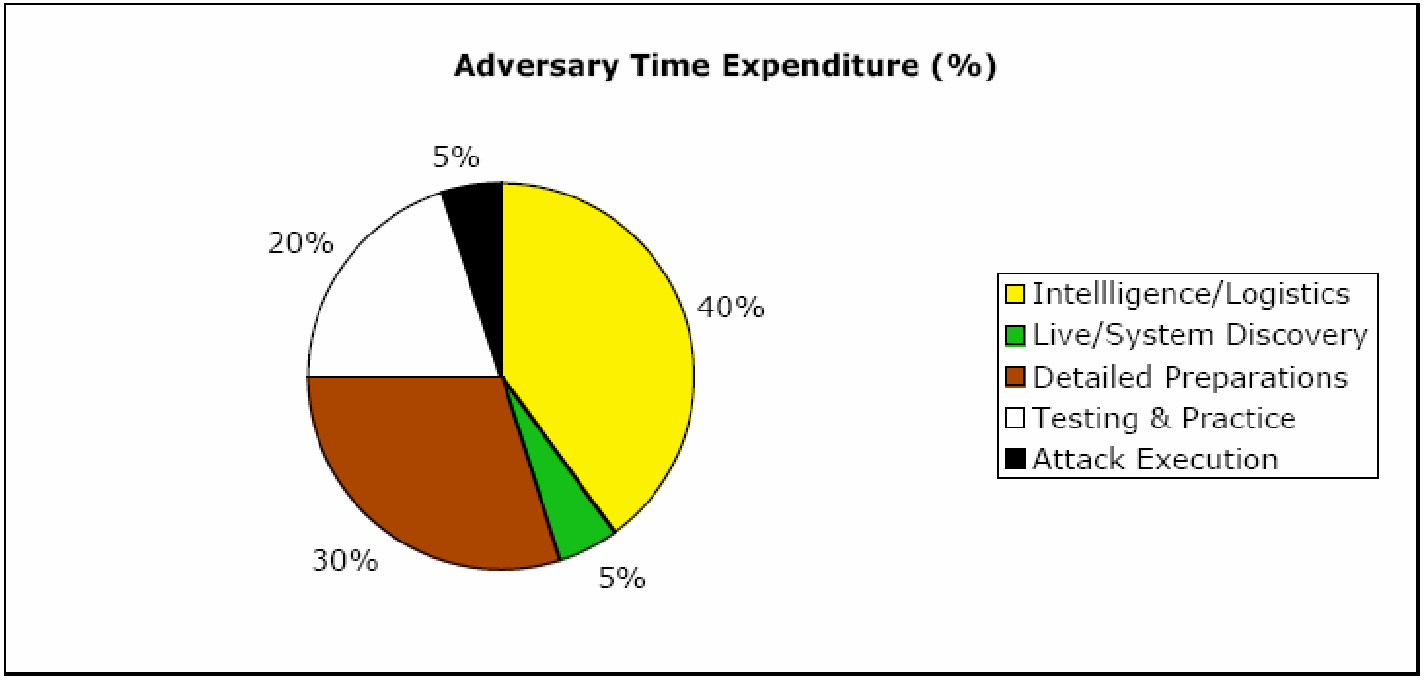


Figure 2: Adversary Time Expenditure[ii]

Cyber Adversaries (cont.)

- In order to properly model our adversaries and the threats the system may suffer we need to know all previous information, This information will be the one that will allow us to model them properly and create an appropriate schema for them. As they say “If you know your enemy you won half the battle”

Schema for Cyber Adversaries

- Choosing the correct schema for the adversary is extremely important. The schema will allow you analyzing and modeling since it will guide and focus you in your adversary.

Schema for Cyber Adversaries (cont.)

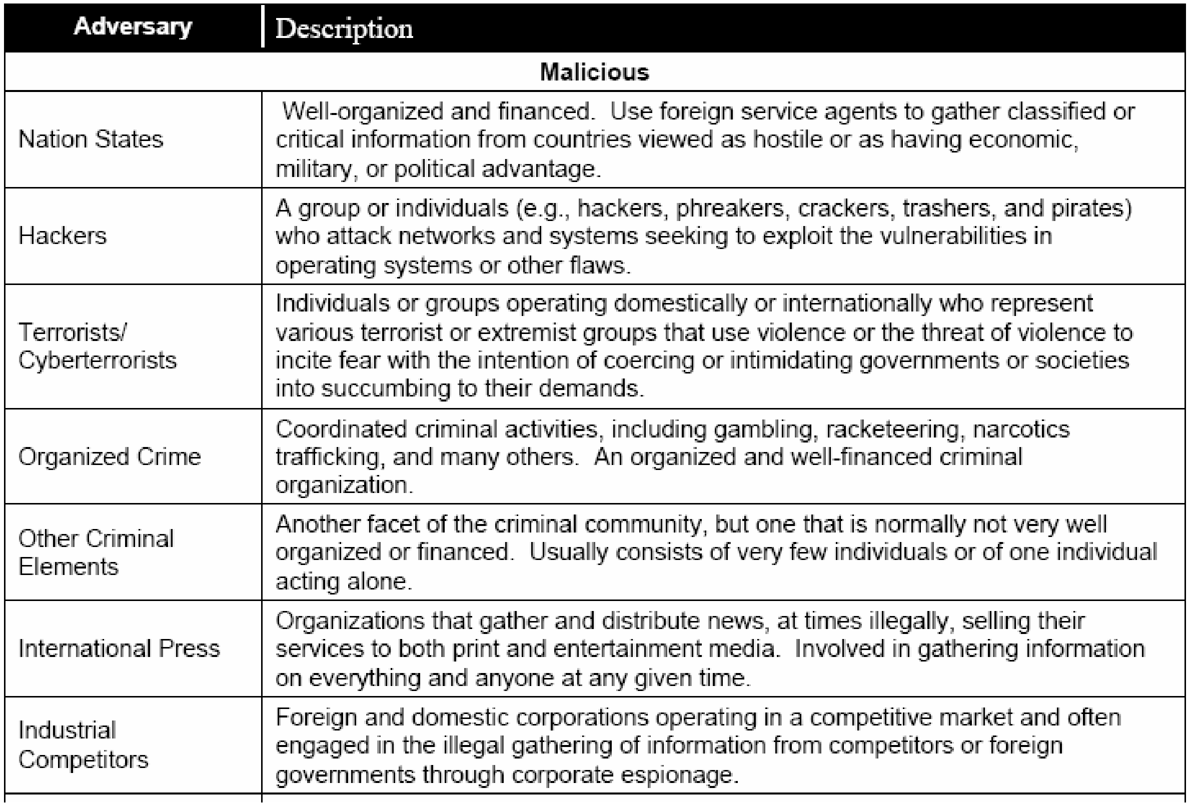
- There are different kinds of schema you can use:
  - Named actor schema
  - Class schema

Schema for Cyber Adversaries (cont.)

- Name Actor Schema:
  - It is usually use for well defined adversaries:
    - Particular country
    - Group or organization
    - Person
  - It is usually misuse in generalizations for which a class schema will be more appropriate

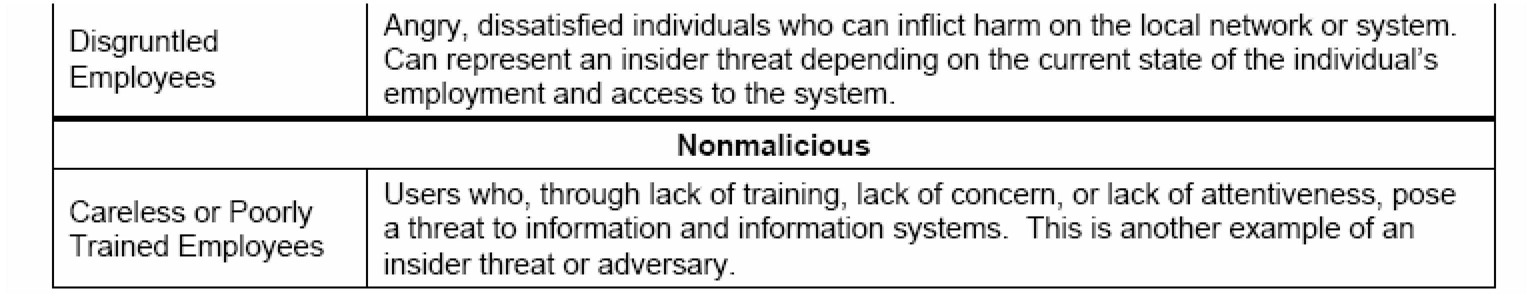
Schema for Cyber Adversaries (cont.)

- A typical named actor schema could be as:



Adversary	Description
Malicious	
Nation States	Well-organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having economic, military, or political advantage.
Hackers	A group or individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities, including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, but one that is normally not very well organized or financed. Usually consists of very few individuals or of one individual acting alone.
International Press	Organizations that gather and distribute news, at times illegally, selling their services to both print and entertainment media. Involved in gathering information on everything and anyone at any given time.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments through corporate espionage.

Schema for Cyber Adversaries (cont.)



Disgruntled Employees	Angry, dissatisfied individuals who can inflict harm on the local network or system. Can represent an insider threat depending on the current state of the individual's employment and access to the system.
Nonmalicious	
Careless or Poorly Trained Employees	Users who, through lack of training, lack of concern, or lack of attentiveness, pose a threat to information and information systems. This is another example of an insider threat or adversary.

Table 1: Example Named Actor Schema

- As you can see not only Malicious adversaries are consider in this schema. In most cases non malicious adversaries will be the more dangerous since they are more difficult to identify and protect against.

Schema for Cyber Adversaries (cont.)

- One this kind of schema has been develop, many analyses proceed to try and develop an understanding of the following main points:
  - Resources
  - Opportunity
  - Motivation
- As we have seen not all kinds of adversaries have clear motives or resources.
- It is also true that in the cases in which this schema is wrongly applied, the researcher finds out that the characterization (definition) of the attacker does not follow the rules of the schema and he should have used another schema which would have focused more in the attacker.

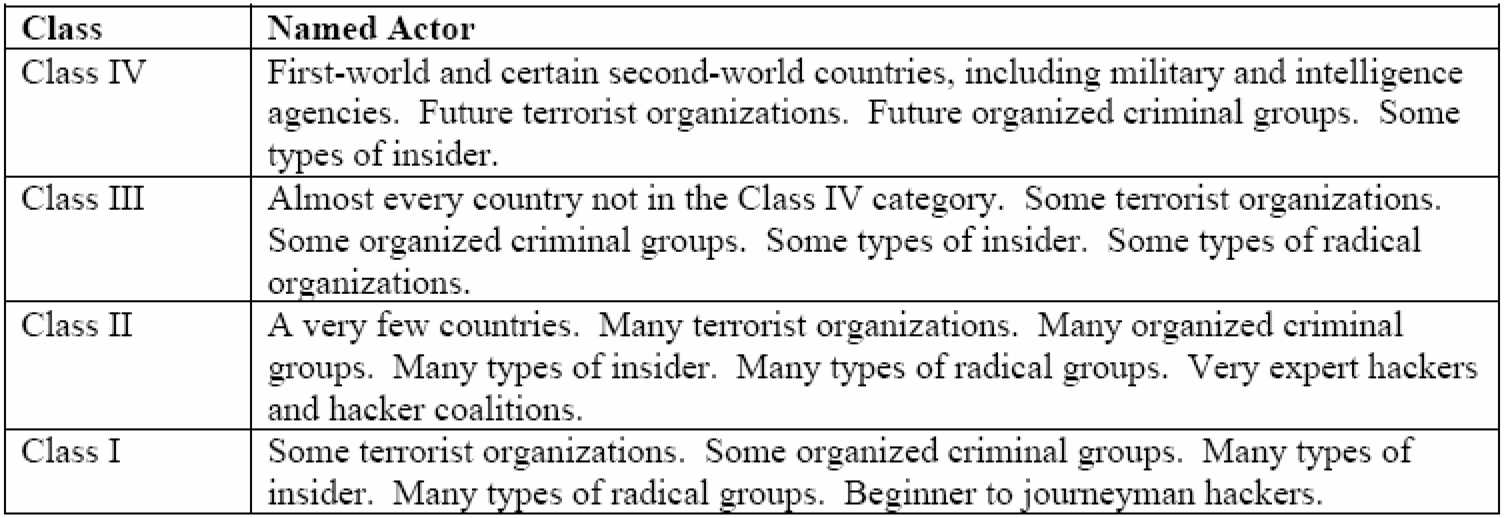
Schema for Cyber Adversaries (cont.)

- The Class schema is another schema that is usually used
- In this schema the attackers are divided in classes with a high degree of abstraction
- The high degree of abstraction allows us to have an starting point in defining the adversary even before we know the attacker.

Schema for Cyber Adversaries (cont.)

- This schema is defined in terms of:
  - Resources
  - Opportunities
  - motivations
- As we have seen, those terms are also use in the named adversary schema, but in this case those terms are the ones use to ‘define’ the class instead of been part of the adversary definition.

Schema for Cyber Adversaries (cont.)



Class	Named Actor
Class IV	First-world and certain second-world countries, including military and intelligence agencies. Future terrorist organizations. Future organized criminal groups. Some types of insider.
Class III	Almost every country not in the Class IV category. Some terrorist organizations. Some organized criminal groups. Some types of insider. Some types of radical organizations.
Class II	A very few countries. Many terrorist organizations. Many organized criminal groups. Many types of insider. Many types of radical groups. Very expert hackers and hacker coalitions.
Class I	Some terrorist organizations. Some organized criminal groups. Many types of insider. Many types of radical groups. Beginner to journeyman hackers.

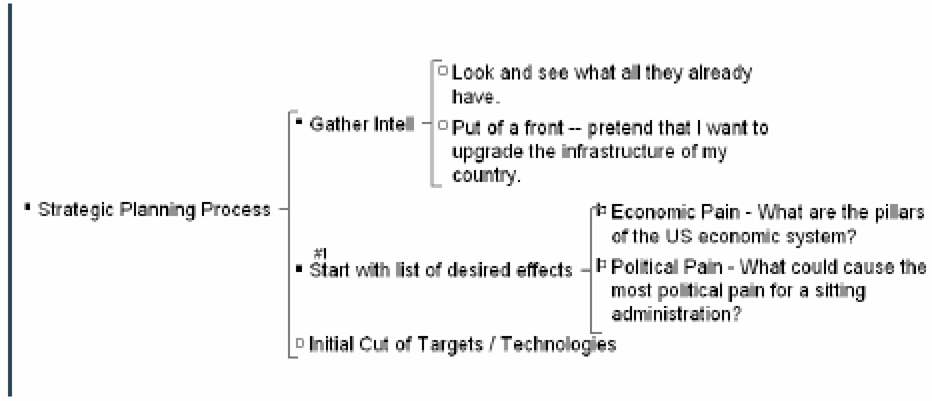
Table 2: Class to Named Actor Type Mapping

Schema for Cyber Adversaries (cont.)

- As we have seen the choose of the schema is important since it will allow us to focus in the attacker properties and “easily” model the adversary according to a set of rules.

Class IV Process Model

- After choosing a schema we can then model the process of the adversary.
- This process can be represented in a warnier/Orr diagram, four our example we use class IV adversaries:



- Strategic Planning Process
  - Gather Intell
    - Look and see what all they already have.
    - Put of a front -- pretend that I want to upgrade the infrastructure of my country.
  - #I Start with list of desired effects
    - Economic Pain - What are the pillars of the US economic system?
    - Political Pain - What could cause the most political pain for a sitting administration?
  - Initial Cut of Targets / Technologies

Figure 3: High Level Warnier/Orr Diagram

Class IV Process Model (cont.)

- The planning model tell us:
  - The adversary will study their enemy to determine what they have in place and how they operate
  - The adversary will develop a list of wanted effects, what he wishes
  - The adversary tales a high-level cut at the target of interest.
- This process is interactive, changes with learning, and refined, complex.

Class IV Process Model (cont.)

- Several areas of this process may contain observables, what we can use to determine an attack.
- Another standing idea is the gathering of information from the adversary. Complex adversaries will always gather information from the objective system. This is usually done thought basic intrusion and we can use it as an observable for our modeling.

Class IV Process Model (cont.)

- Finally this kind of adversary, class IV, has usually very specific objectives and uses complicated and multi-stage attacks. For that active monitoring become important and more observables can be gathered form it.

Class IV Process Model (cont.)

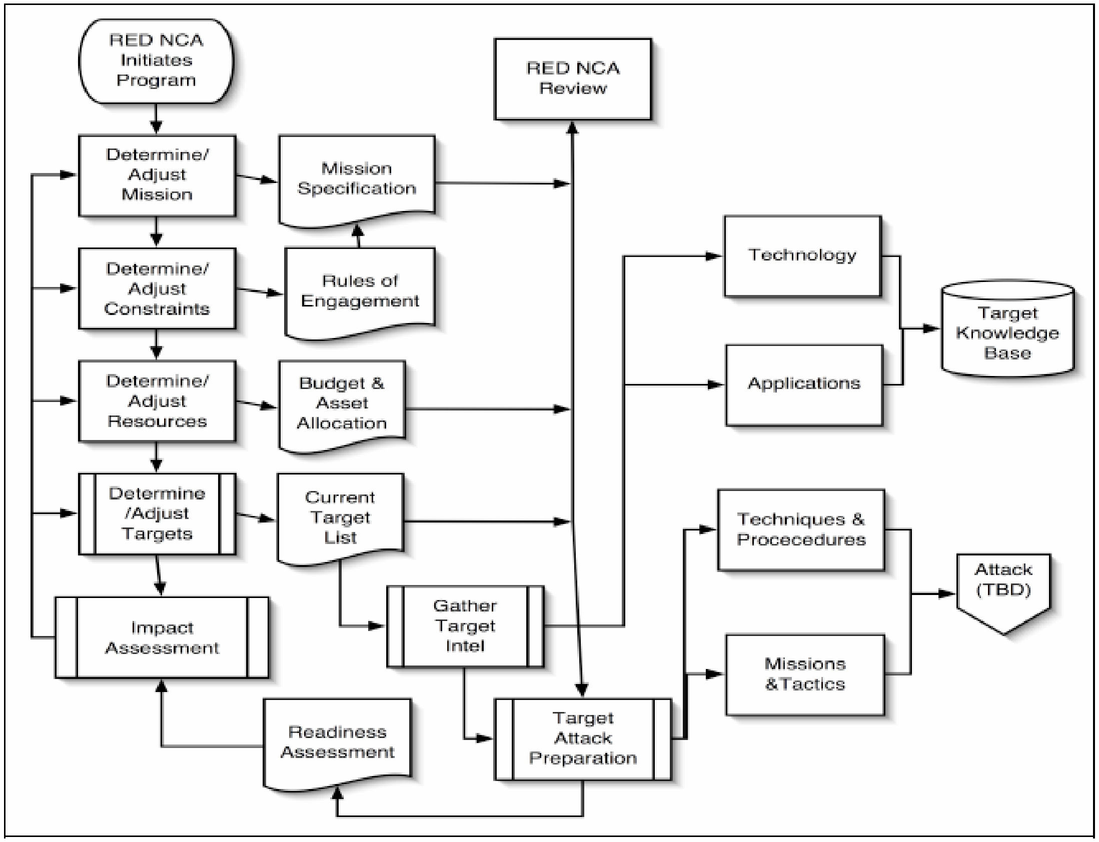

RED NCA Initiates Program
RED NCA Review
Determine/ Adjust Mission
Mission Specification
Determine/ Adjust Constraints
Rules of Engagement
Technology
Target Knowledge Base
Determine/ Adjust Resources
Budget & Asset Allocation
Applications
Determine /Adjust Targets
Current Target List
Techniques & Prococedures
Attack (TBD)
Gather Target Intel
Impact Assessment
Missions &Tactics
Readiness Assessment
Target Attack Preparation

Figure 4: Adversary Target Management Process

Class IV Adversaries and Forensics

- Most current tools and resources are not able to deal with type III and type IV adversaries due to their complexity usually because of their:
  - Complexity
  - High resources

Class IV Adversaries and Forensics (cont.)

- As we have seen in Figure 2 the time the adversary spends in gathering information and preparing for the ‘real’ attack is considerable .: considerable effort should be expended in develop observables in that particular area.
- The adversary target management process also suggest the existence of a set of observables in forensic evidence.

Types of Observables

- There are two main kinds of observable types:
  - State based observables
  - Transition based observables

Types of Observables (cont.)

- State based observables:
  - They are based in the states of the system in both:
    - The state the adversary has reached in the system
    - The state the adversary wants to reach in the system
  - These observables are the most important since they are based on necessary states the adversary has to reach, in other words the adversary needs to do them, so we can look at them to find it out.

Types of Observables (cont.)

- Transition based observables
  - These observables are base in the transition from one state to another in the system by the adversary
  - They are the “steps” the adversary does in order to move from one state to another while the state based observables are based in the initial and end points of the transition

Types of Observables (cont.)

- Both kinds of observables, state and transition based, can be easily put in a graph with nodes as states and transition as edges.
- This graph will help the defender to determine the acts of the adversary and trace his progression to the system, helping enormously in the forensic process.

Types of Observables (cont.)

- Chaining of events in the observables can also allow us to determine what the adversary wanted in the system and therefore focus our investigation in that objective.

Types of Observables (cont.)

- By analyzing and representing all the observables, state and transition based, the defender can start analyzing traces of the adversary in a more structured model

State Analysis

- From study attacks we can determine has to follow multiple steps in order to succeed.
- These steps can be consider sub-goals that the attacker need to do.

Conclusions

- By analyzing the states, transitions, type of attacker… we can generate a model of the adversary and his ‘ways’
- This model allows us to create techniques and software to optimize the detection and response (as in IDS)
- These techniques and software develop from the analysis will allow us to handle the incredible high amount of data that a system processes and which makes the forensic process so difficult.

Conclusion (cont.)

- Relation with precious topics in the course
  - While analyzing protocols is important to produce secure produces we should understand that due to complexity, implementation and coding some ‘holes’ will always be there
  - The methods used, and math representation, in previous topics can help to generalize and represent the attacks and therefore identify observables
  - Those methods dealing with processes are especially important since they help us to identify observables in the transition and state. By analyzing formally the processes we get an invaluable tool in our forensic world.

Conclusion (cont.)

- Final notes:
  - It is my understanding that there were never be a full secure system .: we will get adversaries and .: we need to be able to analyze the attacks and use the information to prevent more.
  - Remember to back-up your data or you will loose information like my presentation ☹

Questions ?

- Any questions ?
- Have a nice summer
- Paper, presentation and related notes will be available in my website:
  - http://www.coe.neu.edu/~imaringa/

Adversary Modeling to Develop Observables

By John Lowry, Rico Valdez, Brad Wood

Presented by: Ignacio Marin-Garcia
imaringa@coe.neu.edu
http://www.coe.neu.edu/~imaringa/