Attacker Classification to Aid Targeting Critical Systems for Threat Modelling and Security Review

A basic procedure in any system preparation is Risk Assessment / Management. Often software project have RA associated with the project itself. Risks tend to run along the lines of 'will the third party component be delivered on time', or 'Lack of skilled resources'. These kinds of risks are associated with delivering the product rather than risks to the product itself once it has been deployed.

There is another set of risks associated with software that need to be considered. These are the risks or threats to the software and the data it manipulates once it has been deployed. In order to help mitigate these threats, applications undergo Threat Modelling early in their development in order to help identify high risk areas of the product.

Cyber Adversaries

Threat Modelling can be a time intensive exercise therefore it helps to know what the highest risk areas are in order to focus the effort. Most often Threat Modelling will be conducted against the highest risk areas and then work through the lower risk areas in order. The question is how do you determine the areas or Attack Vectors that are the highest risk?

One of the ways is to rate your potential attackers, and once you find the ones you will most likely encounter, examine the assets that they are most likely to attack. Once you've identified these assets, thoroughly examine all the inroads and systems protecting these assets.

Different attackers have different interests and targets in mind. For example a script kiddie is most often concerned with public image and notoriety. Therefore they most often attack public facing web sites, and web content with the goal of defacing these sites and leaving their mark to gain this notoriety. This is opposed to an attacker sponsored by a Nation State whose likely targets are public infrastructure systems, mass transit, power and water systems. They are the type that does not want to be discovered and in fact often are not discovered. They are highly trained, with massive financial backing and lots of time and motivation.

Each adversary will also have different intentions with regards to the assets. A script kiddie will just want to change the corporate web page to display a message stating how cool he was that he hacked your site. This often won't involve any serious damage to corporate data or systems. By contrast, an organised crime hacker will often go after sensitive corporate data. The intent may be to perform a cryptovirology attack and hold data hostage, or sniff corporate information such as confidential business plans. The motivation for this being blackmail or extortion.

In determining what kind of attacker a system is likely to encounter, the risks to assets can be more clearly defined and can then be examined more closely. This is especially true where it pertains to determining the scope and depth of Threat Modelling and the security focus of the project.

A Proposed Rating System

At the 2003 Blackhat conference a panel presentation was given on Adversary Characterization and Scoring Systems by Marcus H. Sachs, P.E., Researcher / Instructor, The SANS Institute.Tom Parker, Head Of Research, Pentest Ltd (UK).Eric D. Shaw, Ph.D., Clinical Psychologist, Consulting & Clinical Psychology. Ltd. And Toby Miller, Researcher, www.ratingthehacker.net.

They listed 7 types of attackers likely to be encountered today.

- Unstructured Hacker
- Structured Hacker
- Organized Crime / Industrial Espionage
- Insider (user/supervisor/admin)
- Unfunded Terrorist Group / Hacktivist
- Funded Terrorist Group
- Nation State

While they could arguably be contained in other categories, for the purposes of classification and relating this to Threat Modelling I would add two more classifications to this list for a total of 9.

- Script Kiddie
- Hobbyist Hacker

I have developed a rating system in order to classify potential attackers and therefore aid in focusing Threat Modelling and security reviews in software projects. The rating system is based on simple calculations to give the various categories of attackers values that can be measured and ranked.

There are 5 variables associated with each category that are ranked from 1 to 10.

Title	Description
Skill Level (S)	The technical savvy of the attacker.
Resources (R)	The tools, information, hardware and bandwidth usable by the attacker.
Intent (I)	The harmful intentions of the attacker. Curiosity or serious damage.
Motivation (M)	How hard the attacker will try to succeed.
Likelihood (L)	How likely the system is to be attacked by this type of attacker. This is the variable that changes for each organisation.

Table 1 Explanation of criteria

There are two simple formulae that derive ratings for the attacker category, and are then added to compute a final rating.

Title	Formula
Threat Rating (TR)	(I + M) * L
Capability Rating (CR)	(S + R) * L
Overall:	TR + CR

Table 2 Formulae

This gives us a theoretical maximum Overall Rating of 400 (with all values at 10) with

a minimum of 4 (with all values at 1) and a mean of 100 (with all values at 5).

If we were to perform an attacker analysis for a technical information system that will be used by sales and technical staff for a company that made DVD players it might look like the following:

Title	S	R	I	M	L	TR	CR	Total
Nation Sate	10	10	10	10	1	20	20	40
Funded Terrorist Group	10	10	10	9	1	19	20	39
Unfunded Terrorist Group / Hacktivist	8	7	7	7	5	70	75	**145**
Malicious Insider	8	10	7	8	7	105	126	**231**
Organized Crime / Ind Espionage	**10**	**10**	**9**	**9**	**8**	**144**	**160**	**304**
Structured Hacker	8	7	5	8	2	26	30	56
Unstructured Hacker	8	7	8	8	4	64	60	**124**
Hobbyist Hacker	7	4	1	5	3	18	33	51
Script Kiddie	2	4	7	2	9	81	54	**135**

Table 3 Attacker Classifications

While the S,R,I, and M will remain fairly constant, the Likelihood value will change from company to company. In our case, a DVD player manufacturer is not very likely to encounter attackers of a Nation State or Funded Terrorist Group so the L value for them is low. However, they are quite likely to encounter attackers on an Industrial Espionage level. We could order these categories now based on their Overall Scores

1. Organized Crime 2a. Malicious Insider 2b. Script Kiddie
3a. Hacktivist 3b. Unstrucutred Hacker

For simplicity I haven't charted anything that falls below 100. They are normally low threats due to unlikeliness of encountering them. This is not to say that they won't be encountered, but we are trying to focus on the highest threat areas of the system first.

The ratings for attackers can be graphed much like Risk Ratings using a similar charting style. As you can see Below the 1 is placed in the box where the TR and CR intersect for the Organized Crime attacker classification. Anything falling in the red area should obviously be considered very high risk as these will be the highest threat probability to your system.

Threat Rating									
	200								
	175								
	150								
	125						2a	**1**	
	100			2b					
	75			3a 3b					
	50								
	25								
		25	50	75	100	125	150	175	200
	Capability Rating								

Table 4 Attacker Classification Graph

Now that we have the attacker categories of most interest to us, we can examine their most likely targets. Once we know their most likely targets we can identify the areas of the system that protect or provide access to those targets and identify these attack vectors. This will give us the focus for our threat modelling and security reviews.

Attacker Targets

The target assets that an attacker will focus on will depend largely on the organisation, its systems and what is available to be attacked. I list a few samples here based on our fictional DVD player manufacturer example above. Normally the assets would come from the Asset Identification and Valuation phase of your Risk Assessment and should include tangible and intangible assets.

Target Assets
Company Image
Web Static Cont
Schematics
Enc/Dec Algorithm
DRM Algorithms
Region Overrides
HW / SW Plans
Projected Revenue
Sales Areas
Privileged Logins
Shipping Info

Table 5 Target Asset List

For a baseline we list the attacker categories and the assets of interest to them. This list will vary from organisation to organisation based on assets identified in their Risk Assessment and the assets they possess that their likely attackers will be more interested in. We have here a simplified list for demonstration.

Attacker Class	Targets
Nation State	Nil
Funded Terrorist Group	Nil
Unfunded Terrorist Group / Hacktivist	Shipping information
Insider (user/supervisor/admin)	Schematics Projected sales area Projected revenue Proprietary software/hardware plans Region setting overrides Encoding/Decoding algorithms DRM algorithms
Organized Crime / Industrial Espionage	Schematics Projected sales area Projected revenue Proprietary software/hardware plans Privileged Logins Shipping information
Structured Hacker	Region setting overrides Encoding/Decoding algorithms DRM algorithms Privileged Logins
Unstructured Hacker	Web Site static content Region setting overrides Privileged Logins
Hobbyist Hacker	Region setting overrides
Script Kiddie	Web Site static content Region setting overrides Company Image Privileged Logins

Table 6 Attacker Target Chart

If we then create a chart with the assets across the top, and the attacker categories down the side, we can quickly see which areas will be under the most frequent threat by which column has the most marks.

	Company Image	Web Static Cont	Schematics	Enc/Dec Algorithm	DRM Algorithms	Region Overrides	HW / SW Plans	Projected Revenue	Sales Areas	Privileged Logins	Shipping Info
Nation State											
Funded Terrorists											
Unfunded Terrorists											✓
Insider			✓	✓	✓	✓	✓	✓	✓		
Organized Crime			✓				✓	✓	✓	✓	✓
Structured Hacker				✓	✓	✓				✓	
Unstructured Hacker		✓				✓				✓	
Hobbyist						✓					
Script Kiddie	✓	✓				✓				✓	

Table 7 Attacker Asset Interest Checklist

Now we can see at a glance which assets are under the most threat. If we base this on a scoring system where anything in the red is awarded 3 points, yellow 2, and green 1 point, we can obtain a weighted threat level for assets that will most likely come under threat.

Asset	Calculation
Company Image	1*2 = **2**
Web Static Content	1*1 + 1*2 = **3**
Schematics	1*2 + 1*3 = **5**
Enc/Dec Algorithms	1*2 = **2**
DRM Algorithms	1*2 = **2**
Region Overrides	1*1 + 2*2 + 1*3 = **8**
HW/SW Plans	1*2 + 1*3 = **5**
Projected Revenue	1*2 + 1*3 = **5**
Sales Areas	1*2 + 1*3 = **5**
Privileged Logins	1*1 + 1*2 + 1*3 = **6**
Shipping Info	1*1 + 1*3 = **4**

Table 8 Asset Threat Calculations

From this we can see that Region Overrides is a primary target. Lots of people want to get to it, and those attackers are likely to be encountered. This should identify assets that will need the highest levels of protection and should undergo the full scrutiny of the security team.

Weighted Target List

Keep in mind that this rating only determines a Threat Level for the asset. Each asset will be weighted on importance based on findings in the Risk Assessment phase. After all privileged logins are quite a bit more important due to the impact they can have if compromised than static web site content. These numbers can be combined

with numbers derived during the Risk Assessment phase in order to weight the threat level against each asset.

For our example we will work with an asset weighting from 1-5.
1-Trivial, 2-Low, 3-Medium, 4-Important, 5-Critical. This may vary depending on what manner of asset classification system you have in your organisation.
If we weight the assets listed above based on this scale we end up with:

Asset	Calculation
1. Region Overrides	8 * Important = 32
2. Privileged Logins	6 * Critical = 30
3. Schematics	5 * Critical = 25
4. HW/SW Plans	5 * Critical = 25
5. DRM Algorithms	5 * Important = 20
6. Projected Revenue	5 * Medium = 15
7. Shipping Info	4 * Medium = 12
8. Company Image	2 * Important = 8
9. Enc/Dec Algs	2 * Important = 8
10. Sales Areas	2 * Important = 8
11. Web Static Content	3 * Low = 6

Table 9 Assets ranked by threat level

After determining which weighted assets are under the highest threat we have a basis to start our Threat Modelling and security reviews from. The assets that come out on top of this list are the ones that should be slated for thorough Threat Modelling and security review. In our sample case Region Overrides, Privileged Logins, Schematics, and HW/SW Plans rank at the top of the list. These assets and the systems that manage access to them and data for them need to be put on the radar for thorough Threat Modelling and security review.

This is not to say that things like Corporate Image shouldn't be considered and protected, but for the system under review it is not as likely a target and can therefore be put toward the end of the list. In the event of the inevitable time shortage in the project we can at least ensure that we've examined the most threatened assets.

This shows what areas are most likely to come under attack, and how intense that attack may be. By weighting the attackers according to their abilities and motivation we can get a more accurate picture as to what areas of our system will be under threat and how much threat. Armed with this knowledge, we can dedicate time in our project to make sure that these areas get all the security review that they need to withstand the attacks.

Summary

This system of Attacker Classification will aid software project teams in focusing their efforts on the most vulnerable and high risk areas of the system. It also highlights the assets and systems that will be most abused by potential attackers. By being able to focus on fewer yet more critical parts of the system, the security of those parts can be more closely examined. This is as opposed to having to spread the time and focus of the security team across the entire system and not getting as much in depth work on the critical attack vectors as required.

This is not to say that the entire system should not be scrutinized for security, but with limited resources, and time the critical areas can be identified easier and examined in more detail. Unfortunately in our fast paced IT world, time to market and competitive schedules mean that project timeframes are often much shorter than they should be to ensure thorough end-to-end security reviews and testing. With this system, we can at least ensure that the areas under the most threat do not get overlooked and are thoroughly tested.

Rocky Heckman
http://www.rockyh.net