Taxonomies of Attackers

Franz Rambach
fram008@ec.auckland.ac.nz

Abstract:
If you become aware that an intruder is in your computer system several questions arise e.g. to which type of attacker does this intruder belong. It is very important to answer these questions and to collect information about the intruder so that one can react to the intrusion in an appropriate way. This paper first gives some ideas, which personal properties can characterize an intruder. One important property, which determines the kind of an intrusions are the motives of the attacker. From these three different taxonomies about how an attacker can be classified are derived. These classifications are compared and examples about different attackers and their classification in the different taxonomies are given.

1. Introduction

When your Intrusion Detection System (IDS) says there is an attack going on several questions arise. After confirming the alarm generated by the IDS has not been due to a false alarm, the most important question is of course what should be done. If an intruder wants to break into your system or perhaps is already in your system and has compromised other elements of your network you must develop ways to cope with this. But prerequisite for this is the collection of enough background information such as knowledge about the network topology and information about the intruder. Then a decision must be made which means would be appropriate and finally can be executed. In some situations there might also be the opportunity to predict what the attacker will do next. But - as already mentioned - without enough information about the attacker one will not be able to react appropriately to an intrusion.
There are several questions, which could help to characterize an intruder: Who is the attacker? Where is he? What are his aims? Has he already compromised other systems in the network? Why was he able to get into the system and how did he get into the system?
By answering these questions it will become a lot clearer what should be done next.
This paper deals with the important question who the attacker is. Hence, in the second chapter a basic description how to characterize an attacker upon his personal properties is given. Based on an attacker's motives and knowledge – personal properties - three possible

taxonomies are introduced: A taxonomy based on Pfleeger [Pfl97], one used by the Federal Bureau of Investigation and a third taxonomy described by Icove [Ico97], Yuill [Yui00] and Chapa [Cha96] are explained. In the following chapter these three different taxonomies are compared with each other and similarities are described. The fifth chapter gives two examples and embeds the appearing attackers in the different taxonomies. In the last chapter a summary is given.

2. Characterizing an attacker

If there is a good description of an attacker available the prediction of the course of action is much more precise and the already compromised devices are more easily identified. Hence, it is sensible to answer the question: What do we really know about an attacker?
To answer this question one should collect all possible information about an intruder, so that one can describe him.
First of all, everything, what the intruder has already done, should be observed. This includes the attacks and how he uses the devices and the data he has access to. Yuill [Yui00, p. 686] suggests the attacks can be partly described by watching the following attributes:

- occurrence of activity,
- patterns of behavior, e.g. time, tactics or network access,
- network activity: sources, destination addresses, the path taken,
- devices accessed: hardware, operating system, servers and applications,
- data accessed,
- tools and techniques used,
- files left on systems,
- information that can be used for intrusion-detection,
- degree of success,
- type of security compromised: confidentiality, integrity, availability,
- vulnerability compromised,
- exploits used.

How the attacker uses the data and the devices he has gained access to, can reveal his aims and capabilities. Some examples are “(1) sending messages, e.g. via Internet-chat or e-mail,

(2) storing data, or running servers, on the device, (3) connection hopping for account laundering." [Yui00, page 687]
There are of course other possibilities to get information about the attacker. For example if the malicious user can be detected as an insider there are some attributes automatically given. Another possibility, which increases our knowledge, is if an attacker is identified as an intruder from an earlier attack. So the former collected information about the main patterns of the intrusion can now support to defend the attack.

After this information-collecting phase the actual characterization of the intruder takes place by examining the attacker's **capabilities**, his **personality traits** and his **intentions**. The categorization of the attacker's properties into the mentioned three major groups has shown its usefulness. Further the three categorizes are again subdivided, as shown in Figure 1.

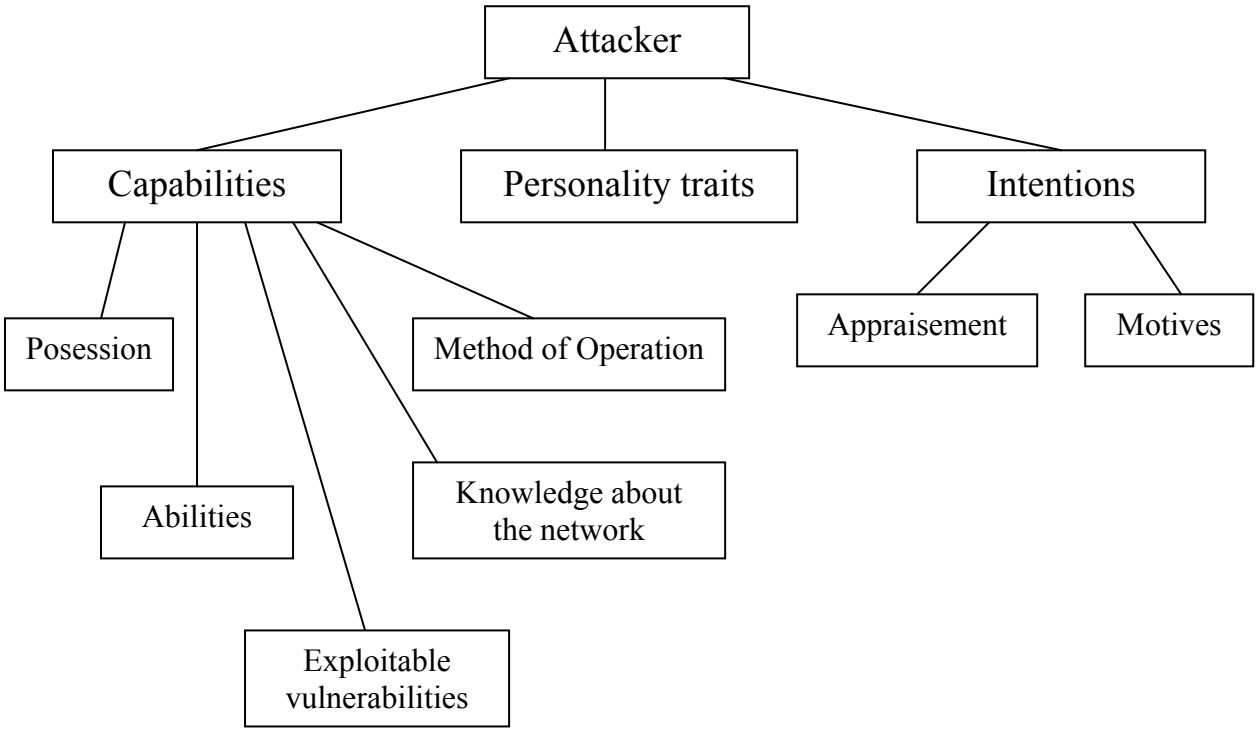

Figure 1: Characterizing an attacker

Capabilities are divided in *abilities*, the *method of operation*, the *knowledge about the network*, the *possession* and the *exploitable vulnerabilities*.
The *abilities* are the possibilities what the attacker can do. These possibilities depend for instance on his computer skills. Computer skills include for example how well he knows the

different operating systems. Perhaps he knows Unix very well but has no experience with Windows. The abilities depend also on the intruder's attack skills. This is the ability to find and exploit vulnerabilities. Another point by which the abilities are influenced is the attacker's tenacity. This is equal to his persistence that means how long he tries to get into a system.
In contrast to the *abilities* does the *method of operation* describe what the attacker really does. Hence, this is a summary of the habits, techniques and peculiarities of the attacker, which consists e.g. of a list of exploits used or techniques used for avoiding detection as erasure of log-file entries [Yui00, p. 688].
The **capabilities** are also based on the *knowledge about the network*. If he for example knows exactly where the server with the data he wants to get access is, he can directly attack it.
The *possessions* of the attacker are the already compromised devices. He can for example use trust relationships to get easy access to other devices.
The last point mentioned by Yuill [Yui00] about **capabilities** is the *exploitable vulnerabilities*. These are the possible devices, which the attacker can compromise.

As the second major category the **personality traits** are also characterizing the attacker beside **capabilities** and **intentions**. Yuill [Yui00] mentions following personality characteristics, which will determine the kind of intrusion an attacker will lead:

- Judgment summarizes the degree to which the attacker thinks clearly. Judgment can be impaired by vices like greed, arrogance, obsession and vengeance.
- Morality governs the degree to which he is willing to inflict loss.
- Patience is needed for stealth and the pursuit of long-term goals.
- Cautiousness influences the risk he is willing to take and the precautions he takes.

[Yui00, page 689]

The three taxonomies introduced in the next chapter are all based at least partially on the **intentions** of an attacker. These **intentions** are again divided in *appraisement* and *motives*. In chapter three the motives are discussed in detail by defining the different taxonomies, which are partly based on the motives. *Appraisement* means how the attacker values network assets. An attacker who only wants access to special data in a special server is not interested for example in the web server. If he can compromise the web server it is not very much gain for him.

3. Different Taxonomies

In this chapter three different taxonomies are introduced. Each of them is based on the motives and/or on the knowledge of the intruder.

3.1 Pfleeger's Taxonomy

Pfleeger [Pfl97] distinguishes between three different attackers (see also figure 2): Amateurs, crackers and career criminals.
The amateurs are the "normal" people who exploit the apparently security flaws to gain an advantage. So is a worker in an office, who can simply read the mail from other users, in Pfleeger's taxonomy an amateur.
The crackers have more knowledge than the amateurs. They see often a challenge to break into a system and most of them have the attitude that there is no real victim. They use the World Wide Web, email, forums, etc. to get the newest information about insecure systems. "There is no common profile or motivation to attackers [crackers]." [Pfl97, page 12]
The career criminals are real experts who started commonly as computer professionals. They break into the systems to get some important data and sell them. This is often their main income.
As one can see Pfleeger's distinction between the three different attackers are based on their motives and knowledge. The amateurs do neither have a special knowledge about security flaws nor a special motive. They only want to get an occasional advantage. In contrast to that crackers search for information about insecure systems and they have a general knowledge about them. Either they have not the knowledge to make a profession out of their attacks or they do not have the motives. On the other hand there is the career criminal who knows very much about the computer system and has a clearly defined motive to earn money with his intrusions.

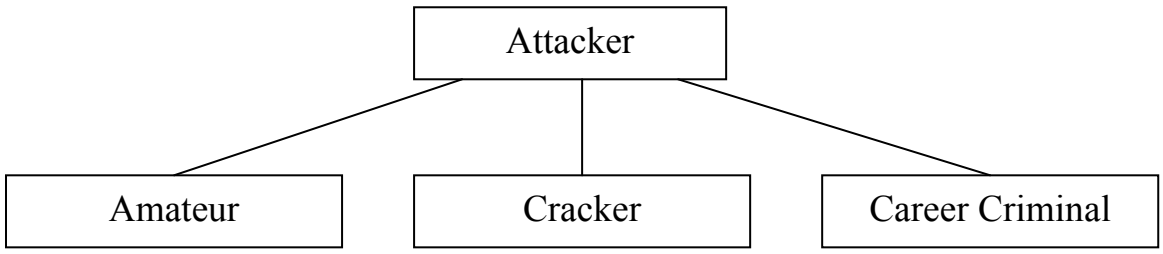

Figure 2: The taxonomy of Pfleeger

3.2 Landreth's Taxonomy

This taxonomy is based on Bill Landreth who has written the book "Out of the inner circle" about computer security. I explain a categorization based on Yuill [Yui00], Icove [Ico97] and Chapa [Cha96] who refer to Landreth.
Landreth distinguishes between five different attackers (see also figure 3): Novice, student, tourist, crasher and thief.

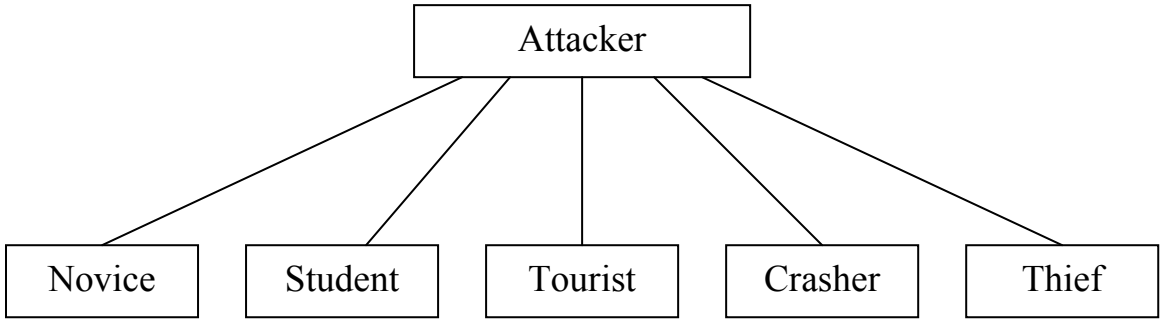

Figure 3: The taxonomy of Landreth

The novice is a young kid - normally between 12 and 14 - who deals with security flaws only a short period of time. After that he becomes a member of one of the four other groups or he is not longer interested in committing such crimes. He sees malicious activities in computer security as a game.
The student is a college-age student who is interested in security. He tries "to find out as much information as possible about the systems they [he] crack[s]." [Cha96]
The tourist is curious about how to break into a system. Normally he logs off very fast except he finds in the intruded system something interesting. His aim is to break into the system and not as the student to study it.
The aim of the crasher - as the name already says – is to produce denial of service. So the common attacks are distributed denial of service (DDoS) attacks. The crasher has often a pseudonym, e.g. THE CRASHER. So he can communicate the victim who has crashed the system and he can get fame among other crashers by publishing his acts.
The thief is the career criminal in Pfleeger's taxonomy. He has very much knowledge about security systems, is very persistent and sells the data he has access to. He chooses his target carefully and is paid for his activities. In contrast to the other groups only a few thieves are ever caught.
Landreth distinguish the different groups especially by their motives. The knowledge of the attacker plays only a minor role in this taxonomy. The novice is most of his free time bored

and is searching something new. For him cracking is something like gaming. The motive of the student is studying the system he cracks. The tourist only wants to manage to break into a system. The goal of the crasher is to crash the system in any way and the motive of the thief is to earn money with his activities.

3.3 FBI Taxonomy

The following taxonomy is based on Icove [Ico97]. The Federal Bureau of Investigation (FBI) has three categories of attackers (see also figure 4): Cracker, vandal and criminal.
The cracker is often a young criminal who sees a challenge in breaking into a computer system.
The vandal has the aim to destroy something electronically. The reasons are often "rooted in revenge for some real or imagined wrong" [Ico97, page 34]. There is not the attitude of seeking a challenge or studying something.
The group of the criminals is again separated in persons "who commit fraud or damage systems and those who undertake espionage."[Ico97, page 34] The criminal is normally a grown-up and can again be compared with Pfleeger's career criminal.
One can easily see that this categorization is based mainly on the motivation. The cracker is searching a challenge in contrast to the vandal who only wants to destroy something. The criminal on the other hand wants to earn money with this kind of crime.

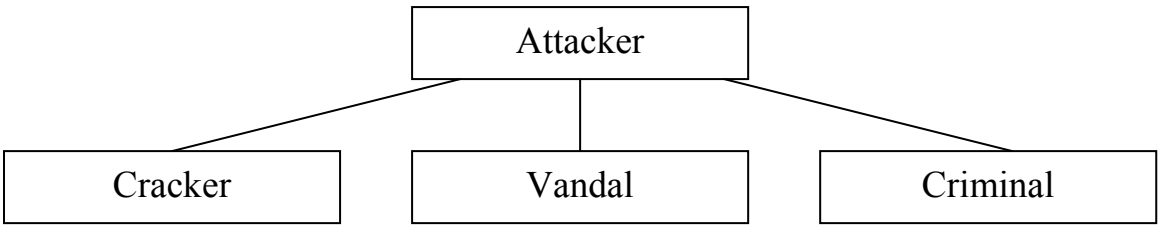

Figure 4: The taxonomy of the FBI

3.4 Other Taxonomies

The taxonomies introduced were based on the knowledge and of the motives of the attacker. There are of course other taxonomies, which are based on other attributes of the attackers. For example one can easily derive from Anderson specification of threats a taxonomy, which "is on the basis of whether or not an attacker is normally authorized to use the computer system, and whether or not a user of the computer system is authorized to use a particular resource in the system." [And80, page 6]

4. Comparison of the introduced taxonomies

We have already seen that these three taxonomies are based on the motives and/or on the knowledge of the attacker. In this chapter the similarities between the different taxonomies are discussed and we will see that they are all very similar. First Pfleeger's taxonomy is compared with Landreth's, then again Pfleeger's with the FBI's and last but not least the FBI's with Landreth's.

4.1 Pfleeger - Landreth

Pfleeger's distinction is based on the knowledge and motives in contrast to Landreth who distinguish only by the motives. This should be kept in mind when we compare both. The summary of this comparison can bee seen in table 1.

We begin in searching Pfleeger's amateur in Landreth's categorization. The amateurs are, as introduced, people with not very much knowledge about security and they gain an advantage by exploiting a security flaw with not much work involved. If we look at Landreth's novice we see much in common: He has also not very much knowledge about security because he deals with it only a short period of time. So we could say that Pfleeger's amateur is in some kind Landreth's novice. All other categories of Landreth do not really fit to Pfleeger's amateur.

Pfleeger's cracker is motivated through several reasons so we will expect to find several groups in Landreth's taxonomy, which fit to the cracker. The cracker "may be [a] university or high school student[s]" [Pfl97, page 12] so it is obvious to look closer at Landreth's student. The aim of the student is to examine the system in which he breaks in. The student has also a much bigger knowledge than the novice. So he has at least one point in common with Pfleeger's cracker. Because there is no motive specified by Pfleeger, the student is a subset of Pfleeger's cracker.

The Tourist fits also very well in Pfleeger's definition of a cracker because the goal of a tourist is to break into a system. In Pfleeger's definition there is also written: "Cracking a computer's defenses is seen as the ultimate victimless crime." [Pfl97, page 12] So another subset of Pfleeger's cracker is found: The tourist.

The crasher can also be seen as Pfleeger's cracker. The motivation "causing chaos, loss or harm" [Pfl97, page 12] is a good description of a crasher, but Pfleeger wrote it as part of the definition of the cracker. Because of this the crasher is again a subset of Pfleeger's cracker.

So there is only Pfleeger's career criminal left and on the other hand the thief. As mentioned in the description of Landreth's taxonomy the thief is the same as Pfleeger's career criminal. Both want to earn money with their activities and they are really specialist in the field of computer security.
We see that both taxonomies are very similar. Landreth's is much more precise because he has more groups involved than Pfleeger.

Pfleeger	Landreth
Amateur	Novice
Cracker	Cracker, Student, Tourist, Crasher
Career Criminal	Thief

Table 1: Comparison of Pfleeger's and Landreth's taxonomy

4.2 Pfleeger - FBI

In this section the taxonomy of Pfleeger is compared with the taxonomy used by the FBI. We should again remember that the taxonomy of Pfleeger is based on the knowledge and on the motives of the attacker in contrast to the taxonomy of the FBI, which is based mainly on the motives.
Besides protecting the United States from terrorist attack, the FBI prioritizes protection of the United States against cyber-based attacks and high-technology crimes as well as espionage [FBI]. So it is obvious that their main interest lays in prosecuting criminals, which are a real threat for the United States. Hence, in their categorization is no group like Pfleeger's amateur, which commits minor, hardly prosecutable crimes.
In contrast to the amateur does Pfleeger's cracker fit in the FBI categorization. He is on the one hand a vandal if he wants to destroy something or he is on the other hand a FBI cracker if he only wants to break into a system.
Pfleeger's career criminal is in the FBI taxonomy the criminal as mentioned before. They have both the aim to earn money with their criminal activities.

Pfleeger	FBI
Amateur	
Cracker	Cracker, Vandal
Career Criminal	Criminal

Table 2: Comparison of the taxonomy used by Pfleeger and the FBI

Both taxonomies have one group in common. It is called criminal career by Pfleeger and simply criminal in the FBI categorization. The cracker in Pfleeger's taxonomy can be found in the group of the crackers or the vandals in the FBI taxonomy. The amateur of Pfleeger cannot be found in the grouping created by the FBI. A summary of this comparison can bee seen in table 2.

4.3 FBI – Landreth

At the end of this comparison chapter there is only the pair FBI and Landreth left.
Like explained in the comparison between the Pfleeger's amateur and the FBI cracker the novice is not in the FBI classification.
We start with the cracker on the FBI side. Landreth's tourist can be grouped in FBI's cracker. The aim of the tourist and in some cases of the FBI cracker is simply to break into the system. So their motives are then the same. Hence, the cracker includes the tourist.
Landreth's student can be seen as part of the FBI cracker because it is a fact that the student breaks into computer systems. The student's goal to study the system is not important for the FBI. Simply the intrusion presents a security risk, which should be prosecuted.
For FBI's vandal it is easy to find a group in Landreth's taxonomy: The crasher. The aim of the crasher is obviously to reduce the availability of a computer system. This can easily be seen as electronic vandalism. So the crasher is a vandal. But FBI's vandal is not equal to Landreth's crasher: For example, an attacker who deletes files on a compromised system is included in FBI's vandal, but such an attacker is not included in Landreth's crasher.
The FBI criminal is the thief in Landreth's taxonomy. This is obvious because both groups have the motive to make a living from exploiting vulnerabilities.
To summarize the main result of this comparison, these two classifications have the Landreth's thief and the FBI criminal in common. FBI's vandal includes Landreth's crasher, FBI's cracker includes Landreth's tourist and student. A category, which fits to Landreth's novice, cannot be found. A summary of this comparison can be seen in table 3.

FBI	Landreth
Cracker	Tourist, Student
Vandal	Crasher
Criminal	Thief

Table 3: Comparison of the taxonomies used by the FBI and Landreth

5. Examples of attackers

In this chapter two different examples of attacks are discussed and the attackers are classified in the different taxonomies. We show that not every attacker can be easily classified with these taxonomies and in some cases there is no right group to which the attacker belongs.

The first example is a distributed denial of service (DDoS) attack executed by a teenager who wants to show his friends how "cool" he is. He wants to achieve this goal with a downloaded tool from the Internet, but he has no idea how the program works. Such children are often called "script kiddies" because they only execute the script they got without knowing how the program operates.
In Pfleeger's categorization it is not clear if such an attacker belongs to the amateurs or to the group of crackers. One argument pointing to the amateurs is that this child does not know very much about security. But he achieves no real benefit by flooding the network although gaining an advantage is defining an amateur. The cracker is characterized in having knowledge about security. In contrast to that the kid has - as already said - no knowledge about how the program works. But Pfleeger also mentions a cracker can "enjoy causing chaos, loss, or harm"[Pfl97, page 12]. Hence, this suggests putting the script kiddy in the class of the cracker. I would put this kind of attacker rather to the amateur group than to the cracker because for me the important point is that the child has no knowledge about security. But it is not clear to which group the script kiddy belongs.
For Landreth's taxonomy it is obvious that this attacker belongs to the crasher group. He wants to crash a system and to get fame among his friends.
In the FBI classification it is also clear where the script kiddy fits in: It is the vandal group because a DDoS attack is clearly electronic vandalism.

The second attack examines the case "of Donald Gene Burleson, a systems security analyst at a Texas insurance company who was upset over being fired. First, he deleted 168 000 of the company's sales commission records. When backup tapes were used to replace the missing files, he then demanded that he be rehired, or else a "logic bomb" in the computer would go off"[Ico97, page 34].
In Pfleeger's taxonomy it is obvious that Burleson is not an amateur because he has a broad knowledge about computer security. He also does not want to earn money with this activity so Burleson is also no career criminal in Pfleeger's classification although he is a computer professional. In addition to that this attacker can hardly be classified as a cracker, because he

seeks no challenge and is aware of his victim, which is his former employer. By extortion he wants to force rehire. Hence, Burleson does not fit in this classification. If I had to put him in one of Pfleeger's groups I would classify him as a career criminal because of his professionalism and his true criminal activities.
In Landreth's taxonomy there is no real group to which he belongs. The aim of a novice to play is not Burleson's goal. Neither is he interested in the computer system nor is it a challenge for him to break into this system. So Landreth's student and the tourist are also not the group to which he belongs. The thief is another example of a group, which he does not fit in. As already mentioned the thief is the same as Pfleeger's career criminal and I have already proven that Burleson does not fit in this category. So there is only the crasher left in this taxonomy, but the crasher does only want to crash the whole system. Again Burleson does not belong to this group. The category of the thief seems to be best suited to him because of the same reasons as explained for Pfleeger's career criminal. He is committing a worse crime by his extortion and can be regarded as a hazardous person.
The FBI categorization is ideal for this case. Here it is obvious that he belongs to the vandals because Burleson destroys the files. His attack and extortion can be "rooted in revenge for some real or imagined wrong" [Ico97, page 34]: His discharge.

6. Conclusion

This paper has introduced three different taxonomies of attackers based mainly on their motives. Summarizing the main results of this article following statements can be made:
Pfleeger's classification is not so specific because some kind of attackers cannot be put in one of his classes, e.g. Burleson.
Landreth's categorization is more useful because he subdivides Pfleeger's cracker group in four other smaller groups: crasher, cracker, student and tourist. Hence, more different, existing groups of attackers have their own group in Landreth's taxonomy and for this the taxonomy is more exact. Once identified the attacker of a computer system as a member of one of these classes more appropriate means can be developed to react to the incident. But there are still some cases, which are not covered with this categorization e.g. the Burleson case.
The FBI classification distinguishes the groups with the aim to prosecute the criminals and misses the fact that there are some smaller crimes committed for example by Pfleeger's amateur. Hence, this taxonomy does also not cover every kind of attacker, but the FBI is able

to put an attacker committing a worse crime in one of their classes and develop ways to cope with such an intrusion.

Because of the fact that all these taxonomies have a lack in the categorization it is not possible to classify every attacker in every taxonomy.

References:

[And80] Anderson, James P. Computer security threat monitoring and surveillance. [Article online] 1980 Feb. 26, Revised 1980 April 15; 6 par. Available from: http://seclab.cs.ucdavis.edu/projects/history/CD/ande80.pdf Accessed 2003 Jun. 9.

[Cha96] Chapa, S., Craig, R. Who Are These Crackers, Anyways? [Website online] 1996 March 31; Available from: http://www.inforeading.com/archive/text_files/mischief/cracking/whocrack.html Accessed 2003 Jun 9.

[FBI] FBI Priorities [Website online] Available from: http://www.fbi.gov/priorities/priorities.htm Accessed 2003 Jun. 9.

[Ico97] Icove, David J. "Collaring the cybercrook: an investigator's view." IEEE Spectrum, vol.34, no.6, June 1997: 31-36.

[Pfl97] Pfleeger, Charles P. *Security in Computing.* 2nd ed. Upper Saddle River, NJ : Prentice Hall PTR, 1997

[Yui00] Yuill, J., Wu, F., Settle. J., Gong, F., Forno, R., Huang, M., Asbery, J. "Intrusion-detection for incident-response, using a military battlefield-intelligence process." Computer Networks: the International Journal of Distributed Informatique, vol.34, no.4, Oct. 2000: 671-97.