The Great Never-Ending Taxonomy Project

(A short[1] story)

by Patrick Cain,
APWG Resident Research Fellow

What is a taxonomy?

A taxonomy, ?http://en.wikipedia.org/wiki/Taxonomy, is a scientific way of classification. The goal of an electronic crime (ecrime) taxonomy is to try and determine groupings of similar crimes to assist in perpetrator and victim identification and to identify similar techniques for detection and investigation. And to use as an aid when dealing with law enforcement types, judges, attorneys and government officials . At least that's my goal.

In the beginning?

Everybody wants to define 'cybercrime' so one can use 'metrics' and 'statistics' for 'scary things'. We did, too, as it makes exchanging data easier if the originator and the recipient speak the same techo-language. So we started an informal taxonomy project. Additionally, we said ‘taxonomy’ instead of ‘common marketing terms’ since one of the goals was to help educate the legal and law enforcement types on various new attacks and techniques and how they relate to rules that put people in jail. So the adventure began...

The first 'this will be easy' cut

We started like everyone else -- by defining 'phishing', and 'pharming', and other stuff and trying to relate them. You quickly find out that there are two broad categories of electronic crime: (1) fraud, and (2) everything else. And 'fraud' covers 95% of the current crimes. And since everyone has their own terms for the same crime (see 419 scam, AFF, et al) defining by the technology term makes for a really complex taxonomy. And a never ending one. And it doesn't help with the judicial education since they speak in *crimes*.

The second, 'that didn't work' attempt

Another version was attempted, but this time shying away from the straight technology name and using the polices' "Types of Cybercrime" definitions. Many law enforcement circles and criminologists split eCrime into three categories:

- 1. Crimes where the computer is the target. For example, DOS attacks, or system compromises
- 2. Crimes where the computer is used as a vehicle for performing the crime, as in being used to launch a DOS attack or to send a threatening email message or as a proxy.
- and 3. Crime where the data on the computer is criminal, as in illegal porn, copyright violation, etc.

This characterization moves the discussion from technological names closer to the actual crime type that was attempted. Unfortunately, crimes can cover multiple of the three categories. In talking with our intended audience, they had direct legal questions on the categories and words and their relation to the actual *crime*. Still. So we moved away from using techie-speak, but we still had a gap to the legalities.

The third try from a different angle

Then I had discussions with various people who would use a taxonomy. Many people wanted to know what the event or crime was called, but came at it from the actual **threat** ?http://en.wikipedia.org/wiki/Threat, or **risk** ?http://en.wikipedia.org/wiki/Risk, not from the resultant crime part. So after some thought, I turned the picture I had around and looked at it from what used to be the end. ISO (ISO27032) defined seven types of *threats* to an Internet-connected object, so I divided them up to make a nice chart. And added some extra types.

The **major threat** categories were: Financial Loss, Proprietary Data Misuse, Personal Data Misuse, Controlling and Access to Prohibited Content, Distribution of Prohibited Speech, Business Interference, Loss of Network Control and Loss of Privacy. Others convinced me that Reputation Loss and Personnel were major threats, too.

Financial Loss

- Fraudulent transactions
- Improper Credential Use
- Laundering Activities
- Extortion

Proprietary Data Misuse

- Possession
- Corruption, Deletion
- Misuse

Personal Data Misuse

- Possession
- Alteration
- Misuse/Trafficing??
- Falsification

(Content Control)

Access to Prohibited Content

- Illegal porn

Distribution of Prohibited Speech

- Hate speech
- Death threats
- Cyber-bullying

Business Interference

- DOS

Loss of Network Control

- Network Service Unavailable ? (DOS)

• Cyber Stalking	• Pirated artistic works	• Network Compromised
(Reputation Loss)	*(Personnel)*	Loss of Privacy
		• Data Aggregation

This did not work out either, as it didn’t relate to, nor help explain, eCrime as the legal friends thought of it.

The current (fourth) Taxonomy

I should at least get credit for trying...although it may be futile...

So, after explaining what I was trying to do, it was suggested to me that I was looking at it wrong. Techies are easy to re-train (note the transition from COBOL to Java) but the legal side of the house is very stoic in their ideas. So this version started with a list of crimes, 'serious crime' in the parlance, and broke them down so that each successive breakdown made it more specific. After enough dissection, the result should be 'phishing', or 'pharming', or '419'. So we went from the major crime 'types' down to how that crime is perpetrated on the Internet. Or, in some cases like murder, isn't perpetrated on the Internet. This way we can explain to the legal community the techie terms but using dissections that they may be familiar with.

Now we just had to figure out how to list the major crime types.

The in-process document is here.

[1] 1. And everlasting, too

Bibliography

(ISO27032) ISO/IEC 27032 Information technology ? Security techniques ? Guidelines for cybersecurity (FDIS)