RIP: A Crime Classification System to Improve eCrime Reporting, Metrics and Response

Patrick Cain
Resident Research Fellow, APWG
The Cooper-Cain Group, Inc.

APWG
Unifying the
Global Response
to Cybercrime

A Problem

- More internet investigations are using different terminology to describe the same activity
- eCrime is evolving from spam, phishing, etc., to "just one message does it all"
  - Categorizing incoming data is getting harder
  - Metric generation is even harder
  - Law enforcement education is more challenging
- Different countries use different terms for the same activity
  - International data exchanges get confusing

A Potential Solution

- Develop a classification system (common terms & categories) for eCrime
  - Allow easier marking of exchanged data sets
  - Provide collection guidance on specific elements
  - End up with cleaner metrics + charts ☺
- This can't be too hard.
  - "…attempting to establish a taxonomy of cybercrime is an artificial and somewhat pointless exercise" – Oxford Internet Institute (2010)

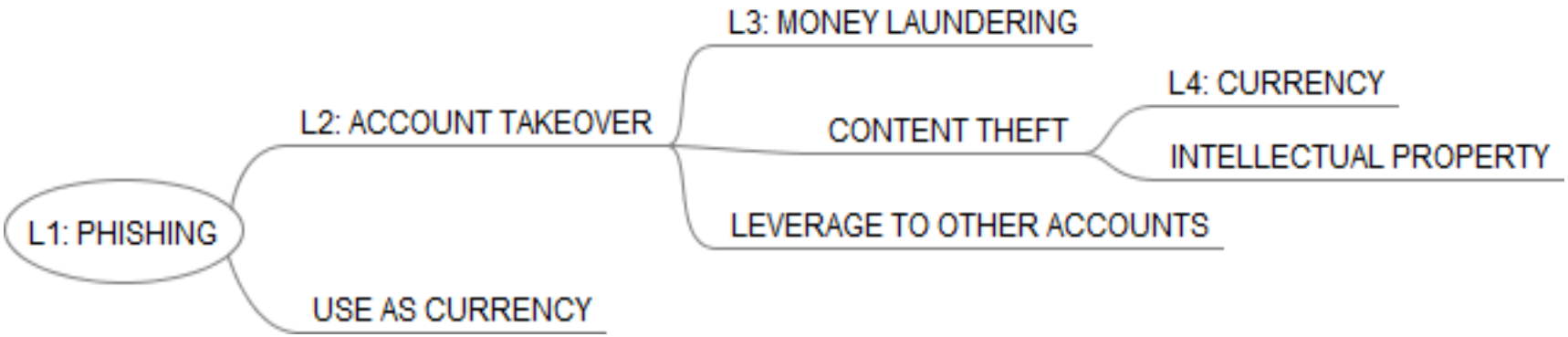
Off we go…

- Write down some types of crime and classify
- We all know what phishing is…
  - But we don't. Everyone has their own definition!
- Task #1 became "come up with some definitions for things we already know"
  - This became a project amongst itself
  - Iain Swaine is running this project

The First Effort
(Classify by Technology Term)

- We can't be the first people trying this…
- David Wall's book "Cybercrime" has a good breakdown of eCrime things
  - Older book, evolution added new things
  - We used it as an example
- Classify by 'technical term'
  - Phishing, 419, farming, etc

Example of First Attempt



L1 = technical term
L2 = general purpose
L3 = criminal activity
(may be multiple L3s)
L4 = gain or output

First attempt cont'd

- A quick scan ended up with two categories:
  - Fraud (95% of the crimes)
  - Everything else

- Stopped and rethought the approach

Second try
(classify by computer crime 'type')

- The FBI has a classification system for eCrime:
  - Crimes where the computer is the ***target***. For example, denial of service (DOS) attacks or system compromises.
  - Crimes where the computer is used as a ***vehicle*** for performing the crime (as in being used to launch a DOS attack), to send a threatening email message, or as a proxy.
  - Crime where the ***data*** on the computer is criminal, as in illegal porn, copyrighted material, etc.

Second (failed) try

- Discussions raised questions
  - specific word choices
  - The relation to the actual *crime*, particularly when the crime was not exclusive to a computer (as in an email message that results in person to person violence)
  - US specific

- More rethinking occurred

Third (failed) try
(Classify by risk or threat)

- Classify the criminal activity by the threat or risk to the victim
  - ISO 27032 seven threats

The threats dissected

- Financial Loss
  - Fraudulent transactions
  - Improper Credential Use
  - Laundering Activities
  - Extortion
- Proprietary Data Misuse
  - Possession, Misuse
  - Corruption, Deletion
- Personal Data Misuse
  - Possession
  - Alteration
  - Misuse/Trafficking??
  - Falsification
- *(Personnel)*
- (Controlling Content)
  - Access to Prohibited Content
  - Pirated artistic works
- Distribution of Prohibited Speech
  - Hate speech
  - Death threats , Cyber-bullying
- Business Interference (DOS)
- Loss of Network Control
  - Network Unavailable (DOS)
  - Network Compromised
- Loss of Privacy
- *(Reputation Loss)*

Nawh…

- Things fall into multiple places
  - E.g., phishing
- Don't really map into 'crimes'

- More rethinking occurred

Fourth (not failed yet) try
(Start from the crime)

- Define standard 'crime' types
  - Ignore the non-internet ones
  - Inject the technical term into a crime

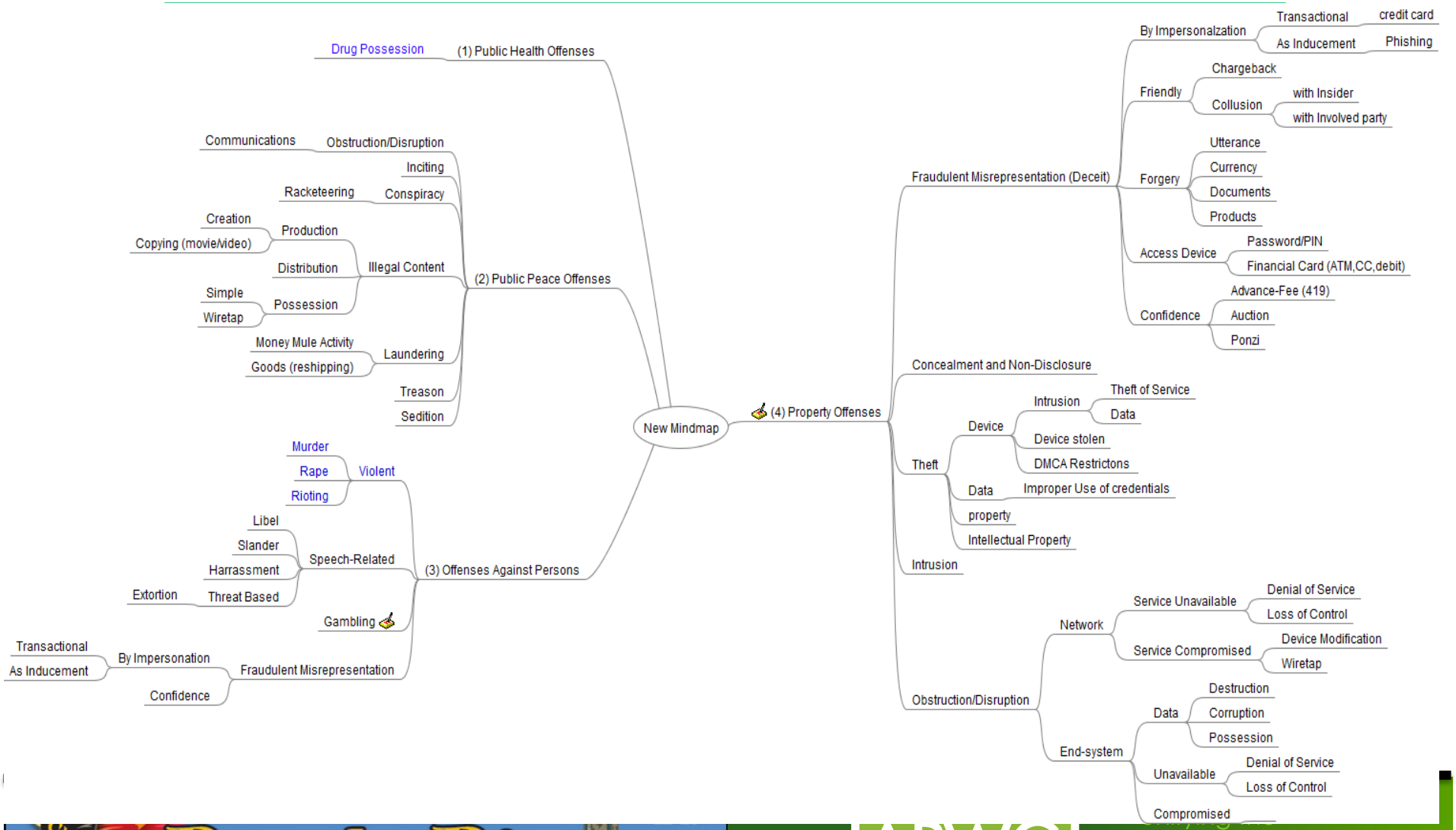
There are four crime 'types':

- Offenses against the ***public peace and order***, such as treason, rioting, and any obstruction of the officers of the law. Offenses against the government are included in this category.
- Offenses against the ***public health and morals***, such as bigamy, the nonmedical sale of narcotics, or the pollution of the public water supplies.
- Offenses against the ***person***, such as murder, manslaughter, or assault.
- Offenses against ***property***, including burglary, theft, fraud, and so on.

Fourth try

- The good side
  - There is international knowledge already
    - LEOs and justice know crime definitions
    - … and we can retrain the techies
- The bad side: it's been tried before.
  - There are Classifications by
    - impact on victim
    - type of perpetrator (or community)
    - Type of apparatus used

The current dissection



Puerto Rico APWG

APWG Global Response to Cybercrime

The work is on-going

- Trying to stay technology neutral
- We're taking our time
- YOU can add value
  - https://repoman.apwg.org/research/wiki/patsTaxonomy