From Criminal to Digital Criminal Profiling: Advances in Criminal Profiling in the Digital Age

George Chlapoutakis

SecurityBible Networks

george.chlapoutakis@secbible.com

http://www.secbible.com

Introduction

- Topics to be covered:
  - Defining criminal profiling
  - Early attempts and models
  - From Criminal to Digital Criminal Profiling
    - Criminal profiling on the Internet
      - Theories and models
    - Defining a digital criminal's profile
      - Conceptual model
      - Issues and considerations
      - Possible vectors to follow

Defining Criminal Profiling

- The **process** of inferring the **physical, mental and behavioural traits** of individuals who have committed a crime through the analysis of various aspects of **the crime scene**, **the crime** itself and **the victims statement**
- Purpose: Intelligence or Evidence?
  - **Intelligence**
    - Not concrete enough to have evidential value

Profiling in the US

- Focus on analysing groups of offenders
- FBI's Behavioural Analysis Unit (BAU)
- "organised/disorganised dichotomy"
  - Sophistication, planning and competence
- Larkin's "marauder" vs "commuter"
  - Close to home vs further away from home
- Cantor & Cohen's Routine Activity Theory

Routine Activity Theory

"any successfully completed violation [that] requires at a minimum **an offender** with both **criminal inclinations** and **the ability to carry out those inclinations**, a person or object providing **a suitable target** for the offender, and **the absence of capable guardians** capable of preventing the violation."(Felson and Cohen, 1980; Felson, 1987)

- Actors: Offender, Target, Supervisors (guardians)
- Supervisors: guardians, handlers and managers
  - with personal, assigned, diffuse and general responsibility
- Opportunity: the time window the offender has in which to commit a crime

Profiling in the UK

- Focus on offenders as individuals
- Attempted to modify the US models to work for individual offenders
  - Through the use of clinical psychology, psychiatry & victimology
- Also focused on victim & witness description validity
- The FBI's BAU models remained as the more scientifically-acceptable.

Profiling in the rest of the world

- Where the US and the UK, the rest of the world largely followed.
- Holland: National Criminal Intelligence Division (NCID) of the National Police Agency.
  - More open to scientific rigour & the scientific community:
    - critical analysis & evaluation, publication of such evaluations
  - Profiling: detective work + behavioural science work.
  - “an instrument for steering an investigation in a particular direction."(Jackson et al., 2006)

Profiling in the rest of the world

- France: Developed a generalised framework for simulating the propensity to offend
- Software agents: simple criminal behaviour model
  - “honesty index" rating of each agent's interest in abiding by the law.
- Result: Existence of a self-organised state through which social dynamics determine and set the line between offenders and non-offenders in the society as a whole.

Criminal Profiling on the Internet

- Internet vs Real World
  - communication and interaction between widely-spaced individuals
  - In almost real time
  - the ability of the offender to attack targets is multiplied
  - ability of attackers to assume virtual identities that are greatly separated from their normal identities

Criminal Profiling on the Internet

- This means that:
  - theories like the Routine Activity Theory need to be modified to address these issues.
    - value, inertia and accessibility
- Also to be taken into account:
  - Globalisation
  - Distributed networks
  - Synopticism and Panopticism
  - Asymmetric relationships
  - Data trails
  - Changes in the actual organisation of criminal activities

The Wall and Marshall & Tompsett methodologies

- Another methodology (Wall and Marshall & Tompsett) classifies Internet crimes according to either:
  - Type
  - Level of Opportunity

Type & Level of Opportunity

- Type:
  - crimes against machines that are integrity-related
  - crimes against machines that are computer-related
  - crimes in the machine that are content-related
- Level of Opportunity:
  - traditional crime: using computers
  - hybrid cybercrime: traditional crime + Internet
  - true cybercrime

The Marshall & Tompsett model

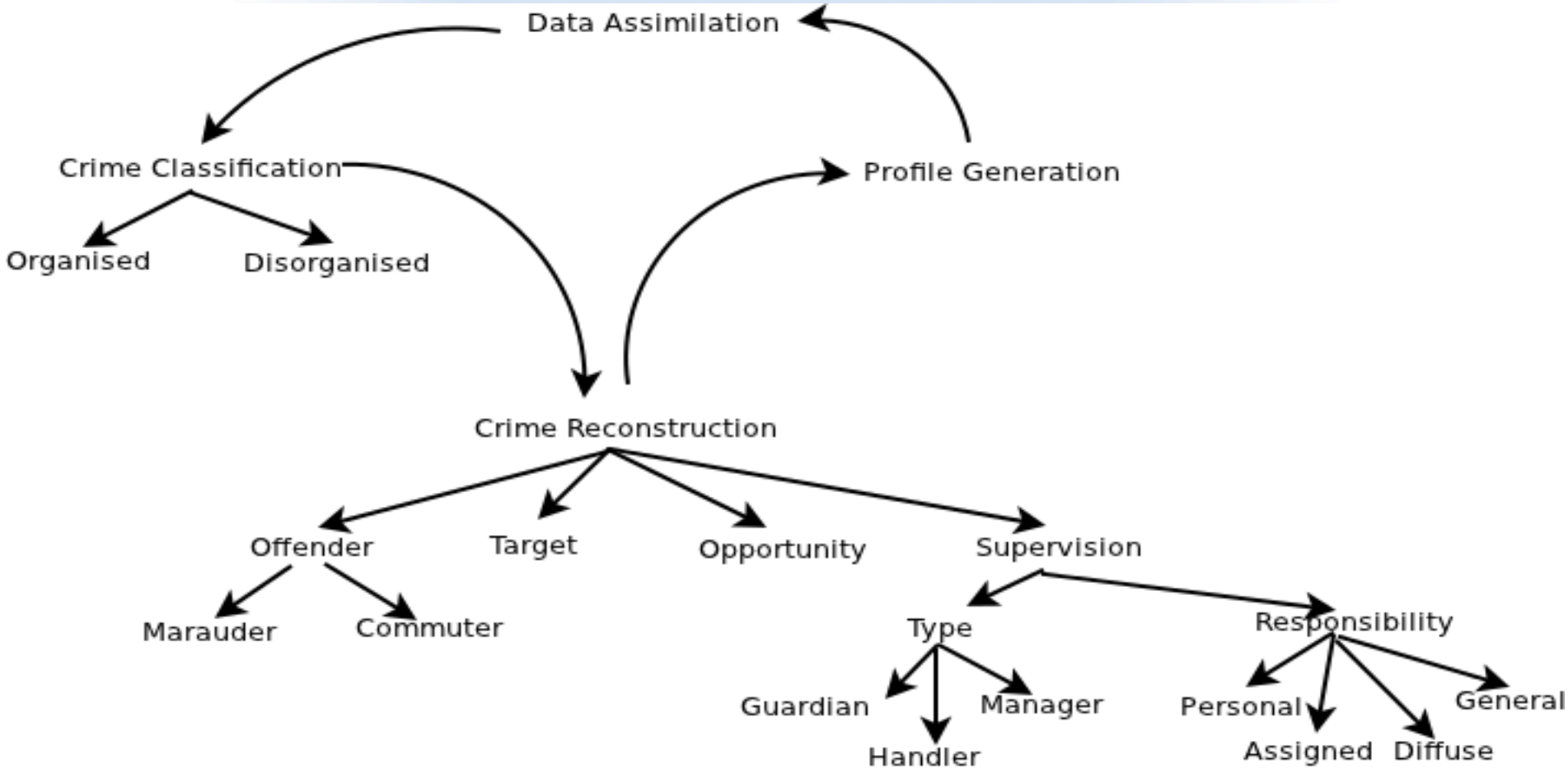
$$L = \frac{C_e * C_f * A}{V_e * (C_g)^x * V_g}$$

- L = likelihood of attack
- Ce = criminal expertise
- Cg + x modifier= importance of the guardianship on the attacker
- Vg = environment and the presence or absence of a guardian
- A = the nature and elements contributing to a successful attack
- Ve = the victim's expertise
- Cf the criminal's freedom

Other modelling methodologies

- Using a number of popular self-descriptory terms used in the computer underground
  - “white-hat", “black-hat”, “gray-hat" hackers, script kiddies etc.
- Using abstract and not rigorous notions
  - like the age of the offender

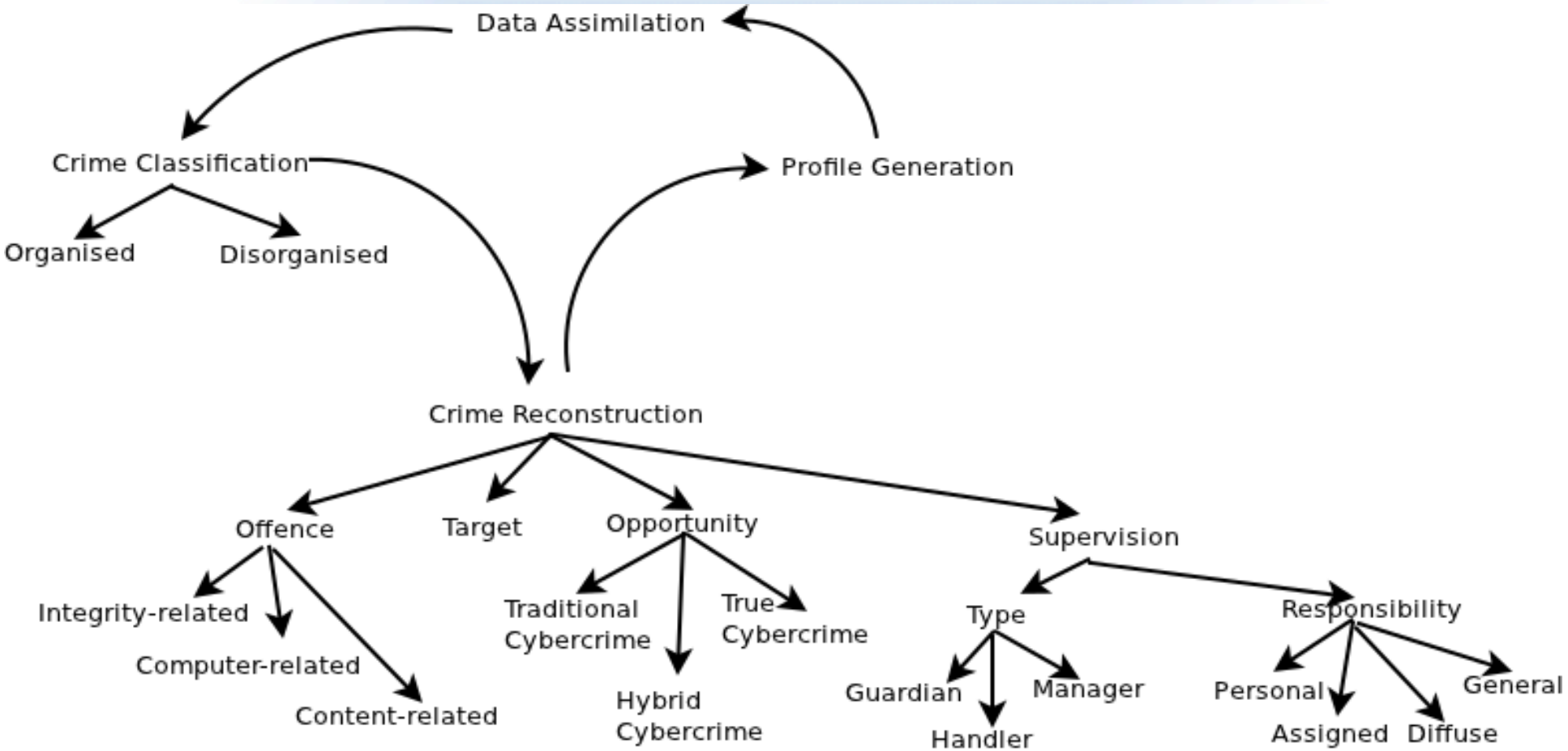
Building a Meat-space Criminal Profile



Turning the Meat-space Criminal Profile to a Digital Criminal Profile

- The process requires:
  - The deviation from the marauder/commuter offender theory to a more Internet-related one
    - where we concentrate on the offence rather than the offender
  - The change in the types of opportunity the offender has
  - The change in the types of supervision available to the victim

The Digital-Criminal Profile



Considerations given the Digital Criminal Profile

- Changes in our thinking:
  - Guardianship →type and responsibility of the supervision
    - dependent on the social structure of the organisation and country
  - Opportunity needs to be inserted into the equation → a measure of time, a time window
    - One that both the criminal and the victim don't really know about.
      - And cannot necessarily predict.

Possible vectors to consider

Methodologies taken from the fields of

- Intrusion Detection
- Computational Statistics

Why?

- Internet-related activities → time series data
  - take into account both the
    - location
    - Patterns
  - of both the criminal and the victim

Conclusions

- We have:
  - Defined criminal profiling
    - Early attempts and models
  - Discussed
    - Criminal profiling on the Internet: Theories and models
    - Defined a conceptual model of a digital criminal profile
    - Some changes in our thinking of digital criminal profiling
    - Some new vectors to follow