PROFILING THE CYBERCRIMINAL

Dr Jason R. C. Nurse
Cyber Security Centre,
Department of Computer Science
University of Oxford

@jasonnurse

Dr Maria Bada
Global Cyber Security Capacity Centre,
University of Oxford

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

CYBERCRIME – THE CHALLENGE

- **Cybercrime** or computer crime is any crime that involves a computer and a network.

- **Cybercrime** is defined as crime committed on the Internet using the computer either as
  - a tool
  - a target

CYBERCRIME – THE CHALLENGE

A) Using the computer as a tool:

- The target is an individual in the real world
- No high level of technical expertise is required
- The objective is to attack a person in a subtle manner and on the psychological level

B) Using the computer as a target:

- Crimes committed by groups of collaborating individuals
- High level technical knowledge and skills are is required
- They require coordination of individuals
- They are sophisticated crimes

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

REFLECTING ON CURRENT RESEARCH & PRACTICE

- Currently research focuses on the
  - Impact of an attack
  - Economic (and financial) harm of an attack

- The stereotype of the uncertain, geeky hacker, relates to the cautious, stealthy approach

REFLECTING ON CURRENT RESEARCH & PRACTICE

- Cyber attacks are:
  - More aggressive
  - More organised
  - Often use extortion
  - Cause fear and uncertainty to victims

REFLECTING ON CURRENT RESEARCH & PRACTICE

- Governments attempt to respond with law
- Corporations with policies and procedures
- Suppliers with terms and conditions
- Users with peer pressure
- Technologists with code

➢ The challenge is to factor in an understanding of criminal behaviour that has been amplified and facilitated by technology (Europol, 2011).

REFLECTING ON CURRENT RESEARCH & PRACTICE

- We need to understand cybercriminal behaviour in order
  - to develop strategies to combat isolated lone cyber criminals
  - and complex and sophisticated cyber criminal networks

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

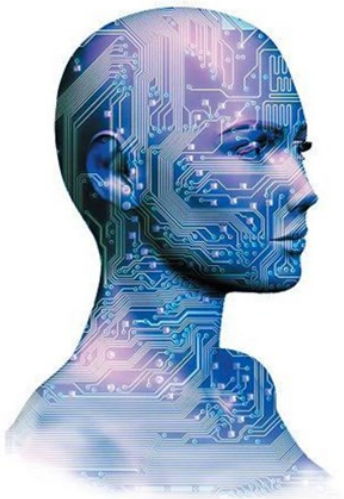
PROFILING THE CYBERCRIMINAL

- The key step in profiling a cybercriminal is identifying specific common characteristics that need to be investigated:
  - personal traits/characteristics
  - social characteristics
  - technical know-how
  - motivating factors

PROFILING THE CYBERCRIMINAL

Personal traits/characteristics

- The innate self
  - Openness
  - Conscientiousness
  - Extroversion
  - Agreeableness
  - Neuroticism



- Life experiences
  - Machiavellianism
  - Narcissism
  - Psychopathy
  - Sensation Seeking maturity
  - Aggressiveness
  - Social-skill problems
  - Superficiality
  - (lack of) self-esteem and personal integrity

PROFILING THE CYBERCRIMINAL

Motivating factors

Hacktivism

Espionage/Sabotage

Monetary gain

Political/religious belief

Curiosity/Boredom

Intolerance

Enhancing self-worth

Emotion/Sexual impulses

Thrill-seeking

Control-manipulate others

PROFILING THE CYBERCRIMINAL

- Rogers M. (2006) has identified types of cyber-criminals distinguished by their skill levels and motivations:
  - Novice
  - Cyber-punks
  - Internals (Insider threat)
  - Coders
  - Information warriors/cyber-terrorists
  - Old guard hackers
  - Professional cybercriminals

PROFILING THE CYBERCRIMINAL

Inductive and deductive profiling

Forensic psychologists use inductive or deductive profiling to make an educated guess of the characteristics of criminals.

A) Inductive criminal profiles are developed by:

- Studying statistical data involving known behavioural patterns
- Demographic characteristics shared by criminals

B) Deductive profiling uses a range of data:

- Including forensic evidence
- Crime scene evidence
- Victimology
- Offender characteristics

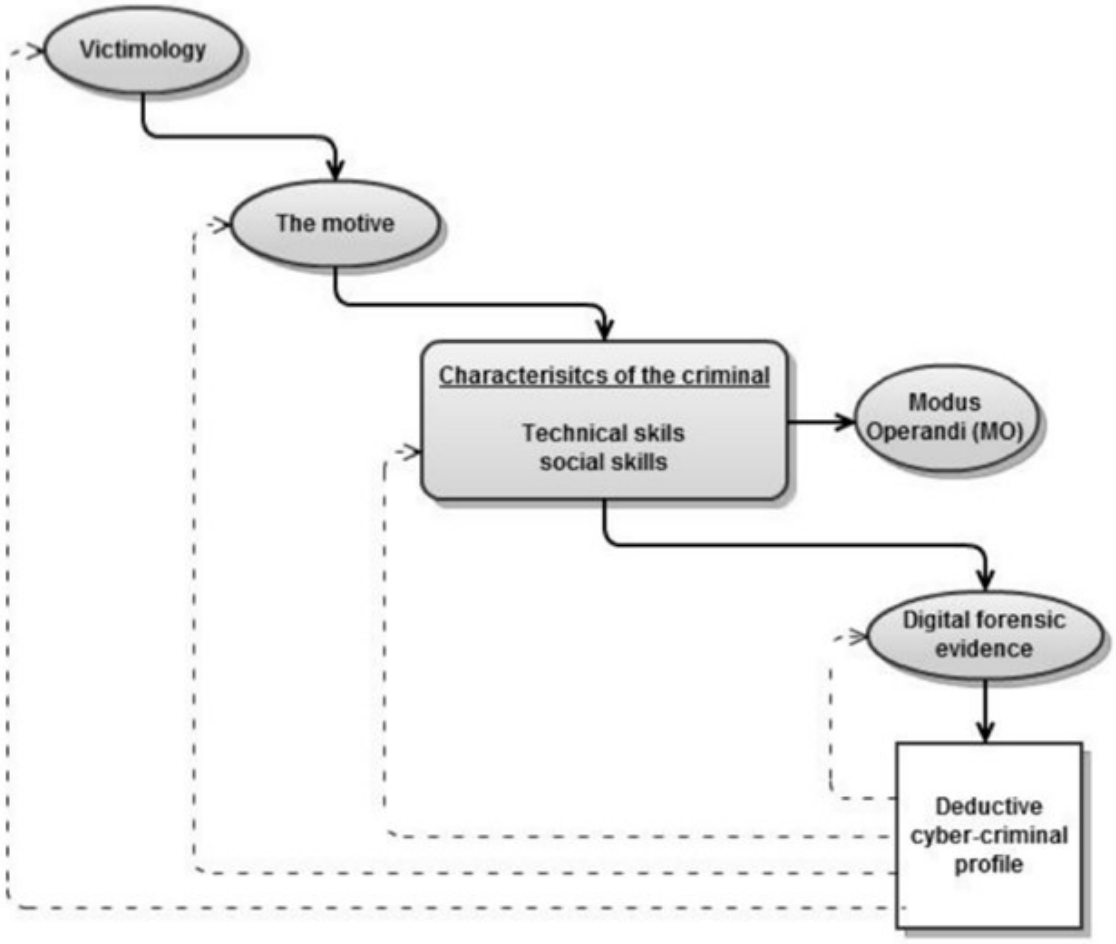
PROFILING THE CYBERCRIMINAL

Models on profiling

A Deductive cybercriminal profile Model (Nykodym et al., 2005)

Information about

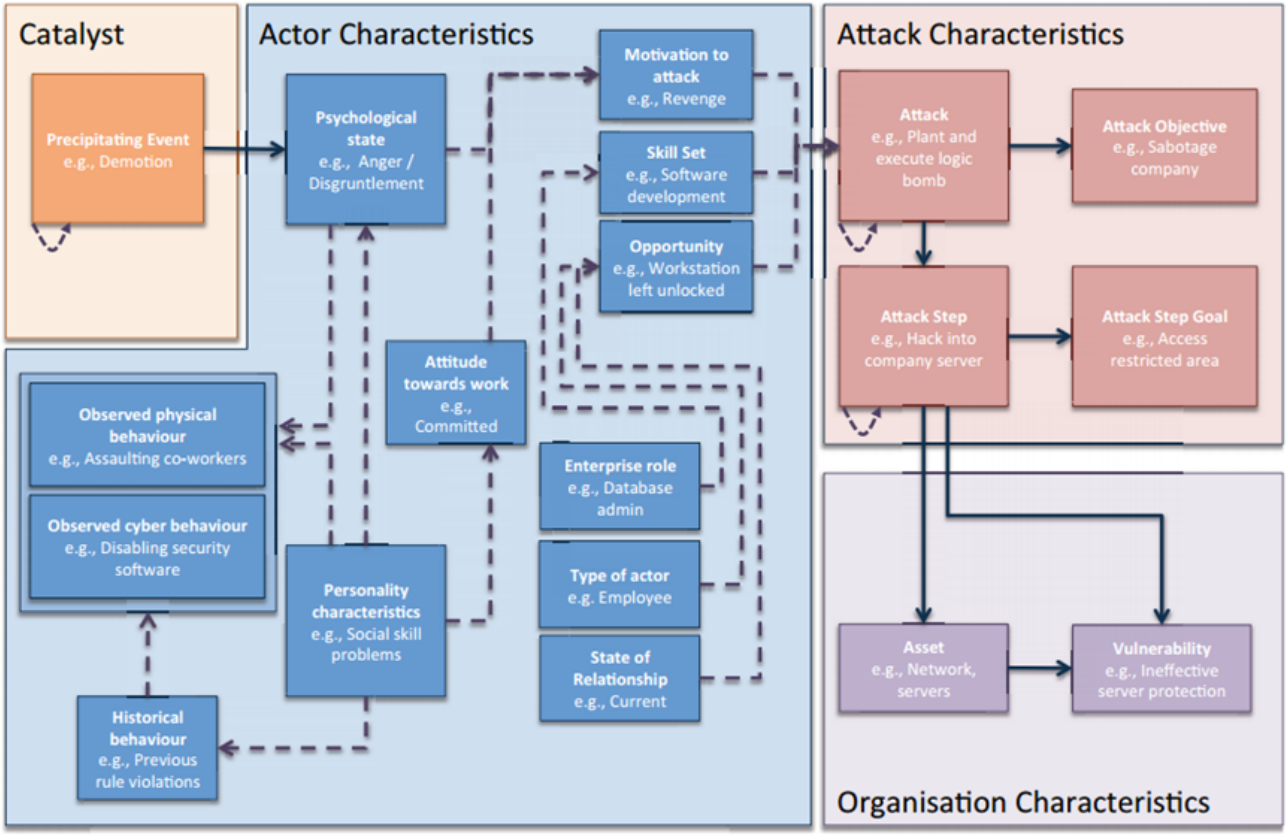
- the victim
- the motive
- the offender
- forensic evidence



PROFILING THE CYBERCRIMINAL

Models on profiling

The Framework for understanding Insider Threat (Nurse et al., 2014)



Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R. and Whitty, M., 2014, May. Understanding insider threat: A framework for characterising attacks. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 214-228). IEEE. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-understanding_insider_threat_framework.pdf

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

CASE SCENARIOS

DUPONT®

What is this? And what's it typically made of?

M. Mitchell – who is he? What did he do?

KOLON

These parties / items are at the centre of one of the largest cases of trade secret theft in history, worth around $900M…

CASE SCENARIOS

Traits / Social characteristics

M. Mitchell worked with DuPont for ~24 years, and was DuPont engineer and Kevlar marketing executive

Mitchell had been a model citizen with no criminal record

Became disgruntled and eventually fired for poor performance

Tech. skills

During his tenure, he copied numerous DuPont computer files containing sensitive and proprietary information to his home computer

Motive

Mitchell entered into lucrative consulting agreements with Kolon Industries, a DuPont competitor, and supplied them with the data (via email), resulting in millions of dollars in losses to DuPont

http://www.tradesecretsnoncompetelaw.com/2010/03/articles/trade-secrets-and-confidential-information/former-dupont-employee-sentenced-to-18-months-for-trade-secret-misappropriation/

http://www.richmond.com/news/article_27284dfe-d106-58b4-91f7-1812756b15cb.html

CASE SCENARIOS - PROFILE

Using Mitchell and others to template the insider cybercriminal that targets Intellectual Property (IP) Theft

PRESENTATION OUTLINE

- Cybercrime – the challenge
- Reflecting on current research & practice
- Profiling the cybercriminal
- Case scenarios
- Future research agenda

FUTURE RESEARCH AGENDA

How can law enforcement benefit from this?

- By understanding the cybercriminal profile law enforcement can better:
  - Develop strategies to combat criminal behaviour manifested online
  - Inform investigative methods

FUTURE RESEARCH AGENDA

- Further development and modelling of cybercriminal profiles
- Gathering more case and cybercriminal data to link types of cybercriminal profiles to types of cyber attacks (i.e., identify the patterns)

- We're open to your insight, ideas, and data(!) as well!

QUESTIONS?

Dr Jason R. C. Nurse

Cyber Security Centre,
Department of Computer Science
University of Oxford

Jason.Nurse [at] cs.ox.ac.uk

@jasonnurse

Dr Maria Bada

Global Cyber Security Capacity Centre,
University of Oxford

Maria.Bada [at] cs.ox.ac.uk

UNIVERSITY OF OXFORD

CYBER SECURITY OXFORD

Global Cyber Security Capacity Centre