Poster: Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement

Mariam Nouh*, Jason R.C. Nurse†, Helena Webb*, and Michael Goldsmith*
*Department of Computer Science, University of Oxford
{mariam.nouh, helena.webb, michael.goldsmith}@cs.ox.ac.uk
†School of Computing, University of Kent
j.r.c.nurse@kent.ac.uk

Title: Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement

Authors: Mariam Nouh, Jason R.C. Nurse, Helena Webb, and Michael Goldsmith

Venue: This poster is related to a paper to appear in Workshop on Usable Security (USEC 2019), co-located with the Network and Distributed System Security Symposium (NDSS) 2019, San Diego, California

Mariam Nouh, Jason R.C. Nurse, Helena Webb, and Michael Goldsmith. Cybercrime Investigators are Users Too! Understanding Outstanding Challenges Faced by Law Enforcement. Workshop on Usable Security (USEC 2019). Internet Society, San Diego, California, Feb 24, 2019. ISBN 1-891562-57-6 https://dx.doi.org/10.14722/usec.2019.23032 (To appear)

Abstract: Cybercrime investigators face numerous challenges when policing online crimes. Firstly, the methods and processes they use when dealing with traditional crimes do not necessarily apply in the cyber-world. Additionally, cyber criminals are usually technologically-aware and constantly adapting and developing new tools that allow them to stay ahead of law enforcement investigations. In order to provide adequate support for cybercrime investigators, there needs to be a better understanding of the challenges they face at both technical and sociotechnical levels. In this paper, we investigate this problem through an analysis of current practices and workflows of investigators. We use interviews with experts from government and private sectors who investigate cybercrimes as our main data gathering process. From an analysis of the collected data, we identify several outstanding challenges faced by investigators. These pertain to practical, technical, and social issues such as systems availability, usability, and in computer-supported collaborative work. Importantly, we use our findings to highlight research areas where user-centric workflows and tools are desirable. We also define a set of recommendations that can aid in providing a better foundation for future research in the field and allow more effective combating of cybercrimes.

Cybercrime Investigators are Users too!

Understanding the Socio-Technical Challenges Faced by Law Enforcement

Mariam Nouh[1*], Jason R.C. Nurse[2], Helena Webb[1], and Michael Goldsmith[1]
[1]Department of Computer Science, University of Oxford, UK
[2]School of Computing, University of Kent, UK
* mariam.nouh@cs.ox.ac.uk

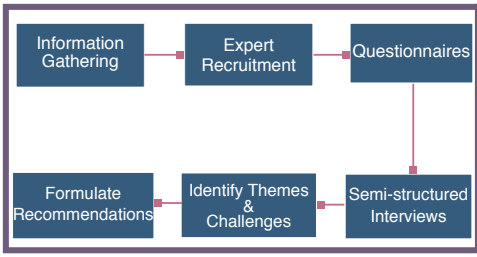
Motivation

- In 2018 the global cost of data breach increased
- Businesses lost an estimated £20BN from data breaches
- Typical methods used by law enforcement when investigating traditional crimes do not always easily apply to cybercrimes
- Current research primarily focuses on developing new solutions and tools that researchers believe are required by cybercrime investigators
- Little research focuses on understanding the actual needs and challenges faced by the investigators

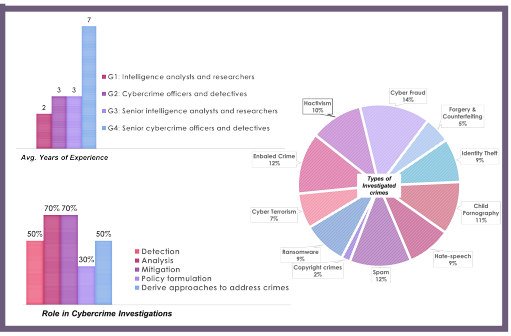
Aims & Objectives

- Study the current practices followed by law enforcement and cybercrime investigators
- Identify the general characteristics related to the investigation process of cybercrimes
- Identify socio-technical challenges currently faced, and areas where new technologies and processes are necessary
- Formulate recommendations for designing and building usable security tools and workflows to improve their day-to-day operations

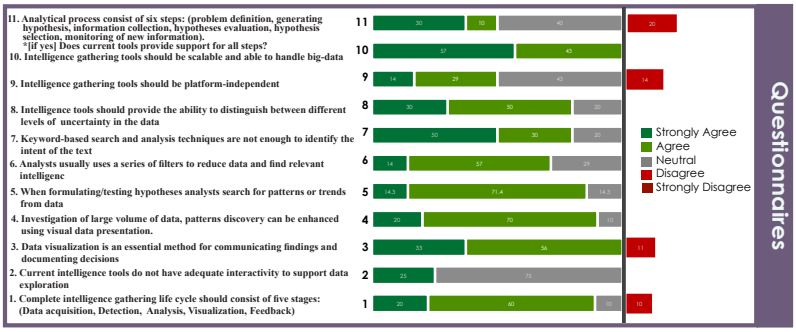
Methodology



Participants



Questionnaires



Themes

Theme 1: Investigation Process

Types of incidents and the process to evaluate them, including workflows and reactive and proactive tasks

Characterising details of investigation process to map the different steps performed and, identify where applicable, how each step can benefit from technology adoption

Theme 2: Collaboration within Investigators

Dynamics within the investigation team, team size, and roles played

Examining context and requirements for processes, systems or tools to support collaborative investigation sessions

Theme 3: Cybercrime Investigation Tools

The different tools currently being used by investigation teams including the advantages gained from using these tools

Understand the perceived usability, availability, and effectiveness of such tools at supporting the investigation tasks. The perceived limitations to be able to enhance them and give better support to investigators

Findings

Reporting of Cybercrimes

- Users face many ambiguities when recording the details of the reported cybercrimes using Action Fraud system
- Lack of structured method to collect the necessary cyber related information, which causes multiple implications on the investigation process
- Increased likelihood of misdirecting reports to the wrong department thus causing delays in addressing the crime and increases the time and effort needed to conduct the investigation
- The process is highly dependent on technical knowledge of the victim and the call-taker preparing the report

A major review of the questions included in the Action Fraud system is needed, and an evaluation of the usability and user experience of the online tool to identify the sources of ambiguity and areas for improvement.

Information Sharing

- UK police forces are decentralized, having a structure of separate 43 police forces may be fit for policing traditional crimes, but may not be the best structure for cybercrimes
- Each cybercrime unit become a silo, operating a different set of processes and tools and unable to interoperate
- Lack of centralised coordination of intelligence sharing between forces and agencies working on cybercrimes
- Intelligence reports produced may be incorrect as they do not have the big picture and are not aware of crimes reported in different regions
- Lack of communication between different local forces results in the missing of possible connections between reported cybercrimes

Better communication, coordination, and data sharing between different units and forces will have a positive effect on mitigating and responding to these crimes.

Technology

- Several budget cuts prevent forces from investing in upgrading the IT infrastructure and acquire advanced tools
- This limits their capabilities and has effects on the efficiency and quality of the conducted investigations
- Lack of a national mandate of tools and systems to be used in cybercrime investigations adds another challenge for collaboration between different cybercrime units.
- A significant portion of the investigation time is spent doing manual tasks that may be saved by automated or semi-automated tools
- Interoperation issues exist for the different tools used, where a lot of the investigation time is spent in manually modifying data to be accessable to different analytical tools

Tools should be designed with the human-in-the-loop concept in mind as investigators need to be able to understand how the tool is working, and how particular results were reached. This is critical to them as they need to be able to explain their findings in court.

References:
1. Mariam Nouh, Jason R. C. Nurse, Helena Webb, and Michael Goldsmith. Cybercrime Investigators are Users Too! Understanding Outstanding Challenges Faced by Law Enforcement. To appear in Workshop on Usable Security (USEC 2019). Internet Society, San Diego, California,Feb 24, 2019. ISBN 1-891562-57-6 https://dx.doi.org/10.14722/usec.2019.23032
2. M. Nouh, J. R. C. Nurse and M. Goldsmith, "Towards Designing a Multipurpose Cybercrime Intelligence Framework," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, pp. 60-67. doi: 10.1109/EISIC.2016.018
3. Lord Stevens. Policing for a better Britain: Report of the independent police commission, 2013
4. https://www.information-age.com/businesses-20bn-data-breaches-last-year-123470278/