

Cyber Security KTN

AI and Forensics Special Interest Group

Notes from workshop held 2nd April 2009

Summary of Discussion

1. AI techniques may be possibly used to 'Baseline the network'. To learn normal states as a basis of detecting abnormal states. Anomaly detection may occur at the level of network events or user behaviour. There was some discussion regarding the issues involved with learning from real-life data sets, including the difficulty of guaranteeing that a data set is fraud free
2. Commercial organisations only react when the “degree of pain, whether that be financial or impact on brand and reputation is significant to the business. In deciding upon projects therefore Ai/Forensic initiatives should be guided by that observation to solve a real problem.
3. There is a real requirement to develop capability at the Information Management and information presentation levels, There are many proprietary network sensors and systems, We don't need more (AI based or not). There may be a role for AI systems to work with existing AI tool-kits however (Encase, FTK, Autopsy, F-Response, FAIR for example) in order to organise, mine and present information to speed the forensic analysis task.
4. Rather than use AI to take “data to court”, which is difficult, maybe the role of AI systems is to undertake the monitoring and alerting process and to then pass this information onto Human Forensic investigators in a manner which expedites the whole process.
5. There is a relationship between AI/Forensics and Information Management and Information Security Systems (IMIS) This is an area where a suitable project may be identified. (See potential initiative 3)
6. Is there a role for AI/Forensics in the Enterprise compliance space, i.e. the aggregation and presentation of information to demonstrate ISO2799 Infosec. compliance (see potential initiative 2)

Potential Projects / initiatives

- Relationship between ISO standards (Ian Brynt) and CyberSec AI/For.
- The Knowledge repository as a way of building joint semantics and knowledge for the joint community
- Red flag” scenario exercise as a way to bring the AI forensic communities together

- IMIS / CyberSec AI/For relationship (Richard Overill KCL)

Session2 Presentation

Content

- Examine the scope of the extended forensic task
- Managing the complexity of the extended forensic task

Issues raised

- The extended forensic process could potentially address (and integrate) questions at the level of infrastructure, information/data, business & knowledge management systems and Social networks.
- How could the AI/ forensic process handle non-local data as evidence, e.g. distributed over a peer network, (issue raised, possible further discussion area)
- Could the AI/ forensic process handle transitory data (seems to be currently no)
- Could AI/Forensics take advantage of (or even influence) remote application and service protocols (issue raised, possible further discussion area)
- Could AI/Forensics take advantage of (or even influence) Digital Rights Management technologies. (issue raised, possible further discussion area)

Straw-man Projects

- DAPHNE – Aggregation and presentation of networked forensic evidence
- ForANTsics – Distributed analysis of the forensic task
- TREMS – Black Box Agents for tracing, revealing and evidence preserving strategies

Edited by Tim Parsons