To See or Not to See:
A Privacy Threat Model for Digital Forensics in Crime Investigation

Mario Raciti, Simone Di Mauro,
Dimitri Van Landuyt, Giampaolo Bella

ISDFS 2025

25/04/25 – Boston, MA

Serbian authorities using spyware to illegally surveil activists, report finds

Advanced mobile forensics products being used to illegally extract data from mobile devices, Amnesty finds

Amnesty International's report shows mobile forensic products from the Israeli firm Cellebrite are being used by police and intelligence services. Photograph: Issei Kato/Reuters

Police encouraged to use facial recognition on any investigation

Inspectorate recommends that no criminal investigation be closed until all available images have been checked against national database

IAN DAVIDSON/ALAMY

Police forces across Britain have been urged to use facial recognition technology in every criminal investigation.

RQ: *What are the privacy threats in a digital forensics crime investigation?*

Agenda

1. Introduction
2. **A Primer on SPADA**
3. **Application of SPADA in DFCI**
4. **A Privacy Threat Model for DFCI**
5. **Conclusions**

Agenda

1. Introduction
2. **A Primer on SPADA**
3. Application of SPADA in DFCI
4. A Privacy Threat Model for DFCI
5. Conclusions

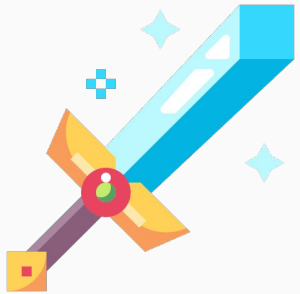
What is SPADA?

SPADA is a methodology for systematic threat elicitation.

Its acronym is composed of the **five variable elements** of threat modelling.

It incorporates both *domain-independent and domain-dependent* threat modelling.

SPADA focuses on completeness while avoiding redundancy and subjectivity.



The Variable Elements of Threat Modelling

The Steps in SPADA

Step 0 — Variable Setup: consists in the choice of the five variables as the initial source of information that is employed in the subsequent steps.

Step 1 — Domain-Independent Threat Elicitation: involves the collection of the threats that the analyst deems relevant.

Step 2 — Domain-Dependent Asset Collection: consists of the collection of a list of assets for the target domain from relevant sources.

Step 3 — Domain-Dependent Threat Elicitation: produces a list of domain-specific threats.

Agenda

1. Introduction
2. A Primer on SPADA
3. **Application of SPADA in DFCI**
4. A Privacy Threat Model for DFCI
5. Conclusions

Application in DFCI – Step 0

Soft and Hard Privacy

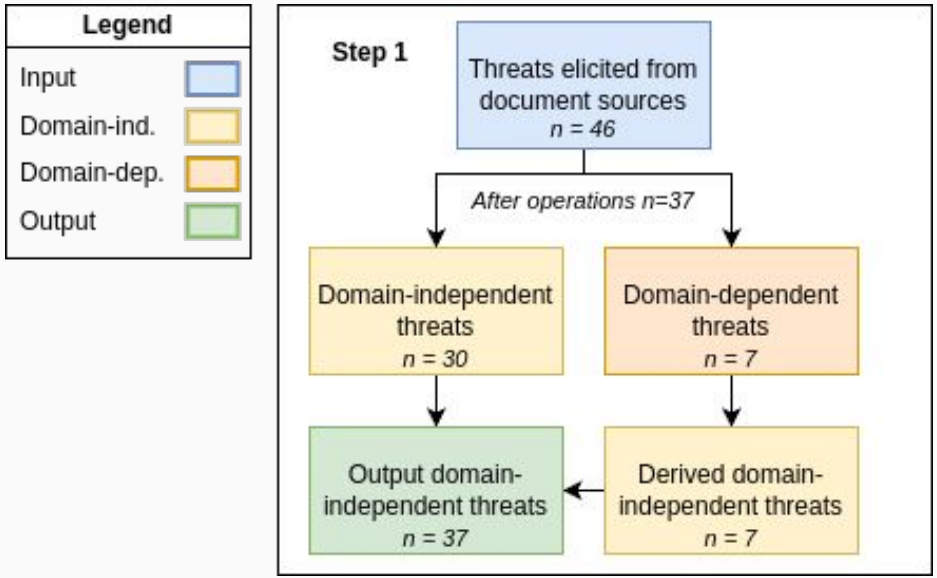
Domain-dependent: DFCI

Seyyar, Chaure, Rowe, Shaik, ISO, CoE DF, CoE EEG, IPOL, NIST, NIJ

Attacker, Data processor/controller, Third party

Abstract

Domain-Independent Threats – Step 1



Domain-Dependency Handling – Step 1

TABLE II: Derivation of domain-independent privacy threats from domain-dependent ones before refining the input list.

Source of doc.	Threat (Domain-Dependent) → Threat (Domain-Independent)
Seyyar et al. [10]	Data process/read for wrong case → Improper data processing or access Unauthorized person access to the big data forensic platform → Unauthorized person access to the big data platform Investigation report (paper documents) sent to wrong destination → Misdelivery of confidential document Access to data after case is closed → Access to data beyond retention period Authorizations not granted at case level → Insufficient access control mechanisms Errors while uploading seized digital material → Errors in data upload or ingestion
Chaure et al. [8]	Erroneous allegations due to deleted files → Erroneous allegations due to deleted files
Rowe [11]	Unwarranted reporting of forensic findings → Unwarranted reporting of findings Surreptitious searches → Covert or unlawful data searches Selling of private forensic data → Illicit sale of private data Criminal use of digital forensics → Malicious misuse of practice Lack of support for privacy management by forensic tool vendors → Lack of support for privacy management by software vendors

Asset Collection – Step 2

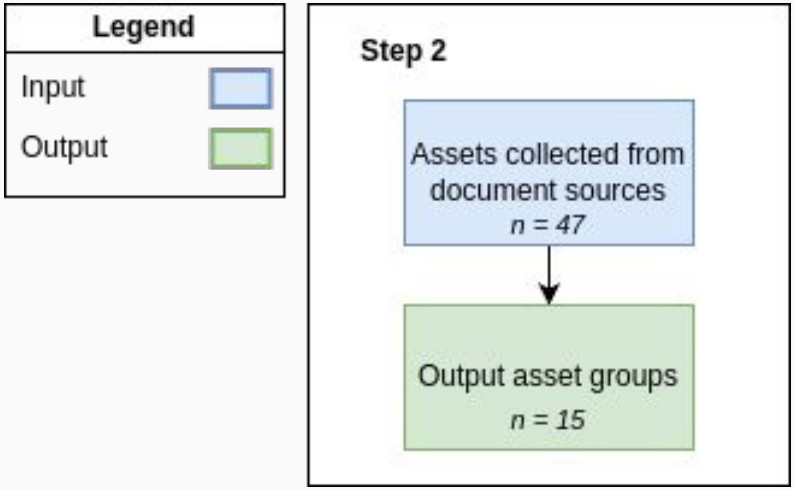
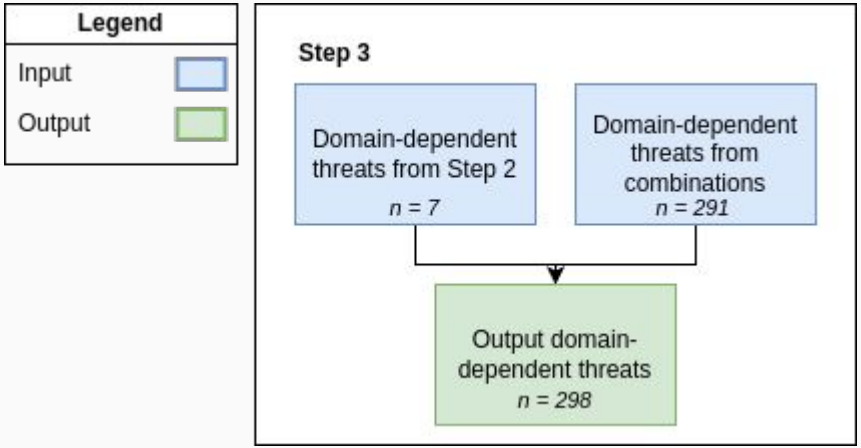


TABLE III: Assets collected in Step 2.

Source of Documentation	Asset
ISO	Storage media
CoE DF, IPOL	Cloud and remote storage
CoE DF	Email and messaging
CoE DF	Communication and network logs
CoE DF	Authentication and access logs
CoE DF, NIST	Forensic tools and equipment
CoE DF, NIJ	Case management databases
CoE DF	Secure forensic workstations
CoE DF	Forensic lab
CoE EEG	Desktop devices
CoE EEG	Mobile devices
CoE EEG	IoT devices
CoE EEG	Location and tracking data
CoE EEG	Cryptocurrency data
IPOL	System and application logs

Domain-Dependent Threats – Step 3



Threat (Domain-Dependent)
Errors while uploading seized digital material
Selling of private forensic data

+

Threat (Domain-Independent)	Asset(s)
Poor training	All assets
Cross-border data privacy concerns	Cloud and remote storage, Email and messaging, Case management databases, Location and tracking data

Agenda

1. Introduction
2. A Primer on SPADA
3. Application of SPADA in DFCI
4. **A Privacy Threat Model for DFCI**
5. Conclusions

TABLE IV: Extract of the privacy threat model for DFCI.

Threat (Domain-Independent)	**Asset(s)**	**Threat Agent(s)**
Poor training	All assets	Data Controller, Third Party
Cross-border data privacy concerns	Cloud and remote storage, Email and messaging, Case management databases, Location and tracking data	Data Controller, Data Processor, Third Party
Lack of privacy management	Forensic tools and equipment, Secure forensic workstations, Case management databases	Data Controller, Data Processor, Third Party
Threat (Domain-Dependent)		**Threat Agent(s)**
Errors while uploading seized digital material		Data Processor, Third Party
Selling of private forensic data		Attacker, Data Controller, Data Processor, Third Party

Partial Validation

Serbian authorities using spyware to illegally surveil activists, report finds

Advanced mobile forensics products being used to illegally extract data from mobile devices, Amnesty finds

Amnesty International's report shows mobile forensic products from the Israeli firm Cellebrite are being used by police and intelligence services. Photograph: Issei Kato/Reuters

Matching threat:

Surreptitious searches

Limitations

Subjectivity not completely solved *(e.g., how to embrace two threats?)* → partially mitigated by applying the *TEAM 3* algorithm.

Variability of privacy laws across jurisdictions → e.g., a threat might be legally accepted.

Real-world constraints may limit the feasibility of implementing certain privacy controls → e.g., time-pressure and resource scarcity.

Agenda

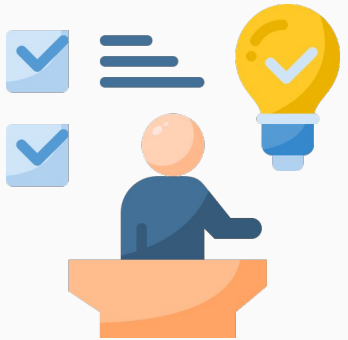
1. Introduction
2. A Primer on SPADA
3. Application of SPADA in DFCI
4. A Privacy Threat Model for DFCI
5. **Conclusions**

Conclusions

We demonstrated how **SPADA** assists in handling **domain-dependency** during threat elicitation.

We advanced a *Privacy Threat Model for DFCI* to:

- **Support forensic investigators** in **mitigating privacy risks** while preserving the evidentiary integrity of forensic processes;
- **Raise awareness** among legal professionals and defendants regarding **potential privacy violations** within forensic investigations.



Future work:

- Ranking threats by likelihood and impact.
- Further automate SPADA (e.g., NLP and LLMs).
- Continue formalisation of DFCI (e.g., anti-forensics and cysec threats).

References

GitHub repository with results.
https://github.com/tsumarios/Threat-Modelling-Research/tree/main/ISDFS25

Raciti, M., Bella, G. The SPADA methodology for threat modelling. *Int. J. Inf. Secur.* 24, 86 (2025). https://doi.org/10.1007/s10207-025-00999-0

Thanks for your attention!

For more information or questions:

mario.raciti@imtlucca.it – mario.raciti@phd.unict.it

https://tsumarios.github.io/

@tsumarios

https://linkedin.com/in/marioraciti

Non-malicious QR (maybe)