From the Computer Incident Taxonomy to a Computer Forensic Examination

Stefan Kiltz[1], Robert Altschaffel[2], Jana Dittmann[1]

[1]Otto-von-Guericke-University Magdeburg
Faculty of Computer Science
Research Group on Multimedia and Security

[2]Otto-von-Guericke-University Magdeburg
Faculty of Computer Science

Acknowledgement: we thank Mr. Carsten Schulz of the Federal Office for Information Security (BSI) for the kind support

Outline

- Motivation
- Basics
  - Our forensic model
  - CERT Taxonomy
- Forensic Examination Taxonomy (FET)
- Examples for using the Forensic Examination Taxonomy
  - Malicious activity
  - Non-malicious occurrences
- Conclusion

Motivation

- Taxonomy - Need for a common language to describe certain matters, sometimes inter-disciplinary (mutually exclusive, exhaustive, unambiguous, repeatable, accepted)
- Widely known CERT-Taxonomy describes a common language for malicious incidents
- Need for a Forensic Examination Taxonomy (FET) to find a common language for computer forensic examinations
- Could be used as a framework for the final report of a forensic examination

Motivation

- Our aim: To extend the application of forensic measures whilst retaining the strict demands placed on IT-forensic investigations, e.g. non-alteration of evidence, comprehensive documentation
- Advantage is the inclusion of *strategic preparation*, i.e. the placement of measures to enhance results of investigations ahead of an incident
- Leads to the following definition:

  IT-forensics is the strict methodological data analysis on storage devices and in IT-networks for the purpose of solving incidents employing the opportunities of strategic preparation from the viewpoint of the operator of an IT-system.

Motivation

- IT-forensics according to our view is centred around five questions about an incident:
  - What has happened / is happening?
  - Where has it happened / is it happening?
  - When did it happen?
  - Which way did it happen?
  - What was / is the cause?
- FET can be an aid to ensure all questions had been addressed

Motivation

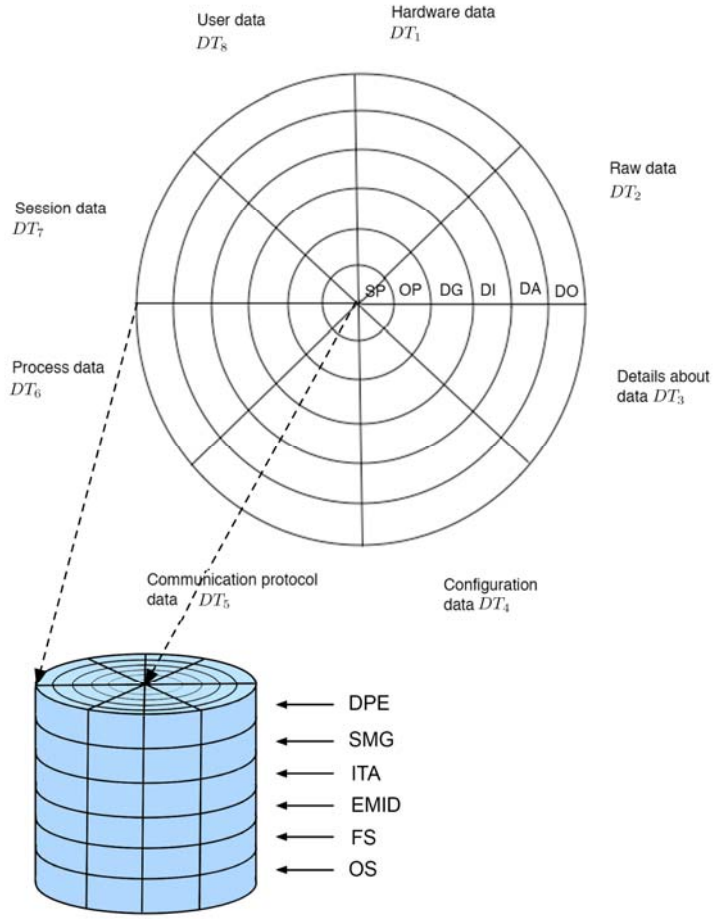
- CERT taxonomy was used as a starting point
- Forensic examinations according to our viewpoint differ in that:
  - Not all incidents are malicious i.e. they are support cases
  - A forensic examination follows a timeline starting with a result, i.e. the symptom
- We use a self-developed model of the forensic process to comprehensively cover all aspects of the investigation

Basics - Our forensic model

- Separated into *Phases*, *Classes of methods*, *Forensic data types*
- *Phases* (mutual exclusive) are used to model sequence details during a forensic investigation, not a new approach (see [Fre07]) but novel phase of strategic preparation is included, being beneficial for the operator of an IT-system conducting a forensic investigation
- *Classes of methods* (mutual exclusive) classify forensic capabilities of software (e.g. a database application), not only dedicated forensic suites gather forensically relevant data - ensures independence from particular software solutions
- *Forensic datatypes*, a layered approach similar to ISO/OSI model (not mutual exclusive), used to determine input and output data of forensic tools/methods, describe the forensically relevant data as a data source

[Fre07] F. Freiling, A Common Process Model for Incident Response and Digital Forensics, Proceedings of the IMF2007, 2007

Our forensic model (cont'd)



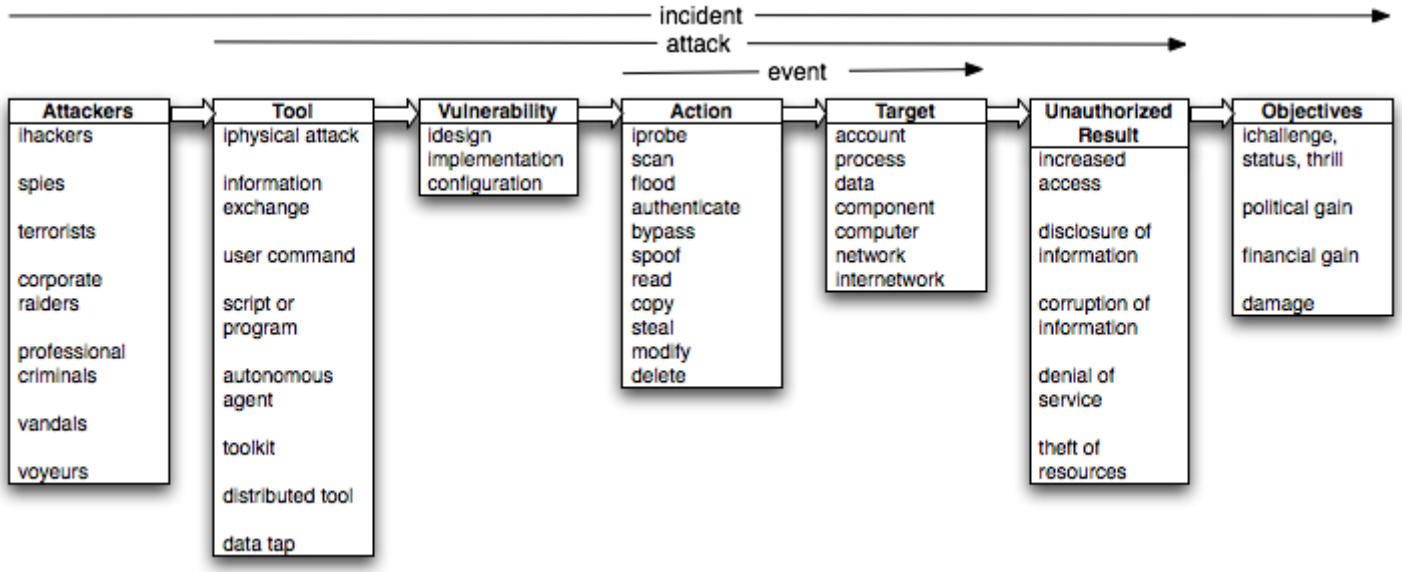
- Phases :
  - Strategic preparation (*SP*)
  - Operational preparation (*OP*)
  - Data gathering (*DG*)
  - Data investigation (*DI*)
  - Documentation *(DO)*

- Classes of methods:
  - Operating system (*OS*)
  - File system *(FS)*
  - Explixit means of Intrusion detection *(EMID)*
  - IT application (*ITA*)
  - Scaling methods for evidence gathering *(SG)*
  - Data Processing and Evaluation (*DPE*)

Our forensic model (cont'd)

- Forensic datatypes:
  - Hardware data (DT_1)
  - Raw data (DT_2)
  - Details about data (DT_3)
  - Configuration data (DT_4)
  - Communication protocol data (DT_5)
  - Process data (DT_6)
  - Session data (DT_7)
  - User data (DT_8)

Basics - CERT Taxonomy



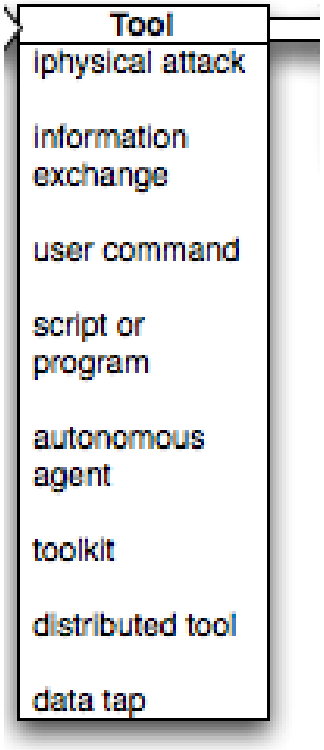
Taken from : J. D. Howard and T. A. Longstaff, “A common language for computer security incidents (sand98-8667),” Sandia National Laboratories, Tech. Rep. ISBN 0-201-63346-9, 1998.

Attackers

- Renamed category as Origin
- Added Malfunctioning Hardware and Malfunctioning Software
- Added Lack of Resources
- Grouped all user-based incidents as User
- The category is both exhaustive and mutually exclusive

Tool

- Changed physical attack to physical damage to also address non-malicious incidents
- User command and script or program also cover non-malicious activities
- Added Information exchange to address social engineering
- The category is both exhaustive and mutually exclusive
- Problems arise with the granularity of the items



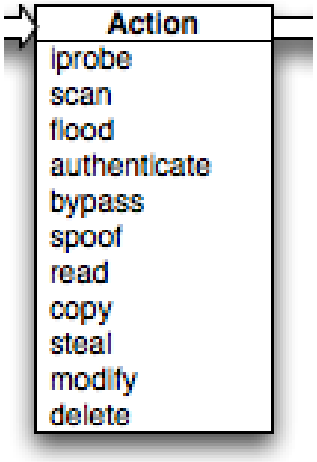
Vulnerability

- Added human behaviour to include non-technical means of unauthorised access and modification
- information gathering such as social engineering
- No need for an item such as hardware erosion, boils down to design, implementation or configuration vulnerabilities
- The category is both exhaustive and mutually exclusive

Action

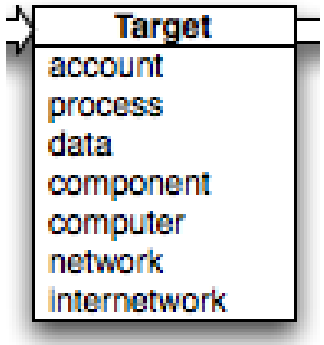
- FET covers also for non-malicious incidents
- Added disable to address hardware and software failures

  to ensure completeness
- Necessary because modification would render the category non-mutual exclusive



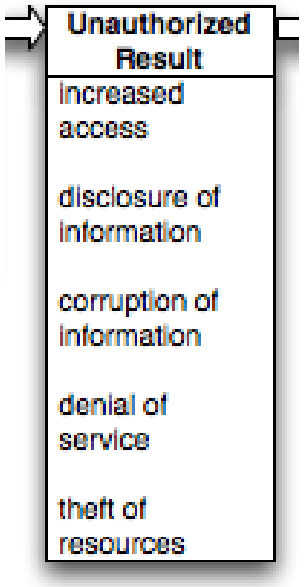
Target

- Account and data from the CERT taxonomy were not considered mutual exclusive
- Partly used the forensic data types to model targets
- Added Process
- Added User Data, Configuration Data and Session Data
- Kept Component, Computer, Network and Internetwork



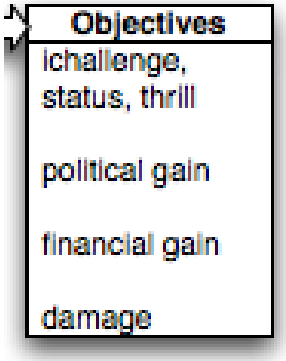
Result

- Added the Security Aspects as another category
- Integrity, Authenticity, Confidentiality, Non-Repudiation, Availability
- Remaining problem: non-malicious incidents cannot be always described using security aspects, although some security aspects share a similarity with safety aspects (e.g. Integrity)



Objective

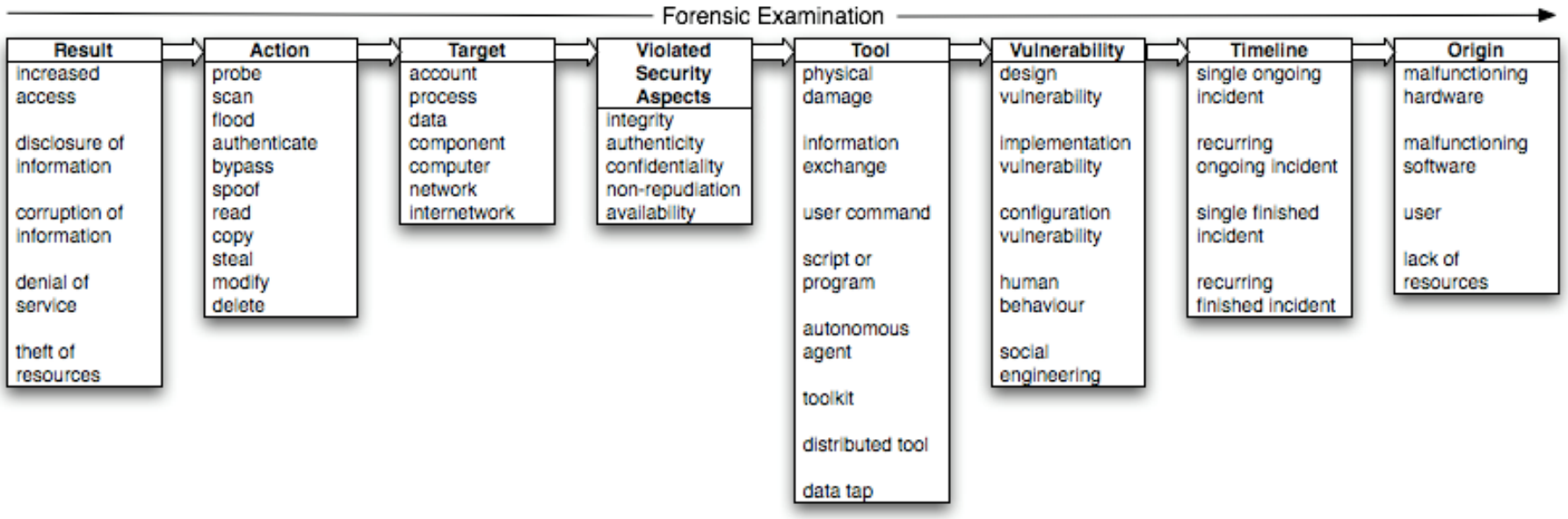
- It is not the task of the examiner to judge intensions of malicious attackers
- Also, with data from an IT-system alone it is impossible to tie evidence to a particular individual let alone an objective
- So this category is dropped in the FET



Timeline

- New category not present in the original CERT Taxonomy
- Added to reflect a very important aspect of forensic investigations - time
- Separated into:
  - single finished incident
  - recurring finished incident
  - single ongoing incident
  - recurring ongoing incident

Forensic Examination



Examples - malicious activity

- Scenario: unknown perl scripts executed on a webserver on a linux-based system noticed by an unavailable website -> result
- Position and MAC times of the script and logfiles of the webserver were investigated
- Attacker modified the system behaviour by providing an external configuration file

Result	Action	Target	Violated Security Aspects	Tool	Vulnerability	Timeline	Origin
theft of resources	modify	computer	availability	user command	configuration vulnerability	single finished incident	user

Examples - non-malicious

- Scenario: A linux-based system is rendered unusable through lack of main memory
- Logfiles show increased amount of visitors beyond the capacity of the system
- Configuration vulnerability in allowing the webserver to spawn more processes than the system could handle
- System needed to be shut down, with that the incident was finished

Result	Action	Target	Violated Security Aspects	Tool	Vulnerability	Timeline	Origin
denial of service	flood	computer	availability	script or program	configuration vulnerability	single finished incident	lack of resources

Conclusion

- We showed the need for a Forensic Examination Taxonomy to aid in assuring the comprehensiveness of an investigation
- Non-malicious activity was added to open forensic investigations to the field of support cases whilst retaining the strict methodological principles of criminal investigations
- We showed how the CERT taxonomy could be adapted to fulfil the requirements of forensic examinations
- Categories had to be altered, removed and added as well as the sequence thereof to incorporate the forensic proceedings
- Further research necessary esp. in the granularity of the items in the categories
- Exhaustiveness is a big problem, FET needs to be updated constantly

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG FAKULTÄT FÜR INFORMATIK

AMSL Advanced Multimedia and Security Lab

Thank you for your attention!