Evidential Notions of Defensibility and Admissibility with Property Preservation

Raphael Phan, Ahmad R. Amran, John N. Whitley, David J. Parish

Evidential Notions of Defensibility and Admissibility; with Property Preservation

Raphael C.-W. Phan, Ahmad R. Amran, John N. Whitley, and David J. Parish

Loughborough University
within the High Speed Networks (HSN) Lab
of the Electronic and Electrical Engineering department
LE11 3TU, UK
{r.phan, a.r.amran, j.n.whitley, d.j.parish}@lboro.ac.uk

Abstract. For security-emphasizing fields that deal with evidential data acquisition, processing, communication, storage and presentation, for instance network forensics, border security and enforcement surveillance, ultimately the outcome is not the technical output but rather physical prosecutions in court (e.g. of hackers, terrorists, law offenders) or counter-attack measures against the malicious adversaries.
The aim of this paper is to motivate the research direction of formally linking these technical fields with the legal field. Notably, deriving technical representations of evidential data such that they are useful as evidences in court; while aiming that the legal parties understand the technical representations in better light. More precisely, we design the security notions of evidence processing and acquisition, guided by the evidential requirements from the legal perspective; and discuss example relations to forensics investigations.

1 Motivation

For the security fields that involve evidential data acquisition (e.g. monitoring or surveillance), processing, communication, storage and presentation (or reconstruction), such as network forensics [6, 9], border security and enforcement surveillance, the ultimate outcome is not so much the technical output but rather the physical prosecutions in court (e.g. of hackers, terrorists, law offenders) or counter-attack measures [10] against the adversaries behind malicious attacks.

This paper motivates the research direction of formally linking the above-mentioned technical fields with the legal field. The approach we suggest is to design the relevant security notions and the technical methods of evidence processing and construction [7] guided by the evidential requirements from the legal perspective.

2 Directions

In more detail, we advocate the need to treat the following particular research directions, all of which are open problems to date.

- Formal definitions [12] of evidential notions: we classify evidential usefulness in terms of how usable it is as the evidence (define this as *admissibility*) and whether the processes applied to the evidence from crime scene to court are legally appropriate (define this as *defensibility*). Doing so provides the framework to guide the design of technical evidential collection and construction, as well as gives a sound mapping between the technical and legal fields so to avoid ambiguity during the transition from one field to another and/or throughout the life cycle of the evidence. This is crucial as defensibility requirements dictate that continuity of evidence be ensured from crime scene (or observed event) through to court room.
- Design of property-preserving processes for evidential data e.g. acquisition, duplication, storage, reconstruction: it is important that the evidence have continuity [14] from crime scene to court. Therefore, as the evidence is processed along the way, there is a need to ensure that the processes preserve the evidentiary properties [8] of the evidence such as provenance [14], integrity and admissibility.
- Design of abstract evidential data constructs satisfying legal admissibility requirements.

In this paper, we treat the first research direction. The last two directions are our on-going research.

3 Notions

We first define the primitive security properties desired for evidential data. We then define our main evidential notions, namely defensibility (dealing with the validity of the *process*) and admissibility (dealing with the validity of the *final evidence* presented to court).

3.1 Primitive Properties

Integrity, (source) authentication and linkability are the underlying properties that form the base of wider notions including defensibility and admissibility.

Integrity and Source Authentication. The integrity property and source authentication property of some evidential data can be based on cryptographic notions of integrity e.g. INT [1], and unforgeabiilty (UF) [4].

Linkability. Let $w(E^S, ID)$ denote a function that evaluates the weight of evidence E^S at state S of the evidence life cycle with respect to how much it links to a particular individual of identity ID. An evidence E^S is said to be *linkable* (LNK) to a particular person of identity ID if the weight of the evidence $w(E^S, ID) > \varepsilon$ for some negligible ε.

3.2 Defensibility

This notion can be defined to include the preservation of the properties of integrity, data provenance (a.k.a. chain of custody) and relevance (in terms of necessity, and linkability to the suspect and to the crime or event).

Property Preservation. The gist of the notion of property preservation (PPr) relates to the state of the evidential data E still retaining a particular property P even after undergoing a function $f(\cdot)$.

Let $f(\cdot)$ denote a function $\in \{\texttt{acquisition}, \texttt{processing}, \texttt{storage}, \texttt{communication}, \texttt{presentation}, \texttt{reconstruction}\}$ operating on some evidence E^S at state S. See Fig. 1.

If E^S exhibits a property P, denoted as $\Pr[E^S \mapsto \mathsf{P}] > \varepsilon$ for some negligible ε, then $f(\cdot)$ is said to be property-preserving in the sense of P if $f(E^S)$ also exhibits property P, i.e. $\Pr[f(E^S) \mapsto \mathsf{P}] > \varepsilon$.

Define an adversarial game where adversary A interacts with a forensics challenger and is allowed oracle access to any $f(\cdot) \in \{\texttt{acquisition}, \texttt{processing}, \texttt{storage}, \texttt{communication}, \texttt{presentation}, \texttt{reconstruction}\}$. Furthermore, A is given samples of some evidence E^S exhibiting property P. The game ends when A outputs an evidence $\tilde{E}^S$.

Define A's advantage in winning the game as

$$\begin{aligned}\mathsf{Adv}_A^{\mathsf{PPr}} = ((\Pr[E^S \mapsto \mathsf{P}] > \varepsilon) \wedge (\Pr[f(E^S) \mapsto \mathsf{P}] < \varepsilon)) \vee \\ ((\Pr[E^S \mapsto \mathsf{P}] < \varepsilon) \wedge (\Pr[f(E^S) \mapsto \mathsf{P}] > \varepsilon)).\end{aligned}$$

A function is property-preserving in the sense of P if $\mathsf{Adv}_A^{\mathsf{PPr}} < \varepsilon$.

The adversarial winning condition here captures the case where a function $f(\cdot)$ negates the existence of an evidence E's property P.

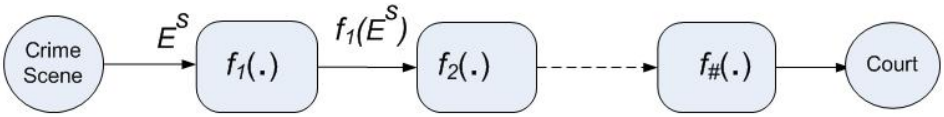

Fig. 1. Evidential data going through multiple processes from crime scene to court.

Provenance. This requires the integrity maintenance of custody information i.e. information about which party is responsible (holds the custody) over the evidence, at each state of the process from crime (or event) scene to court.

Relevance. For the relevance notion, we emphasize that besides capturing how the necessary evidential data are acquired and processed, as well as including linkability, the notion should also capture the assurance that non-necessary data is not represented e.g. private data that will intrude the privacy of non-involved passers-by who just happen to be there. This is an interesting open problem, since for instance current enforcement monitoring systems such as CCTVs and border security controls do not formally assure privacy preservation and this notion of relevance.

3.3 Admissibility

This notion emphasizes on the verification of the final evidence in terms of its integrity, provenance and relevance. Herein, adversarial games can be defined for each of the properties. While integrity will be more straightforward, the provenance property should include a measure of the evidential data origin including source (e.g. IP address for network forensics, or identification details of the suspect) and event/crime location details, whereas the relevance property is as discussed above in subsection 3.2.

4 Exemplification

To be more illustrative, we present some brief instances to exemplify the applicability of Section 3's notions in network forensics.

4.1 Integrity and Linkability

Consider an instance of telecommunications service in an organisation, telephone calls taking place on or through corporate switchboards (PABXs).

Such switchboards routinely provide data about the numbers called and the time and duration of calls. They do so as a means to monitor costs for outgoing calls and to check on service quality with respect to internal calls. The logs produced can be of considerable value in many kinds of investigations. Some businesses routinely record phone calls as a check against disputed transactions, or to see whether their employees are misbehaving (misuse, corporate sabotage, terrorism etc).

In a forensic situation, the immediate and important issue is to be able to demonstrate that the logs and/or recordings are reliable and have not been tampered with. It is helpful to be able to say something about the specific PABX and what logging facilities exist. There should be some statements about how they were collected, by whom, what precautions were taken, and how selections of data were made. The data should also be subjected to some form of integrity check, as a guard against post-capture tampering and forgery. They can specifically be linked to alleged individuals and circumstances. Thus, any evidential data will be considered for weight of fact with respect to its persuasiveness and probative value.

4.2 Provenance, Weight of Evidence and Property Preservation

In any type of investigation, the forensics challenger must follow an investigation process. That process begins with the step of assessing the case and documenting them in an effort to identify the crime and the location of the evidence. An evidence's chain of custody (data provenance) must be prepared to know who handled the evidence, and every step taken by the forensic investigator must be documented for inclusion in the final report.

Sometimes a computer and its related evidence can determine the chain of events leading to a crime for the investigator as well as provide the evidence which can lead to conviction. For instance, in a network attack instance; each adversary could have his own unique motives, methods and skills. He begins with little or no information about the target. However, depending on his skills, he might be able to construct a detailed roadmap that may enable the adversary to compromise the target. The adversary's approach generally covers several of these seven steps (or all of them based on their motives, methods and skills): 1) Perform a footprint analysis e.g., IP address, domain name, location, subsidiaries etc; 2) Enumerate information e.g., type and version of OS, ftp, mail and services running etc; 3) Attack the network and penetrate systems that

have high vulnerabilities e.g., knowledge gained from published Common Vulnerability and Exposure (CVEs); 4) Escalate privileges to have access control e.g., social engineering and/or brute force; 5) Raid information and user records; 6) Install backdoor to circumvent trusted programs; 7) Leverage the compromised system. Any evidential data of any of these or more would cause a certain degree of severity to the damage done, and this relates to the weight of evidence.

Finding the evidence, discovering relevant data, eradicating external avenues of alteration, gathering the evidence, and preparing a chain of custody are processes where evidential properties need to be preserved through to court. A forensics challenger must ensure that evidential data still exhibits a particular property (e.g. integrity) from when they are first gathered and seized at the crime scene, through the processes of the chain of custody preparation, evidence transportation to and/or storage at forensics labs, to ultimately the court room.

5 Remarks

Defensibility methods could be designed as essentially protocols that have underlying security mechanisms for integrity checking (e.g. message authentication codes or hashes keyed by secrets), source authentication (e.g. digital signatures) and traceability. Parties are used to model the interaction from one intermediary spatial point or representative form to another during the course of the evidence from crime scene through to court.

Admissible methods could be designed as mechanisms rather than protocols as they do not involve interaction among parties but rather apply to the evidential properties of the final evidence.

Having explicit and non-ambiguous notions and processes allow the proper mapping from technical evidence processing of monitored scene through to legal courts and enforcement, and this will lead to effective evidential systems where the processing of evidential data is non-wasteful and fit for purpose.

References

1. M. Bellare and C. Namprempre, "Authentication Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," Advances in Cryptology - Asiacrypt '00, LNCS, vol. 1976, 2000, pp. 531-545.
2. M.A. Caloyannides, "Forensics is so 'Yesterday'," IEEE Security and Privacy, vol. 7, no. 2, 2009, pp. 18-25.
3. B.D. Carrier, "Digital Forensics Works," IEEE Security and Privacy, vol. 7, no. 2, 2009, pp. 26-29.

4. S. Goldwasser, S. Micali and R. Rivest, "A Digital Signature Scheme Secure against Adaptive Chosen-Message Attacks," SIAM Journal on Computing, vol. 17, no. 2, 1988, pp. 281-308.
5. A.J. Kearsley, "Electronic Document Management: Legal Admissibility of Evidence Held in Digital Form," Computer Law & Security Report, vol. 15, no. 3, 1999, pp. 185-187.
6. E.E. Kenneally, "Digital Logs - Proof Matters," Digital Investigation, vol. 1, 2004, pp. 94-101.
7. E.E. Kenneally and C.L.T. Brown, "Risk Sensitive Digital Evidence Collection," Digital Investigation, vol. 2, 2005, pp. 101-119.
8. S. Mocas, "Building Theoretical Underpinnings for Digital Forensics Research," Digital Investigation, vol. 1, 2004, pp. 61-68.
9. B.J. Nikkel, "Improving Evidence Acquisition from Live Network Sources," Digital Investigation, vol. 3, 2006, pp. 89-96.
10. R.C.-W. Phan, J.N. Whitley and D.J. Parish, "Adversarial Security: Getting to the Root of the Problem," Proc. iNetSec '10, to appear.
11. C. Reed, "The Admissibility and Authentication of Computer Evidence - a Confusion of Issues," Computer Law & Security Report, vol. 6, no. 2, 1990, pp. 13-16.
12. P. Rogaway, "Practice-Oriented Provable Security and the Social Construction of Cryptography," Eurocrypt '09, invited talk, May 6, 2009.
13. M. Solon and P. Harper, "Preparing Evidence for Court," Digital Investigation, vol. 1, 2004, pp. 279-283.
14. P. Turner, "Digital Provenance - Interpretation, Verification and Corroboration," Digital Investigation, vol. 2, 2005, pp. 45-49.