Chapter 1

SCENARIOS FOR RELIABLE AND SECURE DIGITAL EVIDENCE

Nicolai Kuntze, Carsten Rudolph, Thomas Kemmerich, Barbara Endicott-Popovsky

Abstract A notion for secure digital evidence and a technical solution with hardware-based security in devices producing digital evidence was proposed in 2012. This paper revises that proposal and discusses three distinct scenarios where forensic readiness of devices and secure digital evidence are relevant. It is shown, how the different requirements of the three scenarios can be realized using a hardware-based solution. The scenarios are: lawful interception of voice communication, automotive black box, precise farming. These three scenarios come from very distinguished application domains. Nevertheless, they share a common set of security requirements for processes to be documented and data records to be stored.

Keywords: Secure digital evidence, admissibility, forensic readiness, lawful interception, automotive black box, precise farming

1. Introduction

Traditional approaches to digital forensics [21] are concerned with the reconstruction of events within digital systems that often are not built for the creation of evidence. However, many scenarios exist where devices are built that produce digital data records for which admissibility is relevant [4]. Technological solutions exist to use hardware-based security to bind digital records to a particular state of a device. A notion of secure digital evidence and a generic process to set-up and deploy such a solution was previously described by the authors [7, 13, 14]. The next step in the work is to discuss the applicability and relevance of the topic of secure digital evidence in the context of concrete, practical scenarios. Further, the legal implications of possible attacks on digital scenarios

needs to be discussed and the suitability of the proposed notion of digital evidence needs to be evaluated. Finally, the possibility of efficient and economic realization needs to be assessed.

2. Secure Digital Evidence

This section briefly recapitulates the notion of secure digital evidence and the technical solution previously proposed by the authors [13].

2.1 A notion of Secure Digital Evidence

A data record can be considered secure if it was created authentically by a device for which the following holds:

- The device is physically protected to ensure at least tamperproof-evidence. The data record is securely bound to the identity and status of the device (including running software and configuration) and to all other relevant parameters (such as time, temperature, location, users involved, etc.[1])
- The data record has not been changed after creation.

Digital Evidence according to this definition comprises the measured value (e.g. a photo and speed measurement [19]) and additional information on the state of the measurement device. This additional information on the state of the measurement device aims to document the operational environment providing evidence that can help lay the foundation for admissibility.

2.2 A possible solution to generate Secure Digital Evidence

The content and format of data records produced on a device will depend on various factors, such as the hardware design of the device, software running on the device, and the configuration implemented. Further, once a digital data record is produced, integrity, confidentiality and authenticity must be ensured by some mitigating control such as the use of secure cryptographic algorithms for encryption and digital signatures (similar requirements are also applicable for long term archiving [25]. Also, solutions for secure long-term archiving must be considered.

The proposed solution is based on a device that is produced and configured in a way that results in admissible evidence which is correct and

[1]The actual set of parameters and the protection levels depend on the scenarios and on the type of data record

reliable as long as the device is not physically manipulated or corrupted. Various types of attacks need to be considered for such a device. Attacks include attacks on communication channels, attacks via various physical interfaces (e.g. USB [3]), or attacks exploiting weaknesses of software running on the device. If the goal is to manipulate digital data before it is protected by a digital signature, attacks need to change software or configurations on the device in order to change the actual creation of the data records. Thus, one possible technical solution is to use a so-called Trusted Platform Module [16] to bind data records to the status of the device at the time of creation of the data record. This status can include all executable software started on the device since last reboot, configuration parameters, other parameters on the device's environment such as location or temperature.

In order to support forensic readiness [8,17] of the device, the hardware-based solution needs to be embedded in a process establishing all necessary information in order to confirm admissibility later. These steps can be summarized as follows:

1 Produce hardware security anchor (e.g. TPM): The hardware security anchor must be produced at a high security level.

2 Certify hardware security anchor: Security properties of the hardware security anchor should be documented in a security certificate with an appropriate security level.

3 Certify platform: In addition to the single security chip, the means of its integration into the platform and the properties of the root of trust for measurement are relevant and should be verified and certified.

4 Produce software: Relevant infrastructure software such as operating system, drivers, and application are produced and validated.

5 Installation, initialization and certification of software: It must be ensured, that software installation and initialization has occurred properly, has not been manipulated, and that security certification does indeed cover all relevant aspects.

6 Define location, valid temperature, etc.: Certify reference measurement values for calibrated devices.

7 Generate and certify signing keys: Since the scheme described above relies heavily on cryptography, and therefore on secure generation, distribution and storage of keys, these processes require

verification and certification. Because of the range of possible use cases, it is difficult to find and recommend one single algorithm.

8 Define location, valid temperature, etc.: Parameter ranges for correct use of the system must be established and then, either the occurrence of lower or higher temperatures prevented, or the infrastructure design changed to avoid problems. As an example, perhaps temperature control could be included in the device in order to satisfy temperature requirements.

9 Installation of device: The installation and initialization process is critical as this is the phase where keys can be generated and exchanged.

10 Establish communication with server: The establishment of client server communication is in principle well-understood; however, there is no efficient solution currently for binding SSL keys to underlying attestation values and also the platform to which the key owner claims it belongs.

11 Reference measurement record: For attestation to make any sense, reference values for the correct state of the device must be established in order to check for manipulation.

12 Document and store reference records and transfer to server: In addition to reference methods, it can also be useful to store a number of data records on the server side in order to enable sanity checks.

13 Start the boot process and time synchronization: the conditions to begin operation have been met.

14 Evidence collection: Finally, sensor data can become data records that potentially can become evidence. For this reason, data records are time-stamped using the TPM.

3. Secure Digital Evidence in Lawful Interception

In many countries, law enforcement can apply for the right to intercept communication data [12, 22]. For good reasons, the process of lawful interception usually is highly regulated [1]; however, the admissibility of data records achieved through lawful interception leaves various open questions. The discussion in this section concentrates on the security and reliability of the collected data itself.

3.1 Scenario and requirements for digital evidence

Consider the scenario where interception is done at the premises of a network provider and possibly executed through another service provider. An interface that enables data interception needs to be available and a device connected to this interface. This device collects all data available on the interface.

3.2 Specific characteristics of the scenario

Large streams of data need to be signed. Parts of the data might need to be deleted for privacy reasons without invalidating the signature, but still clearly showing where data was deleted. Example, VoIP streams.

3.3 Possible realizations

Use a hybrid approach. Bind the key for stream signatures to the TPM. Frequently change the key and attest that the key is bound to a particular state of the device. Digitally sign and store quote signatures and signatures on the data stream in a way that they can be clearly related.

4. Secure Digital Evidence in Automotive Black Boxes

A black box in a car is a device that is used to record various parameters of the car's control units. The data recorded by the black box can be used for diagnosis, i.e. to identify malfunction of the car. Further, data recorded by the black box can also be used to resolve disputes, e.g. in the case of an accident.

Most noticeable in the area of event data recorders (EDR) [11], less-refined versions of the so-called black box carried by aircraft, are motor vehicle event data recorders (MVEDRs) [5] as defined by the IEEE 1616a within the IEEE 1616 family of standards. IEEE 1616a aims to preserve the data quality and integrity needed to meet federal collection standards like the currently pending Motor Vehicle and Highway Safety Improvement Act of 2011, or Mariah's Act in the US. Data collected by EDRs has already been used in civil and criminal cases [9]. Additionally, an insurance company in the U.S. is promoting basing policy rates on the recorded behavior of the driver within an EDR provided by the company.

4.1 Scenario and requirements for digital evidence

The EDR is implemented as a separate control unit connected to one of the central communication buses in the car. It can monitor traffic on the bus and other control units can actively report the status or event information to the black box EDR. EDRs can record whether or not brakes were used, the speed at the time of impact, the steering angle, and whether seat belts were worn during the crash. The data collected within an EDR reflects the behavior and situation of the car before and during an accident or over even longer periods of time.

Every action of the driver, or the subsequent devices in the car, result in events to the car's EDR. As the device is under control of the owner of the car, evidence collected through an integrated event recorder is suspect to modification, deletion or injection. The consequences of such a tampered EDR vary with respect to the use case in which the collected data is employed.

Typical usage today of data collected in a car is for maintenance purposes and diagnostic aims. The intended use in the next generation will be to reconstruct the events leading to an accident and analyzing the driver's reactions according to the situation [10]. Therefore, each data item collected by an EDR is used to determine the individual involvement, and thus the liability, of the driver during the accident. Extended uses are recording behavior for longer times allowing analysis of the behavior of a specific driver in various traffic situations. Insurance companies are interested in adapting insurance rates to these profiles to allow risk-aware pricing schemes. Again, the data collected results in direct financial impact to the car's owner.

Both scenarios presented provide the owner of the car a strong incentive to modify the EDR's records. As in the first case, evidence could be destroyed that a misbehavior of the driver (e.g. speeding) happened the second the monthly rate for the insurance company was lowered. Modifying the behavior of such an EDR in terms of modifying the software would provide even stronger incentives since a manipulation of the collected records is not required.

4.2 Specific characteristics of the scenario

Creating digital data that can be used in court to determine who is responsibile is quite different from a documentation process over the length of time that would be required for data collection to be used for pricing insurance plans. Foremost, recording incidents is time critical allowing for the recording and signing of events even when they occur a

very short time before a crash. In case of an accident, it is required that as much data as possible be covered by verifiable signatures.

Data recorded is considered to be available as clearly defined data structures. The data stored is intentionally limited and reduced to small data sizes. This behavior supports the implementation of crash records under time critical situations. It should be noted that an independent power supply is not assumed to be available in cars due to cost and engineering reasons. Therefore, it is extremely important to reduce the write cycles for evidence to make sure that relevant evidence is captured.

Long-term storage of data records [23] needs to be local, i.e. within the box, providing an enclosed and isolated system with special measures against physical destruction. Only restricted memory is available for long-term storage.

4.3 Possible realizations

In principle, the basic design for a device generating secure evidence can also be applied to develop a black box; however, the criticality of the timing requires changes to the protocol. First, store the data record and subsequently sign, time-stamp and bind to quote information. Unsigned events recorded directly before a crash can still be considered valid as long as all signed data records that happened prior show that the status of the device is okay.

5. Secure Digital Evidence in Precise Farming

The evolution of technology in agricultural processes has changed the way that different steps in farming are executed [2]. Examples include the calculation and planning for fertilizers or creating the correct mixture of chemicals for plant protection [24]. These technologies provide the means for a very precise use of seeding material, fertilizer, etc. Large farms can be managed and controlled based on recorded data. Especially in the growing market for sustainable agriculture and eco-farming, there is a need for a qualitative value monitoring of the processes and the materials used such as of seeds, fertilizers etc. Further, farming subvention schemes for funding a farmer to grow particular crops are automatically controlled using data records produced by the machines used in these processes. Parameters include GPS positions to calculate the location and size of the area and the types of crop [26].

5.1 Scenario and requirements for digital evidence

The scenario consists of devices installed in the different types of farm machinery (tractors, harvesters, operating devices like fertilizer distribution equipment) and a central computer that collects and evaluates all the different data records. Depending on the particular use of the data records, different types of requirements exist. If genetically manipulated crops are used, it is very important to be able to reliably document where exactly the crops have been planted. In the case of fertilizers and pesticides or fungicides a wrong calculation of the amount of chemicals used in a particular area can create extensive damage. In the case of a question as to the predicted origin of farm produce or proper verification of the innocuousness of pesticides or fungicides, etc., this evidence is relevant. This becomes even more important as consumer concern increases regarding eco farming products and the evidence of eco farming. Further, when the data is used as proof for subventions as to which crop was grown in which area, manipulating these data records can be used to calculate wrongful subvention claims.

Under the above circumstances, it is necessary to integrate monitoring to ensure, that there is no hidden deployment of forbidden material or processing in the fields. To solve this problem, supervision of the area could be realized by drones. A European research project called Smart Inspectors is developing a drone-system for supervision of agriculture areas [18]. This system could be equipped with a TMP to be combined with the scenario described here.

5.2 Specific characteristics of the scenario

Because of the potential number of devices and systems involved, a communication network must be used for transferring the data to a central storage unit. This includes a network between several locations using the Internet as the carrier platform. For reliability and convenience, an 802.11 network should be used. Encryption of data as well as documented access control to all entities is required. Therefore the entire system considered in this scenario is much more complex than the automotive black box scenario. Considering the whole verified process, it will be necessary to bring three systems together to secure the entire scenario:

- farm monitoring system (described here)
- automotive black box

- smart inspection system.

The devices for this scenario should be highly usable and robust because they will be used outdoors and therefore exposed to rough weather conditions. Zero-touch configuration [15] for security mechanisms would be very useful as a design feature.

5.3 Possible realizations

Assuming correctness of the sensor measurements, the generic concept of a device for generating secure evidence can be applied directly; however, devices for secure documentation in precise farming technology need to consider that various sensors contribute to the data records and that most of them potentially can be manipulated. Therefore, a solution must be designed that combines the attestation of the platform with some kind of run-time validation for the correctness of the sensor information. Additionally, as physical manipulations to the sensor or to the environment of the sensor are possible, a straightforward technical solution is difficult. Nevertheless, using Trusted Computing as well as protection mechanisms for sensors, or plausibility calculations for a collection of sensors, these devices can be protected.

Additionally data transfer between the devices and the central storage unit must be secured and enabled for overall verification of the data, as well as of the condition of the sensors. TPM can be used for the verification. (Here a process must be defined for creation of a complete chain of evidence.) The resulting evidence will be created on the device side, and stored on the storage side, of the system. TPM certificates will be used for authentication of the device / storage to prevent an attack from any non-authorized device.

It is possible, that a farmer could use a non-confirmed device for bringing non-allowed materials onto his fields. To detect this, a smart-detection device could be used. In the "Smart Inspector" project, a drone will be developed and equipped with infrared cameras (IR) and radar systems for detection of unusual behavior or manipulation of the field's infrastructure.

6. Conclusions

We have discussed three distinct scenarios where the concept of employing a hardware device designed to produce admissible digital evidence is relevant. It was shown, that although requirements for each are quite different, all three scenarios can be realized using the solution proposed in 2012 by the authors. Future work will include identifying and analyzing additional scenarios in which this solution is relevant and

testing the solution in actual circumstances. The concept of forensic readiness, discussed at length years ago [6] is now realized and available for specific applications. It is anticipated that as the bar is raised on the admissibility of digital evidence due to the successful implementation of the technology described in [20] more applications requiring this solution will emerge.

References

[1] Y. Akdeniz, N. Taylor, and C. Walker. Regulation of investigatory powers act 2000 (1): Bigbrother. gov. uk: State surveillance in the age of information and rights,[2001]. *Criminal Law Review*, pages 73–90, 2001.

[2] H. Auernhammer. Precision farmingthe environmental challenge. *Computers and electronics in agriculture*, 30(1):31–43, 2001.

[3] D. Barrall and D. Dewey. Plug and root, the usb key to the kingdom. *Presentation at Black Hat Briefings*, 2005.

[4] R. Boddington. *Digital Business Security Development: Management Technologies*, chapter Digital evidence. IGI Global, 2011.

[5] M. Committee et al. Ieee standard for motor vehicle event data recorders (mvedrs), 2004.

[6] B. Endicott-Popovsky, B. Chee, and D. Frincke. Role of calibration as part of establishing foundation for expert testimony. In *Paper presented at the 3rd Annual IFIP WG 11.9 Conference.*, Orlando, FL, 2007.

[7] B. Endicott-Popovsky and D. Frincke. Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. In *Information Assurance Workshop, 2006 IEEE*, pages 133–139. IEEE, 2006.

[8] B. Endicott-Popovsky, D. Frincke, and C. Taylor. A theoretical framework for organizational network forensic readiness. *Journal of Computers*, 2(3):1–11, 2007.

[9] R. Fay, R. Robinette, D. Deering, and J. Scott. Using event data recorders in collision reconstruction. *SAE Technical Paper*, pages 01–0535, 2002.

[10] H. Gabler, D. Gabauer, H. Newell, and M. ONeill. *Use of Event Data Recorder (EDR) technology for highway crash data analysis*, volume 298. Transportation Research Board of the National Academies, 2005.

[11] A. German, J. Comeau, B. Monk, K. McClafferty, P. Tiessen, and J. Chan. The use of event data recorders in the analysis of real-world crashes. *Proc. CMRSC-XII*, pages 10–13, 2001.

[12] S. Gleave. The mechanics of lawful interception. *Network Security*, 2007(5):8–11, 2007.

[13] N. Kuntze and C. Rudolph. Secure digital chains of evidence. In *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 Fifth IEEE International Workshop on*, may 2011.

[14] N. Kuntze and C. Rudolph. Constructing and evaluating digital evidence for processes. In *Systematic Approaches to Digital Forensic Engineering (SADFE), 2012 Fifth IEEE International Workshop on*, October 2012.

[15] N. Kuntze and C. Rudolph. On the automatic establishment of security relations for devices. *Proceedings of the IEEE IM*, 2013.

[16] C. Mitchell. *Trusted computing*, volume 6. Iet, 2005.

[17] S. Ngobeni, H. Venter, and I. Burke. A forensic readiness model for wireless networks. *Advances in Digital Forensics VI*, pages 107–117, 2010.

[18] B. R. Smart inspectors. INTERREG IV A. http://www.hochschule-rhein-waal.de/en/forschungszentrum/forschungsprojekte/smart-inspectors.html.

[19] R. Retting, S. Ferguson, and A. Hakkert. Effects of red light cameras on violations and crashes: a review of the international literature. *Traffic Injury Prevention*, 4(1):17–23, 2003.

[20] J. Richter, N. Kuntze, and C. Rudolph. Securing digital evidence. In *Fifth International Workshop on Systematic Approaches to Digital Forensic Engeneering*, pages 119–130, 2010.

[21] C. Taylor, B. Endicott-Popovsky, and D. Frincke. Specifying digital forensics: A forensics policy approach. *digital investigation*, 4:101–104, 2007.

[22] E. TC-STAG. Security techniques advisory group (stag); definition of user requirements for lawful interception of telecommunications: requirements of the law enforcement agencies, 1996.

[23] C. Wallace, U. Pordesch, and R. Brandner. Long-term archive service requirements. *Request For Comments–RFC*, 4810, 2007.

[24] N. Wang, N. Zhang, and M. Wang. Wireless sensors in agriculture and food industryrecent development and future perspective. *Computers and electronics in agriculture*, 50(1):1–14, 2006.

[25] A. Waugh, R. Wilkinson, B. Hills, and J. Dell'Oro. Preserving digital information forever. In *Proceedings of the fifth ACM conference on Digital libraries*, pages 175–184. ACM, 2000.

[26] S. Wolf and S. Wood. Precision farming: Environmental legitimation, commodification of information, and industrial coordination1. *Rural sociology*, 62(2):180–206, 1997.