Chapter 1

ON THE CREATION OF RELIABLE DIGITAL EVIDENCE

Nicolai Kuntze, Carsten Rudolph, Aaron Alva, Barbara Endicott-Popovsky, John Christiansen, Thomas Kemmerich

Abstract Traditional approaches to digital forensics are concerned with the reconstruction of events within digital systems that often are not built for the creation of evidence. This work focuses on the idea of incorporating requirements for forensic readiness– designing-in features and characteristics that support the use of the data produced in these devices being used as evidence. This paper explores legal requirements that such evidence must meet as the basis for developing technical requirements for the design of such systems. An approach is proposed that could be used to develop devices and establish processes crafted for the purpose of creating digital evidence. The authors suggest that the legal view be incorporated into device design as early as possible to allow for the probative value required of the evidence produced by such devices.

Keywords: Secure digital evidence, event correlation, digital chains of evidence, trusted computing, digital forensics, ESI, admissibility, forensic readiness

1. Introduction

This paper discusses courtroom admissibility of data found in devices that are deployed on networks which, in the course of business, collect, compute, store or distribute data that potentially can be relevant as digital evidence. One of the authors has written extensively on the concept of 'network forensic readiness' defined by Tan as "Maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response [21, 9, 8]." Implementation of forensic readiness is good security. It enables pursuit of legal redress against a malicious insider or external intruder and documents due care in the event of civil litigation claiming networked systems are not adequately

defended. Nevertheless, while much of the effort expended in the field of digital forensics is concerned mainly with methods and technologies that recover data evidence stored on computer hardware, this work concentrates on a slightly different issue, namely the admissibility of data collected and stored by network devices deployed on networks to collect, compute, store or distribute data that potentially can be relevant as legal evidence. These authors contend that the time to consider admissibility of such evidence is upstream as the devices are being designed and developed, not after these devices are deployed and data records are created and stored. Examples of devices that could become collectors of potential legal evidence include traffic cameras (e.g. for speeding, red-light, or road tolls), all kinds of calibrated devices (e.g. petrol pumps, digital scales, metering devices), but also devices for logging of activities in enterprise networks (e.g. e-mail, stock market activities).

Thus, the discussion in this paper concentrates on how such a device can be made to create digital evidence securely without physical intervention. All devices will have some kind of electronic interface and software module designed to transfer data, to perform maintenance, to configure the device, to install updates or to interact with the device in other ways. Experience has shown that software has weaknesses and that one never can assume a device to be 'unhackable.'[1] Examples like the Stuxnet worm show that even devices not directly connected to the Internet and with restricted software can be attacked [19]. Further, changes to software do not leave any traces and a device can be changed from the correct state to a manipulated state and back without any record of having done so, if not designed properly. The current approach by practitioners in the IT community seems to be to assume that "if a device has not been proven untrustworthy, then it is acceptable" [11]. The question of forensical soundness concentrates mainly on the processes to recover forensic evidence [14]. For mobile devices NIST [22] demands that digital evidence is recovered from a device *under forensically sound conditions* but the question of unnoticed manipulations of the device remains open. In the IT security community such a conclusion is generally seen as very dangerous or plainly wrong.[2] A more suitable approach would be to build systems for which some properties can be proven to hold under reasonable assumptions [12]. Furthermore, while any such device will need to allow some set of 'trusted people' the ability to pen-

[1]Both the CVE (Common Vulnerabilities Enumeration) database http://cve.mitre.org/ and the NVD (National Vulnerability Database) are testaments to the overwhelming numbers of software flaws that exist in basic tools of our digital infrastructure.

[2]UW CISO Kirk Bailey in lectures at the Agora (Seattle, WA) 2011 emphasizes the need for healthy skepticism on the part of security practitioners. Trust but verify!

etrate the device under authorized circumstances, there will need to be some means to track this activity in order not to invalidate the devices use as a reliable gatherer of evidence. Current approaches to trusted computing development enable the development of secure systems that allow trusted person access. Further, at the procedural level, it could be reasonable to require that personnel operating the systems shall not be able to manipulate data records eligible as digital evidence.

1.1 Defining 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 tamper-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.[3])
- 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) and additional information on the state of the measurement device. This additional information on the state of the measurement device aims to document the operation environment providing evidence that can help lay the foundation for admissibility. As in the case of calibration of breathalyzers, for example, if the measurement device is modified, such information should also be recorded as part of amassing information supportive of admissibility. This will permit, at a later date, the linking of the software version used to collect the evidence in question. This information would permit an expert witness to testify to the known vulnerabilities of that particular software version and thus the likelihood of attacks.

1.2 Making Devices Forensically Ready

By incorporating requirements into device design that focus on 1) potential admissibility of data records created by the device and 2) creating additional documentation that would support arguments for admissibility, we establish devices that are 'forensically ready.' Subsequent transport and secure storage of digital evidence are not part of this discussion,

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

although they must be considered by anyone responsible for operating a network in a manner that ensures collection of competent legal evidence. However, for the purposes of this article, we assume that digital evidence is created and stored in the device in question, and that there exists reliable mechanisms to maintain authenticity and integrity of the data records and also to provide non-repudiation for any steps of handling or changing the data, perhaps relying on some kind of digital signature which is often the case. For long-term security, archiving schemes can be used where digital signatures are replaced with some other security mitigations, anticipating that employed cryptographic algorithms will become unreliable due to increasingly sophisticated attacks or evolving computing capabilities. Physical attacks on devices are also not included in the discussion. We are assuming that, as in many cases, it will be sufficient to install tamper-evident devices (e.g. by using sealed boxes, installing devices in physically controlled rooms, etc.). Constructing real tamper-proof devices is expensive and difficult. Experience in IT security, as evidenced in the CWE and NVD databases, clearly shows that all solutions that rely on software are not secure on current hardware architectures. Thus we are focusing on security at the mechanism level– how we develop and implement requirements for forensic readiness. Digital evidence requires that additional security mechanisms be implemented into the hardware that will render them impossible to be manipulated without physical access to the device.

2. Relating device security, software security and 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. Also solutions for secure long-term archiving must be considered.

This paper proposes that a device can be produced and configured in a way that results in admissible evidence which is correct and reliable as long as the device is not physically manipulated or corrupted; however, many examples show that it is very difficult to build devices without vulnerabilities [13, 15, 6]. Even very restricted appliances such as electronic voting machines or components in industrial control systems have been successfully attacked. The following discusses some of the unintended legal consequences affecting admissibility of evidence and corresponding

threat scenarios. Although this list is not exhaustive, it begins to lay a technical basis for creating devices that will yield reliable digital evidence. Next steps will involve a systematic analysis of threats and risk assessments for each individual case described below.

2.1 Attacking communication channels

Devices can be equipped with various wired and wireless communication technologies and all of them, theoretically, can be subject to attacks. Restricting communication channels is often not possible as they are needed for efficient operations or maintenance access.

All external interfaces can be used by attackers to penetrate and gain control of a device to exploit its weaknesses and manipulate its results. Furthermore, if the collected evidence on the device also includes data collected via communication interfaces, attacks on the communication channels can change data before it is compiled into an evidentiary record on the device. Once a data record is created on the device and protected using digital signatures, for example, integrity and authenticity cannot be violated by attacking those communication channels.

In subsequent sections, it is assumed that attackers can get access to the device either via remote communication (e.g. WLAN, Ethernet, GSM) or by direct physical interface or near-field wireless communication (e.g. USB, Bluetooth).

2.2 Outsiders attacks

Devices that use state-of-the-art access control, in principle, can require that each access demand suitable credentials that might not available to the attacker; however, various attack vectors can provide access to the device, anyway. Software flaws can be exploited either to increase the access rights of a user with legitimate restricted access to the system, or to install malicious software via existing interfaces (e.g. network interfaces or maintenance interfaces). This malware can be used subsequently to take control of the device.

Furthermore, physical access to the device can be used to change device status without actually physically manipulating the device (e.g. if opening the device would break seals). One example of a manipulation that can require physical access is booting another operating system. By doing so, access control mechanisms can be circumvented and the behavior of the device can become fundamentally different. Moreover, this manipulation can potentially be done without leaving any visible traces on the device and, even worse, changes on stored data, stored original software, and configurations can cause wrong or malicious behavior af-

ter booting the original operating system. Such intermediate access to the device can also be used to create persistent threats that at first do not change the behavior of the device but can be used anytime later to induce malicious behavior and to manipulate potential evidentiary records.

A worst case scenario might be when attackers either hide their attacks so that they remain unnoticed or can restore the original state of the device, leaving no traces of manipulation. Such successful attacks can be repeated or executed at will with Trojan programs inserted and obfuscated from identification.

Protection against outsider attacks requires strong physical security, highly secure software, or devices with no external communication interfaces at all. An operational strategy might be to store data records on a storage medium inside a physically protected and sealed box.

2.3 Insider attacks

Insiders have credentials (e.g. passwords, SmartCards) that will allow them to access a device. Thus, they can easily change configuration parameters or install different software. Furthermore, they may be able to restore the original state of the device that would obliterate any record of their having had access.

Note that having the authority to decide on valid software and configuration is similar to the authority to calibrate and seal a device. Even for calibrated non-digital measuring devices, authorized individuals can manipulate the device. Thus, specifying respected roles in the digital world is critical. When developing technical solutions one needs to assume that parties involved are trusted. Nevertheless, one cannot always assume that personnel ultimately operating the device can be trusted. Therefore, all roles and their particular responsibilities must be made very clear, and technical solutions designed, in a way that only minimal trust is required.

3. Legal perspective

With all of the vulnerabilities and threats of systems producing digital evidence, the authenticity of such evidence is subject to greater scrutiny in the courts of law. Digital evidence must contain a validated and well-documented chain of evidence that aligns with standards put in place formally or informally by the legal system. This digital chain of evidence will be used for the court to decide whether the evidence is admissible as valid evidence. While the legal system in the United States has a history of using past court precedence as guidance in ruling on issues

at hand, the high complexity of information systems forced a deviation away from precedence [6].

3.1 Jurisdiction

Described in this section are Rules and Procedures that apply only to the United States courts. Within the U.S. court system, the decision for admissibility is given to the judge. Each judge may have different requirements within this set of guidelines, and each case may require a different scale of proof.[4] Throughout this section, careful attention is given to the applicability of rules based on jurisdiction.

3.2 Definition of ESI

To allow digital evidence– known widely as "Electronically Stored Information" or "ESI" [4]– to be admissible in courts within the United States, there is a procedural process which will be discussed in this section. The Rules which this process must adhere to are the basis by which admissibility questions are addressed. The definition of Electronically Stored Information as written by the Federal Rules of of Civil Procedure (FRCP) do not specifically define ESI. Instead the FRCP state a definition of what could be regarded:

> Any party may serve on any other party a request... to produce and permit the party making the request, or someone acting on the requestors behalf, to inspect, copy, test, or sample any designated documents or electronically stored information including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained[5].

3.3 Rules Guiding ESI

For Electronically Stored Information or ESI, the "2006 Amendments" to the Federal Rules of Civil Procedure brought clarity to dealing with digital evidence. This new guidance ensures that parties must cooperate to create and carry out a discovery strategy that also considers costs involved with gathering electronic evidence[6]. The applicability of Rules guiding ESI is dependent on the type of digital evidence being presented. Within the scope of systems used for digital evidence collection (such as electronic toll booths or traffic cameras), the Rules which apply fall under the category of "Computed Stored Records and Data" with overlap on the applicable rules under the category of "Digital Photographs."

[4] [6] quoting Weinstein on Evidence 900.06[3].
[5] [6] citing [2].
[6] [6] citing [16]

Note that many of the authentication methods outlined by these rules overlap with other types of electronic evidence. Applicable Federal Rules of Evidence are:

- Witness with personal knowledge (901(b)(1))
- Expert testimony (901(b)(3))
- Distinctive Characteristics (901(b)(4))
- System or process capable of proving a reliable result (901(b)(9))[7]

For guidance on other forms of electronic evidence in relation to admissibility, and the applicable rules for each form see [4]. Specifically noted are Federal Rules of Evidence 104, 901, and 902 in order to confirm authenticity of evidence.

3.4 Past Precedence in Admissibility

Though the Federal Rules of Civil Procedure mandate the procedures that guide admissibility of evidence, there have also been frameworks created through past law that offer a useful methodology to an architect of a digital evidence collection system. What is called the 'Daubert test' is a set precedence for determining if scientific evidence, including digital evidence, is admissible as valid evidence in a court case. Formed in the United States Supreme Court's decision on Daubert v. Merrell Dow Pharmaceuticals Inc. [7], this test is also confirmed by Rule 702 in the Federal Rules of Evidence of 1975 [3]. The stated purpose of this test is to determine the reliability of scientific evidence by engaging in a "preliminary assessment of whether the reasoning or methodology underlying the test is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts at issue."[8] Tested through this method is:

1. whether the proffered knowledge can or has been tested,
2. whether the theory or technique has been subjected to peer review and publication,
3. the known or potential rate of error, and
4. whether the theory or technique has gained general acceptance in the relevant scientific discipline.[9]

The Daubert test, and supporting Rule 702, must be applied in all U.S. Federal Courts to all types of expert testimony [5, 3]. This Federal Courts mandate of the Daubert test provides a legal framework for the

[7] See Paul Grimm & Kevin F. Brady in Appendix A to [4].
[8] [10] quoting [7]
[9] [10] quoting [7]

research conducted on the creation of a reliable digital chain of evidence that can be applied to a broad range of digital evidence. Use of the Daubert test requirements as a legal framework enables the chain of evidence described in this paper to map directly to U.S. Federal Court requirements, and to other courts of law that use the Daubert test.

3.5 Cost considerations

A properly created digital chain of evidence is crucial to the admissibility of evidence, thus it is necessary to create an information system that properly preserves ESI (Electronically Stored Information). The cost considerations are two-fold: any such system must be 1) cost-effective to build and maintain and 2) prevent fines from record spoliation.

According to the Federal Rules of Civil Procedure 26(b)(2) [1], ESI that is cost-prohibitive to retrieve may still be ordered by the court to go through discovery. It is in the interest of the party controlling a digital evidence collection system to have an easy and quick method for proper record retrieval. Thus, "[I]f a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk[.] [17]"

Other requirements for a cost-effective record retrieval method are to mitigate the risk of being subject to spoliation litigation. Incurring fines based upon record spoliation can be very costly to an organization. A "federal common law of spoliation" has arisen, giving an implied judicial requirement of systems to protect against spoiled records.[10] Additionally, statutory or regulatory requirements may apply which also require certain demands for record keeping. It is best interest to avoid these fines that are seemingly benign, but costly.

3.6 Summary of Legal Perspective

This section has approached the admissibility of digital evidence from two directions: 1) the procedures that require collaboration of both parties in a legal case to discover ESI to be used in a case, and 2) a framework used by the court to determine whether submitted evidence will be admissible. There is great overlap in both approaches, although the presentation of both elements provides a more comprehensive look into the legal environment within the United States.

From a legal perspective, due diligence must be done in order for courts to consider digital evidence admissible. The use of the Daubert

[10] [6] See [20] and [16]

test framework sets a high bar for this diligence. Use of this framework will guide the technical creation of devices that must produce a chain of digital evidence. Application of this technical approach will enable digital evidence to have strong supporting verification for evidence admissibility, providing digital forensic readiness. The next section will incorporate these principles into technical guidance for creating devices that will create a digital chain of evidence– essentially rendering the device "forensically ready."

4. Technical solutions for the creation of digital evidence

The legal requirements towards the creation of digital evidence as discussed in the previous section imposes strong requirements on the security of individual technical devices as the evidentiary records but also on the processes involved in the processes for validating the device and software running on the device, for transmitting and storing evidence records, for linking evidence records to a chain of evidence, and also for verifying evidence records in the case of a dispute. The following subsections provide an overview of existing technical approaches starting from securing the actual creation on the individual device, looking at the infrastructure, and finally the processes involved.

4.1 Individual Device

Devices with various interfaces pose particular problems. Besides typical communication network interfaces, direct or close-range access via USB, for example, increase the complexity of protecting devices from physical access, let alone network attacks. As discussed previously, the complexity of current state-of-the-art devices presents a challenge for constructing a secure device that is both efficient and useable. Therefore, taking a pragmatic approach to securing digital evidence on these devices, the authors suggest focusing on establishing assurance that the device was not manipulated at the time of the creation of the evidentiary record.

One approach might be to establish a cryptographic binding of evidence to the status of the device [18]. This can be achieved by using the existing technology of Trusted Computing [15] as specified by the Trusted Computing Group. The so-called Trusted Platform Module (TPM) can establish a hardware root of trust in the device. The security-level of a specialized security chip can be compared to Smart-Card security. In combination with a first trusted step in the boot process, the TPM can be used to store, and securely report, measure-

ment values documenting all software that was loaded after the current boot started. Further, the TPM provides the functionality to sign data records combined with these measured values and also to time-stamp data records to reliably reflect time relationships. The first prototypes of traffic cameras secured by this technology are available [24, 23]. In addition to the so-called attestation of the current boot process of a device as established by Trusted Computing, there also exist approaches that go beyond attesting to only one boot cycle. The cumulative attestation proposed by LeMay and Gunter [13] provides additional records and attests to the history of the boot process.

In contrast to the Trusted Computing approach, measurement values are not completely deleted for each re-boot, but a cumulative measurement chain is generated over several boot processes. This approach ensures that the device has not been booted in an insecure start after the cumulative measurement has started. It should be noted that, by using hardware-based roots of trust protection, this also prevents some types of insider attacks where insiders try to produce false evidence. The trust in the status reporting of a particular device is rooted in certain core roots of trust. The TPM is one prominent example of an available root of trust for reporting. These roots of trusts are built and certified by public bodies to be tamper-proof, or at least hard to tamper. This reduces the possible attack vectors that could result in modification of the reported status of the device, even to authorized insiders like administrators.

4.2 Infrastructure

It should be noted that securely creating a data record is not sufficient to establish secure digital evidence. The device producing the record must be integrated into an appropriate infrastructure that can be structured into two parts: 1) elements that collect the data that then is stored in the evidence record and 2) securely transmitting RDS and maintaining long-term storage of that data. Data collection is not only about maintaining the integrity of the data. Correctness of sensor data depends on many other factors, such as physical parameters of the environment (e.g. temperature or humidity), the location of the device and the physical integrity of the sensor itself. Some of these factors can be controlled by additional sensors; the status of these could be included in the reporting from the hardware-based attestation mechanisms.

Nevertheless, physical manipulation of the sensors is always possible. Threat modeling and risk analysis can provide analysis of residual risks remaining after Trusted Computing is implemented. Integrity and authenticity of data records can be maintained through use of public key

cryptography. Since the private key can be stored exclusively inside a hardware security chip, this aspect of the infrastructure can be secured in this manner. Also solutions for long-term archiving exist (e.g. by renewing digital signatures before their algorithms are broken and signatures become useless). The mechanisms for this type of protection are well-established and can be efficiently implemented. However, digital evidence can contain personal identifiable information (PII), requiring application of privacy enhancing technologies to digital evidence. Additional infrastructure is needed if several individual evidentiary records are linked to a *chain of evidence*[12].

4.3 Process

In addition to technical solutions for securely creating and storing digital evidence and digital evidence chains, organizational processes must enable the correct implementation and reproducibility of these technical solutions. Verification and checking of digital evidence cannot be restricted to checking a single digital signature per evidence record. It also needs to include additional checks on cryptographic key certificates and validation of the status of the devices involved in the creation of evidence records. Various types of digital certificates for cryptographic keys or software measurement values will be necessary. Additional checks can be required such as certification of the platforms involved in the creation of evidence records. A chain of evidence (or most probably a tree or several linked trees) would require going through this process for each type of digital evidence and to establish all necessary links between evidence records.

The following describes a proposed procedure required in advance of actually producing signed digital evidence:

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 the key owner claims it belongs to.

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.

5. Conclusions

This paper provides a concept for the development of devices capable of securely collecting digital evidence. Furthermore, the discussion of the legal view of the problem of the suitability of data records to become digital evidence lays the groundwork for developing technical requirements for these devices. The paper describes technology that either exists or is being developed that can ensure that these devices become forensically ready and the data they produce can become evidence. In addition, the need to provide tight integration between these technologies and the administrative procedures that maintain them, has been highlighted. The authors make the case that these aspects must be incorporated into device design to ensure the probative value of evidence collected on them.

Suggested steps for forensic readiness are recommended. This is by no means a complete list of processes, but rather a proposed approach that must be integrated into existing environments, demonstrating the complexity of the modifications to existing systems that must be made to ensure the admissibility of the data they produce. This underlines the need for more research in this area in order to ensure more convenient and less complex designs. Future work will explore this line of investigation, developing prototypes and validating the approach presented in this paper.

References

[1] Fed. R. Civ. P. 26(b)(2).

[2] Fed. R. Civ. P. 34(a).

[3] Fed. R. Evid. 702.

[4] K. F. Brady, C. R. Crowley, P. F. Doyle, M. E. O'Neill, J. D. Shook, and J. M. Williams. The Sedona Conference commentary on ESI evidence & admissibility: a project of the sedona conference working group on Electronic Document Retention, 9, Fall; 2011/10 2008.

[5] M. Calhoun. Scientific evidence in court: Daubert or frye, 15 years later. *Washington Legal Foundation*, 23(37), August 2008.

[6] J. Christiansen. Discovery and admission of electronic information as evidence. Manuscript submitted for publication, 2008.

[7] Daubert v. Merrell Dow Pharmaceuticals, Inc., 113 S. Ct. 2786, 1993.

[8] 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.

[9] 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.

[10] D. S. Fridman and J. Janoe. The State of Judicial Gatekeeping in California. In *Judicial Gatekeeping Project*. Harvard Law School, Harvard Law School, February 1999.

[11] N. Kuntze. Informal interviews with it operations personnel, 2011.

[12] 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.

[13] M. LeMay and C. Gunter. Cumulative attestation kernels for embedded systems. *Computer Security–ESORICS 2009*, pages 655–670, 2009.

[14] R. McKemmish. When is digital evidence forensically sound? In *IFIP Int. Conf. Digital Forensics*, pages 3–15, 2008.

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

[16] G. L. Paul and B. H. Nearon. *The discovery revolution: e-discovery amendments to the Federal rules of civil procedure*. American Bar Association, Apr. 2006.

[17] Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526, 1997.

[18] 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.

[19] B. Schneier. The story behind the stuxnet virus. *Forbes.com*, Oct. 2010.

[20] Silvestri v. General Motors Corp., 2001.

[21] J. Tan. Forensic readiness. *Cambridge, MA:@ Stake*, 2001.

[22] J. W. and A. R. Guidelines on cell phone forensics. NIST Special Publication 800-101, 2007.

[23] T. Winkler and B. Rinner. Applications of trusted computing in pervasive smart camera networks. In *Proceedings of the 4th Workshop on Embedded Systems Security*, page 2. ACM, 2009.

[24] T. Winkler and B. Rinner. Trustcam: security and privacy-protection for an embedded smart camera based on trusted computing. In *Advanced Video and Signal Based Surveillance (AVSS),*

2010 Seventh IEEE International Conference on, pages 593–600. IEEE, 2010.