On the Creation of Reliable Digital Evidence

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

Chapter 1

ON THE CREATION OF RELIABLE DIGITAL EVIDENCE

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

Abstract Traditional approaches to digital forensics deal with the reconstruction of events within digital devices that were often not built for the creation of evidence. This paper focuses on incorporating requirements for forensic readiness – designing in features and characteristics that support the use of the data produced by digital devices as evidence. The legal requirements that such evidence must meet are explored in developing technical requirements for the design of digital devices. The resulting approach can be used to develop digital devices and establish processes for creating digital evidence. Incorporating the legal view early in device design and implementation can help ensure the probative value of the evidence produced the devices.

Keywords: Digital evidence, admissibility, forensic readiness

1. Introduction

This paper discusses the courtroom admissibility of data found in devices deployed in networks which, in the course of business, collect, compute, store or transmit data that can be relevant as digital evidence. Network forensic readiness is defined by Tan [16] as "maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of incident response." Clearly, implementing forensic readiness is a good security practice. It enables the pursuit of legal redress against a malicious insider or an external attacker, and helps document due diligence in the event of civil claims that computer systems and networks were not adequately defended.

Several authors (see, e.g., [4, 5]) argue that the time to consider the admissibility of evidence is upstream, as devices are being designed and

developed, not after the devices are deployed and data records are created and stored. Examples of devices that are collectors of potential evidence include traffic cameras (e.g., speeding, red lights and tolls), various calibrated devices (e.g., digital scales and metering devices), and devices that log activities in enterprise networks (e.g., e-mail and stock market transactions).

The focus of this paper is how such devices can be made to create digital evidence in a secure manner without physical intervention. Every device has an electronic interface and software module designed to transfer data, perform maintenance, configure the device, install updates and interact with the device in other ways. Experience has shown that software has weaknesses and that a device cannot be assumed to be "unhackable." The Common Vulnerabilities Enumeration (CVE) Database and the National Vulnerability Database (NVD) are testaments to the large numbers of flaws that exist in software tools. Meanwhile, the Stuxnet worm has demonstrated that even devices that are not directly connected to the Internet and those with restricted software can be attacked [15]. Furthermore, if a device is not designed properly, software can be modified without leaving any traces and the device can be changed from a correct state to a manipulated state and back without any record of having done so.

In general, IT practitioners tend to assume that, if a device has not been proven untrustworthy, then it is acceptable. The question of forensic soundness concentrates mainly on the processes used to recover evidence [10]. In the case of mobile devices, NIST [7] recommends that digital evidence should be recovered "under forensically sound conditions." However, the question of undiscovered manipulations of a device remains an open issue. In the IT security community such a conclusion is generally seen as very dangerous or plainly wrong. What is needed is healthy skepticism on the part of security practitioners – trust but verify.

Thus, a suitable approach is to build systems for which some properties can be proven to hold under reasonable assumptions [8]. Furthermore, while a device would have to permit some "trusted entities" to penetrate it under authorized circumstances, there must be some means to track this activity in order not to invalidate the use of the device as a reliable gatherer of evidence. Trusted computing approaches facilitate the development of secure systems that allow trusted access. But at the operational level, it is also important to ensure that users cannot manipulate data records that potentially constitute digital evidence.

2. Secure Digital Evidence

A data record can be considered to be secure if it was created in an authentic manner by a device for which the following properties hold:

- The device is physically protected to ensure at least evidence of tampering. 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 (e.g., time, temperature, location and involved users). The actual set of parameters and the protection levels depend on the scenario and on the type of data record.
- The data record has not been changed after creation.

Digital evidence according to this definition comprises the measured values (e.g., photograph and speed measurement) and additional information about the state of the measurement device. The additional information about the device state serves to document the operational environment and provide evidence that can help lay the foundation for admissibility. For example, when calibrating a breathalyzer, information about any modifications made to the device should be recorded as part of the process of collecting information that supports admissibility. This could permit, at a later date, the linking of the software version used to collect the evidence in question. Also, an expert witness could be brought upon to testify to the known vulnerabilities of the particular software version and, thus, the likelihood of attacks.

3. Forensically Ready Devices

A device can be established as "forensically ready" by incorporating design requirements that focus on: (i) potential admissibility of data records created by the device; and (ii) creating additional documentation that would support arguments for admissibility.

Note that the subsequent transport and secure storage of digital evidence are not part of this discussion, although they must be considered by anyone responsible for operating a network in a manner that ensures the collection of competent legal evidence. In particular, we assume that digital evidence is created and stored in the device in question, and that there exist reliable mechanisms to maintain the authenticity and integrity of data records and to provide non-repudiation for any steps of handling or changing the data, perhaps relying on digital signatures (which is often the case). For long-term security, archiving schemes can be used where digital signatures are replaced with some other security

controls, since the cryptographic algorithms that are employed could become unreliable due to increasingly sophisticated attacks and evolving computing capabilities.

Physical attacks on devices are considered in this discussion. We assume that it is sufficient to install tamper-evident devices (e.g., using sealed boxes or installing devices in rooms that are physically secured). Tamper-proof devices are expensive and difficult to construct, and pure software solutions are not secure on current hardware architectures. Therefore, we focus on security at the mechanism level – how requirements are developed and implemented for forensic readiness. Digital evidence requires additional security mechanisms to be implemented at the hardware level to ensure that the devices cannot be manipulated without physical access.

4. Securing Devices and Software

The content and format of data records produced on a device depends on several factors, including the hardware design, software running on the device and device configuration. After a digital data record is produced, its integrity, confidentiality and authenticity must be ensured by applying certain security controls such as encryption and digital signatures. Also, solutions for the secure, long-term archiving of data records must be considered.

This paper proposes that a device should be produced and configured in a manner that results in admissible evidence, which is correct and reliable as long as the device is not physically manipulated or corrupted. Unfortunately, it is extremely difficult to build devices that do not have vulnerabilities [3, 9, 12]. The paper discusses some of the unintended legal consequences that affect the admissibility of evidence and the corresponding threat scenarios. Although the discussion is by no means comprehensive, it helps define a technical basis for creating devices that would yield reliable digital evidence.

4.1 Communication Channel Attacks

Devices are equipped with various wired and wireless communications technologies, all of them subject to attacks. It is often not possible to restrict communication channels because they are needed for efficient operations and maintenance.

An external interface can be used by an attacker to penetrate and gain control of a device to exploit its weaknesses and manipulate its results. If the evidence on the device also includes data collected via communication interfaces, attacks that target the corresponding communication

channels can change the data before it is compiled into an evidentiary record on the device. After a data record is created on the device and protected using digital signatures, it is much more difficult to target data integrity and authenticity by attacking the communication channels.

In the following sections, we assume that attackers can obtain access to a device either remotely (e.g., using WLAN, Ethernet or GSM) or via a direct physical interface or a near-field wireless technology (e.g., USB and Bluetooth).

4.2 Outsider Attacks

Devices that use strong access control mechanisms, in principle, can require that each access request submit suitable credentials that might not be available to an attacker. However, access control mechanisms can be circumvented in many ways. For example, software flaws can be exploited to obtain higher access privileges. Alternatively, malicious software can be installed using network interfaces or maintenance interfaces; the malware can be used subsequently to take control of the device.

Physical access to a device can be leveraged to change the device status. An example is booting a device using a different operating system, which could circumvent the access control mechanisms and modify device behavior. Such manipulation could be done without leaving visible traces on the device and, even worse, visible changes to the stored data, software and configurations. Intermediate access to a device can also be used to create persistent threats that, at first, do not change the behavior of the device, but can be used at some point in the future to induce malicious behavior and to manipulate potential evidentiary records.

The worst-case scenarios involve attackers hiding their activities so that they remain unnoticed and attackers restoring devices to their original states so that there are no traces of manipulation. Such attacks can be executed at will using Trojan programs or rootkits that are thoroughly obfuscated.

Protecting against outsider attacks requires strong physical security, highly secure software and devices with no external communication interfaces. A good operational strategy is to store the data records on a storage medium inside a sealed box that is physically protected.

4.3 Insider Attacks

Insiders have credentials (e.g., passwords and smartcards) that allow them to access a device. These credentials enable them to easily change configuration parameters or install different software. Furthermore, the

credentials may enable them to restore the original state of the device and remove any trace of access.

The authority to decide on the valid software and configuration is similar to the authority to calibrate and seal a device. Also, one cannot always assume that the personnel who ultimately operate the device are trusted. Therefore, all roles and responsibilities must be made very clear. Furthermore, technical solutions should be designed to accommodate minimal trust on the part of users.

5. Legal Perspective

Given the vulnerabilities and threats to systems that produce digital evidence, the authenticity of evidence may have to be proven prior to its admission in legal proceedings. Digital evidence must therefore have a well-documented and validated chain of evidence that demonstrates its reliability consistently with the rules of evidence and case law applicable in the jurisdiction in question. The digital chain of evidence is used by the court to decide whether or not evidence is admissible. This section discusses the rules and procedures that apply to U.S. federal courts; state courts tend to follow the lead of federal courts.

U.S. courts use a combination of procedural rules and case law precedence as guidance when ruling on evidentiary issues. However, the complexity of information systems and the relative novelty of digital evidence issues often require the court to make decisions on applying rules and precedents in new ways to new or different situations [3]. The U.S. legal system gives judges the right to decide on the admissibility of evidence. Each judge has some degree of discretion in interpreting the rules and case law, and each case may require a different type of analysis (from [3] citing [11]).

5.1 Electronically Stored Information

The rules of evidence and court procedural rules establish a process for the admission of digital evidence (widely known as "electronically stored information" [1]) in federal court. The rules to which this process must adhere constitute the basis for addressing admissibility questions. The Federal Rules of Civil Procedure do not specifically define electronically stored information. Instead, they describe what could be regarded as electronically stored information (from [3] citing [20]):

> *"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."

5.2 Rules

The 2006 amendments to the Federal Rules of Civil Procedure brought some clarity to methods for dealing with digital evidence. These rules require parties to cooperate in creating and carrying out a discovery strategy that also considers the costs involved in gathering digital evidence (from [3] citing [13]). The specific application of the rules for electronically stored information is dependent on the type of digital evidence being presented, and the architecture and functionality of the system(s) in which it is created and stored and from which it is produced. A wide variety of systems and applications may produce digital evidence (e.g., electronic toll booths and traffic cameras), so the specific evidentiary rules that may apply fall under different categories, such as "Computed Stored Records and Data" and "Digital Photographs."

In general, the potentially 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)) (see Appendix A in [1])

Note that many of the authentication methods provided for in these rules overlap with other types of electronic evidence. Interested readers are referred to [1] for guidance on other forms of electronic evidence in relation to admissibility. Specifically noted are Federal Rules of Evidence 104, 901 and 902 for proving the authenticity of evidence.

5.3 Admissibility

While the Federal Rules of Civil Procedure and Evidence mandate the procedures that guide the admissibility of evidence, judicial rulings (case law) also provide requirements and guidance for architects of digital evidence collection systems. The well-known Daubert test, based on a 1993 Supreme Court case [22], is often used to determine if scientific evidence, including digital evidence, is admissible as valid evidence in court. The Daubert test is constituent with Rule 702 [21]. The purpose of the 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" ([6] quoting [22]). This method tests: (i) whether the proffered knowledge can or has been tested; (ii) whether the theory or technique has been subjected to peer review and publication; (iii) the known or potential rate of error; and (iv) whether the theory or technique has gained general acceptance in the relevant scientific discipline ([6] quoting [22]).

The Daubert test and Rule 702 must be applied in all U.S. federal courts to all types of expert testimony [2, 21]. The Daubert test, therefore, provides a legal framework for research focused on the creation of a reliable digital chain of evidence that can be applied to a broad range of digital evidence. Using the Daubert 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.

5.4 Cost

A properly created digital chain of evidence is crucial to the admissibility of evidence. In order to do this, it is necessary to create an information system that properly preserves electronically stored information. Cost considerations include the cost of building and maintaining the system, balanced against the potential costs of producing digital evidence and the potential penalties for spoliation (corruption or loss) of digital evidence.

Under Federal Rule of Civil Procedure 26(b)(2) [19], a party may be required to produce electronically stored information even if the costs of production are prohibitive. It is, therefore, in the interest of the party controlling a system that may be required to produce digital evidence to have a quick, easy and reliable method for evidentiary information 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" [18].

Another potential exposure that may be avoided by building systems with the production of digital evidence in mind is penalties for spoliation of evidence. Penalties for avoidable spoliation can be very expensive, and the court can even decide that spoliation of important evidence is grounds for ruling under which a party can lose the case altogether. The federal "common law" of spoliation therefore creates an important incentive for implementing systems that protect against the loss and corruption of potential digital evidence [3, 13, 17]. Statutory or regulatory requirements may impose additional requirements for record keeping.

On balance, then, it may be very much in an organization's financial interest to accept the additional costs of acquiring or developing and maintaining digital evidence creation and retention systems in order to avoid potentially much greater losses in litigation.

5.5 Summary

In summary, the admissibility of digital evidence can be approached from two directions: (i) the procedures that require collaboration of both the parties in a legal case to discover the electronically stored information that is used in the case; and (ii) a framework used by the court to determine whether or not the submitted evidence is admissible. There is considerable overlap between the two approaches, although the presentation of both elements provides a more comprehensive perspective into the U.S. legal environment.

From a legal perspective, due diligence must be demonstrated in order for courts to consider digital evidence as admissible. The Daubert test framework sets a high bar for this diligence. The framework can guide the technical development of devices that must produce a chain of digital evidence. The next section incorporates these principles into technical guidance for developing devices that create a digital chain of evidence – essentially rendering the device "forensically ready."

6. Technical Solutions

The legal requirements for the creation of digital evidence as discussed in the previous section impose strong requirements on the security of the individual technical devices as well as on the processes for: (i) validating the devices and their software; (ii) transmitting and storing evidentiary records; (iii) linking evidentiary records to a chain of evidence; and (iv) verifying evidentiary records in the event of a dispute. The following subsections discuss the technical approaches involved in securing the individual devices, the infrastructure and the various processes that are involved.

6.1 Individual Devices

Device interfaces are particularly problematic. Besides typical communication network interfaces, USB interfaces that provide direct or close-range access complicate the task of protecting devices from physical access, let alone network attacks. As discussed previously, the complexity of state-of-the-art devices presents a challenge in constructing secure devices that are both efficient and useable. Therefore, we take a pragmatic approach to securing digital evidence on these devices. In par-

ticular, we believe that it is vital to establish assurance that the device was not manipulated at the time the evidentiary record was created.

One approach is to establish a cryptographic binding of evidence to the status of the device [14]. This can be achieved by using trusted computing technologies [12]. A trusted platform module (TPM) can be used to establish a hardware root of trust in the device. In combination with a first trusted step in the boot process, the TPM can be used to store and securely report measurements that document all the software that was loaded after the current boot started. The TPM also provides the functionality to sign data records combined with the measurements, and also to timestamp data records to reliably reflect time relationships. Some traffic camera prototypes secured using this technology are already available [23, 24].

Approaches have been developed that go beyond the attestation of the current boot process of a device. An example is the cumulative attestation technique proposed by LeMay and Gunter [9], which provides additional records and attests to the history of the boot process. In contrast with the trusted computing approach, measurement values are not completely deleted at each reboot, but a cumulative measurement chain is generated over several boot processes. This approach ensures that the device has not been booted in an insecure state after the cumulative measurements have started.

Note that using hardware-based roots of trust also prevents certain types of insider attacks, including those where insiders attempt 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 a prominent example of a root of trust that can be used for reporting. A root of trust must be constructed and certified to be tamper-proof or at least hard to tamper. This would reduce the likelihood of attacks that modify the reported status of the device, even to authorized insiders such as systems administrators.

6.2 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 is structured into two parts: (i) elements that collect the data stored in an evidentiary record; and (ii) elements that securely transmit data and maintain the long-term storage of the data.

Data collection is not only about maintaining data integrity. The correctness of sensor data, for example, depends on many factors, including

environmental parameters (e.g., temperature or humidity), 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 sensors should 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 help assess the residual risks after trusted computing is implemented. The integrity and authenticity of data records can be maintained through the use of public key cryptography. A private key can be stored exclusively on a hardware security chip, enabling this aspect of the infrastructure to be secured. Also solutions for long-term archiving exist (e.g., by renewing digital signatures before their algorithms are broken and signatures become useless). Such protection mechanisms are well-established and can be implemented efficiently. However, digital evidence can contain personal identifiable information, which requires the application of privacy enhancing technologies. Also, additional infrastructure is needed if several individual evidentiary records are linked to a chain of evidence [8].

6.3 Process

In addition to the technical solutions for securely creating and storing digital evidence and digital evidence chains, organizational processes must enable the correct implementation and reproducibility of the technical solutions. The verification of digital evidence cannot be restricted to checking a single digital signature per evidentiary record. Checks should also be performed on cryptographic key certificates and the status of the devices involved in the creation of evidentiary records should be validated. Various types of digital certificates for cryptographic keys and software measurement values would be necessary. Additional checks may be required, such as certification of the platforms involved in the creation of evidentiary records. A chain of evidence – or most probably a tree or several linked trees of evidence – would require going through this process for each type of digital evidence and establish all the necessary links between evidentiary records.

In summary, the following procedure is required in advance of producing signed digital evidence:

- **Implement Hardware Security Anchor:** The hardware anchor (e.g., TPM) must function at a high security level.
- **Certify Hardware Security Anchor:** The security properties of the hardware anchor should be documented in a security certificate with an appropriate security level.

- **Certify Platform:** The security chip and its integration in the platform should be verified and certified.
- **Develop and Validate Software:** Relevant software such as the operating system, drivers and applications should be developed and validated.
- **Install, Initialize and Certify Software:** It is vital to ensure that the software has been installed and initialized correctly, that the software has not been manipulated, and that the security certification covers all the relevant aspects.
- **Establish Reference Measurements for Calibrated Devices:** Define and certify the reference measurements (e.g., location and temperature) of calibrated devices.
- **Generate and Certify Signing Keys:** Since the scheme relies heavily on cryptography, specifically, the secure generation, distribution and storage of keys, these processes must be certified. Because of the range of possible use cases, it is difficult to recommend a single algorithm.
- **Define Parameter Ranges:** The parameter ranges for the correct operation of devices must be established. Operation outside the defined ranges should be prevented or the design should be modified to avoid problems.
- **Install and Initialize Devices:** The installation and initialization process is critical because it is where the keys are generated and exchanged.
- **Establish Communication with Server:** The establishment of client server communication is well understood. However, no efficient solution exists for binding SSL keys to the underlying attestation values and to the platform.
- **Record Reference Measurements:** For attestation to make any sense, the reference values for the correct device state must be established.
- **Document and Store Reference Records and Transfer to Server:** In addition to the reference measurements, it is important to store a number of data records on the server side to enable checking.
- **Start Boot Process and Time Synchronization:** This is done only after the conditions to begin operation have been met.

- **Collect Evidence:** Sensor data is collected in the form of data records that potentially constitute evidence. For this reason, the data records must be timestamped using the TPM.

7. Conclusions

It is essential to develop and deploy devices that can collect digital evidence in a secure manner. The legal perspective of the suitability of data records to become digital evidence lays the groundwork for developing technical requirements for these devices. Several technologies exist or are being developed to ensure that these devices are forensically ready and that the data they produce can become evidence. However, the technologies and the administrative procedures that maintain them must be tightly integrated. Indeed, all these aspects must be incorporated into device design to ensure the probative value of the collected evidence.

The forensic readiness steps recommended in this paper are by no means a complete list. Rather, they constitute 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 underscores the need for more research to ensure less complexity and more user convenience. Our future work will explore this line of investigation, developing prototypes and validating the overall approach.

References

[1] K. Brady, C. Crowley, P. Doyle, M. O'Neill, J. Shook and J. Williams, The Sedona Conference Commentary on ESI Evidence and Admissibility, The Sedona Conference, Phoenix, Arizona, 2008.

[2] M. Calhoun, Scientific evidence in court: *Daubert* or *Frye*, 15 years later, *Washington Legal Foundation*, vol. 23(37), pp. 1–4, 2008.

[3] J. Christiansen, Discovery and admission of electronic information as evidence, in *E-Health Business and Transactional Law: 2010 Cumulative Supplement*, J. Sullivan (Ed.), BNA Books, Arlington, Virginia, pp. 427–452, 2010.

[4] B. Endicott-Popovsky, B. Chee and D. Frincke, Calibration testing of network tap devices, in *Advances in Digital Forensics III*, P. Craiger and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 3–19, 2007.

[5] B. Endicott-Popovsky and D. Frincke, Embedding forensic capabilities into networks: Addressing inefficiencies in digital forensic investigations, *Proceedings of the IEEE Information Assurance Workshop*, pp. 133–139, 2006.

[6] D. Fridman and J. Janoe, The state of judicial gatekeeping in California, presented at the *Criminal Justice Gatekeeping Seminar*, 1999.

[7] W. Jansen and R. Ayers, Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[8] N. Kuntze and C. Rudolph, Secure digital chains of evidence, *Proceedings of the Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2011.

[9] M. LeMay and C. Gunter, Cumulative attestation kernels for embedded systems, *Proceedings of the Fourteenth European Conference on Research in Computer Security*, pp. 655–670, 2009.

[10] R. McKemmish, When is digital evidence forensically sound? in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 3–15, 2008.

[11] J. McLaughlin (Ed.), *Weinstein's Federal Evidence: Commentary on Rules of Evidence for the United States Courts*, Matthew Bender, New York, 1997.

[12] C. Mitchell, *Trusted Computing*, Institute of Engineering and Technology, London, United Kingdom, 2005.

[13] G. Paul and B. Nearon, *The Discovery Revolution: e-Discovery Amendments to the Federal Rules of Civil Procedure*, American Bar Association, Chicago, Illinois, 2006.

[14] J. Richter, N. Kuntze and C. Rudolph, Securing digital evidence, *Proceedings of the Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 119–130, 2010.

[15] B. Schneier, The story behind the Stuxnet virus, *Forbes.com*, October 7, 2010.

[16] J. Tan, Forensic readiness (`isis.poly.edu/kulesh/forensics/forensic_readiness.pdf`), 2001.

[17] U.S. Court of Appeals (Fourth Circuit), Silvestri v. General Motors Corp., *Federal Reporter Third Series*, vol. 271, pp. 583–595, 2001.

[18] U.S. District Court (Northern District of Illinois), In re Brand Name Prescription Drugs Antitrust Litigation, *Westlaw*, no. 360526, 1995.

[19] U.S. Government, Rule 26(b)(2), Federal Rules of Civil Procedure, *United States Code*, p. 156, 2006.

[20] U.S. Government, Rule 34(a), Federal Rules of Civil Procedure, *United States Code*, p. 195, 2006.

[21] U.S. Government, Rule 702, Federal Rules of Evidence, *United States Code*, p. 357, 2006.

[22] U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals, Inc., *United States Reports*, vol. 509, pp. 579–601, 1993.

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

[24] T. Winkler and B. Rinner, Trustcam: Security and privacy-protection for an embedded smart camera based on trusted computing, *Proceedings of the Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance*, pp. 593–600, 2010.