Helmut Reimer
Norbert Pohlmann
Wolfgang Schneider *Eds.*

ISSE 2013 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2013 Conference

Springer Vieweg

ISSE 2013 Securing Electronic Business Processes

Helmut Reimer • Norbert Pohlmann
Wolfgang Schneider (Eds.)

ISSE 2013 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2013 Conference

Springer Vieweg

Editors
Helmut Reimer
TeleTrusT – Bundesverband IT-Sicherheit e.V.
Erfurt, Germany

Norbert Pohlmann
Gelsenkirchen, Germany

Wolfgang Schneider
Darmstadt, Germany

ISBN 978-3-658-03370-5
DOI 10.1007/978-3-658-03371-2

ISBN 978-3-658-03371-2 (eBook)

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2013950028

Springer Vieweg

Typesetting: Oliver Reimer, Jena

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Contents

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the tenth ISSE book – another mark of the event's success – and with about 25 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ammar Alkassar**, Sirrix AG (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **John Colley**, EMEA & (ISC)2 (United Kingdom)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, KU Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Michael Hartmann**, SAP (Germany)
- **Jeremy Hilton**, Cranfield University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Marc Kleff**, Siemens Enterprise Communications (Germany)

- **Hasse Kristiansen**, Ernst & Young (Norway)
- **Jaap Kuipers**, Id Network (The Netherlands)
- **Manuel Medina**, ENISA
- **Patrick Michaelis**, Research In Motion (Germany)
- **Norbert Pohlmann** (chairman), Institute for Internet Security, Westfälische Hochschule, Gelsenkirchen (Germany)
- **Bart Preneel**, KU Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Marc Sel,** PWC (Belgium)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **Claire Vishik**, Intel (United Kingdom)
- **Erik R. van Zuuren**, Deloitte (Belgium)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

TeleTrusT – IT Security Association Germany

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities.

TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is carrier of the "European Bridge CA" (provision of public key certificates for secure e-mail communication), the quality seal "IT Security made in Germany" and runs the IT expert certification program "TeleTrusT Information Security Professional (T.I.S.P.)". TeleTrusT is member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year's European Security Conference ISSE is being organized in collaboration with eema and LSEC and supported by the European Commission and ENISA.

Contact:

TeleTrusT – IT Security Association Germany
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17, 10115 Berlin, GERMANY
Tel.: +49 30 4005 4306, Fax: +49 30 4005 4311
http://www.teletrust.de

EEMA

Since 1987 EEMA has been Europe's leading independent, association for eID and Security. To keep in step with industry developments and member requirements, it recently reinvented itself to focus more specifically on Cyber security and eID technologies and services. Since then, EEMA has become the leading eID and Identity forum in Europe operating across both private and public sector in Europe, working with its European members, governmental bodies, partners, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA also partners with the European Commission, ENISA, TeleTrusT, BCS, LSec and TDL, and involves its members in collaborative European commission projects such as STORK 1 & 2 (eID interoperability) pan-European project; a three year project – SSEDIC – Scoping the Single European Digital Identity Community and has recently won two other FP7 projects – Future ID and Cloud for Europe.

EEMA is the lead organization for the renowned ISSE conference (Information and Security Solutions Europe) and conducts many studies for the EU on interoperability of eID and other related issues. EEMA holds a number of ID related conferences during the year and these are well attended by its members and non-members alike for instance "Trust in the Digital World" in partnership with TDL and "Digital Enterprise Europe" as well as many one day events throughout Europe.

EEMA's remit is to educate and inform over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its members is available to other members free of charge.

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a member of EEMA, and any employee of that organisation is then able to participate in EEMA activities. Examples of organisations taking advantage of EEMA membership are Siemens, Hoffman la Roche, Volvo, ING, RaboBank, KPMG, Deloitte, Novartis, TOTAL, Ericson, Adobe, Magyar Telecom Rt, Nets, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

Cloud Security, Trust Services, eId & Access Management

pohlmann@internet-sicherheit.de

Draft of a Dynamic Malware Detection System on Trustworthy Endpoints

Andreas Speier · Christofer Fein · David Bothe
Eric Reich · Norbert Pohlmann

Institute for Internet Security
Westphalian University of Applied Sciences Gelsenkirchen
{speier | fein | bothe | reich | pohlmann}@internet-sicherheit.de

Abstract

Malware infected computer systems can be found with increasing evidence in private and commercial fields of use. Always exposed to the risk of a "Lying End-Point", an already manipulated security application that pretends to run on a clean computer system, the demand for new security solutions continues to rise. Project iTES ("innovative Trustworthy Endpoint Security"), government-funded by the German Federal Ministry of Education and Research, introduces a new system to enhance security while preserving usability. Based on an existing virtualized system which diversifies the software to a specific form of use, the project aims to develop new sensors to monitor the system dynamically and deliver real-time responses.

1 Introduction

Malware infected computer systems can be found with increasing evidence in private and commercial fields of use. Even technically advanced countries fall victim to severe damages caused by malicious software. Prevention of such attacks has to result in hardening computer systems against malware activity. Critical applications like online banking and e-commerce introduce a profitable field for criminal individuals, which significantly raises the need for trusted data processing even more. Conventional security solutions available today already offer thorough countermeasures, but are often exposed to manipulation by malware themselves. Always being subject to the risk of a "Lying End-Point", an already manipulated security application that pretends to run on a clean computer system [SSDD07], the demand for new security solutions continues to rise.

Project iTES[1] introduces a new system to enhance security while preserving usability. The system architecture needs to guarantee the reliability of a security solution with provable integrity to prevent attacks. Typical computer systems will be assembled regarding private used and professional used software components to serve as a reference for behavior analysis (see section 2.4).

Common Trusted Computing technologies combined with virtualization create a secure software environment to isolate malware, which provides a basis for innovative and trustworthy security systems. A core intention of iTES is to combine already existing security technologies and

1 http://ites-project.org

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_1,

advance them through innovative developments. Continuous usage of security software will be fortified by virtualization and integrity-measures of its components. Another important part is the development of software sensors (see section 2.5) for dynamic malware behavior analysis and detection by a security software guest system.

In section 2.3 the architecture of a physical client is outlined. The inner structure, like the main security concept (see section 2.1-2.2) and the software sensors (see section 2.5) are described in detail. The software separation is mentioned in section 2.3.

The secure environment with the multiple client concept and the central component are described in general in section 3.

2 System Architecture

Common trusted computing technologies offer manipulation detection and possibilities to attest configurations of computer systems. Virtualization adds the separation of single applications within strong isolated compartments. The hypervisor is the interface between the host system and a virtualized guest system. In our system this interface is also intended to integrate sensors to perform dynamic malware analysis (see section 2.4).

2.1 Integrity

Proving the integrity is one of the main goals in securing a system. The integrity of the guest system has to be examined before the startup routine by calculating checksums of the virtual machine configuration files. A complete check of the virtual machine image is a time consuming task and may take several minutes as shown in table 1. In the shown example a single 13 GB OS image has been subjected to the hash algorithms shown, on a middle class business notebook using some well-known hash algorithms. On a system as described in this paper, there will be at least four guest system images. Therefore a smarter integrity check has to be developed to perform rapidly before the virtual machines are permissible to be started. A pre-boot investigation will be done on security relevant components of the virtualized system. These components have to be compared with their pre-defined secure states. A deviation from the defined initial state has to be identified as abnormal configuration [Pohl08]. In this case the virtual machines start procedure has to be denied and the configuration of the system as a whole must be reestablished as described in section 2.2.

Table 1: Mean checksum calculation time (s) on 13GB image file, read from disk

Algorithm / Disk Technology	**HDD**	**SSD**
md5	~112 s	~49 s
sha1	~128 s	~85 s
sha256	~117 s	~51 s
sha512	~120 s	~61 s

Human Factors, Awareness & Privacy, Regulations & Policies

Enhancing Transparency with Distributed Privacy-Preserving Logging

Roel Peeters[1] · Tobias Pulls[2] · Karel Wouters[1]

[1]KU Leuven & iMinds, COSIC (Belgium)
{roel.peeters | karel.wouters}@esat.kuleuven.be

[2]Karlstad University, PriSec (Sweden)
tobias.pulls@kau.se

Abstract

Transparency of data processing is often a requirement for compliance to legislation and/or business requirements. Furthermore, it has recognised as a key privacy principle, for example in the European Data Protection Directive. At the same time, transparency of the data processing should be limited to the users involved in order to minimise the leakage of sensitive business information and privacy of the employees (if any) performing the data processing.

We propose a cryptographic logging solution, making the resulting log data publicly accessible, that can be used by data subjects to gain insight in the data processing that takes place on their personal data, without disclosing any information about data processing on other users' data. Our proposed solution can handle arbitrary distributed processes, dynamically continuing the logging from one data processor to the next. Committing to the logged data is irrevocable, and will result in log data that can be verified by the data subject, the data processor and a third party with respect to integrity. Moreover, our solution allows data processors to offload storage and interaction with users to dedicated log servers. Finally, we show that our scheme is applicable in practice, providing performance results for a prototype implementation.

1 Introduction

Transparency is recognised as a key privacy principle, e.g., in the EU Data Protection Directive 95/46/EC Articles 7, 10, and 11; and in the Swedish Patient Data Act ("Patientdatalagen") SFS (2008:355). The Swedish Patient Data Act states that every patient have the right to see who has accessed their electronic healthcare record (EHR), i.e., access logs to EHRs have to be kept and made available to patients. This kind of transparency of data processing is often a requirement for compliance with legislation and/or business requirements, as well in healthcare as in other sectors, e.g., bookkeeping in the financial sector. Transparency of data processing, in general, may increase end-users' trust in the data processor[1], especially if the data processing is distributed as in cloud computing [KJM+11]. The need for building trust is also a big part in why transparency towards citizens is a key element of eGovernment services [UN12].

1 We use the technical terminology of data processor and user, as opposed to the EU Data Protection Directive in which a more formal/legal terminology (data controller, data subject) is used.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_6,

Security Management

Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment

Claire Vishik[1] · Frederick Sheldon[2] · David Ott[1]

[1]Intel Corporation
{claire.vishik | david.e.ott}@intel.com

[2]Oak Ridge National Laboratory
sheldonft@ornl.gov

Abstract

Cybersecurity practice lags behind cyber technology achievements. Solutions designed to address many problems may and do exist but frequently cannot be broadly deployed due to economic constraints. Whereas security economics focuses on the cost/benefit analysis and supply/demand, we believe that more sophisticated theoretical approaches, such as economic modeling, rarely utilized, would derive greater societal benefits. Unfortunately, today technologists pursuing interesting and elegant solutions have little knowledge of the feasibility for broad deployment of their results and cannot anticipate the influences of other technologies, existing infrastructure, and technology evolution, nor bring the solutions lifecycle into the equation. Additionally, potentially viable solutions are not adopted because the risk perceptions by potential providers and users far outweighs the economic incentives to support introduction/adoption of new best practices and technologies that are not well enough defined. In some cases, there is no alignment with predominant and future business models as well as regulatory and policy requirements.

This paper provides an overview of the economics of security, reviewing work that helped to define economic models for the Internet economy from the 1990s. We bring forward examples of potential use of theoretical economics in defining metrics for emerging technology areas, positioning infrastructure investment, and building real-time response capability as part of software development. These diverse examples help us understand the gaps in current research. Filling these gaps will be instrumental for defining viable economic incentives, economic policies, regulations as well as early-stage technology development approaches, that can speed up commercialization and deployment of new technologies in cybersecurity.

1 Introduction

Applications of theoretical economics to the introduction of new security technologies already exist. Studies of asymmetric information in computing environments, models of monetary economics, economic models for liability, as well as exploration of the economic positioning of informational products in general could be helpful in evaluating available options and defining the nature of optimal economic incentives. These studies may also help to establish the metrics necessary to build a multidisciplinary scientific framework for examining prospective security technologies and design relevant economic incentives.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_12,

Cybersecurity, Cybercrime, Critical Infrastructures

pohlmann@internet-sicherheit.de

Digital Forensics as a Big Data Challenge

Alessandro Guarino

StudioAG
a.guarino@studioag.eu

Abstract

Digital Forensics, as a science and part of the forensic sciences, is facing new challenges that may well render established models and practices obsolete. The dimensions of potential digital evidence supports has grown exponentially, be it hard disks in desktop and laptops or solid state memories in mobile devices like smartphones and tablets, even while latency times lag behind. Cloud services are now sources of potential evidence in a vast range of investigations and network traffic also follows a growing trend and in cyber security the necessity of sifting through vast amount of data quickly is now paramount. On a higher level investigations – and intelligence analysis – can profit from sophisticated analysis of such datasets as social network structures, corpora of text to be analysed for authorship and attribution. All of the above highlights the convergence between so-called data science and digital forensics, to tack the fundamental challenge of analyse vast amount of data ("big data") in actionable time while at the same time preserving forensic principles in order for the results to be presented in a court of law. The paper, after introducing digital forensics and data science, explores the challenges above and proceed to propose how techniques and algorithms used in big data analysis can be adapted to the unique context of digital forensics, ranging from the managing of evidence via Map-Reduce to machine learning techniques for triage and analysis of big forensic disk images and network traffic dumps. In the conclusion the paper proposes a model to integrate this new paradigm into established forensic standards and best practices and tries to foresee future trends.

1 Introduction

1.1 Digital Forensics

What is digital forensics? We report here one of the most useful definitions of digital forensics formulated. It was developed during the first Digital Forensics Research Workshop (DFRWS) in 2001 and it is still very much relevant today:

> *Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.[Pear01]*

This formulation stresses first and foremost the scientific nature of digital forensics methods, in a point in time when the discipline was transitioning from being a "craft" to an established field and rightful part of the forensic sciences. At that point digital forensics was also transitioning from being mainly practised in separated environments such as law enforcement bodies and enterprise audit offices to a unified field. Nowadays this process is very advanced and it can be

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_17,

said that digital forensics principles, procedures and methods are shared by a large part of its practitioners, coming from different backgrounds (criminal prosecution, defence consultants, corporate investigators and compliance officers). Applying scientifically valid methods implies important concepts and principles to be respected when dealing with digital evidence. Among others we can cite:

- Previous validation of tools and procedures. Tools and procedures should be validated by experiment prior to their application on actual evidence.
- Reliability. Processes should yield consistent results and tools should present consistent behaviour over time.
- Repeatability. Processes should generate the same results when applied to the same test environment.
- Documentation. Forensic activities should be well-documented, from the inception to the end of evidence life-cycle. On one hand strict chain-of-custody procedures should be enforced to assure evidence integrity and the other hand complete documentation of every activity is necessary to ensure repeatability by other analysts.
- Preservation of evidence – Digital evidence is easily altered and its integrity must be preserved at all times, from the very first stages of operations, to avoid spoliation and degradation. Both technical (e.g. hashing) and organizational (e.g. clear accountability for operators) measures are to be taken.

These basic tenets are currently being challenged in many ways by the shifting technological and legal landscape practitioners have to confront with. While this paper shall not dwell much on the legal side of things, this is also obviously something that is always to be considered in forensics.

Regarding the phases that usually make up the forensic workflow, we refer here again to the only international standard available[ISO12] and describe them as follows:

- Identification. This process includes the search, recognition and documentation of the physical devices on the scene potentially containing digital evidence.[ISO12]
- Collection – Devices identified in the previous phase can be collected and transferred to an analysis facility or acquired (next step) on site.
- Acquisition – This process involves producing an image of a source of potential evidence, ideally identical to the original.
- Preservation – Evidence integrity, both physical and logical, must be ensured at all times.
- Analysis – Interpretation of the data from the evidence acquired. It usually depends on the context, the aims or the focus of the investigation and can range from malware analysis to image forensics, database forensics, and a lot more of application-specifics areas. On a higher level analysis could include content analysis via for instance forensics linguistics or sentiment analysis techniques.
- Reporting – Communication and/or dissemination of the results of the digital investigation to the parties concerned.

1.2 Data Science

Data Science is an emerging field basically growing at the intersection between statistical techniques and machine learning, completing this toolbox with domain specific knowledge, having as fuel big datasets. Hal Varian gave a concise definition of the field:

[Data science is] the ability to take data – to be able to understand it, to process it, to extract value from it, to visualize it, to communicate it.[Vari09]

We can see here the complete cycle of data management and understand that data science in general is concerned with the collection, preparation, analysis, visualization, communication and preservation of large sets of information; this is a paraphrase of another insightful definition by Jeffrey Stanton of Syracuse University School of Information Studies. The parallels with the digital forensics workflow are clear but the mention in both definition of visualization deserves to be stressed. Visualization is mostly never mentioned in digital forensics guidelines and standards but as the object of analysis move towards "Big Data", it will necessarily become one of the most useful tools in the analyst's box, for instance in the prioritization phase but also for dissemination and reporting: visual communication is probably the most efficient way into a human's brain but this channel is underused by most of today forensic practitioners.

If Data Science is concerned with "Big Data", what is Big Data anyway? After all big is a relative concept and prone to change with time. Any data that is difficult to manage and work with, or in other words datasets so big that for them conventional tools – e.g. relational databases – are not practical or useful.[ISAC13] From the point of view of data science the challenges of managing big data can be summarized as three Vs: Volume (size), Velocity (needed for interactivity), Variety (different sources of data). In the next paragraph we shall see how this three challenges dovetail nicely with the digital forensics context.

2 Challenges

"Golden Age" is a common definition for the period in the history of digital forensics that went roughly from the 1990s to the first decade of the twenty-first century. During that period the technological landscape was dominated by the personal computer, and mostly by a single architecture – x86 plus Windows – and data stored in hard drives represented the vast majority of evidence, so much so that "Computer Forensics" was the accepted term for the discipline. Also the storage size allowed for complete bitwise forensic copies of the evidence for subsequent analysis in the lab. The relative uniformity of the evidence nature facilitated the development of the digital forensic principles outlined above and enshrined in several guidelines and eventually in the ISO/IEC 27037 standard. Inevitably anyway they lagged behind the real-world developments: recent years brought many challenges to the "standard model", first among them the explosion in the average size of the evidence examined for a single case. Historical motivations for this include:

- A dramatic drop of hard drives and solid state storage cost (currently estimated at $80 per Terabyte) and consequently an increase in storage size per computer or device;
- Substantial increase in magnetic storage density and diffusion of solid-state removable media (USB sticks, SD and others memory cards etc) in smartphones, notebooks, cameras and many other kinds of devices;
- Worldwide huge penetration of personal mobile devices like smartphones and tablets, not only in Europe and America, but also in Africa – where they constitute the main communication mode in many areas – and obviously in Asia;
- Introduction and increasing adoption by individuals and businesses of cloud services – Infrastructure services (IAAS), platform services (PAAS) and applications (SAAS) – made possible in part by virtualization technology enabled in turn by the modern multi-core processors;

- Network traffic is ever more part of the evidence in cases and the sheer size of it has – again – obviously increased in the last decade, both on the Internet and on 3G-4G mobile networks, with practical but also ethical and political implications;
- Connectivity is rapidly becoming ubiquitous and the "Internet of things" is near, especially considering the transition to IPv6 in the near future. Even when not networked, sensors are everywhere, from appliances to security cameras, from GPS receivers to embedded systems in cars, from smart meters to Industrial Control Systems.

To give a few quantitative examples of the trend, in 2008 the FBI Regional Computer Forensics Laboratories (RCFLs) Annual Report[FBI08] explained that the agency's RCFLs processed 27 percent more data than they did during the preceding year; the 2010 Report gave an average case size of 0.4 Terabytes. According to a recent (2013) informal survey among forensic professionals on Forensic Focus, half of the cases involve more than on Terabyte of data, with one in five over five Terabytes in size.

The simple quantity of evidence associated to a case is not the only measure of its complexity and the growing in size is not the only challenge that digital forensics is facing: evidence is becoming more and more heterogeneous in nature and provenience, following the evolving trends in computing. The workflow phase impacted by this new aspect is clearly analysis where, even when proper prioritization is applied, it is necessary to sort through diverse categories and source of evidence, structured and unstructured. Data sources themselves are much more differentiated than in the past: it is common now for a case to include evidence originating from personal computers, servers, cloud services, phones and other mobile devices, digital cameras, even embedded systems and industrial control systems. File formats

3 Rethinking Digital Forensics

In order to face the many challenges but also to leverage the opportunities it is encountering the discipline of digital forensics have to rethink in some ways established principles and reorganize well-known workflows, even include and use tools not previously considered viable for forensic use – concerns regarding the security of some machine learning algorithms has been voiced, for instance in [BBC+08]. On the other hand forensic analysts' skills need to be rounded up to make better use of these new tools in the first place but also to help integrate them in forensic best practices and validate them. The dissemination of "big data" skills will have to include all actors in the evidence lifecycle, starting with Digital Evidence First Responders (DEFRs), as identification and prioritization will see their importance increased and skilled operators will be needed from the very first steps of the investigation.

3.1 Principles

Well-established principles shall need to undergo at least a partial extension and rethinking because of the challenges of Big Data.

- Validation and reliability of tools and methods gain even more relevance in a big data scenario because of the size and variety of datasets, coupled with the use of cutting-edge algorithms that still need validation efforts, including a body of test work first on methods and then on tools in controlled environments and on test datasets before their use in court.

Mobile Security & Applications

pohlmann@internet-sicherheit.de

Protected Software Module Architectures

Raoul Strackx[1] · Job Noorman[1] · Ingrid Verbauwhede[2]
Bart Preneel[2] · Frank Piessens[1]

[1]iMinds-DistriNet, KU Leuven
Celestijnenlaan 200A, 3001 Leuven, Belgium
{Raoul.Strackx | Job.Noorman | Frank.Piessens}@cs.kuleuven.be

[2]iMinds-COSIC, KU Leuven
Kasteelpark Arenberg 10, 3001 Leuven, Belgium
{Ingrid.Verbauwhede | Bart.Preneel}@esat.kuleuven.be

Abstract

A significant fraction of Internet-connected computing devices is infected with malware. With the increased connectivity and software extensibility of embedded and industrial devices, this threat is now also relevant for our industrial infrastructure and our personal environments. Since many of these devices interact with remote parties for security-critical or privacy sensitive transactions, it is important to develop security architectures that allow a stakeholder to assess the trustworthiness of a computing device, and that allow such stakeholders to securely execute software on that device. Over the past decade, the security research community has proposed and evaluated such architectures. Important and promising examples are *protected software module architectures*. These architectures support the secure execution of small protected software modules even on devices that are malware infected. They also make it possible for remote parties to collect *trust evidence* about a device; the remote party can use the security architecture to collect measurements that give assurance that the device is in a trustworthy state.

In this paper we outline the essential ideas behind this promising recent line of security research, and report on our experiences in developing several protected module architectures for different types of devices.

1 Introduction

Any programmable device is at risk of being reprogrammed, exploited, or infected with malware by attackers. This risk goes up significantly for network-connected devices, as exploitation or infection can now be done remotely. Protection against this threat is significantly harder for devices that are *open* in the sense that they support software extensibility, possibly even by several parties that do not necessarily trust each other. Historically, the first such devices were classical computers (desktops and servers), and history has taught us that the threat of malware infection and other software attacks against these devices is very real indeed.

Over the past years, more and more embedded computing devices are being connected to the Internet, and many of these devices are open to some extent to software extensibility. Examples include smartcards that support over-the-air updates, programmable sensor-networks, set-top boxes and internet-connected TV's as well as SCADA (supervisory control and data acquisition) systems that control important components of our critical infrastructure. The increasing connec-

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_21,