First IEEE International Workshop on Information Forensics and Security

Workshop Guide

IEEE

IEEE Signal Processing Society

Contents

Preface

Plans for an IEEE Workshop on Information Forensics and Security probably began shortly after the inception of the IEEE Transactions on Information Forensics and Security. It has been surprisingly difficult to execute this plan, taking a period of over two years. We hope participants find the effort worthwhile.

The first IEEE Workshop on Information Forensics and Security (WIFS'09) is sponsored by the IEEE Signal Processing Society. Our aspiration is that WIFS'09 is the first in a long line of workshops/conferences associated with the SPS Technical Committee on Information Forensics and Security. Our aim is that WIFS'09 and its successors will offer a venue for knowledge exchange that encompasses a broad range of disciplines on Information Forensics and Security and facilitates the exchange of ideas between the various disparate communities. By so doing, we hope that researchers will identify new opportunities for collaboration across disciplines and gain new perspectives.

We would like to thank the sponsors British Telecommunications plc., Ingenico, the Digital Communications Knowledge Transfer Network, the European Office of Aerospace Research and Development, Thomson, and Hewlett-Packard for their support. We would also like to express our special thanks to Gwenaël Doërr for his relentless efforts to keep us all on track. It is not an exaggeration to say that this Workshop would not have happened without Gwenaël’s tireless efforts. Finally, we thank all the other organizers of WIFS'09 and, last but not least, the WIFS'09 Program Committee and external reviewers.

Ingemar Cox
Moti Yung

Organization Committee

General Chairs
Ingemar Cox – University College London, UK
Moti Yung – Google Inc., USA

Technical Program Chairs
Ton Kalker – Hewlett Packard Labs, USA
David Naccache – École Normale Supérieure, France

Local Arrangements Chair
Gwenaël Doërr – University College London, UK

Financial Chair
Frank Stone – University College London, UK

Tutorials Chair
Fabien Petitcolas – Microsoft Research Ltd., UK

Publications Chair
Stefan Katzenbeisser – Technische Universität Darmstadt, Germany

European Liaison
Benoit Macq – Université Catholique de Louvain, Belgium

North American Liaison
Pierre Moulin – University of Illinois Urbana–Champaign, USA

Latin American Liaison
Ricardo de Queiroz – Universidade de Brasilia, Brazil

Far East Liaison
Qibin Sun – Hewlett Packard, China

Webmaster and IT Support
Neil Marjoram – University College London, UK

About the Reviewing Process

We are pleased to announce that our call for papers has attracted over 120 submissions from 25 countries. Each manuscript has been reviewed by 3 independent reviewers. To best serve the quality of the workshop and allow attendees to benefit from all the scientific material presented at WIFS, the PC Chairs have decided to adapt the conference's logistics by turning the specialized parallel tracks into a succession of 9 sessions totalling 39 papers (30% acceptance rate), reflecting our intention to create a high quality scientific venue.

In addition to the regular technical program, IEEE WIFS will feature 3 keynote presentations delivered by renowned expert, namely David Bénichou, Bruce Schneier, and Mikko Hyppönen. On the Sunday before the start of the workshop, WIFS participants have the opportunity to choose from 4 tutorials on selected topics of Information Forensics and Security. Finally, thanks to the generosity of our financial sponsors, we are glad to announce that IEEE WIFS'09 will grant a Best Paper Award and a Best Student Paper Award during the gala dinner based on the votes of the members of the Technical Program Committee.

We trust that you will find this an exciting program.

Ton Kalker
David Naccache

Technical Program Committee

Jan Allebach – Purdue University, USA
Mauro Barni – Università di Siena, Italy
Vijayakumar Bhagavatula – Carnegie Mellon University, USA
Joseph P. Campbell – MIT Lincoln Laboratory, USA
Ingemar J. Cox – University College London, UK
Robert Cunningham – MIT Lincoln Laboratory, USA
Nora Dabbous – Ingenico, France
Ricardo de Queiroz – Universidad de Brasilia, Brazil
Edward J. Delp – Purdue University, USA
Alexander W. Dent – Royal Holloway, UK
Eric Filiol – Department of Defense, France
Jessica Fridrich – Binghamton University, USA
Renato Iannella – National ICT Australia, Australia
Anil Jain – Michigan State University, USA
Ton Kalker – Hewlett Packard Labs, USA
Stefan Katzenbeisser – Technische Universität Darmstadt, Germany
Markus Kuhn – University of Cambridge, UK
Deepa Kundur – Texas A&M University, USA
C.–C. Jay Kuo – University of Southern California, USA
Jean–Louis Lanet – University of Limoges, France
Serge Lefranc – Université Paris VII, France
Richard Lippmann – MIT Lincoln Laboratory, USA
Benoit Macq – Universite Catholique de Louvain, Belgium
Roy Maxion – Carnegie Mellon University, USA
Nasir Memon – Polytechnic Institute of NYU, USA
Fred Mintzer – IBM, USA
Pierre Moulin – University of Illinois at Urbana–Champaign, USA
David Naccache – École Normale Supérieure, France
Fabrice Pizzi – Groupe Eiffage, France
Florian Praden – École Normale Supérieure, France
Bart Preneel – Katholieke Universiteit Leuven, Belgium
Gwénaël Rouillec – Gendarmerie Nationale, France
Kazue Sako – NEC Labs, Japan
Pierangela Samarati – Università degli Studi di Milano, Italy
Andrew Senior – Google Inc., USA
Qibin Sun – Hewlett Packard, China
Jim Wayman – San Jose State University, USA
Min Wu – University of Maryland, USA
Moti Yung – Google Inc., USA

Keynote Talks

The Seven Cybercriminal Families
David Bénichou
Tribunal de Grande Instance deNanterre, France
Monday 7th December, 1.40-2.40 pm

"The seven cybercriminal families" is an empiric approach of the fight against cybercrime. Contrary to some ambitious (or frightening) classifications, this one is the result of years dealing with the reality of cybercrime, which is sometimes quite different from the archetypal representations given by non neutral actors (governments, companies). Knowing the motivations, the weaknesses, but also the strengths of real cybercriminals is the best way to give a proportional and efficient response. It is useless to be a lord on the Net, chief of an army of bots, if you're not able to cook an egg, or to shake a hand. On the other hand, traditional rude bandits need new affordable talents to invest new markets. Regarding the question of organized cybercrime, it's probably the age of disillusion: after streets, whorehouse, banks and casinos it's only a new place to make easy money for usual criminals. Hence, brilliant hackers and viruses are probably the modern figures of slavery.

The Psychology of Security
Bruce Schneier
British Telecommunications plc., UK
Tuesday 8th December, 9-10 am

Security is both a feeling and a reality. You can feel secure without actually being secure, and you can be secure even though you don't feel secure. We tend to discount the feeling in favour of the reality, but they're both important. The divergence between the two explains why we have so much security theatre, and why so many smart security solutions go unimplemented. Several different fields – behavioural economics, the psychology of decision making, evolutionary biology – shed light on how we perceive security, risk, and cost. It's only when the feeling and reality of security converge that we can make smart security trade-offs.

Fighting Organized Online Crime
Mikko Hyppönen
F-Secure, Finland
Wednesday 9th December, 9-10 am

Virus writers like we used to know them have disappeared. They have almost completely been replaced by organised and professional for-profit gangs. These gangs make millions with malware. But how does this underground economy work? How do the criminals turn malware into money? And how do they move their funds from the cyberworld into real world? Where are they from? And how exactly do they work? And, most importantly: why have we been unable to fix these problems?

Tutorials

Mobile Device Forensics
Richard Mislan (Purdue University, USA)
Sunday 6th December, 9-12 am, BT Auditorium

As ubiquitous societal components, mobile phones continue to become increasingly prevalent. With a shrinking footprint and a seemingly ever-increasing storage capacitance, these devices can be warehouses of information about our daily lives. Just as mobile phones permeate our social fabric, they are also becoming more and more crucial as evidentiary devices in civil and criminal investigations. Thus, our law enforcement, intelligence and private investigation communities are grasping for ways to get evidence off each and every mobile device. Some tools and techniques exist for such investigative work; however, there is not yet one good solution. The various manufacturers, models, operating systems, protocols, and cables lend to a combinatorial explosion that leaves most criminal investigators grasping for a cohesive solution. Through this tutorial, Professor Mislan will present the current state of Mobile Device Forensics, in all its glory!

Privacy Enhancing Technologies - Biometrics: A Case Study
Patrizio Campisi (Università degli Studi “Roma TRE”, Italy)
Sunday 6th December, 9-12 am, BT Media Suite

Privacy is one of the most critical issues that may limit the public acceptance of systems which collect, process, or produce personal information. When an individual gives out his biometrics, either willingly or unwillingly, he discloses unique information about his identity. This implies that, under some circumstances, his biometrics can be replicated for the purpose of identity theft, and misused to discriminate or profile the user for undeclared secondary purposes. Therefore the need to protect privacy arises. The purpose of this tutorial is to give an overview of both the procedural and the technological tools which can be used to deploy privacy compliant biometric based authentication systems. Specifically, the potential privacy-invasive biometric misuses are described. Some procedural approaches to deploy privacy compliant biometric applications are given. Privacy enhancing technologies are introduced: cancellable templates, biometric cryptosystems, and data hiding techniques are described in detail within the biometric framework and their pros and cons are analyzed. An overview of the major international projects on the development of privacy sympathetic biometric based authentication systems and a list of useful available online resources are eventually given.

Analysis of Encrypted Traffic

Nikita Borisov (University of Illinois at Urbana Champaign, USA)
Sunday 6th December, 2-5 pm, BT Media Suite

Security and privacy of online communications are pivotal concerns. Cryptographic tools providing essentially unbreakable encryption are now near-ubiquitous, but traffic patterns, such as packet headers, timings, and sizes, can still tell a detailed story about you even if all your data are encrypted - from a list of web sites you visit and people you correspond with to keystrokes typed on an encrypted connection and words you say on encrypted VoIP calls! I will overview the state of the art in encrypted traffic analysis, including common techniques and countermeasures and how they are used in various applications. I will also discuss some open problems and future research directions in the field.

Digital Rights Management Beyond Access Control

Teddy Furon (THOMSON Security Lab, France)
Frédéric Lefebvre (THOMSON Security Lab, France)
Gwenaël Doërr (University College London, UK)
Sunday 6th December, 2-5 pm, BT Auditorium

In the late 90's, several converging factors triggered a significant change in the entertainment industry: (i) the transition from analog copies to digital clones (copying no longer degrades the signal), (ii) the rapid development of the Internet to exchange data, and (iii) the release of efficient software tools (peer-to-peer) to "socialize" multimedia content. As a result, the entertainment industry experienced a rather drastic loss of royalties' income and it reacted by deploying protection technologies referred to as Digital Rights Management (DRM). Unfortunately, this created huge consumer frustration as early access control based DRM technologies inherently denied usages much valued by customers e.g. playing the songs/movies that you have paid for on all the devices that they own. As a result, DRM quickly became hugely controversial and there seems today to be only two exit strategies: provide interoperability between incompatible proprietary DRM systems or push DRM outside the user home.

This second choice is currently receiving increasing attention, especially in the music industry. The security primitives are no longer in the devices, but there are helping purging the networks from illegal contents or monitoring data exchange in order to accurately re-distribute royalties to artists. Such non intrusive protection technologies are commonly referred to as fingerprinting and will be fully detailed during this tutorial. Active fingerprinting refers to linking contents to consumer identities, in order to trace back dishonest users illegally re-distributing the content. Passive fingerprinting refers to extracting from contents perceptually important features so that the computer recognizes the content.

Technical Program

Monday, 7th December 2009

9h00-9h20: Welcome address

9h20-10h20: Watermarking and Perceptual Models
Chair: Mauro Barni, Università di Siena, Italy.

Rony Darazi, Pilar Callau, and Benoit Macq (Université Catholique de Louvain, Belgium) – "*Secure and HVS-Adaptive Exhibition Spread Transform Dither Modulation Watermarking for Digital Cinema*"

Abstract: In this paper, we propose a secure watermarking scheme based on Spread Transform Dither Modulation (STDM) method for Digital Cinema. The embedding is performed in the JPEG2000 decoding pipeline after the de-quantization and prior to the inverse discrete wavelet transform (IDWT). We exploit the wavelet properties related to the Human Visual System (HVS) in order to have a trade-off between Fidelity and Robustness, while preserving Security. We design a pixel-wise masking vector that modulates the spreading vector in such a way that preserves its security. Our results show that the proposed method is robust against traditional image processing attacks. The proposed scheme can also survive the camcording attack, a pre-processing step is done in the detection for this end.

Nikolaos Galatsanos (University of Ioannina, Greece) **and Antonis Mairgiotis** (University of Patras, Greece) – "*A Hierarchical Spatially Adaptive Image Model for Perceptual Mask Design and Multiplicative Watermark Detection*"

Abstract: In this work motivated by a hierarchical spatially adaptive image prior that we have developed for additive watermarking; we first, propose a new perceptual mask which improves robustness of additive watermark detectors in the spatial domain. The proposed mask is based on the local image variations along the two principal directions and enhances the watermark's energy while satisfying the imperceptibility requirement. Second we extent the application of the proposed hierarchical image prior for the multiplicative watermarking problem and we propose new watermark detectors. Numerical results are provided that demonstrate both the value of the proposed mask, and the improved sensitivity as compared to additive watermarking, with the same image model, of the proposed multiplicative watermark detector. Furthermore, we demonstrate its improved robustness compared to other state of the art similar in spirit watermark detectors.

Federica Battisti, Marco Carli, and Alessandro Neri (University of Roma TRE, Italy) – "*QIM-DM Watermarking Optimization Based on Inter-frequency Contrast Masking in the DCT Domain*"

Abstract: In this paper a watermarking scheme based on the Human Visual System (HVS) is presented. A Quantization Index Modulation - Dither Modulation scheme is used in the Discrete Cosine Transform domain for the embedding. The watermark quantization step is selected according to the inter-frequency masking effect computed by using a HVS-inspired objective image quality metric. Experimental results demonstrate the effectiveness and the robustness of the proposed solution.

10h20-10h40: Coffee break

10h40-12h00: Forensics
Chair: Edward Delp, Purdue University, USA.

Steven Simske, Margaret Sturgill, Paul Everest, and George Guillory (Hewlett-Packard Laboratories, USA) – "*A System for Forensic Analysis of Large Image Sets*"

Abstract: Counterfeiting is a major concern for brand owners. Since printing is used to convey brands, brand owners should be able to analyze images of printed areas to gauge if the printing was performed by an authentic or a counterfeit printer/label converter. In this paper, we describe a system that uses a small set of pre-classified images (either authentic or counterfeit images from the same source) for initial training, and thereafter adaptively classifies and clusters images from multiple sources as they join the population to be classified. Authentic images and multiple sources of counterfeit images are identified, and secondary links between the non-compliant samples are provided. The system currently uses a set of 420 metrics which are filtered to a smaller set of features that can reliably describe our known set. This filtered set of features, or feature signature, is used for the search and clustering thereafter. We describe the use of this system to streamline and enhance investigations for a global brand protection program.

Matthias Kirchner and Thomas Gloe (Technische Universität Dresden, Germany), "*On Resampling Detection in Re-compressed Images*"

Abstract: Resampling detection has become a standard tool in digital image forensics. This paper investigates the important case of resampling detection in re-compressed JPEG images. We show how blocking artifacts of the previous compression step can help to increase the otherwise drastically reduced detection performance in JPEG compressed images. We give a formulation on how affine transformations of JPEG compressed images affect state-of-the-art resampling detectors and derive a new efficient detection variant, which better suits this relevant detection scenario. The principal appropriateness of using JPEG pre-compression artifacts for the detection of resampling in re-compressed images is backed with experimental evidence on a large image set and for a variety of different JPEG qualities.

Aravind Mikkilineni, Deen King-Smith, Saul Gelfand, and Edward Delp (Purdue University, USA) – "*Forensic Characterization of RF Devices*"

Abstract: We present a framework for forensic identification of RF devices using specially designed probe signals. This framework applies to a broad range of devices.

Probe signals, device models, feature selection and classifier design are described, and experimental results are given to verify our approach.

Johan Garcia and Thijs Holleboom (Karlstad University, Sweden) – "*Retention of Micro-fragments in Cluster Slack – A First Model*"

Abstract: In current forensic practice it is regularly needed to determine whether some set of files have been present on a storage medium or not. File carving techniques are readily used as a tool in such examinations. However, if all clusters holding the files searched for have been overwritten, remains of the previous files only resides in the cluster slack. In this work we elaborate on the factors that influence how many such cluster slack "micro-fragments" that can be expected to be detected. We identify a set of factors that influence the micro-fragment retention characteristics. One such characteristic is the file size distribution of the files overwriting the original files. We derive analytical expressions for three different file size distributions, which allows us to examine the retention characteristics even if the overwriting files come from different sources.

12h00-13h40: Lunch break

13h40-14h40: Keynote talk #1
David Benichou, "The Seven Cybercrime Families"

14h40-15h00: Coffee break

15h00-16h40: Traitor Tracing
Chair: Antonius Kalker, Hewlett-Packard, USA.

Jose Moreira, Marcel Fernandez, and Miguel Soriano (Technical University of Catalonia, Spain) – "*A Note on the Equivalence of the Traceability Properties of Reed-Solomon Codes for Certain Coalition Sizes*"

Abstract: Fingerprinting codes are used to prevent dishonest users from redistributing copyrighted material. In this context, codes with the traceability (TA) property are of remarkable significance, since they provide an efficient way to identify traitors. Codes with the identifiable parent property (IPP) are also capable of identifying traitors, requiring less restrictive conditions than the TA codes at the expense of not having an efficient decoding algorithm, in the general case. Other codes that have been widely studied but possess a weaker traitor-tracing capability are the secure frameproof codes (SFP). It is a well-known result that TA implies IPP and IPP implies SFP. The converse is in general false. However, it has been conjectured that for Reed-Solomon codes all three properties are equivalent. In this paper we investigate this equivalence, and provide a positive answer for families of Reed-Solomon codes when the number of traitors divides the size of the code field.

Boris Skoric (Eindhoven University of Technology, The Netherlands), **Stefan Katzenbeisser** (Technische Universität Darmstadt,Germany), **Hans Georg Schaathun** (University of Surrey, UK), **and Mehmet Celik** (Civolution, The Netherlands) – "*Tardos Fingerprinting Codes in the Combined Digit Model*"

Abstract: We introduce a new attack model for collusion-secure codes, called the combined digit model, which represents signal processing attacks against the underlying watermarking level better than existing models. In this paper, we analyze the performance of two variants of the Tardos code and show that both variants can accommodate the new model and resist collusion attacks with only a modest increase in code length as compared to the results for the commonly used restricted digit model.

Luis Pérez-Freire (Gradiant, Spain) **and Teddy Furon** (Thomson Security Lab, France) – "*Blind Decoder for Binary Probabilistic Traitor Tracing Codes*"

Abstract: This paper presents a new decoder for probabilistic binary traitor tracing codes which is based on classical hypothesis testing and estimation theory. This new decoder is blind, in the sense of ignoring a priori the collusion attack it is facing. It basically performs a joint estimation of the collusion channel and the probability that each user takes part in the collusion. The experimental results shown in the paper have been obtained with the classical Tardos code, although the proposed decoder works with arbitrary probabilistic binary codes. Another remarkable advantage of this blind decoder is its ability to successfully cope with collusion channels far more general than the classical Marking Assumption, including channels that produce erasures and random decoding errors.

Yen-Wei Huang and Pierre Moulin (University of Illinois at Urbana-Champaign, USA) – "*Capacity-Achieving Fingerprint Decoding*"

Abstract: We study randomized fingerprinting codes that achieve the fundamental capacity limits subject to the so-called Boneh- Shaw marking assumption. Two decoding schemes are studied in particular: the joint decoder is capacity-achieving but computationally intense, while the simple decoder is suboptimal but efficient. We provide tight bounds as well as numerical results for capacities and study the difference between these two schemes. Finally, security strategies for both the fingerprint embedders and the collusive attackers are presented.

Teddy Furon (Thomson Security Lab, France) **and Luis Pérez-Freire** (Gradiant, Spain) – "*Worst Case Attacks Against Binary Probabilistic Traitor Tracing Codes*"

Abstract: This article deals with traitor tracing which is also known as active fingerprinting, content serialization, or user forensics. We study the impact of worst case attacks on the well-known Tardos binary probabilistic traitor tracing code, and especially its optimum setups recently advised by Amiri and Tardos, and by Huang and Moulin. This paper assesses that these optimum setups are robust in the sense that a discrepancy between the foreseen numbers of colluders and its actual value doesn't spoil the achievable rate of a joint decoder. On the other hand, this discrepancy might have a dramatic impact on a simple decoder. Since the complexity of the today's joint decoder is prohibitive, this paper mitigates the impact of the optimum setups in current realizable schemes.

Tuesday, 8th December 2009

9h00-10h00: Keynote talk #2
Bruce Schneier, “The Psychology of Security”

10h00-10h20: Coffee break

10h20-12h00: Biometry
Chair: Patrizio Campisi, Università degli Studi Roma Tre, Italy

Francesco Beritelli and Andrea Spadaccini (University of Catania, Italy) – “*Heart Sounds Quality Analysis for Automatic Cardiac Biometry Applications*”

Abstract: In this paper we propose a cardiac biometric system for human identity verification based on an automatic selection algorithm of the best subsequence of a DHS (Digital Heart Sound) signal. The quality score is based on the cepstral distance between homogeneous cardiac sounds. Performance of the algorithm proposed, expressed in terms of equal error rate, is similar to a DHS manual segmentation-based system, but offers the advantages of a fully automatic biometric application.

Takao Murakami and Kenta Takahashi (Hitachi Ltd., Japan) – “Accuracy Improvement with High Convenience in Biometric Identification using Multi-hypothesis Sequential Probability Ratio Test”

Abstract: Biometric identification has lately attracted attention because of its high convenience; it does not require a user to enter a user ID. The identification accuracy, however, degrades as the number of the enrollees increases. Although many multimodal biometric techniques have been proposed to improve the identification accuracy, it requires the user to input multiple biometric samples and makes the application less convenient. In this paper, we propose a new multimodal biometric technique that significantly reduces the number of inputs by adopting a multihypothesis sequential test that minimizes the average number of observations. The results of the experimental evaluation using the NIST BSSR1 (Biometric Score Set - Release 1) database showed its effectiveness.

Yige Wang, Shantanu Rane, and Anthony Vetro (Mitsubishi Electric Research Laboratories, USA) – “*Leveraging Reliable Bits: ECC Design Considerations for Practical Secure Biometric Systems*”

Abstract: It is well-known that a biometric fuzzy vault can be constructed by applying an error correcting code (ECC) to a biometric signal. This is attractive because authentication only requires the check bits of the ECC to be stored on the access control device, whereas the personal biometric traits need not be stored. For a given coding rate, the ECC attempts to correct the errors between an enrolment biometric and the provided probe, and authenticates if it is successful in doing so. Unfortunately, most implementations of biometric fuzzy vaults have very poor robustness to the inherent noisiness of biometric measurements. In this paper, we provide ECC design considerations for secure biometric systems, which provide both better robustness and greater security. In particular, for any feature extraction algorithm, we propose to reorder the feature bits according to their reliability, and associate the reliable bits with high-degree variable nodes in the graph of the ECC. Further, the reliability of a bit is measured at enrolment and used to initialize the ECC decoding. Experiments on an extensive database show considerable reduction in the false reject rate, while restricting the successful attack rate to a very low value.

Fokko Beekhof, Sviatoslav Voloshynovskiy, Oleksiy Koval, and Taras Holotyak (University of Geneva, Switzerland) – "*Fast Identification Algorithms for Forensic Applications*"

Abstract: In this work a novel fast search algorithm is proposed that is designed to offer improved performance in terms of identification accuracy whilst maintaining acceptable speed for forensic applications involving biometrics and Physically Unclonable Functions. A framework for forensic applications is presented, followed by a review of optimal and existing fast algorithms. We show why the new algorithm has the power to outperform the other algorithms with a theoretic analysis and confirm this using simulations on a large database.

Abhishek Nagar and Anil Jain (Michigan State University, USA) – "*On the Security of Non-invertible Fingerprint Template Transforms*"

Abstract: Many transformation functions have been proposed for generating revocable or non-invertible biometric templates. However, their security analysis either ignores the distribution of biometric features or uses inefficient feature matching. This usually leads to unrealistic estimates of security. In this paper we introduce a new measure of non-invertibility, called the Coverage-Effort (CE) curve which measures the number of guesses (Effort) required by an adversary to recover a certain fraction (Coverage) of the original biometric data. In addition to utilizing the feature distribution, the CE curve allows estimation of security against partial recovery of biometric features. We analyze the CE curves obtained using different instances of a mixture of Gaussians based feature transform for fingerprint templates. Our analysis shows that knowledge of the fingerprint minutiae distribution reduces the effort required to obtain a specified coverage.

Sviatoslav Voloshynovskiy, Oleksiy Koval, Taras Holotyak, and Fokko Beekhof (University of Geneva, Switzerland) – "*Privacy Enhancement of Common Randomness Based Authentication: Key Rate Maximized Case*"

Abstract: In this paper, we consider security-privacy issues in authentication techniques based on the extraction of common randomness. We demonstrate that the key rate-privacy leak pairs can be enhanced using reliable components extraction from specially designed random projections. The decrease of bit error probability is estimated and its impact on the key rate and privacy leak is evaluated. Several authentication schemes with new helper data protocol are proposed.

12h00-13h40: Lunch break

13h40-15h00: Privacy and Anonymity
<u>Chair:</u> David Naccache, École Normale Supérieure, France.

Mauro Barni, Pierluigi Failla (University of Siena, Italy), **Vladimir Kolesnikov** (Bell Laboratories, USA), **Riccardo Lazzeretti** (University of Siena, Italy), **Annika**

Paus, Ahmad-Reza Sadeghi, and Thomas Schneider (Ruhr-University Bochum, Germany) – "*Efficient Privacy-Preserving Classification of ECG Signals*"

Abstract: We describe a privacy-preserving system where a server can classify an ElectroCardioGram (ECG) signal without learning any information about the ECG signal and the client is prevented from gaining knowledge about the classification algorithm used by the server. The system relies on the concept of Linear Branching Programs (LBP) and a recently proposed cryptographic protocol for secure evaluation of private LBPs. We study the trade-off between signal representation accuracy and system complexity both from practical and theoretical perspective. As a result, the inputs to the system are represented with the minimum number of bits ensuring the same classification accuracy of a plain implementation. We show how the overall system complexity can be strongly reduced by modifying the original ECG classification algorithm. Two alternatives of the underlying cryptographic protocol are implemented and their corresponding complexities are analyzed to show suitability of our system in real-life applications for current and future security levels.

Zekeriya Erkin (Delft University of Technology, The Netherlands)**, Thijs Veugen** (TNO Information and Communication Technology, The Netherlands)**, Tomas Toft** (Aarhus University, Denmark)**, and Reginald L. Lagendijk** (Delft University of Technology, The Netherlands) – "*Privacy-Preserving User Clustering in a Social Network*"

Abstract: In a ubiquitously connected world, social networks are playing an important role on the Internet by allowing users to find groups of people with similar interests. The data needed to construct such networks may be considered sensitive personal information by the users, which raises privacy concerns. The problem of building social networks while user privacy is protected is hence crucial for further development of such networks. K-means clustering is widely used for clustering users in a social network. In this paper, we provide an efficient privacy-preserving variant of K-means clustering. The scenario we consider involves a server and multiple users where users need to be grouped into K clusters. In our protocol the server is not allowed to learn the individual user data and users are not allowed to learn the cluster centers. The experiments on the MovieLens dataset show that deployment of the system for real use is reasonable as its efficiency even on conventional hardware is promising.

Fabio Dellutri (University of Rome Tor Vergata, Italy)**, Luigi Laura** (Sapienza University of Rome, Italy)**, Vittorio Ottaviani, and Giuseppe F. Italiano** (University of Rome Tor Vergata) – "*Extracting Social Network from Seized Smartphones and web Data*"

Abstract: In this paper we propose an approach that allows one to get information about the social network of an individual by complementing the information provided by its (smart)phone with the data publicly available on the net. Our approach is based on a profile graph, whose nodes are the people involved and the (weighted) edges represent their mutual links. In a first phase, a preliminary version of the graph is built by using all the information available in the seized smartphone; later, the obtained graph is refined by mining publicly available data from the Web. Finally, the graph is clustered to generate cliques of people. All the phases of the process, described above, are performed by an integrated and interactive software tool, that allows the user to rapidly recover a smartphone's owner social network. Merging the information coming from the Web with the information stored on the mobile device allows to reach “clearer” results resolving homonimy problems by combining two different data sources, thus improving the precision of link weighting.

Michael Sterckx, Benedikt Gierlichs, Bart Preneel, and Ingrid Verbauwhede (K.U. Leuven, Belgium), “*Efficient Implementation of Anonymous Credentials on Java Card Smart Cards*”

Abstract: The Direct Anonymous Attestation scheme allows to map procedures with an imperative requirement for anonymity, such as voting, to the electronic world while offering provable security. However, the scheme is complex and requires demanding computations to be performed on a tamper-proof device. Such devices, e.g. secure smart cards, are typically resource constrained. We present the first implementation of the (simplified) Direct Anonymous Attestation protocols suitable for contemporary Java Card smart cards. We point out performance bottlenecks and provide efficient solutions which allow our implementation to terminate within acceptable time.

15h00-15h20: Coffee break

15h20-17h00: Content Fingerprinting
Chair: Frédéric Lefebvre, Thomson R&D, France.

Wei-Hong Chuang, Avinash Varna, and Min Wu (University of Maryland, USA) – “*Modeling and Analysis of Ordinal Ranking in Content Fingerprinting*”

Abstract: Content fingerprinting provides a compact representation of multimedia objects for copy detection. This paper analyzes the robustness of the ordinal ranking module frequently used in content fingerprinting by examining the changes in ranks as local variations are introduced in feature values. Closed-form expressions to measure such sensitivity are derived when feature values are jointly Gaussian-distributed. The results show that sensitivity depends on the strength of local variation, the total number of blocks, and the correlations among blockbased feature values. Experiments with both synthesized data and image data validate the analysis and provide interesting insights, inspiring an approach to reduce the sensitivity.

Avinash Varna and Min Wu (University of Maryland, USA) – “*Modeling Content Fingerprints using Markov Random Fields*”

Abstract: Content fingerprints are widely employed for identifying multimedia in various applications. A “fingerprint” of a video or audio is a short signature that captures unique characteristics of the signal and can be used to perform robust identification. Several fingerprinting techniques have been proposed in the literature and are often evaluated using benchmark databases. To complement these experimental evaluations, this paper develops a theoretical model for content fingerprints and evaluates the identification accuracy. Fingerprints and the noise are modeled as Markov Random Fields and the optimal decision rule for matching is derived. An algorithm to compute the probability of correct detection and the false alarm rate by estimating the density of states is described. Numerical results are provided for a model of a block based binary fingerprinting scheme and the influence of the fingerprint correlation and the noise on the detection accuracy is studied.

Mehrdad Fatourechi, Xudong Lv, Z.Jane Wang, and Rabab K. Ward (University of British Columbia, Vancouver, Canada) – "*Towards Automated Image Hashing Based on the Fast Johnson-Lindenstraus Transform (FJLT)*"

Abstract: Perceptual image hashing has become increasingly popular for copy detection and indexing in digital photography. While many researchers have focused on proposing image hashing algorithms that are robust under a variety of content preserving attacks, little attention has been paid to some of the relevant practical issues, such as estimating the parameter values for these algorithms and improving their speed. The present work addresses these concerns by automatic parameter estimation for the recently proposed Fast Johnson-Lindenstrauss Transform (FJLT) image hashing algorithm. Our simulation results using benchmark images manipulated under content-preserving operations demonstrate that the proposed algorithm finds a set of parameter values that make FJLT-based image hashing significantly faster, while achieving high performance.

Stefan Thiemert, Martin Steinebach, Stefan Nürnberger, and Sascha Zmudzinski (Fraunhofer SIT, Germany) – "*Security of Robust Audio Hashes*"

Abstract: discriminating content, e.g. for automated tracking systems and filters for file sharing networks. When they are used in security relevant applications, such as in content-fragile watermarks or for recognizing illegal content, the security of the hash value generation becomes an important issue. In this paper we discuss possible attacks on robust hash algorithms. As an example we describe a possible attack on the audio fingerprint of Haitsma et al., resulting in a different hash value while keeping the audio files perceptually similar.

18h00-23h00: Gala dinner at Guildhall

Wednesday, 9th December 2009

9h00-10h00: Keynote talk #3
Mikko Hypponen, "Fighting Organized Online Crime"

10h00-10h20: Coffee break

10h20-12h00: Watermarking, Steganography and Information Hiding
Chair: Jessica Fridrich, SUNY Binghampton, USA.

Tomas Filler and Jessica Fridrich (SUNY Binghamton, USA), "*Wet ZZW Construction for Steganography*"

Abstract: Wet paper codes are an essential tool for communication with non-shared selection channels. Inspired by the recent ZZW construction for matrix embedding, we propose a novel wet paper coding scheme with high embedding efficiency. The performance is analyzed under the assumption that wet cover elements form an i.i.d. Bernoulli sequence. Attention is paid to implementation details to minimize capacity loss in practice.

Maria V. Ortiz Segovia, George Chiu, and Jan Allebach (Purdue University, USA) – "*Using Forms for Information Hiding and Coding in Electrophotographic Documents*"

Abstract: Common forensics tasks such as verifying ownership, authenticity, and copyright of a document can be accomplished through the use of imperceptible marks or signatures inserted during the printing process. Prior research has investigated techniques to embed and recover extrinsic information from electrophotographic text documents and halftone images. But in the absence of suitable halftone patches or text characters, another strategy to embed signatures in the document is needed. In this study, the use of the frames or borders that surround the contents of security documents such as bank statements, event tickets and boarding passes is proposed. While this new embedding context broadens the embedding domain, it also offers the possibility of using error-correcting coding techniques from the area of communications. Experimental results show that the addition of coding methods to the embedding scheme improve the embedding capacity and provide more robustness to our system.

Chuhong Fei (A.U.G. Signals Ltd., Canada**), Raymond Kwong** (University of Toronto, Canada**), and Deepa Kundur** (Texas A&M University, USA) – "*Secure Semi-Fragile Watermarking for Image Authentication*"

Abstract: This paper proposes a secure semi-fragile authentication watermarking algorithm for natural images by embedding two complementary watermarks for content change analysis. Two authenticator watermarks are generated and embedded in different regions of the images: one for detecting malicious modifications and the other for estimating the degree of the changes. The proposed scheme is able to distinguish common content-preserving changes from malicious content-changing modifications. Simulations on real images demonstrate the effectiveness of the authentication watermarking scheme.

Michele Scagliola, Fernando Pérez-González (University of Vigo, Spain**), and Pietro Guccione** (Politecnico di Bari, Italy) – "*An Extended Analysis of Discrete Fourier Transform – Rational Dither Modulation for Non-white Hosts*"

Abstract: A deep analysis of discrete Fourier transform - rational dither modulation (DFT-RDM), developed to cope with linear time invariant filtering, is here presented. This study has been motivated by the significant increase of the error probability suffered by DFT-RDM for non-white hosts, in spite of the low bit-error rate achieved for white hosts under the same attack filter. The theoretical analysis of DFT-RDM has been generalized to non-white Gaussian hosts providing an explanation to the measured performance degradation. Afterwards an extension of DFT-RDM, named Whitened DFT-RDM, is proposed to achieve the same bit-error rates for white and non-white Gaussian hosts. Experimental results are also presented that validate the developed analysis and illustrate the performance enhancement provided by the proposed extension of DFT-RDM, with both non-white Gaussian signals and real audio clips.

Matthew Gaubatz and Steven Simske (Hewlett-Packard, Co., USA), "*Printer-Scanner Identification via Analysis of Structured Security Deterrents*"

Abstract: Device identification, the ability to discern the (separate) devices by which a document was produced and/or imaged, can be leveraged in the design of quality assurance (QA) systems as well as the practice of forensic analysis. It is shown that QA metrics associated with printed security markings provide a useful approach for performing multiple device identification, i.e., printer-scanner identification. While some previous methods have focused on properties of sensors to extract signatures from general image data, the proposed approach leverages the highly structured nature of color tile deterrents to predict device (combination) signatures based on a limited amount of information. Constraints introduced by the deterrent structure yield a relatively simple classification strategy with strong performance using a 10-dimensional feature vector. Sixteen printer-scanner combinations (composed from 4 printers and 4 scanners) are tested using this method. Results illustrate device signature prediction performance that is competitive with current state-of-the-art approaches based on physical models of the devices involved.

12h00-13h40: Lunch break

13h40-15h00: Device Identification
Chair: Ingemar Cox, University College London, United Kingdom.

Tian-Tsong Ng (Institute for Infocomm Research, Singapore) **and Mao-Pei Tsui** (University of Toledo, USA) – "*Camera Response Function Signature for Digital Forensics – Part I: Theory and Data Selection*"

Abstract: Camera response function (CRF) is a form of camera signatures which can be extracted from a single image and provides a natural basis for image forensics. CRF extraction from a single-image is in theory ill-posed. It relies on specific structures in an image that offer glimpses of the CRF. Therefore, the challenges in CRF extraction are first in identifying structures of such property, second in locating such structures in an image, and third in extracting the CRF attributes from the selected structures. In our past work, we proposed that CRF attributes can be found on linear structures in an image and extracted using linear geometric invariants. In this paper, we show additional properties on linear geometric invariants, propose a more robust way to select linear structures in an image, and provide a model-based method to extract CRF attributes from the linear structures. This paper is divided into two parts. Part I is devoted to the theory of linear geometric invariants and the robust selection of linear structures. The linear structure candidates obtained from the method in Part I are used to instantiate the edge profiles for CRF extraction in Part II. The paper as a whole presents a reliable method for CRF extraction, together with rigorous analysis which gives useful insights into the method. In the first half of Part I, a simpler proof that links the equality of linear geometric invariants to a linear-isophote surface is given. As a by-product, the proof leads to an additional way to detect linear-isophote surfaces which uses only the first-order partial derivatives and improves detection reliability. In the second half of Part I, the variance of linear geometric invariants is shown to have a structure which can be used to improve the robustness in detecting linear-isophote surfaces.

Tian-Tsong Ng (Institute for Infocomm Research, Singapore) – "Camera Response Function Signature for Digital Forensics – Part II: Signature Extraction"

Abstract: Part I of this two-part paper proposed a robust way to detect local points on linear-isophote surface in an image. Only a subset of these points corresponds to linear surface in image irradiance and provides useful information about the camera response function (CRF). In Part II, we show that, for some images, this subset of linear points could constitute a very small portion of the candidate set and the remaining points are often considered as noise. Our previous approach was to eliminate the noise using a learning-based method. The learning-based method could only reduce the noise but not eliminate it completely. Hence, it fails when the proportion of linear points is too small. As a main contribution in Part II, we introduce the concept of edge profile and consider the candidate points as discrete samples of an edge profile. Instead of eliminating the unwanted candidate points as noise, we use them to instantiate the edge profiles. Assuming that every edge profile has a linear component in image irradiance, the interactions of the edge profiles in the space of linear geometric invariants may correspond to the linear part which is CRF-indicating. Such a model is shown to be sound and effective in both simulation images and real camera images.

Nitin Khanna and Edward J. Delp (Purdue University, USA) – "*Source Scanner Identification for Scanned Documents*"

Abstract: Recently there has been a great deal of interest using features intrinsic to a data-generating sensor for the purpose of source identification. Numerous methods have been proposed for different problems related to digital image forensics. The goal of our work is to identify the scanner used for generating a scanned (digital) version of a printed (hard-copy) document. In this paper we describe the use of texture analysis to identify the scanner used to scan a text document. The efficacy of our proposed method is also demonstrated.

Gökhan Gül (University of Kiel, Germany) **and İsmail Avcıbaş** (Başkent University, Turkey) – "*Source Cell Phone Identification Based on Singular Value Decomposition*"

Abstract: Micro and macro statistical features based on Singular Value Decomposition (SVD) have been proposed for source cell-phone identification. The performance of the proposed features is evaluated with naïve and informed classifiers for the identification of original images as well as images under several manipulations. The results have been compared to the state-of-the-art and it has been observed that SVD based features are comparable to their counterparts in the literature at reduced complexity.

15h00-15h20: Coffee break

15h20-16h40: Cryptography and Protocols
Chair: Stefan Katzenbeisser, TU Darmstadt, Germany.

Tiziano Bianchi (Università di Firenze, Italy)**, Thijs Veugen** (TNO Information and Communication Technology, The Netherlands)**, Alessandro Piva** (Università di Firenze, Italy)**, and Mauro Barni** (Università di Siena, Italy) – "*Processing in the Encrypted Domain using a Composite Signal Representation: Pros and Cons*"

Abstract: The current solutions for secure processing in the encrypted domain are usually based on homomorphic cryptosystems operating on very large algebraic structures. Recently, a composite signal representation has been proposed that allows to speed up linear operations on encrypted signals via parallel processing and to reduce the size of the encrypted signals. Though many of the most common signal processing operations can be applied to composite signals, some operations require to process the signal samples independently from each other, thus requiring an unpacking of the composite signals. In this paper, we will address the above issues, showing both merits and limits of the composite signal representation when applied in practical scenarios. A secure protocol for converting an encrypted composite representation into the encryptions of the single signal samples will be introduced. A case study clearly highlights pros and cons of using the composite signal representation in the proposed scenarios.

Kevin Bauer, Damon McCoy, Dirk Grunwald, and Douglas Sicker (University of Colorado, USA), "*BitStalker: Accurately and Efficiently Monitoring BitTorrent Swarms*"

Abstract: BitTorrent is currently the most popular peer-to-peer network for file sharing. However, experience has shown that Bit-Torrent is often used to distribute copyright protected movie and music files illegally. Consequently, copyright enforcement agencies currently monitor BitTorrent swarms to identify users participating in the illegal distribution of copyright protected files. These investigations rely on passive methods that are prone to a variety of errors, particularly false positive identification. To mitigate the potential for false positive peer identification, we investigate the feasibility of using active methods to monitor extremely large BitTorrent swarms. We develop an active probing framework called BitStalker that identifies active peers and collects concrete forensic evidence that they were involved in sharing a particular file. We evaluate the effectiveness of this approach through a measurement study with real, large torrents consisting of over 186,000 peers. We find that the current investigative methods produce at least 11% false positives, while we show that false positives are rare with our active approach.

Julien Bringer, Hervé Chabanne (Sagem Sécurité, France**), Gérard Cohen, and Bruno Kindarji** (Telecom ParisTech, France) – "*RFID Key Establishment Against Active Adversaries*"

Abstract: We present a method to strengthen a very low cost solution for key agreement between RFID devices. Starting from a work which exploits the inherent noise on the communication link to establish a key by public discussion, we show how to protect this agreement against active adversaries. For that purpose, we unravel integrity (I)-codes suggested by Cagalj et al. No preliminary key distribution is required.

Benedikt Gierlichs, Elke De Mulder, Bart Preneel, and Ingrid Verbauwhede (K.U. Leuven, Belgium) – "*Practical DPA Attacks on MDPL*"

Abstract: There exist only two articles that present clear results of practical DPA attacks against an MDPL prototype chip and both are essentially in favour of its security. Unsuccessful attacks are however only weak evidence of security, and at present it is unclear to what extent some proposed theoretical concepts affect the security provided by MDPL in practice. We fill this gap and present results of an extensive case study of attacks against an MDPL prototype chip. In contrast with other practical works, we demonstrate successful DPA attacks and show that MDPL implementations, resistant to standard DPA attacks, can be broken in practice. Further, we show that the underlying concept of the folding attack, i.e. analysis of probability densities, indeed exposes MDPL's greatest weakness: the masking renders the circuit more vulnerable to attacks than a circuit with a fixed mask. In addition, our analysis leads to novel insights into the power consumption properties of MDPL in real silicon.

16h40-17h00: Farewell address

Gala Dinner

As the home of the City of London, Guildhall has been the centre of City government since the Middle Ages. The word 'guildhall' is said to derive from the Anglo-Saxon 'gild' meaning payment, so it was probably a place where citizens would pay their taxes. The present Guildhall was begun in 1411 and, having survived both the Great Fire of London and the Blitz, it is the only secular stone structure dating from before 1666 still standing in the City.

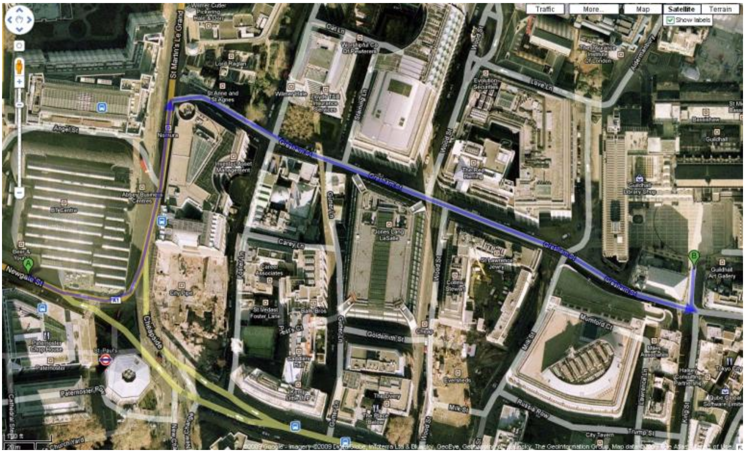
It is likely that at least one earlier guildhall existed on or near the current site. References to a London guildhall are made in a document dating back to 1128 and the current hall's west crypt is thought to be part of a late-13th century building. Remains of a long-lost Roman amphitheatre discovered in 1987 underneath what is now Guildhall Yard indicate that the site of Guildhall was significant as far back as Roman times.

The Great Hall is the third largest civic hall in England, where royalty and state visitors have been entertained down the centuries. It has been the setting for famous state trials, including that of Lady Jane Grey in 1553. The imposing medieval hall has stained glass windows and several monuments to national heroes including Admiral Lord Nelson, the Duke of Wellington and Sir Winston Churchill.

IEEE WIFS 2009 banquet will be hold in the East and West Crypts, which lie beneath Guildhall, and are the largest medieval crypts in London. The East Crypt is the oldest part of Guildhall, dating back to Edward the Confessor (1042) and is considered to be one of the earliest and one of the finest examples of its kind in England. The stained glass windows depict Geoffrey Chaucer, William Caxton, Sir Thomas More, Sir Christopher Wren and Samuel Pepys. The West Crypt was built in the 12th century and would have originally been the ground floor of the building. After the Great Fire of London in 1666, it completely collapsed and was sealed; after extensive restoration it was opened again in 1973. Six clusters of circular columns in Purbeck marble support a fine groined roof, comprising stone, chalk and bricks, the principle intersections being covered with carved bosses of heads, shields, and flowers.

Address: Guildhall, Gresham Street, London, EC2
Date: Tuesday 8th December 2009
Time: 6-9 pm
Dress code: Business casual
Directions:

1. Exit BT building and turn left towards the tube station
2. At the crossing, turn left onto St Martin's Le Grand
3. Take the first right onto Gresham Street
4. The 5th street on your left should lead you to Guildhall through the Art Gallery entrance



Financial Supporters

The organizers would like to express their deepest thanks to the various organizations which supported IEEE WIFS'09 in London in one way or the other. The event would not have been possible without their help.

Hosted by
BT

ingenico®

EUROPEAN OFFICE of AEROSPACE R&D

Digital Communications
Knowledge Transfer Network

hp®

THOMSON