1st Luxembourg-Polish Workshop on Security and Trust

LPWST'2010

May 6-7, 2010
Castle of Bourglinster, Luxembourg

http://lpwst2010.uni.lu

Program

Day 1 (6th of May)

08h00 Registration of the participants

09h00 Opening session: short introduction by the officials from the University of Luxembourg, Polish Academy of Sciences and Warsaw University of Technology

09h20 Invited speakers

Mrs. Barbara Labuda, Polish Ambassador in Luxembourg
Mr. Germain Dondelinger, Commissaire du Gouvernement

10h00 Coffee break

10h30 Session 1: Information Security Management

Peter Ryan: *Security and Trust in Voting Systems*
Wojciech Mazurczyk and Krzysztof Szczypiorski: *Information Hiding in Communication Protocols: Network Steganography*
Ralph-Phillipp Weinmann: *On Temporal Memory Errors*
Christoph Schommer: *Data Mining in Security Applications*

12h15 Lunch

14h00 Session 2: Cryptography and Privacy I

Alex Biryukov and Ivica Nikolic: *Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others*
Miroslaw Szaban and Franciszek Seredynski: *Constructing Cellular Automata - based S-boxes*
Sjouke Mauw, Sasa Radomirovic and Mohammad Torabi Dashti: *Minimal message complexity of asynchronous multi-party contract signing*
Hugo Junker and Jun Pang: *Quantifying Voter-controlled Privacy*

15h40 Coffee Break

16h00 Session 3: Protocol & Model Checking

Wojtek Jamroga: *Markov Temporal Logic*
Ton van Deursen and Sasa Radomirovic: *On the non-compositionality of untraceable RFID protocols*
Wojciech Penczek: *Model Checking of (Timed) Security Protocols*
Miroslaw Kurkowski*: Verifying (Timed) Security Protocols with VerICS*

20h00 Gala dinner (Mansfeld Restaurant**)**

Day 2 (7th of May)

09h00 Session 4: Cryptography and Privacy II

Franck Leprévost: *Rational torsion points of Jacobians of modular-like genus 2 curves*
Andrzej Paszkiewicz: *On properties and applications of special types irreducible polynomials over small finite fields*
Guillaume Aucher: *Privacy policies with dynamic logic*

10h15 Coffee break

10h45 Session 5: Network Security

Zbigniew Kotulski, Bogdan Księżopolski, Pawel Szałachowski: *Calculating security metrics for security protocols: a proof of concept*
Marek Ostaszewski*: On Capturing Vital Properties of Denial of Service Attacks Using Metaheuristic Approaches*
Jaroslaw Skaruz and Franciszek Seredynski: *Tracking Intruders in Web Application*

12h00 Lunch

14h00 Session 6: Trust, Reputation and Security Assessment

Eugen Staab: *Reliable Information Acquisition in the Presence of Attackers*
Christoph Schommer and Jayanta Poray: *Recommending Trust in Conversational Streams By Explorative Mind-Maps*
Barbara Kordy and Patrick Schweitzer: *Attack-Defense Trees*

15h20 Closing session

18h00 Debriefing session involving the heads of the involved institutions on the future collaboration (4 persons). Visit of Luxembourg by the remaining participants

Abstracts

Session 1: Information security management

Security and Trust in Voting Systems

By: Peter Ryan (UL).

In this talk I discuss the security requirements and threats in voting systems. I present some schemes that strive to provide a high degree of ballot privacy and verifiability with minimal trust assumptions, in particular the Pret a Voter and Pretty Good Democracy schemes. I will also discuss issues concerning voter understanding of and confidence in such security mechanisms.

Information Hiding in Communication Protocols: Network Steganography

By: Krzysztof Szczypiorski and Wojciech Mazurczyk (WUT).

The main aim of network steganography is to hide secret data inside users' normal data transmissions, ideally so it can't be detected by third parties.

One of the most popular steganographic techniques is to use a covert channel, which offers an opportunity to "manipulate certain properties of the communications medium in an unexpected, unconventional, or unforeseen way, in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel," to quote Wikipedia.

Covert channels may be dangerous to company networks as they can lead to the leakage of confidential information. However, it is hard to assess what bandwidth of a covert channel poses a serious threat. Generally, it depends on the security policy that is implemented by the organisation concerned. The ideal case will be to eliminate all possibilities of hidden communication, but practically it is not possible as the number of steganographic techniques is high and still growing rapidly.

The presentation will give a general overview in this area and will be a chance to present algorithms proposed by Network Security Group (secgroup.pl) from Warsaw University of Technology, Poland.

On Temporal Memory Errors

By: Ralf-philipp weinmann (UL).

A Memory corruption that can be controlled by an attacker can be considered one of the most powerful outcomes of a security-relevant bug. Static analysis and model checking has facilitated the automatic detection and subsequent elimination of large classes of programming errors causing memory corruption, such as buffer overflows. Together with mitigations for stack and heap overflows, these spatial memory errors - one of the dominant classes of security problems in the 1990s - have become almost extinct.

Although both classes of memory errors - spatial and temporal - have been known since the 1960s, bugs of the latter kind have remained unexploited until very recently. This talk looks at why the popularity for temporal memory errors is picking up and what can be done to detect them.

Data Mining in Security Applications

By: Christophe Schommer (UL).

Since many years, the efficiency and potential behind Data Mining stimulates the hope of detecting hidden but useful findings in masses of data. The explorative nature of Data Mining is highly attractive but quite ambitious, since a series of process steps like a data quality assurance, the analytical planning, and the interpretation of relevant information must be performed until any kind of deployment can be started. Just like statistical (verificative) approaches, Data Mining depends on the nature of data (``if nothing is in the data then we can not find anything'') but even stringently necessitates the presence of human analysts having expert knowledge in the application domain.

Altogether, Data Mining is a very potential discipline regarding its application in one of the today's important areas: security. Many analytical performances and achievements exist since years - for example forensic linguistics, detection and characterisation of computer network intruders and spies, risk analysis, plagiarism, and so forth -, and some others have become quite popular, like for example data privacy issues or the combat of terrorist activities.

With respect to this, the talk gives a brief overview of existing security-related directions and discusses several business scenarios that base on a real customer project. We concern with telephone premium calls with costs, which are for example technical hotlines, advices for insurance or juridical questions, or phone sex, and will come up with examples for phone connections indicating phone addiction, conspiracy, and conspiracy using automated devices. We present a software solution that supports the raise of a suspicion by the presence of abnormality with quarterly ad-hoc disclosures and that has been successfully applied with BAFIN, the Federal Financial Supervisory Authority of Germany. Finally, we deal with real data from the State Office of Criminal Investigation / Free State of Saxony and make some analytical ``mining runs'' to demonstrate the potential of Data Mining.

Session 2: Cryptography and Privacy I

Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others

By: Alex Biryukov and Ivica Nikolic (UL).

While differential behavior of modern ciphers in a single secret key scenario is relatively well understood, and simple techniques for computation of security lower bounds are readily available, the security of modern block ciphers against related-key attacks is still very ad hoc. We make a first step towards provable security of block ciphers against related-key attacks by presenting an efficient search tool for finding differential characteristics both in the state and in the key (note that due to similarities between block ciphers and hash functions such tool will be useful in analysis of hash functions as well). We use this tool to search for the best possible (in terms of the number of rounds) related-key differential characteristics in AES, byte-Camellia, Khazad, FOX, and Anubis. We show the best related-key differential characteristics for 5, 11, and 14 rounds of AES-128, AES-192, and AES-256 respectively. We use the optimal differential characteristics to design the best related-key and chosen key attacks on AES-128 (7 out of 10 rounds), AES-192 (full 12 rounds), byte-Camellia (full 18 rounds) and Khazad (7 and 8 out of 8 rounds). We also show that ciphers FOX and Anubis have no related-key attacks on more than 4-5 rounds.

Constructing Cellular Automata – based S-boxes

By: Miroslaw Szaban and Franciszek Seredynski (IPIPAN).

Substitution and permutation boxes are based elements of many block ciphers, but in Feistel approach of block cipher, the S-boxes are most important. S-boxes are tools of nonlinear transformation of information in the cipher process. Classical S-boxes are usually represented by specially designed tables, which are used today in current cryptographic standards, such as DES - an example of Feistel cipher, or Rijndael -AES example of S-P network algorithm. As the result of developing cryptanalysis methods current ciphers do not ensure enough safety of ciphers. Therefore, the open research issue now is to design new more sophisticated classes of S-boxes and it is performed with use of many methods. In this paper we present a concept of S-boxes based on cellular automata (CA-based S-boxes). An exhaustive experimental analysis of the proposed CA-based S-boxes in terms of non-linearity, autocorrelation, balance and strict avalanche criterion shows that CA-based S-boxes have cryptographic properties comparable or better than the classical S-box tables. The interesting feature of the proposed S-boxes is a dynamic structure, fully functionally realized by a simple CA, while the classical S-boxes are represented by predefined fixed table structures requesting predefined sizes of memory.

Minimal message complexity of asynchronous multi-party contract signing

By: Sjouke Mauw, Sasa Radomirovic, Mohammad Torabi Dashti (UL).

Multi-party contract signing protocols specify how a number of signers can cooperate in achieving a fully signed contract, even in the presence of dishonest signers. This problem has been studied in different settings, yielding solutions of varying complexity. Here we assume the presence of a trusted third party that will be contacted only in case of a conflict, asynchronous communication, and a total ordering of the protocol steps.

Our goal is to develop a lower bound on the number of messages in such a protocol. Using the notion of abort chaining, a specific type of attack on fairness of signing protocols, we derive the lower bound n^2 + 1, with n>2 being the number of signers involved. We obtain the lower bound by relating the problem of developing fair signing protocols to the open combinatorial problem of finding shortest permutation sequences. This relation also indicates a way to construct signing protocols which are shorter than state-of-the-art protocols. We illustrate our approach by presenting the shortest three-party fair contract signing protocol.

Quantifying voter-controlled privacy voting

By: Hugo Jonker and Jun Pang (UL).

Privacy is a necessary requirement for voting. Without privacy, voters can be forced to vote in specific ways, and the forcing party can check their compliance. But offering privacy does not suffice: if a voter can reduce her privacy, an attacker can force her to do so. We introduce the notion of choice groups as a measure of privacy, and provide formal definitions. We illustrate how this notion can be used to better understand privacy concerns in voting systems, and how the notion of choice groups is formalised to quantify privacy. By combining this with models of various degrees of voter collaboration, we can quantify the privacy under a voter's control.

Session 3: Protocol & Model Checking

Markov Temporal Logic

By: Wojtek Jamroga (UL).

Most models of agents and multi-agent systems include information about possible states of the system (that defines relations between states and their external characteristics), and information about relationships between states. Qualitative models of this kind assign no numerical measures to these relationships. At the same time, quantitative models assume that the relationships are measurable, and provide numerical information about the degrees of relations. We explore the analogies between qualitative and quantitative models of agents, and propose a multi-valued logic for reasoning about what agents can expect to enforce. We also suggest in what way the logic can be used for specification of security-related properties.

On the non-compositionality of untraceable RFID protocols

By: Ton van Deursen and Sasa Radomirovic (UL).

It is well known that protocols that satisfy a secrecy or authentication property when executed in isolation do not necessarily satisfy the same property when they are executed in an environment containing other protocols. We show that the same is true for a privacy property known as untraceability. We demonstrate this fact on a family of recently proposed RFID protocols by Lee, Batina, and Verbauwhede. We invalidate the authentication and untraceability claims made for several of the family's protocols.

We also present man-in-the-middle attacks on untraceability in all of the protocols in the family. Similar attacks can be carried out on some other protocols in the literature, as well.

Finally, we briefly indicate how to repair the protocols.

Verifying (Timed) Security Protocols with VerICS

By: Miroslaw Kurkowski and Wojciech Penczek (IPIPAN).

Automated verification of cryptographic protocols is a very active and important area of computer science, which has been an object of an intensive research for several years in both academic and commercial institutions. Algorithmic approaches include mainly methods based on model checking. Intuitively, model checking of a cryptographic protocol consists in checking whether a model of the protocol contains an execution or a reachable state that is representing an attack on the protocol.

In the talk we will propose two new methodologies for verifying untimed and timed security protocols.

The main idea of the first approach consists in using networks of synchronized (timed) automata for modelling the executions of a protocol and separately the knowledge of the participants about the secrets used. Thanks to that we develope a very distributed representation of a participant behaviour in protocol executions, which is crucial for an efficient symbolic encoding and model checking. We show several experimental results obtained using the toolkit VerICS.

The second approach uses a formalism for the automatic verification of security protocols based on multi-agent systems semantics. We give syntax and semantics of a temporal-epistemic security-specialised logic and provide a lazy-intruder model for the protocol rules that is arguably particularly suitable for verification purposes. We exemplify the technique by finding a (known) bug in the traditional NSPK protocol.

Session 4: Cryptography and Privacy II

Rational torsion points of Jacobians of modular-like genus 2 curves

By: Franck Leprévost (UL).

The security of many public-key protocols, like e.g. the Diffie-Hellman Key Exchange Protocol, relies on the difficulty to solve in practice some discrete logarithm problem (DLP). Such a DLP can be expressed in any cyclic finite group G. It turns out that the group of rational points of elliptic curves defined over a finite field leads to appropriate groups G. Beyond elliptic curves, Jacobians of curves of higher genus are nowadays also used for public-key purposes (either constructive, or destructive). Among these curves, some moreover have a rich arithmetic meaning: modular curves. They are used in cryptology, in error-coding theory, in the construction of very rare quadratic fields, in Fermat's last theorem, etc. We consider here a specific modular curve, $X_0(23)$, and construct other genus 2 curves sharing one of its arithmetic properties: their Jacobians all have a rational point of order 11, and generalize $X_0(23)$ in some specific sense.

On properties and applications of special types of irreductible polynomials over small finite fields

By: Andrzej Paszkiewicz (WUT).

In my presentation I shall focus on three types of sparse irreducible polynomials over finite fields called trinomials, pentanomials and lexicographically youngest polynomials. By *t*-nomial we mean a monic polynomial with exactly *t* non-zero coefficients. It will be addressed the methodology of testing irreducibility of such polynomials up to high degrees and applications to fast arithmetic over finite fields dedicated for hardware solutions. For practical testing we developed a programming package which deals with polynomials having their degrees up to one hundred millions. It runs well on “ordinary” office PC computers and is between 2 to 6 times faster than the popular software package with C++ code written by Victor Shoup.

With the aid of our package we were able to enlarge existing tables of irreducible trinomials, and pentanomials. By the occasion we corrected existing tables published by Gao, Howell and Panario, and we disproved a (plausible) hypothesis by von zur Gathen which concerns the so called sedimentary polynomials. We also observed an interesting fact that the number of pentanomials over GF(2) has its growth rate very close to a quadratic function of its degree. It also will be discussed some questions concerning statistical behavior of that polynomials in a bit larger finite fields up to GF(17).

Privacy policies with dynamic logic

By: Guillaume Aucher (UL).

Privacy policies are often defined in terms of permitted messages. Instead, in this talk we derive dynamically the permitted messages from static privacy policies defined in terms of permitted and obligatory knowledge. With this new approach, we do not have to specify the permissions and prohibitions of all message combinations explicitly. To specify and reason about such privacy policies, we extend a multi-modal logic introduced by Cuppens and Demolombe with update operators modeling the dynamics of both knowledge and privacy policies. We show also how to determine the obligatory messages, how to express epistemic norms, and how to check whether a situation is compliant with respect to a privacy policy. We axiomatize and prove the decidability of the modal logic.

Session 5: Network Security

Calculating security metrics for security protocols: a proof of concept

By: Zbigniew Kotulski, Bogdan Księżopolski, Pawel Szałachowski (WUT).

Historically, the Internet was created as a network for honest users. Threats and a need of protection came out later, together with expansion of the Internet into real life. Therefore, the countermeasures applied against threats are often ad-hoc and, what it follows, overestimated and inflexible when external conditions are changing. Thus, the Future Generation Internet needs a different, more systematical approach to network security.

One of the most important task to guarantee an adequate protection in the Internet is the skill of comparing security levels (required and provided) or measuring the security level. In this paper we propose a method of expressing the security level by numbers enabling comparing the level of protection for different countermeasures applied. First, we propose a simple mathematical model for calculating the security level of a security protocol. Next, we present a computer tool (called SPOT - the Security Protocol Optimizing Tool) making easier studying all security elements applied in the numerical model and in the protocol. Finally, we give an example of application of the model to optimization of some network security protocol.

On Capturing Vital Properties of Denial of Service Attacks Using Metaheuristic Approaches

By: Marek Ostaszewski (UL).

The Internet takes part of daily activities both professional and personal of roughly 25% of the population on Earth. One of the mechanisms responsible for security of information over the Internet are Intrusion Detection Systems (IDSs), which detect attempts of accessing or corrupting unauthorized data (attacks). Certain group of attacks is oriented on blocking the legitimate user from accessing authorized data over network by generating artificial traffic that by sheer volume saturate the communication link. They are called Distributed Denial of Service (DDoS) attacks and pose particular problem to IDSs. The amount of data to analyze, variability of attack patterns and similarity to regular traffic render classical IDS approaches ineffective.

Our work focuses on the problem of analysis of DDoS properties in order to effectively manage the attack traffic. A dynamic clustering method based on some metaheuristics is applied to the network traffic following the changes of trends and focussing on traffic repetitiveness, the inherent property of DDoS. The clusters parameters are transformed into time series and passed to a search method. This evolutionary-based algorithm is oriented on finding classification functions that minimize the number of incorrectly classified instances in the input data. Single and multi-objective approaches are considered. The latter offers important possibility of choosing the most suited classifier set adapted to the profile of the analyzed traffic.

Tracking Intruders in Web Application

By: Jaroslaw Skaruz and Franciszek Seredynski (IPIPAN).

In the paper we present intrusion detection system based on application of two different nature inspired algorithms: recurrent neural networks (RNN) and Gene Expression Programming (GEP). The objective of the system is anomaly detection in web application caused by intruders performing SQL attacks. SQL attacks are those attacks that take the advantage of using SQL statements to break into the web application. The problem of detection of this class of attacks is transformed to two problems: time series prediction and classification. SQL queries are used as a source of events in a protected environment. To differentiate between normal SQL queries and those sent by an attacker, we divide SQL statements into tokens and pass them to our detection system based on recurrent neural network (RNN), which predicts the next token, taking into account previously seen tokens. In the learning phase tokens are passed to a RNN trained by backpropagation through time (BPTT) algorithm. Then, two coefficients of a rule are evaluated. The rule is used to interpret RNN output. In the testing phase RNN with the rule is examined against attacks and legal data to find out how evaluated rule affects efficiency of detecting attacks. False alarms rate of this method of detecting intruders is compared with the results obtained from GEP performing classification task between normal and misuse SQL queries. RNN with the classification rule outperforms GEP. For statements constituted from 9 to 19 tokens average false alarm rate of RNN is about 5% while GEP misclassification equals to 13%.

Session 6: Trust, Reputation and Security Assessment

Reliable Information Acquisition in the Presence of Attackers

By: Eugen Staab (UL).

In distributed systems in which autonomous entities exchange information with each other, these entities have the freedom to provide incorrect information. This becomes especially relevant in scenarios where entities have incentives to do so, e.g., in peer-to-peer networks or volunteer computing systems. Cryptographic mechanisms can help to ensure data integrity and authenticity. However, while these mechanisms achieve a reliable transmission of information, they do not prevent the creation of incorrect information in the first place. Therefore, additional mechanisms are necessary to enable an entity to assess the correctness of acquired information. The main problem here is that in many cases the explicit verification of acquired information is infeasible, for instance due to high costs. In this talk, we present different generic approaches that help to ensure the correctness of information in this situation: a spot-checking mechanism, a trust model and a collusion detection mechanism.

Recommending Trust in Conversational Streams By Explorative Mind-Maps

By: Christoph Schommer and Jayanta Poray (UL).

In the presence of a natural conversation, we propose an explorative-adaptive-associative mind-map system to recommender trust for each conversing partner. An explorative mind-map is a simulation of the human mind and altogether a management framework that emerges automatically from the data signals it gets. It is a non-verificative but dynamic system that changes its complexity continuously and that fosters on symbolic cells according to internal activation states. Generally, the structure mirrors a mental state where the oblivion of associated facts arrive once the stimulation decreases. Consider now k mind-maps for each of the conversational partner where one mind-map represents the own contribution to a conversation and k-1 mind-maps an own belief about each conversational partner, respectively, our hypothesis is that a merge of someone's own mind-map with each conversing (partner) mind-map will support the computation of trust or distrust, depending on the computed distance value.

Attack-Defense Trees

By: Barbara Kordy (UL).

Security assessment of complex systems is a standard but suboptimal procedure due to its informal nature. While a formal approach would be desirable, but out of reach, a systematic approach would be beneficial and feasible. Attack trees, introduced by Schneier and formalized by Mauw and Ooostdijk, are a well--known methodology to describe the possible security weaknesses of a system. An attack tree basically consists of a description of an attacker's goals and their refinement into sub-goals.

In order to provide an excellent systematic and practical security assessment methodology we extend attack trees with defense nodes. These nodes allow us to represent countermeasures that a defender can employ to prevent given attack components. Therefore, we define attack--defense trees (ADT) where nodes of both types --- attack or defense --- may appear at any level of the tree.

In this work, we provide a formal basis for attack--defense trees. We present their syntax and discuss possible semantics. We also investigate interesting properties of ADTs, and show how to analyze an attack/defense scenario by using attributes.

Misc information

Location

The 1st Luxembourg-Polish Workshop on Security and Trust will be held in the conference room of the Castle of Bourlinster:

Castle of Bourlinster
8, rue du Chateau
L-6162 Bourglinster
Phone: +352 78 78 781

The lunches and coffee breaks will take place in the castle.

To reach the castle, several possibilities:

- **By car**: 15 minutes car drive from Kirchberg campus:
  - [Motorway A1/E44 direction Trier, take exit 8]
  - Motorway A7/E29 direction Ettelbruck/Echternach
  - Take exit 1, turn right direction Echternach/Junglinster
  - In Gonderange, take direction Bourglinster

- **By public transport**: (21 minutes from Hamilius)
  - Bus line 100 (direction Larochette, Bleech)
  - Bus stop: "Bourglinster, Am Duerf"
  - From here, reach the castle (8 rue du chateau – on the left in the following map)

Gala Dinner

A gala dinner is organized on May 6th, 2010 at 20h00 in the Brasserie Mansfeld, located in Luxembourg:

Brasserie Mansfeld (Club restaurant)
3, rue de la Tour Jacob
L-1831 LUXEMBOURG - CLAUSEN

Phone: +352 43 90 11

Question? Remarks?

Do not hesitate to contact us for more information:

lpwst-2010@lists.gforge.uni.lu