

C6 Systems and Network Security Doctoral Workshop

Time: Friday, 17.09.2010

Location: Humboldt-Building, Lecture Room 204

Chairmen: W. Kühnhauser, G. Schäfer (DE-Ilmenau)

9:00 a.m.	S. Malipatlolla, S. A. Huss (DE-Darmstadt)
<p>A Novel Technique for FPGA IP Protection</p> <p>The configuration data sequence of a field programmable gate array (FPGA) is an intellectual property (IP) of the original designer. With the increase in deployment of FPGAs in modern embedded systems, the IP protection of FPGA hardware designs has become a necessary requirement for many IP vendors. There have been already many proposals to overcome this problem using symmetric encryption techniques but these methods need a cryptographic key to be stored in a non-volatile memory located on FPGA or in a battery-backed RAM (Random Access Memory) as done in some of the current FPGAs. The expenses with the proposed methods are, occupation of larger area on FPGA in the former case and limited lifetime of the device in the latter. In contrast, we propose a novel method which combines the dynamic partial reconfiguration (dynamic PR) feature of an SRAM-based FPGA with the public key cryptography (PKC) to protect the FPGA configuration files without the need to store any keys on FPGA. Using our method, not only the high-end FPGAs but also the low-end FPGAs with partial reconfiguration capabilities are secured. The proposed method has been implemented on a Xilinx Virtex-5 FPGA platform.</p>	
9:20 a.m.	M. Meichau (DE-Ilmenau); S. Steinbrecher, St. Groß (DE-Dresden)
<p>JASON: A Scalable Reputation System for the Semantic Web</p> <p>The recent development of the Internet, especially the expanding use of social software and dynamic content generation commonly termed as Web 2.0 enables users to find information about almost every possible topic on the Web. On the downside, it becomes more and more difficult to decide which information can be trusted in. In this paper we propose the enhancement of Web 2.0 by a scalable and secure cross-platform reputation system that takes into account a user's social network. Our proposed solution Jason is based on standard methods of the semantic web and does not need a central entity. It enables the fast and flexible evaluation of arbitrary content on the World Wide Web. In contrast to many other reputation systems it provides mechanisms to ensure the authenticity of web content, thus, enabling the user to explicitly choose information published by trusted authors.</p>	

9:40 a.m.	R. Schmidt (DE-Eching); G. Schäfer (DE-Ilmenau)
-----------	---

Towards Efficient Resource Management for Vehicle-to-Vehicle Communications

Reliability is one of the key requirements for Intervehicle communication in order to improve safety in road traffic. This paper describes the difficulties of Intervehicle communication being under high load. We focus on an analysis of the state-of-the art MAC protocol IEEE P802.11p and its limitations. With a simple model based on signal propagation and Signal-to-Interference ratio, we determine the theoretic reduction of the communication range. We further determine the network capacity which provides a quantification of the situation of high load on the channel. In a simulation experiment, we highlight that severe packet loss can occur. The communication range can be reduced by up to 90%. It is common trend to handle this problem by controlling the load on the channel in a decentralized manner. A common load metric, e.g. the channel busy time, is the key input parameter. We evaluate the correlation between the channel load metric and the actual reduction of the transmission range on average and in the worst case.

10:20 – 10:40 a.m. Coffee break
--

Secure Multicast in Internet-wide VPN

As more and more sensitive communication takes place over the Internet, security becomes a major objective in many areas. This leads to an extensive deployment of virtual private networks (VPNs) providing a cheap alternative to traditional dedicated lines by allowing private communications over public infrastructures. Despite being standardized for more than a decade, there is no efficient solution for distributed group communications in these scenarios. Network load increases equally to the number of participants as data has to be transmitted individually for every single recipient, leading to a waste of bandwidth and higher latency. Existing application-level multicast approaches have to deal with poor topologies, limited performance, and insufficient reliability as the VPN is not aware of the additional overlay and consequently cannot optimize it. Additionally, multiple multicast streams can lead to overloaded links as end-user applications can influence routing decisions only insufficiently. However, group communications are rather important in order to allow efficient distribution of video messages, audio streams and software updates.

Thus, realizing group communications by transparent IP-multicast is a major challenge for dynamic VPN overlay services. Even though transferring the traditional peer-to-peer push approach to a VPN-based multicast overlay seems a straightforward approach, interesting detail problems occur, i.e., additional topology control mechanisms are needed to ensure good security and reliability properties. Our system, called STORM, is realizing a transparent, single-source multicast distribution tree for IP-multicast with the help of a number of distributed algorithms. It is able to rate nodes based on their age to efficiently integrate mobile nodes and make attacks on the availability more sophisticated. Further metrics like delay, bandwidth, and hop count can be considered to construct and optimize efficient topologies. Moreover, tree balancing will occur to reduce latency and improve reliability as well as resilience against random failures or specific attacks.

11:00 a.m.	R. Golembewski (DE-Ilmenau)
------------	-----------------------------

DoS resistant Distributed Time Synchronisation for Virtual Private Networks

Time synchronicity is an important basis for many processes in modern IT infrastructures. Digital signing of messages and temporary user tickets in a Kerberos environment are two examples, where synchronized clocks are desired. Focussing on designing an algorithm with robustness against attackers, any hierarchical or centralized approach must be disregarded. The most popular mechanism for the use in wired IP networks is the Network Time Protocol (NTP) [Mills, 2006] with a possible deployment in global scenarios. Apart from that, several synchronization methods exist for local area networks, like dedicated cluster heartbeat infrastructures. The last-mentioned mostly making a use of MAC-Layer access for a preferably high accuracy. Also distributed algorithms sometimes using a hierarchical structure for propagating the synchronization data. Thus, a denial-of-service (DoS) attack is possible by compromising nodes, that act as an initiator, or nodes with a high number of children. Therefore, a solution for this problem must be a fully distributed approach without any hierarchical needs. Inside of a VPN infrastructure, some important security goals are realized inherently. Communicating nodes are authenticated against each other and the transfer of data is confidential and integer. This is a big advantage over other use cases, because of the impossibility of attacks like modification, eavesdropping or replaying. In this paper, we describe a new distributed approach for a secure time synchronization method without DoS vulnerabilities. The NTP-Protocol can be used to ensure the global synchronicity between VPN and surrounding. Even if no NTP-Server is available, the synchronization of all inner nodes is guaranteed. Furthermore, we will show the ability to adapt the node's local clock-drift to the network, what results in a stable behaviour in the case of a temporarily partitioned scenario, where no communication between the separated subnets is possible. Several attacker models (internal and external) are used to evaluate the robustness of the algorithm. Simulation results and realtime measurements are proving the ability to defend external delay attacks, as well as the robustness against a certain percentage of internal attackers.

12:00 noon – 1:30 p.m. Lunch

End of Lecture Session
