

C6 Systems and Network Security Doctoral Workshop

Time: Thursday, 16.09.2010

Location: Humboldt-Building, Lecture Room 204

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

1:30 p.m.	A. Fischer, W. Kühnhauser (DE-Ilmenau)
Causal Trusted Computing Bases Today's trusted computing base (TCB) designs are guided by seeking generality to support a wide variety of security policies. As such they are powerful general-purpose TCBs, and implementing them inevitably leads to complex implementations. Consequently, correctness, robustness and tamperproofness of a TCB's implementation are quite hard to verify. If a TCB is a set of functions required to enforce and protect a system's security policies, TCBs by definition only contain functions required by the system's security policies and thus provide minimal functionality. Applying this definition, however, poses the problem to exactly identify causal dependencies between security policies and TCB functions. In this idea paper we present a research concept that specifies causal dependencies between security policies and TCB functions and properties, aiming at reducing the size and complexity of a TCB's implementation. Our approach leads to a functionally scalable TCB design that allows for causal dependency analyses. As a result, we establish a promising breeding ground for analysing the correctness, robustness and tamperproofness of a TCB's implementation.	
1:50 p.m.	F. Girlich, M. Rossberg, G. Schäfer, Th. Böhme, J. Schreyer (DE-Ilmenau)
Scrubbing the Vivaldi network Coordinate System Over the last years network coordinate systems have gained much attention as they allow for an elegant estimation of distances between peer-to-peer endsystems. Most prominent representative of these approaches is Vivaldi, which is using a mass-spring-damper system to embed peers in a two-dimensional euclidean coordinate space with an additional height coordinate to model access delays to the core network. In unimpaired overlay networks this simple method leads to a good approximation of pairwise delays. Unfortunately, like most distributed algorithms, Vivaldi is likely to suffer from byzantine failures and several attack methods and countermeasures have been proposed. In this paper we present several novel issues and countermeasures, and in particular examine an attack method to exploit violations of the triangle inequality.	

2:10 p.m.	S. Wozniak, T. Gerlach, G. Schäfer (DE-Ilmenau)
-----------	---

Secure Multi-hop Localization in Wireless Ad Hoc Networks

Wireless Ad Hoc Networks offer a wide variety of possible applications in the context of sensor networks ranging from environmental monitoring to intrusion detection and battlefield surveillance. An important service for these applications is the precise and accurate localization of the participants. Equipping each node with GPS is often considered an expensive and impractical approach. Thus the problem of localizing sensors using only a small fraction of anchor or beacon nodes, which are aware of their location, has gained much attention from researchers in the past decade. Many schemes assume cooperative behavior among the nodes to achieve localization. Since many applications require the deployment of nodes in an adversarial environment, the problem of providing secure and robust localization has led to a variety of mechanisms aiming at either preventing the attacker from disturbing the process of localization, detecting and repairing such intervention or using robust statistical methods like least median of squares to offer graceful degradation in the face of an attack. Yet most approaches require single-hop communication between nodes and anchors to conduct distance measurements using received signal strength indicator, time of arrival or time difference of arrival. In contrast, multi-hop schemes require only a small amount of anchor nodes for localization. Such mechanisms often provide a rough estimation by flooding the location of the anchor nodes into the network. Nodes receiving this information forward it to their neighbors while either incrementing a hop counter or summing up distance measurements along the path. With participants receiving the location and distance to at least three anchor nodes, they are able to estimate their own location. The nodes subsequently refine this estimate by iteratively exchanging locations and distance measurements with their direct neighbors. Despite their promising nature, not much effort has been made in the past to secure multi-hop localization schemes. This work identifies objectives to be fulfilled by multi-hop based mechanisms aiming to provide secure localization and analyzes strengths and possible weaknesses of existing approaches regarding these objectives.

2:50 – 3:10 p.m. Coffee break

3:10 p.m.	I. Muhammad, K. Panitzek, M. Mühlhäuser, Th. Strufe (DE-Darmstadt)
<p>First Thoughts on a Secure and Reliable Peer-To-Peer Service Platform</p> <p>Harnessing the P2P paradigm to provide a distributed service platform for the implementation of online social networks, IPTV, emergency first response systems, multi-player online games, or especially cloud computing platforms raises novel security challenges. Critical resources have to be allocated and shared in a decentralised manner in all these applications. P2P systems, though inherently robust to churn, generally are not resilient to adverse behaviour. Yet, it is paramount to guarantee fair use and especially to make them immune to internal as well as external adversaries. In this paper we outline our future research directions to ensure security and reliability of P2P service platforms, in dynamic as well as hostile environments. Our focus lies on the challenge to guarantee fair and reliable load balancing while keeping the services available and secure.</p>	
3:30 p.m.	M. Trapp, G. Schäfer, M. Fischer (DE-Ilmenau)
<p>Heterogeneity in Peer-to-Peer Live-Streaming</p> <p>Application Layer Multicast (ALM) has become a popular form of content distribution, due to its inherent scalability properties and the overcoming of the client-server-bottleneck. Content is distributed from a source to a large number of peers by utilizing their resources for redistributing the stream to other peers. So, the system can grow independently from the source's upload bandwidth. Caused by an increasing availability of high-speed radio communication (eg. 3G or LTE), a large fraction of devices, taking part in future ALM systems, will be mobile and hence not as stable as stationary ones (eg. breakdown of the radio connection). These devices make use of various access technologies at once and will be highly heterogeneous in their available bandwidth. So, a vertical handover can have huge impact on a peer's ability to forward content. After analyzing current mobility protocols and finding no suitable approach, we developed an integrated approach to handle mobility and node heterogeneity within an ALM system that can preserve the operability of the system even in a worst-case scenario with high mobility load.</p>	

3:50 p.m.	M. Fischer (DE-Ilmenau)
<p>IPTV - The Case for Peer-to-Peer Live-Streaming</p> <p>Internet Protocol Television (IPTV) is becoming more and more popular and will burden future networks heavily with traffic, especially if deployed with a classic client-server-like approach. Besides, it does not scale. Application Layer Multicast (ALM) and its Peer-to-Peer (P2P)-like content distribution is a promising technology to overcome the bottleneck of client-server and to relieve core networks from redundant transmissions. Nevertheless, since relying on unreliable end-users, ALM systems are more susceptible to node churn and DoS attacks, so that appropriate countermeasures and a careful system design are required. We describe the architecture of an IPTV system based on ALM, present a formal IPTV model and summarize several research challenges in such a scenario. Our system is intended to optimally adapt its resources to a changing user behaviour and to build topologies that are efficient and robust at the same time by minimizing reconstruction costs caused by changes in the user compound.</p>	
End of Lecture Session	