Informatik-Oberseminar

Rheinisch-Westfälische Technische Hochschule Aachen
Lehrstuhl für Informatik IV

RWTH

EINLADUNG

Zeit:	Freitag, 9. Juli 2010, 14.00 Uhr
Ort:	Hörsaal AH 6, Ahornstr. 55
Referent:	Andriy Panchenko, M.Sc.
Thema:	Anonymous Communication in the Age of the Internet

Privacy on the Internet is becoming a concern as an already significant and ever growing part of our daily activities is carried out online. While cryptography can be used to protect the integrity and confidentiality of contents of communication, everyone along the route on which a packet is traveling can still observe the addresses of the respective communication parties. This often is enough to uniquely identify persons participating in a communication. Anonymous communication is used to hide relationships between the communicating parties. These relationships as well as patterns of communication can often be as revealing as their content. Hence, anonymity is a key technology needed to retain privacy in communications.

We first present the design and evaluation of a novel lightweight anonymization protocol based purely on open standards. It significantly outperforms other existing approaches for anonymization while only slightly sacrificing the level of provided protection. We next propose and analyze an innovative approach for scalable distribution of information about anonymization networks. It has security properties similar to a centralized directory, but scales gracefully and does not require to trust any third party. We use analytical models and simulations to validate our approach. We then consider performance issues of anonymization networks. To this end we develop and evaluate path selection metrics for performance-improved onion routing. The results show that applying our methods, users can obtain a significant increase in performance without harming their anonymity. Alternatively, users can get a dramatic performance boost with little sacrifice in anonymity. We provide a practical approach to empirically analyze the strength of anonymity different methods of path selection provide in comparison to each other. Finally, we investigate several attacks against anonymous communication systems. Most notably, we present the traffic analysis attack against encrypted HTTP streams sent through different anonymizers with surprising results showing the effectiveness and ease of website identification in encrypted channels transfered through the commonly used anonymizers. Moreover, we show under which condition and how innocent-looking application layer data can be used to speed up traditional attacks that are targeted at the network layer identification of a users' peer partners. We also propose and briefly discuss different countermeasures hampering these attacks.

Es laden ein: Die Dozenten der Informatik