Dan Forsberg

Topic 1
Distributed Authentication, Authorization, and Accounting (AAA)

Description:

Generally AAA servers reside in a centralized location of an administrative domain and AAA procedures require contacting the AAA server. For a distributed, more scalable, and faster network access authentication and authorization, one could think that AAA should also be distributed.
- What are the problems when distributing AAA?
- How existing AAA architectures address the scalability problem? Accounting can be left for further study.

One affecting factor on the AAA system design is the ability to store user preferences and user profiles. Centralized system supports this nicely as the profile is stored in one place, but in a distributed system this is more difficult.

Goal:

Resulting paper describing the problems related to decentralization of AAA. Paper describes how the existing solutions address the AAA scalability by localizing and/or distributing the AAA process. Find out state-of-the-art of the current distributed AAA mechanisms, both not supporting and supporting user profiles. Good comparison between them.

Suitability of the topic:

Student should know different kinds of authentication (and Authorization) mechanisms and protocols in high level (like Public Key, userid+passwd, Kerberos etc.). Demanding, as there are not many direct references.

Papers/links:

Wei Liang; Wenye Wang, "A local authentication control scheme based on AAA architecture in wireless networks," Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, vol.7, no.pp. 5276-5280 Vol. 7, 26-29 Sept. 2004 URL:
 http://ieeexplore.ieee.org/iel5/9623/30416/01405108.pdf?isnumber=30416"=STD&arnumber=1405108&arnumber=1405108&arSt=+5276&ared=+5280+Vol.+7&arAuthor=Wei+Liang%3B+Wenye+Wang

(Quintet handling in UMTS-AKA) 3GPP Technical Specification 3GPP TS 33.102, "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 4)", 3rd Generation Partnership Project, December 2001.

Topic 2
Attacks against peer-to-peer (P2P) networks and countermeasures

Description:

p2p (peer-to-peer) networks have become popular because of their
nature to store data in a distributed manner. However, one needs
to think that what prevents an attacker adding/deleting data on
the p2p network as well as providing false answers for other p2p
network nodes.
        - Find out different kinds of attacks and countermeasures
          identified for p2p networks.

Goal:

Goal is to find out typical attacks against p2p networks and
state-of-the-art countermeasures for securing p2p network
protocols and data against attackers.

Suitability of the topic:

Student should be familiar with p2p protocols and protocol
security.

Papers/links:

Naoum Naoumov, Keith Ross, "Exploiting P2P systems for DdoS
attacks", ACM International Conference Proceeding Series; Vol. 152
URL: http://doi.acm.org/10.1145/1146847.1146894

Dimitri DeFigueiredo, Antonio Garcia, and Bill Kramer, "Analysis
of Peer-to-Peer Network Security using Gnutella", URL:
http://www.cs.berkeley.edu/~daw/teaching/cs261-
f02/reports/defig.pdf#search=%22p2p%20network%20security%22