AAA Protocol, Network Remote Access, and Directory Services

Parts of this lecture’s notes were adapted from Wikipedia’s “AAA Protocol” (http://en.wikipedia.org/wiki/AAA_protocol) and “Directory Service” (http://en.wikipedia.org/wiki/Directory_services).

1. AAA

In computer security, AAA commonly stands for authentication, authorization, and accounting. It refers to a security architecture for distributed systems that enables control over which users are allowed access to which services and that keeps tabs on how much of the resources they have used. Two network protocols providing this functionality are particularly popular: the RADIUS protocol and its newer Diameter counterpart.

Authentication refers to the process where an entity’s identity is authenticated, typically by providing evidence that it holds a specific digital identity, such as an identifier and the corresponding credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, digital signatures, and phone numbers (calling/called).

The authorization function determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions, for example: time-of-day restrictions, physical location restrictions, or restrictions against multiple access by the same entity or user. Typical authorization in everyday computer life might be, for example, to grant reading access to a specific file for an authenticated user. Examples of types of service include but are not limited to: IP address filtering, address assignment, route assignment, quality of service/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.

Accounting refers to the tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, and billing. In addition, it may record events like authentication and authorization failures as well as audit functionality, verifying that correct procedures were carried out based on accounting data. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user or other entity, the nature of the service delivered, when the service began and when it ended, and if there is a status to report.

AAA servers in CDMA data networks are entities that provide Internet Protocol (IP) functionality to support the functions of authentication, authorization, and accounting. Types of AAA servers include the following:
- **Access Network AAA (AN-AAA):** Communicates with the RNC in the Access Network (AN) to enable authentication and authorization functions to be performed at the AN. The interface between AN and AN-AAA is known as the A12 interface;
- **Broker AAA (B-AAA):** Acts as an intermediary to proxy AAA traffic between roaming partner networks (i.e., between the H-AAA server in the home network and V-AAA server in the serving network). B-AAA servers are used in CRX networks and enable CRX providers to offer billing settlement functions;
- **Home AAA (H-AAA):** The AAA server in the roamer’s home network. The H-AAA is similar to the HLR in voice. The H-AAA stores user profile information, responds to authentication requests, and collects accounting information; and
- **Visited AAA (V-AAA):** The AAA server in the visited network from which a roamer is receiving service. The V-AAA in the serving network communicates with the H-AAA in a roamer’s home network. Authentication requests and accounting information are forwarded by the V-AAA to the H-AAA, either directly or through a B-AAA.

Current AAA servers communicate using the RADIUS protocol. A detailed discussion of the RADIUS protocol can be found at Wikipedia [RADIUS](http://en.wikipedia.org/wiki/RADIUS). As such, TIA specifications refer to AAA servers as RADIUS servers. However, future AAA servers are expected to use a successor protocol to RADIUS known as Diameter. The behavior of RADIUS AAA servers in the CDMA2000 wireless IP network is specified in TIA-835.

Other common AAA protocols are Terminal Access Controller Access-Control System (TACACS) and Terminal Access Controller Access-Control System Plus (TACACS+). TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS is defined in RFC 1492 and uses either TCP or UDP port 49 by default. A later version of TACACS, introduced by Cisco in 1990, was called Extended TACACS, or XTACACS. The XTACACS protocol was developed by and is proprietary to Cisco Systems. TACACS+ is a revision of TACACS.

Cisco Systems began supporting TACACS in its networking products in the late 1980s, eventually adding their own extensions to the protocol, which the company then called XTACACS, or extended TACACS. In the simple, non-extended form, Cisco’s implementation was compatible with the original TACACS, while the extended form – XTACACS – was not. The protocol continued to evolve over the following years and in 1996 became what Cisco called TACACS+, in which the individual tasks of authentication, authorization, and accounting were separate processes. Also, while the XTACACS and TACACS use UDP port 49, TACACS+ uses TCP port 49. TACACS+ uses the TCP protocol and encrypts the entire packet except the header.

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon, or simply TACACSD. This server was normally a program running on a host. The host would
determine whether to accept or deny the request and send a response back. The TIP, or routing node accepting dial-up line connections, which the user would normally want to log into, would then allow access or not based upon the response. In this way, the process of making the decision is opened up and the algorithms and data used to make the decision are under the complete control of whoever is running the TACACS daemon.

TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Some administrators recommend using TACACS+ because TCP is seen as a more reliable protocol. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates the two operations.

2. Directory Service and LDAP

A directory service is the software system that stores, organizes, and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, a name in a directory may be associated with multiple pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Directories may be very narrow in scope, supporting only a small set of node types and data types; or they may be very broad, supporting an arbitrary or extensible set of types. In a telephone directory, the nodes are names and the data items are telephone numbers. In the DNS, the nodes are domain names and the data items are IP addresses (and alias, mail server names, etc.). In a directory used by a network operating system, the nodes represent resources that are managed by the OS, including users, computers, printers, and other shared resources. Many different directory services have been used since the advent of the Internet, but this article focuses mainly on those that have descended from the X.500 directory service.

A simple directory service called a naming service, maps the names of network resources to their respective network addresses. With the name service type of directory, a user doesn’t have to remember the physical address of a network resource; providing a name will locate the resource. Each resource on the network is considered an object on the directory server. Information about a particular resource is stored as attributes of that object. Information within objects can be made secure so that only users with the available permissions are able to access it. More sophisticated directories are designed with namespaces as Subscribers, Services, Devices, Entitlements, Preferences, Content, and so on. This design process is highly related to identity management.
A directory service defines the namespace for the network. A namespace in this context is the term that is used to hold one or more objects as named entries. The directory design process normally has a set of rules that determine how network resources are named and identified. The rules specify that the names be unique and unambiguous. In the X.500 directory service standards and the LDAP, the name is called the Distinguished Name (DN) and is used to refer to a collection of attributes – Relative Distinguished Names (RDNs) – which make up the name of a directory entry.

A directory service is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. A directory service is an important component of an NOS (Network Operating System). In the more complex cases, a directory service is the central information repository for a Service Delivery Platform. For example, looking up “computers” using a directory service might yield a list of available computers and information for accessing them.

Replication and distribution have very distinct meanings in the design and management of a directory service. The term replication is used to indicate that the same directory namespace – the same objects – are copied to another directory server for redundancy and throughput reasons. The replicated namespace is governed by the same authority. The term distribution is used to indicate that multiple directory servers holding different namespaces are interconnected to form a distributed directory service. Each distinct namespace can be governed by different authorities.

**Comparison with Relational Databases**

There are a number of things that distinguish a traditional directory service from a typical relational database. Of course there are exceptions, but in general:

- directory information is read more often than it is written, which makes features related to transactions and rollback less important; and
- data can be redundant if it helps performance.

Directory schemas are defined as object classes, attributes, name bindings, and knowledge (namespaces), with the following properties:

- some attributes are mandatory (called must), and each of the object classes must have values for them;
- some attributes are optional (called may), and they can be defined for one instance but can be omitted with the absence treated somewhat like NULL in a relational database;
- some attributes are multi-valued allowing multiple naming attributes at one level, such as machine type and serial number concatenated or multiple phone numbers for “work phone”;
• attributes and object classes are standardized throughout the industry and formally registered with the IANA for their object ID. Therefore, directory applications seek to reuse much of the standard classes and attributes to maximize the benefit of existing directory server software;
• object instances are slotted into namespaces – that is, each object class inherits from its parent object class (and ultimately from the root of the hierarchy) adding attributes to the must/may list; and
• directory services are often a central component in the security design of an IT system and have a correspondingly fine granularity regarding access control – who may operate in which manner on what information.

Directory services were part of an Open Systems Interconnection (OSI) initiative to get everyone in the industry in agreement on common network standards to provide multi-vendor interoperability. In the 1980s, the ITU and ISO came up with a set of standards – X.500 – for directory services, initially to support the requirements of inter-carrier electronic messaging and network name lookup. The Lightweight Directory Access Protocol, LDAP, is based on the directory information services of X.500, but uses the TCP/IP stack and a string encoding scheme of the X.500 protocol DAP, giving it more relevance on the Internet.

There have been numerous forms of directory service implementations from different vendors. Systems developed before the advent of X.500 include:

• Domain Name System (DNS): the first directory service on the Internet, which is still used everywhere today;
• Hesiod: based on DNS and used at MIT’s Project Athena;
• Network Information Service (NIS): originally named Yellow Pages (YP), Sun Microsystems’ implementation of a directory service for Unix network environments, which served a similar role as Hesiod;
• NetInfo: developed by NeXT in the late 1980s for NEXTSTEP. After being acquired by Apple, it was released as open source and used as the directory service for Mac OS X before being deprecated in favor of the LDAP-based Open Directory. Support for NetInfo was completely removed with the release of 10.5 Leopard;
• Banyan VINES: the first scalable directory services offering;
• NT Domains: developed by Microsoft to provide directory services for Windows machines prior to the release of the LDAP-based Active Directory in Windows 2000. Windows Vista continues to support NT Domains but only after relaxing the minimum authentication protocols it supports; and
• Windows Registry.

LDAP Implementations

Among the LDAP/X.500 based implementations are the following:
- **Active Directory**: Microsoft’s modern directory service for Windows, originating from the X.500 directory it created for use in Exchange Server, first shipped with Windows 2000 Server and supported by successive versions of Windows;
- **eDirectory**: Novell’s implementation of directory services, which supports multiple architectures including Windows, NetWare, Linux, and several flavors of Unix and has long been used for user administration, configuration management, and software management. eDirectory has evolved into a central component in a broader range of identity management products. It was previously known as Novell Directory Services;
- **Red Hat Directory Server**: Red Hat released a directory service that it acquired from AOL’s Netscape Security Solutions unit as a commercial product running on top of Red Hat Enterprise Linux called Red Hat Directory Server and as the community supported 389 Directory Server project;
- **eNitiatives ViewDS Directory Server**: originally developed by Telstra Research Laboratories (previously Telecom Australia) in Clayton, Victoria, Australia as an X.500 Directory server known as View500 to run online White & Yellow Pages services. ViewDS was acquired by eNitiatives in 2000. It differs from other X.500 Directory products in that it has a built-in indexing engine capable of indexing all attributes and also supports a range of different types of searching and matching of entries, such as word matching, stem matching, synonym matching, acronym matching, component matching, misspelling matching, and sounds like matching. This matching is available in multiple languages, including Pinyin and Traditional Mandarin. ViewDS is LDAPv3 compliant and is also the world’s first directory to support the XACML standard for Policy Based Access control onto all attributes stored in the directory, with an inbuilt combined Policy Decision Point (PDP) and Policy Information Point (PIP) as well as two Policy Administration Tools (PAPs). ViewDS is also CCEB ACP133EdD (Military) and IATA ATN-AMHS standards compliant and supports the storage of XML objects, data, and schema in the directory using the draft IETF XML Enabled Directory standard. It also supports SPMLv2.0, DSMLv2, and SCIM 1.0. ViewDS is widely used in the government, aviation, health, and defense sectors;
- **Open Directory**: Apple’s Mac OS X Server uses a directory service named Open Directory, which implements LDAP using a customized build of OpenLDAP and integrates support for both SASL and Kerberos authentication. It uses plugin architecture to work with other LDAPv3 directories, including proprietary solutions like Active Directory and eDirectory;
- **Apache Directory Server**: Apache Software Foundation offers a directory service called ApacheDS;
- **Oracle Internet Directory (OID)**: Oracle Corporation’s directory service, which is compatible with LDAP version 3;
- **CA Directory**: CA Directory contains a pre-caching engine that can index all attributes used in LDAP search filters and cache all attributes returned in search results;
• Alcatel-Lucent Directory Server: CTIA 2009 4G - Service Creation & Development Award Winner offering enhanced performance, high availability, and proven efficiencies;
• Sun Java System Directory Server: Sun Microsystems’ current directory service offering;
• OpenDS: an open source directory service implementation from scratch in Java, backed by Sun Microsystems;
• IBM Tivoli Directory Server: a customized build of an old release of OpenLDAP;
• DirX Directory Server: from Atos, ex-Siemens software;
• Windows NT Directory Services (NTDS): later renamed Active Directory, replaces the former NT Domain system;
• Critical Path Directory Server;
• OpenLDAP: derived from the original University of Michigan reference LDAP implementation (as are the Netscape/Red Hat/Fedora/Sun JSDS servers) but significantly evolved. It supports all current computer architectures, including Unix and Unix derivatives, Linux, Windows, z/OS, and a variety of embedded/realtime systems;
• Isode Limited: high performance and high availability LDAP and X.500 servers;
• Lotus Domino; and
• Nexor Directory.

There are also plenty of open-source tools to create directory services, including OpenLDAP and the Kerberos protocol, and Samba software which can act as a Windows Domain Controller with Kerberos and LDAP backends. Administration is done using GOsa or Samba provided SWAT. More discussion on LDAP can be found at Wikipedia [LDAP](http://en.wikipedia.org/wiki/LDAP).