

AUTHENTICATING UNIX/LINUX USERS USING ACTIVE DIRECTORY 2008

Neil Waybright

Presented to UUASC

12/4/2008

About Me...

I am an SE at a large storage system vendor

In a recent previous life I managed the UNIX team at a Ventura County company that is the largest biotech company in the world. During that time we moved a large portion of our production, test, and development UNIX systems (RHEL, Solaris 8+) to AD authentication

Agenda

- ▣ Authentication
- ▣ How is that different from authorization?
- ▣ Why use directory services at all?
- ▣ Why Active Directory?
- ▣ Why 2008?
- ▣ Why use Kerberos for authentication?
- ▣ Why not for authorization?
- ▣ Why use LDAP for authorization?
- ▣ Service credentials
- ▣ **SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism)**

Authentication

- ▣ From Greek: *αυθεντικός*; real or genuine
- ▣ In this context refers to verifying the identity of an individual at the computer
- ▣ In computer security shorthand notation authentication is known as A1, AuthN, or Au
- ▣ Many argue it is not entirely possible to perfectly identify the user in front of a computer without error (too easy to cheat in practice)

Authentication Factors (1)

- ▣ Factors are generally classified into three classes (in the order of strength of allocation:
 - **the application factors:** Something that *is applied*, for example to a vehicle the applicant individual drives (e.g., a license plate, an RFID label or an active token up to the quality of an automatically operating cell phone).

Authentication Factors (2)

- **the ownership factors:** Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)

Authentication Factors (3)

- the **knowledge factors**: Something the user **knows** (e.g., a password, pass phrase, or personal identification number (PIN))
- the **inherence factors**: Something the user **is or does** (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier).

More Authentication Factors

- ▣ Additionally other authentication factors include for example these categories:
 - Social networking or
 - A *web of trust* forming relationships between authentication credentials
 - *Location-based authentication*, such as that employed by credit card companies to ensure a card is not being used in two places at once.
 - *Time-based authentication*, such as only allowing access during normal working hours.

Caveats on Authentication Factors

- ▣ Normally such additional authentication factors apply with individuals in conjunction with physically carried authentication factors

How is that different from authorization?

- ▣ The authorization process is used to decide if person, program or device X is allowed to have access to data, functionality or service Y.
- ▣ The authentication process is usually a necessary first step and is used as input to the authorization process.
- ▣ Authorization is not a simple question like “Is this Fred?”, but embodies much more complex questions like “Which files can this Fred read?”
- ▣ In formal notation is known as A2, AuthZ, Az

Why use directory services at all?

- ▣ We usually have more than one computer
- ▣ We usually want the same protections applied everywhere
- ▣ We want to make sure no system gets overlooked, even if it were out of commission when a change is made
- ▣ Must avoid “lost updates”
- ▣ Auditability
- ▣ Etc., etc., etc....

Why Active Directory?

- ▣ Because we have to have it for other reasons (windows environment)
- ▣ Robust replication
- ▣ DR built in
- ▣ Very good performance (in general)
- ▣ Easy to find staff familiar with AD
- ▣ Training, books, articles readily available
- ▣ Auditors understand it fairly well

Why 2008?

- ▣ Server core (Look Ma! No GUI!)
- ▣ Reduced attack surface
- ▣ Active Directory Light-Weight Directory Services (AD LDS)
- ▣ Power Shell

We need a solution

Operating
Systems

R. Stockton Gaines
Editor

Using Encryption for Authentication in Large Networks of Computers

Roger M. Needham and
Michael D. Schroeder
Xerox Palo Alto Research Center

Use of encryption to achieve authenticated communication in computer networks is discussed. Example protocols are presented for the establishment of authenticated connections, for the management of authenticated mail, and for signature verification and document integrity guarantee. Both conventional and public-key encryption algorithms are considered as the basis for protocols.

Key Words and Phrases: encryption, security, authentication, networks, protocols, public-key cryptosystems, data encryption standard

CR Categories: 3.81, 4.31, 4.35

In 1978 Roger Needham and Michael Schroeder gave us one (props to Lowe for his 1995 paper on an attack that needed addressing

Why use Kerberos for authentication?

- ▣ Kerberos solves a really hard problem very well
 - Authenticating a user against a centralized directory with a minimum of trust of any component in between
 - Standards-based with no royalties
 - Thoroughly studied by academics and carefully analyzed by a large number of “eyes”
- ▣ Several of the authors were available for hire by MS

Generating a Keytab

- ▣ Create a new computer account in the domain (must specify as pre-2000 computer to get a properly formed keytab)
- ▣ On the AD controller run:
 - ▣ `ktpass -princ HOST/fqdn@REALM -mapuser DOMAIN\name$ -crypto DES-CBC-MD5 +DesOnly -pass password -ptype KRB5_NT_SRV_HST -out filename`
- ▣ Securely copy to UNIX host computer and copy to `/etc/krb5.keytab` (`/etc/krb5/krb5.keytab` on Solaris) mode 0600

Creating a /etc/krb5.conf

```
1. [logging]                                example.com
2. default =                                14. # }
   FILE:/var/log/krb5libs.log
3. kdc =                                     15. [domain_realm]
   FILE:/var/log/krb5kdc.log
4. admin_server =                           16. .example.com = EXAMPLE.COM
   FILE:/var/log/kadmind.log
5. [libdefaults]                             17. example.com = EXAMPLE.COM
6. default_realm = EXAMPLE.COM
7. dns_lookup_realm = true
8. dns_lookup_kdc = true
9. #[realms]
10. # EXAMPLE.COM = {
11. # kdc = host.example.com:88
12. # admin_server =
   host.example.com:749
13. # default_domain =
```

```
example.com
14. # }
15. [domain_realm]
16. .example.com = EXAMPLE.COM
17. example.com = EXAMPLE.COM
18. [kdc]
19. profile =
   /var/kerberos/krb5kdc/kdc.co
   nf
20. [appdefaults]
21. pam = { debug = false
22. ticket_lifetime = 36000
23. renew_lifetime = 36000
24. forwardable = true
25. krb4_convert = false
26. validate = true
```

Why not use Kerberos for authorization?

- ▣ No facility for it
- ▣ Main thing Kerberos provides in the end is a mechanism for exchanging small amounts of data with the Key Server
 - Perfect for authentication exchanges
 - Not good for large authorization exchanges

Why use LDAP for authorization?

- ▣ LDAP a type of database optimized for read-mostly environments
- ▣ Came from the directory world and is well suited for the task
- ▣ Authorizations are just another set of attributes for LDAP
- ▣ Well established standards
- ▣ A number of high performance implementations available

Service credentials

- ▣ Services can be principals as well
- ▣ Kerberos originally required symmetric authentication (how do I know I am talking to the print server?)
- ▣ Useful for adding auditability to service transactions
- ▣ Can enable things like kerberized Apache servers that can use kerberos tickets to authenticate web users
- ▣ Single sign-on for UNIX users as well

/etc/ldap.conf

```
1. host 10.10.10.10 base dc=example,dc=com?sub
   dc=internal,dc=neilwaybright
   ,dc=us
2. uri ldap://win208b.neilwaybright
   .us/
3. pam_login_attribute sAMAccountName
4. Binddn cn=dirsearch,cn=Users,dc=int
   ernal,dc=neilwaybright,dc=us
5. bindpw adldapbindpw
6. scope sub
7. ssl no
8. pam_filter objectClass=User
9. nss_base_passwd dc=example,dc=com?sub
10. nss_base_shadow
11. nss_base_group dc=mydomain,dc=com?sub?
   &(objectCategory=group)(gidn
   umber=*)
12. nss_map_objectclass posixAccount user
13. ss_map_objectclass shadowAccount user
14. nss_map_objectclass posixGroup group
15. nss_map_attribute gecos cn
16. nss_map_attribute homeDirectory
   unixHomeDirectory
17. nss_map_attribute uniqueMember member
```

/etc/pam.d/system-auth

```
1.  #%PAM-1.0 # This file is auto-
    generated.
2.  # User changes will be destroyed
    the next time authconfig is run.
3.  auth required
    /lib/security/$ISA/pam_env.so
4.  auth sufficient
    /lib/security/$ISA/pam_unix.so
    likeauth nullok
5.  auth sufficient
    /lib/security/$ISA/pam_krb5.so
6.  auth required
    /lib/security/$ISA/pam_deny.so
7.  account sufficient
    /lib/security/$ISA/pam_krb5.so
8.  account required
    /lib/security/$ISA/pam_unix.so
9.  account sufficient
    /lib/security/$ISA/pam_succeed_i
    f.so uid < 100 quiet
10. account required
    /lib/security/$ISA/pam_deny.so
11. password requisite
    /lib/security/$ISA/pam_cracklib.
    so retry=3
12. password sufficient
    /lib/security/$ISA/pam_unix.so
    nullok \use_authtok md5 shadow
13. password required
    /lib/security/$ISA/pam_deny.so
14. session required
    /lib/security/$ISA/pam_limits.so
15. session required
    /lib/security/$ISA/pam_unix.so
```

Final Steps

- ▣ Edit `/etc/nsswitch.conf` and add `ldap` to the `passwd`, `group` and `shadow` lines (e.g. `passwd: files ldap`).
- ▣ Try a `kinit <AD username>` (you will be prompted for the AD password of the user) and see if you get a credential
- ▣ Examine the credential with `"klist"`
- ▣ You have to add the `pam_mkhome.so` module if you want AD users to be able to log in that don't have pre-existing home directories

Solaris is different....

- ▣ Take a look at the instructions in Scott Lowe's blog at <http://blog.scottlowe.org/2007/04/25/solaris-10-ad-integration-version-3/>
- ▣ Solaris needs “user” credentials for the hosts instead of host credentials

Suse 9 Setup

The image shows two windows from the YaST Control Center. The left window is the main YaST interface with a sidebar on the left containing categories like Software, Hardware, System, Network Devices, Network Services, Security and Users, and Misc. The main area displays various services as icons, including DHCP Server, DNS Server, DNS and Host Name, HTTP Server, Host Names, Kerberos Client (highlighted with a yellow arrow labeled '2'), LDAP Client, Mail Transfer Agent, NFS Client, and NFS Server. The right window is titled 'YaST2 Kerberos Client Configuration'. It has two radio buttons: 'Do Not Use Kerberos' (unselected) and 'Use Kerberos' (selected). Below are 'Basic Kerberos Settings' with input fields for 'Default Domain' (MYDOMAIN.COM), 'Default Realm' (MYDOMAIN.COM), and 'KDC Server Address' (domainserver.mydomain.com). There is an 'Advanced Settings...' button and 'Back', 'Abort', and 'Finish' buttons at the bottom. A yellow arrow labeled '3' points to the 'Advanced Settings...' button.

a. Edit the `/etc/security/pam_unix2.conf` file. (make a backup first!) The location of this file depends on the distribution you are using. In SUSE its located in the security subdirectory. Add the following lines:

```
auth: use_krb5 nullok
account: use_krb5
password: use_krb5 nullok
session: none
```

SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism)

- ▣ Uses GSS-API to provide the kerberos front-end work for applications
- ▣ Permits transparent forwarding of kerberos tickets for access
- ▣ SINGLE SIGN-ON as a reality
- ▣ Excellent explanation of the issues at http://www.ibm.com/developerworks/webSphere/library/techarticles/0809_lansche/0809_lansche.html
- ▣ <http://blog.scottlowe.org/2006/08/10/kerberos-based-sso-with-apache/>

Questions?

- ▣ Slides as presented are already up at www.waybright.org/neil/presentations
- ▣ I'll polish the slides and have slides revised with the questions and comments up by the end of the week next week.

References

- http://www.windowsnetworking.com/articles_tutorials/Authenticating-Linux-Active-Directory.html
- <http://blog.scottlowe.org/2006/08/08/linux-active-directory-and-windows-server-2003-r2-revisited/>

References

- ❑ <http://blog.scottlowe.org/2007/04/25/solaris-10-ad-integration-version-3/>
- ❑ <http://technet.microsoft.com/en-us/library/bb742433.aspx>
- ❑ http://www.ibm.com/developerworks/webSphere/library/techarticles/0809_lansche/0809_lansche.html
- ❑ <http://blog.scottlowe.org/2006/08/10/kerberos-based-sso-with-apache/>