Tuning in to H.323 / LDAP security

- What this presentation is about
  - RADvision ECS registration control via LDAP
  - information and configs needed to reproduce results
  - a small step in H.323 / LDAP integration
  - discussion of a possible vidmid authentication directory

- What this presentation is NOT about
  - discussion of video schema proposals
  - discussion of all possible client server configurations
  - endorsement of any specific vendor gear


H.323 / LDAP Security
OARnet

Project scope

- Investigate H.323 gatekeeper / directory “authentication”
- Understand details of RADvision ECS implementation
- Present findings and submit recommendations
- Discussion of results

Project notes

- Increased security
- More moving parts
- More to troubleshoot (security v. functionality)
- Potential long term gain

Overview of findings

- RADvision ECS GK will talk to an LDAP directory
- H.323 client registration can be proxied through the GK to a directory
- Does not perform RFC1777 LDAP authentication

RFC1777 / 2251 authentication

- Simple authentication over TLS
- LDAP_Result == 0 sent as a bind response to DN/userPassword bind attempt
- Practical implementation usually involves a search on “mail | cn” attribute, returning the DN.

RADvision ECS dependencies

- A stable software revision
- Point and click tab on ECS to enable LDAP
- Set ECS to check directory for matching presence of “rvuseralias” attribute for registration
- Allocate and configure proprietary DIT in the directory for ECS use
- Specific directory entries need to be in place

Schema modifications

- RADvision objectclasses (ECS CD2)
- RADvision attributes (ECS CD2)
- ftp.radvision.com, thanks <chris@radvision.com>
- iplanet aci attributes (docs.iplanet.com)
- Custom schema mods / DNs available

Test gear profile

- RADvision ECS / NT box
- iplanet 4.12 DS / Sun netra t1 / S8
- VCON client / NT box
- Mt.Dew / Doritos

The observer effect

- No client response to denied registration
- No client response to successful registration
- Sparse RADvision implementation docs
- Hard coded ECS schema / DN requirements
- No (direct) support for LDAP over SSL

Assessment of results

- Marginal increase security of H.323 conferences, when not using SSL
- Enable a distributed registration process
- Parallel step in making H.323 registration more manageable
- Possible ip telephony applications (don’t phreak out)
- Distributed interdisciplinary collaboration necessary to make any real progress

Recommendations (for vendors)

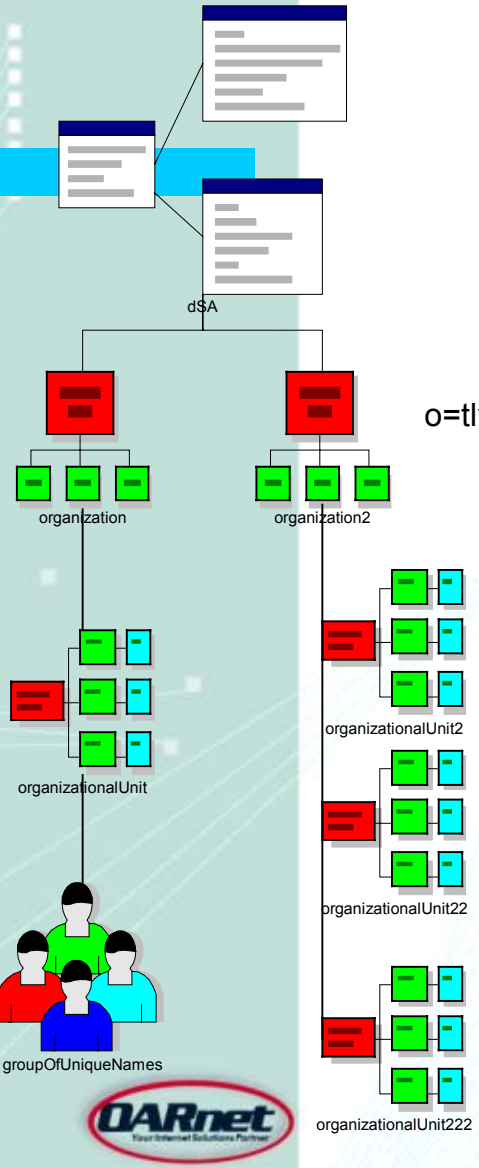
- Allow for schema modification on gatekeepers
- Code RFC1777 LDAP authentication in GK as LDAP clients
- Extend H.323 clients to test and report registration status
- Support native SSL in GK as an LDAP client (use stunnel until then)
- Loan me your gear to test, verify and report on against a known DIT

What's next?

- OARnet will host a reference directory for Internet2 vidmid testing at ldap.enss.net or vidmid.osu.edu
- Both client (GK) and directory schemas will be made available
- Deployment of YACeViD

YACeViD

vidmid.osu.edu



dc=vidmid, dc=osu, dc=edu

o=tlv.radvision.com

cn=Radvision Administrator, ou=Groups

cn=static information, cn=h323 zone

cn=online information, cn=h323 zone

uid=aschool@oar.net

cn=gk list, cn=h323 zone

4 October 2001


Albert School
aschool@oar.net
OARnet

```
##############################################################################
# Master schema/DN ldif for use with RADvision ECS
#
# $Id: rvzone_schema.ldif,v 1.4 2001/09/07 19:46:19 aschool Exp aschool $
# Extracted from multiple evolving and possibly copyright sources.
# For educational / demonstration use only.
#
# Albert School <aschool@oar.net>
#
#       o radvision root node addition to
#         $IPLANET_HOME/slapd-$NODE/config/slapd.ldbm.conf
#       o radvision ECS schema mods
##############################################################################
# $IPLANET_HOME/slapd-$NODE/config/slapd.ldbm.conf mod
#
# echo "o=tlv.radvision.com" > slapd.ldbm.conf
#
##############################################################################
# Radvision schema mods
#
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( rvgkdesc-oid NAME 'rvgkdesc' )
attributetypes: ( rvgkdist-oid NAME 'rvgkdist' )
attributetypes: ( rvGkDns-oid NAME 'rvGkDns' )
attributetypes: ( RVgkId-oid NAME 'rvgkid' )
attributetypes: ( RVgkIpCs-oid NAME 'rvgkipcs' )
attributetypes: ( RVgkIpRas-oid NAME 'rvgkipras' )
attributetypes: ( rvgkmode-oid NAME 'rvgkmode' )
attributetypes: ( RVgkPrefix-oid NAME 'rvgkprefix' )
attributetypes: ( RVuserAlias-oid NAME 'RVuserAlias' )
attributetypes: ( RVuserId-oid NAME 'rvuserid' )
attributetypes: ( rvUserIndex-oid NAME 'rvuserindex' )
attributetypes: ( RVuserIpCs-oid NAME 'rvuseripcs' )
attributetypes: ( RVuserIpRas-oid NAME 'rvuseripras' )
attributetypes: ( RVuserPsswd-oid NAME 'rvuserpsswd' )
-
add: attributetypes
attributetypes: ( rvgkdesc-oid NAME 'rvgkdesc'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( rvgkdist-oid NAME 'rvgkdist'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.27'
        SINGLE-VALUE )
attributetypes: ( rvGkDns-oid NAME 'rvGkDns'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26'
        SINGLE-VALUE )
attributetypes: ( RVgkId-oid NAME 'rvgkid'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26' )
attributetypes: ( RVgkIpCs-oid NAME 'rvgkipcs'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( RVgkIpRas-oid NAME 'rvgkipras'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( rvgkmode-oid NAME 'rvgkmode'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( RVgkPrefix-oid NAME 'rvgkprefix'
```

```
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26'
        SINGLE-VALUE )
attributetypes: ( RVuserAlias-oid NAME 'RVuserAlias'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26' )
attributetypes: ( RVuserId-oid NAME 'rvuserid'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26'
        SINGLE-VALUE )
attributetypes: ( rvUserIndex-oid NAME 'rvuserindex'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.27'
        SINGLE-VALUE )
attributetypes: ( RVuserIpCs-oid NAME 'rvuseripcs'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( RVuserIpRas-oid NAME 'rvuseripras'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15'
        SINGLE-VALUE )
attributetypes: ( RVuserPsswd-oid NAME 'rvuserpsswd'
        DESC 'User Defined Attribute'
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.26'
        SINGLE-VALUE )
-
delete: objectclasses
objectclasses: ( rvuseronline-oid NAME 'rvuseronline' )
objectclasses: ( rvfolder-oid NAME 'rvfolder' )
objectclasses: ( rvgk-oid NAME 'rvgk' )
objectclasses: ( rvuserstatic-oid NAME 'rvuserstatic')
-
add: objectclasses
objectclasses: ( rvuseronline-oid
        NAME 'rvuseronline'
        DESC 'User Defined ObjectClass'
        SUP 'top'
        MUST ( rvuserindex $ objectclass )
        MAY ( RVuserAlias $ rvuserid $ rvuseripcs $ rvuseripras $ aci ) )
objectclasses: ( rvfolder-oid
        NAME 'rvfolder'
        DESC 'User Defined ObjectClass'
        SUP 'top'
        MUST ( cn $ objectclass )
        MAY ( aci ) )
objectclasses: ( rvgk-oid
        NAME 'rvgk'
        DESC 'User Defined ObjectClass'
        SUP 'top'
        MUST ( rvgkid $ rvgkipcs $ rvgkipras $ rvgkmode $ objectclass )
        MAY ( rvgkdesc $ rvgkdist $ rvGkDns $ rvgkprefix $ aci ) )
objectclasses: ( rvuserstatic-oid
        NAME 'rvuserstatic'
        DESC 'User Defined ObjectClass'
        SUP 'top'
        MUST ( RVuserAlias $ objectclass )
        MAY ( rvgkid $ rvuseripcs $ rvuseripras $ rvuserpsswd $ aci ) )
```

```
##############################################################################
# Initial DN population ldif for use with RADvision ECS
#
# $Id: rvzone_dn.ldif,v 1.2 2001/09/07 19:30:24 aschool Exp aschool $
# Extracted from multiple evolving and possibly copyright sources.
# For educational / demonstration use only.
#
# Albert School <aschool@oar.net>
#
#       o radvision ECS initial DN population
##############################################################################
#
#
dn: o=tlv.radvision.com
objectclass: top
objectclass: organization
aci: (targetattr != "userPassword || rvuserpsswd || rvuseralias || rvuseripras || rvuseripc
        (target="ldap:///*,o=tlv.radvision.com")
        (version 3.0;acl "Anonymous Access to RADvision DIT (!WARNING! use this for develop
        allow(read, search , compare)
        (userdn = "ldap:///anyone")
        ;)
aci: (targetattr ="*")
        (version 3.0;acl "RADvision Administrators Group";
        allow(all)
        (groupdn = "ldap:///cn=radvision administrator, ou=groups, o=tlv.radvision.com")
        ;)

dn: cn=h323 zone, o=tlv.radvision.com
objectclass: top
objectclass: rvfolder
cn: h323 zone

dn: ou=Groups, o=tlv.radvision.com
objectclass: top
objectclass: organizationalunit
ou: Groups

dn: cn=radvision administrator, ou=Groups, o=tlv.radvision.com
description: Entities with radvision access to this directory server
objectclass: top
objectclass: organizationalunit
objectclass: groupofuniquenames
ou: Radvision Administrators
cn: Radvision Administrators
uniquemember: uid=RADman, cn=radvision administrator, ou=groups, o=tlv.radvision.com

dn: uid=RADman, cn=radvision administrator, ou=Groups, o=tlv.radvision.com
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
cn: Radvision Administrator
sn: Administrator
givenname: RADvision
uid: RADman
userpassword: radtest

dn: cn=static information, cn=h323 zone, o=tlv.radvision.com
objectclass: top
objectclass: rvfolder
cn: static information

dn: cn=online information, cn=h323 zone, o=tlv.radvision.com
objectclass: top
objectclass: rvfolder
cn: online information
```

```
dn: cn=gk list, cn=h323 zone, o=tlv.radvision.com
objectclass: top
objectclass: rvfolder
cn: gk list

dn: rvuseralias=NAME:Albert School 0123456789,cn=static information,cn=h323 zone,o=tlv.radv
objectclass: top
objectclass: rvuserstatic
rvgkid: KRAD1
rvuseralias: NAME:Albert School 0123456789
rvuserpsswd: radtest

dn: cn=KRAD1,cn=online information,cn=h323 zone,o=tlv.radvision.com
cn: KRAD1
objectclass: top
objectclass: rvfolder

dn: rvgkid=KRAD1,cn=gk list,cn=h323 zone,o=tlv.radvision.com
objectclass: top
objectclass: rvgk
rvgkid: KRAD1
rvgkmode: depeche
rvgkipcs: 192.168.244.115 1719
rvgkipras: 192.168.244.115 1719
```