ZVWS and security: Protecting your assets

James Vincent

ZVWS and Security?

What's the big deal?

- Does your company *want* to be in the news?
  - And not in a GOOD way!
- "But my web servers are not open to the public!"
  - In-the-clear userids and passwords get picked up by other company employees too
  - Internal data/system breaches are more common than you think

VELOCITY SOFTWARE

ZVWS – Velocity Web Server

Primary function

- Support Velocity web applications
  - ZVIEW, PORTAL, zPRO
- Host web sites
  - www.velocitysoftware.com
  - www.vmworkshop.org
  - www.linuxvm.com
  - ...and more!

VELOCITY SOFTWARE

Securing resources

Resource access can be:

- Open (unsecured – think “http:”)
- Secured with user and password
  - Still insecure on http!
- Encrypted communication (SSL)
- Two-factor authentication
  - client certificate authentication + userid/pwd

VELOCITY SOFTWARE

Secured with user/pswd

Basic HTTP authorization

- WWW-Authenticate response header
- Userid:password
- Encoded in base64

- Secure access to application, but data is NOT secure on the wire

VELOCITY SOFTWARE

Userids and passwords

Userid and passwords

- Can be defined directly to zVWS
- CP directory
- ACIGROUP
- ESM
- RACF group names
- Cookies
- Security exit
- LDAP/AD

VELOCITY SOFTWARE

LDAP authentication

LDAPAUTH EXEC (zVWS 4310)

Controlled via

- ESM_EXIT LDAPAUTH (ZVWS AUTHLIST directive)

LDAPAUTH CONFIG

- HOST ldap.forumsys.com
- PORT 389
- BASE dc=example,dc=com
- RC_NOTAUTH 20
- RC_ERROR 16

VELOCITY SOFTWARE

HTTPS secured connection

SSL history

- Developed by Netscape in 1995
- SSLv3 released in 1996
- TLS 1.0 released in 1999
  - Vulnerable to hackers (POODLE, BEAST, etc)
  - End of Life June 30th 2018
- TLS 1.1 (2006)
- TLS 1.2 (2008) is current
  - Protects against known vulnerabilities

VELOCITY SOFTWARE

HTTPS (continued)

- TLS 1.3 is now approved
  - faster and more secure
  - In “last call” for development
- Each release is better, stronger, faster
- Browser complain or refuse connections for old protocols

VELOCITY SOFTWARE

SSL handshake

Client and server perform handshake

- settle on TLS version and cipher suite
- client authenticates server certificate
- server authenticates client certificate (optional)
- negotiate shared secret key

All communication is then encrypted

Strong cipher = data is protected

Data can not be modified

VELOCITY SOFTWARE

The Velocity SSL solution

z/VM did not offer *native* SSL solution

…so Velocity Software developed one

zSSL released in 2000

- **Provided utility for keys and certiticates**
- **Certificate specified on zVWS PORT directive**
- **Supports TLS 1.0**
  - **"seasoned" cipher suite**
- **Supports client certificates**
- **Functionally stabilized (version 4.2.1.9)**

VELOCITY SOFTWARE

client certificate support

ZVWS (via zSSL) supports *client certificates*

- authenticates the client
- used by CAC (Common Access Card)
- Certificate fields available to ESM exit
- Can secure on client certificate itself (CABUNDLE)
- Or can secure based on fields in the certificate
  - 22 fields available

VELOCITY SOFTWARE

IBM SSL Server released in 2008

Z/VM 5.4 included native SSL support

- No longer requires a Linux solution

z/VM 6.4 SSL is even better

- Supports current protocols (TLS 1.2)
  - (and the older ones but ignore that!)
- Supports modern strong ciphers
- No client certificate support (yet)
  - RFEs exist for both HTTPS and FTPS
  - RFE 118753 for HTTPS

VELOCITY SOFTWARE

More on SSL Server

SSL certificates

- Certificate DB on GSKADMIN
- Manage via GSKKYMAN utility
- Self signed certificates (for TEST ONLY)
- Send CSR to Certificate Authority
  - Install CA cert to your DB and refresh SSL
- Root CA certificates from the Certificate Issuer
  - i.e., DigiCert

VELOCITY SOFTWARE

More on SSL Server

Installation points

- Update PROFILE TCPIP
  - Certificate is specified on the xxx TCPIP PORT statement
  - Example: 443 TCP webserver SECURE certname
- Change CONFIG ZVWS port directive
  - PORT 443

VELOCITY SOFTWARE

More on SSL

- Should you redirect all http to https?
  - zVWS will help do that easily!
- Migration procedure provided for zSSL
  - Export certs out of zSSL and into SSL Server
- Velocity support FTP is SSL capable
  - See the Install Guide for details
- Velocity HTTPS web sites run SSL Server
  - https://www.velocitysoftware.com/customer/ptrack/

And the bottom line is…

VELOCITY SOFTWARE

Velocity recommends...

If you're using zSSL, migrate to SSL Server

- Let the z/VM SSL servers handle the encryption heavy-lifting, while zVWS concentrates on being an awesome web serve

If not yet using HTTPS, do it soon!

- Protect your zVIEW/PORTAL applications
- Without it, *your* data, and userids/passwords are exposed

Don't be sorry, get secured!

VELOCITY SOFTWARE

The End

Questions or lunch time?

VELOCITY SOFTWARE