Wholesome Practices for Securing a FOSS VistA Stack

K.S. Bhaskar
ks.bhaskar@fisglobal.com
+1 (610) 578-4265
http://fis-gtm.com
Acknowledgements

• Developed in collaboration with

Jon Tai
Software Developer, Medsphere Systems Corp.
jon.tai@medsphere.com
Objective

• Convert “unknown unknowns” into “known unknowns”
What is security?
What is security?

• Simplistic view
  – Ensuring that the wrong people don't have access
  – Ensuring that the right people have access
    • Including that the wrong people don't stop the right people from their access
  – Knowing who has had access and what they have done
What is security?

- **Simplistic view**
  - Ensuring that the wrong people don't have access
  - Ensuring that the right people have access
    - Including that the wrong people don't stop the right people from their access
  - Knowing who has had access and what they have done

- **Complex view**
  - Machinery to implement your simplistic view
What is security?

• **Simplistic view**
  – Ensuring that the wrong people don't have access
  – Ensuring that the right people have access
    • Including that the wrong people don't stop the right people from their access
  – Knowing who has had access and what they have done

• **Complex view**
  – Machinery to implement your simplistic view

• **Ultimate view**
  – Knowing how well your simplistic view represents reality
In our imperfect universe

• Absolute security does not exist
• Practical security is a matter of trade-offs between
  – The value of what is being protected
  – The potential cost of its loss (including litigation liability & criminal prosecution)
  – Cost of protection
  – Usability of the protected asset
• Don't forget wetware, also known as “Layer 8”
Security Policy

• Yes, you do need a written security policy
  – Identification
    • What are the information assets?
    • Who legitimately needs access?
    • To what? Why? When?
  – Standards
  – Actions

• Yes, you should go through business exercises simulating simulated security violation scenarios

• Even if you are Superman, think about times when you must be away

http://www.sans.org/resources/policies/Policy_Primer.pdf
http://www.sans.org/reading_room/whitepapers/policyissues/1331.php
Pieces of the Puzzle

HIPAA

Web Enabler
OS

VistA
GT.M
Linux

Plain text
TCP/IP

CIS/CPRS
OS

Browser
OS

Terminal Emulator
OS
HIPAA

- Hire an expert or do it yourself
- Not discussed further here

http://www.sans.org/resources/policies/#hipaa
http://www.sans.org/reading_room/whitepapers/hipaa/
The Layers

• Client (OS, browser, terminal emulator)
• Network
• VistA
• GT.M
• Linux

• (Interactions)
Clients

• Security starts at the end user's device
  – Hardware/physical
    • Stolen laptops can contain sensitive information
      – Fortunately, standard VistA clients do not store patient information on the client
      – There may be information on the swap file
  – Software
    • Operating system
    • Web browser (if VistA applications are accessed through a web browser)

• Malware & social engineering can be used to steal sensitive information and passwords
Securing Clients

- Keep software current with latest security patches
- Use appropriate anti-virus, anti-malware, and personal firewalls (e.g., http://www.clamwin.com)
- Use dedicated client machines for VistA – no web-browsing and general use (set up dual boot of separate Windows partitions to reuse hardware)
- Ensure that only approved & secured clients are allowed to access VistA (e.g., via network routing)
- Encrypt disks (e.g., http://www.truecrypt.org)
  - Don't forget to encrypt swap files if you use them
• Why network security?
  – VistA is accessed over the network
    • Not just clients, but also interfaces with other servers
  – You can prevent a wide range of attacks on your VistA server by limiting access at the network level
    • The VistA server has no need to be directly accessed from the Internet at large
Controlling Traffic

• Separate types of devices to different subnets/VLANs
• The router/firewall acts as a traffic cop
• Follow the principle of least privilege
  – Only give devices on a subnet the amount of access they require to function, but no more
  • Devices on the phone subnet should not be able to access your VistA server
“Trusted” Networks

• Even on a trusted network, devices on a subnet may be able to see traffic destined for other devices on that subnet
  – This can happen even if you're using a switch, e.g., ARP spoofing
  – Keep unknown devices off your network
  – Use protocol-level encryption
Encryption

• Encryption should always be used when traffic is traveling over untrusted networks such as the Internet
  – TCP/IP
    • VPNs create an encrypted “tunnel”
    • Add-on software (e.g., stunnel – http://stunnel.org)
  – Protocol-level encryption
    • Example: HTTPS
    • Use certificates to ensure you know who you're talking to

• Something to ponder: can you really trust your LAN?
Securing Endpoints

• Even the best encryption can be defeated if the endpoint is not secure
  – Key loggers and video cameras can steal passwords
  – Screen scrapers can steal sensitive information
  – Consider something like Dasher (http://www.inference.phy.cam.ac.uk/dasher) for password entry

• Applies to both clinical desktops at the hospital/clinic and remote VPN clients
  – If you can't control or guarantee the environment of your remote clients, don't give them access
  – Consider remote desktop (http://www.rdesktop.org/) or VNC (e.g., http://www.tightvnc.com)
Wireless

• Protect your wireless with a secure encryption standard such as WPA2
  – Some vendors may have their own proprietary protocols - the robustness of these protocols is less well known
  – Avoid WEP and WPA which have known weaknesses

• Also use protocol-level encryption
  – Assume new vulnerabilities will be found tomorrow
VistA

- VistA has its own user database and permissions scheme
  - Access Code
  - Verify Code
  - Electronic Signature Code
  - Keys
  - Menus
A/V/ES Codes

• Access and verify codes are similar to usernames and passwords
  – In the VA, the access code was treated as sensitive information – essentially, it was a password that the IT department also knew

• Electronic signature code is used to sign orders and notes
Security Keys

• Users are assigned various security keys
  – Multiple users can hold the same key
  – Keys typically grant permissions to the holder
  – Some are mutually exclusive
    • ORES allows you to write orders; typically given to doctors
    • ORELSE allows you to release orders; typically given to nurses

http://medsphere.org/docs/DOC-1361
Menus

• Functionality is grouped into menus
  – Tree-like structure
  – Menu items typically locked with keys
  – Primary menu option is executed when user first logs in
  – Secondary menu options are available
    • Allows jumping to another branch of the tree
    • Also used to restrict access to applications
      – OR CPRS GUI CHART
Access determined by OS based on users & groups
GT.M Recommendations

• Restrict GT.M access to a group
• Set user / group ownership and permissions correctly for database files and journal directories
• Put read-only users on replicating (secondary) instances
• Use database encryption
• Use journaling – and randomly audit journal files
• Consider mechanisms for logging access
Linux

- Dedicate servers for VistA production
- Build up from barebones with minimal required functionality; don't strip down a bloated installation
- Access only to those who need it
- Administration access via sudo
- Record all user logins and every keystroke by root users
- Implement authentication /authorization at data-center level
- Consider encrypted file systems (will require manual access on boot)

http://www.puschitz.com/SecuringLinux.shtml
http://www.bastille-unix.org/
Physical

• Secure access to the server
  – What happens if it gets stolen?
    • Ensure any sensitive information not on an encrypted database resides on an encrypted file system
    • Swap – put on encrypted file system or generate random key at startup

• Secure the media
  – What about backups?
    • Backups of encrypted GT.M databases are also encrypted
  – What happens if a disk crashes?
Looking ahead

• The Cloud
  – Access to the virtual server is probably reasonably secure
    • Trust (that they have done it right) but verify
  – Virtual disks may or may not be secure, especially considering the long term
    • Encrypt file systems or databases
¿¿Questions??  ¡¡Comments!!