

Securing a FOSS Vista Stack

Jon Tai

Software Developer, Medsphere

jon.tai@medsphere.com

K.S. Bhaskar

SVP, Fidelity Information Systems

ks.bhaskar@fnis.com / +1 (610) 578-4265

Objective

- To 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

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
 - Cost of protection
 - Usability of the protected asset
- (Don't forget wetware, also known as "Layer 8")

HIPAA

- We're not the experts

<http://www.sans.org/resources/policies/#hipaa>

The Layers

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

- (Interactions)

Security Policy Document(s)

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

http://www.sans.org/resources/policies/Policy_Primer.pdf

http://www.sans.org/reading_room/whitepapers/policyissues/1331.php

Client

- Security starts at the end user's device
 - Hardware/physical
 - Stolen laptops can contain sensitive information
 - Fortunately, VistA's architecture does not store patient information on the client
 - Software
 - Operating system
 - Viruses and other malware can be used to steal sensitive information and passwords
 - Web browser (if VistA applications are accessed through a web browser)

Securing Clients

- Operating system and browser software should be kept up-to-date with latest security patches
- Appropriate anti-virus, anti-malware, and personal firewall software should be used
- Create a policy to ensure that only secured clients are allowed to access VistA

Network

- 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 does not need to be directly accessible to 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

Encryption

- Encryption should always be used when traffic is traveling over untrusted networks such as the Internet
 - VPNs create an encrypted “tunnel”
 - Protocol-level encryption
 - Example: HTTPS
 - Use certificates to ensure you know who you're talking to

“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

Securing Endpoints

- Even the best encryption can be defeated if the endpoint is not secure
 - Key loggers can steal passwords
 - Screen scrapers can steal sensitive information
- This applies to both clinical desktops at the hospital/clinic and remote VPN clients

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 are less well known
 - Avoid WEP and WPA which have known weaknesses
- Consider using protocol-level encryption in case future weaknesses are found

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

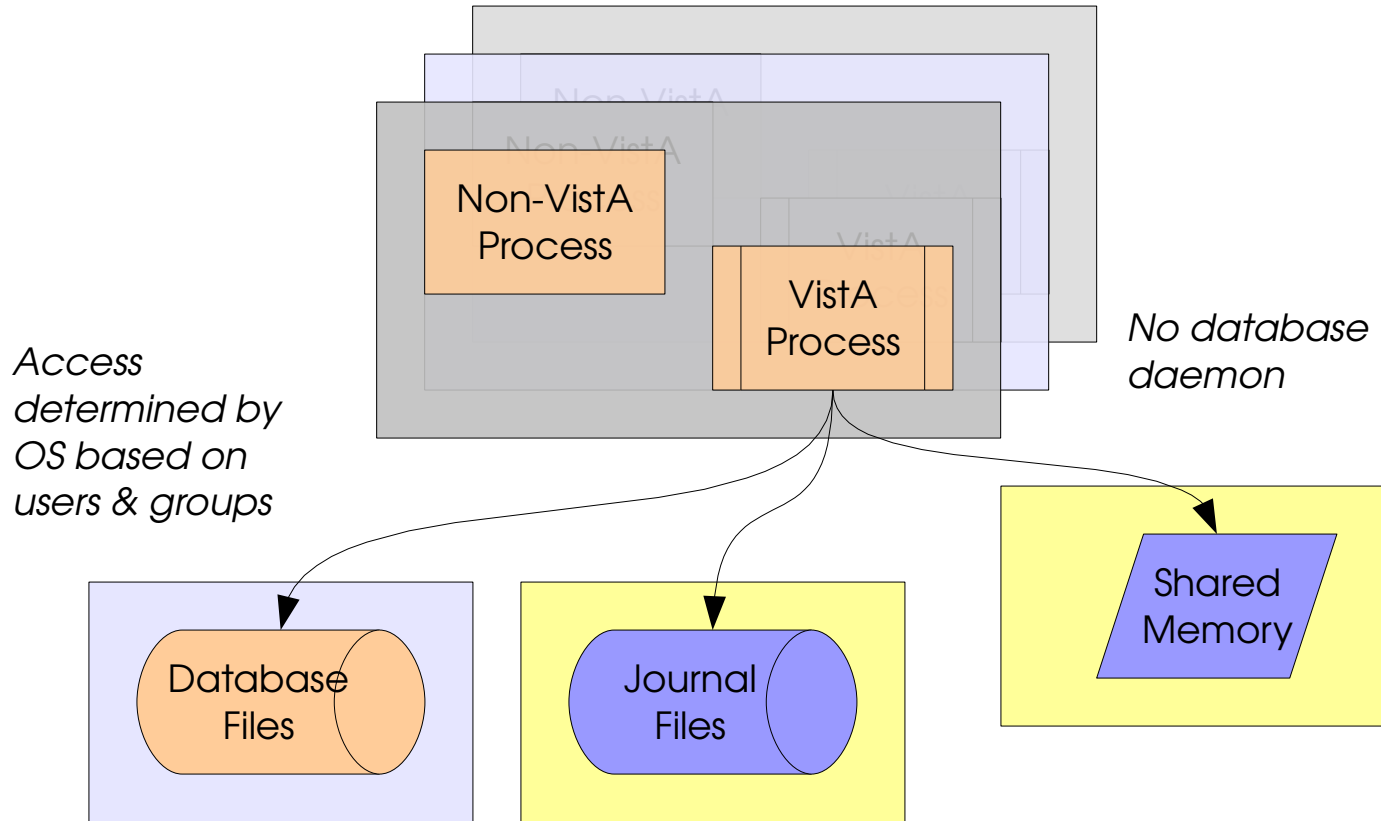
Security Keys

- 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

Menu

- 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

GT.M



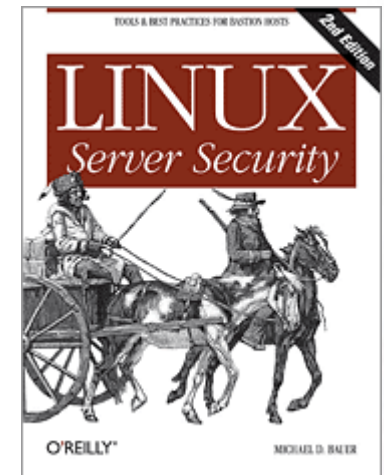
GT.M Recommendations

- Restrict access to GT.M to a group
- Set user / group ownership and permissions correctly for database files and journal directories
- Put read-only users on secondary instances

http://www.fidelityinfoservices.com/user_documentation/html/rn_tb/GTM_Security_Philoso

Linux

- Use the VistA server only for VistA production instances
- Restrict access to the machine to those who need access
- Record all user logins and every keystroke by root users
- Consider encrypted file systems



<http://www.puschitz.com/SecuringLinux.shtml>

<http://www.bastille-unix.org/>

Physical

- Secure access to the server
 - What happens if it gets stolen?
- Secure the media
 - What about backups?
 - What happens if a disk crashes?

Looking ahead

- The Cloud
 - Access to the virtual server is probably reasonably secure
 - Virtual disks may or may not be secure, especially considering the long term
 - Encrypt file systems or databases (coming in GT.M March/April 2009)

?? Questions?? !! Comments!!

