

Platform Hardening



Part 1: What is it and Why do we need it

CONTACTS

- ✘ Michael Gough – CISSP, CISA
 - + Senior Risk Analyst - Comptroller of Public Accounts
 - + Author – ‘SkypeMe!’ and ‘Video Conferencing over IP’ by Syngress Press
 - + Contributor to the Center for Internet Security Benchmarks.



AGENDA

- ✘ Part 1 – *What* is Platform Hardening and *Why* do we have to do it
- ✘ Part 2 – *What* do we need to do and *How* do we need to prepare to Harden systems
- ✘ Part 3 – *How* to Harden (Win, *NIX, Cisco, Handhelds)

WHAT

× Is Platform Hardening?

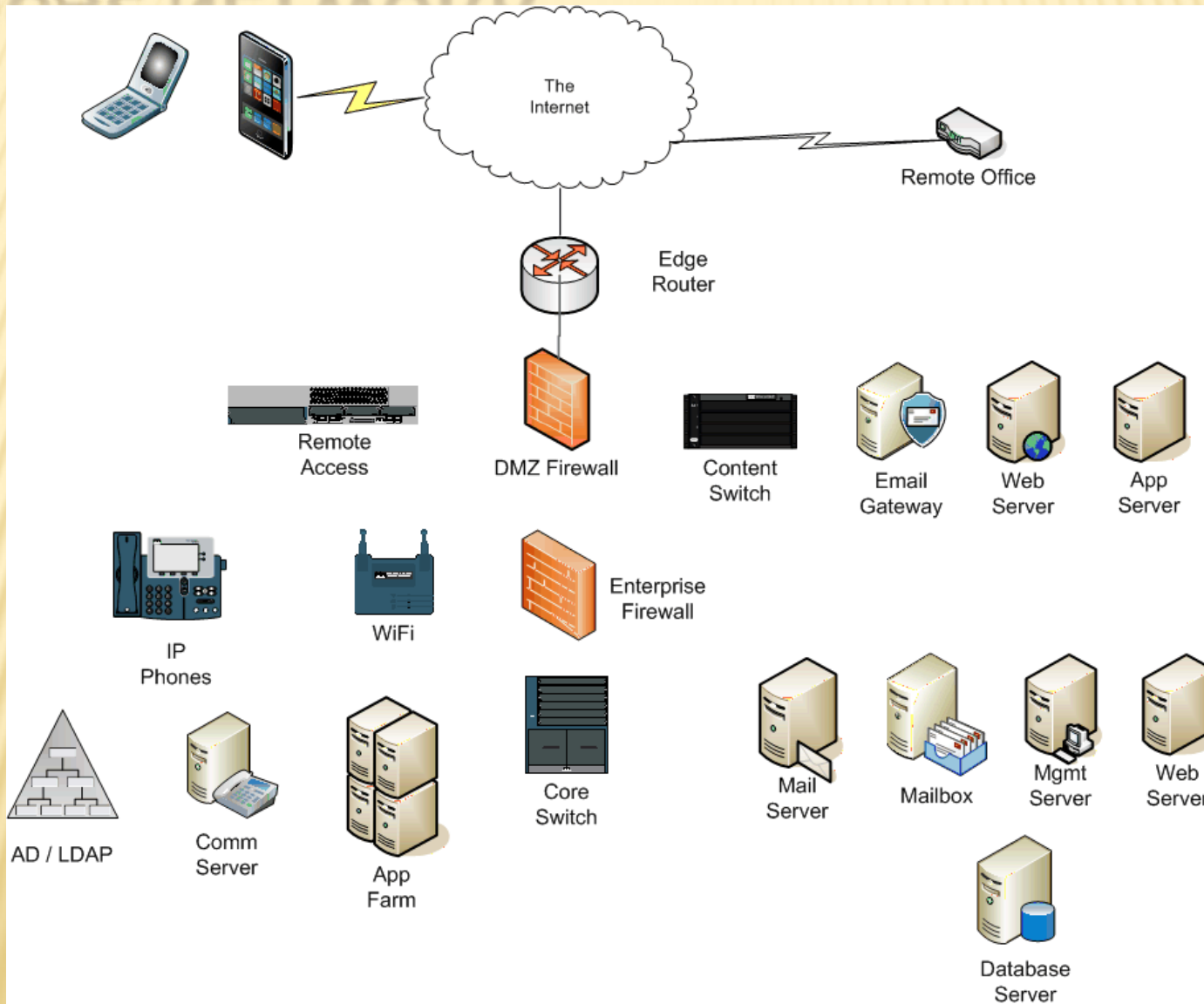
WHAT IS A PLATFORM?

- ✘ A Platform consist of all components that are a part of and can be configured on any type of, or group of Information Systems including but not limited to the following components:
 - + BIOS
 - + Hardware included in or on the system
 - + The booting or Base Operating System (B_{os})
 - + Any Virtual Operating System (V_{os})
 - + Any Guest operating system
 - + Any applications
 - + Any middleware
 - + Any databases
 - + Any storage device
 - + Network that connects it all (firewalls, routers, switches, VoIP)
 - + Any security applications installed on the completed system
 - + And of course... ALL configuration settings (auditing, options, etc.)

PLATFORMS



TYPICAL NETWORK



WHAT IS HARDENING?

- ✘ Bret Hartman, CTO at RSA says it is “appropriate (security) settings and removing unused code,”
- ✘ Hardening is a goal of deploying a system in the most secure state as possible, yet maintain functionality and reducing as many threat vectors as possible.

WHAT IS HARDENING?

- ✘ Hardening is the process of securely deploying systems.
- ✘ Hardening is the practice of 'least privilege'
- ✘ Hardening is not just the operating system
- ✘ Hardening includes:
 - + Understanding what you actually need to run on the system !!!
 - + DOCUMENTATION !!! (Policy, Standards & Guidelines)
 - + Operating systems
 - + Virtual servers
 - + Coding
 - + Application settings
 - + Database setup & configuration
 - + Network devices
 - + Portable devices
 - + Etc., etc. etc...

WHAT IS PLATFORM HARDENING?

- ✘ Platforms are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained.
- ✘ One of the required steps to attain this assurance is to ensure that the platforms are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

* From UT Medical Branch