CERIAS

the center for education and research in information assurance and security

Hardening Network Embedded Devices

Blake Self, Dr. Eugene Spafford

The goal of this project is to use existing vulnerability mitigation technology on network embedded devices to obtain significant security benefits with a minimal performance hit. For this project, three different linux based router operating systems were examined and modified.

Operating Systems:
OpenWRT
DD-WRT
Cisco E2100L

Hardware:
Linksys WRT54G V2
- BCM4712 @ 200Mhz
- 16 MB RAM

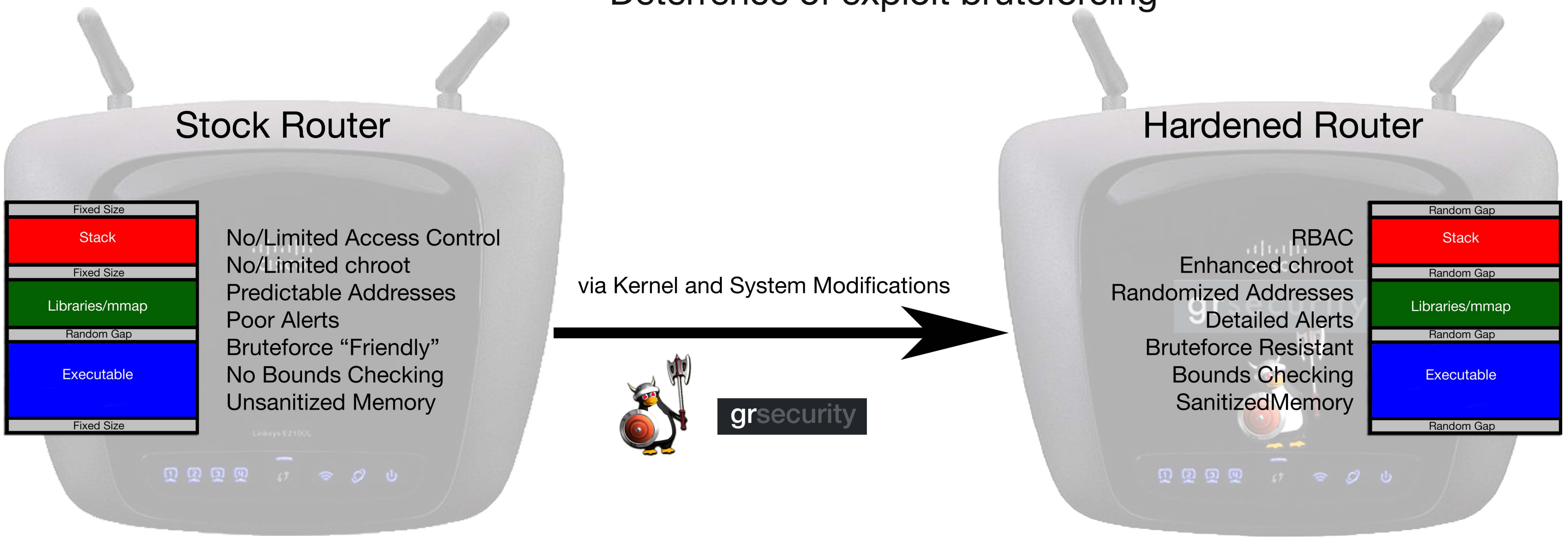
Linksys WRT54G2 V1
- BCM5354 @ 240 Mhz
- 16 MB RAM

Buffalo WHR-G125
- BCM5354 @ 240 Mhz
- 16 MB RAM

Linksys E2100L
- AR9130 @ 400 Mhz
- 64 MB RAM

Security Systems:
Grsecurity
PaX

Key Technologies:
Role-based access control
Capability auditing
Hide kernel processes
Enhanced chroot restrictions
Security alerts and audits that contain the IP address of the person causing the alert
Randomization of stack and mmap base
Randomization of heap base
Bounds checks user/kernel copying into/from kernel heap
No kernel modification via /dev/mem, /dev/kmem, or /dev/port
Reduction of the risk of sensitive information being leaked by arbitrary-read kernel bugs
Sanitizes memory at the lowest level of the kernel allocator
Deterrence of exploit bruteforcing



Stock Router

Fixed Size
Stack
Fixed Size
Libraries/mmap
Random Gap
Executable
Fixed Size

No/Limited Access Control
No/Limited chroot
Predictable Addresses
Poor Alerts
Bruteforce “Friendly”
No Bounds Checking
Unsanitized Memory

via Kernel and System Modifications

Hardened Router

RBAC
Enhanced chroot
Randomized Addresses
Detailed Alerts
Bruteforce Resistant
Bounds Checking
SanitizedMemory

Random Gap
Stack
Random Gap
Libraries/mmap
Random Gap
Executable
Random Gap

PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center