

---

# Vulnerability Summary

## May 2004

Paul Asadoorian  
Lead IT Security Specialist  
Brown University

---

# Vulnerabilities

---

- Linux Kernel Multiple Bugs
- Home Firewall/Routers
- Apple OS X Vulnerabilities
- Hacking Printers: Part 2

# Linux Kernel Multiple Bugs

---

- Examples:
  - sctp\_setsockopt() Integer Overflow
  - Framebuffer Code Unspecified Vulnerability
  - Setsockopt MCAST\_MSFILTER Integer Overflow Vulnerability
  - do\_fork() Memory Leakage Vulnerability
  - CPUFreq Proc Handler Integer Handling Vulnerability

## What does all this mean?

# Paul's Guide to Linux Kernel Vulnerabilities

---

- Terminology
- Local Vs. Remote Exploits
- Upgrading your kernel
- Resources

# Terminology

---

- **Exploit** – A program written to take advantage of a security vulnerability
- **Buffer** – A place in memory
- **Stack** – Memory used by programs for temporary storage and local variables
- **Heap** – Memory used by variables, very dynamic

# More Terminology

---

- **Library** – A pre-compiled collection of sub-routines
  - library.dll = Windows
  - liblibrary.so = Unix
- **Privilege escalation** – Gaining more rights than you are allowed (like r00t)

# Fun Terminology

---

- Buffer Overflow



# Fun Terminology

---

```
/*
 * beer.c
 */

void main() {

char pint[10];           /* Pint beer mug */
char half_pint[1];      /* Half pint beer mug */

memset(pint, 0x41, 10); /* Fill pint, mmmm yummy */
strcpy(half_pint, pint); /* Pour pint into half pint */
}
```

Credit: <http://www.l0t3k.net/biblio/b0f/en/bofs4kids.txt>

# Local Vs. Remote

---

- Local buffer overflow or privilege escalation exploits are bad
  - Kernel vulnerabilities are usually local
- Brute force lower privilege account, then get root
- Exploit service running not running as root
- Do you really trust ALL your users?

# Upgrading Your Kernel

---

- Backup your existing kernel!
- Read specific docs for your distribution
- Standardize on a kernel for your environment
- When in doubt, ask 😊

# Kernel Upgrading

---

- Red Hat/Fedora
  - <http://www.redhat.com/support/resources/howto/kernel-upgrade/>
- Debian
  - <http://www.debian.org/doc/manuals/debian-faq/ch-kernel.en.html>
- General Kernel Hacking
  - <http://www.digitalhermit.com/linux/Kernel-Build-HOWTO.html>
    - Was under review, almost complete

# Linux Kernel Multiple Bugs

---

- <http://www.security.nnov.ru/search/document.asp?docid=6201>
- <http://www.securityfocus.com/bid/10211>
- <http://www.securityfocus.com/bid/10179>
- <http://www.securityfocus.com/bid/10201>
- <http://www.securityfocus.com/bid/10233>
- <http://www.securityfocus.com/bid/10143>

# Linux Kernel Multiple Bugs

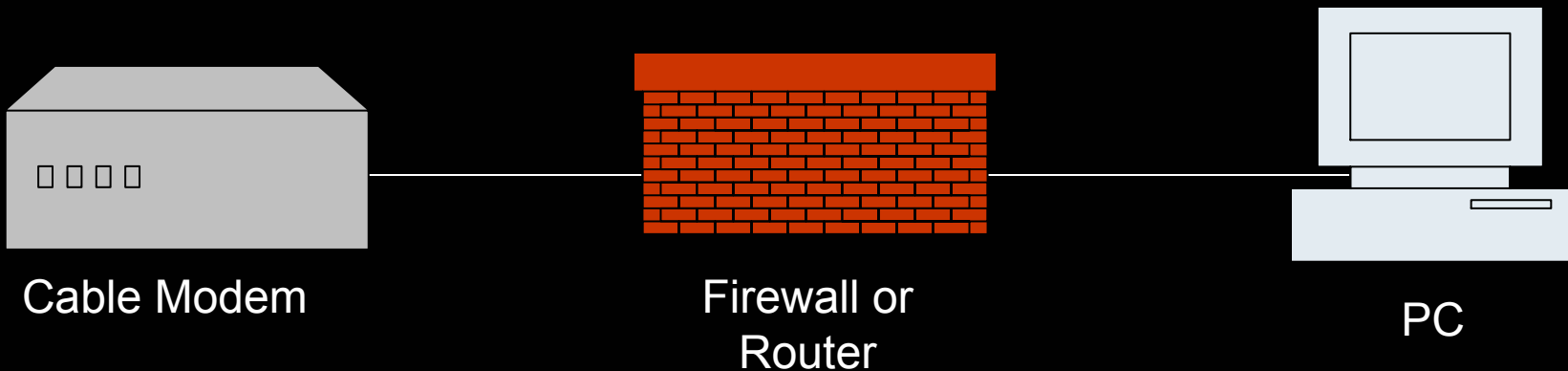
---

- <http://www.securityfocus.com/bid/10141>
- <http://www.securityfocus.com/bid/9691>
- <http://www.securityfocus.com/bid/9570>
- <http://www.securityfocus.com/bid/10330>
- <http://www.securityfocus.com/bid/9985>

# Home Firewall/Routers

---

- Is it a firewall or a router?



# Home Firewall/Routers

## SMC Routers Unauthorized Access

---

- Bug that leaves external administration enabled
- No password required
- Anyone can administer your firewall
- That's bad

# Home Firewall/Routers

## SMC Routers Unauthorized Access

---

- Vulnerable Systems
  - SMC Router 7008ABR (part number 750.9814 with firmware 1.032)
  - SMC Router 7004VBR (version 1, firmware 1.231)
- Other SMC models and firmware versions may be vulnerable

# Home Firewall/Routers

## SMC Routers Unauthorized Access

---

- Workarounds
  - Enable the router's firewall in its "Advanced Setup".
  - Forward port 1900 of the router to a non-existent internal IP address such as 192.168.2.248 (if it isn't in use).

# Home Firewall/Routers

## NetGear Protection Bypass

---

- URL Protection feature
  - No user can go to [www.warez.com](http://www.warez.com)
  - Even better \*.doubleclick.com
- Long URLs are able to bypass this protection
- Could also be a buffer overflow (Not confirmed)

# Home Firewall/Routers

## NetGear Protection Bypass

---

- Model Netgear RP114 known to be vulnerable
- New firmware not yet available
- Watch those kiddies in the mean time 😊

# Home Firewall/Routers

## Linksys Information Leak

---

- DHCP server does not handle BOOTP packets correctly
- Reveals portions of memory in response
- This allows you to sniff traffic, passwords, and other information

# Home Firewall/Routers

## Linksys Information Leak

---

- According to hacker comments:

*“I have successfully used this technique to steal the admin username and password”*

- Exploit exists and also claims to crash device

# Home Firewall/Routers

## Linksys Information Leak

---

- Claims to work on
  - Fully updated BEFSR41 and BEFW11S4
  - BEFN2PS4, BEFSR41, BEFSR81, BEFSX41, RV082, BEFCMU10, BEFSR11, BEFSR41W, BEFSRU31, BEFVP41, WRT55AG, WRV54G, WRT51AB
- No word on a fix from Linksys

# Home Firewall/Routers Defense

---

- Upgrade firmware often
- Test your firewall (nmap, [www.insecure.org](http://www.insecure.org))
- Retrieve and review your logs
- Put Linux on your Linksys?
  - <http://www.sveasoft.com/modules/phpBB2/viewforum.php?f=6>

# Home Firewall/Routers

---

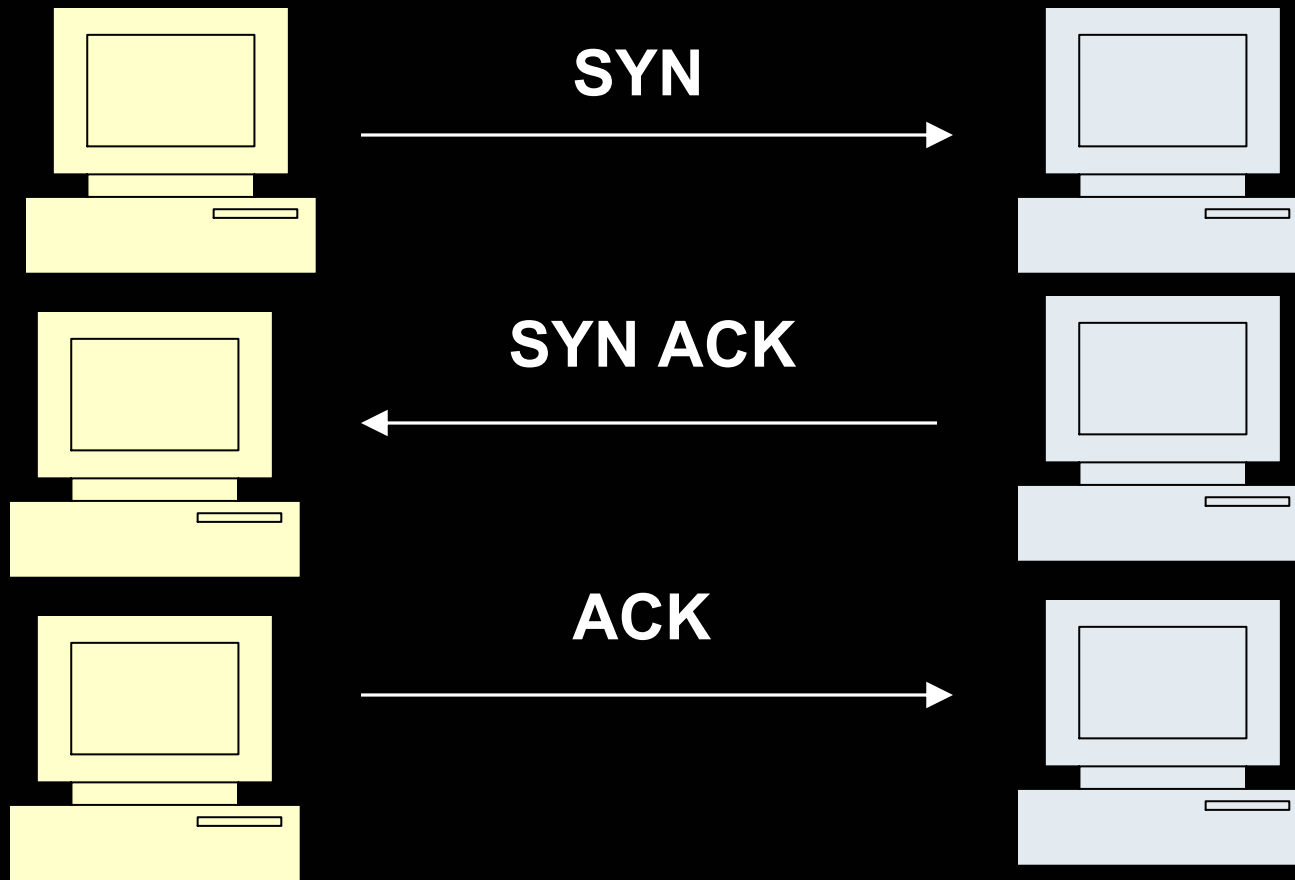
- SMC Routers Unauthorized Access
  - <http://www.security.nnov.ru/search/news.asp?binid=3681>
- Netgear Protection Bypass
  - <http://www.security.nnov.ru/search/news.asp?binid=3711>
- Linksys Information Leak
  - <http://www.security.nnov.ru/search/news.asp?binid=3703>

# Hacking Printers – Part 2

---

- Printers are computers
  - OS
  - IP Stack
  - Listening services
- This means vulnerabilities!
- Poor man's IP Stack included

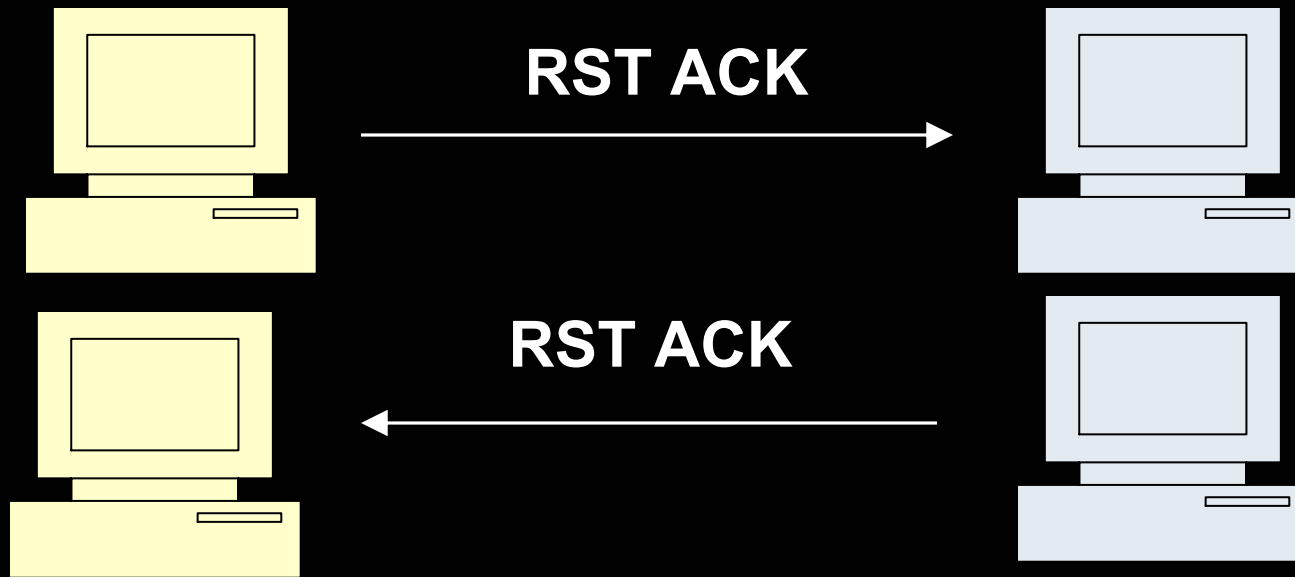
# Hacking Printers - Part 2



**Normal TCP 3-Way Handshake**

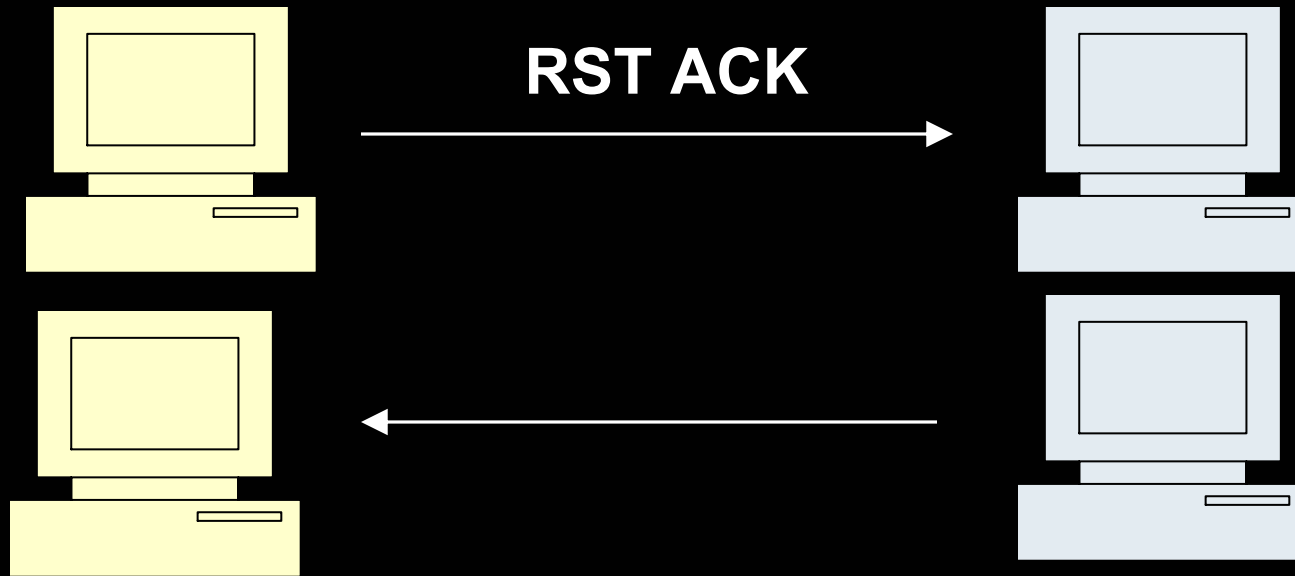
# Hacking Printers - Part 2

---



# Hacking Printers - Part 2

---



# Hacking Printers - Part 2

---

11:50:10.944550 **MY.SUB.NET.11.6667 > MY.SUB.PRNT.25.1024:**

**R** [tcp sum ok] 121325388:121325388(0) ack 1288864225

win 0 (ttl 64, id 568, len 40)

0x0000 4500 0028 0238 0000 4006 814b \*\*\*\* 450b

0x0010 \*\*\*\* b119 1a0b 0400 073b 474c 4cd2 81e1

0x0020 5014 0000 7d3d 0000

11:50:10.948337 **MY.SUB.PRNT.25.1024 > MY.SUB.NET.11.6667:**

**R** [tcp sum ok] 1:1(0) ack 0 win 0 (ttl 58, id 3196, len 40)

0x0000 4500 0028 0c7c 0000 3a06 7d07 \*\*\*\* b119

0x0010 \*\*\*\* 450b 0400 1a0b 4cd2 81e1 073b 474c

0x0020 5014 0000 7d3d 0000 0000 0000 0000

# Hacking Printers – Part 2

---

- Find all printers on the network easily
- Very stealthy, RST packets can blend
- Most printers are vulnerable
  - Store files
  - Proxy traffic

# Hacking Printers – Part 2

---

- Upgrade firmware
  - Doesn't always fix vulnerabilities
- Disable unused services
- Firewall printers from Internet
  - Possibly remove default gateway

# Apple OS X Vulnerabilities

---

- AppleFileServer fails to properly handle certain authentication requests
  - <http://www.kb.cert.org/vuls/id/648406>
- Help system may interpret inappropriate local script files
  - <http://www.kb.cert.org/vuls/id/578798>
- "disk://" URI handler stores arbitrary files in a known location
  - <http://www.kb.cert.org/vuls/id/210606>

# Website Of The Month

---

“LOT3K, Digital <blank> <blank>”

<http://www.l0t3k.org/>

- Excellent resource, great articles:
  - “Chrooting Apache and PHP in BSD Howto”
  - “Understanding TCP Reset Attacks, Part I”

# /\* The End \*/

---

- Other cool links:
  - <http://packetstormsecurity.nl/>
  - <http://www.security.nnov.ru/>
  - <http://www.cert.org>
  - <http://www.whitehats.com>
  - <http://rr.sans.org>
  - <http://www.incidents.org>
  - <http://www.astalavista.com/>
  - <http://www.l0t3k.org/>

