Secure Coding

Weasel
nomad **m**obile **r**esearch **c**entre

Introduction

Outline

- Vulnerabilities Overview

Types of Vulnerabilities

  - General
  - Language Specific
- Best Practices
  - General
  - Language Specific
- Tools
- Conclusion
- Q & A
- Links


Vulnerabilities

Types of Vulnerabilities

- Buffer Attacks
  - Buffer Overflow
  - Buffer Parsing
- Format String Attacks
  - %s in logging/debugging routines
- Race Conditions
  - World writeable temp files
  - Server/Client MITM
- Authentication Attacks

- Authorization Attacks
  - Holes in Authorization Mechanism
  - Too Much Trust of User Input
- Cryptography Attacks
  - Weak Algorithms
  - Poor Implementation


Best Practices

Best Practices - General

- Protect User Input
  - Restrict Input (and Output) to Acceptable Characters
  - Restrict and Flush the Buffer Properly
- Use Well-Tested Code
  - Especially for Parsing
- Code Reviews
  - By !You
  - Prioritize and Schedule
- Policies and Guidelines
  - Comprehensive Guidelines w/ Sign-off
  - Enforce the Policy
- Set PATH Environment Variable

Best Practices – General (cont.)

- Set Permissions to Minimal Required (Least Privilege Principle)
- Don’t Use Copy Functions that Do Not Check the Buffer Length
- Don’t Offload Security to the Client
- Centralize I/O Check Functions
- Validate/Be Aware Environment Variables (i.e. an altered IFS to change command line switches, or multiple entries for the same var)
- Robust Error Handling(Fail Safe)

Best Practices - C

- Use Protected Sting Functions
  - strncpy() > strcpy()
  - strncat() > strcat()
  - snprintf() > sprintf()
  - fgets() > gets()
- Use exec() instead of system()
  - $buffer = “/bin/ls; /bin/cp /etc/shadow ~/shadow”
  - system($buffer);
    - # /bin/ls
    - # /bin/cp /etc/shadow ~/shadow
  - exec($buffer);
    - # /bin/passwd

Best Practices – Web

- Strip/Deny Unwanted User Input
  - Meta Characters
  - Value Assignments
- Check Buffer Length Upon Input/Output/Copy
- Parse with Well-Known Libraries
  - i.e. CGI.pm for Perl
- Don’t Store Access Information in Accessible Sources
  - You never know when MOD_PHP is going to dump your source

Tools

Credit to John Marchesini

Tools – Black Box Testing

- Passive Monitoring
  - Wired Sniffing – Ethereal, tcpdump, Sniffer Pro (Ettercap for switched)
  - Wireless Sniffing – Kismet, Airsnort, etc
  - IDS/IPS (very limited use)
- Active Attacks
  - Local Attacks – QA Applications, Macro Tools
  - Remote Attacks – Netcat, telnet

Tools – Component Testing

- Library and API Calls, Persistant State
  - strace, ltrace (*nix)
  - Sysinternals.com (several Windows Tools)
  - System Tools – top, ps, etc…
- Runtime Injection
  - BEAST
- Reverse Engineering
  - Disassemblers/Debuggers
    - SoftICE, DataRescue's IDA Pro, OllyDbg

Tools – Source Code Review

- RATS, Flawfinder, ITS4, Klocwork (Static)
- CodeAssure Suite(both Static and Binary)

NOTE: As with many security tools, or tools in general, these tools provide output for analysis, they do not replace a skilled reviewer.

Conclusion


Q & A

Links

•Secure Programming for Linux and UNIX HOWTO – Creating Secure Software
http://www.dwheeler.com/secure-programs

Secure UNIX Programming FAQ
http://www.whitefang.com/sup

NCSA Secure Programming Guidelines
http://archive.ncsa.uiuc.edu/Grid/ACES/security/programming

How to Write Secure Code
http://www.shmoo.com/securecode

SECPROG
http://www.securityfocus.com/frames/?content=/forums/secprog/intro.html

INFOCUS – Secure Coding – David Wong
http://www.securityfocus.com/infocus/1596

Links - Tools

SPIKE
http://www.resources-freesoftware.shtml

BEAST
http://www.sisecure.com/company/ourtechnology/beast.shtml

ltrace
http://freshmeat.net/projects/ltrace

Ethereal
http://www.ethereal.com

Netcat
http://netcat.sourceforge.net

IDA Pro
http://www.datarescue.com

Flawfinder
http://www.dwheeler.com/flawfinder

Links – Tools (Cont.)

ITS4
http://www.citigal.com/its4/

Kismet
http://www.kismetwireless.net/

Klocwork
http://www.klocwork.com/products/inspect.asp

OllyDbg
http://home.t-online.de/home/Ollydbg

Ettercap
http://ettercap.sourceforge.net

RATS
http://www.securesoftware.com

SoftICE
www.compuware.com/products/driverstudio/softice.html