Basics of Secure Software Design, Development and Test

Michael Howard
mikehow@microsoft.com
Senior Security Program Manager
Security Engineering Group & Comms
Microsoft Corp.

Last update: 8-Feb-2005

Agenda

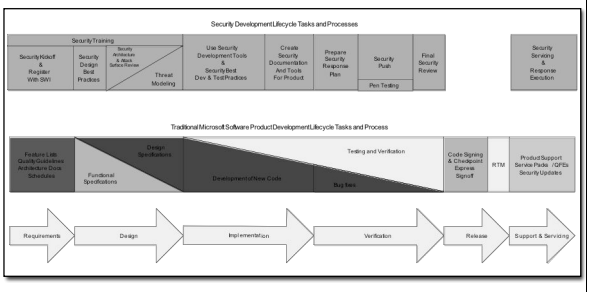
- Who?
- Trustworthy Computing
- Security Development Lifecycle
- Secure Design Tenets
- Threat Models
- Security Testing
- Coding Issues

The Security Engineering & Communications Group

- Help you secure your products
- "Security-as-in-threats" NOT "Security-as-in-crypto"

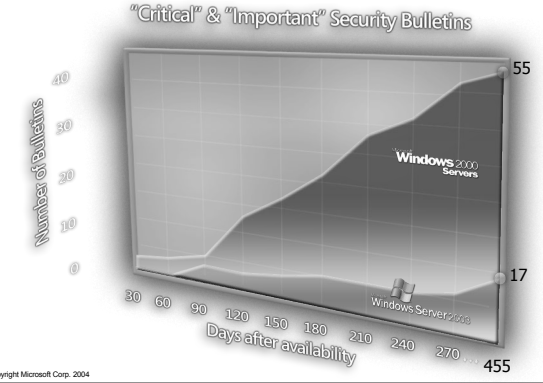
mailto:switeam
http://swi
http://msnsecurity/sdl

Security Development Lifecycle



5

Early Results of the SDL



6

A Case Study: MS04-011

VULNERABILITY IDENTIFIERS	IMPACT OF VULNERABILITY	WINDOWS 2000	WINDOWS XP	WINDOWS SERVER 2003
LSASS Vulnerability - CAN-2003-0533	Remote Code Execution	Critical	Critical	Low
LDAP Vulnerability – CAN-2003-0663	Denial Of Service	Important	None	None
PCT Vulnerability - CAN-2003-0719	Remote Code Execution	Critical	Important	Low
Winlogon Vulnerability - CAN-2003-0806	Remote Code Execution	Moderate	Moderate	None
Metafile Vulnerability - CAN-2003-0906	Remote Code Execution	Critical	Critical	None
Help and Support Center Vulnerability - CAN-2003-0907	Remote Code Execution	None	Critical	Critical
Utility Manager Vulnerability - CAN-2003-0908	Privilege Elevation	Important	None	None
Windows Management Vulnerability - CAN-2003-0909	Privilege Elevation	None	Important	None
Local Descriptor Table Vulnerability - CAN-2003-0910	Privilege Elevation	Important	None	None
H.323 Vulnerability* - CAN-2004-0117	Remote Code Execution	Important	Important	Important
Virtual DOS Machine Vulnerability - CAN-2004-0118	Privilege Elevation	Important	None	None
Negotiate SSP Vulnerability - CAN-2004-0119	Remote Code Execution	Critical	Critical	Critical
SSL Vulnerability - CAN-2004-0120	Denial Of Service	Important	Important	Important
ASN.1 "Double Free" Vulnerability - CAN-2004-0123	Remote Code Execution	Critical	Critical	Critical
Aggregate Severity of All Vulnerabilities		***Critical***	***Critical***	***Critical***

Code fixed in Windows Server 2003 (50%)

Code <u>not</u> fixed in Windows Server 2003 (50%)

Extra Defense in Windows Server 2003 (29% of)

7

Secure Design

- Reduce Attack Surface
  - Defense in Depth
  - Least Privilege
  - Secure Defaults

8

Defense in Depth (MS03-007)

Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable	Code fixed during the Windows Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Default maximum URL length (16kb) prevented exploitation (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)
Even if it there was an exploitable buffer overrun	Would only 'network service' privileges – commensurate with a normal user

9

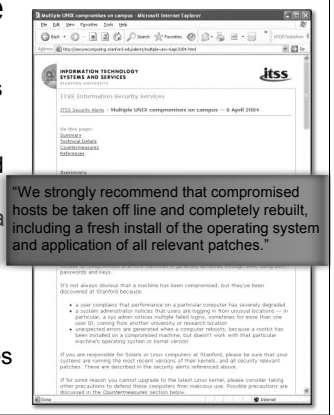
Least Privilege Problem Definition

- Not being an administrator helps ensure users cannot easily compromise a computer or the network
- The #1 ask of IT administrators interested in increased security and reducing TCO
  - Increased reliability
- Attractive to Abby, as it improves computer security and parental controls
  - Part of the spyware issue

10

Least Privilege

- Don't just run as admin so stuff works
  - Attacker's stuff works too!
- Look at Network and Local Service
- Don't write user data to HKLM, C:\Program Files or %windir%
  - Use HKCU or %userprofile%
- Don't open resources for ALL_ACCESS



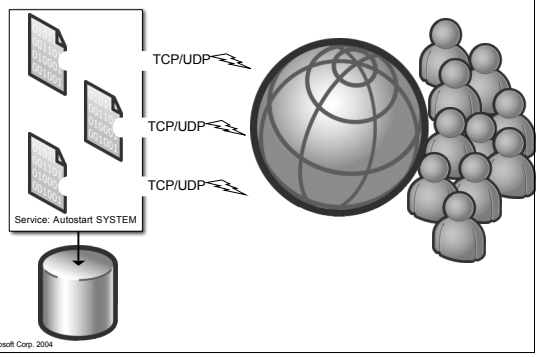
11

Secure Defaults

- Less code running by default = less stuff to attack by default
- Slammer & CodeRed would not have happened if the features were not enabled by default
- Reduces the urgency to deploy security fixes
  - A 'critical' may be rated 'important'
- Defense in depth removes single points of failure
- Reduces the need for customers to 'harden' the product
- Reduces <u>your</u> testing workload
- Reduce your attack surface <u>early</u>!

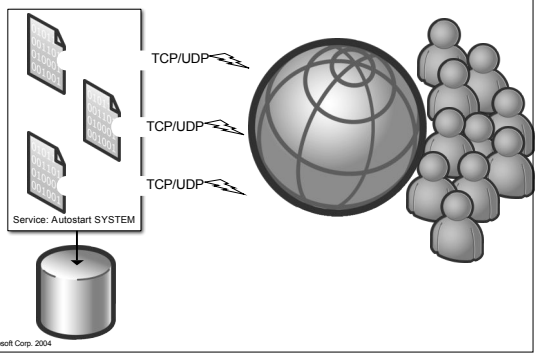
12

Attack Surface Reduction (ASR) Ideas



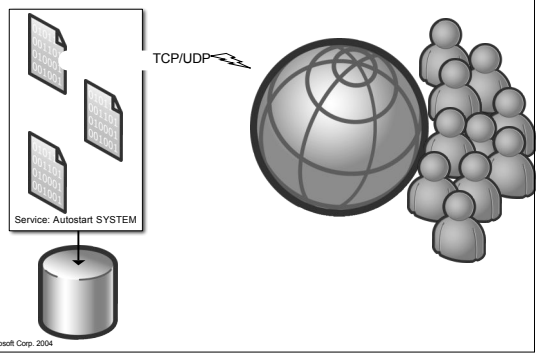
13

Turn off less-used ports



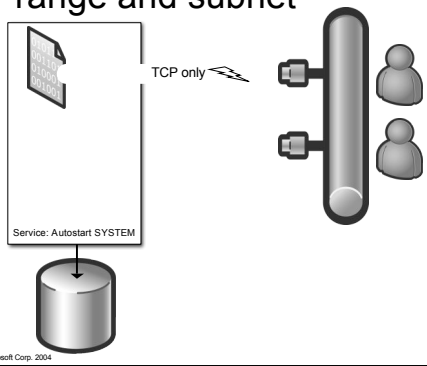
14

Turn off UDP connections



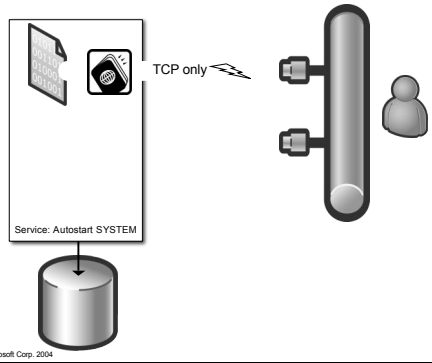
15

Restrict requests to a small IP range and subnet



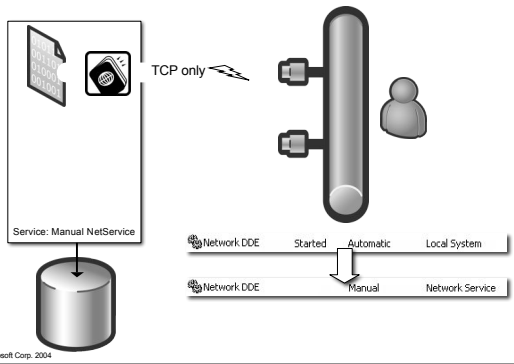
16

Authenticate Connections



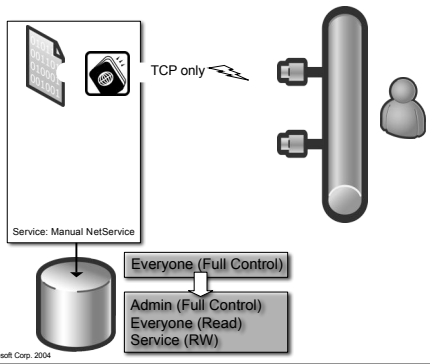
17

Reduce Privilege and Disable



18

Harden ACLs

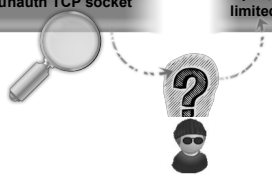


19

Increased Attack Surface means Increased Security Scrutiny…

- On by default
- Running as SYSTEM
- Open, unauth TCP socket

- Off by default
- Running with least priv
- Open, TCP socket limited to local subnet

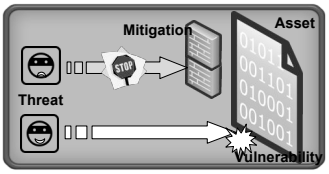


20

21

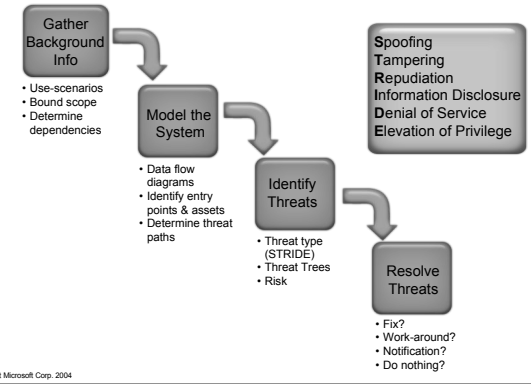
Threat Analysis

- Secure software starts with understanding the threats
- Threats are not vulnerabilities
- Threats live forever, they are the attacker's goal(s)



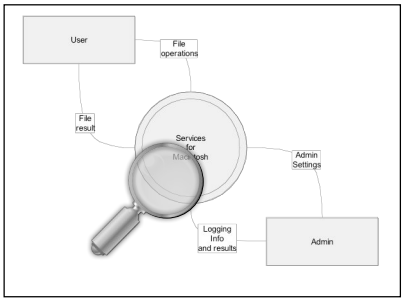
22

A Threat Modeling Process



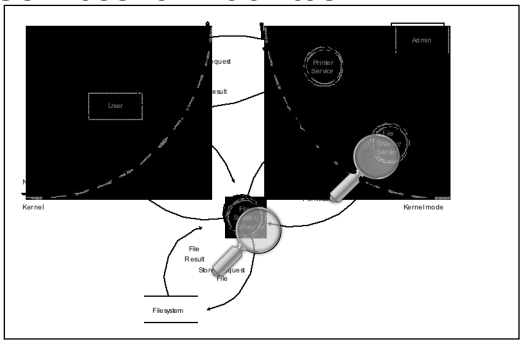
23

Context Diagram Services for Macintosh



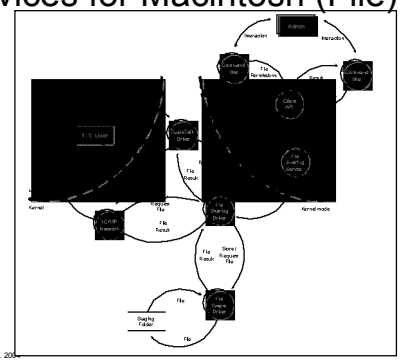
24

Level-0 DFD Services for Macintosh



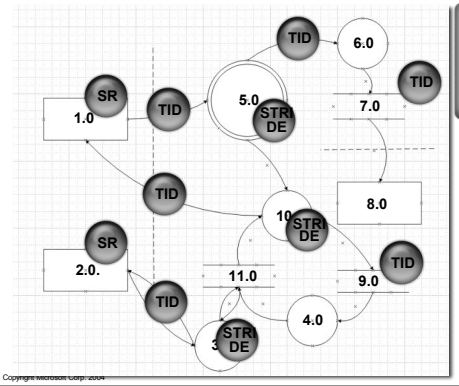
25

Level-1 DFD
Services for Macintosh (File)



26

Determining Threat Types



Each element in the DFD is susceptible to one or more threat types

27

DFD Elements are Threat Targets
A "Work list"

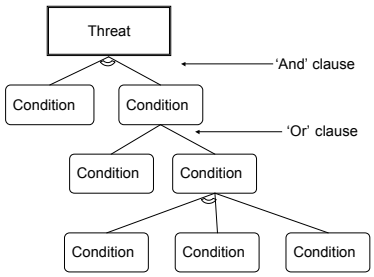
Data Flow	S	T	R	I	D	E
1 → 5		✓		✓	✓	
5 → 6		✓		✓	✓	
6 → 7		✓		✓	✓	
7 → 8		✓		✓	✓	
Data Store						
7		✓		✓	✓	
9		✓		✓	✓	
11		✓		✓	✓	
Interactor						
1	✓		✓			
2	✓		✓			
8	✓		✓			
Process						
3	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓

Each ✓ is a potential threat to the system.

Each threat is governed by the conditions which make the threat possible

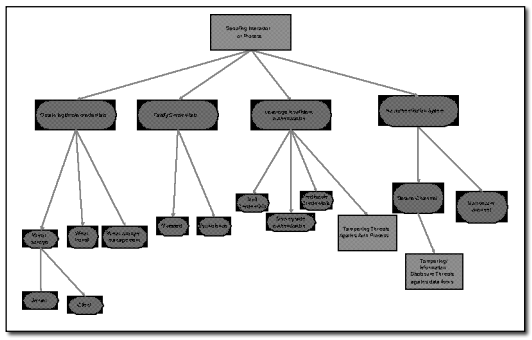
28

Threat Tree Format



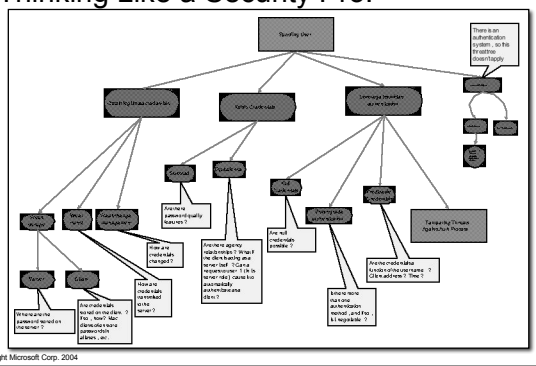
29

Threat Tree Pattern Examples
Spoofing



30

Threat Tree Pattern Examples
Thinking Like a Security Pro!



31

A Special Note about Information Disclosure threats

All information disclosure threats are potential privacy issues.
Raising the Risk.
Is the data sensitive or PII?

32

Calculating Risk with Numbers

- DREAD etc.
- Very subjective
- Often requires the analyst be a security expert
  - On a scale of 0.0 to 1.0, just how likely is it that an attacker could access a private key?
- Where do you draw the line?
  - Do you fix everything above 0.4 risk and leave everything below as “Won’t Fix”?

33

Calculating Risk with Heuristics

- Simple rules of thumb
- Derived from the MSRC bulletin rankings

34

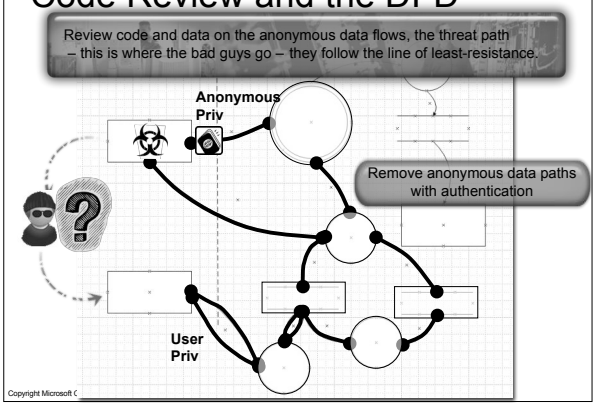
Mitigation Techniques

Threat	Mitigation Feature
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiaton
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Attend "Secure Design Principles"

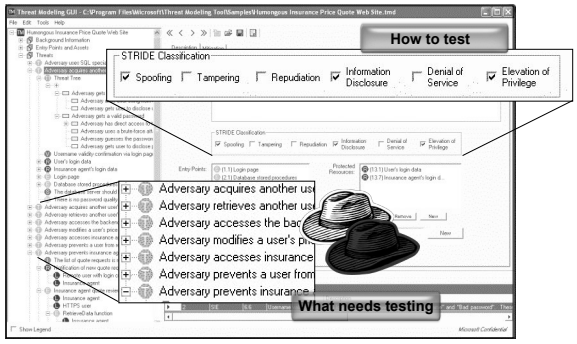
35

Code Review and the DFD



36

Testing Threats

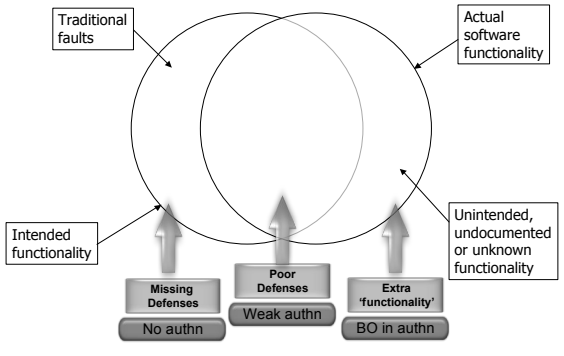


37

Security Testing

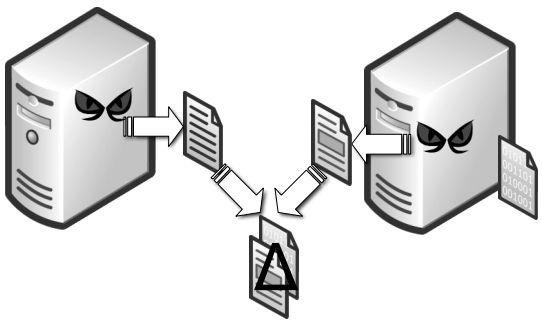
39

Security Testing



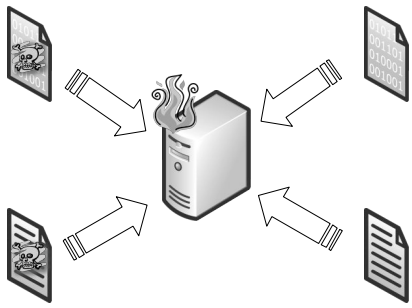
40

Testing Like an Attacker ‘Footprint’ the application



41

The Nature of Fuzzing



42

Fuzz the data!

Container
- Name (On)
- Link to other (Ol)
- Exists (Oe)
- Does not exist (Od)
- No access (Oa)
- Restricted Access (Or)

Network
- Replay (Nr)
- Out-of-sync (No)
- High volume (Nh)

Name/Contents
- Length (Cl)
- Random (Cr)
- NULL (Cn)
- Zero (Cz)
- Wrong type (Cw)
- Wrong Sign (Cs)
- Out of Bounds (Co)
- Valid + Invalid (Cv)
- Special Chars (Cp)
- Script (Cps)
- HTML (Cph)
- Quotes (Cpq)
- Slashes (Cpl)
- Escaped chars (Cpe)
- Meta chars (Cpm)

Length
- Long (Ll)
- Small (Ls)
- 0-Length (Lz)

43

Attack Ideas

- Rule #1 – There are no rules
  - Attacks by admins are uninteresting
- If you provide a client to access the server, don't use it!
  - Mimic the client in code
- If you rely on a specific service build a bogus one

44

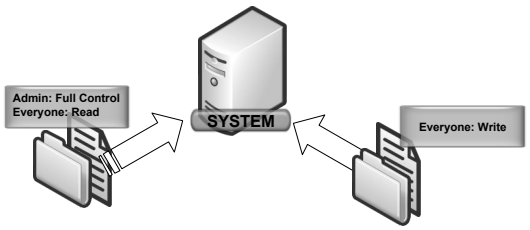
"Bang for the Buck" Attack Ideas

- Consume files?
  - Try device names and '..'
  - Look for: hangs, access to other files
  - Fuzz data structures
  - Look for: AVs or memory leaks (appverifier)
- Look for PII data in information disclosure threats
- ActiveX (especially Safe For Scripting)
  - Look at each method/property and ask, "what could a bad guy do"

45

“Bang for the Buck” Attack Ideas

- Look for privilege elevation boundaries
  - Pushing data from low-priv to high-priv process



46