



RANDY FRANKLIN SMITH'S
ULTIMATE WINDOWS SECURITY

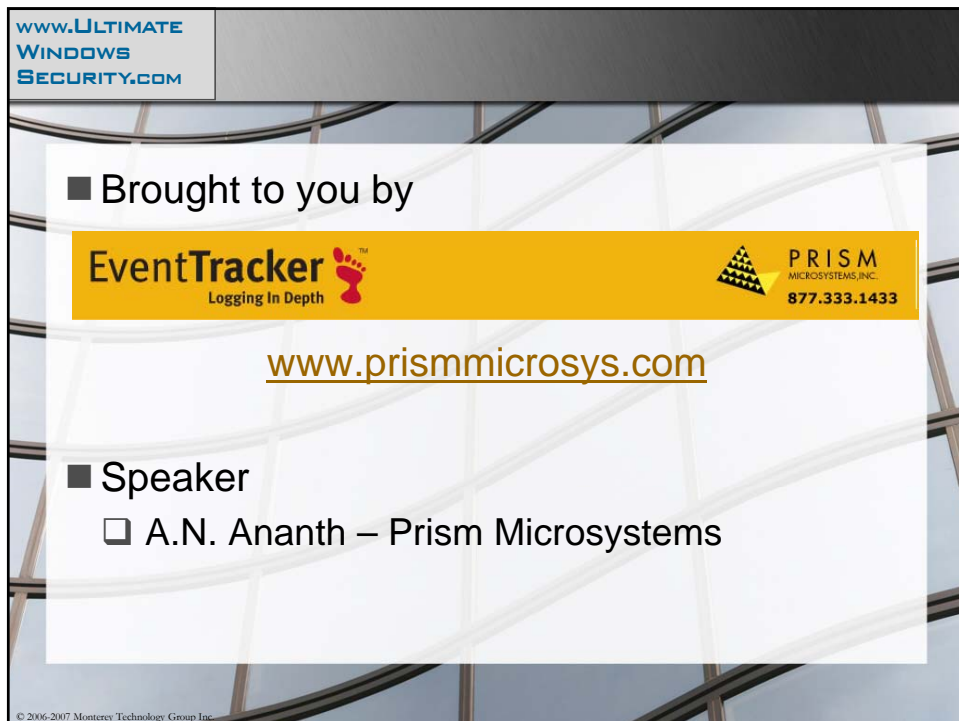
Auditing Program Execution with the Security Log

Security Log Secrets
Randy Franklin Smith





PRISM MICROSYSTEMS

Download slides now at
<http://www.ultimatewindowssecurity.com/programexecution.zip>
Don't forget to dial in
(641) 715-3222, access code 480-348-260



www.ultimatewindowssecurity.com

■ Brought to you by



www.prismmicrosys.com

■ Speaker

- A.N. Ananth – Prism Microsystems

© 2006-2007 Monterey Technology Group Inc.

www.ultimatewindowssecurity.com

Key Points

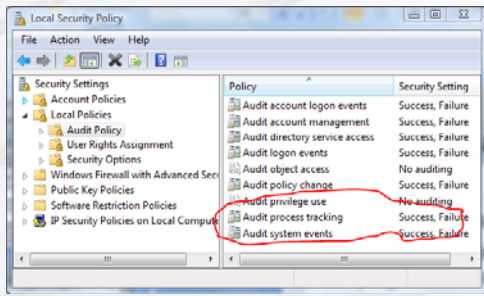
- Auditing Program Execution with the Security Log
 - Audit setup
 - Event IDs
 - Putting knowledge to work
 - What programs did this user execute?
 - How long did the program run?
 - Detect new programs run for the first time
 - What are all the unique programs executed on this server over a period of time?
 - How to recognize new malware

3

www.ultimatewindowssecurity.com

Auditing Program Execution with the Security Log

- Setup
 - Just enable “Audit process tracking”
 - On all computers where you want to track program execution



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

4

www.ultimatewindowssecurity.com

Auditing Program Execution
with the Security Log

■ Event IDs

- ❑ 592 - A new process has been created
- ❑ 593 - A process has exited

5

www.ultimatewindowssecurity.com

Auditing Program Execution
with the Security Log

■ Event ID 592

Event Type:	Success Audit
Event Source:	Security
Event Category:	Detailed Tracking
Event ID:	592
Date:	10/18/2007
Time:	2:29:14 PM
User:	ELMW2\Administrator
Computer:	RFSW3R2
Description:	A new process has been created: New Process ID:2167588800 Image File Name:\WINNT\system32\notepad.exe Creator Process ID:2167187648 User Name:administrator Domain:ELMW2 Logon ID:(0x0,0x804C2)

6

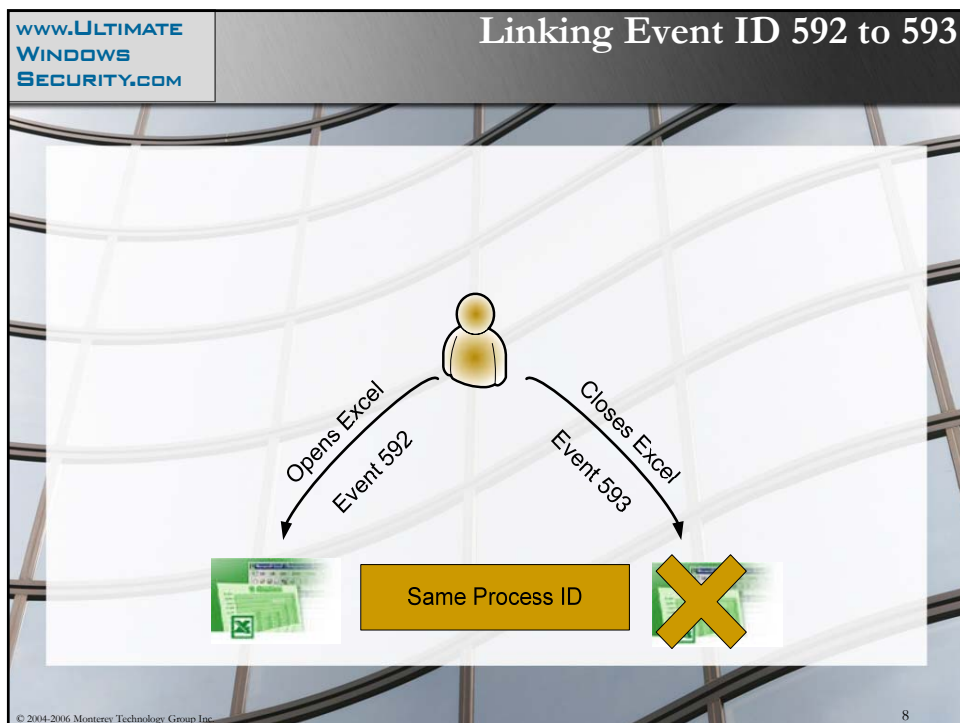
www.ultimatewindowssecurity.com

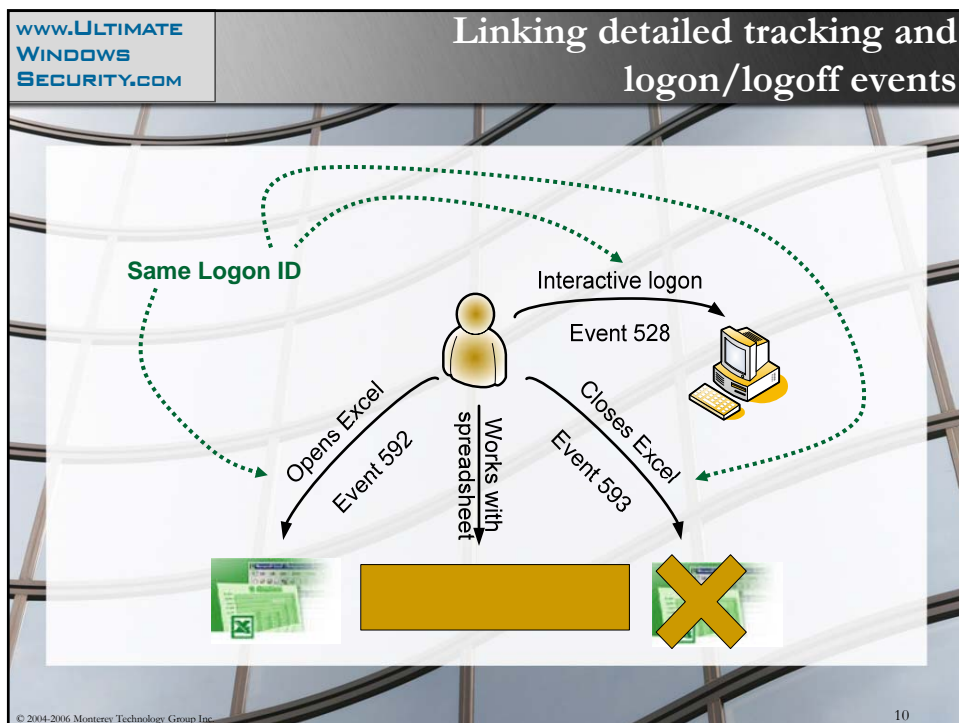
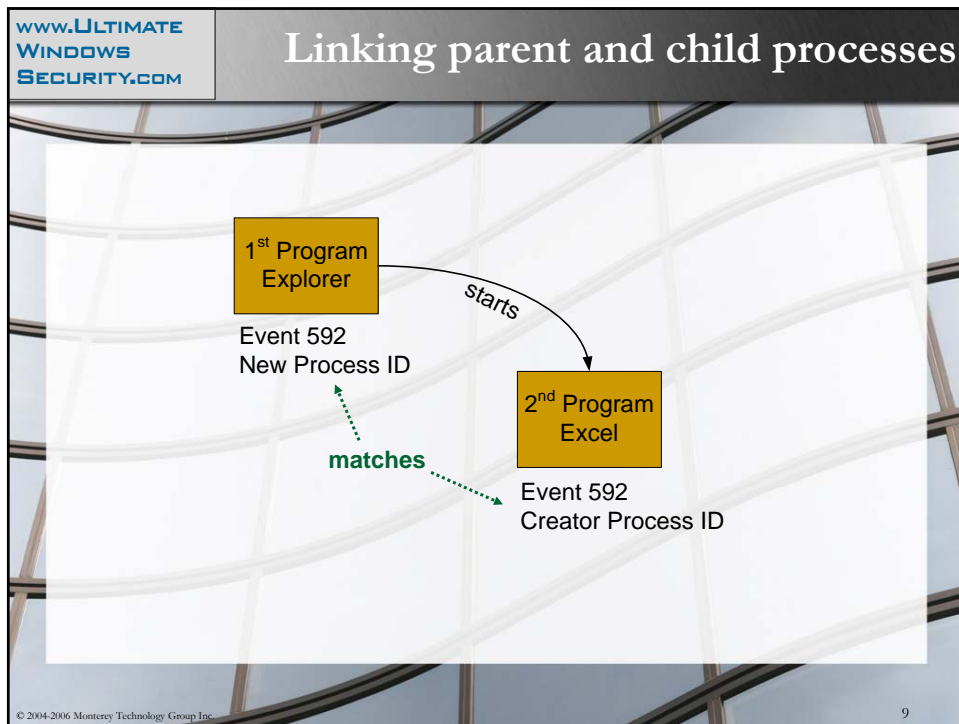
Auditing Program Execution
with the Security Log

■ Event ID 593

Event Type:	Success Audit
Event Source:	Security
Event Category:	Detailed Tracking
Event ID:	593
Date:	10/18/2007
Time:	2:29:14 PM
User:	ELMW2\Administrator
Computer:	RFSW3R2
Description:	A process has exited: Process ID:2084 Image File Name:C:\WINDOWS\system32\notepad.exe User Name:administrator Domain:ELM Logon ID:(0x0,0x158EB7)

7





www.ultimatewindowssecurity.com

Auditing Program Execution with the Security Log

- Putting knowledge to work
 - ❑ What programs did this user execute?
 - ❑ How long did the program run?
 - ❑ Detect new programs run for the first time
 - ❑ What are all the unique programs executed on this server over a period of time?
 - ❑ How to recognize new malware

11

www.ultimatewindowssecurity.com

Auditing Program Execution with the Security Log

- What programs did this user execute?

Report

Event Type:	Success Audit
Event Source:	Security
Event Category:	Detailed Tracking
Event ID:	592
Date:	10/18/2007
Time:	2:29:14 PM
User:	ELMW2\Administrator
Computer:	RFSW3R2
Description:	A new process has been created: New Process ID:2167588800 Image File Name:\WINNT\system32\notepad.exe Creator Process ID:2167187648 User Name:administrator Domain:ELMW2 Logon ID:(0x0,0x804C2)

Filter

12

www.ULTIMATE
WINDOWS
SECURITY.COM

Auditing Program Execution with the Security Log

■ How long did the program run?

Opens Excel
Event 592

Closes Excel
Event 593

Same Process ID

13

www.ULTIMATE
WINDOWS
SECURITY.COM

Auditing Program Execution with the Security Log

■ Putting knowledge to work

- ❑ What are all the unique programs executed on this server over a period of time?
 - Collect 592s over period of time
 - Get a distinct list of image filenames from 592s

14

www.ULTIMATE
WINDOWS
SECURITY.COM

Auditing Program Execution with the Security Log

- Detect new programs run for the first time
 - Establish baseline
 - Previous slide
 - Start checking new 592s against baseline
 - New image filename? → alert!

15

www.ULTIMATE
WINDOWS
SECURITY.COM

Auditing Program Execution with the Security Log

- How to recognize new malware
 - Establish baseline for entire organization
 - Alert on new image file names
 - Caveat: doesn't address non EXEs

16

www.ultimatewindowssecurity.com

Auditing Program Execution with the Security Log

■ How was the user logged on when he ran this program?

□ Link back to logon event

- Event ID 528 or 529
- Correlate by logon ID
- Check logon type

Event ID 528
 Successful Logon:
 User Name:administrator
 Domain:ELM
 Logon ID:(0x0,0x558DD)
 Logon Type:2
 Workstation Name:W2MS
 Source Network Address:10.42.42.170

Event ID 592
 A new process has been created:
 New Process ID:2167588800
 Image File
 Name:\WINNT\system32\notepad.exe
 Creator Process ID:2167187648
 User Name:administrator
 Domain:ELMW2
 Logon ID:(0x0,0x558DD)

www.ultimatewindowssecurity.com/logontypes.html

17

www.ultimatewindowssecurity.com

Auditing Program Execution with the Security Log

■ Where was the user when he executed the program?

□ Link back to logon event

- Event ID 528 or 529
- Correlate by logon ID
- Check logon type

Event ID 528
 Successful Logon:
 User Name:administrator
 Domain:ELM
 Logon ID:(0x0,0x558DD)
 Logon Type:2
 Workstation Name:W2MS
 Source Network Address:10.42.42.170

Event ID 592
 A new process has been created:
 New Process ID:2167588800
 Image File
 Name:\WINNT\system32\notepad.exe
 Creator Process ID:2167187648
 User Name:administrator
 Domain:ELMW2
 Logon ID:(0x0,0x558DD)

18

www.ultimatewindowssecurity.com

Auditing Program Execution
with the Security Log


- Remember
 - ❑ Enable “Audit process tracking events”
 - ❑ Filter on 592
 - And 593 if you want to know how long the program ran
 - ❑ Link back to 528/529 for logon information
 - ❑ Baseline image file name to detect new programs

19

www.ultimatewindowssecurity.com

- Speakers
 - ❑ Randy Franklin Smith
 - A. N. Ananth
- Brought to you by

EventTracker[™]
Logging In Depth

 PRISM
MICROSYSTEMS, INC.
877.333.1433

© 2006-2007 Monterey Technology Group Inc.