Software Forensics

Robert M. Slade, MS, CISSP
rslade@vcn.bc.ca
http://victoria.tc.ca/techrev/rms.htm
Electronic Fingerprints

• Introduction and definitions
• Forensic linguistics signatures and fingerprints
• Presentation in court
Introduction and definitions

- digital forensics
- computer forensics - data recovery
- network forensics - packets, headers and logs
- software forensics - code analysis
- forensic linguistics
  - authorship analysis, stylistics, stylometry, forensic linguistics, or forensic stylistics
Objectives of Software Forensics/Programming

• intention/purpose/function of malware
• versions and "families" of malware
• cultural or group identity of programmer
• specific identity of programmer
Software Forensics History

• Virus research
• Forensic programming
Forensic linguistics signatures and fingerprints

• Individual identification
  – Group identification

• Content analysis
  – Error analysis

• Non-content analysis
  – Additional non-content indicators
Objects and tools

• objects of analysis
  – text strings, source code, object (machine) code

• fp tools
  – trial runs (bait/goat systems/files)
  – hex editors
  – sector/disk access (f-pbr, f-boot, DEBUG)
  – disassemblers (DEBUG, Codeview, IDA Pro)
Knowledge base

• Assembly/machine language programming concepts
  – CPU structure, operations
  – registers, memory usage
  – opcodes, interrupts
Programming cultures and cultural indicators

• user interfaces and commands
  – (MS Windows/CUA, text editors)

• program structures (MS Windows vs UNIX)

• program versions (Ohio/Den Zuk)
  – virus and malware families and variants

  (Jerusal, Melissa/Papa/credit charge message)

• compiler signatures
Programming cultures and indicators

- functions
- interface
- programming style
- program requirements
- most indicators come from reviewing/using many programs
- indicators change as development technology changes
  - in 1990 CUA indicated IBM experience, now indicates Windows
user interface

- Winamp uses amplifier/stereo interface
- DOS "/" switches
- UNIX "-" switches
- WordStar, Sidekick follow UCSD Pascal editor
- Perfect Writer followed emacs
- help systems
- Windows - tree structure and index - must know keyword
- Word Perfect - keyboard shortcuts, function lookup, synonyms
- PINE - key commands - only a few pages for the whole set
program structure

• Windows large multifunction programs
• UNIX small single function programs
• Windows APIs and libraries
• UNIX piping
• Windows interface integrated, down to OS level
• UNIX interface over simple programs
program requirements

- will program run on older CPUs, limited memory, limited disk space
  - originally programmed on limited hardware?
  - programmer used to limited hardware?
- does program conserve memory at the expense of cycles?
  - programmer used to limited memory, good program runs at all
- does program conserve cycles?
  - programmer used to "real time" programming restraints
- latter examples indicated at machine level only
  - only in optimized code, indicates assembly programming
Function indicators

- heuristic signatures (PSQR)
- operation/port scanning and logs
- Interrupts
- dangerous operations
Cusum analysis

- Cusum chart of text written by the same author
  - chart from "Analysing for Authorship" and may be found at http://hometown.aol.com/qsums
Cusum analysis

- Cusum chart of text written by different authors
  - chart from "Analysing for Authorship" and may be found at http://hometown.aol.com/qsums

Copyright Robert M. Slade, 2002-5
419 and phishing
Presentation in Court

• Rules of evidence
• Hearsay
• Technical issues
• Expert witness
Legal and ethical considerations

- Canadian law
  - "cause to be modified"

- international law

- evidence and proof
  - "hacker code"

- ethical standards

- disclosure and special considerations for malware

- present
Summary

- forensic linguistics provides strong corroboration
- these techniques must be presented carefully in court