Arriving at an Anti-forensics Consensus

Examining How to Define and Control the Anti-forensics Problem

Ryan Harris
CERIAS, Purdue University
DFRWS 2006

What is the problem?

- Lack of agreement about how to define anti-forensics
- No way to classify anti-forensic methods

Some current views of anti-forensics

- Ways to "avoid detection" or "break industry tools" Foster & Liu
- Hiding a system intrusion attempt Shirani

Based on Saferstein's definition

- Anti-forensics:

  "Methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system."

Viewing anti-forensics differently

- Ways to "...limit the identification, collection, collation and validation of electronic data..." Peron & Legary
- "Attempting to limit the quantity and quality of forensic evidence..." Grugq

Evidence and process based definition

- Anti-forensics:

  Any attempts to compromise the availability or usefulness of evidence to the forensics process.

Categorizing anti-forensic methods

Peron & Legary	Rogers
Hiding	Data hiding
Destroying	Artifact wiping
Preventing from being created	
Manipulating	
	Trail obfuscation
	Attacks against the process & tools

Proposed categories

- Evidence Destruction
- Evidence Hiding
- Evidence Source Elimination
- Evidence Counterfeiting

Evidence Destruction

- Dismantling evidence or making it unusable to the investigative process
- Physical example: Wiping fingerprints
- Digital example: Wiping a filesystem

Evidence Hiding

- Removing evidence from view
- Physical example: throwing a gun into the sewer
- Digital example: Steganography

Evidence Source Elimination

- Neutralizing evidentiary sources
- Physical example: Wearing gloves during a crime
- Digital example: Disabling audit trails

Evidence Counterfeiting

- Creating a “faked” version of the evidence
- Physical example: planting fingerprints
- Digital example: Using a different user’s account

Anti-forensic attacks - human element

- Alert investigators
- Education
- Real world experience
- “Thinking outside the box”

Anti-forensic attacks - tool dependence

- Tool assumptions
- Implementation bugs

Anti-forensic attacks – physical/logical

- Storage space
- Time
- Money

Presentation references

- J. C. Foster and V. Liu. Catch me if you can... In *Blackhat Briefings 2005*, 2005. URL http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf.
- Grugq. The art of defiling: Defeating forensic analysis. In *Blackhat Briefings 2005*, 2005. URL http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-grugq.pdf.
- C. S. J. Peron and M. Legary. Digital anti-forensics: Emerging trends in data transformation techniques. n.d. URL http://www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf.
- M. Rogers. Anti-forensics. 2005. URL http://www.cyberforensics.purdue.edu/docs/Lockheed.ppt.
- R. E. Saferstein. *Criminalistics: An Introduction to Forensic Science.* Prentice Hall, Upper Saddle River, NJ, 6th edition, 1998.
- B. Shirani. Anti-forensics. High Technology Crime Investigation Association, 2002. URL http://www.aversion.net/presentations/HTCIA-02/anti-forensics.ppt.

Questions/Comments?