Detection of Insider Turning Behaviors with Forensic Methods

2012-01-24

DoD CyberCrime Conference

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

This research was funded in part by DARPA contract W31P4Q-11-C-0216

Your speaker

- Knowledge, Skills, and Experience:
  - POST certified trainer in these areas, admitted to testify as an expert in Federal, State, and Local Criminal and Civil digital forensics matters, published refereed and other articles on the subject, authored a book on the subject and another book closely related to it, taught at Federal Law Enforcement Training Center in this area, taught graduate classes at University of New Haven in this area, teaches graduate classes and heads the Ph.D. program at CalSci in digital forensics, DARPA funded researcher in using digital forensic methods to detect insiders, etc.
- Education:
  - B.S., M.S., and Ph.D. in relevant field

Outline

- What is a turning behavior?
- How can we detect it with forensic methods?
- The details of current technologies
- Questions / Comments?

Turning behaviors

- A typical scenario
  - Loyal individual authorized to perform functions
  - Something happens
  - They start to question their loyalty
  - More things happen
  - They start to do bad things
  - They realize that they might get caught
  - They cover up
  - They do really bad things

Turning behaviors

- An actual case
  - Longstanding employee on travel
  - Loses a receipt and cannot get reimbursed
  - They're not fair to me, why should I be punished
  - It happens again, they mock up receipts to get paid
  - They realize that they might get caught
  - They start deleting fake paperwork as they get paid
  - They start to fake receipts for phoney expenses
- They were caught after stealing more than $1M

Turning behaviors

- An actual case
  - Network administrator managing a critical network
  - Change of boss requires more rigor in their work
  - Why take orders from them when they need me?
  - Financial and companion pressure builds
  - They use the network to set up a personal business
  - They are detected, reprimanded, told to stop
  - They use technical concealment and expand
  - They repeatedly crash the network and “save the day”
- They were convicted on counts including sabotage

Turning behaviors

- An actual case
  - Systems administrator for highly sensitive systems
  - Abused by peers because of sexual orientation
  - Question loyalty openly among Internet groups
  - Hazing gets worse by far
  - They start talking to opposition intel organizations
  - They realize that they might get caught
  - They find ways to operate without obvious detection
  - They exfiltrate large volumes of sensitive information
- Currently pending trial for many leaked documents

Turning behaviors - example

- An actual case
  - VP sales/marketing after years of service
  - Their ideas for growth are not adequately taken up
  - They start to think they should be in charge
  - They have an opportunity to build a competitor
  - They start to move information to a pre-startup
  - They realize that they might get caught
  - They start deleting the records of their exfiltration
  - They leave the company and start the competitor
- Lost $10M in a civil suit – gained a $500M business

Outline

- What is a turning behavior?
- How can we detect it with forensic methods?
- The details of current technologies
- Questions / Comments?

Detecting turning behaviors

- It's not the crime
  - They are authorized to do what they are doing
  - If they are disloyal in doing it, it's still authorized
  - After the big damage is done may be too late
- It's the cover-up
  - When they start to realize they might get caught
  - They tend to cover up their bad acts
  - They tend to escalate after they become confident in their ability to go it and not get caught
  - So the cover up starts before the big damage is done

Detecting cover-ups

- A cover-up implies “changing history”
  - Deleting/destroying/hiding undesired records
  - Creating desired records
  - In other words, forgery
- Forgery is simple in the digital world – isn't it?
  - Delete bad records / create good records
  - Example email “forgery”:

    telnet mail.all.net - helo joe.com

    mail from <fc@joe.com> - rcpt to <joe@all.net>

    data ... - . - quit
  - The mail goes through – looks real enough

Detecting cover-ups

- Simple forgery is easy – and easily detected
  - Computers generate redundant records
  - Simple forgery tends to ignore this
  - So it fails to find and forge all the redundant records
- Email example detection questions:
  - Are the IP address and server name inconsistent with actual patterns from other (legitimate) deliveries?
  - Are the header fields (e.g., Message-ID) consistent with other messages from the same source?
  - Are the reception records consistent with the records kept on the purported sending system?
  - Does the asserted sender deny having sent it?

Forged expense receipt example

- Simple forgery is easy – and easily detected
  - Computers generate redundant records
  - Simple forgery tends to ignore this
  - So it fails to find and forge all the redundant records
- Phony receipt example questions:
  - Is printer used inconsistent with the claimed source?
  - Are scan records consistent with stored scanned files?
  - Is the font of the receipt internally consistent?
  - Is the print date later than the activity date?
  - Are amounts consistent with Benford's law?

Stolen records example

- Simple cover-ups are easy – and easily detected
  - Get records, email them out, delete the local copies
  - Computers generate redundant records
  - Simple cover-ups tend to ignore this
  - So they fails to cover up all the redundant records
- Example stolen record questions:
  - Are database queries consistent with claimed uses?
  - Are local copies consistent with backup copies?
  - Are SQL logs consistent with records found?
  - Are cached copies consistent with stored copies?
  - Are email server logs consistent with user email logs?

What's the common thread?

- Changing history is not so easy to do undetectably
  - Redundant records created by systems make faking all redundant records very hard to do correctly
  - But cover-ups only need to hold for a limited period and against limited scrutiny
- Attempts to change history are often readily detected
  - After the fact, inconsistent changes are often detected
  - Self-proclaimed experts commonly miss obvious things
  - Most detected insiders turning are rank amateurs when it comes to covering up their activities
- But to find we must look
  - Most detection is only after we have the suspect

From post-facto to pre-facto

- How do we move from forensics to detection?
  - ...
  - They start to do bad things
  - They realize that they might get caught
  - **They cover up**
  - ...
- It's not the crime, it's the cover-up
  - Detect the cover-up in time and you may beat the high consequences that ultimately result
  - But there are significant challenges there...

Outline

- What is a turning behavior?
- How can we detect it with forensic methods?
- The details of current technologies
- Questions / Comments?

Challenges with current methods

- Legal issues
  - Probable cause, reasonable suspicion, and searches
    - Corporate / classified systems may have exceptions
    - Investigation in non-LE context are problematic
    - You need the evidence of a crime to search
    - If you had the evidence, you wouldn't need to search
  - The “systems administration” approach
    - Normally an exception to maintain proper operations
    - But trying to slide it in that way is problematic
    - Can you “willy nilly” look for “bad” insider things?
- Technical issues
- Research issues

Challenges with current methods

- Legal issues
- Technical issues
  - Suppose you can look – how do you do it?
    - You have to know what to look for
    - There are many possible cover-up indicators
    - How do you deal with false positives and negatives?
  - What / how much data do you have to preserve?
    - You can't keep the state of all machines for all time
    - If you could, searching it would be problematic
    - How small is the needle and how big the haystack?
- Research issues

Challenges with current methods

- Legal issues
- Technical issues
- Research issues
  - You need “informed consent” - how do you get it?
    - If you don't tell them you are looking for insiders, it's not informed consent
    - If you do tell them, insiders may avoid doing bad things during the experiment
  - How do you get base rate data
    - Since you don't know about any “real” insiders till you get to the end of the prosecution process, how do you judge an indication as to being true or false?

Our current approach

- Identify inconsistencies (from known turning behaviors)
  - Gather examples from current / closed cases
    - Research the details for known turning cases
    - Do you have any data that would help?
    - These tend to involve classified content/systems
  - Identify feasible detection candidates
    - We have found some number of large classes
- Find low base rate presumptive positives
- Particularize by seeking additional data to resolve cause
- Individualize by the process of elimination
- Provide detailed evidential basis for conclusions

Our current approach

- Identify inconsistencies (from known turning behaviors)
- Find low base rate presumptive positives
  - Similar systems environments are necessary for this
    - These tend to be classified systems for government
  - Collecting large amounts of data from many systems
    - Even more classification issues in the aggregate
  - Identify feasible candidates with low base rates
    - We have identified some number of subclasses
- Particularize by seeking additional data to resolve cause
- Individualize by the process of elimination
- Provide detailed evidential basis for conclusions

Our current approach

- Identify inconsistencies (from known turning behaviors)
- Find low base rate presumptive positives
- Particularize by seeking additional data to resolve cause
  - This emulates the human investigative process
    - Identify causal sequences for classes of indicators
    - Test for traces of different causal chains
    - Disregard cases refuted by enough traces
    - Recurse to the next causal step
  - NOTE: non-unique causes for most digital traces
- Individualize by the process of elimination
- Provide detailed evidential basis for conclusions

Our current approach

- Identify inconsistencies (from known turning behaviors)
- Find low base rate presumptive positives
- Particularize by seeking additional data to resolve cause
- Individualize by the process of elimination
  - Who are the possible suspects
    - Those with (recursive) access?
  - Who was present at the times?
    - What is the evidence for this?
    - Is it internally consistent?
    - If not, what are the explanations, etc.?
- Provide detailed evidential basis for conclusions

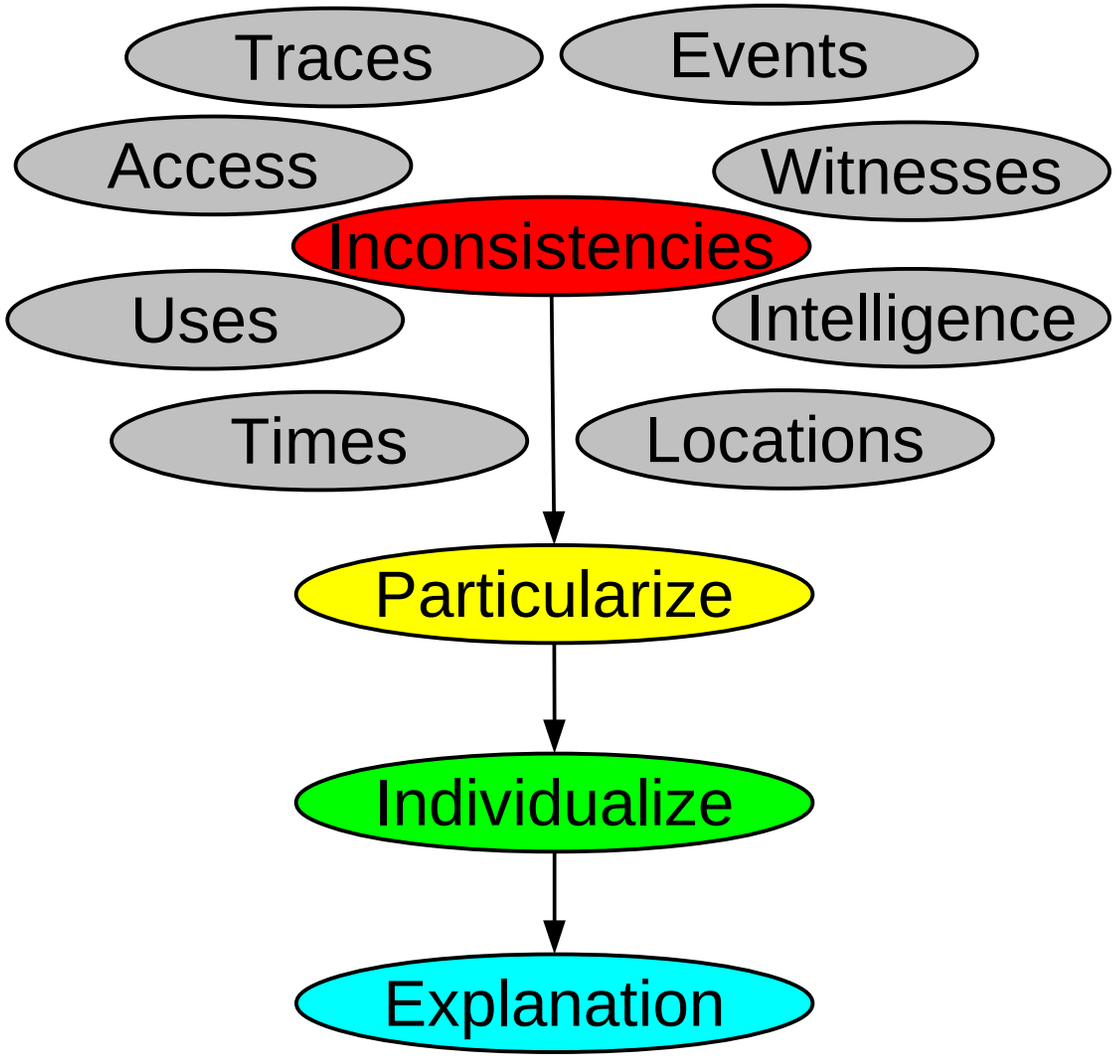
Our current approach

- Identify inconsistencies (from known turning behaviors)
- Find low base rate presumptive positives
- Particularize by seeking additional data to resolve cause
- Individualize by the process of elimination
- Provide detailed evidential basis for conclusions
  - The basis is in terms of:
    - Inconsistencies found (and details of traces and why)
    - Hypothesized causal chains confirmed and refuted
    - Recurse till particularized
    - Recurse till individualized
    - Explained in English sentences with supporting data
    - Linked to sources of traces for forensic verification

Demonstration

Summary

- **What it does:** Detect inconsistencies produced by insiders covering up bad acts as they change loyalties.
- **Data expectations:** redundant information from internal and external sources.
- **Output:** Detected indicators, particularization, and individualization with the detailed basis for each identified situation.
- **What it tells us:** That certain individuals are covering up their behaviors.



Outline

- What is a turning behavior?
- How can we detect it with forensic methods?
- The details of current technologies
- Questions / Comments?

Thank You

http://all.net/ - fc at all.net