Forensic Methods for Detecting Insider Turning Behaviors

2012-05-25

IEEE WRIT

Workshop on Research on the Insider Threat

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

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?

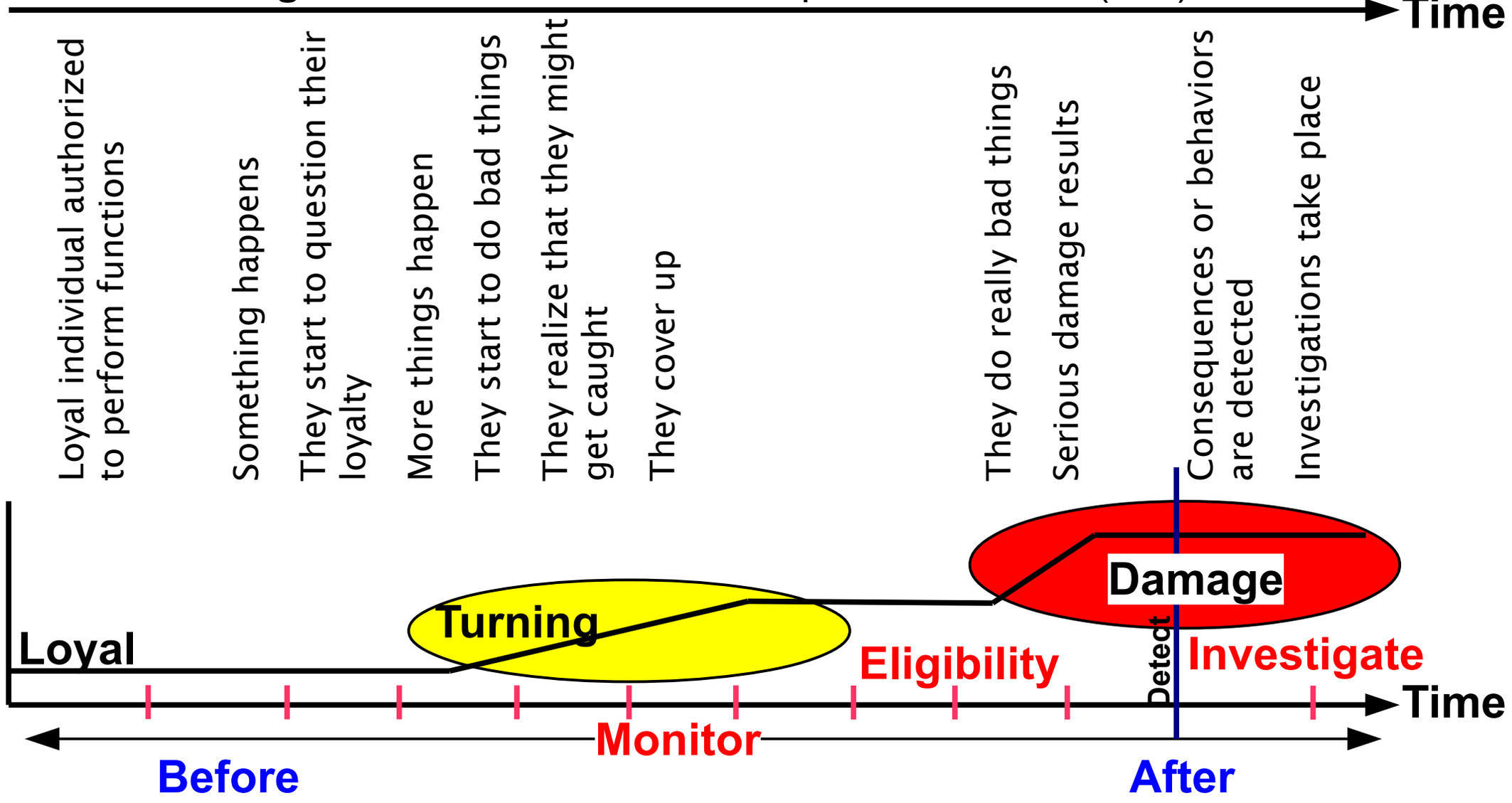
Turning behaviors - example

- An example 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

J. Yang and K. Gelles, “Poll reveals 75% prefer an honest day's work” in USA Today, November 18, 2011, citing a Monster.com survey.

Turning behaviors

- **Current processes:**
  - **Eligibility:** Access to a lot of data based on permission – use control
  - **Monitor:** Limited access - operational necessity for continuity
  - **Investigate:** Limited access UNTIL probable cause (etc.)

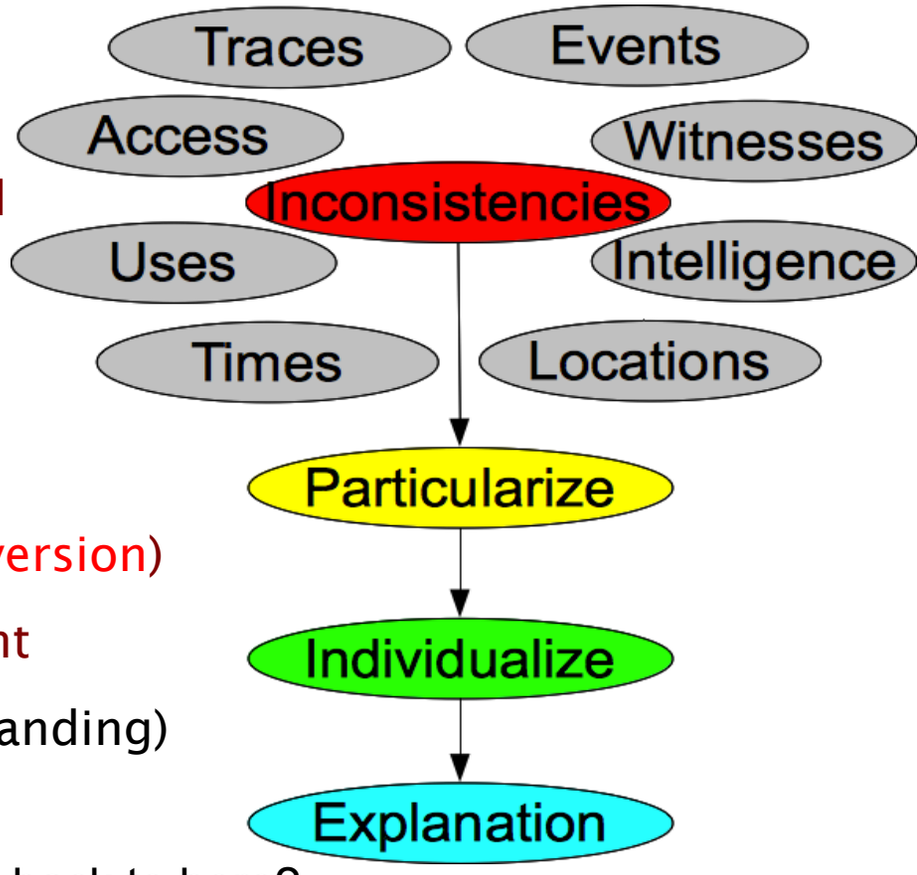


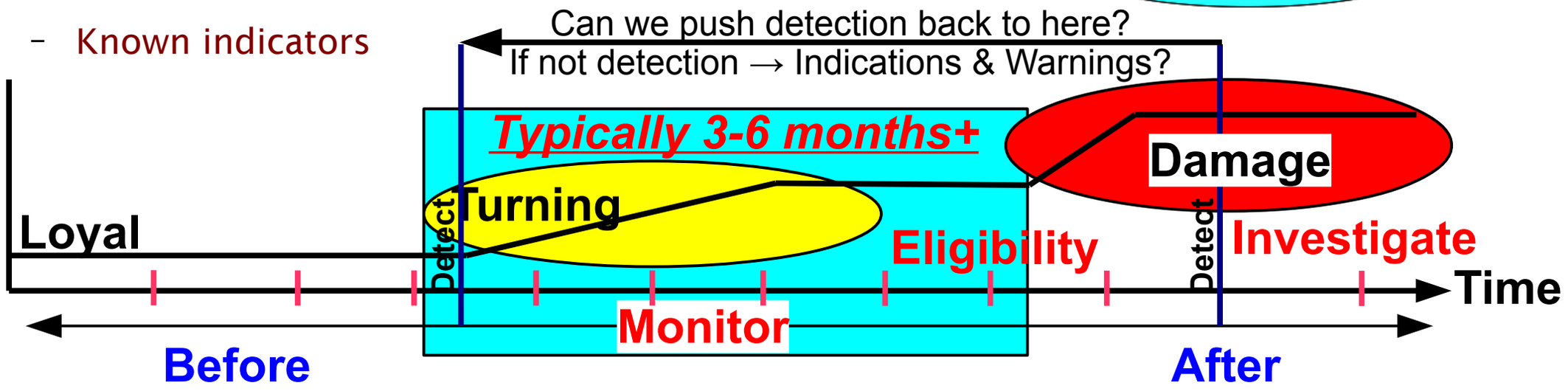
Turning behaviors

- An example 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

Detect 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 (a.k.a., subversion)
  - They tend to escalate after they become confident
- Detect their tradecraft (requires timely data and understanding)
  - Inconsistencies
  - Known indicators



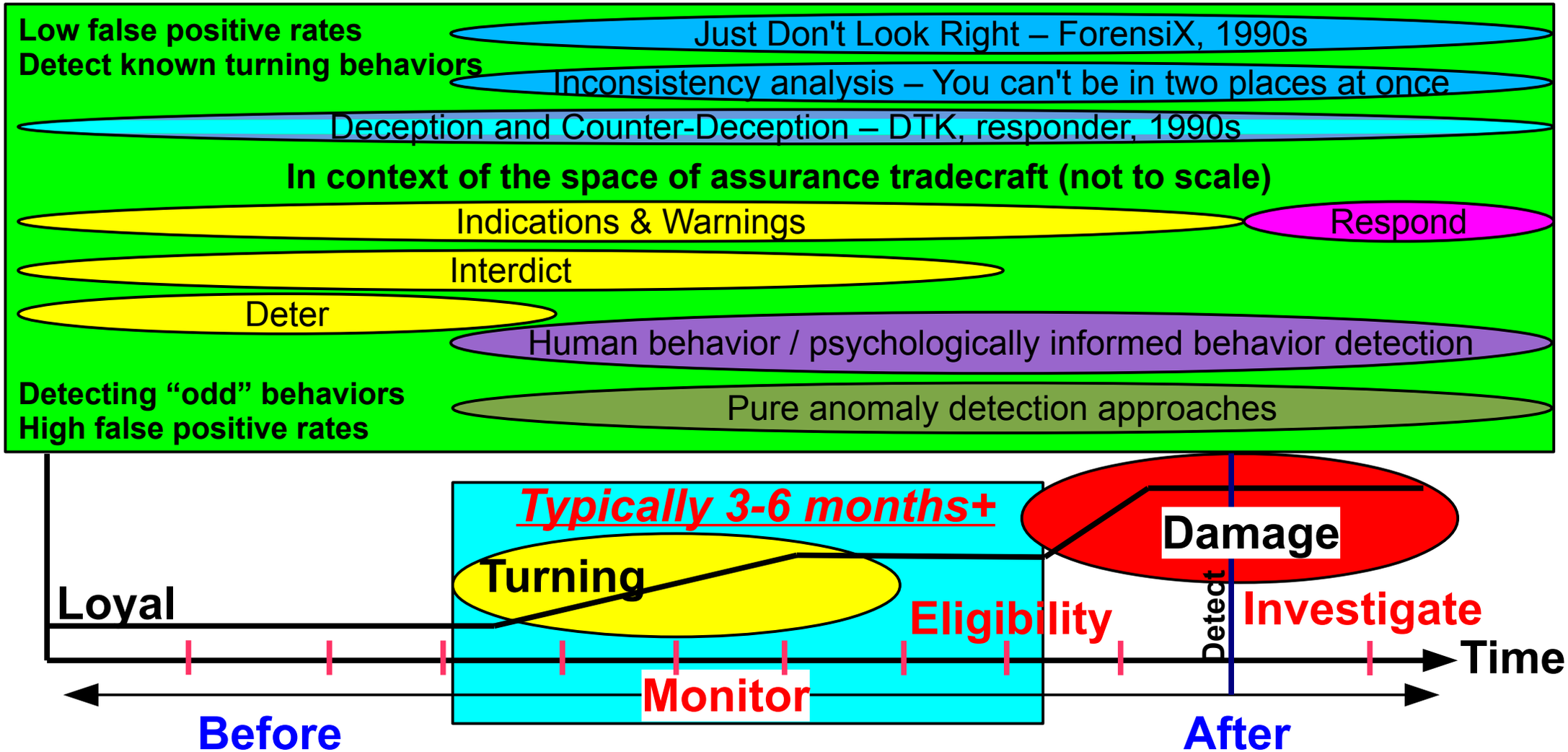


Outline

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

A bigger picture

- Tradecraft is used to conceal bad acts: [we know this from our ongoing studies]
  - Detect specific classes of tradecraft (e.g., JDLR) [specific cases and methods]
  - Detect the presence of tradecraft (e.g., inconsistencies) [specific cases and methods]
- Bigger picture: Detect damage and react → {Deter, Interdict, I&W, Respond, Adapt}



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?

```
Delivered-To: lizzrose@gmail.com
Received: by 10.210.113.9 with SMTP id l9cs410537ebc;
        Tue, 07 Jul 2010 17:36:00 -0800 (PST)
Received: by 10.141.35.21 with SMTP id n21mr4478671rvj.258.122643738269;
        Tue, 07 Jul 2010 17:35:58 -0800 (PST)
Return-Path: <wes@williamshapirolaw.com>
Received: from OMTA04.emeryville.ca.mail.comcast.net ([76.96.30.35])
        by mx.google.com with SMTP id 8si11684599ywg.6.2010.11.07.07.10.56;
        Tue, 07 Jul 2010 17:35:58 -0800 (PST)
Received: from Fearless ([69.181.207.29])
    by OMTA04.emeryville.ca.mail.comcast.net with comcast       id
 DCFP1c0010ebx0M8QCFPNi; Tue, 07 Jul 2010 17:35:57 +0000
Date: Tue, 07 Jul 2010 17:35:58 -0700
From: William Shapiro <wes@williamshapirolaw.com>
Subject: I enjoy eating Cheese Burgers and Fries
To: lizzrose@gmail.com
Message-id:
```

Simple forgery is easy – to detect

- 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

Outline

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

Our current approach

- Identify inconsistencies (from known turning behaviors)
- Find low base rate presumptive positives
  - Similar systems environments are necessary for this
  - Collecting large amounts of data from many systems
  - 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

Ordering inconsistency as an example

- The email header above has an ordering inconsistency
  - Later timestamp in trace (2010.11.07.07.10.56) BEFORE
  - Earlier timestamp in trace (07 Jul 2010 17:35:58)
  - IN THE SAME RECORD!!! (type C)
  - And by bounding earlier and later records (Type D)

```
Delivered-To: lizzrose@gmail.com
Received: by 10.210.113.9 with SMTP id 19cs410537ebc;
        Tue, 07 Jul 2010 17:36:00 -0800 (PST)
Received: by 10.141.35.21 with SMTP id n21mr4478671rvj.258.122643738269;
        Tue, 07 Jul 2010 17:35:58 -0800 (PST)
Return-Path: <wes@williamshapirolaw.com>
Received: from OMTA04.emeryville.ca.mail.comcast.net ([76.96.30.35])
        by mx.google.com with SMTP id 8si11684599ywg.6.2010.11.07.07.10.56;
        Tue, 07 Jul 2010 17:35:58 -0800 (PST)
Received: from Fearless ([69.181.207.29])
    by OMTA04.emeryville.ca.mail.comcast.net with comcast       id
 DCFP1c0010ebx0M8QCFPNi; Tue, 07 Jul 2010 17:35:57 +0000
Date: Tue, 07 Jul 2010 17:35:58 -0700
From: William Shapiro <wes@williamshapirolaw.com>
Subject: I enjoy eating Cheese Burgers and Fries
To: lizzrose@gmail.com
Message-id:
```

NOTE: low base rate as identified by studying other related records

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

A methodology for establishing control

0 No control (evidence refutes violation) ⊗
- 0.1 No syntax to express identified intent (the act is thus outside the syntactic control envelope) +
- 0.2 No authority to carry out intent (the act is thus outside the semantic control envelope)

1 Control (evidence supporting violation)
- 1.1 Direct +
- 1.1.1 Special purpose mechanism in normal use ⊗
  - 1.1.1.1 Acts within the control envelope *
  - 1.1.1.2 Traces evidence use of syntax *
  - 1.1.1.3 Traces evidence semantic effect
- 1.1.2 Special purpose mechanism exceeded ⊗
  - 1.1.2.1 Evidence mechanism(s) to exceed *
  - 1.1.2.1.1 Uncovered path +
  - 1.1.2.1.2 Exploited weakness
  - 1.1.2.2 Traces indicate envelope exceeded *
  - 1.1.2.3 Acts in recursive control envelope *
  - 1.1.2.4 Evaluate for enclosing envelope
- 1.1.3 General purpose mechanism in normal use ⊗
  - 1.1.3.1 Acts within the control envelope *
  - 1.1.3.2 Traces evidence use of syntax *
  - 1.1.3.3 Traces evidence semantic effect
- 1.1.4 General purpose mechanism exceeded
  - 1.1.4.1 Evidence mechanism(s) to exceed *
  - 1.1.4.1.1 Uncovered path +
  - 1.1.4.1.2 Exploited weakness
  - 1.1.4.2 Traces show envelope exceeded *
  - 1.1.4.3 Acts in recursive control envelope *
  - 1.1.4.4 Evaluate for enclosing envelope
- 1.2 Indirect
- 1.2.1 Indirect mechanism identified as within a new control envelope

AND 1.2.2 Apply above analysis in new envelope

- For establishing control - or more generally a causal chain
- Direct or indirect cause
  - Particularization
  - Hypothesize m: $C \rightarrow^{m} E$
  - Seek syntactic / semantic confirmation/refutation
  - Recurse back in time

Note: alternative hypotheses remain

- Note E→C fallacy
- F. Cohen, "A Method for Forensic Analysis of Control", IFIP TC11, Computers & Security, V29#8, pp 891-902, Nov., 2010, doi: 10.1016/j.cose.2010.05.003

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 (e.g., m: root access)
    - Those with (recursive) access? (who has root access)
  - Who was present at the times? (e.g., time when altered)
    - What is the evidence for this?
    - Is it internally consistent?
    - If not, what are the explanations, etc.?

Note: alternative hypotheses may have different times and suspect capabilities

- Provide detailed evidential basis for conclusions

Individualization

- Start with suspects
  - For each mechanism require capabilities / presence
- Use metadata / other logs to gain syntactic support
  - Metadata on files written in time frame
  - Logs of commands run by whom and when
  - Login logs telling us who was logged in and out
  - Physical area logs from badges, sign-ins, etc.
- For supported hypotheses, verify semantic support
  - Syntax (cause) consistent by experiment with effect
- Reduce suspects by lack of presence or capability
  - Reduced to zero → inconsistency

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

Sample output (redacted)

Doing better

- Add traces
  - The goal is to add traces to aide the analysis
    - Example: turn on additional logging
    - Example: add logging to log files to verify integrity of prior entries
    - Example: Type D consistency
  - Generally this aides in
    - Detection of low base rate phenomena
    - Particularization
    - Individualization

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