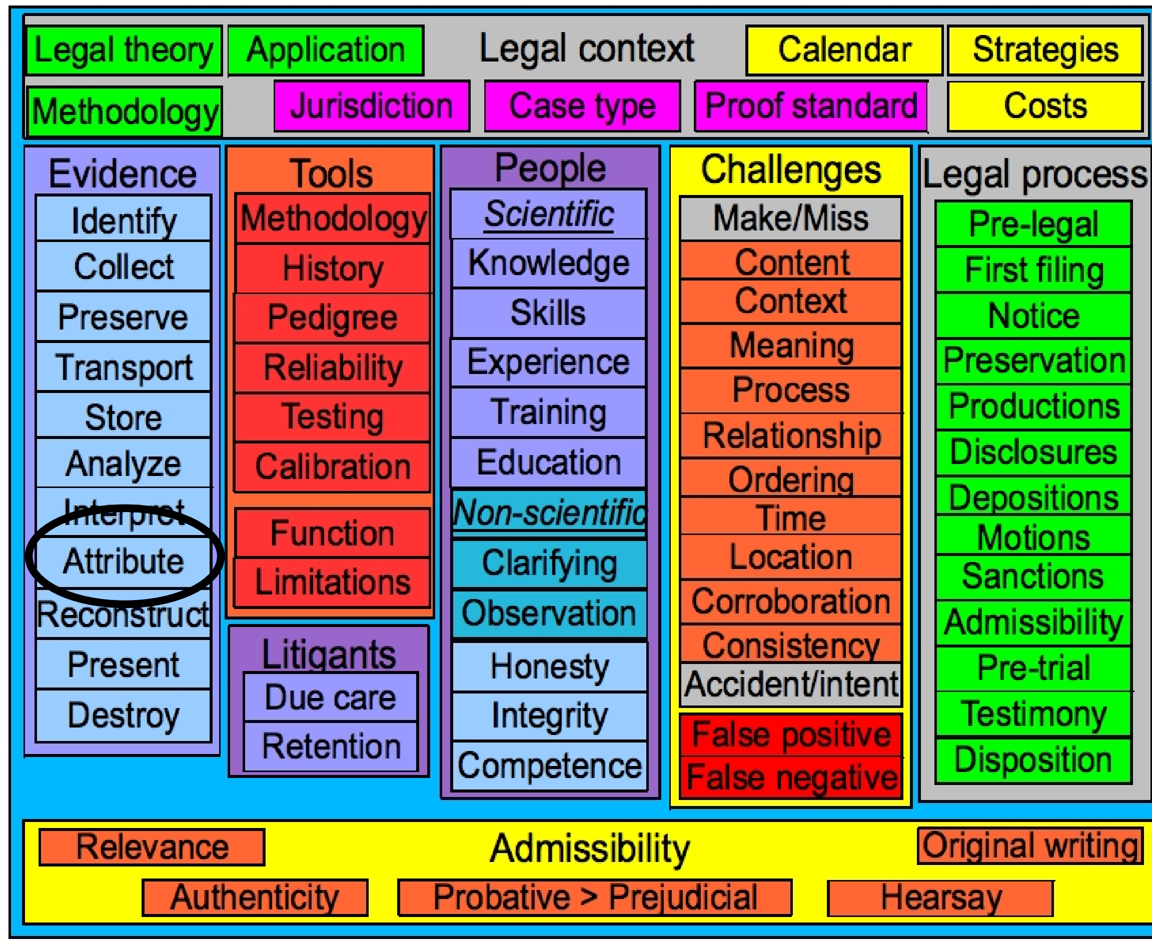
Attribution of Messages to Sources in Digital Forensics

HICSS – Jan 7, 2010

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

Outline

- Background of the speaker and subject
- Attribution
- Limits of current methods
- Attribution with higher certainty
- Your turn!



Your speaker

- Education:
  - B.S. Electrical Engineering (C-MU '77)
  - M.S. Information Science (Pitt '81)
  - Ph.D. Electrical Engineering (USC '86)
- Experience:
  - >30 years of information protection R&D, design, engineering, testing, implementation, and operation
  - >20 years since first digital forensics case
- CEO - Fred Cohen & Associates
  - Enterprise information protection architecture
  - Digital forensics for high-valued legal cases

CalSci

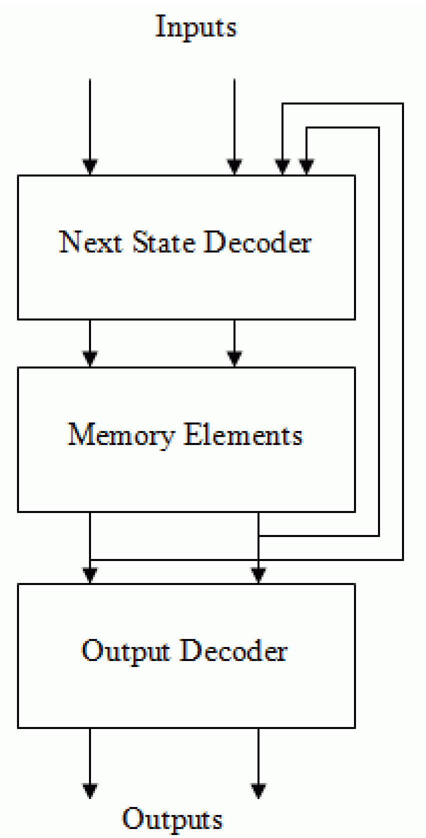
- President – California Sciences Institute
  - Starting doctoral classes in 2010-01?02?
- M.S. And Ph.D. Program in National Security
  - Technical aspects of these fields
- M.S. In Advanced Investigation
- Ph.D. In Digital Forensics
  - The first Ph.D. program in Digital Forensics in the United States
- calsci.org

What does he know about the subject?

- Knowledge, skill, experience, training, education FRE 701-6
- Knowledge, Skills, and Experience:
  - [Countering] attribution of messages to sources
  - Rose v. Albritton, Superior Court of the County of San Francisco, Case No.: FDV-09-806677, July 14, 2009 (testified as an expert)
  - [United States v. Bayly, et. al., United States - District Court for the Southern District of Texas, case no. Cr. No. H-03-363. 2004-10-25 (testified as an expert)]
  - [Beyond Systems, Inc. Plaintiff, v. Kraft Foods, Inc., et al., Defendants. Case No. 8:08-CV-00409, currently in United States District Court for Maryland]
  - [ASIS Internet Services, v. Optin Global, Inc., et. al., - US District Court – Northern district of California Case No. C-05-5124 JCS, 2008-01-07]
  - Susan Polgar v. US Chess Federation et. al. (4 cases including) US District Court – Northern district of Texas C.A. NO. 5-08CV0169-C
- Education:
  - B.S., M.S., and Ph.D. in relevant field

Basics of traces

- Traces
  - FSMs take digital inputs and state and produce digital outputs and state
  - Some of the outputs may be stored and/or captured
  - The stored/captured outputs available to the examiner are called "traces"
- Traces are the result of some process
  - Many possible processes may produce any particular trace
  - What process produced the traces?



Basics of messages

- A message is sent from sender to recipient(s)
  - The message is encoded as a sequence of bits
  - The sending of those bits normally leaves traces
  - Some of those traces may be available to the examiner
- Examples:
  - IRC, IM, AppleTalk, etc. messages
  - Newsgroups, electronic mail
  - FAX messages, voicemail
  - Twitter, SMS, etc.
- Who actually sent them? How do we know?

Basics of “forged” messages

- Almost anyone from almost anywhere can send a bit sequence into the Internet (e.g.,)
  - Simple Mail Transfer Protocol (SMTP) protocol to a Mail Transfer Agent (MTA)
  - helo joe.com
  - mail from:<k@j.l>
  - rcpt to:<o@y.k>
  - data
  - (the sequence of bits for headers/body)
  - .
- Did the person k@j.l send this to o@y.k?

Outline

- Background of the speaker and subject
- Attribution
- Limits of current methods
- Attribution with higher certainty
- Your turn!

Attribution as causality

- To attribute message M to person P, we are, in essence, showing that P caused M
  - Correlation is not causality
  - Causality demands certain things
- Example scientific requirements:
  - Cause comes before effect
    - Don't forget the “speed of light” in the media
    - Digital systems have computational complexity as an added “speed of light” issue
    - Time precision, accuracy, reliability, etc.
  - A causal chain from cause to effect is needed
    - Before does not imply because

Things people have tried

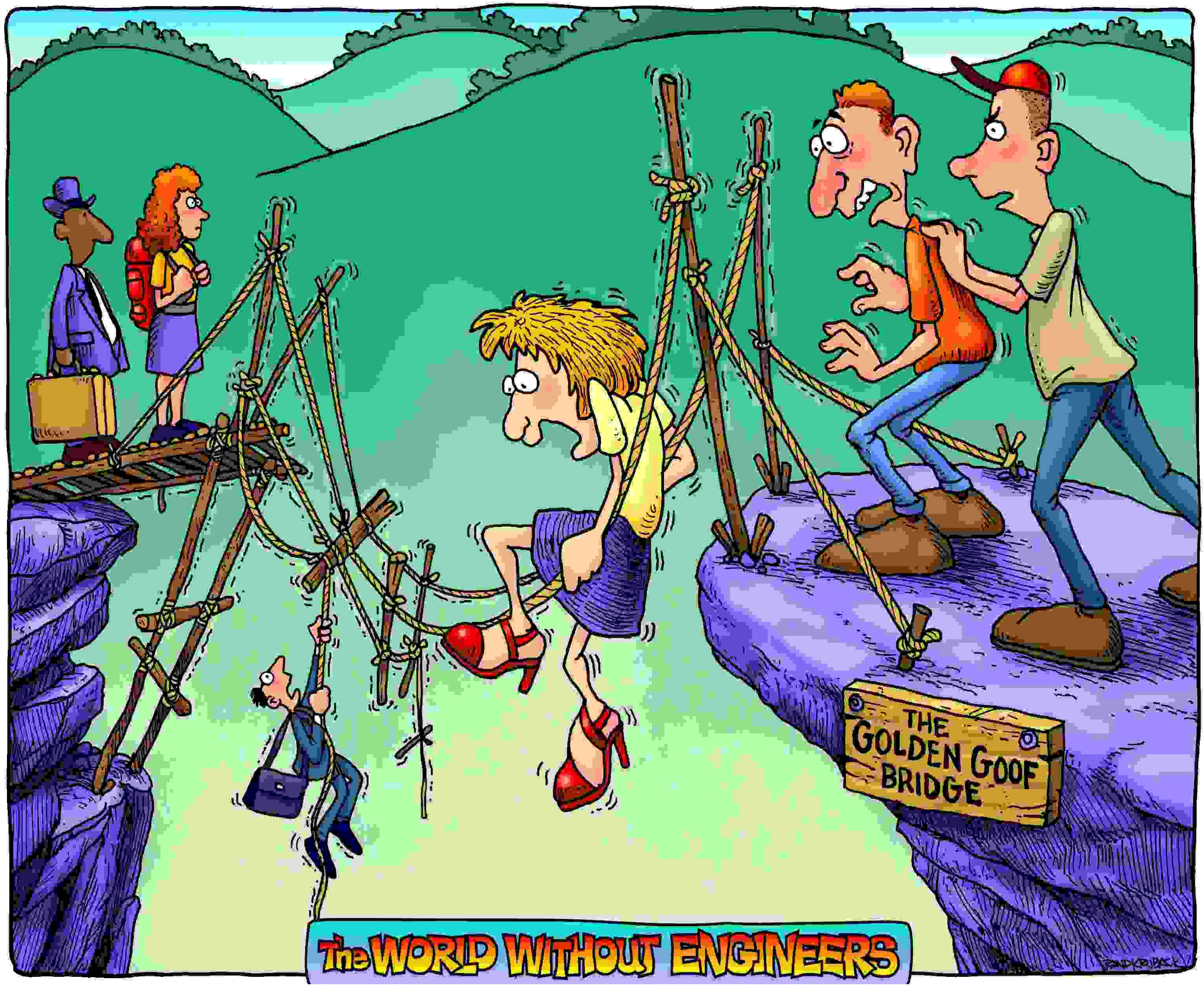
- Level 1, 2, 3, and 4 attribution
  - 1: Direct cause (next computer over)
  - 2: Indirect cause (the computer that originated it)
  - 3: Who did it (the person at that computer)
  - 4: What did it (the organization behind it)
- Authentication technologies
  - Biometrics (2% false positive for 1/1000 actors)
  - Usage patterns (e.g., Web click patterns)
  - Textual analysis (e.g., your phrasology)
- All of these assume no malicious actors/Trojans

Legal issues

- The need for a scientific basis
  - FRE 701-6?
- The standard of proof
  - Preponderance of the evidence (>50%)
  - Beyond a reasonable doubt (>??%)
- Issues of admissibility
  - Of evidence
  - Of expert presenting results
  - Of methods used and results produced

Outline

- Background of the speaker and subject
- Attribution
- Limits of current methods
- Attribution with higher certainty
- Your turn!



Problems with attribution today

- End-to-end authentication approaches
  - Are rarely present or used
  - Depend on trustworthy infrastructure and application
  - Depend on control over keys and key management
  - Are not used by those trying to avoid attribution
- Subverted computers are commonplace
  - Several current worms infest millions of computers
  - Many computers have many different infestations
  - In most forensics cases, all possible subversions cannot be sought or detected

More attribution problems

- Network traffic mechanisms conceal sourcing
  - Proxy servers, gateway computers, NAT gateways, firewalls, large-volume aggregated service providers, virtualization, load balancers, etc.
  - Mobility and highly available distributed access, wireless, coffee shops, Internet cafes, building area networks, etc.
  - Identity information is widely varied across and between these networks and systems, and rarely based on a trusted mechanism or association to an actual person.

More attribution problems

- Simple forgeries are easy (see above)
- Means, motive, and opportunity exist
  - Means available to anyone able to contact content or systems involved (anyone in the Internet)
  - Motive is case-dependent - classic human motives
  - Motivated actors vary widely, and include w/o limit:
    - Parties to the action and their friends or enemies
    - Innocent third parties through errors or omissions
    - Competitors wishing to shift blame
  - Opportunity ∃ for {originator, intermediary, recipient}

Common claims and problems

- Claim: Message portions are self-authenticating
  - Anyone can put any sequence into any message
- Claim: Form and style indicate “authorship”
  - If I quote Mark Twain, did he originate the message?
  - If it sounds like Twain, is it necessarily Twain?
  - Does the use of “youns” mean I am from Pittsburgh?
- Claim: Presence of common sequences
  - Little current scientific basis for optimal parsing or identification of relevant sequences
  - Even if common authorship, that does not imply common message origination (I forward your tweet)

Common claims and problems

- Claim: Similar group of message (content)
  - For a corpus of 4053 messages, 7531 similarity groupings were found...
  - What are the metrics of similarity and what do they mean?
- Claim: Similar timing or physical properties
  - Often useful fur ruling out attribution (can't produce that result in this much time)
  - Cumulative effect of ruing out possibilities may meet the standard of proof

Outline

- Background of the speaker and subject
- Attribution
- Limits of current methods
- Attribution with higher certainty
- Your turn!

Two classes of approaches

- Consistency and inconsistency
  - Use the redundant nature of traces, events, and claims to determine consistency
  - The number of possible traces, consistencies, inconsistencies, and techniques is too large to practically exhaust
- Legal process to gain additional records
  - Subpoena additional evidence
  - Examine for consistency

Unavailable records

- The "chain" from here to there
  - Missing links may be unavoidable
    - Uncooperative parties
    - Destroyed records or records never produced
  - Legal process may reveal other related traces
    - Repeat till causal chain completed
  - Incomplete causal chain may remain
    - Does it meet the standard of proof?
    - Can you show the first M and last N steps?
    - What subset of steps can be shown?

Automated analysis

- Volumes dictate automation
  - 100,000 messages is no longer rare in cases
  - Millions of messages are still rare today
  - Many techniques defy manual application
- Tools must meet legal criteria
  - Scientific methodology as evidenced by peer reviewed articles in the scientific literature
  - Proper application of methodology by tools and those who use those tools
  - Testing, calibration, and error rates evidenced

Tools for facilitating analysis

- Extract message-like sequences from traces
  - Traces often in the form of collections (mbox)
  - Messages may have semi-structured “headers”
  - Messages generally have content (bodies)
  - It is often helpful to generate derived traces
    - Traces derived from original traces
    - Reformatted / normalized to some standard
    - Linked back to the original traces
- Associated structured content
  - Headers have {“key”,”value”} pairs ({From:, ...})
  - Message headers formed by identified process

More tools for messages

- Reception analysis
  - Time sequences of events revealed (use UTC)
  - Often traces from multiple locations
- Histogram analysis
  - Sorting by “hop” into “time slots” reveals flow(t)
  - Activity (distance) can reveal processes
  - Anomalies may become apparent in flows
- MD5 and similar “fingerprint” analysis
  - Allows duplicates to be found
  - Can be applied to portions or entire messages
  - May reveal extremely similar sequences

Still more tools for messages

- Correlation
  - List all cases of A in B AND C in D (e.g.,
    - From “joe” AND Date “Tue”
    - From IP address AND Message-ID: KKK[0-9]+
- Match-correlation (n^2 time and space)
  - Identifies how many lines are shared between each pair of messages / headers / bodies
  - Finds near-duplicates and similar “related” messages with closer matches indicating more similarity
  - Finds exact copies and “imperfect duplicates” in which duplicates are slightly altered

Still more tools for messages

- Reception tree analysis (n log(n) time)
  - Shows the tree structure of how messages arrived at their final destination
  - Reveals internals of infrastructures used
  - Reveals common delivery paths and quantities
- N-tuples (n^2 time and space)
  - General purpose grouping of messages into sets with commonalities
  - Greatest-common-factor (GCF) analysis based on defined sets of factors
  - Creates different groupings of messages based on sets of factors

What tools reveal

- Basic goal is to identify [in]consistencies
  - Type C (trace to trace)
    - Different content, identical “unique” identifiers
    - Identical headers, different bodies
    - Multiple messages, identical “unique” identifiers
    - Unrealistic or inconsistent travel rates
    - Over- or under-consistent delay times
    - Ordering errors and header sequence errors
    - Common content with different sourcing / delivery
    - Integrity flaws like mismatched digital signatures
    - Travel patterns inconsistent with normal process
  - Type D (trace to event)

What tools reveal

- Basic goal is to identify [in]consistencies
  - Type C (trace to trace)
  - Type D (trace to event)
    - Time zones inconsistent with asserted locations
    - Damages claims inconsistent with timings and volumes
    - Commonality claims inconsistent with traces
    - Consistency with non-claimed event sequences / inconsistencies with claimed event sequences
- Without the tools, these sorts of inconsistency are hard to find in high volume cases
- With them, inconsistencies may not be found

Recent case examples

- Tools now used for "standard processing"
- In the last year they have revealed:
  - Fabrications of collections (e.g., mailbox files not created by "normal business practice")
  - Fabrication errors (e.g., duplicates with slightly varied headers, identical headers different bodies, multiple "unique" Message-ID entries)
  - Similarity groupings (e.g., identifying a complex header sequence in 64 out of 200,000+ messages, 63 previously attributed to an unattributed suspect, and the 64th which links to known accounts and behaviors of a known suspect)

Conclusions

- At the end of the day, the surety has to meet the legal requirements based on the case at hand
- Existing methods individually are of only limited power for establishing causality
- Consistency analysis combined with causal chains and automation makes far more complex attributions with far higher surety feasible
- However:
  - All information examined to date is consistent with X and inconsistent with other identified Y
- Is not “proof positive”

Outline

- Background of the speaker and subject
- Attribution
- Limits of current methods
- Attribution with higher certainty
- Your turn!

Thank You

http://calsci.org/ - calsci at calsci.org

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