Digital diplomatics, consistency analysis, and digital forensics

2014-09-25
Beijing, China

Dr. Fred Cohen

Abstract

- Diplomatics is the name of a scientific field started in the 1600s by the famous French scientist Mabilon. It because foundational to the development of the rules of evidence for Western law, and is the basis of the modern field of questioned document examination
- At the heart of diplomatics was the concept that a legitimate record would be consistent with the methods, processes, and people who created it and the material used in those processes.
- The traces of the documentary form in the context of the archival fonds and historical knowledge could be used to detect inconsistencies between the record and the manner in which it was supposed to come to be in order to challenge and confirm or refute claims of authenticity.
- This talk is about using the concepts of diplomatics and the modern methods of consistency analysis to form the modern science of digital diplomatics
- It uses examples to demonstrate the utility and the limits of digital diplomatics today and suggests a line of study leading to a new way to undertake digital forensic examination.

Outline

- Background, history, and where we are all heading
  - Diplomatics (circa 1681 and forward)
  - The digital era – what we forgot to do
  - Logging, metadata, intrusion detection, and anomaly detection
  - Surveillance societies in the digital era
- Digital diplomatics – the concept
  - Redundant records and inconsistency detection
  - Triggering and supporting digital investigations
  - Addressing the physics of digital information
  - An alternative future to the surveillance society
- Questions / comments / discussion

Diplomatics (circa 1600 and forward)

- Francois Damelle – 1609 - systematic document examination
- Mabillon (1681)
  - Published analysis of ~200 documents
    - Divided into categories, examined with regard to material, ink, language, script, punctuation, abbreviations, formulas, subscripts, seals, special signs, chancery notes,etc.
    - Created descriptions to allow the detection of forgeries and identified ground truth based on recurrence of intrinsic and extrinsic elements in documents from same time and place
  - Used redundancy to test for consistency
    - Based on correlation, however...
    - Causality in the form of known chanceries or scriptoria traditions (cause) and capabilities of scribes over the ages (mechanism).
    - No ground truth available: documents too old for eye witnesses and supporting documentary evidence was also in question

Core concepts from diplomatics

- Later works: correlation is not causality
  - Similar effects do not imply similar causes or mechanisms
  - More generally, effect does not imply cause
  - Cause acts through Mechanisms to produce Effects ($C \rightarrow^{m} E$)
  - Authenticity of records is related to the procedure of creation
- Questioned documents (records) get questioned on a basis
  - Example, ownership of land based on historical documents
  - Hopefully a scientific basis of Consistency / Inconsistency between claimed $C \rightarrow^{m} E$ and observed phenomena
- Core concepts of classical diplomatics
  - Inconsistency based on physicality
  - Inconsistency based on form

Core concepts from diplomatics

- Inconsistency based on physicality
  - Nature of the media fixing the form, imprint method, transfer
    - A new piece of paper formed out of recycled paper products from trees grown for the purpose is different than and differentiable from a piece of paper formed in the 1700s.
    - Heavier weight presses push inks deeper into the fibers of paper, while laser printers use a different deposition process than inkjets.
    - “Hand”, ink type and makeup, Carbon 14 levels, materials, instruments, tool marks, oils from hands, fibers from clothes,
  - If the “Hand” doesn't fit, you must acquit (OJ Simpson humor)
- Inconsistency based on form

Core concepts from diplomatics

- Inconsistency based on physicality
- Inconsistency based on form
  - Form of documents or records, regardless of the content
    - Structure of the documentary form, rules of record making, elements present / missing, etc.
  - Known formats, fields, syntax, locations of entry areas on forms.
  - Spelling, language, usage, methods of form use, font, etc.
  - Redundancy within the record, in the fonds, and across fonds.
- What about content?
  - Diplomatics largely ignores content per-se
    - e.g., A wills this piece of furniture to B
    - In essence, there is no way to address this in diplomatics

Questioned document analysis in China

- 250 B.C. - Authentication in archives and records management
  - Chinese officials used fingerprints to seal official documents
  - Presumably there was a process to verify these at the time
  - Some claim this is as old as 9,000 years...
- Chinese forensic medicine led the World in the 1200s
  - His Duan Yu 洗冤集錄 (The Washing Away of Wrongs) on how to distinguish drowning from strangulation as detailed by Song Ci (宋慈 , 1186–1249) in 1248.
- Chinese Seals – 1390 A.D.
  - Seals to mark documents – no consistency checking found
- I found no early Chinese questioned document analysis
  - Do you of any earlier consistency checking?

How things work in the paper world

- We may think of the bureaucracy as a waste – but...
  - I want to buy something of great and lasting value (e.g., land)
  - You want to sell the land to me in exchange for lots of money
  - How do we both make certain we are getting value for value?
- The government provides a way to do this
  - You establish ownership via public records and prove it to me
    - You have the right to sell the land (registered deed)
    - The land is what you assert it to be (deed details property)
    - It has (or not) restrictions (right of ways, use limitations, etc.)
  - I establish finances via demonstrable money and provenance
    - I have the money to buy it from you (bank balance + loan)
    - The money is from a legitimate source (not stolen – how I got it)
    - The money is not encumbered (liens, holds, etc.)

Paper world continued...

- Moment of sale
  - I bring the documents for the money (certified funds)
  - You bring the documents for the deed (certified deed)
  - We exchange (you deposit the funds, I register the deed)
- Each of these steps may involve different diplomatics
  - Each piece of paperwork has specific physicality and form
    - Deed and certified funds on specific paper type with certain type of ink and with seals intact, with various required signatures / stamps / seals, with sequence numbers and dates, in a format defined by the relevant governing bodies, etc.
  - Each piece of paperwork involves multiple independent parties
    - Both parties to the transactions sign, as does a notary public authorized by government to attest to signatures, and there is an extensive paper trail of independent acts by parties in fonds

Challenges to paper records

- When a paper record is challenged, diplomatics comes to bear
  - Certified copies or originals of records and metadata may be requested from relevant bodies
    - Notary public(s), Public records and/or archives, Financial institutions, Title and escrow companies, Individual parties
    - Each is attested to by the independent parties to the act
  - Each document is examined for physical and documentary form
    - Identified forgeries imply punishment to the attesting party
  - All of these records should match up in a valid transaction
    - If some mismatch, the courts uses experts to identify what is most likely the truth and makes a ruling based on the evidence
- The fundamental point:
  - Independent redundant records are cross checked in context of the fonds to demonstrate trustworthy reliable records

The digital area – what we forgot to do

- Come the computer (the industrial age of the brain)
  - Better, faster, cheaper at every repetitive process than people
  - The reputation: so good it never makes a mistake
  - The reality: Mistakes are made... errors, omissions, malice
    - Computer (hardware) errors – nothing is really perfect
    - Human (software) errors – nobody is really perfect
    - Omissions – and lots of them and lots more to come
    - Malice – subversion of the systems be intentional actors
- What did we do wrong?
  - We forgot about the redundancy that made diplomatics work
  - We didn't intentionally create it (but we accidentally left some)
  - We actively worked to eliminate it
    - So we got the brittle systems we largely see today

Challenges in the digital era

- Independent redundant records are not systematically created
  - None of the classic physical properties are available
  - Form and format are generated as needed from underlying data
  - Multiple independent parties don't usually hold parts of the trail
    - → No obvious way to demonstrate trustworthy reliable records
    - Perhaps the fonds can save us?
- Fonds are not operated with well defined and tracked methods
  - Records are bit sequences stored on malleable (r/w) media
  - Moved around those media and from media to media over time
  - Operated with ever-changing software, hardware, methods
  - With no permanent defined archival form or metadata
- We cannot really demonstrate trustworthy reliable records

Logging, metadata, IDS, and ADS

- Come the errors → Come the investigations → Come the tools
  - Logging – so we have a record of what happened (debugging)
    - → Use the logs in investigations to try to figure it out
      - → Log analysis tools to reduce human workload and do it better
  - Metadata (not) – file dates, times, UID, etc. (support file system)
    - → Use file times to investigate and try to figure it out
      - → Metadata (computer/network) tools for efficiency
  - Intrusion detection – because they keep breaking in
    - → Use and create more log data and look for known bad things
      - → IDS systems to automate the process and get to real-time
  - Anomaly detection – because weird things happen
    - → Characterize (statistically) normal and look for deviations
      - → ADS systems to automate the process and get to real-time
- It's all by accident of history and the way we created systems

Surveillance societies in the digital era

- Since we cannot be sure, the best we can do is:
  - Watch and record more things more of the time
  - When bad things are detected look at the records
  - Try to figure out what happened from those records
- But at what cost?
  - Privacy is nearly dead because of the intensity of surveillance
  - Surveillance has a long history of abuse
    - Political (chilling effect), Personal (spouse/friends/enemies/etc.) Financial (advertising, competitors, etc.), Criminal (better crime)
  - Surveillance saps time, money, effort that could be productive
    - Advancing humanity, science, art, education, roads, forests, etc.
- And we still keep losing the race
  - More cases, more harm, more often, to more parties over time

Outline

- Background, history, and where we are all heading
  - Diplomatics (circa 1681 and forward)
  - The digital era – what we forgot to do
  - Logging, metadata, intrusion detection, and anomaly detection
  - Surveillance societies in the digital era
- Digital diplomatics – the concept
  - Redundant records and inconsistency detection
  - Triggering and supporting digital investigations
  - Addressing the physics of digital information
  - An alternative future to the surveillance society
- Questions / comments / discussion

Redundant records and consistency checking

- Digital records contain inherent redundancy
  - The sequencing of data on a disk vs. the metadata of the files
  - The audit records produced vs. the programs run
  - The network records of DNS lookups vs. the Web access logs
  - Lots and lots of other examples...
  - Note: we can add systematic redundancy if desired...
- Subversion of records maintaining consistency is (very) hard
  - Mathematical complexity of fully consistent alteration is high
  - Redundancy crosses many systems in many cases
  - You have to break into many places to fully cover your tracks
  - BUT... checking for consistency may also be hard...
- Inconsistency → **impossibility** for the physics of the situation

Recent advances in consistency checking

- 2014 – Computers and Security –
  - "Time and Space Interval Record Schedule Consistency Analysis for Atomic Items without Interactions in Open Spaces with Stationary Locations"
  - Time and space interval (finite time/space granularity)
  - Record schedule consistency (records of places at times)
  - Atomic items (things can be at one region of space at one time)
  - Without interactions (ignores additional interaction constraints)
  - Open Spaces (no movement or path restriction) [generalized]
  - Stationary locations (records produced at fixed places)
- Can be checked in O(n*Log(n)) time and n space (practical)
  - Many common "detective mysteries" solutions can be done automatically with this method

Example of an inconsistency

- My credit card used near SFO Gate 12 at 1300 on Sep 20, 2014
  - Record indicates I was physically present at SFO at that time
- My credit card was used to check into Intercontinental at 1200 on Sep 21, 2014 in Beijing, China (note time zone/date change)
  - Record indicates I was physically present in China at that time
- My credit card was used to purchase a coffee at Starbucks in San Jose, CA at 1500 on Sep 20, 2014
  - Record indicates I was physically present in San Jose at 1500
- They cannot all be true
  - Because there is no schedule that allows all 3 to happen
    - No path to get me from SFO to SJ to Beijing in time
  - They are not always that simple, but you get the idea...

Triggering and supporting investigations

- Inconsistency does not finish the task – it starts it
  - Inconsistency can prove a set of things to be (jointly) untrue
    - Refutation of a hypothesis only
  - Failure to refute does not imply truth
    - But try to tell a lie and see how hard it is to do really well...
- Detection triggers investigation
  - The key to inconsistency is that it produces NO false positives
    - If you find inconsistency → you better investigate
- Compare this to IDS/ADS
  - IDS/ADS: Adjust false positive and negative rates to available investigative resources
  - Inconsistency: Rarely triggered but always worth investigating
    - Because the records **can not** be right

But which ones are wrong?

- Inconsistency doesn't answer the question – it identifies it
  - Was I in SFO and went to San Jose?
  - Was I in SFO and went to Beijing?
  - Was I in San Jose and the rest are false?
  - Was I in San Jose and Beijing and flights were early?
  - Did I not use commercial air (military supersonic jets)?
  - Are the records wrong as to time in San Jose?
  - Did someone forge my credit card in San Jose? SFO? Beijing?
- Investigation is required to reconcile records with reality
  - No current model of how to systematically eliminate possibilities
  - Some notions, but no scientific basis available (yet)
  - But we think this can be addressed by/in real cases

The physics of digital information

- Inconsistency analysis is really based on an underlying physics
  - Cause works via mechanisms to produce effects
    - C $\rightarrow^{m}$ E – Causality is the foundation of all science
  - A scientific theory must be testable by experiment
    - The experiment can show the theory to be wrong
  - When a theory is refuted, we adapt the theory
- Inconsistency is demonstrated by refuting a hypothesis
  - A person cannot be in two places at once
    - It takes time to get from place to place
      - Not enough time → Not possible → The records cannot be true
  - Hypothesis: The records are all true
    - Refutation means the hypothesis is wrong →
      - The records are not all true

Not the solution to all problems

- Inconsistency in records is indicative of
  - Subversion of the record-keeping system
    - The record-keeping system is not reliable
  - OR Errors in the mechanisms
    - The record-keeping system is not reliable
- Legally, it may not matter which...
  - Unreliable records cannot be admitted in most legal cases
    - China requires 95% certainty
      - But how do you prove it?
    - US requires more probative than prejudicial
      - But once inconsistency is found, you cannot determine why
        - Without an investigative process producing $C \rightarrow^{m} E$
  - And now we have another theory to test
    - Which cannot be proved correct – only refuted...

An alternative to the surveillance society

- Today, much of the world is building surveillance – why?
  - We cannot be certain of what the records we have tell us
  - So we keep making more of them hoping to make it better
- But what if, instead, we built better record-keeping systems
  - Diplomatics resolved this issue legally for ~350+ years
  - Then computers “unsolved” it
  - Back to the future
- Start with the theory that works
  - Independent parties attesting to facts in a legally binding way
  - Records in sequence in controlled repositories with rules
  - Metadata to demonstrate accuracy and reliability of records
- Implement it in computers for efficiency – but keep key properties

Making it work

- Step 1: Establish the systematic approaches for acts
  - Credit card data used to buy things at a store
  - Inventory reduction associated with the item
  - Records at the checkout reflecting the purchase
  - Presence of a signature / PIN code at a device
  - Shipping records (for shipped purchases) ...
- Step 2: Establish the properties of the record-keeping systems
  - Records entered sequentially in each database with record ID
  - Record formats contain specific fields in formats
  - Metadata for each record includes (see the COP table)
  - Time and date stamps ordered within (threshold)
  - Network traffic and locations involved and their metadata
  - Quantities feasible per unit time

Making it work part 2

- Step 3: Reconcile records at a theoretical level
  - No inventory indicator → Database should not yield record
  - No checkout record → Database should not yield record
  - No checkout record → No inventory reduction
  - Inventory reduction → Should be no checkout record for it
  - Transaction volume exceeds inventory flow rate
  - (better yet a theoretical model of the system)…
- Step 4: Detect inconsistencies between theory and practice
  - An act not consistent with the theory of operation
    - → Should be investigated
    - → Act should be stopped in a timely fashion (if high valued)
    - → Source of inconsistency should be sought and eliminated

Outline

- Background, history, and where we are all heading
  - Diplomatics (circa 1681 and forward)
  - The digital era – what we forgot to do
  - Logging, metadata, intrusion detection, and anomaly detection
  - Surveillance societies in the digital era
- Digital diplomatics – the concept
  - Redundant records and inconsistency detection
  - Triggering and supporting digital investigations
  - Addressing the physics of digital information
  - An alternative future to the surveillance society
- Questions / comments / discussion

Forensic investigations

- In any digital forensics examination
  - Record consistency checks should be done
    - Inconsistencies → unreliable records
    - No inconsistencies ⇏ reliable records
    - Consistency checks can only refute, not prove reliability
  - But how many checks are enough?
    - Enough to exceed the required reliability threshold
      - In China, to the point of 95%+ certainty of reliability
    - How do you establish this?
      - Perhaps in my talk next year I will be able to answer it
- In a system seeking to support forensics
  - Metadata should be created for forensics
  - Systems should be designed to support diplomatic analysis

Thank You

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