THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 6 | Number 1 Article 3

2011

A Case Study in Forensic Analysis of Control

Fred Cohen
California Sciences Institute, Fred Cohen & Associates

A Case Study in Forensic Analysis of Control

Fred Cohen
CEO - Fred Cohen & Associates
President - California Sciences Institute

ABSTRACT

This paper describes a case study in which a method for forensic analysis of control was applied to resolve probative technical issues in a legal action. It describes one instance in which the analysis was successfully applied without challenge, addresses the details of most of the different facets of the analysis method, and demonstrates how such analysis provides a systematic approach to using technical methods to address legal issues as a case study.

Keywords: Turing capability, control, digital forensics, case study

INTRODUCTION AND BACKGROUND

Laws such as [1] and [2] are used to assert that a criminal or civil violation has potentially taken place when a suspect acts so as to "knowingly and without permission" "access" a computer system and "intentionally cause damage", or similar language. Technical questions for the digital forensic evidence (DFE) examiner include, without limit, whether or not such a claim is (1) possible in a particular situation, (2) (in)consistent with the available traces, and (3) attributable to the suspect or others. A detailed method for analysis in these situations was provided in [3] and is applied in this case study.

The matter at hand

In the case at hand, Plaintiff accused Defendant of taking control of Plaintiff's computer as part of efforts undertaken to send unsolicited commercial email to Plaintiff's systems. The claims asserted, in essence, that Defendant, in sending unwanted electronic mail messages, violated statutes by sending undesired electronic mail messages. In doing so, the claim asserted that:

> Defendant knowingly sent or caused to be sent electronic mail messages, without Plaintiff's permission.
>
> In doing so, Defendant caused a program under Defendant's direct or indirect control to access or cause access to Plaintiff's computer(s).
>
> In doing so, Defendant caused Plaintiff damage when disk space, computer time, and other resources were consumed as a side effect of the software that handled these messages.

Thus, under various laws unrelated to the laws regarding unsolicited commercial

email, Defendant was suing Plaintiff.

Background on the analysis method

As described in [3], and using terminology therefrom, the examiner evaluating such a claim, must consider whether and to what extent the claims are (1) possible given the circumstances asserted, (2) (in)consistent with the traces, and (3) attributable to Defendant.

The notion of "control" is introduced, [3] in part, to help deal with issues of mens rae. The notion is based on the concept that to be in violation of such a statute, a party must have at least two things; (1) the ability to act so as to express intent, and (2) the ability to have that expressed intent carried out. Without these two elements, asserting that a party knowingly and intentionally caused something to take place is problematic. The overarching analysis methodology of [3] is outlined here, and is the only methodology we are aware of for forensic analysis of control today (numbering added):

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

Throughout the remainder of this paper, we will refer to these elements of the analytical framework by placing them in curly brackets (e.g., {1.1.3.1} indicates "Acts within the control envelope" for a "general purpose mechanism in normal use"). "~" is used for "not shown" (e.g., {~1.1}) and ! for refutation (e.g., {!1.1.4.1.1} → shown false).

Attribution to source is also required to demonstrate a violation by any particular party, if and only if control has been established, and is beyond the scope of [3] or this paper.

Additional background literature

Analysis of control for forensic purposes is problematic for several reasons. Perhaps the most problematic overall issue is that demonstrating causality in a definitive way from traces would require require demonstrating that the envelope of prior state and input sequences to the relevant finite state automata that could produce the available traces are such that the only consistent explanation is the identified causal chain. This is usually infeasible without complete traces or equivalent partial traces because digital space converges with time.[16] Complete traces are essentially never available in modern systems.[16] Various reconstruction approaches have been used to demonstrate feasibility of a causal chain [7][12][14] leading to particular traces and use of reduced state representations have been used to try to us incomplete traces to restrict prior state and input envelopes [13], none of these are currently computationally feasible for real world situations such as the ones at issue in this matter.

The approach that may be taken to establish some level of viability for a legal theory asserting taking control is to produce traces adequate to demonstrate a feasible taking of control through reconstruction.[3] In this approach, existing traces are driven forward in time through a reconstruction that has adequate fidelity regarding the relevant factors to show that the traces are consistent with the legal theory. [7][12][13][14] Of course these reconstruction approaches are subject to challenges that demonstrate trace and/or event inconsistencies between the reconstruction and the totality of evidence in the case, as well as challenges based on all of the assumptions of the reconstruction and alternative reconstructions.[3]

An alternative to full reconstruction is a logical analysis that is adequate to demonstrate what has to be demonstrated. For example, we would hope that most experts would agree that, subject to some reasonable additional constraints, (A1) the root user in a Unix environment can place any desired bit sequence in any user

file. While such consensus may not be present in many situations, [16] analytical approaches largely depend on it and it will be assumed here.

At the end of the day, since no claim of taking control is likely to be fully demonstrable from available evidence, and certainly is not in most modern real-world systems, the issue must be settled in terms of partial traces that create evidence supporting each side of the issue.[3] For example, even if a complete causal chain from a source to a target is not available, there may be partial traces demonstrating the presence of activities at a source (e.g., a recording of keystrokes at a user workstation) and effects of such activities at a destination (e.g., logs of activities that would normally result from those same keystrokes being applied at the target at the same time frame and in the same sequence) that may be adequate to establish control to some level of certainty or quality.

Based on the identified consensus assumption (A1), we might reasonably conclude that for the identified root user, {1.1.3} applies to any activity that root user would perform on their own system. {1.1.3.1} A stronger demonstration of a particular act (e.g., deleting a file) would be the presence of traces indicative of a particular command to perform that act (e.g., "rm /etc/passwd" in the log of console commands),{1.1.3.2} and traces of the results of that command that are consistent with that act. (e.g., no such file present) {1.1.3.3} We might then reasonably come to a logical conclusion that {1.1.3.1}*{1.1.3.2}*{1.1.3.1}→{1.1.3}→{1.1}→{1} and that the actor logged in as the root user appears to have had control and performed the act.

In such cases the weight of the accumulated evidence associated with traces and events, assuming relevance, reliability, and other similar things could be shown, would presumably be adequate to be presented to the trier of fact. Similar evidence by the opposing side would have a similar threshold of admissibility and the trier of fact would be left to decide the issues. For example, if traces normally present are missing, this would make the reliability of the claims more dubious, particularly if the reconstruction produced them and the traces from the other party did not.

Suppose, for example, that the accused individual claims that they were elsewhere at the time and that facility logs kept by an independent special purpose system indicate that the individual was elsewhere at the time and no such records indicate that they were present at the location of the console of the computer at issue at the time. The individual might reasonably claim that the facility logs showed they were elsewhere, and since that they don't have the ability to produce false logs from the normal user interface ({~1.1.1.1} → {~1.1.1}), and no evidence was present that those logs were acting improperly ({~1.1.2.1}*{~1.1.2.2}→{~1.1.2}), and since this is a special purpose system ({~1.1.3} * {~1.1.4}), it is reasonable to conclude that the accused had no direct control over the facility logs ({~1.1.1} * {~1.1.2} * {~1.1.3} * {~1.1.4} → {~1.1}).

Presumably, this would be admitted to demonstrate the innocence of the accused. But the accuser might then assert that there are other ways to get around such mechanisms, including trading badges with someone else. {1.2} In this new scenario, a new control envelope is present {1.2.1} and the above analysis can then be repeated within this new control envelope. In the new claimed control envelope, the facility log operates normally but the mechanism's intended use is asserted to be exceeded {1.1.2} by an exploited weakness {1.1.2.2} by the accused and their alleged partner. Traces are present of the excess {1.1.2.2} in the presence of the alleged partner in the location with the console the acts are within the recursive control envelope for the partner and the accused ({1.1.1.1} * {1.1.1.2} * {1.1.1.3} → {1.1.1} for both working together → {1.1.2.3} * {1.1.2.4}), and thus {1.1.1} → {1.1}(indirect) → {1.2} → {1}, and the violation is supportable by available traces. However, the "evidence" part of {1.1.2.1} is weak without some corroboration of the partnership or the acts.

CASE DETAILS

Specific claims and basis

In the matter at hand, [8] specific claims were made with regard to Defendant's sending or causing to be sent, electronic mail messages. In particular, and without limit, those claims included (in pertinent parts and in summary):

> **1. Violations of California Business and Professions Code 17529.5 -** The claimed basis being the allegation that (a) Plaintiff suffered actual damages by receiving the alleged emails, ... (d) Plaintiff's servers were forced by Defendants' intentional acts to spend at least 20 times more time processing Defendants' alleged emails used storage space, used bandwidth, and used more workstation storage and processing time than they otherwise would have had to spend, (e) Plaintiff's workstation suffered degraded performance by Defendants' acts, (f) Plaintiff had to spend time before loading alleged emails into his workstation to read and process the alleged messages, ... (h) Defendants forced Plaintiff to spend time sending and receiving responses to emails in order to try to stop further emails, and (i) Plaintiff suffered damages as a result of these alleged acts.
>
> **2. [Redacted - irrelevant to these issues]**
>
> **3. Trespass to Chattels -** The claimed basis being that (a) Defendant took control over Plaintiff's servers and workstations without authorization, (b) instructions sent by Defendants caused Plaintiff to be unable to access, read, or send desired email messages, (c) Defendants forced Plaintiff's server to use resources, memory, and disk space and that during that time computers were unable to perform tasks that Plaintiff desired them to perform, (d) Defendants forced Plaintiff to perform more computer system maintenance and monitoring to reduce the risk of data loss, and (e) Plaintiff suffered damages as a result of Defendants' actions.

> **4. California Penal Code 502 -** The claimed basis being that (a) Defendants were not authorized to access Plaintiff's computer systems by sending messages to Plaintiff's email server, (b) Defendants were not authorized to use Plaintiff's servers to relay alleged messages when sending the alleged emails, (c) Defendants knowingly and without permission used or caused to be used computer services of Plaintiff's computers by allegedly sending alleged messages, (d) Defendants knowingly and without permission accessed and without permission added data to Plaintiff's computer systems by allegedly sending the alleged email messages, (e) Defendants knowingly and without permission accessed and without permission accessed and caused to be accessed Plaintiff's computer, computer system, and computer networks by allegedly sending the alleged email messages, ...

In simple terms, Plaintiff claims that Defendant took unauthorized control over Plaintiff's computers using a distributed coordinated attack [11] (a.k.a., a botnet) and, in doing so, trespassed and caused harm.

In this paper, the issues of attribution of Plaintiff-identified messages to Defendant are irrelevant and further details in this area will be eschewed. The issues associated with trespass to chattels has been examined in legal detail [10] and in technical detail [7] elsewhere. The remaining issues then ultimately come down to "knowing", permission or the lack thereof, access, and access causing identified damages.

Details of issues

Issues of permission

In the matter at hand, authorization for normal external use of simple mail transfer protocol (SMTP)[4][6] and domain name server (DNS)[5] services was granted de-facto by the open and unlimited access granted by Plaintiff to anyone from anywhere to (1) retrieve DNS records and (2) send electronic mail messages using the SMTP protocol. No other relevant authorization was involved in this matter. The traces proffered by Plaintiff indicate that the HELO protocol was in use in many or most messages. The HELO protocol and details of its proper reception and application are defined in RFC821.[4] In some cases the EHLO protocol was used as defined in RFC2821.[6]

Plaintiff claimed that such authorization was for the exclusive purpose of sending messages that Plaintiff desired to get, but in practice, there was no way for an external party to differentiate such a thing, and no explicit authorization was made for such use. Rather, the service was made available to all. This is a legal issue, not a technical one, and it was not sustained for Plaintiff by the court. Subsequent legal rulings have indicated that technically authorized behavior are authorized in the more general sense, and this would tend to support this interpretation.

Issues of knowledge

Depending on the specific statutes, knowledge may be codified in different ways.

For the issues at hand, we will assume that knowledge constitutes knowledge of the acts undertaken and not of the consequences of those acts. This greatly favors Plaintiff in this case, and an alternative analysis based on knowledge of the consequences asserted as damaging might also be explored. That alternative is not explored herein.

Issues of access

The issue of access is key to this matter, and more specifically, the issues of (1) what access is granted and not granted through the permission, and (2) whether and to what extent that access was exceeded.

Issues of causing identified harm

The issue of causality in this analysis is not simply an issue of an event sequence that started with the transmission of a message and resulted in identified harm. The overall event sequence within which any such event sequence lies is also at issue.

For example, if Plaintiff installed and configured their system so as to produce large quantities of log files and chose to store those log files in locations where they disrupted other operations, then any asserted claim of harm would, at a minimum, be shared by Plaintiff and Defendant.

To the extent that such acts were not within the normal acts of a party such as Plaintiff, or to the extent that Plaintiff failed to meet diligence standards with regard to such configurations, liability might fall entirely with Plaintiff. For example, a Plaintiff who captured complete Ethernet traffic logs and stored them on a floppy disk along with the critical data generated by their email system would surely run out of space quickly and could not reasonably claim to be operating as a normal Internet Service Provider.

Issues of what constitutes harm and its quantity.

Analysis of damages is not the subject of this paper, however, it may have to meet a threshold for legal purposes, and be quantifiable, time limited, and of a legally identified type in order to be accepted by the courts. This issue is covered in more detail in [7].

Basis of the claims

Plaintiff asserted evidence consisted of, (1) a collection of asserted traces of electronic mail messages from Plaintiff's computers, (2) depositions, declarations, reports, and other similar documents by parties and their experts but none by 3rd parties or their representatives, (3) depictions of how a user might see alleged messages, (4) a spreadsheet listing apparent asserted claims, (5) a file containing what is apparently statistics of some sort, and (6) a file containing what was asserted to be contemporaneous notes by Plaintiff. Note that none of these include any traces extracted from from any computer not in Plaintiff's infrastructure, such as traces from originating computers or intermediate computers involved in the sending of the alleged messages.

ANALYSIS OF THE ISSUES IN THIS MATTER

Following the general layout of the analysis provided above, in order to establish control or a lack thereof, the analysis starts by examining direct control.

Is direct control by Defendant demonstrated?

In order to establish direct control{1.1}, for each relevant interface, system, or mechanism at issue, special {1.1.1 or 2} and general purpose {1.1.3 or 4} are differentiated, normal and control envelope exceeding use are differentiated {.1 or 2 OR .3 or .4}, and the analysis proceeds.

The mechanisms are special purpose

The analysis method differentiates between general- (i.e., if it can emulate a (finite) Turing Machine, as described in [9]) and special-purpose (lacking that ability) mechanisms, devices, operating environments, programs, and interfaces. In the matter at hand, general purpose computers were in use by Plaintiff, but claims in this case were made only with regard to normal external interface use of the simple mail transfer protocol (SMTP)[4] and domain name service (DNS) [5] protocols on their normal ports, and in quantities and timings consistent with the normal design and operating parameters of Plaintiff's systems. {1.1.1 and 1.1.3}

From [3] as detailed above, and upon examination of the protocols identified, the mechanisms available to Defendant through SMTP[4] and DNS[5] are special purpose.{1.1.1} In particular, neither SMTP nor DNS protocols allow storage and retrieval of content through the protocol, a necessary but not sufficient requirement for finite Turing equivalent computation. DNS only returns a pre-defined subset of what was sent to it along with stored data not under the control of the protocol user and is a stateless protocol. SMTP has similar constraints except that it includes a TCP state and several bits of state associated with progress through the protocol, but this state cannot be used to store and retrieve substantial data because the FSMs of the SMTP protocol respond with only fixed responses based on state, each selected from only a few possibilities, and the SMTP protocol does not provide for any operations other than those that move from state to state (i.e., no logical operations such as AND, OR, etc.). This then implies "For special purpose mechanisms, no matter what the intent of the person ultimately responsible for the input, in normal operation, the mechanism can only carry out the intent of the designers as expressed by the implementation and configuration."[3] Both of the mechanisms at issue, in normal use, are special purpose. {1.1.1}

The control envelope was not apparently exceeded

The analysis method differentiates between normal use {1.1.1} and use that exceeds the normal control envelope of the special purpose interface. {1.1.2} In the case of an SMTP server or DNS server, the envelope of normal use for an Internet Service Provider (ISP), which Plaintiff asserts he is, includes some quantity of requests that are unfruitful to the ISP. Courts have ruled that ISPs have

a duty to scale their infrastructure so as to accept some such level of requests, and that it is part of the nature of the Internet that some such requests will be misdirected, erroneous, or otherwise present.

In this case, no evidence was provided nor claims made that Defendant or anyone acting on behalf of Defendant exceeded the normal control envelope of the identified protocols{~1.1.2}, that the volume involved was excessive {~1.1.1.3} or even that it was a significant percentage of the normal traffic in Plaintiff's servers. Further, Plaintiff configured his servers so as to accept requests directed toward non-existent accounts, so that traffic that would otherwise not have been sent was in fact sent and this appears to be responsible for all asserted messages proffered.

Direct control was not demonstrated

Thus the analysis is restricted to identifying whether or to what extent traces are present to evidence (1) the use of syntax elements that could cause the identified effects, {1.1.1.2} and (2) that such use of such syntax elements, if there was any, had the effects asserted. {1.1.1.3}

The use of syntax elements

In examining the syntax elements of the SMTP and DNS protocols [4][5][6] I found no syntax that would allow Defendant or anyone else using the external interfaces to the SMTP or DNS services to affect direct control over storage space, processing methods in use, resource allocation, use of systems not including the receiving servers themselves, memory usage or allocation, maintenance functions, monitoring, or risk management decisions. {!1.1.1.2} Thus there was no way, for example, for Defendant or anyone else using such interface to enable or disable logging, filtering, storage, allocations, priorities, or anything else of that sort. {!1.1.1.3}

Even if there were such a capability, (e.g., at a low-level, packet prioritization may be in effect in some routing infrastructure), no traces were provided to indicate that any such methods were used so as to alter the use levels defined by the configuration in the computer that was defined by Plaintiff's sole acts. {~1.1.1.2, ~1.1.1.3, ~1.1.2} Lacking any traces supportive of such acts, even if syntax elements were available to support such acts, {if 1.1.2} no evidence is apparently available {~1.1.2.1, ~1.1.2.2} to show that Defendant undertook any such acts.

Evidence of effects

Lacking a syntax to express such a semantic as enabling or disabling logging, filtering, storage, allocations, priorities, or anything else of that sort, there is no associated semantic expressible by Defendant from the limited interface asserted as used. {!(1.1.1.1 → 1.1.1.3) → !1.1.1.3} → {0.1}

However, even if there were such syntax, no traces were provided to indicate that any such semantics were ever carried out by any mechanism Plaintiff asserts

Defendant used. {~1.1.1.3} Lacking any traces supportive of such semantics, no evidence is apparently available to show that Defendant caused such semantics to be executed.

Was indirect control by Defendant demonstrated?

Plaintiff made no claim and demonstrated no mechanism by which indirect effects of Defendant could have altered the normal control envelope of the identified protocols. {~1.2.1} Thus the it is reasonable to conclude that no claims or evidence support indirect control.{→ ~1.2} However, at best, Plaintiff's entire claim is one of indirect control. Plaintiff claims, in essence, that by using the interface in the normal fashion, indirect control was exerted that caused the identified asserted damages. In order to evaluate indirect control, it is necessary to start with a set of candidate mechanisms and, for each such mechanism, identify whether and to what extent that mechanism provided control as identified in the direct control approaches. Performing the same analysis on the indirect control assertion that was provided without substantial trace or analysis as a basis, we might use the following approach.

The mechanisms are special purpose

As discussed earlier, the indirect control mechanisms that might be asserted are no more than all side effects of acts performed by the directly controlled mechanisms. {1.2 ⊂ 1} Since all of the direct control mechanisms are special purpose, so must be any indirect control paths, so long as the normal control envelope was not exceeded. {1.1.1}

The control envelope was not exceeded

In this case, no claim was made in excess of the direct control envelope {~1.1.2}, no traces or evidence was given or asserted to support such a claim,{~1.1.2.1, ~1.1.2.2} and no uncovered paths or exploited weaknesses were asserted or identified from traces.{~1.1.2.1.1 * ~1.1.2.1.2 → ~1.1.2.1} Lacking any of these, there is no basis in the methodology for asserting or supporting special purpose mechanisms operating in excess of normal control envelopes. {~1.1.2}

Plaintiff was in direct control of the mechanisms

In this case, Plaintiff owned and operated the server computers at issue, installed, configured, and used the operating environments, software, configuration files, settings, and all other aspects of the mechanisms asserted to have been accessed and altered. To the extent that the analytical method is a valid approach to analysis, it may reasonably be applied to all parties, and in this case, to Plaintiff. We will use {P: …} to indicate Plaintiff control.

The mechanisms included general purpose ones

Plaintiff, through ownership and unlimited access to and control of the hardware, was in possession and control of all of the mechanisms operating within those environments. {P:1} Since these are general purpose computers with the finite version of Turing capability, Plaintiff had general purpose use of those

mechanisms.{P:1.1.3} In addition, Plaintiff had special purpose access to special purpose interfaces and, at his sole discretion, could have altered such interfaces to provide general purpose use to himself or others.{P:1.1.2} No traces were provided to support or refute any such contention, if it were ever to be made. {~P:1.1.2}

The mechanisms were in normal use by Plaintiff

Since Plaintiff owned the mechanisms at issue, there is no sense in which the authorizations associated with its use could have been exceeded by Plaintiff. Even if Plaintiff were to use uncovered paths or exploited weaknesses, such use remained within Plaintiff's authority. {P:1.1.3. P:1.1.1}

Plaintiff's control envelope included claimed effects

The control envelope of general purpose unlimited access to all systems and mechanisms at issue was sufficient for Plaintiff to have enabled or disabled logging, controlled use of filtering, limited or controlled use of all areas of storage and allocations, set any implementable priorities for operations, or anything else of that sort. {P:1.1.3.1} With Plaintiff's authorized access, all of the syntax and semantics required to invoke such control was directly available to Plaintiff at all relevant times. {P: 1.1.3.1}

Claims evidence use of syntax and semantic effects

Plaintiff indicated that he configured the systems at issue, {P:1.1.3.2, 1.1.3.3} including (1) installing operating environments and software that handled SMTP and DNS requests, (2) placing storage for servicing of those requests and storage of logs therefrom as he desired, (3) configuring such servers so as to log in excess of default logging and thus increasing the storage associated with such logs, (4) installing, configuring, and operating filtering technologies in use, (5) setting priorities for operations of different services on the systems in use, and in excess of default, and (6) authorizing receipt of electronic mail messages addressed to user identities that did not otherwise exist on said systems so as to accept messages, consume bandwidth, produce logs, store messages, and otherwise consume resources that otherwise would not have been consumed.

At any time, Plaintiff could have altered any of these settings to limit damages, prevent transmissions, eliminate logs, eliminate filtering, or otherwise limit effects. But Plaintiff continued to operate these systems in this way over a period of years. {P:1.1.3.1 and 1.1.3.2 and 1.1.3.3}

Using the same criteria as was used in the analysis of the claims made by Plaintiff against Defendant, Plaintiff expressed intent to produce the effects asserted by Plaintiff as violative by so configuring his system to produce these effects, Plaintiff admits that he expressed such intent, and admits that his expressed intent was acted upon by his systems and mechanisms. In addition, traces provided by Plaintiff are consistent with that intent being expressed and acted upon. {P:1.1.3.1 * 1.1.3.2 * 1.1.3.3 → 1.1 → 1}

By this analysis method, Plaintiff was in control of the systems at issue at the times at issue.

Defendant had no control over non-server activities

Following the same analytical process, time and space consumption on servers and systems not directly involved in the reception of traffic from Defendant can similarly be ruled out in terms of intentional causation. In the matter at hand this included claims regarding bandwidth used to download asserted messages, space consumed on auxiliary systems, and time consumed in gathering the asserted messages.

SMTP has no control over non-server activities

SMTP has no syntax expressing control over forwarding, downloading, backing up, retrieving, or analyzing messages.{!1.1.1.1} Examination of [4] and [6] evidences that no such protocol element exists and no claims of exceeding control envelopes was made. {~1.1.2}

DNS has no control over non-server activities

DNS protocols have no syntax for expressing control over forwarding, downloading, backing up, retrieving, or analyzing messages.{!1.1.1.1} Examination of [5] evidences that no such protocol element exists, and no claims of exceeding control envelopes was made. {~1.1.2}

Plaintiff was in control of non-server mechanisms

In this case, Plaintiff owned and operated the non-server computers at issue, installed, configured, and used the operating environments, software, configuration files, settings, and all other aspects of the mechanisms asserted to have been accessed and altered. To the extent that the analytical method is a valid approach to analysis, it may, again, reasonably be applied to all parties, and in this case, to Plaintiff.

The mechanisms included general purpose ones

Plaintiff, through ownership and unlimited access to and control of the non-server hardware, was in possession and control of all of the mechanisms operating within those environments.{P:1} As general purpose computers with the finite version of Turing capability, Plaintiff had general purpose use of those mechanisms. {P:1.1.3}

The mechanisms were in normal use by Plaintiff

Since Plaintiff owned the mechanisms at issue, there is no sense in which the authorizations associated with its use could have been exceeded by Plaintiff. Even if Plaintiff were to use uncovered paths or exploited weaknesses, such use remained within Plaintiff's authority. {P:1.1.3. P:1.1.1}

Plaintiff's control envelope included claimed effects

The control envelope of general purpose unlimited access to all systems and mechanisms at issue was sufficient for Plaintiff to have enabled or disabled

logging, controlled use of filtering, limited or controlled areas of storage and allocations, used or not used bandwidth or processing power for any desired function, set priorities for operations on any implementable basis, or anything else of that sort. {P:1.1.3.1} With Plaintiff's authorized access, all of the syntax and semantics required to invoke such control was directly available to Plaintiff at all relevant times. {P:1.1.3.1}

Claims evidence use of syntax and semantic effects

Plaintiff indicated that he configured the systems at issue, {P:1.1.3.2, 1.1.3.3} including, (1) installing the operating environments and software that stored, transmitted, received, and processes the content in question, (2) placing storage and processing power where he desired, (3) configuring systems and networks so as to move content already identified by him or his systems as "spam" from place to place, (4) storing multiple copies of "spam" in different places, (5) installing, configuring, and operating filtering technologies in use so as to continue processing, storing, and transmitting identified "spam" after it was so identified, (6) setting priorities for operations of different services on the systems in use, and (7) taking time to look at items that had already been definitively identified and segregated by his systems as "spam", all so as to consume bandwidth, produce logs, store messages, and otherwise consume resources that otherwise would not have been consumed.

At any time, Plaintiff could have altered any of these settings to limit damages, prevent transmissions, eliminate logs, eliminate filtering, or otherwise limit effects. But Plaintiff continued to operate these systems in this way over a period of years. {P:1.1.3.1 and 1.1.3.2 and 1.1.3.3}

Using the same criteria as was used in the analysis of the claims made by Plaintiff against Defendant, Plaintiff expressed the intent to produce the effects asserted by Plaintiff as violative by so configuring his system to produce these effects, Plaintiff admits that he expressed such intent, and admits that his expressed intent was acted upon by his systems and mechanisms. In addition, traces provided by Plaintiff are consistent with that intent being expressed and acted upon. {P:1.1.3.1 * 1.1.3.2 * 1.1.3.3→1.1.3→1.1→1}

By this analysis method, Plaintiff was in control of the systems at issue at the times at issue.

AS REPORTED

As reported, the following summary conclusions were stated in this matter. Indications in parens indicate what elements of the claims, identified in pertinent parts above, are apparently refuted by the summary results. These conclusions are presented in pertinent parts as well from documents in [8] and use language identified within [3] and [7] to express results precisely:

Plaintiff has not shown that any breakin occurred anywhere or that his systems were taken control of

"I have found no reliable scientific or technical basis in any of the information I have been provided to support any claim that the physical infrastructure was interfered with, that any alteration or forgery of any IP address took place, that any alteration or forgery of any TCP or UDP datagram took place, or that any alteration of any DNS or email system, request, or response took place in this matter...

It appears that none of the sorts of vulnerabilities or attack mechanisms known and widely discussed within the computer security community were in any way involved in anything claimed by Plaintiff in this case and that Plaintiff does not assert that Defendants exploited any vulnerability or weakness or used such any mechanism to attack Plaintiff's systems.

I found no reliable scientific or technical basis ... to support the claim that the [messages] or Defendants took control of Plaintiff's computer.

Plaintiff could easily have refused [messages] based on any number of criteria if [they] were in any way determined to be illegitimate or not appropriate to reception, but failed to do so. Plaintiff's servers were, apparently, configured to accept [messages] not [addressed to] users of his systems, but rather for the sole purpose of authorizing and inviting messages not bound for such users. … If this were not so, the [messages] would and could never have been sent. In all cases, it appears that Plaintiff's computers were only carrying out the intent expressed in the input to the extent that it was within the intent of the designers and the constraints of the implementation and configuration, which was under the sole control of Plaintiff. In step after step, Plaintiff apparently configured his computers so as to choose to accept the [messages] stating (literally) "OK" and only granted permission to send the [messages] after going through multiple control steps for each ... This does not appear to me to meet the definition of "take" or "control" by anyone other than Plaintiff.

It appears that Plaintiff in this case had access to and had the ability to perform analysis of information reflective of the operation of his system and to adjust its allocation of space, time, and other resources, to control what was and was not logged, stored, retained, and disposed of, to change prioritization of different processes within those systems to meet his desired operational needs, to control which email addresses accepted email messages, which areas of disk and memory were used to store what, which software was run, and every other aspect of what resources were used in what ways within his systems. Defendants did not have even the ability to express any desires related to the control of these things through the interfaces provided by Plaintiff, and thus had no control over any of these things. Under his sole control and at his sole discretion, Plaintiff decided to maintain or adjust his systems so as to produce the results produced by his systems, and expressed that desire and control by authorizing all of these things as

expressed by his configuration of his systems in the manner and fashion so as to produce the results he got.

Plaintiff has failed to show and has denied the ability to show that anyone sent the [messages] through intermediary computers by illegally breaking into any computers used to send those messages to Plaintiff. (1(d)) It appears that Plaintiff's authorized programs, mechanisms, and configurations were in continuous control over the actions of Plaintiff's computers at all times, and only Plaintiff's knowing and intentional acts authorized any alleged emails to be sent to Plaintiff. (2(d), 2(e), 2(f), 3(a), 3(b), 3(c), 3(d), 4(a), 4(b), 4(c), 4(d), 4(e))"

Plaintiff system operation was unimpaired

"Plaintiff in this case had sole control over the priorities set within the server and workstation for the execution of the various services at issue and other programs and services operating within those systems.

To the extent that one process was prioritized over another or that one sort of operation was performed while another was not, this was based on Plaintiff's configurations of Plaintiff's systems, and was apparently under Plaintiff's sole control.

Plaintiff expressed his intent with regard to the services he provided by allocating different priorities and resources for different processes and mechanisms operating within his servers, and those servers apparently carried out his expressed intent.

Plaintiff, at any time, could have expressed different intent, including without limit, by (1) disabling [messages] sent to the email addresses that he configured for the purpose of receiving the [messages], (2) changing storage allocation, (3) changing priorities associated with processing, or (4) through any number of other available methods under his sole control.

I found no reliable scientific or technical basis in any of the information I have been provided to support the claim that the [messages] in any way impaired the operation of Plaintiff's computers.

It appears that all of the alleged acts associated with sending the [messages] identified by Plaintiff in this matter are part and parcel of the process by which email is processed by computers configured and intended to receive such messages by Plaintiff. (2(d), 2(e), 2(f), 2(h), 2(i), 3(a), 3(b), 3(c), 3(d), 4(a), 4(b), 4(c), 4(d), 4(e))"

SUMMARY AND CONCLUSIONS

The notion of control as discussed in [3] was applied to evaluate the claims of, in effect, "knowingly and without permission", "access", and "cause damage". This case study shows how the methodology of [3] can be and was applied to issues in a specific legal matter and how its application results in resolution of issues with regard to control. The paper, while not fully covering all possibilities from [3]

shows both a demonstration of control and demonstration of non-control, in this case showing that Plaintiff had control and Defendant did not.

It appears that the methodology of [3] is usable for the purpose it was intended for and that its application can be used to bring technical clarity to the legal questions at hand. However, there are clearly limitations to this approach. It depends on analysis that is non-trivial to undertake. While the particular case studied was readily resolvable in these terms, other cases may not be. The analysis also depends on the different theories of the case, and as such, it is useful for bringing light to the legal theories and their technical limits.

REFERENCES

[1] USC 18, PI, Ch47, § 1030, *Fraud and related activity in connection with computers*. http://www.law.cornell.edu/uscode/18/1030.html [Whoever (5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.]

[2] CA Penal Code Section 502, *Unauthorized Access To Computers, Computer Systems and Computer Data* [any person who commits any of the following acts is guilty of a public offense:(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. (3) Knowingly and without permission uses or causes to be used computer services. (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network. (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.]

[3] F. Cohen, "*A Method for Forensic Analysis of Control*", IFIP TC-11 Computers and Security, V29, #8, (2010) pp 891-902.

[4] RFC 821

[5] P. Mockapetris, "*Domain Names – Implementation and Specification*", RFC 1035 available at ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt defines Internet standard 13, November, 1987.

[6] RFC 2821

[7] F. Cohen, "*Digital Forensic Evidence Examination - 2nd Edition*", ASP Press, 2010

[8] Case BC375173, William Silverstein v. Liquid Minds, LLC, et. al.

[9] Turing, "*On Computable Numbers, with an Application to the Entscheidungsproblem*", London Math Soc. Ser 2. Vol 42,Nov 12,1936,230-265.

[10] *Intel Corporaiton, Plaintiff and Respondent, v. Kourosh Kenneth Hamidi, Defendant and Appellant*. No. S103781. Supreme Court of California.

[11] F. Cohen, "*A Note on Distributed Coordinated Attack*", IFIP-TC11, `Computers and Security', V15, #2, 1996, pp. 103-121(19).

[12] P. Gladyschev, "*Formalising Event Reconstruction in Digital Investigations*", Dissertation, University College, Dublin, 2004-0-8.

[13] B. Carrier, "*A Hypothesis-Based Approach to Digital Forensic Investigations*", Dissertation, Purdue University, 2006-05, also available as CERIAS Tech Report 2006-06.

[14] F. Cohen, "*Two models of digital forensic examination*", IEEE SADFE, 2009-05-21, Oakland, CA

[15] F. Cohen, "*Digital Forensic Evidence Examination - 3re Edition*", ASP Press, 2011, Chapter 3 available online at "http://infophys.com"

[16] F. Cohen, J. Lowrie, and C. Preston, "*The State of the Science of Digital Evidence Examination*", IFIP Advances in Digital Forensics VII, pending publication, Springer, 2011.