Preparing for the Next Wikileaks: Making Forensics Techniques Work

Robert F. Erbacher, *Member, IEEE*

***Abstract*—The success of Manning in acquiring and releasing US State Department cables provides strong implications for the likelihood of similar insider threat attacks occurring again in the future. Such future attacks will likely employ more sophisticated methodologies. The first goal of this paper is to begin examining what such sophisticated insider threat attacks might include. Traditionally, organizations have avoided employing insider threat detection mechanisms due to the high rate of false positives and false negatives. This is a consequence of the chaotic nature and sheer volume of data needing analysis. A second goal of this paper is to begin proposing mechanism by which insider threat detection can be made feasible, especially in critical domains. More specifically this paper proposes multiple layers of event detection which when correlated over time will provide identification of significant irregularities requiring investigation.**

***Index Terms*—Forensics, Law Enforcement, Intrusion Detection, Computer Crime, Insider Threat**

I. Introduction

The recent Wikileaks release of 260,000+ US state department cables [30] proved sufficiently successful that it must be presumed that similar releases will be attempted again in the future; success being the release of sensitive information, creation of embarrassment for the US, and the creation of strained international relations/diplomacy. It should be noted that similar releases of document are occurring from other organizations; such as Bank of America [25]. Obviously, not all releases will be damaging but we must prepare for the next attempt, as we must assume beforehand it will be damaging. When preparing for the next Wikileaks we must consider what we know about the most recent Wikileaks event:

- The data was collected and extricated from the classified arena without notice.
- Knowledge of the methodology employed comes from Lamo, an ex-hacker.
- It appears no internal evidence exists validating Manning as the perpetrator.
- No direct link has been found associating Manning and Assange, Wikileak's founder.
- When attempting to develop techniques to defend against such attacks we are limited by what the government has released about the event.

These points establish much of the goal of this paper, both in defending against such attacks and preparing for the prosecution of such attacks. Interestingly, the documents released on Wikileaks continue to be uncleared [20]. This raises additional issues of identifying individuals with security clearances who may have accessed the data, leading to issues of "Mishandling Classified Material". Ultimately, the goal is not only collect to data effective at identifying such insider threat but providing this data in a form that is legally admissible [9].

II. Wikileaks: What We Know

Clearly, we are dependent on the government releases to the media for everything that is known about Manning's acquisition of classified documents. What does seem to be clear from what the media has published is that what we do know about Manning's acquisition of classified documents has come from Lamo, a known ex-hacker turned informant. This is both from interviews with Lamo and his chat logs with Manning. Lamo himself has been considered to be untrustworthy [15]. This is important since there has so far been no indication that evidence has been acquired internally from the secure systems themselves. This is probably the biggest concern since it shows the true extent to which detection of such insider threats are limited. Additionally, it can provide enormous limitations on prosecutions due to the lack of evidence. A summary of some of the key points that has been reported [39] are:

- Manning lip synced Lady Gaga music while writing to CDs [31]; making people think he was listening to Lady Gaga music during the process.
- Manning learned of Lamo from news articles on him and contacted him to seek guidance and approval about his exploits. Much of what we know comes from their chat logs. [23]
- No connection can currently be made between Manning and Assange [4], preventing prosecution of Assange. A key question is the extent to which Assange assisted Manning in acquiring and disseminating the classified documents [4].
- Sensitive portions of the Assange/Lamo chat logs have not been released [4].
- Manning described the operation security of the facility in detail [12].
- The facility was described as being insecure [12].

Manuscript received March 15, 2011.

Robert F. Erbacher is a Senior Principal Scientist with the Northwest Security Institute, Redmond, WA 98052 USA, (e-mail: Robert.Erbacher@gmail.com).

- Manning hacked into the classified data which was outside his authorization to access [24].
- Manning may have used steganography [29].

The lack of knowledge about any of the other aspects of the acquisition of the classified documents is particularly troubling; both due to the fact that it went unknown and the fact that not knowing the specifics makes it difficult to ensure developed technology meets the needs of detecting such actions in the future. Additionally, the need to be able to show how the material was transmitted to Assange, possibly proving a greater involvement by Assange, enforces the need for additional data. The fact that private and international assets are involved may make some identification impossible in the US and shows the need for earlier internal detection of potential problems.

III. PREPARING FOR FUTURE ATTACKS

Obviously, we cannot continue to ignore issues of insider threat detection. In addition, we must consider what the methodology of a new insider threat attack might embody. Specifically, we can assume that the recent compromise of state department cables likely used a naïve attack, downloading all documents en-masse without concern for detection since little or no insider threat detection is ever done. A more sophisticated attack will be organized around multiple phases to avoid detection:

1. The actor will use systems they have previously used, preferable systems they have used frequently.
2. The actor will catalogue the location of classified documents.
3. The actor will create a script to initiate a low and slow [8] mechanism to acquire all of the previously identified classified documents.

Similarly, more sophisticated mechanisms will be employed for the exfiltration of data. We know more details on how Manning exfiltrated the data, namely he placed the files on a CD labeled as a Lady Gaga music CD. This CD wasn't scrutinized beyond the label. A CD was used since flash devices and thumb drives are disallowed on classified systems but CD drives are allowed. While we can assume that further protections will be incorporated, a fundamental tenant of computer security is that a computer system can never be made perfectly secure [3]. Thus, it will be more time consuming to exfiltrate the data collected through the intrusion detection methodology, but eventually a hole will be found. Possible mechanisms for exfiltration could include:

- Identifying a system in which the writeable aspect of a CD drive was accidentally not disabled.
- Inserting devices into plug and play PCI slots.
- Transferring the files through other mediums left unprotected, either purposefully or accidentally: Bluetooth, firewire, usb, video channel, etc. Video channels are particularly interesting given their bandwidth and the fact that many current video cards have multiple video output ports.
- Covert channels. Transmitting the data wirelessly to a mobile device through fan speed, cpu frequency, disk spinups, etc.
- Physically removing a system device with the data stored on it: hard drive, system bios chip, video card, etc.

Most of these formats should be protected; the goal of pointing out these different avenues is to relate the complexity of the problem. As the saying goes, you only have to make one mistake for someone to identify and take advantage of a vulnerability. These examples also show that as the sophistication of attackers increases, so does the possible avenues for exfiltration, à la using the video port for data extraction from a classified system.

A further step in the data exfiltration would be the inclusion of anti-forensic techniques. Even in the case of using a CD labeled as Lady Gaga music, the anti-forensic techniques will allow evasion of more invasive examination of the CD. Examples of anti-forensic techniques [14][16] include:

- Appending the classified data to the end of real music or executable files. Such files would run normally without the extra data being detectable without deep file inspection.
- Placing the classified data in clusters marked as bad.
- Deleting the files.
- Embedding the files into other documents, such as Microsoft office documents. Many other document formats allow similar forms of embedding.
- Storing the files in unallocated portions of the disk.
- Storing the files in the flash bios of the device.

There are literally dozens of anti-forensic techniques that can be applied.

The multiple steps required for the exfiltration of data, especially the massive volume of data linked with the recent Wikileaks releases, provides multiple avenues for the identification of potential data compromises. These multiple avenues provide an opportunity to reduce the number of false positives and false negatives. The goal with such detection is twofold: limiting exposure of compromised data and acquiring data for legal action while it is still available. Figure 1 exemplifies one potential system for the multilevel detection of data compromise. Essentially, this proposed system relies on the idea of ensemble of techniques, relying on both different types of alerts as well as many techniques within each type of alert. For instance, many techniques associated with anomaly detection associated with intrusion detection and insider threat detection have been published and would be applicable to the task. Individually, however, these techniques generally have high false positive and false negative rates; such rates are even higher for insider threat than for intrusion detection. This ensemble of techniques also provides resilience against *byzantine general* type attacks, a critical concern with insider threat. We divide the detection of an insider attack into several primary categories:

- Insider threat detection – detection of the attack or acquisition of data. We propose rule systems to reduce the scale and scope of the data and ensembles of techniques for the detection process.
- Exfiltration detection – detection of the removal of data from the classified network and associated systems. Monitoring of data transfers that may lead to exposure of data, e.g., *covert channels*.
- Behavior analysis – this can be a reported or a detected behavior from any world: real, virtual, digital.
- Visualization – detection through manual inspection of data both raw and generated.
- Situational awareness – correlation of alerts for identification of related activity indicative of a coordinated goal and not an isolated event.

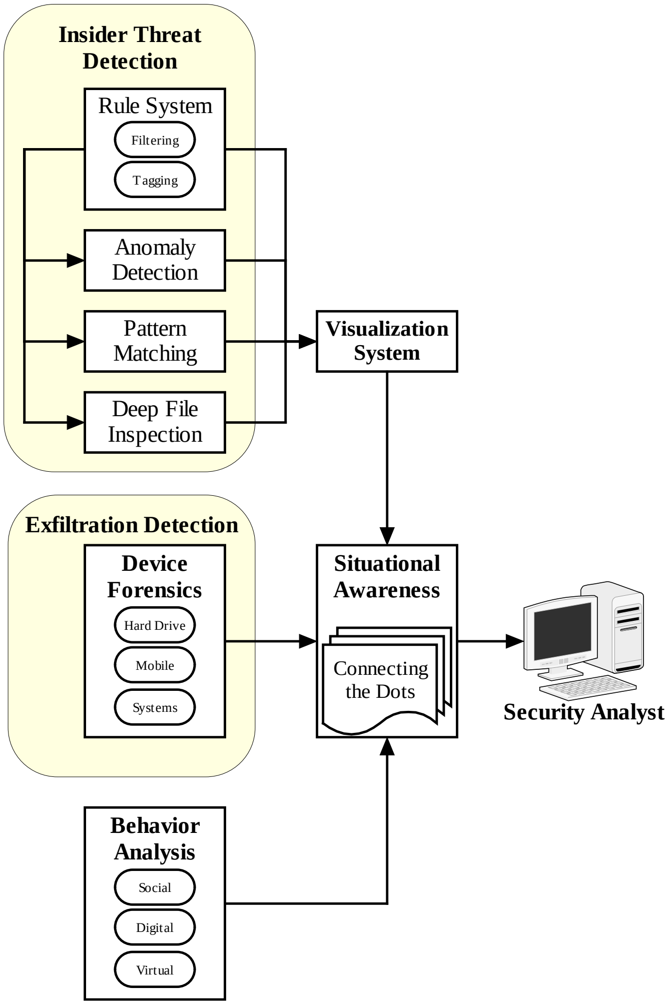

Fig. 1: Example if integration of ensemble of techniques for usable insider threat detection.

A. *Insider Threat Detection*

The long-term nature of any insider threat analysis capability will essentially be examining and correlating data after the fact, falling into the domain of forensic analysis. This is further exemplified by the fact that the initial goal of an attacker is to obfuscate their activities, i.e., apply anti-forensic techniques to avoid detection. For instance, the sophisticated methodology discussed previously would lead to most system parameters remaining consistent:

- Duration of system usage would follow normal usage patterns.
- Memory usage would remain consistent, especially after the first few files are downloaded.
- Compute cycle usage would remain low; though the small bumps in compute cycles while the system does not have an active user would be detectable. This would not eliminate the possibility of valid background processes but would provide another alert to be considered in correlation with all other events.

There will however be parameters directly detectable as being anomalous. Again, many of these alerts in isolation would likely not warrant further investigation. It is the consideration of multiple alerts that will identify scenarios requiring further analysis. Such parameters include:

- Sudden increases in the usage of disk space.
- Detectable increases in the number of classified documents touched. This could be volume of data.
- Increased volume of data transferred on the network over time. The goal of the sophisticated paradigm is to keep the rate of transmission within typical parameters.

In addition to the positive and negative indicating parameters for insider threat, the sheer volume of data needing analysis directs the mechanisms for the development of detection systems. Completely general insider threat detection systems are likely completely infeasible. There is simply too much data and typical network behavior is simply too chaotic. Thus, the goal is to identify mechanisms by which the scope of the analysis can be reduced in order to make it feasible.

The Wikileaks scenario provides a perfect test case as it provides a scenario that intrinsically contains a reduced scope. Namely, the Wikileaks scenario is focused on classified data. This greatly reduces the volume of data and range of data that is being accessed and transferred. It also reduces the complexity and scale of the problem at hand. This can be further improved by ensuring individuals truly limit the amount of classified data they access to what they must absolutely access.

1) *Rule-Based Systems*

The first step would be to employ a rule-based system [2][26] configured especially for the specific task. In essence, the rule-based system would take raw data and act as a prefilter to the rest of the analysis system. This would provide the benefit of eliminating most anomalies that would be detectable through insider threat detection systems. Examples of specific rules we would want to consider for a scenario such as Wikileaks may be as follows:

- An individual, by default, has unlimited access to data they create. Obviously, this is a rule that would be revoked if an individual leaves their position or loses their clearance. This rule handles the situation where an individual accesses data frequently while it is being generated.

- Access to new classified data would likely be ignored while access to older data would generate an alert. For instance, when a new cable is stored on the network there would likely be multiple accesses to it initially as those needing to know the nature of the cable accessed it. Afterwards, accesses would became less frequent but would still occur, such as with new employees or the generation of new reports. This can be thought of as aging the data initially before beginning to generate alerts.
- When an individual is associated with one or more anomalous events, increase the amount of data being collected associated with that user's activities and their systems.
- Ignore accesses to any data not on the classified network.
- Report accesses to the cables stored on the Wikileaks site as anomalous events.

Similarly, for diverse situations, it will likely be necessary to identify similar mechanisms by which the scope can be reduced. Additionally, the example rules listed is in no way complete but is merely designed to exemplify how the rule system would be used.

2) Pattern Matching and Anomaly Detection

Pattern matching [38], statistical analysis [18], data mining [19], machine learning [27], and anomaly detection [1] are the most traditional classifications for the majority of existing intrusion detection techniques. There are too many techniques to actually summarize them here. The lack of actual deployment itself is an indication of the unsuccessfulness of the techniques in detecting attacks with low false positive and false negative rates. It is for this reason that we are proposing a full system in conjunction with these techniques.

Additionally, by using an ensemble of these techniques we acquire the maximum range of possible detections, minimizing false negatives. Optionally, we can require a certain number of detections for reduced false positives. The advantage of the infrastructure and linkages identified in Figure 1 is that when a single technique identifies an anomaly, the rule-based system can increase data collection associated with that system. Further, the situational awareness can be configured either to ignore or display such unverified events. When displayed they can be ignored by the analyst while it is without any correlations.

Finally, the ensemble of techniques can be used to defend against byzantine general type attacks. This is a particular concern with insider threats when the attacker can easily inject obfuscating attacks or attempt to match the attack to existing background noise.

3) Visualization System

The use of visual analytics will be especially critical for the identification of the more sophisticated attacks, such as low and slow attacks which may be infeasible to identify computationally. It is with visualization that we can truly exemplify the detection of insider threat through our metaphor of reduced scope. Given the domain of insider threat and reduced scope of classified documents we can consider how existing visualization techniques can be applicable to the detection of insider threat. Figure 2 provides an example of our existing visualization technique designed specifically for the detection of low and slow port scans, in red [8]. This visualization technique can also detect other types of scans, such as focused scans; Figure 2 shows the detection of a mysql port scan in yellow.

This can be applied to classified documents, as in a sophisticated Wikileaks scenario, by considering the target to be classified documents instead of network ports. An individual accessing large numbers of documents will have a similar appearance with the document accesses appearing to saturate. This will work for both single attackers and multiple colluding attackers. It is important to keep in mind that even when such an anomaly is detected that it does not guarantee impropriety. The next step is to question, likely the individual's supervisor, if it is acceptable, within the scope of their duties, etc. Ultimately, this is a critical component of forensics: asking questions.

Scalability can be further supported by segregating the full domain into sub-domains, in which classified data is segregated by type and/or sub-network, making insider threat detection feasible within the sub-domains individually.

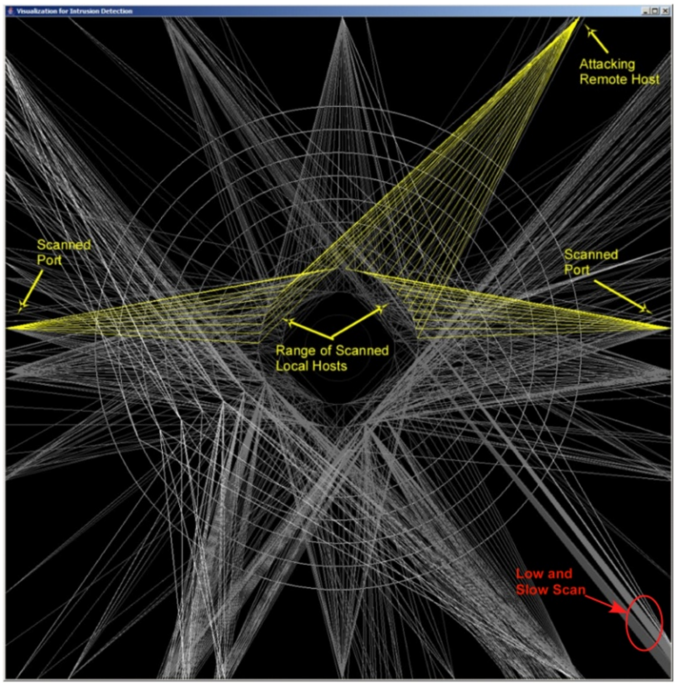
Visualization for Intrusion Detection
Attacking Remote Host
Scanned Port
Scanned Port
Range of Scanned Local Hosts
Low and Slow Scan

Fig. 2: Visualization designed for the detection of low and slow network scans.

A second visualization example is shown in Figure 3. This visualization shows a second example of an existing visualization that would be applicable to the detection of insider threat. This is an example of our tri-linear visualization technique [6], based off of ternary displays. This display is designed to show anomalous communication behavior. The longer a communication is ongoing the darker blue the associated zone the node is placed in will be. Specifically, Figure 2 shows a single local node that has suddenly started communicating, as shown by its history trail. Additionally, two local communicating nodes are shown, displayed adjacent to one another. As these nodes communicate over a long period of time their zone will turn blue. This display can be used to show sophisticated scenarios in which a local node is communicating with a classified system over a very long period of time.

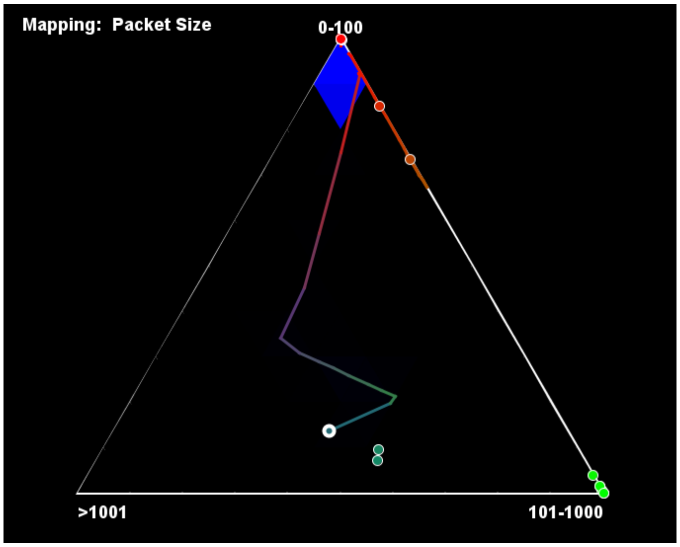

Fig. 3: Ternary visualization designed for the detection of anomalies.

B. *Device Forensics – Exfiltration Detection*

The goal with device forensics is to handle the scenario in which an individual is identified leaving a classified area with a mobile storage device of some form: flash drive, cell phone, laptop, optical disk, PCI card with a flashable bios, etc. Government rules state that such devices are not permitted in secure areas. However, what happens if a device is accidentally brought into a classified area. The policy for such devices is critical, for instance:

- Destroy the device.
- Send the device out for analysis by experts.
- Provide immediate on-site analysis. Release if the device can be *guaranteed* clean.

Destroying the device or sending it out for analysis would likely lead to reduced compliance; i.e., an individual will hide the fact that the device was brought into the classified area. This could lead to a slippery slope of ever reducing compliance. In any case, an event would likely be generated for future correlation.

The difficulty is that the device forensics must be performed by individuals who may have only minimal training and no real expertise. This requires automated tools to perform a forensic analysis, performing deep file inspection [22] to bypass any anti-forensic techniques which may have been employed.

C. *Behavior Analysis*

The government recently released a memo suggesting the use of “psychiatrists and sociologists to measure the ‘relative happiness’ and the ‘despondence and grumpiness’ of employees.” [28] Interestingly, the original premise of intrusion detection similarly focused on behavior [1][17][10][11]. Such tools, however, have traditionally suffered from high false positive and false negative rates [21]. While such tools have improved the false positive and false negative rates remain the fundamental concern preventing their deployment and adoption. For instance, the typical argument against such techniques is that attackers will simply adapt their activity so it appears normal. Ultimately, this is a focus of this paper, proposing mechanisms by which insider threat detection can be made feasible through correlation of multiple levels of events. The government goes further in identifying “unusually high occurrences of foreign travel, contacts, or foreign preference” as well as past or present participation in Wikileaks or OpenLeaks. The proposed rule-based system should easily allow for the identification of such accesses and activities by employees, from work computers at least.

In both cases, alerts can be provided to the analyst identifying not only changes in behavior but characterizations of behavior. In fact Erbacher et al. specifically examined the application of visualization towards the analysis of behavior [10] and behavior characterization [11]. We must reduce the number of alerts from traditional intrusion detection systems but identify when characterization is of concern; i.e., suddenly listening to music characterized by death or depression.

D. *Document Tracking*

Related to the issue of identifying accesses to classified documents is the attribution of documents. The Wikileaks scenario provides a critical example of the need for attribution since there currently is no link between Manning and Assange (Wikileaks), adding to the challenge in proving that Manning was in fact the individual that released the documents. As mentioned previously, most of the evidence comes from Lamo himself and his logs with Manning; the validity and provability of these logs remains a further challenge itself. Such attribution is incorporated to an extent with some sources. For example, purchasing an image or music file online will often embed a unique identifying watermark in the source file. Similarly, applications can have unique identifiers embedded into the executable code unique for an individual.

In the case of the state department cables, the value of the cables comes from the ability to validate them. Thus, it is the original images that are critical. Damaged source files or OCR’d files aren’t of value, thus similar watermarking of the files is feasible. This would require that all accesses go through a distribution server to ensure the documents are watermarked when retrieved. This would help eliminate the problem of individual documents being acquired and compromised which would be impossible to detect. This doesn’t deal with many other scenarios; for which attribution is a known challenge problem, such as:

- The document is validly acquired by an individual, whose computer is then compromised, implicating the wrong individual.
- Data that cannot be effectively watermarked, such as generated data or other textual/binary data. This would include the results of computer simulations of nuclear weapons.
- Documents that *need* to be accessed en-masse.
- The distribution server *itself* is compromised.
- The actual document isn’t needed, as it is with state department cables. For instance, nuclear weapon blueprints or trajectory formulas, etc.

E. Situational Awareness

As can be seen, especially with respect to the rule-based systems, we will be generating a large number of events. The goal with the situational awareness portion of the detection environment is to aid analysts in connecting the dots by correlating events within a single display, providing a single visual domain. This allows the government to be much more effective with respect to security. An individual meeting criterion for a single alert, i.e., being despondent or grumpy, should clearly raise concern of the individual but is not likely a definitive indicator that they will compromise classified material. However, connecting the dots between multiple events will provide extremely rapid indications of a problematic individual before actual damage can occur, with much greater accuracy than arbitrarily targeting individuals matching a single event; i.e., we don’t want to accuse someone of *thinking* about compromising data. Examples of the ways in which a situational awareness environment should provide for correlation include:

- Correlation of activities across multiple machines in order to identify coordinated efforts and differentiate attacks of concern in the spatial domain.
- Correlation of activities across users to identify collusion.
- Correlation of activities over time, especially long periods of time. This will identify slow attacks, coordinated efforts, attacks with higher levels of intent, etc.
- Visual representation of relationships such that extraordinary conditions are perceptually distinguished. This leads to rapid analysis and identification and reduced time requirements even for extremely large data sets.
- Interaction techniques (selection) to aid in the analysis of anomalous activity and to aid in the correlation of events originating from selected users/hosts.
- Combinations of heuristic and animated visualization techniques to aid in the analysis of events by representing said events through multiple views of the data.
- The situational awareness environment could integrate alerts across domains and sub-domains.

This is exemplified by VisAlert, Figure 4. Many isolated events can be seen but also a series of events affecting individual machines, such as that exhibited by the lines highlighted in green. One of the goals of the environment in total is to reduce the number of events in the situational awareness environment for final analyst review, to eliminate obfuscation and excessive cluttering.

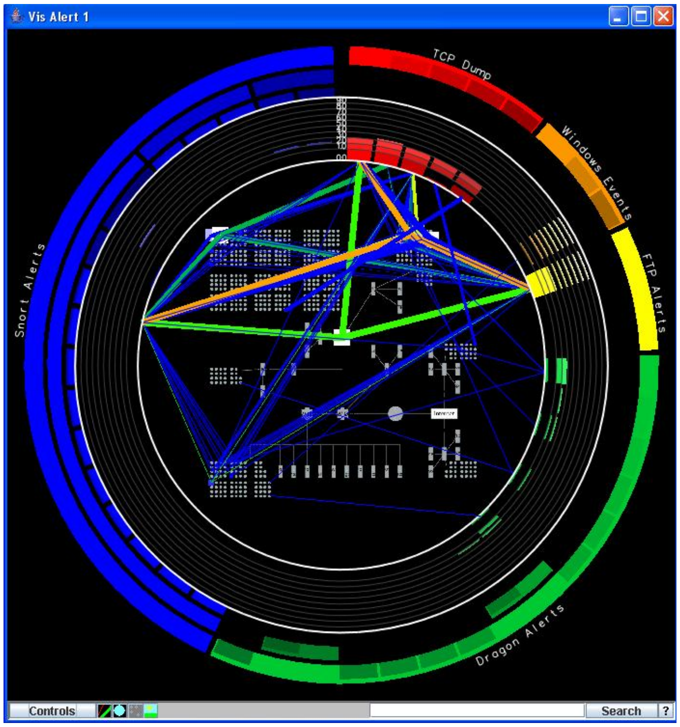

Fig. 4: The situational awareness visualization environment VisAlert exemplifying correlation and the ability for such environments to aid in connecting the dots.

IV. ANALYSIS PROCESS

The analysis process associated with our proposed environment, Figure 5, is designed to be cyclic and adaptive. In essence, there is simply too much data for all of it to be manually analyzed at all times. Thus, the goal is to configure the environment to analyze the bulk of the data through automatic tools. Select data will be analyzed manually through the visualization, such as access to classified data not *owned* by the actor. All identified events are then passed to both the correlation environment and back to the rule-based system. The key here is to adapt the rule-based system to allow more data and events associated with the identified anomaly to be collected and analyzed. This will allow other related events to be identified and the severity of the event escalated. This is done by un-filtering existing data and increasing the amount of data actively being collected. An example event sequence could take on the following stages:

1. Default rule system collects minimal information about John Doe. All government accesses to Wikileaks is monitored due to its improper storage of classified documents
2. John Doe accesses Wikileaks → Anomalous Event
   A. Modify rule-system to escalate monitoring of John Doe, focusing on his accesses to classified data if possible.

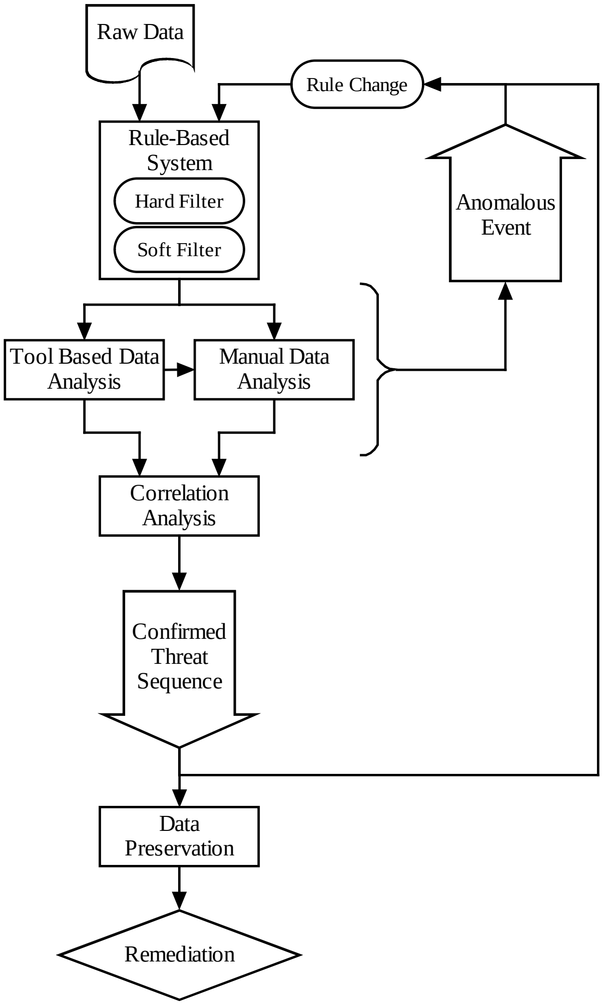

Fig. 5: Proposed operational forensic analysis process.

3. John Doe accesses classified data → event
    A. Verify that John Doe has permission and need to know for the accessed data.
    B. Monitor John Does computer systems, focusing on internal data transfers that could be indicative of covert channels.
1. John Doe directly transfers data over the monitor port → Anomalous Event
    A. John Doe is stopped while exiting classified area and he is searched for digital media of any form.
    B. John Doe's access to classified areas is restricted.
    C. The classified area is searched; there is always the possibility he stored data on a device left in the classified area to be retrieved later.
2. Digital media is identified → Event
    A. The digital media is analyzed for classified data, especially obfuscated data.
3. All data is preserved for remediation.

When data monitoring is escalated, the additional information to be collected could be manually configured. The additional data being collected could be based on:

- Fixed levels – Initial data collection for an individual would be level 0, minimal collection. As events are identified and concerns increase the level is increased until level *n* in which the user's activities are monitored at the keystroke level.
- Selective based on domain of concern – When an anomaly is identified increased data collection of *directly* associated data. If the concern is associated with classified data then monitor access to classified data. If the concern is e-mail usage then monitor e-mail accesses.

V. Conclusions

The recent Wikileaks release of US state department cables has made it clear that insider threat cannot be ignored. We have proposed a system focused on the reduction of scope of analysis in conjunction with intrusion detection and forensic techniques to make insider threat detection feasible. Cognitive task analysis (CTA) [5][7][13] will be critical to identify what techniques are truly needed by analysts. Such CTAs must be performed specifically for the tasks identified in this paper. This will be of particular value in identifying what capabilities will be well received by employees. Forensics in particular for insider threat due to the expected obfuscation and anti-forensic techniques the attacker will employ.

Many aspects of protecting against insider threat scenarios such as Wikileaks requires that government policies be in place before hand. This is critical for identifying what activity is acceptable and what must be challenged. For instance, what approval is required before accessing classified documents? Additionally, when should data preservation occur and to what level of detail? Such policies must prepare for the need to apply criminal law. In the manning case, the implication is that no data from the classified systems themselves is available; making criminal prosecution more difficult.

References

1. Dorothy E. Denning, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, Vol. SE-13, No. 2, February 1987, pp. 222-232.
2. R. Baldwin, "Rule-Based Analysis of Computer Security," Technical Report, Massachusetts Institute of Technology Cambridge, MA, 1988.
3. Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley Professional, 2002.
4. Sean Bonner and Rob Beschizza, "Wired.com: Lamo/Manning Wikileaks chat logs contain no unpublished references to Assange or private servers," *boingboing*, December 29, 2010,
5. D'Amico, A. and Whitley, K. (2008) "The Real Work of Computer Network Defense Analysts," VizSEC 2007: *Proceedings of the Workshop on Visualization for Computer Security*. Berlin; Heidelberg: Springer-Verlag, pp. 19–37.

6. Robert Whitaker and Robert F. Erbacher, "A Tri-Linear Visualization for Network Anomaly Detection," *Proceedings of the SPIE '2011 Conference on Visualization and Data Analysis*, San Francisco, CA, January 2011, pp. 78680P-1...78680P-12.

7. Robert F. Erbacher, Deborah A. Frincke, Sarah J. Moody, Glenn Fink, “A Multi-Phase Network Situational Awareness Cognitive Task Analysis,” *Information Visualization Journal*, pp. 204-219, 2010.

8. Robert F. Erbacher and Karen A. Forcht, “Combining Visualization and Interaction for Scalable Detection of Anomalies in Network Data,” *Journal of Computer Information Systems*, Vol. 50, No. 4, Summer 2010, pp. 117-126.

9. Robert F. Erbacher, “Validation for Digital Forensics,” *The International Conference on Information Technology - New Generations (ITNG)*, Las Vegas, NV, April 2010, pp. 756-761.

10. Robert F. Erbacher and Menashe Garber, “Visualization Techniques for Intrusion Behavior Identification,” *Proceedings of the IEEE Information Assurance Workshop*, West Point, NY, June 2005, pp. 84-91.

11. Robert F. Erbacher, “Visual Behavior Characterization for Intrusion Detection in Large Scale Systems,” *Proceedings of the IASTED International Conference On Visualization, Imaging, and Image Processing*, Marbella, Spain, September 3 - 5, 2001, pp. 54-59.

12. Jonathan Fildes, “Hacker explains why he reported ‘Wikileaks source’,” *BBC News*, June 7, 2010.

13. Foresti, S. and Agutter, J. (2004) “Cognitive Task Analysis Report,” University of Utah, CROMDI.

14. Garfinkel, S., “Anti-Forensics: Techniques, Detection and Countermeasures,” *Proceedings of the 2nd International Conference on i-Warfare and Security* (ICIW), Naval Postgraduate School, Monterey, CA, pp. 8-9, 2007.

15. Glenn Greenwald, “The strange and consequential case of Bradley Manning, Adrian Lamo, and Wikileaks,” *Salon.com*, June 18, 2010.

16. Henrique, G. Wendel, “Anti-Forensics: Making computer forensics hard,” *Proceedings of Code Breakers III*, São Paulo, Brazil, Setember 2006.

17. Trent Henry, “Securing the Enterprise with Network Behavior Anomaly Detection,” Research Report, The Burton Group, October 2003.

18. Akira Kanaoka and Eiji Okamoto, “Multivariate Statistical Analysis of Network Traffic for Intrusion Detection,” *Proceedings of the 14th International Workshop on Database and Expert Systems Applications* (DEXA'03), September 2003, pp. 472-476.

19. Wenke Lee and Salvatore J. Stolfo. 1998. Data mining approaches for intrusion detection. In *Proceedings of the 7th conference on USENIX Security Symposium - Volume 7* (SSYM'98), Vol. 7. USENIX Association, Berkeley, CA, USA, 6-6.

20. Eric Lipton, “Don’t Look, Don’t Read: Government Warns Its Workers Away From WikiLeaks Documents,” *The New York Times*, December 4, 2010.

21. John McHugh, “Intrusion and Intrusion Detection,” *International Journal of Information Security*, Volume 1 Issue 1 (2001), pp 14-35, 2001.

22. Sarah J. Moody and Robert F. Erbacher, “SÁDI – Statistical Analysis for Data type Identification,” Proceedings of the *3rd IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA, May 2008, pp. 41-54.

23. Denver Nicks, “Private Manning and the Making of Wikileaks,” *This Land Press*, September 23, 2010.

24. Quinn Norton, “Wikileaks Critic Adrian Lamo Defends Manning Decision,” *Gizmodo*, July 20, 2010.

25. Nelson D. Schwartz, “Facing Threat from Wikileaks, Bank Plays Defense,” *The New York Times*, January 2, 2011.

26. Sebring, M.M., E. Shellhouse, M. Hanna and R. Whitehurst, “Expert Systems in Intrusion Detection: A Case Study.” *Proceedings of the 11th National Computer Security Conference*, October 1988.

27. Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, Wei-Yang Lin, “Intrusion detection by machine learning: A review,” *Expert Systems with Applications*, Volume 36, Issue 10, December 2009, Pages 11994-12000.

28. Jaikumar Vijayan, “WikiLeaks fiasco prompts new Fed effort to boost data security,” *ComputerWorld*, January 6, 2011.

29. Kim Zetter and Kevin Poulsen, “Update: Ex-Hacker Denies Alleged Wikileaker Gave Him Classified Documents,” *Wired*, August 1, 2010.

30. Kim Zetter and Kevin Poulsen, “State Department Anxious About Possible Leak of Cables to Wikileaks,” *Wired*, June 8, 2010.

31. Matthew Zuras, “The Lady Gaga/Wikileaks Link: How Bradley Manning Easily Stole Classified Files,” Switched.com, July 10, 2010.

32. *State v. Armstead*, 432 So.2d 837, 839 (La. 1983).

33. *American Law Reports* 4th, 8, 2b.

34. *Omychund v Barker* (1745) 1 Atk, 21, 49; 26 ER 15, 33

35. http://www.law.cornell.edu/rules/fre/index.html

36. http://en.wikipedia.org/wiki/Federal_Rules_of_Evidence

37. http://en.wikipedia.org/wiki/Digital_evidence

38. http://www.iss.net/securing_e-business/security_products/intrusion_detection/index.ph

39. “Key Wikileaks-Manning Articles,” http://firedoglake.com/key-wikileaks-manning-articles/