The Evolution of Cybersecurity Investigations
A Comparison of Cliff Stoll's Techniques in The Cuckoo's Egg with Modern Methods

I. Introduction

The field of cybersecurity is crucial in our modern digital age, as cyber threats and attacks become more frequent and sophisticated. In 1986, Cliff Stoll, an astronomer turned system administrator, discovered a group of hackers engaged in military espionage, thanks to a minor accounting error on his computer system at Lawrence Berkeley National Laboratory. Stoll's investigation, chronicled in his book "The Cuckoo's Egg," provides a 'bird's eye' view of the beginning of Digital Forensics. This paper compares the tools and methods used in 1986 with those available today, to evaluate the advantages and limitations of each set of tools and methods. By analyzing Stoll's techniques and modern cybersecurity investigation methods, this paper aims to provide insights into how digital forensic investigations have advanced.

Although network monitoring tools were not as sophisticated as they are today, some basic tools were available in 1986, such as network analyzers and packet sniffers, they had limitations and required significant technical expertise to operate effectively. Stoll also wrote some of his own custom tools to analyze network traffic but most of what he did was done manually, such as examining log files and conducting manual searches of the system.

The scientific mind and approach to cybersecurity investigations are as crucial as the technical tools and methods available. While Cliff Stoll's investigation in 1986 lacked the sophistication of modern tools, his scientific way of thinking laid the foundation for modern cybersecurity investigations and his tenacity and persistence in following up on even the smallest leads could never replace the most advanced tool. The significance of adopting a scientific mindset and methodology, is evident from Stoll's account of his investigation. That mindset, combined with modern tools and techniques, are essential to combating cybersecurity threats. By comparing Stoll's techniques with modern cybersecurity investigation methods, this paper evaluates the advantages and limitations of each set of tools and methods. Additionally, it identifies investigative steps or methods available in 1986 but not utilized by Stoll, and how their application could have impacted his investigation. Ultimately, this paper provides insights into the evolution of cybersecurity investigations and underscores the importance of understanding the mind of a hacker and adopting a scientific approach to address cybersecurity threats in the current digital age.

Overview of Stoll's Investigation

Cliff Stoll's investigation into the hacking of Lawrence Berkeley National Laboratory (LBL) in 1986 was a pioneering effort in the early days of cybersecurity. His investigation involved several steps to identify and track the hackers and their activities. Here's an overview of what Stoll did:

- *Discovery:* It began with a small but significant inconsistency; the system's time-sharing model, which meticulously tracked resource allocation for billing, showed a 75-cent discrepancy. This anomaly in the accounting system, indicated a discrepancy between the recorded usage (and the associated billing) and the actual usage of the system. Diving into the depths of the billing records, Stoll harnessed the principles of time-sharing and resource allocation to trace the unauthorized activities. By correlating budget overruns with system usage reports, he could identify sessions that didn't match legitimate user profiles.

- *The Honeypot:* Cliff Stoll isolated the hacker to a special computer by setting up what is often referred to as a "honeypot." He moved sensitive files to a secured location and then created a tempting set of decoy files on a system that he closely monitored. This strategy was effective in isolating the hacker's activities to a controlled environment where Stoll could monitor every move without the risk of further compromising the network's integrity or sensitive information.

Stoll's Methods:

- *Isolation:* Stoll isolated a large section of the network's crucial information far away from the locations that the intruder had been frequenting. He did so to thwart a serious violation of secure data while setting up a cunning lure in the process.

- *Honeypot:* placing fictional classified information in a computer system known to be breached by a hacker is hacking a hacker. These data files are fabricated in the sense that they look just like the real ones, but they are not. The whole purpose is to make the hacker believes he has found valuable information. Because the access is illegal, the fact that he is in somebody else's computer system is illegal. Mention the laws do not apply to him.

  The "special computer" was configured with extensive logging to monitor access. Stoll utilized the monitors and printers he had borrowed to observe the system's operations and print out every stroke the hacker made as it happened.

  The hacker's persistent connection to this honeypot allowed Stoll to gather enough data for a successful trace. By keeping the hacker's activities contained within the monitored system, Stoll worked with the telephone company and law enforcement to trace the phone calls and determine the hacker's physical location.

- *Physical surveillance:* Stoll observed the lab's computer room to catch the intruders, hoping to catch the intruders in the act. This attempt, however, was unsuccessful. Nevertheless, it indicated Stoll's commitment to the investigation.

The data collected from Stoll's honeypot and network monitoring tools was analyzed to identify the methods and behavior patterns of the intruders. This analysis ultimately led to the ability to pinpoint the hackers' activities as occurring within Germany.

- *Law Enforcement Collaboration:* Stoll notified the FBI and other police agencies about the hack and gave them the information he had gathered. As a result, they teamed up with German officials to investigate.

- *Legal action:* Stoll's examination consequently prompted the detainment and sentence of the cyber criminal, Markus Hess, and his accomplices. The examination and accompanying lawful continuing brought about critical new inclusion all throughout the planet and encouraged realization of the security of our information.

In summary, Stoll's research techniques were notably innovative and indicated the importance of the collaboration among a policy and a commercial association that can attack cybercrime. His actions have had an influence on the investigation of modern cybersecurity and remind us of the need for enduring dynamism and attentiveness to fend off the dangers of cyberspace.

II. Comparison of Early Tools with Modern Tools

1986

Stoll's investigation techniques were predominantly based on manual analysis and observation since there were few automated tools available at the time. He spent countless hours sifting through log files and network traffic trying to piece together the hackers' activities. Some of the specific tools and methods employed by Stoll in 1986 included:

Custom scripts: Stoll constructed scripts from scratch that recorded when the hacker began each session, how long it went on, and every command the hacker entered. He also made a script that would alert him the moment the hacker came on-line so he could react in real time. In addition, he created scripts to help crack Leo's enormous database of hacker logs. For instance, he smoothed the mass of data into an analysis base by creating scripts that could sort the data by time, duration, and IP address.

Log file analysis: Stoll dedicated a substantial amount of time to analyzing various network system-generated logs. He printed thousands of lines of log data on several loaned dot matrix printers and searched through them for evidence of a subtle or unusual security breach – such as failed logins or unauthorized access to sensitive data – that network security systems had missed.

Physical observation: Real world observation involved Stoll spending extended periods in the computer lab, actively monitoring the systems and network communications. He watched the activity on the computer screen, looking for any traces of odd behavior or illicit access.

Social engineering: Stoll used social engineering tactics to gather information about the hackers, posing as a journalist to contact the hackers' internet service provider and acquire information about their activities.

It's worth noting that Stoll's investigation techniques relied largely on his own expertise and intuition, as there were few automated tools available at the time. For example, Stoll's some of the clues to the hacker's identity came from a colleague who informed him the hacker was using heathen Unix commands (not Berkeley Unix) and analyzing some of his login choices (Hunter and its German translation, Jaeger).

Another clue came from conducting an experiment using the Kermit file transfer protocol to determine why there was a consistent 3-second delay in packet travel time on the network he was monitoring.

Stoll first tested Kermit file transfers within the network and found that the transfer times were fast, indicating that the network was not the cause of the delay. Next, he transferred a file from his computer to a remote machine, which also had a 3-second delay. However, when he transferred the file back to his computer, the transfer time was significantly faster.

This led Stoll to conclude that the delay was due to the remote machine's operating system, which was using a different network buffer size than his computer. Through this experiment, Stoll demonstrated the importance of understanding the underlying technology and systems involved in network communication, as well as the need for systematic troubleshooting and problem-solving in cybersecurity investigations. He was also able to conclude that the hacker was overseas.

Probably the most important 'low-tech' method that Stoll used was borrowed from his true field of astronomy: "if you didn't write it down, it didn't happen." Stoll kept detailed notes in a notebook and used scientific methods, which he borrowed from physics but are applicable to any scientific discipline. These methods involved recording observations, applying physical principles, and speculating, but only trusting proven conclusions (Stoll, 46-47).

The Current Year

Today, cybersecurity investigations have evolved significantly with the introduction of new technologies, tools, and methods. In comparison to Stoll's investigation techniques in 1986, modern cybersecurity investigation methods showcase several differences.

Packet sniffing is still a common technique used in cybersecurity investigations today. However, modern tools like Wireshark and tcpdump have become more sophisticated and powerful.

Additionally, intrusion detection and prevention systems (IDS/IPS) like Snort, can automatically monitor network traffic and alert security teams to potential threats.

Log file analysis has also evolved with automated tools that can process and analyze vast amounts of log data much more quickly and accurately than manual analysis. Security information and event management (SIEM) systems can collect, correlate, and analyze log data from various network systems, providing real-time alerts and insights into potential security threats.

Physical observation is less common in modern cybersecurity investigations due to the advent of remote access and cloud computing. Instead, security teams rely on monitoring software and tools that can remotely monitor and analyze network traffic and system activity.

Social engineering tactics are still commonly used, but the landscape has changed significantly. Phishing attacks and other social engineering tactics have become much more sophisticated, and modern tools like email filters and web content filters can help prevent these attacks before they reach end-users.

In addition, modern cybersecurity investigations incorporate tools such as malware analysis tools, threat intelligence platforms, and digital forensics tools. These tools and methods available today are much more sophisticated and powerful than those available in 1986, and new tools and techniques will likely continue to emerge, making cybersecurity investigations even more effective in the future.

III. Modern Techniques for Cybersecurity Investigation

If a cybersecurity investigator were faced with a scenario like the one in The Cuckoo's Egg, there are several modern techniques they would likely use to investigate and respond to the threat:

Network Forensics: Advanced network forensic tools such as packet sniffers, network flow analysis, and intrusion detection and prevention systems (IDS/IPS) would help investigators analyze network traffic to identify anomalous activity and potential intrusions, enabling them to take appropriate action.

Malware Analysis: Specialized tools would be used to analyze any discovered malware or malicious code. Malware analysis tools can help identify the malware's behavior, including its capabilities, origin, and potential impact on the system.

Digital Forensics: Digital forensic tools would be used to examine any compromised systems or devices for evidence of the intrusion. Investigators would analyze log files, file systems, and memory dumps to identify any evidence of malicious activity.

Threat Intelligence: Investigators would use threat intelligence sources, such as open-source intelligence (OSINT) and commercial threat feeds, to identify any known threats or vulnerabilities associated with the attacker or malware.

Incident Response: In the event of a confirmed intrusion, investigators would implement an incident response plan to contain the threat, eradicate the malware, and restore normal operations. This would involve taking systems offline, patching vulnerabilities, and implementing additional security measures to prevent future attacks.

Cliff Stoll versus Snort

A modern example of an Intrusion Detection System (IDS) is Snort, which is a widely used open-source network intrusion detection system. Let's compare its functions with Cliff Stoll's manual logging system from "The Cuckoo's Egg":

Similar Functions:

1. Network Monitoring: Both Snort and Stoll's system monitor network traffic for suspicious activities. Stoll manually watched the network connections on his monitors, while Snort automates this process.
2. Network Logging: Stoll's system used dot matrix printers to log the hacker's activities, and Snort also logs network activities. However, Snort's logs are digital and more structured, making them easier to analyze.
3. Alerts: Stoll set up alerts to notify him when the hacker was active. Similarly, Snort generates alerts based on predefined rules when it detects suspicious activities.

Different Functions:

1. Snort performs real-time analysis of network traffic by using sophisticated algorithms to detect several different types of attacks and the anomalies that are common with such activities as DDoS attacks. In contrast, Stoll's manual system depended entirely on his personal skill in observation and analysis.

2. Rule-Based Detection: Snort’s detection engine operates on a rule-based system, where each rule specifies a particular kind of malicious activity. Stoll's discovery was reliant on his hunch and hands-on observation into the hacker's behavior.

3. Scalability: Because it is automatically and efficiently processed, Snort can monitor complex and large networks receiving a big load of traffic. In comparison, Stoll's network system was limited to the small network he was attempting to review solely through the manual process.

4. Adaptability: Snort offers the chance for its users to tailor their own rules and to account for new, evolving threats. Stoll, on the other hand, used a manual methodology. He was fixed in his ways and utilized skills and knowledge unique only to him.
5. This tool provides a number of useful data analysis features. The tool is designed to work in conjunction with other, more advanced data analysis features. This tool not only is able to conduct more advanced data analysis, but is also able to use other programs to visualize data. The program also has forensic capabilities built into it. - Stoll had to manually correlate data from different sources, and print out logs to analyze the data.

In summary, while both Snort and Cliff Stoll's manual logging system serve the purpose of detecting unauthorized activities on a network, Snort offers a more automated, scalable, and sophisticated approach with its real-time analysis, rule-based detection, and integration with other security tools.

Overall, modern cybersecurity investigations rely on a combination of network forensics, digital forensics, threat intelligence, and incident response to identify and respond to security threats effectively. By employing these modern techniques, investigators can investigate and respond to potential security incidents, preventing significant damage to their organization.

Advantages and Disadvantages of Modern Techniques

Advantages:

Speed: Modern techniques such as network forensics and malware analysis allow investigators to quickly analyze large amounts of data, identify potential threats, and respond to them faster than ever before.

Automation: Many modern cybersecurity investigation tools are highly automated, making it easier for investigators to analyze and respond to threats without the need for significant manual intervention.

Accuracy: Modern tools often provide highly accurate results, allowing investigators to more easily identify threats and take appropriate action.

Scalability: Many modern tools can scale to analyze large amounts of data across a wide range of devices, networks, and environments, making it easier for investigators to investigate complex threats and incidents.

Disadvantages:

Complexity: Complexity can be a real problem with modern tools because they often require considerable training and expertise to be used effectively. This can result in mistakes, false positives, and other errors that can impact the accuracy of an investigation.

Cost: Many of today's cybersecurity investigation tools are costly, making them inaccessible to smaller organizations or those with a limited budget.

Privacy concerns: Some modern tools for network forensics and digital forensics, may raise privacy concerns when investigators are examining data from personal devices or networks.

False Positives: Some modern tools are too good at capturing data which may generate false positives, which can lead to wasted time and resources investigating false alarms.

Overall, the advantages of modern techniques for cybersecurity investigations generally outweigh the disadvantages. However, investigators must be aware of the limitations and potential drawbacks of these tools and techniques to ensure that they are using them effectively and responsibly.

In general, modern approaches to the exploration of cybersecurity indisputably offer more advantages compared to more traditional techniques. However, investigators should stay vigilant while using these to avoid their potential shortcomings.

Hypothetical

Determining exactly how unused investigative steps from 1986 might have influenced Cliff Stoll's investigation is speculative at best. However, we can consider some potential outcomes:

- Collaboration with Other Institutions: If Stoll had worked with other organizations experiencing similar security breaches, the combined efforts could have sped up the process of identifying the hacker's methods and objectives through the sharing of information and insights. Gaining access to a more extensive range of resources, expertise, and personnel could have bolstered overall surveillance and analysis, and potentially helped identify the hacker more quickly.

- Pursuing More Aggressive Legal Measures: By taking tougher legal steps, Stoll likely would have forced telephone companies and other entities to cooperate more rapidly, in turn expediting his chances of cornering the hacker. By establishing clear legal prerogatives early in the investigation, Stoll might have adopted a more straightforward and assertive approach, overcoming bureaucratic hurdles more quickly. Additionally, a legal push arguing the seriousness of the breach might have steered more investigative resources his way.

The combination of these approaches could have potentially made Stoll's investigation more thorough. However, it's crucial to acknowledge that his work was pioneering for the era and laid the groundwork for what would evolve into modern cybersecurity practices. Stoll's innovative efforts are what have led to the advanced cybersecurity strategies we rely on today. Moreover, it's notable that, irrespective of the methods employed, Stoll was contending with a broader issue of limited cybersecurity threat awareness. The lack of immediate interest from

the FBI, despite Stoll's warnings and an alarming breach at an Army base with missile capabilities, underscores this point.

In conclusion, although it is possible that further investigation methods could have improved the effectiveness and efficiency of Stoll's investigation, it is unclear what actual impact those methods might have had. Because the techniques of that time were not widely used and not completely understood, it is difficult to say how they might have affected the results of the investigation.

V. Conclusion

In conclusion, the findings presented in this paper have significant implications for the field of cybersecurity investigations. By comparing Cliff Stoll's techniques in The Cuckoo's Egg with modern methods, it is clear there have been substantial advancements in digital forensic tools, data analytics, and threat intelligence. These advancements have greatly improved the ability of investigators to identify and track cyber criminals, highlighting the importance of continuously analyzing the latest technological advances and updating investigation techniques accordingly. The paper also emphasizes the need for investigators to continually adapt and improve their techniques in response to the constantly evolving threat landscape.

Overall, this paper underscores the importance of remaining vigilant in the fight against cybercrime and embracing advancements in technology to effectively combat these threats. The findings presented here provide a strong foundation for continued research and development in the field of cybersecurity investigations, ultimately contributing to a safer and more secure digital environment.

VI. References

Mitnick, Kevin D. (2011). Ghost in the wires: My adventures as the world's most wanted hacker. Little, Brown.

Pollitt, Mark (2010). A history of digital forensics. In K. P. Chow & S. Shenoi (Eds.), Advances in digital forensics VI (pp. 3-15). International Federation for Information Processing.

Sikos, Leslie F. (2020) Packet analysis for network forensics: A comprehensive survey, Forensic Science International: Digital Investigation, Volume 32. (https://www.sciencedirect.com/science/article/pii/S1742287619302002)

Stoll, Cliff. (1989). The Cuckoo's Egg: Tracking a spy through the maze of computer espionage. Doubleday.