Palantir: A Framework for Collaborative Incident Response and Investigation

Himanshu Khurana, Jim Basney, Mehedi Bakht, Mike Freemon, Von Welch, Randy Butler
NCSA, University of Illinois
1205 W. Clark St., Urbana IL 61801, USA
{hkhurana, mbakht2}@illinois.edu, {jbasney, mfreemon, vwelch, rbutler}@ncsa.uiuc.edu

ABSTRACT

Organizations owning cyber-infrastructure assets face large scale distributed attacks on a regular basis. In the face of increasing complexity and frequency of such attacks, we argue that it is insufficient to rely on organizational incident response teams or even trusted coordinating response teams. Instead, there is need to develop a framework that enables responders to establish trust and achieve an effective collaborative response and investigation process across multiple organizations and legal entities to track the adversary, eliminate the threat and pursue prosecution of the perpetrators. In this work we develop such a framework for effective collaboration. Our approach is motivated by our experiences in dealing with a large-scale distributed attack that took place in 2004 known as Incident 216. Based on our approach we present the *Palantir* system that comprises conceptual and technological capabilities to adequately respond to such attacks. To the best of our knowledge this is the first work proposing a system model and implementation for a collaborative multi-site incident response and investigation effort.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and protection

General Terms

Security

Keywords

incident response, digital investigation, multi-site collaboration

1. INTRODUCTION

Increasing awareness of cyber-security incidents in terms of their prevalence, impact on productivity and financial loss have motivated organizations to ramp-up their security stance and better prepare for dealing with such incidents, for example, by establishing Computer Security Incident Response Teams (CSIRTs) [8] and setting up digital investigation procedures [26]. Such capabilities allow for incident response that results in full recovery and patching to prevent relapse as well as for working with law enforcement when appropriate to pursue criminal prosecution. While measuring the success of these capabilities is not easy, anecdotal evidence and an increasing deployment rate indicates their effectiveness. However, a new breed of large-scale distributed cyber-attaks is emerging that is characterized by a set of motivated, dedicated and resourceful adversaries that attack a number of hosts, sites and organizations that apan multiple countries. In these attacks adversarial motivations range from demonstrating hacking skills to criminal intent for financial gain, and specific targets range from sensitive data theft and public image maligning to network disruptions (e.g., via denial-of-service). These attacks can be overwhelming to individual organizations responding on their own.

A prime example of such a large-scale distributed attack and our motivating use case is a series of cyber attacks known as *Incident 216* [32]. This incident took place in 2004 and involved an attacker from a foreign country who compromised the integrity of a large number of hosts in U.S. government, higher education, and commercial institutions and similar institutions abroad. The incident response and investigation process for Incident 216 brought to fore new requirements and challenges for dealing with large-scale multi-site attacks in a collaborative manner. That is, there is a need to develop a framework for effective collaboration on incident response and investigation tasks by sharing information and resources.

Establishing trust is a major challenge for these collaborations. First, the affected organizations are chosen by the attacker(s), rather than the organizations themselves, so there may be no existing relationships in place between the organizations. Second, since the collaborations would typically need to take place only after an incident occurs, involve many organizations and last for the duration of the response/investigation, they need to be short term and dynamic in nature. Third, the collaborations need to deal with data and information that is sensitive and private in nature. This includes 1) sharing of logs across institutional boundaries with user information in them that faces issues of security and privacy, 2) interaction with law enforcement and 3) interaction with the media.

IDtrust '09, April 14-16, 2009, Gaithersburg, MD
Copyright 2009 ACM 978-1-60558-474-4 ...$5.00.

These aspects of the collaboration lead to several challenges that must be addressed when designing a collaboration framework. First, the framework must provide a means for managing the tasks and processes for response and investigation undertaken by the CSIRTs of the collaborating organizations; i.e., determine who should do what and when. Second, in order to manage the tasks the organizations must place trust in each other and provide a means to share information and resources. Third, the framework must provide trustworthy information and data management with effective access control given the sensitive nature of the collaborations.

In this work, we review lessons learned from Incident 216 and propose an effective collaboration framework, that comprises a system model as well as a system design and prototype implementation that allows multiple organizations and legal entities to actively collaborate for investigating and responding to cyber-attacks. While the proposed response and investigation system is distributed in nature, it is centrally managed by a trusted entity, which we call an Independent Center for Incident Management (ICIM). The system model for the response and investigation process defines the roles, responsibilities and processes undertaken by multiple organizations (including law enforcement) to achieve full recovery and prosecution. The system design carefully addresses security and privacy of the data (e.g., security and network logs) and messages (e.g., emails, instant messages, web boards) exchanged across organizations during the response and investigation process. The security architecture provides identity-based and role-based authorization to facilitate sharing and collaboration according to organizational policies and trust relationships. The prototype system implements roles and processes for responding to and investigating an incident, incorporates tools for the collaborative response and digital investigation process, and provides adequate security and privacy.

Our approach builds on several well-known principles for effective collaboration. For trust establishment we adopt a mutual incentives based approach where organizations participate so they can learn more information and can get access to additional resources in order to respond to and recover from the attacks in their organization. Furthermore, we use a collaborative access policy enforcement approach so that organizations providing leadership in the response process can collectively define access policies. For managing tasks and processes we focus on identifying specific tasks that warrant collaboration and integrate them in a well-defined process workflow for each organization. Finally, for managing data and information we use role based access control with the least privilege principle in mind. We use these principles to design a framework that addresses this important problem of large-scale cyber-attacks.

Dealing with multi-site attacks has long been an important issue for the security community. For example, Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs) have been setup around the world for vulnerability and exploit tracking as well as facilitating coordination between CSIRTs. We believe that institutions like CERTs and ISACs could potentially serve as ICIMs in our system model. By doing so they would extend their current capabilities to support more effective multi-lateral *collaboration* between the sites, providing significantly improved incident response and investigation.

Our work is the first to develop a framework for supporting multi-site collaborative digital investigation and incident response. We integrate the two areas of prior work, namely, digital investigation and incident response, by developing models for Roles and Responsibilities as well as Processes that identify their interaction. Furthermore, we propose to extend the scope of CERTs/ISACs to support effective *collaborations* involving multiple organizations by additionally becoming ICIMs.

The rest of this paper is organized as follows. In the next Section we present lessons learned from Incident 216. In Section 3 we discuss the requirements, challenges and approach. In Sections 4 and 5 we specify the system model. In Section 6 we discuss the security architecture. In Section 7 we discuss the challenge of trust establishment. In Section 8 we describe the prototype implementation, and we provide an evaluation of our approach in Section 9. In Section 10 we discuss related work and we conclude in Section 11.

2. INCIDENT 216: LESSONS LEARNED

The scenario motivating our work is an attack by an individual or group against hosts, sites, and organizations across multiple countries. A prime example and our motivating use case is a series of cyber attacks known as *Incident 216*. This incident took place in 2004 and involved an attacker from a foreign country who compromised the integrity of a large number of hosts in U.S. government, higher education, and commercial institutions and similar institutions abroad. While the ultimate motivations of the attacker remain unknown, he seemed to be primarily interested in building this network of compromised hosts for his own personal interests.

The attacker behind Incident 216 used a well-organized process for compromising a large number of hosts and then harvesting user passwords to continue to expand his set of compromised hosts. The attacker initially compromised some number of hosts using known exploits. He then installed trojan secure shell (SSH) clients on these systems that harvested host, username and password tuples as users used the trojan SSH clients to logon to other systems. The attacker then used those stolen credentials to logon to those systems and then gained administrative privileges via known exploits for privilege escalation. Once administrative privileges were gained, the attacker would then install a rootkit to hide himself and trojan the SSH clients to use the new system to gather further account information to repeat the process and grow the base of compromised systems. As discussed by [32], he used the SSH "known hosts" file to find new attack targets.

Besides the fact that the attacker's collection of compromised systems was spread across multiple domains, the attacker also had supporting infrastructure that was also spread over multiple domains. Figure 1 shows these supporting systems, which included:

- **A Password Collector.** Every time a trojan SSH client captured a hostname, username and password tuple, it sent this information over the network to the Password Collector host. The Password Collector host was one of the compromised hosts where the attacker installed a service to collect and record these tuples for latter use.
- **A Dynamic DNS Service**. The trojan SSH clients

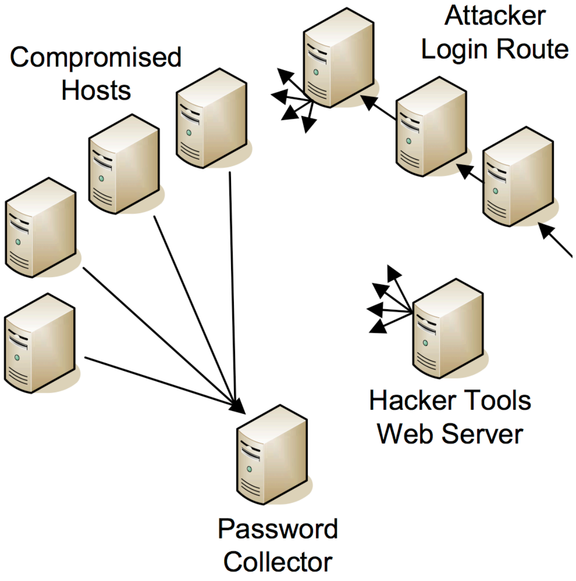


Figure 1: Topology of Incident 216 Attacker Network

used a statically configured hostname to address their network traffic with the captured tuples. This hostname was managed by the attacker through a public dynamic DNS site that allowed him to manage the mapping of the hostname to an IP address anonymously via a web form. This allowed him to move the Password Collector several times during the investigation when he felt it was potentially discovered and being monitored.

- **Hacker Tools Repository**. On one of the hosts the attacker compromised, he installed a set of exploits that he used for privilege escalation. These tools were made available via a web server already installed on the host. After gaining access to a new host, he would download these tools and use them to gain privileged access.

- **Login Route**. Instead of logging in directly from his local system to compromised systems, the attacker always went through a series of distributed intermediate systems. Presumably this was done to make the task of tracking a session back to the attacker difficult.

Investigation of Incident 216 was a difficult task because it required data acquisition across a wide range of distributed systems. Within a week of the initial discovery of the attacker, the investigation spanned a dozen sites. Eventually, the attacks spanned tens of sites in multiple countries. Many of the system administrators at the various sites were willing and even eager to help in the investigation, but often lacked the skills or time to assist, even with just understanding the events at their own site.

The result was a highly manual investigation process with the lead investigators walking sites through data gathering on their local systems, and then collecting, managing and analyzing this data. Communication between the various investigators was ad hoc, with a combination of telephone and email. At one point in the investigation it became clear that the intruder was monitoring the email of a security administrator, motivating the use of email encryption, which was cumbersome for group messaging.

NCSA staff worked side-by-side with FBI investigators to investigate and solve these attacks. One of the hardest challenges investigators faced during the investigation was the lack of knowledge in the field to identify the attacks at each of the attacked sites and hosts, without any existing coordination between sites that had been attacked. Further complicating this was a void of automated analysis of the security log information that was available, leaving the investigation up to few individuals who analyzed all of the data by hand. The NCSA investigation team committed over 3000 hours in the pursuit of this investigation. In addition to the forensic investigation from security log analysis, considerable effort was undertaken by legal teams in multiple countries to identify the perpetrator and build sufficient evidence against the perpetrator to hold up in court. This aspect of the investigation also faced hurdles in effective collaboration between prosecutors in multiple countries as well as collaboration among law enforcement personnel and system administrators. The total duration of the investigation lasted over nine months with extensive delays caused by the repeated time-consuming tasks of establishing trust between the attacked sites as well as in dealing with the complexity of the attack and the tasks required for both incident response and forensic investigation.

3. REQUIREMENTS, CHALLENGES AND APPROACH

In this section, we outline the challenges that need to be overcome and the requirements that need to be met for effective collaborative response and investigation of large scale distributed attacks. We then outline our approach, which is then detailed over the next three sections.

Requirements and Challenges. In dealing with large-scale attacks with Incident 216 being an example, the incident response and investigation process faces three kinds of challenges.

First, it is hard to establish adequate levels of trust between the involved institutions and personnel. Institutions are reluctant to share information and communicate over such matters while effective response to such attacks requires them to share information, data (e.g., logs) and communicate regularly. The core issues behind the reluctance are security, privacy and financial concerns. For example, logs contain user data that needs to be protected by law, leakage of information to media and competitors can harm the institution's image and lead to financial losses, leakage of information to the adversaries can worsen the ongoing attacks causing further delays in recovery, and investment of personnel time towards regular communication without a clear view of benefits can be perceived as a waste of resources.

Second, even after establishing adequate levels of trust, managing all the tasks and processes in the response and investigation processes is hard. There are a myriad of tasks and activities that need to be executed and managed. This includes, for example, detecting the attack, evidence gathering and storage, forensics and discovery of the attack, restoring services, eradicating vulnerabilities and flaws, sharing data and logs, collaborative decision making, information sharing and analysis, and legal prosecution. Typically, such a complex set of tasks and activities are organized into intuitive phases such as preparation, analysis, recovery, etc. However, in large-scale attacks different institutions can be in different phases and, furthermore, depending on the attack sequence and evidence discovery, institutions can have multiple phases active. Management of tasks and activities is further complicated by the duration of the response and investigation process, which lasted several months in the case of Incident 216. Such long durations make ad-hoc approaches insufficient.

Third, at the core of the response and investigation process is analysis of the digital system that includes logs and alerts gathered by various system components such as IDSs, server logs, and network logs. These logs can be large in size (100s of MBs or several GBs per day is not uncommon) and have varying formats across different organizations. Consequently, the tools needed to analyze the digital systems as well as personnel skills required to do so are not always available with all organizations that are part of a large-scale attack. Furthermore, in a collaborative response and investigation effort all of this data will need to be managed for the duration of the effort.

Approach. In this work we take a comprehensive approach of defining a system model, specifying the security architecture and describing the system implementation to address all of these requirements. The proposed system model comprises two components: 1) a *Roles and Responsibilities Model* that defines the entities involved in the response and investigation, their responsibilities and their interactions and 2) a *Process Model* that defines the various phases of the response and investigation process as well as the execution of responsibilities in these phases. Combining together these components will ensure that the response and investigation team members will be able to effectively manage the required tasks. In particular, the system model effectively integrates the technical incident response and the legal investigation and prosecution process in a multi-site collaborative manner. The following risks are minimized by this system model: missed or unassigned responsibilities, overlapping responsibilities, unclear reporting functions in a site as well as in the collaborative effort, inability to track global progress and ineffective management of tasks and phases between a site and the collaborative effort.

At the core of the system implementation is a collaborative workspace hosted by the ICIM that is accessible by all team members for managing and analyzing data (such as logs) and communications. While it is possible to implement this workspace in a distributed manner (e.g., using peer-to-peer systems) we chose a more centralized approach based on our model of central management and also to be able to provide better security. In doing so we assume the risks of a single point of failure but benefit from greater security and management assurances. The workspace is equipped with a default set of tools specifically geared towards addressing the above requirements. This includes tools for secure email, instant and web messaging, log and data anonymization, data and evidence storage, and data and log analysis and forensics. For broad adoption we have composed the workspace using open-source tools.

The proposed security architecture is designed to address a large number of threats from both passive and active adversaries. We enumerate these threats in Section 6. Threats from active adversaries are an important concern as we are dealing with active adversaries who specifically attack communications between administrators to disrupt the response process (as observed in Incident 216). An analysis of such threats led to the design of the security architecture that includes strong two-factor authentication, Role Based Access Control authorization, and a secured network perimeter around the servers implementing the workspace. In analyzing the interplay between implementing a flexible workspace and meeting the security requirements, we chose a centralized workspace environment for simpilcity but we believe that a distributed workspace implementation is also feasible though perhaps with higher costs.

Collectively, the workspace along with its default set of tools and the security architecture address the remaining requirements. The presence of such a secured workspace with a plethora of useful tools will make it significantly easier for organizations to establish trust and collaborate on the investigation and response process by committing resources and personnel. Knowing that their data is well protected and can be anonymized, if needed, will encourage them to share data and logs. The workspace also allows the collaborative process to be managed for a long duration, if needed. Lastly, the specific tools in the workspace allow for effective data management and analysis.

4. ROLES AND RESPONSIBILITIES

At the core of any collaborative multi-site response to a large-scale attack is a dedicated team of personnel staffed by the sites and by law enforcement. In this section we identify roles played by these personnel and the responsibilities associated with each role. To ensure that these roles and responsibilities are comprehensive but not significantly overlapping we use the following approach. First, we distinguish between *site roles* and *collaboration roles*. While the same individual may be assigned to both site and collaboration roles, distinguishing the roles allows for contextualization of responsibilities (i.e., site versus collaborative) and supports multiple reporting hierarchies to allow for effective team management. Second, we identify roles that cover technical, managerial, public relations and legal responsibilities. These broad set of roles and responsibilities allow for the specification of comprehensive policies and procedures in dealing with large scale attacks effectively. Specifically, the roles in our proposed model can be divided into the following five categories: 1) Site Technical Roles, 2) Collaboration Technical Roles, 3) Site Legal Roles, 4) Law Enforcement Roles and 5) Other Roles. Third, we place the responsibilities of each role in the context of the response and investigation process, as described in Section 5. Next we describe each role and its associated responsibilities.

The **Site Technical Roles** are responsible for local investigative activities at the site. The **Site Lead** is the person who leads the investigation in a particular site. He/she is also the point of contact for that site in the collaborative investigation process. The **Site Incident Investigator** assists the *Site Lead* with the local investigation, as well as containment, eradication, and recovery activities. The **Site Digital Forensics Specialist** collects, extracts and stores digital evidence locally based on the investigation strategy determined by the *Site Lead*. This role requires expertise with digital forensic tools and adequate training/knowledge to follow the right procedures so that collection and handling of the evidence meets all the legal requirements. The **Secu-**

rity/System Administrator is in charge of maintaining the site Information Technology (IT) system. He/she issues necessary authorizations for evidence collection and investigation. The **Security/System Architect** assists the investigation by sharing his/her knowledge of the IT system and the security design of the system.

The **Collaboration Technical Roles** are responsible for managing and supporting the collaboration. The **Collaboration Incident Lead** leads the investigation into the large-scale attack and also acts as a moderator/coordinator for the entire collaborative investigation process. Typically an experienced investigator in the ICIM is assigned to this role. In the CSIRT model, this is the "incident coordinator" for the designated lead CSIRT [21]. The **Collaboration Investigator** helps the *Collaboration Incident Lead* in investigating the incident(s). This role will be populated by investigators from the sites as well as from the ICIM. The **Collaboration Digital Forensics Analyst** is responsible for extracting relevant data from the evidence collected from individual sites. He/she uses different tools available for the collaborative investigation to perform cross-site analysis and construct a global timeline of the events. This role may also be populated by investigators from the sites as well as from the ICIM. The **Collaboration Workspace Administrator** is the person responsible for maintaining the collaborative environment, which supports exchange of data and messages between sites for the response and investigation process. Since the workspace is hosted by the ICIM, this role should typically be assigned to an administrator from that ICIM.

The **Site Legal Roles** are filled by lawyers, law enforcement, and security personnel local to the site. The **Site Legal Adviser** is a law practitioner associated with a particular site and responsible for advising the *Site Lead* on legal matters. This includes advice on legal and regulatory constraints on what action can be taken, reputation protection and publication relation issues, when/if to advise partners, customers and investors, etc [30]. The legal adviser also plays a crucial role in formulating and checking organizational policies to ensure that there is provision for using forensic tools to collect necessary evidence. The **Site Liason with Law Enforcement** initiates contact with the appropriate law enforcement agency when decided by the *Site Executive*. He/she acts as the point of contact for all reporting and communication between the site incident response team and law enforcement.

The **Law Enforcement Roles** are filled by government personnel. The **Legal Prosecutor** determines when and how the litigation process should proceed. He/she advises the *Site Lead* and/or the *Collaborative Incident Lead* about what legal recourse may be taken against the perpetrator(s) and the appropriate actions to take for building a strong legal case. Finally, when the investigation is successfully over, it is the *Legal Prosecutor* who takes charge and takes appropriate legal steps for prosecution of the perpetrator(s). The **Legal Investigator** is a member of law enforcement who conducts the investigation with the goal of prosecution. This role exists for both a site and the collaboration. In a collaborative environment, a *Legal Investigator* might have to coordinate the investigation with *Legal Investigator(s)* belonging to other agencies and other jurisdictions.

Finally, the following two roles are also crucial in the investigation process. The **Site Executive** is the person having overall administrative or supervisory authority of a particular site. The *Site Lead* must keep the *Site Executive* briefed on the investigation process and follow the *Site Executive's* direction. The **Media Liason** performs the important job of interacting with the media and briefing them about progress of the incident response and the investigation. Utmost care needs to be taken to ensure that no sensitive information gets revealed that might be against the interest of the affected site(s) or might hamper the investigation process.

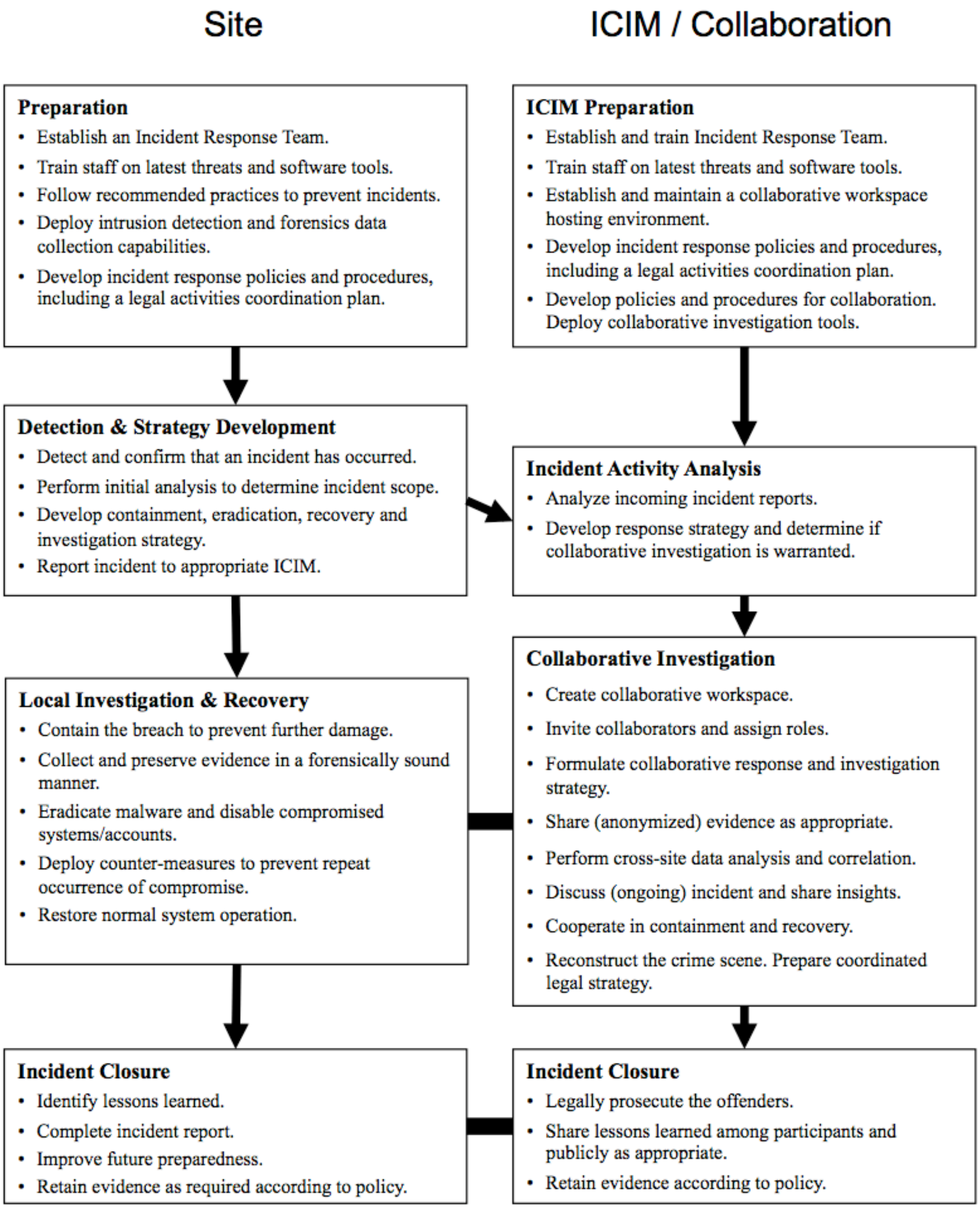
5. PROCESS MODEL

In this section, we propose a process for the multi-site collaborative incident response and investigation approach advocated in this paper. We describe in detail a four-phase model that represents the process that each site goes through locally for incident response and investigation (which leverages the Incident Response Life Cycle presented in [17]), a four-phase model that represents the collaborative process and the interactions between the site and collaborative processes. These phases are illustrated in Figure 2. The collaborative process is assumed to be executed at the ICIM.

Before going to the description of each phase, it needs to be mentioned that the division of the response and investigation process into phases is not a rigid one. If the process enters a particular phase, it does not mean that only activities that are part of that phase are permitted at that point. Rather, the implication here is that at least some part of the process has progressed up to that specific phase but there is every possibility of revisiting a step belonging to an earlier phase if the need arises. Furthermore, different sites might be in different phases as compared to the collaboration depending on the progress of the investigation.

Preparation. The primary goal of the preparation phase is to develop the capability of handling incidents based on risk assessment and lessons learned from prior experience. In a given site the *Site Executive* leads the effort by establishing an Incident Response Team. Regular training of all concerned individuals is arranged to keep pace with the latest security threats and security tools. The site *System Administrator* also plays an important role in the preparation phase by acquiring tools and resources necessary for incident response and effective investigation. Intrusion detection systems (IDSs), centralized logging, and forensic software are some examples of software tools that are deployed for detection of an incident and also for evidence gathering in subsequent phases as part of forensic readiness. Detailed policy and procedure documents are formulated that specify who should be contacted inside and outside the organization when an incident occurs. They also contain information about how that contact can be made and how much information can be shared especially with outside parties; e.g., law enforcement and other incident response teams. Taking steps to prevent incidents from occurring in the first place is also an important part of the preparation phase. *System Administrators* follow a set of recommendend practices (e.g., those given in [17]) to ensure the security of network, systems and applications that includes patch management, malicious code prevention, training to increase user awareness, host security, etc. The site *Security/System Architect* prepares proper documentation about the site's network/system designs to aide incident responders.

To prepare for the legal aspects of incident response and



Preparation

- Establish an Incident Response Team.
- Train staff on latest threats and software tools.
- Follow recommended practices to prevent incidents.
- Deploy intrusion detection and forensics data collection capabilities.
- Develop incident response policies and procedures, including a legal activities coordination plan.

Detection & Strategy Development

- Detect and confirm that an incident has occurred.
- Perform initial analysis to determine incident scope.
- Develop containment, eradication, recovery and investigation strategy.
- Report incident to appropriate ICIM.

Local Investigation & Recovery

- Contain the breach to prevent further damage.
- Collect and preserve evidence in a forensically sound manner.
- Eradicate malware and disable compromised systems/accounts.
- Deploy counter-measures to prevent repeat occurrence of compromise.
- Restore normal system operation.

Incident Closure

- Identify lessons learned.
- Complete incident report.
- Improve future preparedness.
- Retain evidence as required according to policy.

ICIM Preparation

- Establish and train Incident Response Team.
- Train staff on latest threats and software tools.
- Establish and maintain a collaborative workspace hosting environment.
- Develop incident response policies and procedures, including a legal activities coordination plan.
- Develop policies and procedures for collaboration. Deploy collaborative investigation tools.

Incident Activity Analysis

- Analyze incoming incident reports.
- Develop response strategy and determine if collaborative investigation is warranted.

Collaborative Investigation

- Create collaborative workspace.
- Invite collaborators and assign roles.
- Formulate collaborative response and investigation strategy.
- Share (anonymized) evidence as appropriate.
- Perform cross-site data analysis and correlation.
- Discuss (ongoing) incident and share insights.
- Cooperate in containment and recovery.
- Reconstruct the crime scene. Prepare coordinated legal strategy.

Incident Closure

- Legally prosecute the offenders.
- Share lessons learned among participants and publicly as appropriate.
- Retain evidence according to policy.

Figure 2: Process Model

investigation the *Site Executive* devises a legal activities coordination plan in consultation with the *Site Legal Adviser*. This plan provides the *Site Liason with Law Enforcement* basic guidance in coordinating the activities of the local Incident Response Team with that of law enforcement agencies.

Detection & Strategy Development. The main focus of this phase is to accurately detect and confirm that an incident has indeed occurred. Installation of Intrusion Detection System (IDS), antivirus software and other monitoring mechanisms in the preparation phase helps the *System Administrator* identify signs that an incident may have occurred or may be occurring. After getting confirmation about the detection of the incident, an investigation team comprising of a *Site Lead* and one or more *Site Incident Investigators* is created. The *Site Lead* carries out an initial analysis to determine the category, scope and magnitude of the incident as it is vital in choosing the next steps of the response process.

A strategy regarding containment, eradication, recovery and investigation is developed at this phase by the Site Lead. The *Security/System Architect* of the site and the *Site Legal Adviser* play important roles in formulating this strategy by sharing their knowledge about the technical and legal factors respectively. The *Site Lead* then informs the ICIM about the incident. Depending on the perceived scale and scope of the attack the ICIM personnel are invited to play an active role in developing the strategy.

Local Investigation & Recovery. After validating an incident, containing the scope and impact of the attack to minimal level becomes a major concern for the *Site Lead*. Actions regarding containment may include shutting down system(s), segregating a compromised component from the rest of the network, suspension of accounts that are suspected to be compromised, etc. At the same time, the *Site Digital Forensics Specialist* starts the important task of evidence collection. Using forensic software and toolkits, he/she obtains and extracts evidence from various sources while ensuring their integrity and authenticity. Comprehensive documentation, particularly that related to chain of custody of digital evidence, is of utmost importance in this phase. In addition, eradication, for example, malware removal and disabling of breached user accounts (if any), is undertaken to ensure that the site is no longer vulnerable to that attack. Finally, *System Administrators* restore systems to normal operation. Recovery may involve such actions as using backups to restore systems when possible, performing clean installations, etc [17].

Per-Site Incident Closure. Once the incident is over and the system recovery is complete, it is important to identify the lessons that can be learned from the handling of the incident. A report containing a critical review of the entire process is placed before management. Based on that report, the *Site Executive* may take necessary steps for better preparedness that may include modifying the policy and procedures, making changes to the personnel of the incident response team, etc. The *Security/System Architect* may decide to modify the design of the system for better security. Additional software and hardware may be deployed by the *System Administrator* to bolster the defense of the system against future threats. Based on organizational policy, the *Incident Lead* decides on whether to store evidence and in what form. It should depend on factors like whether the prosecution is finished or not, the laws regarding data retention, hardware cost, etc.

ICIM Preparation. Like any site, the ICIM develops capabilities for handling incidents in this phase. This includes training of a response team and developing policies and procedures including a legal activities coordination plan. In addition to developing these capabilities for assisting a single site with an incident, the ICIM develops these capabilities for leading a collaborative effort in responding to a large-scale multi-site attack. This includes training of personnel to lead such collaborative teams and developing collaboration-specific policies, procedures, and legal activities coordination plans.

The cornerstone of preparing for a collaborative response is setup of a **workspace** hosting environment for multi-site collaborative investigation of large-scale cyber-attacks. This environment allows *Collaboration Lead Investigators* to create workspaces and invite site and ICIM personnel to join the collaborative response. Each workspace corresponds to one incident and provides the collaboration access to tools, data and messages for executing the response and investigation process whereby each collaborator lives up to his/her responsibility as per the assigned role. A *Collaboration Workspace Administrator* is assigned for maintenance of this environment.

Incident Activity Analysis. As part of its day-to-day operations the ICIM receives reports about incidents at various sites in its purview. In this phase the ICIM undertakes an analysis of these reports to determine the level of response needed and the role that it needs to play in that response. When the analysis indicates a large-scale attack the ICIM may decide that a collaborative response is warranted. Examples include evidence indicating a growing or active botnet, zero-day exploit that affects multiple sites, website vandalism at multiple sites, and a request to do so from multiple *Site Leads*.

Collaborative Investigation. Once the ICIM decides on a collaborative response a *Collaboration Incident Lead* is identified who proceeds to set up a collaborative workspace for the incident with the assistance of the *Collaboration Workspace Administrator*. The *Collaborative Incident Lead* notifies other sites about the workspace and invites them to join. The *Collaborative Incident Lead* also performs different bootstrapping activities for the workspace including, but not limited to, assignment of *Collaborative Investigators* and *Collaborative Digital Forensics Analyst(s)* from the ICIM and other sites. In addition, depending on local laws and the nature and scale of the attack law enforcement is invited to participate in the collaboration and investigators are assigned appropriate roles.

An initial task of the collaboration is to formulate a strategy regarding containment, eradication, recovery and investigation. This strategy is documented within the workspace and often reviewed and updated as the process progresses. Data analysis is a crucial part of the investigation process. Availability of data from multiple sites opens up the possibility of performing cross-site analysis to establish links among events happening at individual sites. This analysis is conducted by *Collaboration Investigators*, *Collaboration Digital Forensic Analysts* and *Legal Investigators* and requires member sites to share data and communicate regularly. Based on the analysis the collaboration provides support to all sites for containment, eradication and recovery. While this analysis is being conducted, *Collaboration Digital Forensic Analysts* extract and store forensic evidence accumulated by the collaboration for legal prosecution. Based on the evidence, *Collaborative Investigators*, with the help from *Collaborative Digital Forensics Analysts*, reconstruct the digital crime scene/incident [11] and *Legal Prosecutors* and *Legal Investigators* formulate a legal prosecution strategy. As needed *Collaborative Investigators* interact with *Site Incident Investigators* in this phase to assist the latter with local investigation and recovery. One of the benefits of a collaborative effort is that the analysis in this phase can assist local site investigators to come up with strategies for local investigation and recovery. This includes assistance or guidance for evidence gathering and preservation, forensic tool usage, recovery, etc.

Collaboration Incident Closure. Once the investigation is over, appropriate legal steps are taken by the *Legal Prosecutor(s)* for prosecution. The evidence and theory developed in the analysis and reconstruction stage is presented to the appropriate authority. Dissemination of information [13] is another critical task in this final phase. Depending on the policy, the information may be shared with organizations that participated in the incident response or it may be added to a global knowledge repository. Finally, like participating sites, the ICIM should also have a policy on evidence retention for collaborative responses.

6. SECURITY ARCHITECTURE

At the core of our approach for collaborative response and investigation is the workspace environment that allows sites to instantiate incident workspaces and collaborate. Given the sensitive nature of this collaboration security for the workspace environment is crucial. In this section we discuss threats against the environment and our approach for addressing them. In our system design, we have worked to unify our security and system models [14] by modeling system threats and desired security properties.

Threat Model. We consider both insider and outsider threats to the workspace environment. Insiders (i.e., investigators with valid system logins) must obtain access to sensitive forensics data only as deemed necessary for the investigation. When multiple incident investigations are hosted inside the workspace environment, investigators' access must be restricted to only the incidents they are investigating. Furthermore, access to forensics data within an incident investigation must be controlled to minimize disclosure of sensitive site information. In our experience, it is typical for site personnel to share forensics data only with a small number of trusted collaborators. The workspace environment must enable multiple sites to participate in the collaboration while limiting data disclosure between the sites inside the system, including disclosure of identifying information about the participants.

Outsiders include the suspects under investigation and others who would desire to obtain sensitive information from the workspaces or otherwise abuse system resources. Suspects under investigation must not be able to use information from the workspaces to help to cover their tracks or otherwise adjust their attack strategy. Furthermore, we must limit a suspect's ability to disrupt the investigation via denial of service attacks against the workspace environment. Sensitive information that must not be disclosed to outsiders includes digital forensics data (containing sensitive site information), personal details about investigators (such as names, phone numbers, or IP/email addresses), or information about the capabilities and methods of investigators.

Authentication and Access Control. To limit workspace access to valid site and ICIM investigators we use strong two-factor authentication and to limit access to authorized data and resources between and within incident workspaces we use Role-Based Access Control. The security architecture is illustrated in Figure 3.

Role-Based Access Control (RBAC) is a natural choice for meeting the access control requirements of the collaborative environment. We map authenticated system users to per-incident roles following the approach presented earlier in Section 4. Authorized users have permission to create new incident workspaces and manage per-incident role-based permissions within the workspaces they create. Authenticated users have no access to incident workspaces by default. They must be granted per-incident roles by the owner of the workspace.

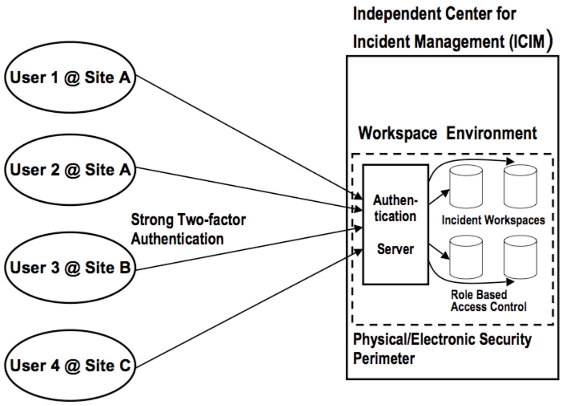


Figure 3: Security Architecture

Network Security. To protect the workspace environment from network-based attack, we establish a physical and electronic security perimeter around the environment that minimizes exposure via firewalls and private networks, requires encryption for all external network traffic, and employs network- and host-based intrusion detection. Database and data analysis services that support the user interface are deployed on a dedicated private network with no direct external network access. Leveraging a small number of standard protocols via well-known open source software enables system administrators to apply standard, best practice network security measures to address common attacks. For greater network security, the environment can be deployed inside a virtual private network to limit exposure to attacks from external networks.

Data Privacy. The collaborative environment must provide tools to enable collaborative incident response while respecting each site's information disclosure policies. The disclosure of sensitive incident data is subject to privacy policies and laws, public relations, the desire to avoid disclosure to competitors and adversaries, and the desire to avoid negatively impacting an ongoing criminal investigation [8, 9, 15]. The ICIM plays a central role in overseeing and directing data disclosure among participants. This is crucial for enabling the collaboration as otherwise the involved organizations may not end up sharing the necessary information. The ICIM may use both technical and business means in supporting data disclosure. Technical means include the use of anonymization techniques that can hide sensitive information where appropriate; e.g., [33]. However, in many cases data may not be suitable for anonymization or may be rendered useless after doing so. In which case, the ICIM can utilize established procedures for obtaining approval from the organizations on each *type* of data such that the investigation team only needs to incur occasional overhead for data sharing. The collaborative environment must support flexible access control policies to facilitate data sharing according to the different information disclosure policies of the different participants. For example, some data may be provided to ICIM personnel only while other data may be shared among all collaborators. Thus, it is not necessary for all participants to agree on a common data sharing policy; instead, participants can specify and implement their desired access control policies on the data they provide to the collaboration.

7. ESTABLISHING TRUST

The collaborative incident response approach that we describe relies heavily on establishing trust between the responders from the affected organizations. As described in the Introduction, trust establishment is a major challenge because the affected organizations are chosen by the attacker, the collaboration may be formed only after the incident occurs, and the collaboration involves sensitive information. We have observed that some organizations have a strict policy against disclosure and cooperation during incident response, so they would be unwilling to participate in a collaborative approach under any circumstances. However, NCSA staff had very positive experiences collaborating with other organizations during the response to Incident 216 and other incidents, which indicates that many organizations see the value in working together to address large-scale distributed attacks. In this section, we discuss three methods for establishing trust during a collaborative response: (1) leveraging pre-existing collaborations, (2) utilizing trusted introducer groups and services, and (3) sharing incident information of interest to the participants.

Leveraging pre-existing collaborations. In today's world of collaborative computing there is an opportunity to create ICIMs with the ability to quickly manage incidents that span these environments. For example, grid computing environments for scientific research, such as TeraGrid, Open Science Grid, the Enabling Grids for E-sciencE (EGEE), and the Worldwide LHC Computing Grid (WLCG), have relatively stable member organizations that trust each other for resource sharing. Due to their common environments and user communities, security incidents can spread between these organizations, which has motivated them to share incident response contact information and establish processes for coordinated response that are primarily email-based. These existing collaborations could directly apply our proposed workspace mechanisms to enhance their existing coordinated processes.

Utilizing trusted introducer groups and services. While we can leverage pre-existing collaborations, we have seen that attackers do not respect their boundaries, and large-scale attacks often affect organizations with no prior working relationships. The incident response community has established groups and services to facilitate trust establishment in these cases. For example, the Trusted Introducer[1] network provides vetted contact information for CSIRTs in Europe and facilitates trusted information sharing among accredited response teams. Other groups such as the Forum of Incident Response and Security Teams (FIRST)[2] as well as CERTs and ISACs act as trusted introducers between organizations impacted by distributed attacks.

Sharing incident information of interest to the participants. Finally, responders can use information about the incident to establish trust with new organizations being invited to join the collaboration. An overview of the incident for new collaborators can be maintained in the incident workspace, including timelines, attack vectors, and recommended mitigation techniques. When new collaborators see that the details in the incident overview match what they are seeing inside their organization, and they benefit from the recommended mitigation techniques listed in the overview, they are more inclined to join the collaborative response effort. Furthermore, specific details about the attack can be very effective at gaining the interest of new collaborators, as illustrated by the following anecdote. During Incident 216, one of the responders needed timely assistance from a new organization and was having difficulty getting a response. He noticed that the attacker had collected the password of one of the CSIRT members from the organization, so he asked him, “Is this your password?” When the CSIRT member recognized his password, he responded, “Now you've got my attention!”

8. DESIGN AND IMPLEMENTATION

We have developed the “Palantir” prototype system to provide a software environment that supports the collaborative response and investigation process. The Palantir system provides the collaborative workspace for discussions and data sharing among incident investigators, as seen in Figure 4. Collaboration mechanisms in the workspace include a *data repository* for log files, network traces, and other forensic data, a *wiki* for providing an overview of the incident for new members, documenting incident details, and keeping a timestamped incident notebook, secure *instant messaging* for real-time discussions, secure *email lists* [7, 19, 20] for ongoing discussions, *anonymization tools* [33] for sanitizing data before it is shared, *analysis tools* [10], and *visualization tools* [36].

Our implementation is a web application built on open source web software that can be accessed by standard web browsers. We use the Liferay Portal[3] platform, running in the Apache Tomcat[4] container, connected to the Apache HTTP[5] server. Building on open source software enables independent verification of software security through source code reviews and scanning, as performed for the Apache HTTP server by the Scan Project[6] and for Liferay and Tomcat by the Java Open Review Project[7].

Liferay supports secure chat services via the standard XMPP (Jabber) protocol using the open source Openfire[8] Jabber server. Responders can chat via a portlet within Liferay (over HTTPS) or via desktop Jabber chat clients running the Jabber protocol over TLS.

For strong two-factor authentication, we support both one-time password (OTP) hardware tokens and PKI-based smartcards. The OTP tokens and smartcards both require a PIN to unlock, providing both “something you have” and “something you know” authentication factors. When the OTP token is unlocked, it displays a one-time use password that the Palantir user enters at the login prompt. When the smartcard is unlocked, it authenticates to the server via the TLS protocol using private cryptographic data residing on the card. While smartcards save the user from manually entering a one-time password, they require hardware and

[1] http://www.trusted-introducer.nl/

[2] http://www.first.org/

[3] http://liferay.com/

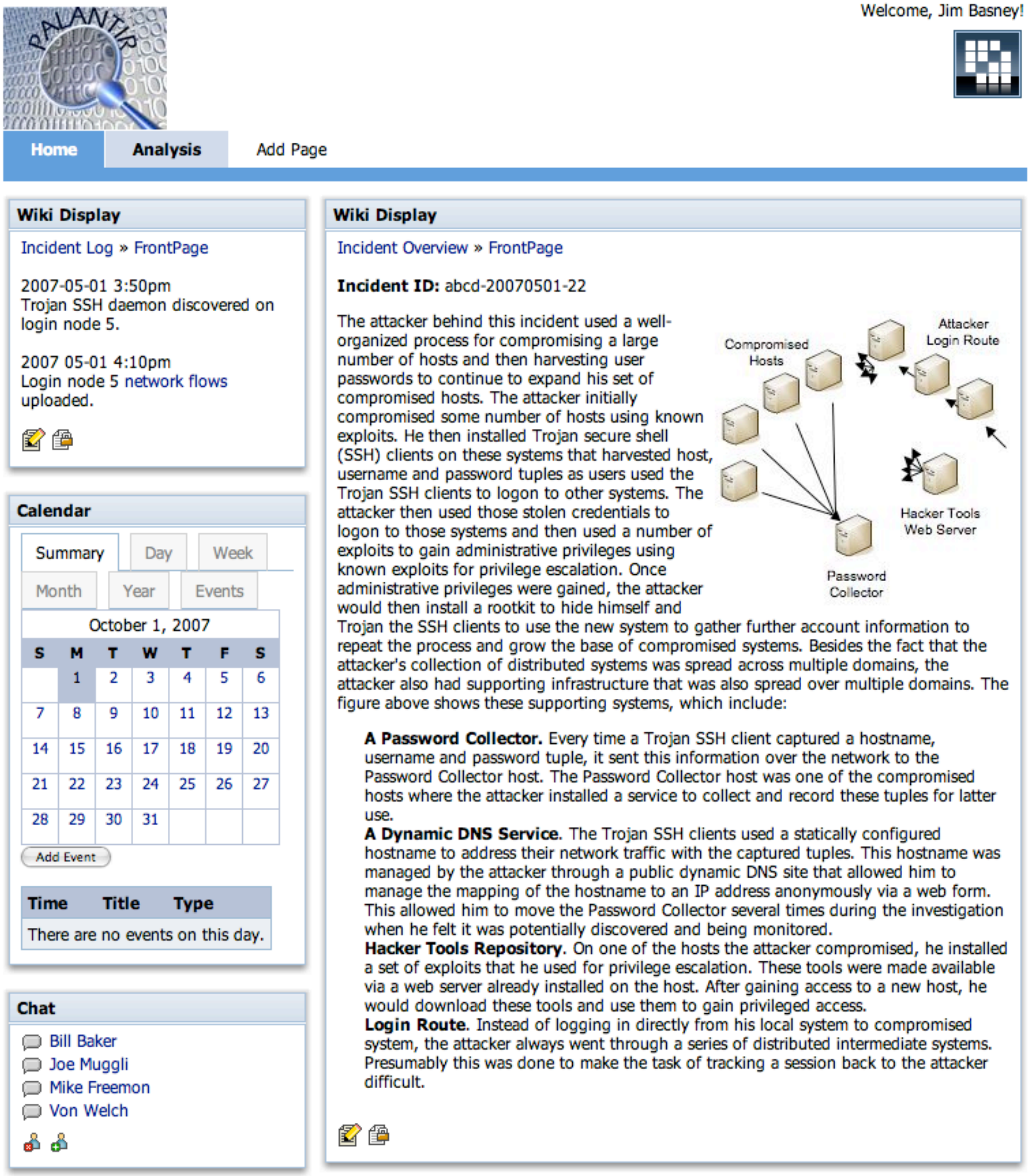
[4] http://tomcat.apache.org/

[5] http://httpd.apache.org/

[6] http://scan.coverity.com/

[7] http://opensource.fortifysoftware.com/

[8] http://www.igniterealtime.org/projects/openfire/



Wiki Display

Incident Log » FrontPage

2007-05-01 3:50pm
Trojan SSH daemon discovered on login node 5.

2007 05-01 4:10pm
Login node 5 network flows uploaded.

Calendar

October 1, 2007

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Time	Title	Type
There are no events on this day.		

Chat

Bill Baker
Joe Muggli
Mike Freemon
Von Welch

Wiki Display

Incident Overview » FrontPage

Incident ID: abcd-20070501-22

The attacker behind this incident used a well-organized process for compromising a large number of hosts and then harvesting user passwords to continue to expand his set of compromised hosts. The attacker initially compromised some number of hosts using known exploits. He then installed Trojan secure shell (SSH) clients on these systems that harvested host, username and password tuples as users used the Trojan SSH clients to logon to other systems. The attacker then used those stolen credentials to logon to those systems and then used a number of exploits to gain administrative privileges using known exploits for privilege escalation. Once administrative privileges were gained, the attacker would then install a rootkit to hide himself and Trojan the SSH clients to use the new system to gather further account information to repeat the process and grow the base of compromised systems. Besides the fact that the attacker's collection of distributed systems was spread across multiple domains, the attacker also had supporting infrastructure that was also spread over multiple domains. The figure above shows these supporting systems, which include:

A Password Collector. Every time a Trojan SSH client captured a hostname, username and password tuple, it sent this information over the network to the Password Collector host. The Password Collector host was one of the compromised hosts where the attacker installed a service to collect and record these tuples for latter use.
A Dynamic DNS Service. The Trojan SSH clients used a statically configured hostname to address their network traffic with the captured tuples. This hostname was managed by the attacker through a public dynamic DNS site that allowed him to manage the mapping of the hostname to an IP address anonymously via a web form. This allowed him to move the Password Collector several times during the investigation when he felt it was potentially discovered and being monitored.
Hacker Tools Repository. On one of the hosts the attacker compromised, he installed a set of exploits that he used for privilege escalation. These tools were made available via a web server already installed on the host. After gaining access to a new host, he would download these tools and use them to gain privileged access.
Login Route. Instead of logging in directly from his local system to compromised system, the attacker always went through a series of distributed intermediate systems. Presumably this was done to make the task of tracking a session back to the attacker difficult.

Figure 4: A Palantir Workspace

software support (i.e., readers and drivers) to interface with the user's desktop.

The open source Secure Email List Services (SELS)[9] software provides support for email-based group discussions in Palantir. SELS uses the OpenPGP standard for compatibility with commonly available email client plugins from the Gnu Privacy Guard (GnuPG) project[10]. SELS uniquely provides end-to-end privacy for email discussion lists using proxy cryptography, whereby messages are protected both on the network and the mailing list server.

The open source Framework for Log Anonymization and Information Management (FLAIM)[11] supports anonymization of log files on the responder's desktop before upload into the collaborative environment, as well as anonymization by the Palantir server during file upload and prior to export.

[9] http://sels.ncsa.uiuc.edu/
[10] http://gnupg.org/
[11] http://flaim.ncsa.uiuc.edu/

Supported log types include pcap, netfilter, NetFlows, and Unix process accounting.

Roles and Responsibilities. We now describe how the roles and responsibilities from Section 4 map to the Palantir system's capabilities.

The *Collaboration Incident Lead* is responsible for creating and managing the incident workspace, with the assistance of the *Collaboration Workspace Administrator*. The *Collaboration Incident Lead* adds *Collaboration Investigators* to the workspace, where they can coordinate their efforts via wiki pages and discussions over instant messaging and email. He also maintains a primary wiki page for the incident with an incident overview, current status, and technical information to be shared among all participants.

Collaboration Investigators learn information about the investigation that informs their local site's response, as well as contribute their knowledge to the collaborative effort. If an investigator obtains information relevant to other sites, he can share it via the workspace. *Collaborative Investigators* can upload evidence for analysis by other *Collaborative Investigators* and *Collaboration Digital Forensics Analysts*. The workspace provides anonymization tools that the *Collaborative Investigators* can apply to their site's data before sharing it.

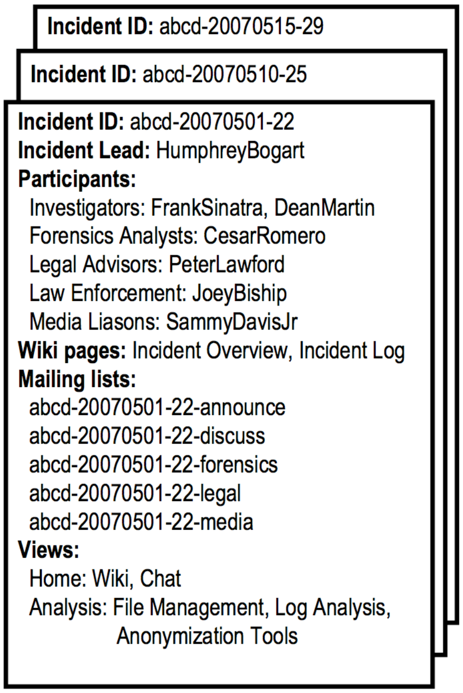
The *Collaboration Digital Forensics Analysts* apply forensics tools available in the workspace to the forensics data provided by the *Collaboration Investigators*. The analysts publish requests for evidence, guidelines for evidence collection, and analytical results to wiki pages to inform the other collaborative participants.

Other areas of the workspace, established by the *Collaboration Incident Lead* as needed, provide forums for collaboration among *Legal Advisors*, *Media Liasons*, and *Law Enforcement*. For example, Media Liasons can draft join press statements in the workspace.

Process Model. The Palantir system does not enforce a specific process model on participants. Instead, the collaborators can use the available tools in the workspace as they see fit according to the response and investigation strategy they have developed. The Palantir system allows subgroups to form and collaborate privately within the investigation workspace, before sharing their results with the larger group. The *Collaboration Incident Lead* can use the incident's secure mailing list to direct and track the group's work. Wiki pages can document current tasks and milestones in the investigation, updated as they are completed. Upon further experience, we may augment the Palantir system with forms and dialogs that facilitate common incident workflows based on best practices.

As we see in Figure 2, coordination is required between the local site incident response and the collaborative process. A simple but important practice for facilitating this coordination is for each site to record their local tracking number for the incident in the Palantir incident wiki. Palantir creates a unique tracking number for each workspace, following the recommendations in [8].

Workspace Template. In order to realize the Roles and Responsibilities Model and the Process Model in incident workspaces, Palantir provides a Workspace Template that is instantiated for every incident. The template provides ready-to-use containers for each workspace where users can be assigned to roles and automatically get access to an authorized set of resources. The template currently implemented in Palantir is described in Figure 5 and is easily customizable. For each role identified in Section 4 the template specifies: 1) the role that can assign users to this role, 2) the default view (interface layout) when this role is activated, 3) set of tools (via Liferay portlets) that this role can access, and 4) a default set of resources (objects such as files) that this role can access via each tool. A factory within Liferay generates the necessary resources and access policies based on the specified template.



Incident ID: abcd-20070515-29

Incident ID: abcd-20070510-25

Incident ID: abcd-20070501-22
Incident Lead: HumphreyBogart
Participants:
Investigators: FrankSinatra, DeanMartin
Forensics Analysts: CesarRomero
Legal Advisors: PeterLawford
Law Enforcement: JoeyBiship
Media Liasons: SammyDavisJr
Wiki pages: Incident Overview, Incident Log
Mailing lists:
abcd-20070501-22-announce
abcd-20070501-22-discuss
abcd-20070501-22-forensics
abcd-20070501-22-legal
abcd-20070501-22-media
Views:
Home: Wiki, Chat
Analysis: File Management, Log Analysis,
Anonymization Tools

Figure 5: Palantir Workspace Template

9. EVALUATION

To evaluate the Palantir approach, we describe how the Palantir system would have assisted in the collaborative investigation effort conducted for Incident 216. Collaboration played a very important role in this investigation for tracking the attacker's widely-distributed activities, understanding the attacker's methods, and finally locating and apprehending the attacker.

Compromise Tracking and Notification. Notifying sites that they had been compromised was one of the most time-consuming activities in the Incident 216 investigation. Network traffic and server logs from the attacker's password collectors and web servers provided information about compromised systems to the incident investigators. Investigators analyzed the latest information each day and notified personnel at newly compromised sites. Network, security, and system administrators at different sites gathered and provided this data to the investigators. The attacker moved the password collector several times, requiring the investigators to contact new administrators to re-establish their monitoring capabilities.

Managing the network and server logs for daily analysis was a manual process. Palantir's data repository provides the capability for administrators to directly upload their data to the investigators via the secure web interface. Investigators can use wiki pages to track which logs have been analyzed and which sites have been contacted. Using Palantir tools, the investigators can automate the daily analysis process.

When contacting newly compromised sites, it is helpful for the investigators to have a standard incident overview to share with site personnel. During Incident 216, this overview was maintained by a single investigator, but Palantir's secure wiki would allow it to be written and updated collaboratively by multiple investigators. Additionally, new sites can obtain logins to the Palantir system to read the wiki pages and participate in the investigation.

Collaborative Analysis. Incident 216 investigators were hindered by their inability to read the encrypted network traffic from the attacker's rootkit. From analyzing network logs, an administrator at one site identified the encryption protocol being used but needed the encryption key. Investigators asked for help from colleagues skilled in reverse engineering, who were able to analyze the rootkit binary to locate the encryption key. With the key, the administrator developed a decryption tool that he shared with the other investigators. Investigators were lucky that the administrator at this site had both access to the rootkit logs and the skill to develop a decryption tool. If this had not been the case, the administrator could have used Palantir to upload the logs to be analyzed by another participant.

This is one of many examples in the Incident 216 investigation of system administrators who were highly motivated to contribute to the investigation. By sharing information with them and allowing them to contribute, the investigation benefited greatly from their expertise.

As described in Section 2, the Incident 216 collaborative investigation and analysis was hindered by ad hoc communication methods. Palantir's secure instant messaging, email lists, and wiki pages provide convenient and trustworthy communication mechanisms for the investigators.

10. RELATED WORK

Starting with work that leverages experiences in dealing with paper evidence [25], considerable effort has been spent in developing models for the digital investigation process. This includes the Digital Forensic Science process [24], the End-to-End Digital Investigation Process [34], an approach for forensics in military settings [16], the Integrated Digital Investigation Model [11], the Digital Crime Scene Investigation process [12], the Enhanced Digital Investigation Model [5], a process for integrating investigations with information flow [13], the FORZA [18] framework that emphasizes legal issues, a two-tier investigation approach [6] and the combined forensics and intelligence gathering framework [31]. Reith *et al.* [28] and Pollitt [26] provide good surveys of these and other related works.

Similarly, models have been developed that deal primarily with how individual sites should respond to incidents, usually with the help of a predesignated incident response team. This includes the Incident Response Life Cycle [17], an incident response methodology [27], guidelines for formation and operation of CSIRTs [8], a study of organization models and their impact on incident response [21], best practices and guidelines [3, 29] and a corporate framework for incident management [23]. Additionally, software systems have been developed to help CSIRTs internally manage incident investigations including ticket tracking [22] and request tracking [35].

Going beyond CSIRTs, a number of efforts have been launched worldwide to establish institutions that coordinate response to large-scale multi-site attacks. Examples include the Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs) currently being operated worldwide.

Our work is significantly different in that we focus on a framework for supporting multi-site collaborative digital investigation and incident response. We integrate the two areas of relevant work, namely, digital investigation and incident response, by developing models for Roles and Responsibilities as well as Processes that identify their interaction. Furthermore, we propose to extend the scope of CERTs/ISACs to support effective *collaborations* involving multiple organizations by additionally becoming ICIMs. In particular, these novel enhancements result in a Process Model (see Figure 2) that allows incident responders and investigators across multiple sites affected by an attack to effectively collaborate in their common goals of investigating and responding to the attacks. To the best of our knowledge this is the first work proposing a system model and implementation for a collaborative multi-site incident response and investigation effort. We believe that this work can help develop capabilities to adequately prepare for large-scale attacks such as Incident 216. The US Department of Homeland Security has conducted two exercises for large-scale cyber attacks, Cyber Storm I (February 2006) and Cyber Storm II (March 2008). From the public report of Cyber Storm I [1] it is clear that even with the presence of CSIRTs, CERTs and ISACs, tools and technologies that provide advanced collaboration capabilities for incident response and investigation are needed.

Many software systems are available to help CSIRTs internally manage incident investigations. Open Source incident ticket tracking systems include Application for Incident Response Teams (AIRT) [22], Request Tracker for Incident Response (RTIR) [35], and System for Incident Response in Operational Security (SIRIOS)[12]. The Internet2 Research and Educational Networking Operational Information Retrieval (RENOIR)[13] project is developing a system for incident reporting to a trusted third-party such as REN-ISAC (Research and Education Networking ISAC)[14]. This work is complementary to ours. We assume good internal incident management and incident reporting mechanisms are in place, and we focus on collaborative incident response in reaction to large-scale, distributed incidents. While individual components of our solution, such as secure wikis and instant messaging, are starting to see more widespread use in the incident response community, we believe our work is the first to bring together these components into an integrated environment for collaborative incident response.

11. CONCLUSIONS AND FUTURE WORK

Organizations with cyber-infrastructure assets face large-scale distributed attacks on a regular basis. Based on lessons learned in dealing with such an attack and the realization that the complexity and frequency of such attacks is increas-

[12] http://sirios.org/

[13] http://security.internet2.edu/csi2/

[14] http://www.ren-isac.net/

ing in general, we argue that is in insufficient to rely on organizational incident response teams or even trusted coordinating response teams. Instead, there is need to develop a framework that allows an effective collaborative response and investigation process that include multiple organization and legal entities to track the adversary, eliminate the threat and pursue prosecution of the perpetrators. To that end we develop a system model and prototype implementation that would provide the ability to execute this collaborative process led by an Independent Center for Incident Management (ICIM). The system model defines an appropriate set of roles and responsibilities as well as the process undertaken by the collaboration. We describe a workspace environment supported by ICIMs and define a security architecture for the environment that leverages the roles in the system model for role based access control. We then describe a prototype implementation of the workspace environment, called the Palantir system, that provides a collaboration access to necessary tools and resources for undertaking the response and investigation while enforcing the security requirements. In addition, we define a workspace template for incident workspaces that supports our system model for roles, responsibilities and processes.

Several directions of future work can greatly benefit the proposed system model and prototype. First, the RBAC model can be enriched with the addition of role hierarchies, delegations and constraints that provide fine-grained access control and advanced policies such as separation-of-duty. Enforcement of constraints will require a reference monitor in the workspace environment, which can be designed by adapting techniques for RBAC in collaborative settings [2]. Second, while the process model does not lend itself to well-defined workflows there exist several tasks that can be combined into workflows for efficiency and correctness; e.g., uploading and analyzing logs. Such workflows can be supported by developing the concept of *wizards* in the workspace environment that allow users to combine tasks into workflows. Third, the usability aspects of the workspace environment can be significantly improved by undertaking usability studies and interface enhancements. Based on comments from early adopters, we are exploring the possibility of supporting command-line and thick-client interfaces to the workspace, using CyberIntegrator [4] to capture data provenance and manage workflows. Fourth, further evaluation of the system in handling real large-scale incidents will help provide useful enhancements and validation.

12. ACKNOWLEDGMENTS

We would like to thank the members of the NCSA Incident Response team, whose efforts in Incident 216 and subsequent discussions led to our understanding of these challenges. Members of that team at the time of Incident 216 included Jim Barlow, Tim Brooks, Aashish Sharma and Jeff Rosendale.

This work was funded by the Office of Naval Research under award number N00014-06-1-1108. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research or the United States Government.

13. REFERENCES

[1] Cyber Storm Exercise Report. National Cyber Security Division, U.S. Department of Homeland Security, September, 2006, 2006.

[2] T. Ahmed and A. R. Tripathi. Specification and verification of security requirements in a programming model for decentralized cscw systems. *ACM Trans. Inf. Syst. Secur.*, 10(2):7, 2007.

[3] C. Alberts, A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek. Defining Incident Management Processes for CSIRTs: A Work in Progress. Technical Report CMU/SEI-2004-TR-015, Software Engineering Institute, Carnegie Mellon University, 2004.

[4] P. Bajcsy, R. Kooper, L. Marini, B. Minsker, and J. Myers. CyberIntegrator: A Meta-Workflow System Designed for Solving Complex Scientific Problems using Heterogeneous Tools. In *Proceedings of the Geoinformatics Conference*, May 2006.

[5] V. Baryamureeba and F. Tushabe. The Enhanced Digital Investigation Process Model. *Process Model Asian Journal of Information Technology*, 2006.

[6] N. Beebe and J. G. Clark. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2):147–167, 2005.

[7] R. Bobba, J. Muggli, M. Pant, J. Basney, and H. Khurana. Usable secure mailing lists with untrusted servers. In *Symposium on Identity and Trust on the Internet (IDtrust)*, 2009.

[8] M. J. W. Brown, D. Stikvoort, K. P. Kossakowski, K. P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek. Handbook for Computer Security Incident Response Teams (CSIRTs). CMU/SEI-2003-HB-002, April, 2003, 2003.

[9] N. Brownlee and E. Guttman. Expectations for Computer Security Incident Response. IETF RFC 2350, June 1998.

[10] Y. D. Cai, D. Clutter, G. Pape, J. Han, M. Welge, and L. Auvil. Maids: mining alarming incidents from data streams. In *SIGMOD '04: Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, pages 919–920, New York, NY, USA, 2004. ACM Press.

[11] B. Carrier and E. H. Spafford. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), Fall 2003.

[12] B. Carrier and E. H. Spafford. An Event-Based Digital Forensic Investigation Framework. In *DFWRS'04: Proceedings of the 4th Digital Forensics Research Workshop*, 2004.

[13] S. Ó. Ciardhuáin. An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, 3(1), Summer 2004.

[14] P. T. Devanbu and S. Stubblebine. Software engineering for security: a roadmap. In *ICSE '00: Proceedings of the Conference on The Future of Software Engineering*, pages 227–239, New York, NY, USA, 2000. ACM Press.

[15] B. Fraser. Site Security Handbook. IETF RFC 2196, Sept. 1997.

[16] J. Giordano and C. Maciag. Cyber Forensics: A Military Operations Perspective. *International Journal*

of Digital Evidence, 1(2), Summer 2002.

[17] T. Grance, K. Kent, and B. Kim. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800-61*, January 2004.

[18] R. S. C. Ieong. FORZA - Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3(Supplement-1):29–36, 2006.

[19] H. Khurana, J. Heo, and M. Pant. From proxy encryption primitives to a deployable secure-mailing-list solution. In *ICICS'06: International Conference on Information and Communications Security*, pages 260–281, 2006.

[20] H. Khurana, A. J. Slagell, and R. Bonilla. SELS: a secure e-mail list service. In *ACM Symposium on Applied Computing (SAC), Security Track*, pages 306–313, 2005.

[21] G. Killcrece, K.-P. Kossakowsk, R. Ruefle, and M. Zajicek. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Technical Report Report: CMU/SEI-2003-HB-001, Carnegie Melon University/Software Engineering Institute, 2003.

[22] K. Leune and S. Tesink. Designing and developing an Application for Incident Response Teams. In *FIRST'06: Forum for Incident Response Teams Conference*, Baltimore, MD, USA, June 2006.

[23] S. Mitropoulos, D. Patsos, and C. Douligeris. On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, 25(5):351–370, July 2006.

[24] G. Palmer. A Road Map for Digital Forensic Research. Technical Report Technical Report DTR-T001-01, Report From the First Digital Forensic Research Workshop (DFRWS), 2001.

[25] M. Pollitt. Computer Forensics: an Approach to Evidence in Cyberspace. In *Proceedings of the National Information Systems Security Conference*, volume 2, pages 487–491, 1995.

[26] M. M. Pollitt. An Ad Hoc Review of Digital Forensic Models. In *SADFE '07: Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, pages 43–54, Washington, DC, USA, 2007.

[27] C. Prosise, K. Mandia, and M. Pepe. *Incident Response and Computer Forensics, Second Edition*. McGraw-Hill Osborne Media, 2003.

[28] M. Reith, C. Carr, and G. Gunsch. An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3), Fall 2002.

[29] R. L. Rollason-Reese. Incident handling: an orderly response to unexpected events. In *SIGUCCS '03: Proceedings of the 31st annual ACM SIGUCCS conference on User services*, pages 97–102. ACM Press, 2003.

[30] R. Rowlingson. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2(3), Winter 2004.

[31] G. Ruibin, C. Kai, Y. Tony, and M. Gaertner. Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. *International Journal of Digital Evidence*, 4(1), Spring 2005.

[32] S. Schechter, J. Jung, W. Stockwell, and C. McLain. Inoculating SSH Against Address Harvesting. In *NDSS'06: The 13th Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2006.

[33] A. Slagell, K. Lakkaraju, and K. Luo. FLAIM: A Multi-level Anonymization Framework for Computer and Network Logs. In *LISA'06: 20th USENIX Large Installation System Administration Conference*, Washington, D.C., Dec. 2006.

[34] P. Stephenson. Modeling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence*, 2(2), Fall 2003.

[35] J. Vincent, R. Spier, D. Rolsky, D. Chamberlain, and R. Foley. *RT Essentials*. O'Reilly Media, Aug. 2005.

[36] X. Yin, W. Yurcik, and A. Slagell. VisFlowCluster-IP: Connectivity-Based Visual Clustering of Network Hosts. In *21st IFIP TC-11 International Information Security Conference (SEC '06)*, May 2006.