UCSF IT SECURITY – APPLICATION FOR SAUTTER AWARD – 2020

UNIFIED SECURITY ARCHITECTURE FOR THREAT DETECTION AND RESPONSE

5/28/2020

OVERVIEW

1. Introduction and Problem Statement:

Higher education, health care, and clinical research computing environments are some of the most challenging environments to protect in the face of a constant cyber security threat. The environments have challenges and the threats have shown to be very real and in the top tier of the global-threat landscape. The threats include patient data, financial fraud, personally identifiable data, ransomware, cutting-edge research, and the infrastructure itself as a launching point for further attacks to name a few. The attackers are motivated by lucrative monetization through exploiting organizations. The Verizon 2020 Data Breach and Incident Response Report stating that the attacker motives for healthcare were 88% financial, and for education, 92% of the attacker's motivation was financial. This includes Nation State actors (also known as Advance Persistent Threats) which seek to advance their national interests by profiling our approach towards healthcare and to harvest UCSF's cutting-edge research.

That is counter played with missions that rely on openness, collaboration, rapid access to information and the ability to interact with other organizations for the research, clinical care and educational missions. Containing costs, ensuring high productivity and autonomy while protecting the data and environment are also key goals. The attackers target the very tools that are key to our organizations missions; email, web servers, personal systems, our personal communications, our social media, our publicly available data as well as compromised data from other breaches.

The challenge is that historically cyber security threat detection and response activities have been disruptive, ad hoc and costly to execute in a distributed environment. Additionally, the speed with which an attacker can be detected, and how fast we can respond to is a key capability to reduce the impact of security issues. That has been the focus for UCSF IT Security and our efforts to unify security architectures and integration threat detection solutions.

Goals:

- Support UCSF's mission by protecting the whole environment
- Ensure minimum necessary impact to users, patients, and students
- Implement and operate modern technology to detect and respond to threats across the environment
- Ensure a cost-effective approach to leverage scale for value
- Reduce the mean time to detect and respond
- Implement a continuous improvement approach

Project Team: Toby Barber (Sautter Award submitter), Raymond Tam, Nicholas Urrea, Robert Tannenbaum, Sarah Mays, Christian Sisenstein, Kristan Beynon, Bryce Leong, Bassem Haidar, and Kevin Simmons.

2. Project Scope and Description

The scope of the project has included re-architecting and implementing a number of technologies for intrusion detection, response and security services. There are also aspects of automation, metrics, system integrations, team reorganization, training and driving strategy for IT security maturity in support of the threat detection and response functions.

Intrusion Detection and Packet Brokers

The journey started with modernization of UCSF’s intrusion detection systems as well as looking at what network artifacts were generated for network security monitoring and investigations when responding to alerts. This project resulted in a design which leverages packet broker technology to provide a number of capabilities and enable services in an academic healthcare research environment.

Packet broker technology allows for monitoring and routing network traffic into security tools in a way that serves seamless routing and failover. This prevents historical issues by adding security tools into the path of network traffic for the Internet and data centers. Additionally, the packet brokers are installed within the network allowing for visibility beyond the border and provide the ability to have internal intrusion detection.

The technology has allowed for a cost-effective approach as well because they allow traffic to be shuttled between locations and to aggregate and balance traffic, meaning security tools could “scale up” vs. “scale horizontally” which allowed us to leverage scale for value. One example is rather than putting in many appliances at points on the network, we were able to shuttle traffic to a single location and purchase a large device or devices at the optimum price point for the solution. This also reduced support cost and complexity.

With this key architectural component, we implemented systems to perform intrusion detection including threat intelligence of software, URLs, IPs, traffic patterns, and other behaviors which are constantly updated by the vendor’s sensors worldwide. The technology also includes malware sandboxing which allows for synthetic execution of the malware in a virtual machine to determine what the malware will do if executed, what other software it may install, what remote locations it may communicate to and how it interacts with the system or leverages the system to attack other systems.

Network Forensic Artifact Generation

In addition to these intrusion detection systems, other components were installed that gather and keep network artifacts which add more detailed context around the alert. The detail includes network communications and profiles communication patterns to build context and reliability around what the threat was doing or attempting to do. This allows for a much more informed approach to investigation and adds context which isn’t available with an intrusion detection system alone and allows that data to be kept for a lengthy period of time in the event of evasion of controls and detections is discovered later.

Email Integration and Automation

Email is one of the most leveraged attack vectors for malicious compromise of systems and networks today. While the historical approach was to punch through the edge of a network attackers have learned that sending a well-crafted email to “phish” someone and is much easier. This can be done leveraging public information since we are a university and then made even more believable by other publicly available information, this is called Open Source Intelligence, or abbreviated as OSINT.

These emails have a number of ways to accomplish their mission. This includes sending links to direct someone to a site that may look like an official website, a link that leads to automatic download of additional malware which then runs on the local system with the user’s privileges. They may also send an attachment that leverages these capabilities or an attachment that is malicious and can compromise the system when the user interacts with the file.

While this all sounds commonplace today, there are other aspects that are more advanced and require advanced solutions. Creating unique attack patterns or using recently compromised systems on the Internet can allow for an attacker to go undetected because an email, the system accessing the email, and the network path to the additional malware or command and control system have historically been separate.

This is an opportunity for unification of capabilities. This integration of email allows us to see any communication made from the system on our network, then any subsequent information or files downloaded are further examined and this process goes back and forth until the attack shows their hand and is detected. This can also happen retroactively meaning an attack can be detected elsewhere in our userbase and/or a network or at another company entirely and we will receive alerts that say, "go back and find out what happened". In a subsequent piece of our project we implemented endpoint detection which adds additional integration.

With this unification also came an opportunity for automation. When a threat is known to not have been interacted with by a user, the best course of action is to prevent the threat from being available to interact with later. We do this via automation whereby the validated threat is automatically removed from the access of the user and if they do happen to have interacted with it, we will be notified and have record of that to perform a remote investigation and only contact and interrupt the user if the threat was indeed shown to have had a risk. This has reduced user interruption dramatically and doesn't require subject matter expert staff to remediate and also avoids further escalation of compromise by remediating the threat rapidly.

Endpoint Integration

In addition to the network pieces, the security monitoring services, and email pieces we have implemented an endpoint agent which allows all of these pieces to be tied together at the key target of an attacker, the endpoint. This can be a desktop, laptop, server, on our network or off our network and allow for alerting and correlation of attacks. An example of this would be when one person was attacked first by email or a web download or executing a malicious file, etc. and as the system interacts with the network and Internet hosts, that attack information can be confirmed on the system. If malware changed a file or access configurations or abused a normal program like a word processor to interact with the Internet, then this is confirmed by correlating network behavior and threat intelligence which what actually happened on the host.

Additionally, this allows for our incident response team to act on other alerts from other detection system and to do an investigation or interact with the system remotely to verify what did or didn't happen. This is a big shift from investigations previously and this is where the user benefit and cost benefit come into play. This is a key aspect to looking for threats that may have come about when a system was not on the network or an attack evaded a network control.

Remote Investigation and Minimal User Disruption Value

All of these pieces are tied together with the services of 24x7x365 monitoring and also with many new remote investigation capabilities. We used to go out and take a user's machine for investigation, hopefully have a loaner for them, maybe disable accounts, remove access to their email or access to documents, all of which was very disruptive and costly. The same goes for IT Security leveraging IT support resources and departmental resources all while delaying remediation of the threat which can result in further compromise and potentially an even bigger incident.

Continuous Improvement

The team also embarked on a long journey to train and improve skills to use the new tools, learn about new threats, execute investigations with many points of data and validation of system behavior vs. personal interpretations and ad hoc decision making.

In addition to those improvements, the teams focused on processes and procedures as well as governance. The teams re-organized to better integrate the engineering functions and perform cross training while sharing information. We've also taken advantage of testing the tools under controlled situations where penetration testers executed attacks in the environment to demonstrate third-party validation of detection tools, services, and the staff's ability to rapidly respond and investigate.

We now regularly report progress to leadership and across governance groups. The teams regularly interact with departmental IT staff and we have a roadmap whereby the centralization of security monitoring is being executed without disrupting the important departmental IT functions.

Lastly, this is ongoing effort and we are following our roadmap to keep improving with the focus of supporting the mission, the patients, the staff and the researchers that make UCSF so amazing!

3. Timeline

- 2016-2019 – Packet Brokers, Intrusion Detection, Internal Intrusion Detection, Security Services and Network Forensic Artifact Generation
- 2017-2019 – Email Protection and Automation
- 2017-2020 (still expanding) – Endpoint Deployment and Integration
- 2018 – Team re-structuring, Expansion and Governance Formalization

4. Outcomes and Impact

- The reduction of impact on the users is dramatic
- Cost avoidance and savings through thoughtful use of technology and architecture
- Measurable return of productivity for users, IT support staff and IT Security
- Efficacy of our investigations mean that we act with purpose
- Large reduction network tickets which didn't have endpoint impact
- Significantly modernized our capabilities
- Partnership with the departments and IT teams who count on IT Security as a partner
- Leadership communication and visibility into threats
- Detection and response speed