A Security Analysis of Police Computer Systems

Benjamin VanderSloot* Stuart Wheaton* J. Alex Halderman
University of Michigan
{benvds, stuartw, jhalderm}@umich.edu

***Abstract*—Every day we entrust our privacy, safety, and security to police officers sworn to protect and serve. While many critical infrastructure computer systems have been well studied, the computer infrastructure supporting these officers remains to be surveyed in public literature. We remedy this by characterizing a sample police department's systems through a security lens, discussing weak points and areas for future work. Pen-testing of the security camera and web application systems were performed to give hard data points on the security of this department's systems. Our characterization shows that the security of the department we study is good overall, but enough weaknesses exist in this department and others to be concerned for the state of police security. We determine that compliance with FBI security policies is an appropriate first step for departments, but it is not sufficient. More research and increased support for security education and resource services is needed in order to defend these critical systems against adapting adversaries.**

1. Introduction

Since the rise of the Internet and "cyberwarfare," security researchers and the government have become increasingly interested in answering the question: "How can we secure our critical infrastructure?" Of course, military systems in the U.S. are wellsecured, given their massive budget. On the contrary, it is generally recognized that non-military systems controlling things like banks, power grids, and nuclear reactors could be easily targeted by terrorists or statesponsored hackers to cause real harm to citizens. As such, there has been an immense research effort focused on securing these types of critical infrastructure systems.

However, there is a noticeable void in the research literature when it comes to one of the most critical societal functions that we all rely on: police. Police departments are entrusted with securing sensitive data and coordinating actions among officers charged with protecting the public. There are many systems in place to do so, and they are largely uncharacterized in the literature. Therefore, we do not know the security dangers they pose to the privacy and safety of the citizens they are designed to protect and serve.

When studying the security of a system, it is neccessary to consider the threat model of who the attackers may be. Throughout our analysis, we consider a broad range of attackers, including web, network, social engineering, and advanced persistent threat. Analysis does not include any insider attacks, or any uncontrolled physical access to the devices owned by the department.

In designing for security, there is often a tension between availability and authorization: data should be available to authorized parties at all times, but should never be accessible by those that are unauthorized. Police systems are no exception. The consequences of losing security properties are magnified in this case, since we entrust officers with our lives every day.

2. Related Work

The study of systems that risk the safety of the general population when compromised is an existing, dense field of work. This context is where we draw from, in order to understand the dynamics of availability and consequences of vulnerability. Among the critical systems that are well studied is Supervisory Control and Data Acquisition, or SCADA devices. These devices, which often control physical infrastructure like power plants or industrial equipment, have been shown in the research literature to be particularly insecure. They were identified to have issues as early as 2006 [12], and have continued to be studied to encompass different systems and more advanced adversaries [15].

A famous prior work on police systems was the study "Why (Special Agent) Johnny (Still) Can't Encrypt" [5]. This study is an in-depth security analysis of a single radio system that features encryption. Not only were there no radios capable of encryption owned by the department we cooperated with, but our work differs in that we lay out all systems within the department at a much higher level. Similarly, Dameff et al. [6] investigated security aspects of 911 call systems, specifically the location-identifying

*These authors contributed equally to this work.

services. While depth is necessary in future work, we feel that a broad analysis is needed to better understand what systems are most in need of the in-depth analysis.

One aspect of public infrastructure that has been studied in a similar vein to our work is that of traffic signals. Cooperation with officials from a road agency led to a thorough study of a system that had not previously been studied by security researchers. Traffic lights, while a much lower target, proved to be very vulnerable to attack [10].

In order to demonstrate potential attacks on police systems, the full scope of the systems must be understood, characterized, and analyzed. Unfortunately, due to policies adopted by the police and software companies, this information is not easy to come by. Our research goal is to help make the security community more aware of the trust that is placed in these systems, and where there may be potential weaknesses.

3. Political and Structural Landscape

While it was once possible to operate a police department as an technological island, isolated from the rest of the world, this is no longer the case. Since there is the ability to connect all criminal justice organizations to each other in order to share information regarding investigations, it is considered irresponsible by professionals in the field to not take advantage of this resource. The United States Department of Justice, Federal Bureau of Investigation (FBI) formed the Criminal Justice Information Services (CJIS) Division in 1992 in order to facilitate this sharing of information, and is now the largest department of the FBI. Since 2001, information sharing has ramped up to bolster terrorism prevention efforts. In order to participate in any of their systems and have access to any databases like the National Data Exchange, a department must adhere to their security policy [17].

3.1. CJIS Security Policy

The CJIS security policy document outlines steps departments must take to secure their Criminal Justice Information (CJI). This includes criminal records, incident history, and property data, among other things. This security policy is the baseline expectation for any department. States may have security policies of their own, but they are rarely more restrictive than the CJIS document.

The policy goes into great detail about many security requirements, from the principle of least privilege to the proper destruction of physical devices. It is at CJIS's discretion when to require two-factor authentication, and for what systems. There are some restrictions on password use, but they are surprisingly weak: passwords must be at least eight characters long and not be a proper name, dictionary word, or the user id. Also of note is the definition of a Physically Secure Location, which offers very little detail; access control can be achieved through a list of all authorized personnel or credentials issued to those personnel. Private contractors are permitted to work with CJI under this policy, given they pass a fingerprinted background check, as we did to be able to perform this study.

Despite being very explicit in its definitions and covering a very wide scope, it is apparent that the policy is insufficient if taken at face value, due to its mostly non-technical nature. The policy lands is not so brief as to be quickly and easily understood, but at the same time not detailed and specific enough to include critical implementation details for some of the requirements.

The security policy is enforced through random FBI technical security audits of departments. This is critical as it ensures departments do, in fact, follow the policy, and that they implement sound security practices. Audits do not occur frequently, however, since only a handful of departments in each state are selected every few years. So while the audits are good for making sure departments are trying to comply, it does not ensure much, nor do much to help departments that may use bad practices not expressly forbidden in the policy. Annual state police audits are performed, but these are mostly non-technical, focusing on policies and personnel.

3.2. Cloud Services

The expansion of third-party applications and cloud services is a recent phenomenon that many police departments want to take advantage of in order to better perform their duties. Companies are touting customized police mobile apps, government-targeted cloud storage, and application-specific services storing data off site like evidence collection and computer aided dispatch. In a recent study [18] by the International Association of Chiefs of Police, 54% of responding departments said they were already using cloud services or considering adoption within 2 years. In addition, 61% stated saving money as a reason for the change, and 52% said "no more software". Clearly, cloud services are convenient and low-cost, but they raise many security concerns for police departments which need to store such sensitive data.

It can be difficult to determine if providers meet the criteria for safely handling CJI. The CJIS Security Policy contains a white paper (appendix G.3) on the use of cloud

services to store and access CJI; the conclusions were that the use of cloud services is acceptable, as long as the department can guarantee CJIS compliance through their usage contract. However, the recommendations rely on technical competence and due diligence on the part of the department. For example, the department must "understand the underlying technologies that the cloud provider uses to provision services", "understand virtualization and other logical isolation techniques that the cloud provider employs", and "fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment." While certainly important, these are tall tasks for departments to take on, and it would be easy for an underfunded or undereducated department to gloss over the details.

3.3. Resources

Along with the guidance the CJIS Security Policy provides, departments have access to many resources for help in securing their systems. Organizations like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the International Association of Chiefs of Police (IACP) provide members with security guides and advisories, among other things. State-sponsored centers like the Michigan Cyber Initiative and the Florida Center for Cybersecurity offer similar services and training. Local organizations like the Metropolitan Washington Council of Governments also exist which have security subgroups designed for the purpose of sharing information.

While departments may have access to these outside resources, the capital resources required to implement security practices are often stretched thin. One county Chief Information Security Officer estimates a standard IT budget allows only 6% to be devoted to security [8]. There has been an encouraging push recently by legislators and the public calling for improved security policies and practices, but this must continue in order to provide departments with continued support through all of these valuable resources.

4. Case Study System Architecture

In order to understand the attack surface area of a department as a whole, we worked closely with the Chief Technology Officer of a police department. This close work included regular and, we believe, honest communication about all systems under his control.

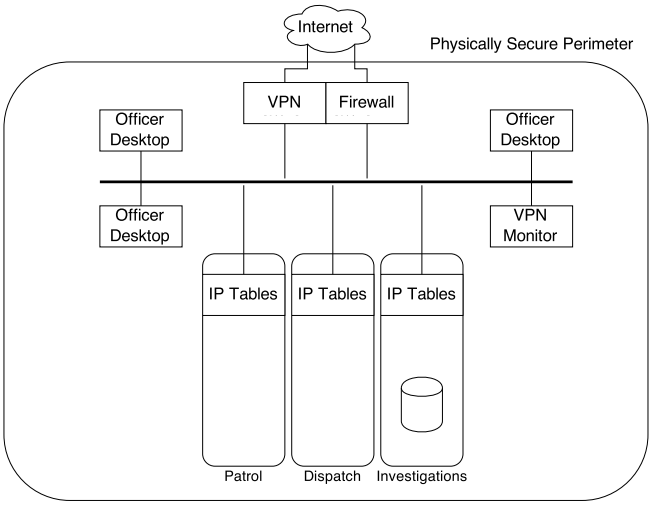

Figure 1: **Local Area Network.** A diagram describing the network in the department studied. There are three major subnets protected from the rest of the network, containing systems related to patrol, dispatch, and active investigations. Many officer desktops are outside of these subnets, but have access through firewalls.

4.1. LAN

The need for everyone to have a computer to perform their job requires the presence of a Local Area Network (LAN) within the department's headquarters. Within this LAN there are a variety of subnets used to control access within the network's address space. The separations into subnets fall along logical boundaries pertaining to what information is accessible on that subnet. The three subnets are: patrol, dispatch, and criminal investigation. Figure 1 shows a representation of the LAN layout. The networks are all only accessible through iptables-based firewalls, one per subnet. Inbound and outbound traffic is filtered by port number and IP. In this way, access is controlled within the network.

A few generic desktop computers with no special privileges exist within the network, but not behind any of the three subnet firewalls. These belong to general staff and have no access beyond the web tools in Section 4.6 and typical organization applications like a mail server and an active directory. Other desktops within the LAN are placed in subnets based on the officer's job role. For example, a detective's computer is going to be in the criminal investigation subnet and a dispatch personnel's computer will be in the dispatch subnet.

There are two externally facing elements of the LAN at the department. The first is the firewall, an annually-

updated commercial Cisco device with intrusion detection to restrict access. This is how general Internet devices reach the servers within the department's LAN. Our contact informed us that this device falsifies its signature in order to pass audits designed to confirm that they comply to the state police department's requirements. This is because it has an insecure configuration out of the box, a requirement stricter than those in the CJIS policy. The current configuration of the router passes CJIS requirements.

The other externally-facing device is a Cisco ASA VPN, using IPSec encryption. Field offices have corresponding VPN hardware to enable printing, communication of sensitive data, and for it to be as if the field office were a part of the department LAN. Devices on the VPN are registered and can be monitored from any computer in the LAN. Unfortunately, there are many false positives; when we saw the list there were multiple devices with "Critical" or "Major" errors. VPN hardware onsite has Ethernet input ports not in use physically disabled as per policy, to prevent physical access concerns.

Our primary concern for the LAN is the poor control over the VPN. Since there are physical VPN boxes in field offices, it is hard to ensure that there are no rogue devices plugged in or that connections aren't being interfered with by a man-in-the-middle attacker. However, the impact of this is minimized by the layers of firewalls and subnets.

4.2. Record Management

Record management is a centralized system, in which departments must communicate to some upstream regional department. From within the local department, communication to the regional department is done over a trusted T1 line: a dedicated physical connection between two points. All communication regarding record management is also done over SSL. In addition to this, the router that drives communications over this T1 line is the property of the regional department, and is therefore only updated by the that regional department.

Officers may access records in one of two ways: either the officer radios back to dispatch, which has a client that can communicate over the T1 line, or the officer uses their computer (the laptop in their squad car). This computer has a VPN connection to the regional department, communicating over a cellular network. It is more common for a technologically-averse officer to call in over radio to dispatch in order to get information. Figure 2 shows a representation of the record management system.

The laptops in the squad cars are the property of the regional department, which slows updates to software, and

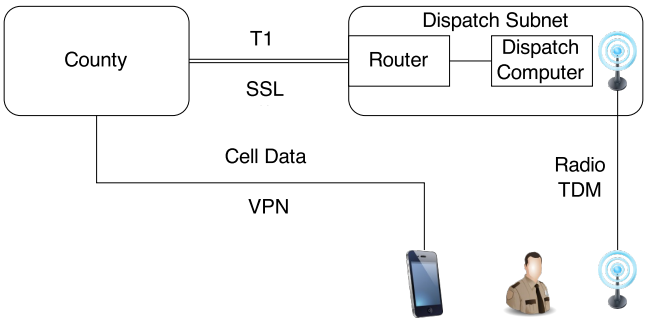

Figure 2: **Criminal Record Access.** There are two means the department uses to acquire records from the FBI CJIS database. First, officers can contact the county office directly through a VPN over cellular data. Second, officers can call dispatch at their own department, who connect to county over TLS on a dedicated T1 line.

restricted our access for testing purposes. In the case of the officers that radio in to dispatch, the computers that dispatch uses to communicate with the regional department are not property of the regional department, just the client software. The local department must blindly trust the security of this consolidated regional system in order to gain a bit of additional information sharing capability. This can be good for incompetent departments who are unable to deal with many security concerns, but it degrades the ability of knowledgeable departments to secure their entire process and creates an access point bottleneck which would cause wider issues if disrupted.

Concerns related to record management surround the upstream service answering requests for records and how much trust is placed on the T1 line. The SSL that is in place to protect traffic on the line is a second line of defense. The physical distance the routers are from the regional department and number of routers the regional department must maintain raises concerns about how strong the SSL configurations and implementations are. This is founded in the known difficulty of securing non-browser SSL [9]. We could not test this without the cooperation of the regional department, since all relevant parts are the property of the regional department. We suspect that a compromise of the T1 line would mean a compromise of communication between the department we studied and the regional department.

4.3. Security Cameras

Security cameras, in general, have been known to be fairly prone to security vulnerabilities. In an attempt to mitigate this concern, the department we investigated has

their cameras connected via Ethernet directly into switches in locked telecom closets at the location. These switches are on a VLAN that communicates back to computers controlled by the department but not inside of the departmental LAN, via an untrusted network. They are programmed to report to a central directory server, which has a static IP address but no domain name. This directory tells the camera the IP address of an archive server to send video stream data to.

In order to access this data, a domain name that is easily derivable from the main domain name (video.department.domain), is opened in a browser and authenticated to. It is worth noting that this web interface is left open outside of the department LAN. A mobile app that uses HTTP to obtain the video feeds was created but never deployed. If it had, the access of security camera streams over an unencrypted channel would be a big security concern.

An attacker may be able to access the locked telecom closet, given the lack of security associated with many lock-and-key systems [3] like ones deployed at the buildings where the cameras are placed. Defining what attacks are possible once this closet is physically compromised is a subject for future research. Many commercial video camera devices come with default passwords and do not immediately prompt for a password change, leaving non-security conscious users extremely vulnerable to attack. Security cameras that operate on a WiFi network are also vulnerable, as they can be brought offline with a deauthentication packet attack [19].

4.4. 911 Call Center

One of the most public-facing and important systems a police department needs is a system for receiving emergency calls to 911. Calls come in and are immediately processed by embedded devices that extract metadata about the call and forward this metadata and the call connection on. These cards are within the LAN of the department and communicate over telnet to the computers at the desks of the 911 dispatchers. The computers ring the phones at the desks and the dispatchers answer calls and perform normal dispatch duties.

Numerous attacks on the 911 call center are possible. When a 911 call is made, it is routed to the nearest Public Safety Answering Point (PSAP). There have been reports of denial-of-service attempts to PSAPs through a worm that used the computer's modem to dial 911 [7], a malicious email attachment that reprogrammed users of Microsoft WebTV's computers to dial 911 instead of a local Internet access number [16], and repeated calls to a single PSAP after compromising a telephone network [1]. Dameff et al. also show that 911 location services can be compromised or fooled to send police to a location of the attacker's choice and that the secret PSAP numbers can be learned by listening to recorded 911 calls [6].

4.5. Dispatch

The most critical piece of the dispatch system is the CentraComm radio system that is common to all police stations in the state of our department of study. The radios communicate over 800MHz channels, using Time Division Multiplexing (TDM) voice packets. The network is aware of radios in the state tuned into the department's channel, and will broadcast the communication only to where the radios are tuned in. In order to be able to talk on a channel in the state radio system, the radio must be authorized by the department, but listening to a channel is possible with any radio. Any rogue radio may be blacklisted from the network.

Also critical to the dispatch system is the terminals the dispatchers see. These are 5250 terminal emulators that connect to an IBM AS400 mini-mainframe within the LAN of the department. This mini-mainframe is in the dispatch subnet, and it periodically dumps data to a MySQL database on a separate server to make data querying easier.

A lack of redundant defense is concerning in this case. Any attacker in the system could tamper with the dispatch terminals because they are functioning in the clear over the LAN. Dispatch is critical to the operation of the department, and could constitute a major target for an attacker looking to delay emergency response.

4.6. Web Services

The department hosts an online portal for a collaboration tool that stores daily operation information (non-CJI). Employees log in to a single sign-on application with typical password credentials and a two-factor authentication token to access this and other portals. The application is hosted on an Infrastructure as a Service (IaaS) cloud platform, meaning a cloud server is provided, but nothing else. This platform still leaves departments somewhat on their own to build and secure their application stack, which is worrisome given the current push for CJI to be moved into the cloud; they might be lulled into a false sense of security because they do not own the server.

As with most organizations today, police departments also run a public-facing website. These can be extensions of city websites and are largely static, barring the existence of an employee login system and associated applications. These

sites contain sanitized police reports, contact information, and other public safety-related messages that need to be conveyed to the general public. This department took advantage of a Platform as a Service (PaaS) offered by a cloud provider, which allows easy development and management of web applications without the maintenance of the server infrastructure as in the IaaS model. Some of these services are very secure, as they are offered by large, security-conscious organizations. Other departments may use less reputable providers or host sites on a homegrown server. Alas, the risk involved is low, as website defacement is a smaller concern in relation to the protection of CJI.

4.7. SCADA

This department is in control of SCADA systems for fire alarms in some area buildings. These devices, called Fire Alarm Control Panels (FACP), are mounted on the walls of the facilities they protect and are connected in a circuit, in order to signal to the department headquarters if one of the sensors (pull levers on the wall) is triggered. This communication occurs over 800mHz radio to another Remote Terminal Unit (RTU) SCADA way station. It is estimated by our contact that these would be difficult to jam, with the logic that the 100W power output from the system would be hard to overcome with a stealthy device.

Once signaled, the RTU communicates to a server through a hard line (crossover ethernet wire) to connect back to a web client running on a firewall-protected department machine using SSL. Instead of plugging in a hard line, departments sometimes use a commercial IP gateway product that provides online switching between servers for auto-backup functionality. This setup can be prone to denial-of-service attacks, however, as was discovered by our contact when a simple port scan of the gateway server was performed, and it immediately crashed. This is a clear example of the tension between security and availability in the public safety world.

4.8. Police Officers

The department requires, per the CJIS Security Policy, that all staff watch a training presentation regarding security practices. Despite this, security knowledge of the officers at the department should be called into question. An anecdote that emphasizes this is about a strange email and attachment that was forwarded onto officers by a concerned citizen. The officer investigated the attachment by opening it on his work computer within the LAN. Fortunately, there were multiple such emails reported to the department, so IT was able to discover and root out the issue. Proper action would have been for the officer to send the document to the computer forensic unit, in order to be studied in a separate network.

There was also a recent case of a prisoner who created an email account to pose as a court clerk member, and sent bail instructions to the prison staff [14]. The prisoner was released and only brought back in days later when he turned himself in. These anecdotes point to a hole in the defenses that technology can't completely fill: the officers themselves. History has shown that people in general are ignorant of sound security practices [20] [11], but those with access to sensitive data like police officers must be held to a higher standard of constant vigilance. The best way to permanently instill good security practices in non-technical individuals remains an open question.

Spearphishing attacks are a major concern regarding the security of police departments. Even anecdotal evidence of an officer opening an attachment on an email flagged to them in advance as suspicious shows a lack of security awareness. Given the prevalence of spearphishing as the first intrusion in corporate espionage [4] and its low cost and technical requirement, this attack vector is an important one for police departments to consider and defend against.

4.9. CJIS Systems

There are a handful of other small systems that are very specialized in their functionality. One of these systems is Picturelink in which mugshots are circulated between departments. Another such system is the fingerprint service. This is accessed by one device in the department that is used to take fingerprints of arrested individuals and prospective employees. The device scans fingerprints digitally and transmits them out of the LAN and to the state centralized service. The fingerprint machine is inside of a controlled holding area, with a waiting bench for the people to be printed, and taking fingerprints is a long and relatively delicate process.

These systems are within the criminal investigation subnet. Due to the strictness of the CJIS Security Policy, only this subnet qualifies for communication with the FBI. This increases the amount of trust that is put on these systems, but they are relatively controlled.

5. Theoretical Attacks

In order to demonstrate how some of our concerns could be strung together into exploits, we have put together some attack descriptions on paper for consideration. These attacks have not been carried out, but have been presented to the

CTO at the department we worked with in order to fix the underlying issues.

We were permitted to scan and check any public facing system for vulnerabilities. However, we were not allowed access to any machines within the department's LAN, VLAN, VPN, or the systems outside of his control. Doing so would violate CJIS standards, and our contact insisted on maintaining strict adherence to the CJIS Security Policy.

5.1. Security Cameras

This attack hinges on simply man-in-the-middling the connection to a mobile security camera viewing client. This can be performed in any number of ways: spoofing a mobile carrier, hosting a wireless network that the officer may connect to [13], compromising a router, or owning a malicious upstream connection. Since the login to the web interface is done over HTTP, without SSL, an attacker can simply steal login information and view the video streams at any point, compromising privacy. Further, since the officer is being man-in-the-middled, any stream can be replaced with a video of the attacker's choosing: possibly one showing no interesting activity. This mobile app has not been deployed for the reasons above, but a department with less security knowledge may not realize the pitfalls of having mobile apps like this when making decisions to leverage popular technologies for convenience.

5.2. Criminal Justice Information

The department uses a collaboration tool to store daily operation information (non-CJI). This application is hosted on an Infrastructure as a Service (IaaS) cloud platform.

When a TLS connection is made to the login page, the server accepts anonymous cipher suites, which provide no server authentication to the user. This allows a man-in-the-middle attacker to impersonate the site and steal login credentials. An internal wiki web service running on the server was out of date, and had a known privilege escalation vulnerability. Any user could execute arbitrary Java code execution [2].

The current network setup leaves only uninteresting internal wiki data exposed to this attack, however, and this server is hosted in the cloud and not behind any firewalls. But the department is rapidly moving in the direction of pushing more and more CJI to the cloud servers. Had this security hole not been closed now, some of this department's CJI may have been exposed on a vulnerable server in the near future.

6. Conclusions

While IT is difficult in general, that difficulty is increased in the context of police systems. An issue that must be faced in the context of police systems is the concept of jurisdiction. Lines are set hard and fast for police IT on what they are responsible for and allowed to change.

Further, CJIS itself faces a very difficult challenge. In order to make data available to all police departments, CJIS must ensure that every department they give access to has the ability to properly defend their systems. This is a fundamental asymmetry that is seen throughout security: that the attacker needs only attack the weakest link to break the system. This is taken to a massive scale for CJIS, with the number of police departments they cover.

In order to mitigate this, CJIS forces compliance to their Security Policy. However, this policy is still vague enough that critical security vulnerabilities are possible in departments that follow the policy and its intent. Login credentials being unencrypted is a simple, yet not uncommon example of this that we found.

From the departmental perspective, there is a potential downside to using CJIS systems, beyond that of the increased surface area to defend. The increased value of compromising the department changes the scope of potential attackers and to what lengths those attackers may go to break their systems. Because sophisticated attacks on these systems are not known to exist in the wild, it is very difficult for a department to give up all CJIS information for hypothetical attacks.

From these issues we can draw some insight about the management of secure systems. Namely, that as the size of a secure system is increased, the difficulty in maintaining the security increases, more so than just the increase in attack area implies. The increased attack area is an obvious aspect of the increased risk, but what may be less obvious is that as a system increases in size it increases in scope, and as a result it becomes a more valuable target. The increased size also makes it so more people have to manage the system, making it easier for one of the people to make a mistake, or misunderstand the increasingly complex rules about who "owns" what parts of the system. Finally, a larger system has more users, making it more likely that one will behave in an insecure way, allowing system compromise. All of these factors compound on each other to make managing a secure system far more difficult as it grows.

We feel there is reason to be optimistic about the state of police system security. The police department we studied had sound defenses-in-depth overall, and a CTO knowledgeable in security practices and mindset. If every

department was similar to the one we studied, we would be well off in terms of security. The CJIS Security Policy can help to strengthen departmental security if its guidelines are followed, due to the broad coverage of topics from physical security to cloud storage. FBI audits can be beneficial to larger departments that get chosen. And finally, many security resources are made available to departments by various groups. The tools and policies needed for success are ready and available, as long as there exists an organizational motivation to improve.

It is unclear whether this motivation exists in most cases, leading to a cause for concern. Misconfiguration of TLS on city employee login servers and the reckless use of unencrypted police logins points to an underlying deficiency in knowledge or resources. While we only have concrete data from one department we worked with, it is of note that many other departments and police software companies shied away from our attempted security conversations. It is our opinion that security through obscurity is an unproductive cognitive model that should not be adopted when securing our nation's critical infrastructure. Even so, the CJIS policies do not go into enough technical detail for one to be fully confident in a department's black-box security systems if CJIS is their sole resource.

Certainly, more work is needed in this area to determine the state of security for police departments. Future work includes generalizing our system characterization and analysis to many departments, investigating the interactions between local, county, state, and federal police, and taking a more focused approach to particular software programs and systems. A non-technical analysis of the security climate amidst government entities would also be beneficial, as it might point to methods departments can use to gain more resources for securing their systems, or discover to what degree most departments actually are compliant with CJIS. Public safety, specifically police, is a piece of our critical infrastructure that is a large, slow target, but whose security measures has not been studied nearly enough by the public. We hope to have laid the baseline foundation for future work to build upon, thus contributing to the important conversation of how to secure our most important computer systems.

7. Acknowledgments

We would like to thank our departmental contact for the understanding and help given.

References

[1] G. Allen. Hacking the 911 system. http://www.911dispatch.com/911/history/hacking911.html.

[2] Atlassian. Confluence security advisory - 2015-01-21. https://confluence.atlassian.com/display/DOC/Confluence+Security+Advisory+-+2015-01-21, jan 2015.

[3] M. Blaze. Cryptology and physical security: Rights amplification in master-keyed mechanical locks. *IACR Cryptology ePrint Archive*, 2002:160, 2002.

[4] M. I. Center. APT1: Exposing one of chinas cyber espionage units. Technical report, Mandiant, 2013.

[5] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze. Why (special agent) Johnny (still) can't encrypt: A security analysis of the APCO Project 25 two-way radio system. In *USENIX Security Symposium*, 2011.

[6] C. Dameff, P. Hefley, and J. Tully. Hacking 911: Adventures in disruption, destruction, and death. In *DEFCON 22*, August 2014.

[7] R. Elnitiarta. BAT911.Worm. Security response, Symantec, February 2007.

[8] A. Freed. Arlington CISO Dave Jordan on why we're losing the cyber war. blog, February 2015.

[9] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: validating ssl certificates in non-browser software. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 38–49. ACM, 2012.

[10] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman. Green lights forever: analyzing the security of traffic infrastructure. In *Proceedings of the 8th USENIX conference on Offensive Technologies*, pages 7–7. USENIX Association, 2014.

[11] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 209–223. IEEE, 2012.

[12] V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in scada networks. *Computers & Security*, 25(7):498–506, 2006.

[13] L. Ma, A. Y. Teymorian, X. Cheng, and M. Song. Rap: Protecting commodity wi-fi networks from rogue access points. In *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops*, page 21. ACM, 2007.

[14] B. News. Wandsworth prison escapee Neil Moore faked bail email. http://www.bbc.com/news/uk-england-london-32095189, march 2015.

[15] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. Scada security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012.

[16] U. D. of Justice. Louisiana man arrested for releasing 911 worm to WebTV users. http://www.justice.gov/criminal/cybercrime/press-releases/2004/jeansonneArrest.htm, February 2004. Press release.

[17] C. I. S. Officer. Criminal justice information services (CJIS) security policy version 5.3, aug 2014.

[18] D. J. Roberts. Cloud computing in law enforcement: Survey results and guiding principles. *The Police Chief*, 80(3):56–58, march 2013.

[19] M. Szczys. WiFi jamming via deauthentication packets. http://hackaday.com/2011/10/04/wifi-jamming-via-deauthentication-packets/, October 2011. Hackaday.

[20] R. West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.