Global Information Assurance Certification Paper

Data, Host and Network Security in an Integrated Juvenile Justice System

Duncan Molony
09/12/2000

"Integration" is one of the hottest buzzwords in industry and government today. It is difficult to read an article or watch a report about business strategy that doesn't contain some mention of integration, and everything coming from the government seems to stress some form of integration. This is a good thing – as long as the powers that be understand that integration means increased risks and increased security. In the area of criminal justice there is a nationwide push to integrate all local and state agencies that are involved in the monitoring, enforcement and research of criminal justice. These Integrated Systems can include police, courts, probation, attorneys, detention facilities, diversion programs, medical professionals and agencies, mental health professionals and agencies, schools, and the list goes on.

There are many barriers to successful criminal justice integration such as political, legal, policy, budget and security. Security is listed last because that is all too often where it falls in a prioritized listing of obstacles. Many of the criminal justice integration efforts are supported by Federal grants that all require "data security" without any specifics on security implementation or a means to gauge the effectiveness of security measures. The emphasis in most of the information available seems to be on the formation of collaborative task forces for integration and the agreements between agencies and not about the technical aspects of integration. In fact, it is common for these efforts attempting to achieve Integrated Justice *Information Systems* to all but ignore the requirements of computer and network hardware and software in the efforts to achieve the desired integration. The equipment and personnel required for the integration are simply not accounted for in budgeting.

I have encountered the above frustrations and others in my work to help implement an Integrated Juvenile Justice Information System. This paper is description of the data, host and network security issues that I face in an integrated system and some measures I am taking to ensure security.

In most states, juvenile data is protected data only accessible to those who are granted access by law. This information not only includes juvenile criminal offenders, but also abused and neglected juveniles as well as adoption records, so protecting the data is truly protecting the innocent. An obvious first step to protecting this data is to ensure that the data is on a physically secure server with tightly monitored access control, and that the backups of the data are encrypted and the tapes stored in a secure location. Virus protection is layered from the host to the servers. In addition, those granted access to the data are seldom allowed to access all data related to a juvenile, therefore data access is further limited by data views and limited user interfaces. In some instances someone may be allowed to view specific data only at certain times during a proceeding. For example, a judge is not allowed to see arrest records of refused charges (charges not prosecuted by

the District Attorney) during a trial. However, if a juvenile is found guilty the judge may be allowed to see such information. This requires an intelligent user interface for the judge that will only display such information at the appropriate times and under the appropriate circumstances. The specific query is accessible only to judges and only when the appropriate criteria have been met, and the query itself is granted access to the data, not any users. For most personnel, log on hours are restricted to standard business hours and password policies enforced for all personnel. To further protect the data which is accessible from some host that are not physically secure, idle time outs are enforced to disconnect the user if the session has been idle for a set amount of time. In addition, all floppy drives on the hosts are deactivated. These measures will protect the data from most non-sophisticated internal users, but log auditing is still required.

All of this is fine for internal protection, but what about integration? This is where it gets tricky. Many of the agencies that need to be a part of the integrated system have varying levels of security and therefore have different requirements of the system. The safest route would be to take the most restrictive policies and build on those, however because of the dynamic of the agencies involved that is not always possible. Everyone always thinks their data is sacred and their security is best. It takes genuine effort and cooperation to agree upon a standard of security for the integration effort as a whole. I wish I was able to provide a model for this security standard, but one is not completed as of this writing. I will however discuss some of the concerns and the solutions being debated.

The first requirement for integration is a means of integration, whether that is dial-in access, VPN connections, or dedicated connections. In my specific circumstances I am dealing with a combination of direct dedicated connections to some agencies, connection through the city's Metropolitan Area Network for others, VPN's for some, and dial-in access for some select individuals. This presents a wide array of risks and limited resources to deal with these risks. My goal is to provide the functionality required for integration with limited access to local systems by outside hosts. The first line of security is a firewall through which all incoming and outgoing traffic must pass.

At first glance the direct, dedicated connection to one agency seems to be the lowest risk until it is considered that this agency is connected to at least 4 other agencies and the Internet. Also, there are close to 1,000 users on this agency's system. All of a sudden this connection isn't looking so innocent. Since this agency provides required data to the system they have to have a clear access point and rights to dump data. In addition, the agency also requires access to specific information generated from our system. To limit exposure, the agency only has inbound access to an FTP server in my DMZ. This data is then scanned for viruses and validated by digital signature before it is merged with my data. Fortunately, all information required by the agency can be emailed to them in the form of an encrypted daily report so there is no need for the agency to have direct interactive access to my systems.

The connection through the City's MAN is a scary proposition. It is needed to connect to several of the agencies but has many risks associated with it. The MAN is maintained by an understaffed, overworked, and under trained MIS department and therefore cannot be

trusted to provide a secure line of communication. In addition, the agencies are also connected to other agencies and each has a dedicated Internet connection. Adding to the risks is the fact that one of these agencies requires direct interactive access to my systems. It is fortunate that this particular agency has personnel working on site at my location performing the majority of the interactive queries so I can have somewhat more control over the access. However, queries need to be run and reports generated from data on my systems, so data does cross the MAN. This is where data encryption, intrusion detection and auditing will help add to the levels of security.

Individuals including doctors, probation officers, and caseworkers connect through VPN and judges through direct dial-in access. The VPN connections require specific VPN clients and short-term passwords. The individuals using the VPN connections have access to only specific case files and only during a specified time period(while the case is active or when their expertise is needed). An idle time-out is also used to prevent a VPN connection form being left open and unattended. The judges require dial-in access to issue orders, review specifics and submit documents. The judges are the only individuals with dial-in access permission and this connection is closely monitored.

In addition to the above security measures, the most sensitive data – adoption records and victim information for example – are always encrypted and access is granted on an absolute need to know basis. In fact, with adoption records only the adoption clerk and the Clerk of Court have any access, not even the system administrators, and even this is closely monitored.

Considering the limited resources and political and legal barriers, the steps outlined above and continued vigilance can provide and adequate level of security for the sensitive data contained in an Integrated Juvenile Justice Information System.

Sources:

Office of Justice Programs, Office of General Counsel. "Integrated Justice Information Systems – The Department of Justice Initiative." April 12, 2000 URL: http://www.ojp.usdoj.gov/integratedjustice/ag-draft.htm (September 8, 2000)

Landsbergen, David and Wolken, George. "Eliminating Legal and Policy Barriers to Interoperable Government Systems." August 12, 1998 URL: http://www.ctg.albany.edu/research/workshop/24-landsbergen.pdf (September 7, 2000)

Carey, Mark. "Taking Down the Walls: Measures to Integrate the Objectives of the Justice System with the Community's" 1997
URL: http://www.ojp.usdoj.gov/nij/rest-just/ch6/takingdown.html (September 8, 2000)

Stoneburner, Gary. "Common Barriers to IT Security." July 1998 URL: http://www.ctg.albany.edu/research/workshop/6-stoneburner.pdf (September 7, 2000)

Matthews, William. "Are online records too public?" June 01, 2000 URL:

http://www.fcw.com/fcw/articles/2000/0529/web-swire-06-01-00.asp (September 8, 2000)

Kelso, J. Clark. "Final Report of the National Integration Resource Center Task Force – The Lisle Report." August 30,1999 URL: http://www.ojp.usdoj.gov/integratedjustice/lisle-fn.htm (September 7, 2000)

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor