HUD's

HOMELESS ASSISTANCE PROGRAMS

Public Access Control:
Community Strategies for Implementation

September 2007

Office of Community Planning and Development
U.S. Department of Housing and Urban Development

Acknowledgements

This document was prepared by Canavan Associates and Cloudburst Consulting Group, Inc. for the U.S. Department of Housing and Urban Development (HUD), Office of Special Needs Assistance Programs in the Office of Community Planning and Development. The primary author of this document is David Canavan of Canavan Associates. This document was reviewed by Michelle Hayes of the Cloudburst Group.

Acknowledgment should be given to those communities and HMIS solution providers that have been successful in implementing public access protocols for providing detailed information for this report. Communities participating in this project requested anonymity to prevent any sensitive details about their implementations from being published.

I. Current Environment

Every Continuum of Care (CoC) in the country wants to be good stewards of the data they collect through their Homeless Management Information System (HMIS). It is clear both anecdotally, and from prior research that CoCs have varying definitions of "good stewardship." With the publication of the HMIS Data and Technical Standards (Standards) in 2004[1], HUD created uniform expectations for the operation of an HMIS.

As HMIS projects have matured from implementation to operation they have become integrated into each community's technology infrastructure. Many communities have progressed beyond baseline standards, adding additional controls or protocols to further protect their HMIS. Public Access Control is one of the baseline practices HUD requires in the Standards. CoCs must prevent unauthorized computers from connecting to their HMIS.

Public access control is required by Section 4.3.1 of the Standards. The standard (shown below) specifically requires CoCs to prevent access to their HMIS from non-authorized computers.

> Public Access. Baseline Requirement. HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks or similar arena (pg. 45931 of FR 49-N-146).

The two technologies mentioned in the text of the standard are based on very different approaches. Public Key Infrastructure (PKI) enables users of an unsecured network, like the Internet, to securely and privately exchange data through use of a cryptographic key pair, commonly called certificates. Certificates, or keys, are issued by a Certificate Authority and distributed to authorized computers and/or users. Typically certificates are installed on an individual workstation or contained on a piece of external hardware (i.e. USB or key fob) that must be connected to a workstation before gaining access to the HMIS. The second technology referred to in the standard is Internet Protocol (IP) filtering which prevents access to HMIS except from machines with identified IP addresses. An Internet Protocol address is a unique number assigned to each computer to manage a network. Both these technologies are discussed in detail later in this report.

[1] http://www.hud.gov/utilities/intercept.cfm?/offices/cpd/homeless/rulesandregs/fr4848-n-02.pdf

While the standard specifically mentions these two technologies, there are several other methods available that meet the baseline public access standard. Additionally, new methods are constantly under development and may prove to be a good fit for communities, while adapting existing technology may prove more appropriate for others. Over the past several years, communities have used different approaches to comply with this standard. Several of these, including multiple PKI methods and IP filtering, are discussed in detail below.

Due to the nature of most HMIS implementations, compliance with this standard requires close cooperation with a community's HMIS solution provider. Most HMIS software solutions use the application service provider (ASP) model. In the ASP model, customers are provided access to the application via the Internet, thereby saving the customer all of the costs and effort associated with hosting and managing the application in-house. Typically in this model, the vendor does not permit access to the underlying IT infrastructure and only authorized users are permitted to access the application. CoCs using this model are unable to negotiate directly with third party providers for PKI solutions without the direct involvement of the HMIS vendor. Communities hosting their own HMIS have several other options available to them since they control the IT infrastructure of their implementation, although they may still require the cooperation of their solution provider. Communities using technologies other than PKI or IP Filtering will in all likelihood still need the cooperation of their HMIS software providers as most solutions require access to the IT infrastructure.

II. PKI and IP Filtering in Theory and Practice

CoCs across the country have taken several different approaches to complying with the Public Access Control standard. Most have implemented either PKI or IP Filtering, while a few HMIS solution providers have made other types of access control technology available. To understand current practices, several communities that have implemented public access controls were contacted and invited to share their experiences.

Each of the communities discussed is a single CoC with a single HMIS implementation. The communities represent a mix of rural, suburban, and urban environments. The majority of HMIS implementations operate independently of the CoC structure with a single project administrator having the autonomy to make technology decisions, while policy decisions are handled by a sub-committee of the CoC.

Public Key Infrastructure in Theory

A PKI is a combination of policies and technology that is generally used to authenticate and encrypt information. CoCs may purchase the technology from different vendors though, many use a PKI made available by their HMIS provider. Some HMIS providers allow communities to implement PKI for free. A public key infrastructure can be configured in several different ways depending on the community's goals. Communities participating in this project used 3 different configurations:

- Certificate assigned to an individual;
- Certificate assigned to an agency; and
- Certificate assigned to an entire implementation.

Each configuration identified above has benefits and challenges. As the complexity of a PKI implementation increases, so does the amount of time necessary to administer, support, and operate it. In its most basic implementation, a community can issue a single certificate, or key, for the entire installation. That is, if the installation is statewide, every user is issued the same key. In this scenario, if one key becomes lost or is no longer controlled by the system owners, then their ability to vouch for this layer of security would be compromised. A simple analogy is if a key to the family house is lost, than the family must change the lock and re-issue each family member a new key. In a statewide implementation with potentially thousands of users needing a new key, re-issuing could prove challenging and would require extensive resources.

The next layer of complexity is to assign a certificate, or key, to each organization in the HMIS. To again use the example of the family home: if a family loses the keys, it does not affect the neighborhood as every house has different keys and different locks. Using the association between the certificate authority and the subordinate certificates, each organization can be issued their own unique key, each recognized as valid. This variation has its own challenges; an implementation with hundreds of agencies could struggle to maintain the integrity of the distribution channels for the keys.

If the CoC is issuing the keys from a central location, the keys must be distributed to each computer authorized to connect to the HMIS. Again, different communities used different solutions in overcoming this challenge. A community can distribute the certificates online, via email, or by physically traveling to each machine. Distributing the certificates online can be challenging as each computer must be configured in the proper way to accept delivery of the certificate. An HMIS administrator may also choose to email the certificates to individual users or a site administrator for installation. Either of these methods ultimately defeats the purpose of the certificate since neither of these technologies are secure modes of transmission. Once it is transferable, individuals may move the certificate without authorization to any machine. In addition, standard email contains no encryption, is not securely deleted, and is frequently stored on third party servers or elsewhere with or without the user's knowledge. An administrator may require a password to prevent unauthorized installation.

The most secure alternative is for the certificate to be created on a disk or other storage format at the central server and then physically delivered to the site. While the certificate would still be transferable, this delivery method ensures it only goes to the intended program/agency location. A certificate can then be locked on to each machine by the site administrator.

At the most complex implementation, an HMIS could issue a certificate to each individual user. This structure requires a tremendous amount of administration and should be undertaken only by organizations that will realize benefits even after investing significantly in administrative, technical, and user support personnel. Issuing a key to an individual requires identity verification, typically by a third party. There is no point in authenticating a user over and over again if a user's identity was never initially established. Once the user's identity is established and the credential is issued, the system owners must determine how to store that credential. Typical storage formats include a USB drive, key fob or other device.

Public Key Infrastructure in Practice

Communities chose their solution based on three key elements: available expertise for support; cost; and ease of use. It became apparent when these factors were examined why almost every community chose to implement a PKI solution offered by their HMIS solution provider. There was no vendor that could compete with the service and price offered by the HMIS provider. Each model discussed in the previous section is being used by at least one of the participating communities. Some of the communities chose one model then switched -- or are in the process of switching models -- due to cost, user satisfaction, ease of use, technical support, or administrative burden. Below are the experiences of communities that have successfully implemented public access controls, outlined by most comprehensive to most streamlined.

Certificates for Every User

An example of a community implementing the most comprehensive PKI solution, matching a single certificate to a single individual is Community #1. In this community, security was the highest priority of their HMIS and the determining factor in all decisions. A vital factor in this city's choice was the availability of state support. The state was already implementing a PKI solution for use in confidential state systems and offered the community the opportunity to join the initiative. As a result, the community did not need to invest any time or money on research, vendor selection, or set up costs.

CoC #1
-Urban CoC
-Implemented HMIS in 2003
-Population between 500,000-1,000,000
-Security was highest priority

While the concept was strong and the support offered seemed adequate to ensure user satisfaction, the community began to encounter some difficulties during implementation. In contrast to the other users of the certificate system, the HMIS users were not state employees. As stated earlier, if communities are going to issue individual certificates to individual users it is useless to repeatedly authenticate that user if their identity was not established at the beginning. While the state already possessed the information necessary to establish the identity of their employees the HMIS project did not. This lack of a single employer created a major obstacle for the community.

The workaround the community and the state implemented was unfortunately not as successful as planned. The process created required every HMIS user to submit primary documents establishing their identity -- including driver's licenses, birth certificates, and social security cards -- to the organization issuing the certificate. The issuing organization then processed the individual's documents and verified that the individual user was in fact the person they claimed to be. This process immediately hit a major obstacle: there is a major difference in the culture of frontline social service staff compared to state employees who require access to confidential data.

Not only were concerns of government intrusiveness immediately raised by the process but several community members became concerned that background checks also were being performed. The issuing organization repeatedly assured the community that there were no background checks and that they were simply verifying identity. The second major obstacle was that many frontline social service staff did not have the requisite documents. In many communities formerly homeless individuals decide to work in the social service system, their experiences and knowledge add immensely to an agency's capacity. These individuals as well as other staff members were unwilling or unable to acquire the documents at their own cost.

While these obstacles delayed the implementation of the solution, it did not derail it. Once HMIS users had submitted all their documents an electronic certificate on a USB drive was issued and delivered to their primary residence. The lag time in the issuing process meant that some users had moved and never received their credentials. After a user received their credential all of the standard possible technology failures came into play. Standard failures include, but are not limited to, poorly configured machines, lost or broken storage devices, and accidental user error. Many agencies began to advocate for a different solution. This community has begun to consider implementing a less rigid system.

Certificates for Every Agency

Issuing a certificate for every agency is feasible for some communities but not for others. Community #2 chose to implement PKI for several reasons. While many agencies cited HUD policy as the primary motive for implementing a public access solution, in this community a stringent state law was the primary motivator. Unlike the previous example, this community experienced almost no obstacles while implementing their PKI.

CoC #2
-Rural County CoC
-Implemented HMIS in 2000
-Population between 200,000 and 300,000
-Implemented PKI in part to comply with state law

Determining if a certificate would be matched with each agency, the HMIS administrator considered several factors: the cost of issuing every user a certificate was prohibitive; the effort to support a user-level solution would be tremendous; and the HMIS solution they use did not support individual certificates. The community decided to implement agency-level certificates, though with some challenges. Each computer in an agency must be installed with a certificate. If a community chooses to physically install each certificate at the agency, each program site must be visited. Depending on the geography of the Continuum, this may or may not be possible for every implementation. Again, it is possible to distribute certificates via the Internet, however in this configuration the certificate loses one aspect being sought by communities- its immobility. As the certificates must expire at some point, HMIS staff will have to re-issue and re-install it, requiring the new certificate to be installed on every computer. Some communities have overcome this problem by delivering each agency's certificate to the agency administrator and delegating responsibility to the administrator for installation and custody.

The administrator reports that the certificates were not difficult to install, taking less than a minute per machine. By keeping a database of expiration dates, the administrator is able to schedule visits prior to expiration to each site for re-installation of new certificates. The end users have not reported any problems and are generally pleased by the fact that the certificate does not interfere with their work. This solution allowed the community to meet the HUD requirements and, more importantly to them, also comply with state law. This combination of technological control and policy is the right balance of cost and benefit for many communities.

One Certificate for the Implementation

Using one certificate for the entire HMIS is the most streamlined method of implementing a PKI, as demonstrated by Community #3. By issuing a single certificate for the entire implementation, the HMIS administrator does not have to manage the process of tracking expiration dates or sorting multiple certificates. A possible weakness in this structure is that if the certificate is lost, misplaced, or stolen, the community has no choice but to re-issue the entire implementation a new certificate. A CoC may use the password feature of a certificate to prevent unauthorized installation. However, if a CoC has 40 agencies accessing the HMIS, it would still be required to install the certificate on the computers of those 40 agency sites. If the CoC is not careful in the manner in which it distributes the certificates, a copy can be lost. This structure also decreases accountability: if a certificate is misused, there is no way to determine the source of the policy violation.

CoC #3
-Suburban CoC
-Implemented HMIS in 2002
-Population between 400,000 and 500,000
-Large county with several cities

The administrator in this community chose to use a single certificate because the need to visit each site on a rotating basis was not feasible with the staffing on the project. With a single certificate, the administrator can install a new one when on site for other business near the expiration of the certificate.

This method provides the simplest method for achieving control over which computers connect to the HMIS. While it allows communities to be in compliance with the standard, a community prioritizing security will want to carefully consider the method used for storage and distribution. Careless handling of the certificate will prevent this layer of control from achieving any actual increase in security. Proper handling of the certificates will permit a CoC to achieve an increase in control over which machines connect to the HMIS with a greater level of assurance than IP filtering.

Summary

The experience of these communities suggests that implementing a cost-effective PKI solution is possible for small and large communities. Smaller communities have been successful without large investments of staff time or money. Smaller communities frequently have less complex, smaller HMIS implementations, which contributes to the success of implementing PKI. In fact, some of the communities utilized free solutions from their HMIS solution providers that required a minimal expenditure of staff time to implement. Larger communities will likely encounter more obstacles, but are also more likely to have the capacity, expertise, and resources to meet those challenges.

The options for location control are limited by HMIS software providers. Without HMIS solution providers integrating PKI into their applications, the ability of communities to implement this control is limited. An alternate to PKI, as discussed earlier, is limiting access through IP filtering.

IP Filtering in Theory

Internet Protocol (IP) Number filtering is a method of permitting certain computers to connect to a network. Each computer in a network is given a unique numerical identification called an IP address, similar to a phone number, to identify it. As long as that computer is connected to the network, the IP number identifies the computer as unique.

IP filtering only permits computers with authorized numbers to connect to the network. IP numbers are programmed into the network by an administrator and are individually permitted to connect. The smaller the network, the fewer IP numbers need to be programmed into the network. As the network grows, the number of machines that need authorization increases. Machines with static IP addresses only need to be authorized once.

In many networks, the IP number is dynamic -- a computer is assigned a number for a period of time. When that time expires, the computer is issued a new IP number. This method is used to make the network function more efficiently. Dynamic IP numbers are frequently used by Internet Service Providers (ISP) when providing broadband or DSL service to their customers. IP filtering is not possible when dynamic numbers are used.

Many HMIS implementations depend on ISPs for their internet service. Smaller homeless service agencies typically do not have IT staff or a large network, so the ISP is responsible for the generation and maintenance of IP numbers. In larger programs, the IT staff can control the duration and distribution of IP numbers, but the network frequently connects to the Internet through one or two points that have static IP numbers.

IP Filtering in Practice

Many agencies are issued dynamic IP addresses from their ISPs. Agencies can pay an additional fee to be issued a static IP number. Unfortunately, even the static numbers issued by ISPs occasionally change. Some of the HMIS vendors that participated in discussions about IP filtering initially used it as a method for preventing unauthorized access to their HMIS. Some HMIS vendors still offer IP filtering for those customers that can utilize it without major alterations to their networks. For implementations that have a large number of computers or frequently changing IP numbers, the required programming time to constantly update the network is untenable and unaffordable.

The process to maintain the IP filter requires the site to document every change of IP numbers. Few HMIS implementations choose this course because they are unwilling to commit the necessary resources. Once the IP numbers are communicated to the HMIS provider, their staff must input the changes into their network to update the filter. If a site changes their IP number without notifying the HMIS provider, they will instantly lose access to the HMIS. The process and time to keep authorization flowing smoothly is considerable.

Understandably, organizations either historically or currently offering IP filtering found that either their customers were uninterested or the administrative burden was too much to be a viable solution for public access control. One of the HMIS providers using PKI offered an IP filtering solution originally but discontinued it because they were unable to keep up with the variance in Internet Protocol numbers. Many programs were using dial-in accounts, Internet Service Providers were using dynamic numbers, and the benefit was minimal.

One community participating in this project chose to utilize IP filtering instead of PKI. This decision was based on the ability of the CoC to obtain static IP numbers for each program: the HMIS software provider supporting the solution; and the small number of programs. Additionally the programs were spread across a wide geography that was too large for the HMIS administrator to travel regularly.

III. Potential of Alternate Technologies

Alternate models to PKI and IP filtering are available to communities. One technology gathers information about the user's computer by collecting information from each machine when initially connected to the HMIS. Examples of the types of information that could be collected include browser information or media access control (MAC) address. This information is recorded in the HMIS and the next time a user connects to the system the information from the current machine is compared to the historical information. If the information matches within a certain margin of error, the user is permitted to connect. If the information is not the same, the connection is declined. This model has been referred to as profiling or thumb-printing computers.

Another model being tested uses the technology known as cookies. These small bits of data are stored by different websites on a user's machine. Cookies are used by many commercial sites for a variety of purposes including customer service, tracking website visits, or storing response to frequently asked questions such as username. The proposed application in HMIS involves placing a cookie on the HMIS user's machine the first time they log in, and then checking for it every time thereafter.

As further innovation in the area of public access control progresses, additional options may become available for communities.

IV. Conclusion

The goal of each technology discussed remains constant -- to protect the information entrusted to the HMIS and CoC. The Data and Technical Standards present an interlocking set of controls to create a degree of security that does not depend on any one method. This model allows for failure of some controls without a failure of the whole system. The more integrated the CoC's security management is to the entire project, the more protected the information.

As more real and perceived barriers to implementing public access controls by both HMIS solution providers and CoCs are overcome, compliance with the standard becomes more achievable for every community. HUD continues to be clear that CoCs must work towards compliance with the public access and all other baseline requirements identified in the Standards.