

Phil,

The NIST work came from Bill Majurski, cc'd on the e-mail.

Glen

-----Original Message-----

From: Phil Barr (HL7) [mailto:pbarr@hl7.org]
Sent: Thursday, February 03, 2005 12:17 PM
To: Marshall Glen
Subject: RE: NLM EHR- Security and policy issues

Glen,

Is what NIST offered a packaged solution? Any estimate on time to implement? Is it being used in production anywhere?

Phil

The implementation used for the IHE demo is open source, running on Linux, supplied by NIST, and has clear implementation specifications, and supports CDA documents. Ready to use. :-)

From: Marshall Glen [mailto:Glen.F.Marshall@siemens.com]
Sent: Thursday, February 03, 2005 10:42 AM
To: Phil Barr (HL7)
Subject: RE: NLM EHR- PHIN-MS

Phil,

See my comments in [green](#).

Glen

-----Original Message-----

From: Phil Barr (HL7) [mailto:pbarr@hl7.org]
Sent: Thursday, February 03, 2005 10:04 AM
To: Marshall Glen
Subject: RE: NLM EHR- PHIN-MS

Glen,

Thanks for the quick and thorough response.

As far as I know, there is no standard work for policy automation for consents. These are typically application business rules, not security infrastructure. There are sound technical reasons for keeping it that way, at least in the short run.

We're interested in obtaining an example of how application business rules have been applied to send and respond to live electronic requests for data from external systems in a way that does not require technical negotiation. Assume a trusted requestor and an identified patient.

No standards exist for this. I know of some proprietary implementations for applications business rules engines. Having dived into this problem to analyze the requirements a while ago, it is one of those fractal-like things that first looks simple but gets complex quickly.

The items you have listed do not address the range ...

Have you been in contact with the CDC and reviewed their work? Perhaps their system fits the bill. It is using very current technologies and protocols. In addition they are near completion of a next version and may be interested in your independent evaluation. It was my understanding that they had done a good deal of independent testing of various aspects of their current system.

Certainly you are not suggesting that each independent installation has to review all of the points you mentioned. Working "certified" components have to be able to fit together. It seems like a reasonable route to use a system configuration such as PHIN-MS which has already proven itself in many real situations.

I have not analyzed the CDC's solution. They may have remarkably different policies and threat profile than an EHR, though. There are independent certified evaluation test laboratories that the government uses already, so that's the most open route to take.

I am suggesting that a "master" protection profile could be produced for EHR, i.e., something that could be used by default. The big issue with such an approach is scalability, so we might actually need a set of protection profiles coarsely granular according to the scale of the user's application.

We also have basic working technology for regional federated EHRs, and that will be demonstrated at HIMSS this year.

Do you know of a working open source alternative that does what we need and that could be plugged in as an alternative?

The implementation used for the IHE demo is open source, running on Linux, supplied by NIST, and has clear implementation specifications, and supports CDA documents. Ready to use. :-)

You referred to one shortcut, XP, which though certified has been the target of numerous high-profile security breaches. I know, nothing is perfect ☺.

There is a certifiable Linux distribution, and some UNIXs are certified. But XP has been certified and is ubiquitous. Let's not be knee-jerk anti-Microsoft. Politically, I'd rather have them in the tent than not.

A finished profile will contain a set of interrelated requirements, with the interrelationships all mapped, in these categories:

- Functional Requirements
 - Audits -there is an audit trail, how it is managed is out of scope.
 - Nonrepudiation - of messages yes, message content to the extent handled by version of CDA
 - Cryptographic support – yes
 - User data protection – not sure of definition beyond encryption
 - Identification and authentication - yes
 - Security management - yes
 - Privacy – out of scope for security envelope, vital to project
 - Protection of the security infrastructure – out of scope
 - Resource utilization – we used a windows 2000 server, ms sql server (not sure how much detail you need)
 - Access to the secured system – out of scope
 - Trusted paths - yes

You can use this profile to perform a a gap analysis of any target system versus.

I agree we should reference the need for out of scope considerations to be met in actual implementations.

It's more than that. Adding security after the fact, or scoping-out things without referencing a security protection profile, significantly alters design. So real-world applicability of the NLM project results could be very much open to question. I don't want that to happen.

Comments?

Phil

From: Marshall Glen [mailto:Glen.F.Marshall@siemens.com]
Sent: Wednesday, February 02, 2005 10:06 PM
To: Phil Barr (HL7)
Subject: RE: NLM EHR- PHIN-MS

Phil,

As far as I know, there is no standard work for policy automation for consents. These are typically application business rules, not security infrastructure. There are sound technical reasons for keeping it that way, at least in the short run.

Within the security infrastructure, I recommend developing what's called a "protection profile". This is a construct outlined by ISO 15408 standard, a/k/a the Common Criteria. It is mandatory to use ISO 15048 for US federal government systems security evaluation. It is also a construct being used by

the CCHIT workgroup on security & reliability, so that's what will likely be used to certify EHR systems. The items you have listed do not address the range of ISO 15408 requirements. Worse, their presence gives an improper, although not obviously so, impression that security has been taken care of.

To create a protection profile, it's good to start with an existing one. Here are some references:

- <http://csrc.nist.gov/cc/index.html> for an overview
- http://www.iatf.net/protection_profiles/profiles.cfm for some well-scoped samples
- <http://www.commoncriteriaportal.org/public/files/ppfiles/capp.pdf> for a wide-scope profile that equates to the now-obsolete C2 commercial-level security designation.

The essence of protection profile development is to start with clear policies, threats, environmental assumptions. From those you get a combine set of objectives for policies to be enforced and threats to be mitigated. Then you proceed to the technical requirements, non-technical assurance activities (such as actually reading audit logs), and additional requirements that should be fulfilled by the environment. It's a very orderly and somewhat intricate yet mechanical process -- after the messy part of defining the security policies & threats, There are catalogs of threats to draw from, though, so it's really all policy-driven.

A finished profile will contain a set of interrelated requirements, with the interrelationships all mapped, in these categories:

- Functional Requirements
 - Audits
 - Nonrepudiation
 - Cryptographic support
 - User data protection
 - Identification and authentication
 - Security management
 - Privacy
 - Protection of the security infrastructure
 - Resource utilization
 - Access to the secured system
 - Trusted paths
- Assurance activity requirements
 - Configuration management
 - Delivery and operation
 - Secure development
 - Guidance documents
 - Life cycle support

- Tests
- Vulnerability assessment

You can use this profile to perform a a gap analysis of any target system versus.

In the end, security is as good as how the policies are implemented and demonstrably enforced. For that reason *any* security-relevant component must have a clearly-stated purpose, audit records to gather evidence that security policies are being enforced and threats are being mitigated, and administrative functions to control the operation of each security-relevant function. A shortcut: most security built into commercially available operating platforms already supplies what you need. I would be more comfortable if you were to simply state, for example, that you are running on MS Windows XP since it has been certified to conform with the capp.pdf document listed above. Just listing a few components tells me that it is likely that someone could hack the EHR security and violate patient privacy without being detected.

IHE already has specifications for enterprise authentication, auditing, user directories, and node authentication. IHE will be developing additional security specifications for EHR-scale applications this year. They are all standards-based. We also have basic working technology for regional federated EHRs, and that will be demonstrated at HIMSS this year. So I also recommend that the NLM project adopt and implement using IHE profiles, and contribute to the IHE work this year. It's worth noting that the VA required IHE conformant systems in its RFPs, per a policy announced this year. I am the liaison from IHE to HL7, so let me know how you'd like to proceed and I can help make it happen.

Speaking as a vendor, I would like to see a clear path articulated from the current state to the NLM vision. I'd recommend that you speak with the HIMSS EHR Vendors Association. Two newly-elected co-chairs of the HL7 EHR TC -- Peter DeVault and Corey Spears -- are also active in the vendors association, so it would be best to work with them. I can also help, if you'd like, since the chair of the vendors association is a co-worker of mine.

That's it for now.

Questions/thoughts?

Thanks,
Glen

From: Phil Barr (HL7) [mailto:pbarr@hl7.org]
Sent: Wednesday, February 02, 2005 17:45

To: Marshall Glen
Subject: NLM EHR- PHIN-MS

Glen,

Hi, I appreciated meeting at the Orlando meeting. Two things:

1) From where I sit a major biggest obstacle to widescale adoption of the NLM project messaging set is the issue of policy automation or as it is called by some consent services. I'm interested in mature work that has been done in this area that we might be able to pull into the project.

2) Thanks for your comments at the Info Session. I was looking for your guidance on the way that PHIN-MS addresses messaging requirements, it's shortcomings, and criteria that we should be recommending to those seeking to do actual implementations. For us it was a shortcut to getting a working demo going.. It handles:

Authentication,
Trusted Certificates,
Transport,
Encryption.

We are interested in documenting it's shortcomings and or variances from HL7 standards and direction.

<http://www.cdc.gov/phinf/messaging/index.htm>

http://www.cdc.gov/phinf/messaging/systems/2003_04_23_An%20Overview%20of%20the%20PHINMS.pdf

Phil

Phil Barr MPH, BSIT, EEET
Manager NLM Project
Health Level Seven, Inc.
3300 Washtenaw Ave., Suite 227
Ann Arbor, MI. 48104-4261
Office: 734-677-7777 x169
Cell: 734-717-4040
pbarr@HL7.org

This message and any included attachments are from Siemens Medical Solutions USA, Inc. and are intended only for the addressee(s).

The information contained herein may include trade secrets or privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful. If you received this message in error, or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by e-mail with a copy to Central.SecurityOffice@shs.siemens.com

Thank you

This message and any included attachments are from Siemens Medical Solutions USA, Inc. and are intended only for the addressee(s).

The information contained herein may include trade secrets or privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful. If you received this message in error, or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by e-mail with a copy to Central.SecurityOffice@shs.siemens.com

Thank you

This message and any included attachments are from Siemens Medical Solutions USA, Inc. and are intended only for the addressee(s).

The information contained herein may include trade secrets or privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful. If you received this message in error, or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by e-mail with a copy to Central.SecurityOffice@shs.siemens.com

Thank you