Trust Profile based Trust Negotiation for the FHIR Standard

Eugene Sanzi and Steven A. Demurjian
Department of Computer Science & Engineering, University of Connecticut, 371 Fairfield Way, Storrs, U.S.A.

Keywords: Trust Negotiation, Trust Profile, FHIR, Authorization, Healthcare.

Abstract: Sensitive healthcare data within Electronic Healthcare Records (EHRs) is traditionally protected through an authentication and authorization process. The user is authenticated based on a username/password combination which requires a pre-registration process. Trust profile based trust negotiation replaces the required human intervention during the traditional pre-registration process with an automated approach of verifying that the user owns the trust profile with digital signatures. To accomplish this, the negotiation process gradually exchanges the credentials within the trust profile to build trust and automatically assign authorization rules to previously unknown users. In this paper, we propose a new model for attaching trust profile authorization data to Fast Healthcare Interoperability Resources (FHIR), a standard created by HL7, in order to integrate the process of trust profile based trust negotiation into FHIR.

1 INTRODUCTION

The healthcare industry is increasingly adopting new techniques for sharing secure healthcare data through Health Information Exchange (HIE) (De Pietro & Francetic, 2018). While integration between electronic healthcare records (EHRs) stored at multiple providers has been hampered due to the difficulty in implementing interoperability standards, the exchange of patient healthcare data between providers is shown to positively affect patient treatment and patient satisfaction (Yasnoff, 2015). However, the authorization to healthcare data between healthcare providers is still attached to the slow username/password combination authentication process which requires explicit pre-registration. This pre-registration slows the dissemination of potentially time-critical sensitive healthcare data by requiring a system administrator to remotely determine a potential user's identity and explicitly assign authorization to the user.

Despite the difficulties in coordinating the exchange of health data, healthcare providers are adopting new technologies that facilitate its exchange. The Fast Healthcare Interoperability Resources (FHIR) (HL7 International, 2020) is a healthcare interoperability standard whose goal is to facilitate the retrieval of healthcare data by providing a common API to locate and exchange healthcare records. FHIR's data exchange structure is built on the concept of a resource, which provides a meaningful set of healthcare related data for transfer. FHIR provides over 125 different resources for: patients, observations, medications, patient consent, etc. Requests for a specific resource are available through a REST API that supports instance level interactions such as: read, vread (version read), update, patch (update a portion of a resource), delete, and history interactions. FHIR has emerged as a popular choice (Posnack & Barker, 2018) for supporting HIE. Microsoft has an azure API for FHIR (https://azure.microsoft.com/en-us/services/azure-api-for-fhir/), and Google has created a cloud healthcare API using FHIR (https://cloud.google.com/healthcare). Large EHR providers such as Epic (Epic Systems Corporation, 2020) and Cerner (Cerner, 2020) have leveraged FHIR to facilitate HIE for patient use.

Trust negotiation (Winsborough et al., 2000) was introduced as a method of building trust between two parties whose identities were previously unknown to each other. In this context, trust is defined as the ability to ascertain that the other party is authorized to obtain the requested sensitive data and will handle the data appropriately. During trust negotiation, each participant possesses a set of credentials capable of describing whether the other participant should consider them trustworthy. The credentials are exchanged between participants throughout several rounds of trust negotiation until there is a

Sanzi, E. and Demurjian, S.
Trust Profile based Trust Negotiation for the FHIR Standard.
DOI: 10.5220/0009830502420251
In *Proceedings of the 9th International Conference on Data Science, Technology and Applications (DATA 2020)*, pages 242-251
ISBN: 978-989-758-440-4

determination that: each participant possesses the set of credentials necessary to obtain trust; or, at least one participant does not possess a trustworthy set of credentials meaning trust cannot be established. One effort (Ryutov et al., 2005) extended trust negotiation by creating an adaptive framework, allowing online business to determine customer trustworthiness based on past purchase value. This adaptive framework has been expanded to include our controller's adaptation to the requestor's role and the specific resource being accessed. In (Vawdrey et al., 2003), trust negotiation was adapted to healthcare by describing a trust negotiation process for obtaining a patient's EHR, but provides only a healthcare license as a credential. In (Elkhodr et al., 2011), a three step trust negotiation process is used for determining the authenticity of a request for healthcare data, but still requires that the identity of the requestor is previously known.

Our prior work proposed and defined a *trust profile* (Sanzi et al., November 2016) as an extension to trust negotiation that defines a set of credentials based on the trust profile owner's history of successful access to sensitive data via trust negotiation. A trust profile is a collection of access history credentials that describe a particular user (the owner) and are digitally signed by a controller, an entity responsible for the secure dissemination of sensitive data. Trust profiles utilize X.509 identity certificates (Cooper et al., 2008), attribute certificates (Farrell & Housley, 2002), and certificate chaining to build trust between controllers in the credentials they have digitally signed (Sanzi & Demurjian, May 2016). The users send a request for data with a subset of their personal trust profile to a controller, which then reads the access history provided, determines whether the credentials are sufficient to establish trust, and releases the data if sufficient trust has been established (Sanzi et al., 2017). If trust negotiation is successful, the controller creates new credentials detailing the new access to sensitive data and sends them to the user with the requested data. These new credentials are then added to the user's personal trust profile to be presented to other controllers during future trust negotiation attempts. This improves upon previous works by providing a standardized set of credentials describing an entire access history, allowing complex requirements to be formulated on the controller side, and new credentials to be obtained during the course of a user's career.

Our work in this paper is part of an ongoing effort to integrate trust profile based trust negotiation into the authorization process of modern EHRs across all of the healthcare stakeholders (e.g., physicians, nurses, insurance billing agents, patients, patient families, etc.). The decentralization of healthcare information has spread across multiple EHRs as patients increasingly are being treated by teams of healthcare specialists in geographically separated locations. Our new proposed method of authorization for the release of sensitive healthcare data is required and replaces the time intensive pre-registration process. The FHIR security model is enhanced by integrating a new capability that incorporates the option for trust profile based trust negotiation during a resource request if the requestor is unknown to the healthcare organization providing FHIR based HIE. In support of this work, we propose a new model that: details trust profile metadata integrated into FHIR resources; and, describes the trust profile credentials needed to obtain access utilizing a combination of role-based access control (RBAC) (Ferraiolo et al., 2001) and mandatory access control (MAC) (Bell & La Padula, 1976). Successful access to FHIR data results in requestors obtaining needed healthcare data quickly and includes dynamic additions to their trust profiles detailing access to the requested resources that can be presented to other FHIR systems during future trust negotiation attempts.

The remainder of this paper is organized into five sections. Section 2 presents background on FHIR, access control models, trust negotiation, trust profiles, and the process of obtaining authorization via trust negotiation supported by trust profiles. Section 3 introduces extensions to our existing trust profile model (Sanzi et al., 2017) for intercepting resource requests to provide trust profile based authorization by annotating FHIR concepts and resource objects with trust profile data, and resolving authorization to the requested resources. Section 4 presents an example of the model applied to the healthcare domain. Section 5 has a conclusion for the paper.

2 BACKGROUND

2.1 Access Control

The *Role-based access control (RBAC)* (Ferraiolo et al., 2001) model binds a set of permissions to operate on data (create, read, update, delete) to roles (e.g., physician, nurse, front desk secretary, etc.). These roles are then assigned to users. When a user is assigned a role, the user may perform any action allowed in that role's permission set. RBAC is a popular access control model in healthcare as a result of its ability to simplify the assignment of complex permissions through role assignment, allowing consistent permissions across each type of job.

During trust negotiation, the user's assumed role allows our controller to map a set of required trust profile credentials to the specific resource requested.

The *Mandatory access control (MAC)* (Bell & La Padula, 1976) model defines a set of sensitivity levels on subjects (users) and objects (data) and allows access to the data if the user meets the required sensitivity level. MAC is generally modeled with levels: top secret (TS) < secret (S) < classified (C) < unclassified (U). If a user wishes to read data, they must meet or exceed the sensitivity level assigned to the data they wish to access. MAC in healthcare can be implemented as a method where the sensitivity level of the data corresponds with the potential for damage if released.

2.2 Trust Profiles

To facilitate the discussion of trust profile concepts, Fig. 1 displays a generalized overview of trust negotiation extended with trust negotiation. The medical authority in the upper left corner establishes trust between HIT Systems A, B, and C below by digitally signing its CA certificates, allowing each of them to trust any certificates signed by the other two. A user's trust profile, consisting of the identity and attribute certificates appearing on the left side of Fig. 1, is endorsed through the digital signatures provided by HIT Systems A, B, and C. A user constructs a digital wallet, which is sent to the controller of an HIT system. The controller utilizes the four Sec objects to be introduced in Section 3 to build a credential expression that describes the entries in the trust profile necessary to release the FHIR resources that they protect.

In Fig. 1, a *trust profile* is a complete collection of a user's entire history of access to sensitive data. In the healthcare field, a trust profile would describe each successful access a healthcare professional is granted to sensitive healthcare data. A *trust profile* is encoded in a series of X.509 encoded identity (Cooper et al., 2008) and attribute certificates (Farrell & Housley, 2002). Healthcare controllers issue one identity certificate per user the first time a user successfully accesses healthcare data from the controller. The accesses are described in sets of attribute certificates attached to the identity certificates. An attribute certificate is attached to an identity certificate by including the identity certificate's serial number and issuer, which is a combination that must be unique to that identity certificate. The attribute certificate is digitally signed by the controller to prevent subsequent modification.

The identity certificates describe a user's public key, and the user proves ownership of the trust profile data by proving ownership of the private key associated with the public key listed in the identity certificates. This also allows the user to claim ownership of any attribute certificate attached to the identity certificate. A healthcare provider must obtain his/her own certificate to allow a controller to act as a certificate authority (CA), allowing them to digitally sign trust profile certificates. The trust profile certificates digitally signed by a healthcare provider are only trusted by another provider during trust negotiation if: the other provider has decided to trust the controller's certificate by adding it directly to a local trust store; or, the other provider trusts the entity that signed the controller's certificate by adding the entity's certificate to a local trust store. A healthcare organization promotes trust by performing as a trusted entity signing the requestor's trust profile entries.

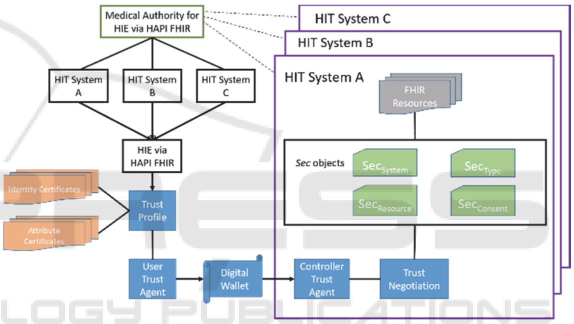

Figure 1: Overview of trust profile based trust negotiation.

Each user may obtain multiple identity certificates (left side of Fig. 1), one from each controller that has granted sensitive data access. Each identity certificate may have one or more attached attribute certificates and the access described within the attribute certificate must refer to data accessed from the controller that signed the attached identity certificate. A controller may only describe accesses that occurred within the EHR it controls. When a user with a trust profile discovers healthcare data, the user first initiates a request for trust negotiation by specifying: the resource being requested, the role the user possesses, and an initial subset of the trust profile referred to as a *digital wallet* (bottom portion of Fig. 1). The controller receives the request, retrieves security metadata for the resource, and builds a *credential expression (ψ)* during trust negotiation located at the bottom of HIT System A's purple box (right side of Fig. 1). The credential expression represents credentials that must be present in the digital wallet to grant the requestor access to the resource. The controller retrieves the four *Sec* objects (inner box of HIT System A) that describe the security constraints on the FHIR resource being requested (top of HIT System A). The controller may generate a set of release actions that depend on the credentials the requestor presents, such as: redacting sensitive data if the credentials are insufficient to release more sensitive data, logging the transaction in different severity logs, or dispatching audit notifications to the local system administrator.

If the credentials passed to the controller within the digital wallet are insufficient, the controller builds a server governance policy (SGP) (Winsborough et al., 2000) that describes the missing requirements. Trust negotiation may occur over several rounds, as the requestor and controller negotiate the release of potentially sensitive trust profile credentials. If the presented credentials are insufficient, negotiation fails and the connection is terminated. If the requestor has presented sufficient credentials to obtain access to the resource, the controller generates new certificates to describe the current data access and sends the certificates and health data back to the requestor. If a new identity certificate is required, the controller asks the requestor for a new public key for the new identity certificate. The controller then performs its release actions depending on the credentials matched to the credential expression and terminates the connection. The requestor receives the healthcare data and trust profile certificates and adds the new certificates to the trust profile. These new certificates may be used during trust negotiation with any controller.

Trust negotiation failures may be caused by a lack of required credentials or by deadlock during the trust negotiation process, where both the requestor and controller require a credential from the other before their own required credential can be released. Our integration of release actions improves the success rate by allowing controllers to relax requirements on the requestor in exchange for a lower rated trust transaction, which may result in data redaction or notes for manual auditing. Oblivious attribute certificates (Li & Li, 2006) can be used to eliminate deadlock by creating certificates that can only be read if the receiver possesses the attributes necessary to read them. With oblivious attribute certificates, data can be exchanged without the possibility of it being readable if the receiver is not authorized to view it.

2.3 FHIR

Fast Healthcare Interoperability Resources (FHIR) (HL7 International, 2020) provides structures for sharing EHR data between healthcare providers. Data is accessed through *resources*. Resources are accessed utilizing a location URL as part of a REST API in conjunction with a logical ID. This allows data that resources describe to sync between separate FHIR systems.

FHIR resources are organized in categories: *foundation resources*, *base resources*, *clinical resources*, *financial resources*, and *specialized resources.* We highlight only a subset relevant for the paper. The *base* resources describe: patients, practitioners, and family relationships; organizations, services, appointments, and encounters. The *clinical resources* are for a patient's health history, including: diagnostic data, medications, care provision, and request/response communication. *HAPI FHIR* (HAPI FHIR, 2020) is a Java implementation of the FHIR resources Patient, FamilyMemberHistory, Condition, Observation, Diagnostic Report, Medication, Immunization, AllergyIntolerance, Coverage, EligibilityRequest, Claim, PaymentNotice, etc. The resources are available through the FHIR standard's REST API.

3 TRUST PROFILE AND FHIR INTEGRATION

In this section, we describe our method for integrating FHIR with a trust profile based trust negotiation approach for dynamic and automatic authorization to requested FHIR resources that extends our prior work on a trust profile model (Sanzi et al., 2017) that encodes several different properties of access to a healthcare system within four types of attribute certificates. The remainder has seven subsections. Section 3.1 explores the interaction between the data encoded in trust profile attribute certificates and a description of the type of security metadata tracked within four different types of *Sec* objects. Each of the four different types of *Sec* object metadata is elaborated on in Sections 3.2, 3.3, 3.4, and 3.5 respectively. Section 3.6 describes the internal structure of the security objects. Section 3.7 describes the way that the security constraints of each of the four *Sec* objects are combined to resolve a request.

3.1 Sec Object Interaction

The trust profile's attribute certificate types track: the associated identity certificate, the attribute certificate issuer, and a timestamp. The attribute certificate types are: affiliation certificates ($AC_{Affiliation}$), data resource access certificates ($AC_{DataResourceAccess}$), data resource confidentiality certificates ($AC_{DataResourceConfidentiality}$), and system confidentiality certificates ($AC_{SystemConfidentiality}$). Affiliation certificates denote current employment with a trusted healthcare provider and signify a thorough manual background check as part of the pre-employment process. Data resource access certificates provide metadata on the role the user possessed during the access, FHIR resource ID, and the system ID representing the FHIR server that serviced the originating request. The data resource confidentiality certificate provides: the confidentiality level of the resource accessed, the FHIR resource ID, and the system ID. The system confidentiality certificate describes the highest level of confidentiality that the certificate subject has accessed on the FHIR server and the system's ID.

In support of trust profile integration, we have modified the HAPI FHIR implementation to enable the creation of a credential expression whose access rules are created based on a configuration. This metadata describes the properties needed in the requestor's trust profile to gain authorization to the resource. The modifications support the creation of multiple credential expressions based on any set of properties specified within the trust profile.

Security metadata for our extension is divided into one of four levels, whose various access rules are combined utilizing the process described in this section to form one credential expression for the entire trust negotiation process. These four levels are:

- *system security* refers to the requirements that the controller must observe in the requestor's trust profile to gain access to any resources
- *resource type security* refers to the protections of an individual type of resource
- *resource security* refers to the actual protection of an individual resource instance on the FHIR server and data within the object
- *patient consent* refers to the ability of a patient to describe which healthcare providers may access each resource, at either the resource type or individual resource level

3.2 System Security Metadata

System security (Sec_{System}) refers to the requirements the controller must observe in the requestor's trust profile to gain access to any resources. This may include a valid affiliation certificate denoting current employment at a trusted healthcare provider and at least one data resource access certificate describing access to a resource under the role requested for the current trust negotiation. *System security* also encompasses the overall highest security clearance the user has been granted on a specific system. As specified in the trust profile model, an identity certificate in a trust profile may have a system confidentiality attribute certificate attached to it that records the highest security clearance previously granted to the trust profile owner by the specific healthcare system that signed it. This certificate is replaced with a newer certificate listing a higher clearance in the event that the controller grants the requestor access to a resource with a higher listed security clearance than the clearance listed in the requestor's system confidentiality attribute certificate. The requestor may be assigned higher security clearances by the FHIR server depending on which trust profile entries the requestor sends to satisfy the generated credential expression. An $AC_{SystemConfidentiality}$ certificate previously digitally signed by the controller may be provided during negotiation to claim a previous confidentiality level assigned by the controller. A system confidentiality level may be assigned based on the perceived damage caused by a potential unauthorized leak of the requested data, and a requestor that meets the confidentiality requirements for portions of the requested resource, but not the entire resource, may result in a *release action (RA)* (Sanzi et al., 2017) that causes the controller to filter data of higher sensitivity from the resource before sending it to the requestor.

3.3 Resource Type Security Metadata

Resource type security (Sec_{Type}) refers to the protection of all of the resources of a given type. Resource types are further divided into base, clinical, and financial resource types (HL7 International, 2019). Each resource type possesses an associated security object that describes the credentials that must be presented by the requestor for the controller to release a resource of the given type. The required credentials are described by a series of *Access History Properties (AHP)*, each describes a single property of access to a sensitive FHIR resource. These credentials are also organized within the security object by the role the requestor assumes for the given trust negotiation transaction. Recall that (Sanzi et al., 2017) specifies that in the initial request for trust profile based trust negotiation, the requestor specifies the role (e.g., family physician, emergency room physician, nurse, billing agent, front desk secretary, etc…) to be assumed for the purposes of negotiation. The controller filters the resources a requestor of a given role accesses based on the perceived needs of a role. For example, a physician role will be allowed to access clinical resources (e.g., summary, diagnostics, medications, care provisions, request and responses) whereas a front desk secretary may be limited to the patient resource (describing the patient's demographic data) under the base category. The role specified by the requestor will also affect the proof the controller requests for assurance of the requestor's membership of the specified role. A family physician requesting a patient's clinical resources may be asked to provide credentials from the trust profile indicating a historical access to the patient's clinical resources whereas a front desk secretary may only have to provide proof of employment (affiliation) via a desk secretary role to access a patient's demographic data.

3.4 Resource Security Metadata

Resource security ($Sec_{Resource}$) protects an individual resource object on the FHIR server and the data within the object. The resource $Sec_{Resource}$ provides security data for is identified within the $Sec_{Resource}$ by a matching identifier. $Sec_{Resource}$ is similar to Sec_{Type} with the exception that it protects an individual resource instance as contrasted to an entire collection of resources of a certain type, increasing the granularity with which a resource is protected. When the request for a FHIR object through trust negotiation is first received, the $Sec_{Resource}$ object attached to the requested FHIR object is retrieved by matching the FHIR ID.

3.5 Patient Consent Security Metadata

Patient consent security ($Sec_{Consent}$) allows the patient described by the FHIR object to provide input as to which healthcare providers may access each resource, at either the resource type or individual resource level. Our $Sec_{Consent}$ security object is based on the principles of patient consent (The Office of the National Coordinator for Health Information Technology, 2019) outlined by The Office of the National Coordinator for Health Information Technology (ONC). Patient consent methods allow patients to consent to HIE among multiple healthcare providers by allowing patients to note when and how their health data is shared whether their health data is shared for treatment, bill payment, or general healthcare operations. Our patient consent object overrides other security objects when present, allowing the patient to have final authority over the disclosure of the health record. The $Sec_{Consent}$ object is built by the patient and attached to the patient's records within a FHIR system, allowing the patient to provide input as to which trust profile credentials are necessary during trust negotiation for the release of different types of FHIR data and FHIR resources.

The patient interacts with the $Sec_{Consent}$ object via a patient portal provided by the healthcare organization maintaining the FHIR server. The patient portal follows the ONC's meaningful consent guidelines (The Office of the National Coordinator for Health Information Technology, 2018) and describes the patient's choices as well as the implication of their options regarding what data will be released to which types of providers under different circumstances. The patient portal interface provided by the healthcare organization presents multiple options that cover different use cases along with descriptions for which healthcare providers have access to the patient's FHIR resources depending on the options chosen. This simplifies the selection process for a patient, allowing the patient to fully comprehend the implications of each choice without needing a deep understanding of trust profiles or trust negotiation. At the healthcare provider's discretion, more granular interfaces can be made available to the patient should the patient have the knowledge to construct more detailed $Sec_{Consent}$ objects. The $Sec_{Consent}$ object contains the same format as the $Sec_{Resource}$ and Sec_{Type} objects with the restriction that a $Sec_{Consent}$ object is only attached to a FHIR resource via ID if the resource ID's patient identifier matches the identifier of the patient creating the $Sec_{Consent}$ object. Additionally, the patient may include multiple instances of a healthcare professional's public key from a trust profile identity certificate. This allows the patient to identify a healthcare professional as being able to access a portion of the patient's healthcare records if the patient has a pre-existing relationship. If a public key is listed as a potential credential to gain access to a FHIR resource, the healthcare professional attempting to access the resource proves ownership of the public key by proving ownership of the associated private key. This is done by digitally signing a message with the private key during trust negotiation in accordance with public key infrastructure.

3.6 Security Object Structure

Each *Sec* object contains a tree structure as illustrated with the Sec_{Type} example in Fig. 2 detailing the specific credentials that must be presented to the controller on a per role basis, as well as release actions required for the release of the resource based on which parts of the credential expression are satisfied. A *Sec* object is organized into a tree structure. The root of the tree contains an identifier that defines the type of *Sec* object. The Sec_{System}, Sec_{Type}, $Sec_{Resource}$, and $Sec_{Consent}$ objects also provide the system ID, resource type ID, resource ID, or patient ID, respectively, that they are responsible for protecting. The next level of the tree represented by the top branch in Fig. 2, which provides a supported list of roles capable of retrieving data of the requested *Sec* object. For example, a Sec_{System} object contains a complete listing of all of the roles that are able to access any sensitive data protected by the controller, whereas Sec_{Type} for an Observation will only contain the roles that are capable of accessing an Observation. Each role contains subtrees representing the AHPs that the controller must request from the requestor's trust profile to grant access if the requestor is assuming that role. An AHP is noted as required, in which case its absence in the credentials during trust negotiation causes trust negotiation to fail; or optional, which allows the FHIR object to be released even if not present. The existence of required or optional AHPs allows more flexibility in the ability to build trust between the requestor and controller by requesting the presence of an AHP without requiring it, while still providing a baseline for AHPs that must be present for the controller to trust the requestor with the release of the requested FHIR object.

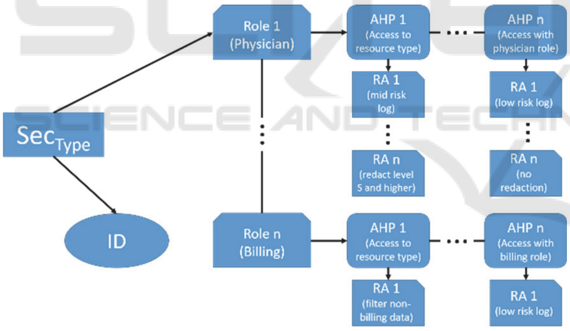
Role 1
(Physician)
AHP 1
(Access to resource type)
AHP n
(Access with physician role)
RA 1
(mid risk log)
RA 1
(low risk log)
SecType
RA n
(redact level S and higher)
RA n
(no redaction)
ID
Role n
(Billing)
AHP 1
(Access to resource type)
AHP n
(Access with billing role)
RA 1
(filter non-billing data)
RA 1
(low risk log)

Figure 2: An example Sec object structure.

Each AHP has an optional set of release actions, RAs, attached to it that describes ancillary actions the controller must take to approve the satisfaction of the AHP requirement by a credential in the requestor's trust profile. The RA for an AHP optionally has: potential additions, modifications, or redactions of the resource before release to the requestor; or specifies side effect actions such as noting the release of the resource at certain risk levels in a multi-level audit log and dispatching audit notifications to the healthcare organization's local security auditor for immediate review. Additions to the resource include contextual data not requested but necessary to understand the resource, e.g., a program for reading X-Ray scans. Modifications to the resource include changes such as translating embedded data into a standard format. Redactions may occur if the requestor's credentials meet a trust level sufficient to access parts of a resource, but not the entire resource. In this case, the sensitive data is redacted, allowing the requestor to obtain the subset of useful data that the requestor is authorized to access. Integrating an RA into a resource is a method that the controller uses to increase the rate of trust negotiation success and disseminate requested PHI without compromising patient security.

Conceptually, each AHP listed in a *Sec* object represents an entry in the requestor's trust profile that proves successful, secure handling of the type of *Sec* object by the role. The healthcare organization that shares the PHI is responsible for determining the AHPs necessary as to whether a requestor is trustworthy. A requestor making a request under a family physician role for their patient's EHR data located at a remote healthcare organization could result in the following requested AHPs and RAs:

- Sec_{System}: Affiliation with any healthcare provider (RA: log as high risk)
- Sec_{Type}: Past access to a resource of the same type within the last year (RA: reduce log level to medium risk, redact resource data with sensitivity: S or higher)
- $Sec_{Resource}$: Optional: Past access to a resource belonging to the patient within the last two years (RA: reduce log level to low risk, audit notification not required, no redaction required)
- $Sec_{Consent}$: Affiliation with a listed healthcare provider (RA: notify patient of access through a healthcare portal)

3.7 Request Resolution

When a request for trust negotiation is initially received, the controller first retrieves each of the four *Sec* objects that will be associated with the request: the *system* object for the FHIR installation as a whole, the *type* object for the type of resource being requested, the *resource* object for the individual FHIR resource by ID, and, the *consent* object associated with the patient. Each *Sec* object must be satisfied by one or more credentials sent by the requestor to determine the requestor's trustworthiness. When the controller receives a requestor's trust profile credential and has finished verifying the credentials authenticity, an attempt is made to match it against the AHPs in each of the four retrieved *Sec* objects. The controller records which of the AHPs has been satisfied, and creates an SGP based on which AHPs remain unsatisfied to send back to the requestor. All of the four *Sec* objects must be satisfied for the trust negotiation to be successful. A *Sec* object may specify that a particular AHP is optional, thereby increasing trust in the requestor and modifying the release actions accordingly. Additionally, the *Sec* object may define a set of AHPs as optional, but require that at least one be met for the *Sec* object to be satisfied. A single trust profile credential is potentially capable of satisfying multiple AHPs across multiple *Sec* objects. During credential exchange, the controller is continually checking the requestor's credentials and matching them to the *Sec* objects until all of the AHPs are satisfied or the requestor chooses not to send another credential. If the requestor chooses not to send another credential, the controller checks whether all of the four *Sec* objects are satisfied, executes the release actions, and provides the resource and new trust profile credentials. The controller's final set of release actions are resolved hierarchically from Sec_{System} to $Sec_{Resource}$ by beginning with the Sec_{System}*'s* set of release actions and combining with Sec_{Type}*'s* release actions, then $Sec_{Resource}$*'s* release actions. When two RAs conflict at different levels, the RA at the lowest level (closest to the individual resource) takes precedence. The $Sec_{Consent}$*'s* release actions are separated from the other three Sec objects and are always executed as specified by the patient. The *consent* object concerns patient notifications but may also filter access to the patient's resources more strictly or release resources more freely to specific healthcare providers and thus override the other three *Sec* objects. Within a single *Sec* object, each AHP contains a ranking, with higher ranking determining which RA is executed if there is a conflict between two RAs in two satisfied AHPs.

4 HEALTHCARE EXAMPLE

In this section, we demonstrate the operation of a trust profile enhanced FHIR installation by providing an example of an implementation in a healthcare setting in Greater Hartford, Connecticut. Jane is a physician working at Family Medicine Center (FMC) as a family physician. Fig. 3 shows the different interactions of Dr. Jane as she proceeds through the trust profiling process to request permission to access a new FHIR resource at another location that she has not been authorized to. During her career, she has gradually built a trust profile containing an access history that describes access to sensitive data from both her local EHR as displayed in the lower left of Fig. 3 and remote access to EHRs maintained by other healthcare providers in the area. While retrieving her patient's EHR, she discovers that the patient has recently been seen at Hartford Hospital (HH) and a new healthcare record of the FHIR *Observation* resource was generated, represented by the Patient Observation in the top middle of Fig 3. Dr. Jane is unknown to HH and HH has no record of her, but maintains a FHIR installation that supports trust profile based trust negotiation.

Dr. Jane begins by initiating a request for trust negotiation to HH under her family physician role for the patient's FHIR resource, which includes a trust profile credential indicating current affiliation with FMC, and sends it to HH. Dr. Jane is now the requestor. The controller at HH receives the request for trust negotiation, identifies the resource being requested, and extracts the trust profile credentials. The controller must now build the credential expression that defines which trust profile credentials are necessary to release the requested resource to Dr. Jane and the release actions it must perform. The controller identifies the four *Sec* objects represented with ovals along the right side and upper left corner of Fig. 3 that describe the credentials Dr. Jane will need to present. These objects are: HH's Sec_{System} object that describes the credentials necessary to access any FHIR resource from HH, the Sec_{Type} object that describes the credentials necessary to access any *Observation* resource, the $Sec_{Resource}$ object that describes the credentials necessary to access the specific *Observation*, and, the $Sec_{Consent}$ object that describes the credentials the patient requires to access a resource they own. The *Sec* objects, AHPs, and RAs represented to the right of Fig. 3 retrieved are:

- Sec_{System}: Current affiliation with any healthcare provider (RA: log as high risk, send audit notification to local auditor)
- Sec_{Type}: Past access to a resource of the same type within the last year (RA: log as medium risk, redact resource data with sensitivity: S or higher)
- $Sec_{Resource}$: Optional: Past access to a resource belonging to the patient within the last two years (RA: log as low risk, audit notification not required, no redaction required)
- $Sec_{Consent}$: Current affiliation (RA: patient notification) or optionally: affiliation with a listed healthcare provider

The controller matches the initial trust profile credential, affiliation with FMC, against each of the four *Sec* objects (green ovals in Fig. 3). The credential satisfies both the Sec_{System} object and the optional $Sec_{Consent}$ requirement since the patient regularly sees Dr. Jane at FMC. Since not all of the objects are fully satisfied, the controller sends a server governance policy (SGP) to Dr. Jane listing the missing AHPs. Dr. Jane receives the request and sends a trust profile entry describing access to one of the patient's *Observation* resources at FMC occurring three months in the past. The controller receives this request and matches it against each of the four *Sec* objects. This new credential satisfies both the Sec_{Type} and optional $Sec_{Resource}$ since the access to the *Observation* resource matches both the Sec_{Type} requirement of access to an *Observation* resource and the $Sec_{Resource}$ requirement of access to an *Observation* resource belonging to the patient, identified by a patient ID. Having satisfied all of the credentials, the controller processes the release actions of each *Sec* object starting with Sec_{System} and ending with $Sec_{Consent}$. $Sec_{Resource}$'s log requirements override the Sec_{System} and Sec_{Type} log requirements, logging the access as low risk, no redaction being performed, and overriding the audit notification requirement. The affiliation with a listed healthcare provider AHP of the $Sec_{Consent}$ object was the AHP that was satisfied and carries no release action. The controller notifies Dr. Jane that the trust negotiation was successful, retrieves the requested *Observation* resource, and generates new trust profile credentials describing Dr. Jane's access to the resource. The requested resource and new credentials are sent to Dr. Jane, who can now examine the patient's observations from HH and add the new credentials to her trust profile.

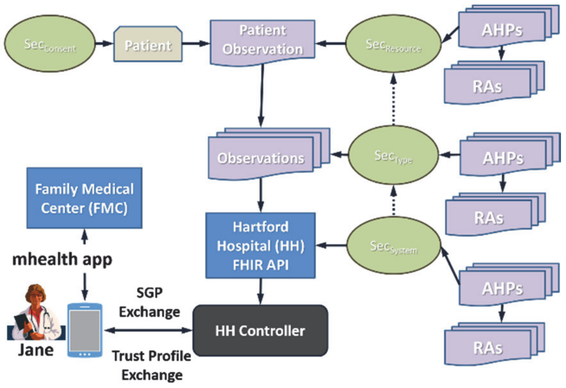

Figure 3: Trust negotiation example.

5 CONCLUSION AND ONGOING RESEARCH

In this paper, we have outlined a methodology for integrating trust profile based trust negotiation into the FHIR environment supported by an example of its operation in a real world healthcare scenario that extends our prior work on trust profiles (Sanzi et al., 2017). The methodology involves applying security constraints for the specific resource requested by the requestor. The security objects request access history properties to allow access at the system level, resource type level, individual resource level, and the patient consent level. The trust profile credentials are composed into a single credential expression by the controller utilizing the requirements listed at each level to provide a complete list of trust profile requirements and to describe release actions for the controller to execute to ensure a valid, secure transaction. Combining the security objects allows the healthcare organization operating a FHIR installation to provide granular permissions for accessing sensitive health data while acknowledging the patient's right to provide guidance towards the dissemination of the patient's EHR. Release actions provide alternatives for trust profile requirements, allowing for proper release of PHI when required. This increased ability to share healthcare data among providers increases patient recovery and satisfaction.

In support of our trust profile effort, we have modified a mobile health application created in support of a Connecticut bill (Connecticut General Assembly, 2015) that is used for concussion management of students in grades kindergarten through high school by school nurses, athletic trainers, parents, etc., to include the integrated trust profile process as described in Section 3 with FHIR. This mobile health application for concussion management is integrated through the HAPI FHIR server to the OpenEMR electronic medical record (https://www.open-emr.org/) with the ability to take information out of OpenEMR using its PHP API and return observation and patient objects for the students that have concussions. Our current research is transitioning our model ideas in Section 3 in order to fully realize the ability to access FHIR resources for doing the trust management as described in Section 3 and illustrated in the healthcare example in Section 4.

REFERENCES

Bell, D. E., & La Padula, L. J. (1976). *Secure Computer Systems: Unified Exposition and Multics Interpretation.* Bedford, Mass.: MITRE Corp.

Cerner. (2020, January 4). *Home*. Retrieved from https://www.cerner.com/

Connecticut General Assembly. (2015). *Substitute for Raised H.B. No. 6722*. Retrieved from https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2015&bill_num=6722

Cooper et al. (2008, May). *Internet X.509 Public Key Infrastructure Certificate.* Retrieved from https://tools.ietf.org/html/rfc5280

De Pietro, C., & Francetic, I. (2018). E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks. *Health Policy, 122*(2), 69-74. doi:10.1016/j.healthpol.2017.11.005

Elkhodr et al. (2011). Enhancing the security of mobile health monitoring systems through trust negotiations. *Local Computer Networks (LCN), 2011 IEEE 36th Converence on* (pp. 754-757). Bonn: IEEE.

Epic Systems Corporation. (2020, January 4). *Epic*. Retrieved from https://www.epic.com/

Farrell, S., & Housley, R. (2002, April). *An Internet Attribute Certificate Profile for Authorization*. Retrieved from The Internet Engineering Task Force (IETF®): https://www.ietf.org/rfc/rfc3281.txt

Ferraiolo et al. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC), 4*(3), 224–274.

HAPI FHIR. (2016). *Server Interceptors.* Retrieved January 10 2020, from https://web.archive.org/web/20190512185820/http://hapifhir.io/doc_rest_server_interceptor.html

HAPI FHIR. (2020). *HAPI FHIR - The Open Source FHIR API for Java*. Retrieved January 10, 2020, from https://hapifhir.io/

Health Level 7 International. (2013). *Confidentiality*. Retrieved January 19, 2020, from http://www.hl7.org/documentcenter/public/standards/vocabulary/vocabulary_tables/infrastructure/vocabulary/Confidentiality.html

Health Level Seven International. (2013). *Unique ID, R1 - 3. HCS Guide Final 2013 0322 JMD.pdf.* Retrieved January 16, 2020, from https://www.hl7.org/documentcenter/public/wg/secure/3.%20HCS%20Guide%20Final%202013%200322%20JMD.pdf

HL7 International. (2019, January 4). *Health Level Seven International*. Retrieved from https://www.hl7.org/

HL7 International. (2019, November 1). *Resourcelist - FHIR v4.0.1*. Retrieved January 19, 2020, from https://www.hl7.org/fhir/resourcelist.html

HL7 International. (2020). *Index - FHIR v4.0.1*. Retrieved January 10, 2020, from http://hl7.org/fhir/

Li, J., & Li, N. (2006, Oct.-Dec.). OACerts: Oblivious Attribute Certificates. *IEEE Transactions on Dependable and Secure Computing, 3*(4), 340-352.

Posnack, S., & Barker, W. (2018, October 1). *Health IT Buzz*. Retrieved January 4, 2019, from https://www.healthit.gov/buzz-blog/interoperability/heat-wave-the-u-s-is-poised-to-catch-fhir-in-2019

Ryutov et al. (2005). Adaptive Trust Negotiation and Access Control. *SACMAT '05 Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 139-146). New York City: ACM New York, NY, USA ©2005.

Sanzi et al. (2017). Integrating Trust Profiles, Trust Negotiation, and Attribute Based Access Control. *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 177-184). San Francisco: IEEE. doi:10.1109/MobileCloud.2017.30

Sanzi et al. (November 2016). Trust Profiling to Enable Adaptive Trust Negotiation in Mobile Devices. In S. Mukherja (Ed.), *Mobile Application Development, Usability, and Security* (pp. 95-116). IGI Global.

Sanzi, E., & Demurjian, S. (May 2016). Identification and Adaptive Trust Negotiation in Interconnected Systems. In A. Malik, A. Anjum, & B. Raza (Eds.), *Innovative Solutions for Access Control Management* (pp. 33-65). IGI Global.

The Office of the National Coordinator for Health Information Technology. (2018, September 19). *Meaningful Consent Overview | HealthIT.gov*. Retrieved January 24, 2020, from https://www.healthit.gov/topic/meaningful-consent-overview

The Office of the National Coordinator for Health Information Technology. (2019, April 17). *Patient Consent for Electronic Health Information Exchange | HealthIT.gov*. Retrieved January 24, 2020, from https://www.healthit.gov/topic/patient-consent-electronic-health-information-exchange

U.S. Department of Veterans Affairs - Office of Public and Intergovernmental Affairs. (2019, July 29). *VA achieves critical milestone in its Electronic Health Record Modernization Program.* Retrieved January 4, 2020, from https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5286

Vawdrey et al. (2003). Trust Negotiation for Authentication and Authorization in Healthcare Information Systems. *Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE* (pp. 1406-1409). IEEE.

Winsborough et al. (2000). Automated trust negotiation. *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings. 1*, pp. 88 - 102. Hilton Head, SC: IEEE. doi:10.1109/DISCEX.2000.824965

Yasnoff, W. A. (2015). *A Feasible and Sustainable Approach to Health Information Infrastructure Via Mobile Devices.* Retrieved Oct. 23, 2015, from http://mediasite.uchc.edu/mediasite41/Play/b409b6fea70b4ec5b3fc34355340ac521d