Novel Information Sharing Syntax for Data Sharing between Police and Community Partners, using Role-based Security

Omair Uthmani[1], Prof William Buchanan[1], Alistair Lawson[1], Dr Christoph Thuemmler (MD)[1], Supt Russell Scott[2], Anne Lavery[2] and Chris Mooney[3]

[1] Centre for Distributed Computing, Networks and Security, Edinburgh Napier University, Edinburgh, UK

[2] National Intelligence Model Development Team, Scottish Police College, Kincardine, UK

[3] Information and Intelligence Unit, Glasgow Community & Safety Services, Glasgow, UK

o.uthmani@napier.ac.uk; w.buchanan@napier.ac.uk; al.lawson@napier.ac.uk
russell.scott@spsa.pnn.police.uk; anne.lavery@spsa.pnn.police.uk;
chris.mooney@strathclyde.pnn.police.uk

Abstract

The exchange of information between the police and community partners forms a central aspect of effective community service provision. In the context of policing, a robust and timely communications mechanism is required between police agencies and community partner domains, including: Primary healthcare (such as a Family Physician or a General Practitioner); Secondary healthcare (such as hospitals); Social Services; Education; and Fire and Rescue services. Investigations into high-profile cases such as the Victoria Climbié murder in 2000, the murders of Holly Wells and Jessica Chapman in 2002, and, more recently, the death of baby Peter Connelly through child abuse in 2007, highlight the requirement for a robust information-sharing framework. This paper presents a novel syntax that supports information-sharing requests, within strict data-sharing policy definitions. Such requests may form the basis for any information-sharing agreement that can exist between the police and their community partners. It defines a role-based architecture, with partner domains, with a syntax for the effective and efficient information sharing, using SPoC (Single Point-of-Contact) agents to control information exchange. The application of policy definitions using rules within these SPoCs is inspired by network firewall rules and thus define information exchange permissions. These rules can be implemented by software filtering agents that act as information gateways between partner domains. Roles are exposed from each domain to give the rights to exchange information as defined within the policy definition. This work involves collaboration with the Scottish Police, as part of the Scottish Institute for Policing Research (SIPR), and aims to improve the safety of individuals by reducing risks to the community using enhanced information-sharing mechanisms.

Keywords

Information sharing syntax; intelligence model; security policy implementation; Role-based security; Police and Public Services; community risks

Introduction

There is need for robust and timely communications between law-enforcement agencies (the police) and their community partners (health care, social work, regional/state administration and other partner agencies). This need arises from awareness that an effective and responsive service requires cooperation on global, national and local levels.

Established national and international agreements for information-sharing include initiatives to share financial and taxation information to combat corruption, money laundering, human trafficking, terrorism and so on. The increasingly global nature of criminal activity, especially in the areas of smuggling and terrorism, has encouraged greater collaboration among law-enforcement agencies [Koenig 2001]. The Serious Organised Crime Agency (SOCA) in the UK, for example, liaises regularly with its counterparts in other regions including the European Law Enforcement Organisation (Europol) and the International Criminal Police Organization (Interpol). In the United States the aftermath of the 11th of September 2001 terrorist attacks emphasised the need for robust inter-agency communication and prompted the creation of the Department of Homeland Security (DHS) [Feinberg 2002]. A key driver for the formation of the DHS was to overcome barriers to cooperation and increasing information sharing among government agencies.

On a local level, agencies are actively encouraged by governments [Police and Crime Standards Directorate (PCSD) and Home Office 2007] to form partnerships and collaborate to ensure provision of effective community services. Working in partnership by sharing information has been particularly successful in public services [Clarence & Painter 1998], [Hudson et al. 1999]. Often, partnership working is a requirement mandated by legal directives. In the UK, for example, Acts of Parliament such as the Health and Social Care Act 2001, Police Reform Act 2002, Community Care Act 2003 and the Children Act 2004 all necessitate information sharing among partner agencies. Where this collaboration fails, the results can increase community risks, and, at worst, can result in tragedy. Examples of this breakdown in communication in the UK include: the Victoria Climbié murder in 2000 [Lord Laming 2003]; the murders of Holly Wells and Jessica Chapman in 2002 [Bichard 2004]; and the death of baby Peter Connelly through child abuse in 2007 [Lord Laming 2009]. Inquiries into these cases point to significant weaknesses in communication between community partner agencies.

Barriers to forming effective partnerships and information exchange include lack of trust between organisations; lack of understanding of policies and legislation; and disparate communication systems. The issue of trust mainly arises from traditional rivalries [Willem & Buelens 2007] between organisations that view each other as competitors rather than collaborators. However, evidence suggests that increased government encouragement to collaborate [Daley 2009], in the form of incentives and legal obligations, has helped in alleviating this situation. Initiatives that highlight best practices and procedures, such as the guidance on the Management of Police Information (MoPI) [Association of Chief Police Officers in Scotland (ACPOS) 2008] within the Scottish and other UK police services, also simplify the interpretation of policies and legal requirements. This ease of interpretation of policies, in turn, alleviates the risks agencies face from non-compliance [Thomas & Walport 2008] and, thus, further aids collaboration.

Initiatives in the area of e-government seek to address the issue of disparate systems by providing a standardised communication framework. These include the e-Government Interoperability Framework (e-GIF) [Cabinet Office 2005] in the UK, the SAGA initiative [Federal Ministry of the Interior 2003] in Germany and the National Information Exchange Model (NIEM) [NIEM Program Management Office 2007] in the US among many others. These initiatives attempt to define a common framework for information exchange and usually involve agencies, private industry, and different levels of government. The NIEM architecture, for example, provides an excellent infrastructure for defining information exchange schema and has the flexibility to integrate with multiple domains, including Emergency Management, Immigration and Intelligence. However, the scope associated with NIEM and other initiatives also makes them complex to implement, especially for smaller organisations and agencies. In addition, as these systems are still being developed and implemented, their success is difficult to determine at this time.

Information Sharing Framework

The syntax proposed in this paper builds upon the principles of best practice within the Scottish Police, such as those highlighted in the guidance on the Management of Police Information (MoPI). This guidance defines principles for police information management, including the processes and procedures under which information may be requested by, and shared with, partner agencies. Thus, MoPI helps to identify organisational policies and legal compliance issues that affect police information sharing.

Once the need to share information with a partner agency is identified and affected procedures and compliance issues defined, the principles highlighted in MoPI can be used to construct an Information-Sharing Agreement (ISA). ISA's define the agreed specific rules, derived from policies, that direct the recording, access, review and dissemination of information between partner agencies. Usually, agencies that have similar functions also have similar ISAs and can be grouped together into domains. From a Scottish policing perspective, common information sharing domains include Police services (POL), Social Services (SOC), Primary healthcare (HCP), Secondary healthcare (HCS), Education (EDU), and Fire and Rescue (FIRE). MoPI also outlines the concept of a Single Point-of-Contact (SPoC), which describes the individuals who are designated as main contacts for the exchange of information between domains. Any exchange of information between the domains, therefore, needs to occur through the designated SPoCs.

Single Point of Contact (SPoC)

Figure 1 illustrates the Single Point of Contact (SPoC) concept described in the guidance on the Management of Police Information (MoPI), which is implemented as software agents that serve as gateways for information requests. The function of these SPoC agents is inspired by firewalls within a computer network. At a basic level, firewalls use a defined set of rules to either permit or deny network traffic. Similarly, SPoC agents validate requests for information exchange based on rules, derived from organisational policies and legislative requirements, as defined in Information-Sharing Agreements (ISA). This means that the agent attempts to match a request for information exchange against the rules defined in the set of rules in the ISA. If the request does not match a rule, the agent will then attempts to match the request against the next rule and so on. Once match is found, the agent will carry out the action (permit or deny), as defined by that rule, and end the searching (as a firewall would). If no matching rule is found in the set, the agent will deny the request. This is similar to the idea of an *implicit* deny criterion used by firewalls where no matching rule is found. In the case that a request is denied, the agent will return information indicating the reason for the denial. The policies defined in the ISA can take the form of restrictions such as limits on the number of search items returned, specified timeframe of validity for an incoming request, and so on.

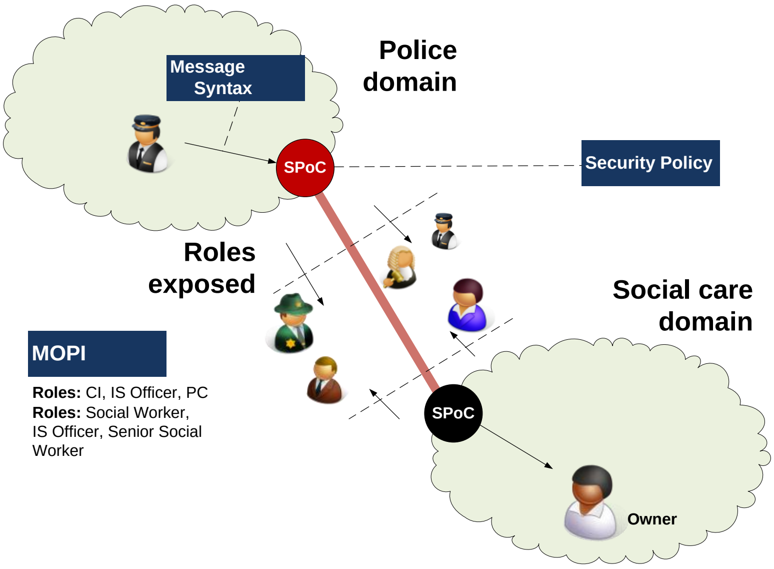


Figure 1: Overview of the architecture

Role-Based System

Figure 2 outlines the general architecture of the proposed role-based system. A core part of the Information-Sharing Agreement (ISA) is to specify those will have access to the shared information. Typically, this involves identifying functional roles that need to access information in order to complete a defined task or job. The information exchange syntax thus uses a hierarchy within domains and roles exposed between domains to facilitate the exchange of information. For example, Analyst (ANA) may be an exposed role from the Child Abuse Investigation (CAI) organisational unit in the Police domain (POL). This role is represented as POL.CAI.ANA, illustrating the full hierarchy. Similarly, an Inspector (INS) from the Missing Persons (MPR) business area of the Police domain would then be represented as POL.MPR.INS. For a Social Worker (SW) role exposed from the Children Day Care Service (CDC) of the Social Services (SOC) domain, the representation would be SOC.CDC.SW. Essentially an exposed role is one that could has permissions for information exchange from another domain. For example, if Social Workers (SOC.CDC.SW) are allowed to request information from Police (POL), then the SOC.CDC.SW role would be defined in the ISA as having permissions for this action. Thus, the SOC.CDC.SW role is exposed from the Social Services domain to the Police domain.

The use of an exposed role also requires an identity mechanism which has the trust of the two domains involved. For next generation systems, Kerberos provides the best method of separating rights from identity, and will provide a more scalable infrastructure. As Figure 2 illustrates the IP is trusted by the two domains, and a ticket is generated which is provided to each of the SPoCs in order to validate the role. Third-party federated identity providers may also be used to provide independent role verification between domains. This system permits the identity verification of a requester to be decoupled from the request for information. A federated model allows for a range of identity providers to be used so that a strong authentication is implemented for highly classified information while a weaker authentication may suffice for less sensitive information.

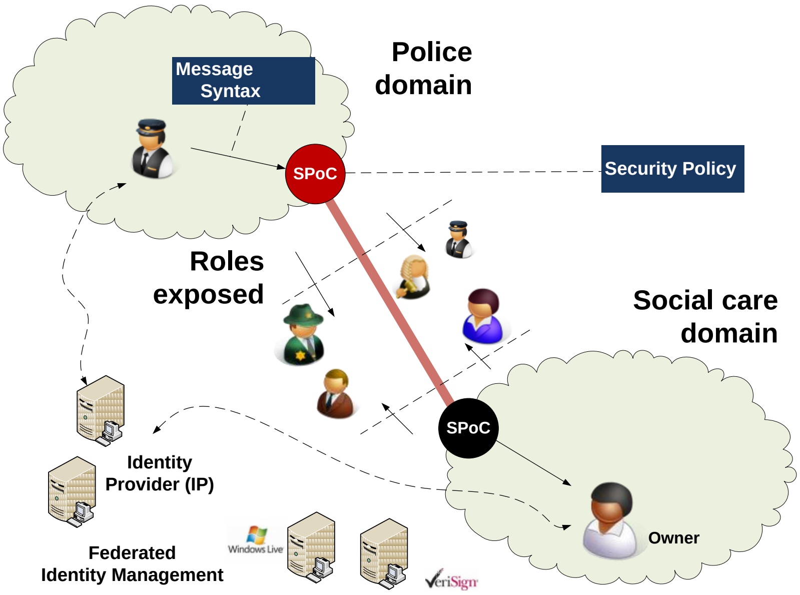
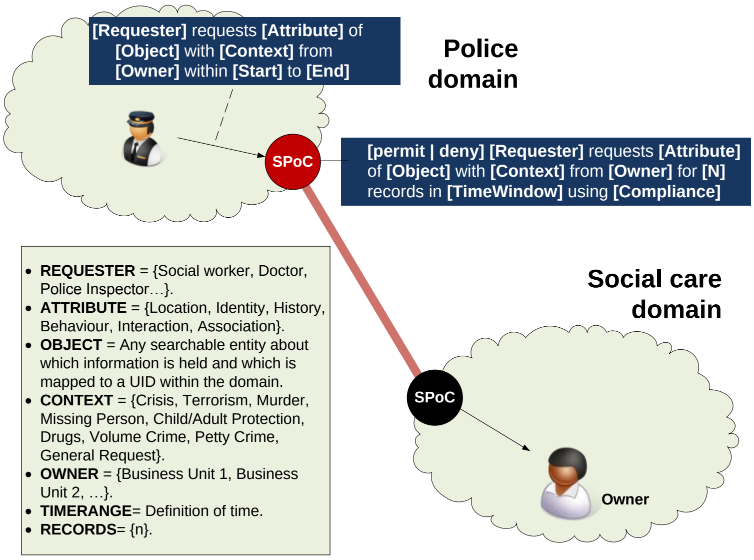


Figure 2: Federated Identity Management

Syntax

A syntactic approach to the concept of information-exchange simplifies the creation and implementation of rules. The main reason for this approach is the vast number of disparate information systems that various police divisions and partner agencies use, which can cause difficulties relating to translation and the resulting misunderstandings. The result, often, is that valuable semantics can be lost in the exchange, which degrades the efficiency of the information-sharing mechanism and undermines the objectives for which the information was being shared in the first place. Common logical definitions, which constrain possible interpretations of any given concept to a finite set, therefore, need to be agreed upon before communication can occur. Figure 3 outlines the syntax of the rule request and of the policy rule, which provide a close match to each other. Most of the fields within these rules are defined within, and generated from, the ISA, but the [Object] field is kept as a free format field, in order that the structure of the databases within the domain does not have to be exposed to other domains. All of the other fields within the rules are thus used to match the request.


[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]
Police domain
SPoC
[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]
Social care domain
SPoC
Owner

- **REQUESTER** = {Social worker, Doctor, Police Inspector…}.
- **ATTRIBUTE** = {Location, Identity, History, Behaviour, Interaction, Association}.
- **OBJECT** = Any searchable entity about which information is held and which is mapped to a UID within the domain.
- **CONTEXT** = {Crisis, Terrorism, Murder, Missing Person, Child/Adult Protection, Drugs, Volume Crime, Petty Crime, General Request}.
- **OWNER** = {Business Unit 1, Business Unit 2, …}.
- **TIMERANGE**= Definition of time.
- **RECORDS**= {n}.

Figure 3: Overview of request and policy implementation syntax

Basing the rule syntax on that can be easily interpreted allows easier rule creation and reduces the possibility for misunderstandings, while allowing the opportunity to inform the structure of the ISA high level policy document. Adding key security elements to this structure yields the proposed syntax for policy rules which are applied into the SPoC:

[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]

A similar matching syntax can then be applied to the request messages:

[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]

Elements of this syntax are defined as:

- **[permit | deny]** This is part of the rule syntax which indicates the action of the rule and defines whether a message meeting the rule criteria will be permitted or denied.
- **Requester** This identifies an exposed role defined in the ISA. For example, this role might be General Practitioner (FAMDOC) or Nurse (NRS), in Primary healthcare (HCP) or a Detective Constable (DETCST) in Police services (POL) domain. The hierarchical format for depicting roles is:

  (Domain).(Organisational Unit).(Organisational Sub-Unit)…Role

  The number of organisational units and sub-units depends on the hierarchy in the domain. For example, a Detective Constable (DETCST) in the Child Abuse Investigation (CAI) organisational unit of the Police (POL) domain may be represented as:

  POL.CAI.DETCST
- **Object**. This refers to any entity about which information is held, including people, vehicles, events and so on. It is a free-form field, where the object definition is not actually defined within the policy rule definition.
- **Attribute**. This is a unit of information describing an Object. Attributes may include details about location (address, mobile phone tracking), identity (name, insurance number), history (prior convictions, documented allegations), behaviour (calm, violent) and association (group memberships, known associates).
- **Context**. This identifies the reason why the information is being shared. The context also governs the level of access and permissions associated with information exchange and, hence, affects the priority accorded to information requests. For example, the Emergency context signifies a threat to life or threat of violence and will require a higher priority allocation than a Vandalism context.
- **Owner**. Defines a role with sufficient privileges to manage all aspects of an information element. The owner has the authority to allow or deny access to an information element, as required by legislation and defined responsibilities. Use of the term owner in this context implies custodianship. This means that the information owner will be responsible for maintaining the integrity (correctness), availability (access) and confidentiality (privacy) of all attributes and objects under their control. In the police context, this role is usually held by an officer of Chief Police Officer rank, or a person delegated by them.
- **[N] records in [TimeWindow]** This is a part of the rule syntax that defines the number of records permitted over a period of time, where [N] can be any positive integer, and[TimeWindow] uses the ISO 8601 Coordinated Universal Time (UTC) format (PYYYY-MM-DDThh:mm:ss).
- **[Compliance]** This is part of the rule syntax that refers to policies and legislative requirements that affect the exchange of information. Common legal requirements affecting information exchange include the Data Protection Act, the Human Rights Act, the Freedom of Information Act, and so on.
- **[Start]** This is part of the request that identifies the start of the date/time period over which sharing is requested, such as for ISO 8601 Coordinated Universal Time (UTC) standard.
- **[End]** This is part of the request that identifies the end of the date/time period over which sharing is requested, such as for ISO 8601 Coordinated Universal Time (UTC) standard.

Object search field

The object search field is free-form, and aims to try and identify the target of the search. If the search field for the object is too wide ranging (such as for “Fred Smith”), the request might go through the SPoC, but when the records are gathered within the Requested domain, the number of records generated might exceed those defined in the policy, and an error will be return. It would then be up to the Requestor to focus their search, and try and reduce the number of records to an allowable number. In the example in Figure 4, the requested rule breaches policy as 100 records have been returned. A subsequent query could ask for [John Fred Doe] which might only return five records, which is within the policy limits. Thus a request can go through a SPoC, but the actual return of the records might still be blocked, based on the number of records that are returned.

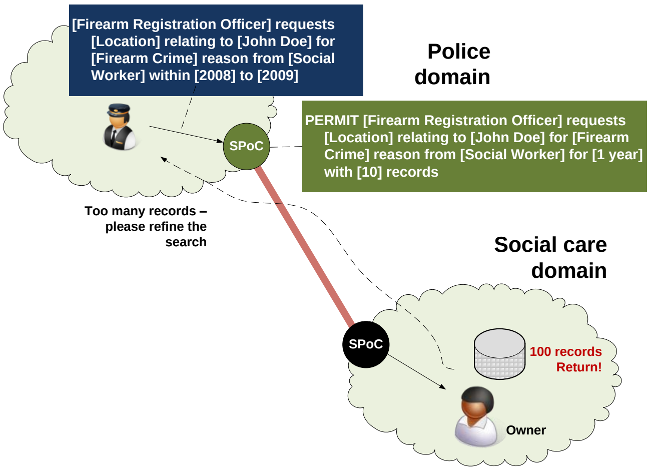

[Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] within [2008] to [2009]
Police domain
SPoC
PERMIT [Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] for [1 year] with [10] records
Too many records – please refine the search
Social care domain
SPoC
100 records Return!
Owner

Figure 4: Context definition

Context and release of information

A key novelty in the proposed system is the use of context for a request, where the ISA will define rights based on the context of the request. For example the rights to data will increase with the context of a missing persons query than for a trivial access to data. It is thus important that the context levels, and associated rights, are clearly defined in the ISA, so that they can be defined within the implementation of the policy. The workflow also need to be carefully defined for the authorization of the context levels, as increasing them normally defines an increased level of access to data. All of the access, though, are audited by the SPoC so that accesses to higher levels of privilege might have to show evidence at a future time. For the release of the information, as illustrated in Figure 6, their also needs to be definition of the anonymization for a given request type, and that there is some workflow that allows a human to possibly check some outgoing results, as anonymization processes might not work correctly.

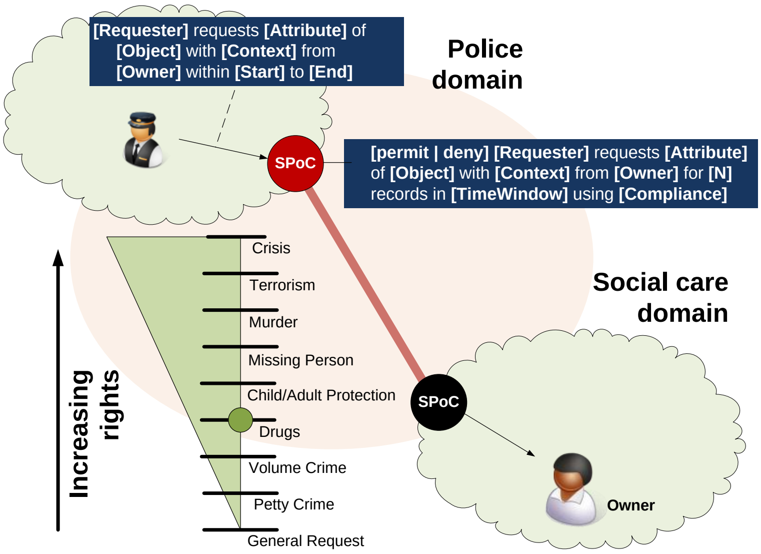

[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]
Police domain
SPoC
[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]
Crisis
Terrorism
Murder
Missing Person
Child/Adult Protection
Drugs
Volume Crime
Petty Crime
General Request
Increasing rights
Social care domain
SPoC
Owner

Figure 5: Context definition

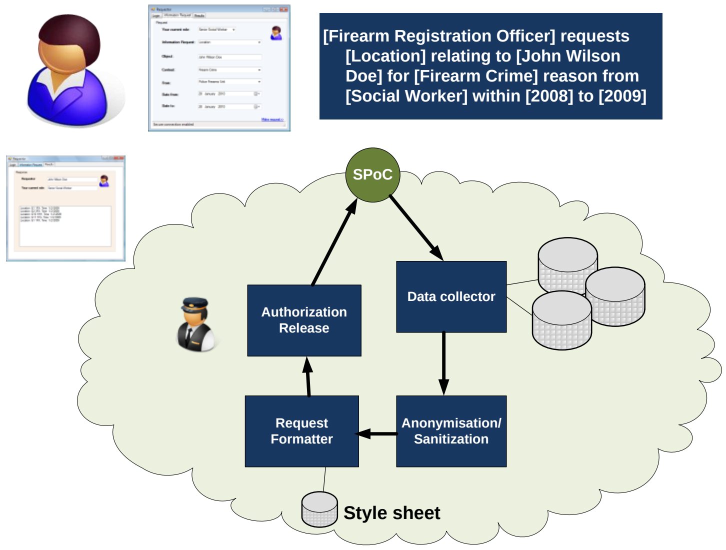

[Firearm Registration Officer] requests [Location] relating to [John Wilson Doe] for [Firearm Crime] reason from [Social Worker] within [2008] to [2009]

Figure 6: Release of information

Example Scenarios

Rules may be used to explicitly permit or deny information exchange requests made by an exposed role. For example, a Senior Family Physician (Requester role=FAMDOCSEN) in Primary healthcare (Requester domain=HCP) is allowed to request a person's medical test results (attribute=MEDTST), from a Laboratory (Owner organisational Sub-unit=LAB) located in a Hospital (Owner organisational unit=HOSP) in Secondary healthcare (Owner domain=HCS), where the person (Object=PERSON) is a patient (Context=PATIENT). A Junior Family Physician (FAMDOCJUN) role from the same domain is not allowed to request this information. These information exchange policies can be used to derive an explicit permit rule (Rule 1) for the FAMDOCSEN role and an explicit deny rule (Rule 2) for the FAMDOCJUN role. These rules would be defined in the Information-Sharing Agreement (ISA) and processed by the SPoC agent (where [PERSON] will be the free-form search field):

Rule 1: **[permit] [HCP.FAMDOCSEN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] for [N] records in [TimeWindow] using [Compliance]**

Rule 2: **[deny] [HCP.FAMDOCJUN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] for [N] records in [TimeWindow] using [Compliance]**

Given the above rules, the following requests may be considered:

Req. 1: **[HCP.FAMDOCSEN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] within [Start] to [End]**

Req. 2: **[HCP.FAMDOCJUN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] within [Start] to [End]**

Thus, a request made by a Senior Family Physician (Request 1) would match Rule 1 and be permitted by the SPoC agent. A similar request made by a Junior Family Physician (Request 2) would match Rule 2 and be denied by the SPoC. In the case of Request 2, the SPoC may return the following message:

Junior Family Physician role does not have permission to access the requested resource.

There may be instances where the ISA only contains an explicit permit rule for a specific role. Any other role would not match this rule and would be implicitly denied. For the previous example, if only Rule 1 was defined in the ISA, then Request 2, not matching any defined rules, would be implicitly denied by the SPoC. In this case, the SPoC may return the following message:

Junior Family Physician is not a defined role in Information-Sharing Agreement.

The context of a request for information exchange affects how the request is handled. For example, a Detective Constable (Requester role=DETCST) in the Domestic Violence (Requester organisational unit=DOM) area in Police services (Requester domain=POL) is allowed to request a person's (Object=PERSON) behaviour information (Attribute=BEHAVIOUR) from the Rehabilitation Support organisation (Owner organisational unit=REHAB) in Social Services (Owner domain=SOC), if this is in relation to a domestic violence investigation (Context=DOM.INVST). This following rule may be derived from this policy:

Rule 3: **[permit] [POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [DOM.INVST] from [SOC.REHAB] for [N] records in [TimeWindow] using [Compliance]**

Thus, the following request, Request 3, made by a Detective Constable would match Rule 3 and be permitted by the SPoC:

Request 3: **[POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [DOM.INVST] from [SOC.REHAB] within [Start] to [End]**

However, if the Detective Constable requested this information in relation to a vehicle parking offence (Context=VPO), as in Request 4, the request would not match a defined rule and be denied by the SPoC.

Request 4: **[POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [VPO] from [SOC.REHAB] within [Start] to [End]**

In this case, the SPoC may return the following message:

Vehicle Parking Offence is not a defined role in Information-Sharing Agreement.

Conclusion

The proposed syntax for information exchange builds upon the best practice principles of the Scottish Police, as outlined in the guidance on the Management of Police Information (MoPI), and incorporates formal data sharing rules as specified in Information-Sharing Agreements (ISAs). It uses a modified concept of SPoC agents that use rules derived from organisational policies and legislative requirements to manage information exchange between partner domains. Thus, the proposed syntax offers a mechanism to automate the information exchange process which integrates with existing systems and policies. SPoC agents ensure compliance with legislation and domain policies and integration with workflow of the roles involved. Currently work is being undertaken on defining use-cases for the interchange of information between the social care and the police domains, as these are possible easier domains to define information exchange. The aim is to show that effective interchange can occur, while using the context field to clearly define the requirements for escalated rights to information. This exchange can thus exist without actually revealing the structure of the databases in each domain, where developers in the domain only require to match the information request syntax formats (as defined within the ISA) to requests for data on their databases.

References

Association of Chief Police Officers in Scotland (ACPOS) (2008), ‘ACPOS Guidance on The Management of Police Information’, The ACPOS NIM Development Project.

Bichard, M. (2004), ‘Bichard Inquiry Report’.

Cabinet Office (2005), *e-Government Interoperability Framework Version 6.1*, e-Government Unit. http://www.govtalk.gov.uk/

Clarence, E. & Painter, C. (1998), ‘Public services under new labour: collaborative discourse and local networking’, *Public Policy and Administration* **13**, 8–22.

Daley, D. M. (2009), ‘Interdisciplinary problems and agency boundaries: Exploring effective cross-agency collaboration’, *Journal of Public Administration Research and Theory* **19**(3), 477–493.

Federal Ministry of the Interior (2003), *SAGA Standards and Architectures for e-government Applications Version 2.0*, kbst publication series, volume 59 edn, Berlin.

Feinberg, L. E. (2002), ‘Homeland security: implications for information policy and practice–first appraisal’, *Government Information Quarterly* **19**(3), 265–288.

Hudson, B., Hardy, B., Henwood, M. & Wistow, G. (1999), ‘In pursuit of inter-agency collaboration in the public sector: what is the contribution of theory and research?’, *Public Management* **1**, 235–260.

Koenig, D. (2001), *International Police Cooperation*, Lexington Books, Lexington.

Lord Laming (2003), ‘Victoria Climbie Inquiry’.

Lord Laming (2009), ‘The Protection of Children in England: A Progress Report’.

NIEM Program Management Office (2007), *National Information Exchange Model (NIEM)*, U.S. Department of Justice. http://www.niem.gov/index.php

Police and Crime Standards Directorate (PCSD) and Home Office (2007), ‘Delivering safer communities: A guide to effective partnership working’.

Thomas, R. & Walport, M. (2008), *Data Sharing Review Report*, UK Ministry of Justice.

Willem, A. & Buelens, M. (2007), ‘Knowledge sharing in public sector organizations: The effect of organizational characteristics on interdepartmental knowledge sharing’, *Journal of Public Administration Research and Theory* **17**(4), 581–606.