Consumer Managed Federated Homes

Rob Brennan, Zohar Etizoni, Kevin Feeney, Declan O'Sullivan Trinity College Dublin

William Fitzgerald, Simon Foley, University College Cork

Abstract

There are emerging opportunities for distributed, composite services, based on the combination of smart homes, networked consumer devices, third-party services and social, geographical or commercial collaborations. However, current home-automation technology tends to focus on the single-home solution, rather than enabling home users can securely share and easily manage the resources and services of their home area network. This article describes a new federated home architecture that addresses these needs, reports on prototyping to date and provides an overview of several important technologies for the next generation of federated homes. Our vision is to support a future of user-centric device and service sharing from home-to-home across the Internet, in a way that does not rely on centralised authority but supports a web of secure, peer-wise trusted relationships between consumers.

1. Introduction

A key factor in the dramatic growth of web 2.0 has been the development of systems that enable easy publication of consumer-generated content. Initially this content was mainly in textual form but increasingly it embraces multi-media offerings. In parallel, advances in consumer electronics and communications technology have ensured that the home has become a smorgasbord of multimedia communications, storage, playback and creation devices and services.

To date most web-based publication approaches have been built around centralised portal-style architectures, such as Netflix, SkyGo, and true peer-to-peer sharing has been mostly limited to basic file-distribution. Although there is some emerging work on cloud-based federation of home services [1]. Despite the proliferation of web-enabled consumer devices, examples of the sharing of dynamic streamed content and services between these devices are few and far between. One can imagine various exciting possibilities that could be enabled by real-time sharing of home devices and services: ad hoc community video surveillance, home broadcasting, remote access to printers or photo displays in a buddy's home, remote environmental monitoring for weather prediction or energy management. In order to realise the full potential of a truly connected world of shared devices and composed services, end-users require facilities to control their participation in these networks according to their particular needs and concerns.

Consider the following illustrative example: Bob has a home area network with a UPnP-enabled media server. His friend Alice has a UPnP-enabled TV and a UPnP-enabled DVR. Bob and Alice want to share access to their devices so that when Bob visits Alice they can watch content from his media server on her big-screen UPnP media-renderer. In addition, Alice wishes to allow Bob to use her UPnP-DVR to record his favourite TV programs so that they can watch them together when he visits. If consumers were capable of easily sharing their home devices and services, many useful variations of this sharing scenario would be enabled. By making such sharing easy to establish and manage, consumer creativity in envisaging and deploying such collaborations could be unleashed. Of course it is worth noting that this is a technical solution and the legal implications of content-sharing are out of scope.

So, how can the types of services available in home-networks be made available, composed and shared by typical end-users? What are the technical limitations of current systems that must be overcome? This article presents an architecture for secure consumer-managed federation of home devices and services. To give context, we highlight important or emerging technologies for secure management of next generation consumer devices. The architecture is elaborated through reports on our prototyping and experimental experiences to date.

2. Requirements

Enabling secure, remote sharing of the varied device and service capabilities of the typical networked home or small enterprise is a non-trivial challenge, especially without recourse to single-vendor or centralised solutions. In some respects, it is a traditional service or network management problem that focuses on resource configuration, integration and access control. However, the networked home, or Home Area Network (HAN), has a number of special challenges compared to traditional service and network management deployments. It is typically operated by non-technical users. Thus, effective HAN configuration may be hampered by a poor understanding of HAN service requirements or underlying technologies. Any viable approach must somehow bridge the gap between user experience and the underlying technical details.

The HAN environment itself is also challenging, it exhibits a great diversity of devices and is highly dynamic with devices joining and leaving the network as they are switched on or off or moved from one location to another. These devices themselves are highly specialised and generally lack the management functionality associated with enterprise or carrier networking equipment. Even if they support some form of dynamic co-ordination and service orchestration mechanism, such as UPnP (Universal Plug and Play), these mechanisms were generally developed primarily for a single home or network use case and have no support for external HAN to HAN sharing of capabilities. There is also a range of co-ordination mechanisms, with different vendors having taken a variety of different technical approaches, and there has been only limited success to date in building multi-system services, especially for generalised sharing. It is thus a requirement of any practical general solution that it must support a wide range of commonly available co-ordination technologies.

In the past, the only viable mechanism for delivering advanced services like IPTV was through tightly-integrated provider chains, in many cases passing from the content subscription service all the way down to the connectivity and network equipment providers. That business model is increasingly outdated as smart new devices bypass network providers to access “over the top” services and consumers demand choice to access their favoured service providers. Consumers who produce and share content and services are no longer accustomed to having their interactions controlled by the device manufacturer or telecommunications provider. There are a number of competing walled gardens of content in the social networking space but the vast majority of content and services on the web remains connectivity provider and device-manufacturer neutral. A third requirement is, thus, that access to the capabilities shared by consumers should be device and network agnostic

Since service or device sharing between HANs – which we describe as *HAN Capability Federation* - implicitly involves exposing aspects of at least one domain, security issues must be at the forefront of our requirements. It is important not to leave the HAN user exposed to new threats by enabling sharing. In order to minimise the risk of unintended exposure, a basic requirement is that access to the devices and services shared by a user be limited to those requests that are necessary to support the shared services that the user has agreed to participate in. It must be possible to authenticate requests for utilisation of shared services and it must be possible to apply fine-grained constraints to how they are used. Thus, users should not be forced to share all of their media files, or, for example, 24x7 access to a video camera service, when it is only a single file, device or service that they wish to share for a particular period of time.

Finally, it must be born in mind that consumer networks largely consist of off-the-shelf, relatively low-power devices made by the cheapest vendor. Thus, solutions that rely on powerful on-device processing facilities are not-applicable in the HAN domain.

3. Related Work

Table 1 provides an analysis of some of the key HAN service protocols in the state of the art. It references their scope, market-uptake, service-orientation, degree of independence from other technologies (generality), non-functional aspects and multi-home-networking readiness. In this article, this latter criteria of multi-home readiness is particularly important, as it indicates to what extent the service protocol supports discovery and access to services from outside the HAN. It can be seen from table 1 that ZeroConf is the only protocol with some support for multi-home networking. It should be noted, though, that this support is not native and requires manual administration and configuration of a DNS server, which is not appropriate for typical home users. To some extent OSGi can also support multi-home setting with distributed OSGi and R-OSGi. However, this is not commonly deployed and requires specific administration. The rest of the protocols and standards (UPnP, DPWS, Jini, SLP, and HAVi), do not natively support service discovery or access to services beyond the scope of a single network.

Property/Protocol		**UPnP**	**DPWS**	**Jini**	**SLP**	**ZeroConf**	**OSGi**	**HAVi**
Scope and Market Uptake	**Application Domain**	Generic, currently focused in consumer electronics	Generic	Generic	Broad TCP/IP services	Broad TCP/IP services	Generic, emerging for set top box	Consumer electronics
	Standardization Body	UPnP Forum	OASIS	Sun (Oracle)	IETF	IETF	OSGi Alliance	HAVi consortium
	Market Acceptance	Very common, promoted by DLNA	Not yet common in HAN	Not common in HAN	Used as part of ZeroConf	Very common	Not common for inter-device interoperability	Not widely used
Service Orientation	**Service Adverts**	Multicast	Multicast	Via lookup service	Multicast	Multicast	Via service registry	Via lookup service
	Service Discovery	Multicast	Multicast	Via lookup service	Multicast	Multicast	Via service registry	Via lookup service
	Service Registry	Not supported	Not supported	Supported	Supported	Supported	Supported	Supported
	Service Description	XML	WSDL	Java API	Not supported	Not supported	Java API	Java API
	Service Invocation	Communication mechanism (SOAP)	Communication mechanism (SOAP)	Communication mechanism (Java RMI)	Service location	Service location	Communication mechanism (Java API)	Communication mechanism (Java RMI)
	Service Composition	Not supported	Compatible with web service composition	Not supported	Not supported	Not supported	Not Supported	Not supported
Generality	**Programming Language**	Any	Any	Java	Any	Any	Java	Java
	Physical Layer	Any	Any	Any	Any	Any	Any	IEEE1394
Non Functional Aspects	**Security**	Available as an add-on	Authentication, integrity, encryption	Authentication, authorization, integrity, encryption	Authentication	Authentication, integrity	Java-based security	Authentication, authorization, integrity
	Performance	Small memory footprint	Small memory footprint	RMI is considered to have better performance than SOAP	Considered scalable because of the abstraction of invocation protocol	Optimised discovery protocol with shutdown mechanisms. Considered scalable.	No specific issues	Designed for small networks

Extensibility	**Multi-home Readiness**	None	None	None	None	Via DNS-SD	R-OSGi/ Distributed OSGi	None

Table 1 Service Protocols and Standards Comparison

4. Technical architecture

This article describes a novel architecture for enabling secure consumer-controlled sharing of HAN devices and services (for which we adopt the generalised term, *capabilities*). Figure 1 presents a high-level overview. Our vision is to support a future of user-centric device and service sharing from home to home and across the Internet in a way that does not rely on centralised authority but supports a web of secure, peer-wise trusted relationships between consumers. The approach is based on the Krox domain controller and service sharing framework [2]. Krox allows consumers to advertise and share home services or device capabilities in a user-friendly way that is independent of the specific HAN control protocols supported by the devices. These capabilities are shared over a control layer built on XMPP (the eXtensible Messaging and Presence Protocol) with peer HANs or other networks. Flexible federation, sharing policy definition and access control of the shared capabilities is enabled by a trusted federal relationship manager (FRM) service [3], which can form a decentralised federation management system by co-operating with other FRMs to establish secure fine-grained capability sharing channels. Network-level access controls, for example HAN firewall configuration, are automatically synthesized from the FRM relationships by a HAN Access Control (FANAC) agent [4] that automatically generates low-level access control device configurations, e.g. for the firewall at the HAN gateway. These configurations are aligned with both the user-configurable, high-level security requirements and the FRM-level capability sharing policies based on semantic models of security threats and countermeasures.

There are three major sub-systems in our architecture – the Krox service sharing system, the federal relationship manager (FRM) and the Home area network Autonomic Network Access Control (FANAC) agent. Each of these sub-systems is described in more detail in the following sub-sections.

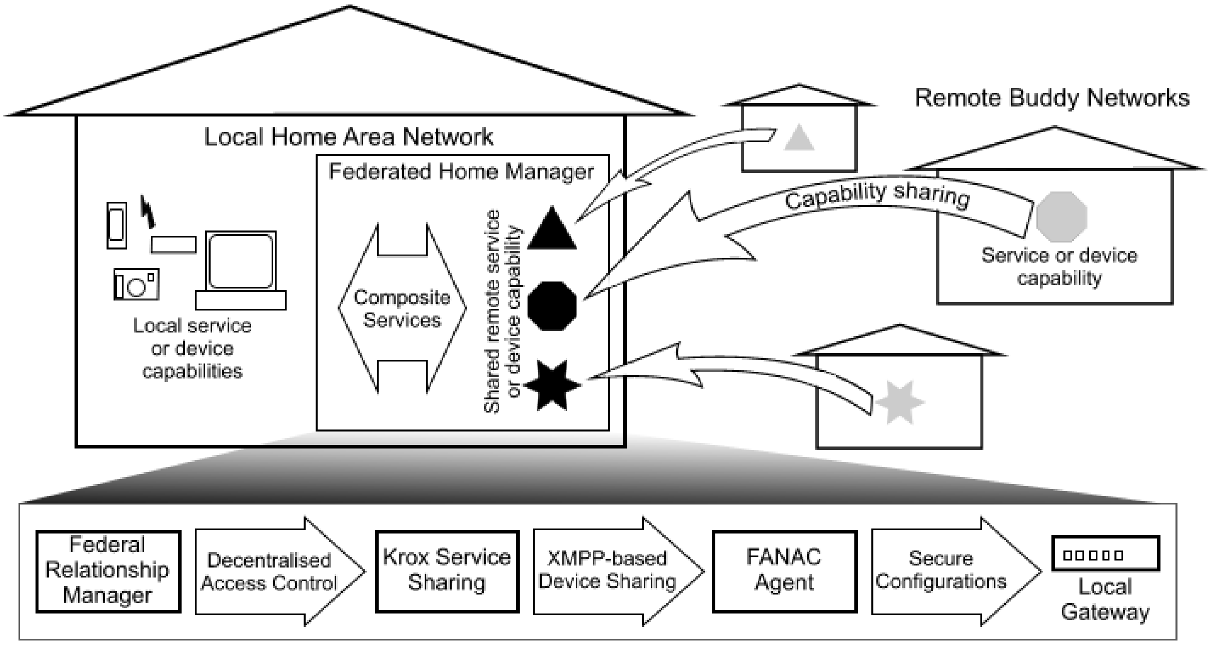

Remote Buddy Networks
Local Home Area Network
Federated Home Manager
Capability sharing
Service or device capability
Composite Services
Shared remote service or device capability
Local service or device capabilities
Federal Relationship Manager
Decentralised Access Control
Krox Service Sharing
XMPP-based Device Sharing
FANAC Agent
Secure Configurations
Local Gateway

Figure 1: Overall System Architecture

4.1 HAN Service Sharing Sub-System (Krox)

The Krox communication subsystem leverages IM&P (Instant Messaging and Presence) infrastructure to carry messages and content streams between HANs. IM&P has gained immense popularity with the advent of instant messaging chat applications. For IM&P standardisation, two working groups were formed by the Internet Engineering Task Force (IETF) at different times, SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE)19 – based on Session Initiation Protocol (SIP), and eXtensible Messaging and Presence Protocol (XMPP) [5] – based on XML streaming, which was originally Jabber's underlying protocol.

The Krox sub-system delivers integrated intra-HAN and inter-HAN service interoperability. It enables HAN services from remote HANs to be discovered in the local HAN and to seamlessly interact and be composed with local HAN services and client applications. It is built on top of the existing XMPP communications infrastructure for instant messaging and presence. The generality of the approach has been demonstrated with prototype implementations for two important service-oriented HAN protocols: UPnP and Jini.

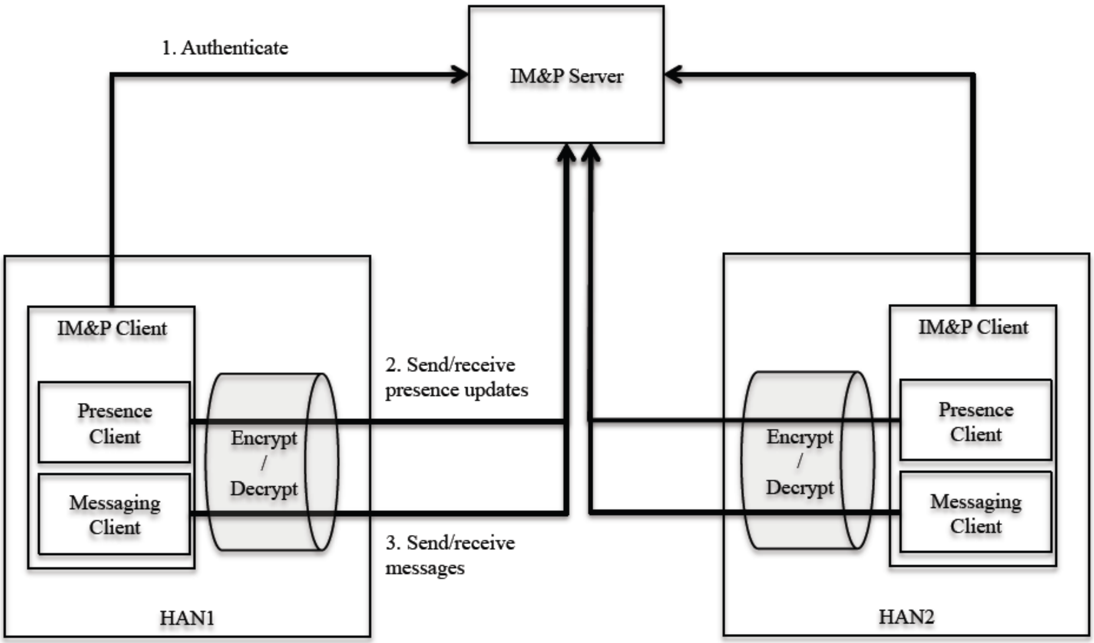


Figure2: Krox Communication Subsystem

Krox supports inter-HAN service interoperability through automatic representation of remote devices and services as "virtual resources" in the local HAN. These "virtual resources" proxy the communication with the remote HAN and provide an interface to the local HAN that is identical to the interface provided by local devices or services of the same technology. For example a remote UPnP media server would be represented in the local HAN using a virtual UPnP device. The virtual device facilitates all the interaction with control point applications in the local HAN by tunnelling the communication over a secure XMPP connection to the remote HAN hosting the live device. There, the tunnelled messages are received by the remote Krox system and forwarded to the live device. Any response messages are tunnelled back to the virtual device. The resource virtualisation is based on the HAN service protocol-based device service interfaces, which are themselves abstracted from a particular device or implementation.

These virtual devices facilitate seamless integration with client applications in the local HAN, e.g. for interoperability and composition with other services in the local HAN. Intra-HAN service interoperability and service composition are integrated with the Krox subsystem architecture through the use of a common service model. This enables interoperation and composition of services from multiple HAN service protocols, originating in both local and remote HANs. Each local virtual resource is automatically generated by Krox for devices from remote HANs that are shared with the local HAN. This is enabled by the availability of service interfaces in a parsable format, e.g. Java (for Jini and HAVi services), XML (for UPnP services) or even WSDL (for the devices profile for web services, DPWS). Orchestration of composite services on the Krox platform is enabled through representation of all HAN services, of whatever HAN service protocol, as native web services. This common representation and interaction style enables the creation of reusable composite services from atomic ones and the deployment of standard service orchestration and management patterns.

The re-use of XMPP-based instant messaging and presence (IM&P) communications infrastructure for the Krox sub-system enables us to present XMPP buddies and sharing as a user metaphor to represent remote HANs and devices. This approach abstracts away low level configuration details, such as IP addresses, from the home user and configuration of sharing with a remote HAN is reduced to adding the username of the remote HAN to “buddy lists”.

4.2 Federal Relationship Manager Subsystem (FRM)

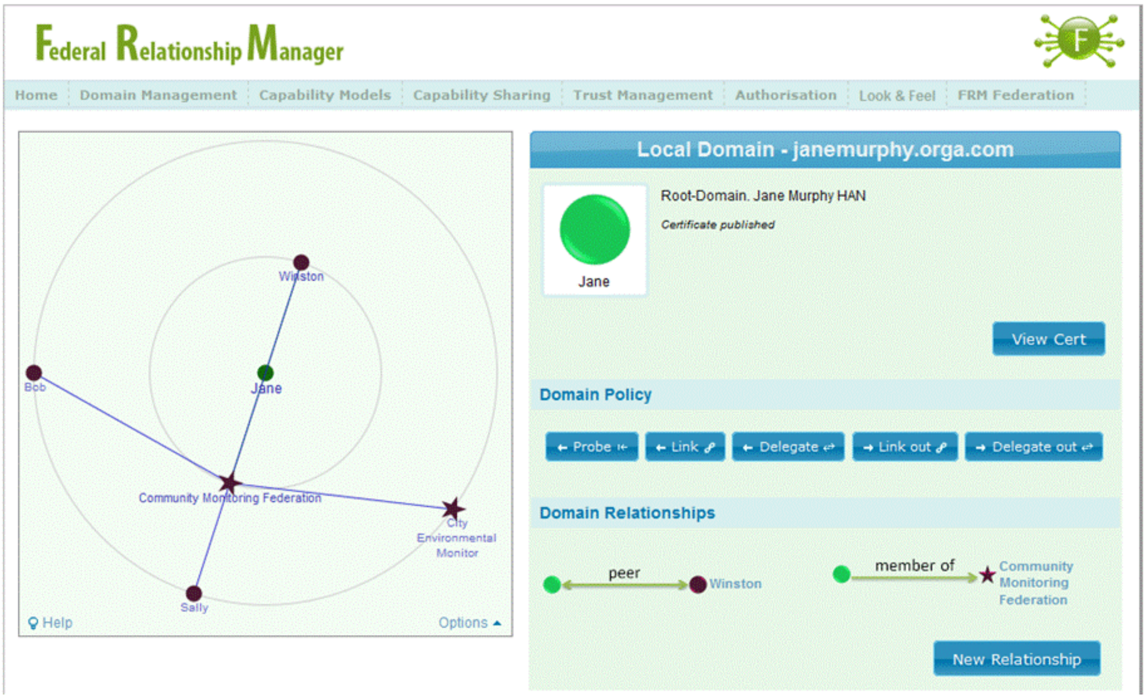
Both the FRM and the FANAC components of our architecture are based upon a Trust Management approach to decentralised security. Trust Management [6] is an approach to constructing and interpreting the trust relationships among public keys that are used to mediate security critical actions. Cryptographic credentials specify delegation of authorisation between public keys. When a request from a principle (key) is made to a networked application to execute a particular action, then, authentication notwithstanding, the application must determine whether the key(s) that made the request is authorised. Trust Management provides assistance to applications in making these decisions and facilitates decentralized policies: authorization may be determined without having to consult some central authorisation server, and users may further delegate their authority without reference to a Central Authority.

The FRM is a policy engineering framework, designed to allow providers to flexibly and securely share access to devices and services with third parties. It provides consumers with a simple user-interface, which enables them to create relationships between their local HAN and remote HANs and to define fine-grained capability sharing agreements between them. The FRM maps the user-level relationships and agreements to trust relationships encoded in secure cryptographic certificates. It supports controlled re-sharing of home devices or services in contexts where these services may ultimately be consumed by third parties with whom the provider has no direct relationship, thus facilitating multi-party federations and complex networks of composed HAN capabilities as well as simple peer-to-peer sharing.

The FRM subsystem uses the mechanism of delegation of Capability Authorities (CAs) to represent capability sharing between domains. A Capability Authority is a certificate that contains a reference to a node on a Capability Model (CM), which represents a service and a set of constraints that can be applied to its invocation. CMs are semantic service descriptions, which define a set of nodes organised in a tree-based partial ordering. Each CM node represents a specific set of constraints that apply to the invocation of the underlying service. The ordering of CM nodes represents constraint encapsulation – that is to say a parent node represents a less constrained invocation than its children.

In order to make a device or service available through the FRM, a capability model (CM) must be created to represent it. CMs describe the service's attributes and organise the potential constraints upon its invocation into a tree-based hierarchy. The recipient of a delegated CA can access the referenced CM through the Capability Authority Information Service (CAIS) provided by the FRM to safely define valid sub-constraints, according to the CM tree structure, and thus delegate sub-CAs to other domains. CAs and sub-CAs can be delegated repeatedly across domains and each delegation can add new constraints to service invocations. When dealing with delegation chains involving multiple domains, a CA may incorporate constraints that have been defined by multiple different domains. Before the service can be safely invoked, all of these constraints must be verified. The FRM's trust management model supports this by allowing credentials proving delegation chain validity to be embedded into CAs.

Figure 3 shows a screenshot with the FRM. Each node on the graph represents a different HAN and the lines between the nodes represent secure capability sharing agreements. In this case Jane has a peer-to-peer sharing relationship with Winston and also belongs to a multi-party community monitoring federation that also includes Bob and Sally.



Local Domain - janemurphy.orga.com

Root-Domain. Jane Murphy HAN

Certificate published

Figure 3: Viewing Federations in the FRM Interface

4.3 Federated Autonomic Network Access Control Subsystem (FANAC)

Network Access Controls (NAC) are widely used to provide endpoint security typically complementing existing application-based security controls. NAC security mechanisms, for instance firewalls, are routinely prescribed as requirements for compliance to security standards such as PCI-DSS and ISO 27000. However, the effectiveness of a NAC configuration may be hampered by poor understanding and/or management of the overall security configuration, which may in turn, unnecessarily expose the enterprise to known security threats. New threats and/or service requirements often result in firefighting by ad-hoc modification to an already large and complex configuration. This complexity is further compounded by the diverse range of NAC mechanisms used to secure an enterprise; ranging from firewalls and proxies to NAC-style controls within applications themselves. In our approach Ontology Engineering techniques are used to provide expert and automated support for the management of NAC configurations. Ontologies are used to describe detailed prescriptions for NAC configurations that are compliant with security standards and best practices. These catalogues of best practice describe how known threats are mitigated by NAC configurations and are continually updated to reflect newly discovered vulnerabilities and revisions to best practice.

A prototype Federated Autonomic Network Access Control (FANAC) configuration agent [3] has been implemented and its high-level components are depicted in Figure 4. A FANAC agent manages, on behalf of the home user, the configuration of multiple NAC controls in the HAN and is modelled using an ontology. FANAC takes a threat-based approach to structure knowledge about the management of a NAC configuration. Semantic Threat Graphs [7], a variation of the traditional threat tree, are encoded within the ontology-based framework in order to relate knowledge about the best practices for configuring HAN network access controls that provide best practice at mitigating security threats to the HAN. Our current implementation provides a knowledge-base of best practices for iptables firewall, TCP wrapper and ejabberd (XMPP application server) host policies.

When a federation request is authorized by the FRM, the FANAC agent reconfigures the NAC controls (ontology) to enable the federation. This NAC reconfiguration, for example, adds the requester to the ejabberd whitelist and adds additional iptable firewall rules to enable a path to the requester. These changes are done so that the resulting configurations are complaint with best practices and thus continue to defend against security threats. The KeyNote trust management system [8] is used to manage the trust relationships between FRM servers and the FANAC agents.

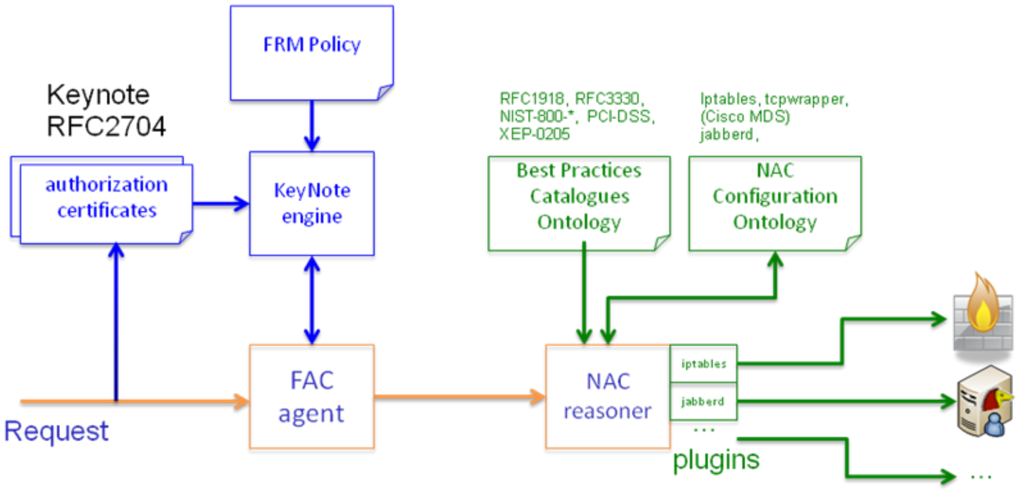

FRM Policy
Keynote
RFC2704
authorization certificates
KeyNote engine
RFC1918, RFC3330, NIST-800-*, PCI-DSS, XEP-0205
Iptables, tcpwrapper, (Cisco MDS) jabberd,
Best Practices Catalogues Ontology
NAC Configuration Ontology
Request
FAC agent
NAC reasoner
iptables
jabberd
...
plugins
...

Figure 4: FANAC Agent Components

5. Dynamic System Behaviour

The message sequence chart pictured in figure 5 shows the coordinated interactions between the architectural sub-systems that occur when a user makes a new capability available to a federation and it is invoked by a member of that federation (the remote HAN). The depicted scenario shows, firstly, the local registration of a new device (1-3), followed by the enabling of capability sharing with remote domains by the user (2-6). Once the capabilities have been shared they can be browsed by remote users (8-11) and, finally, if they have appropriate credentials invoked (12-18). In this case an UPnP-compliant media storage device has registered with the Krox UPnP domain controller, the user has shared that device with a buddy on a remote network and authorised browsing and playback of media files by the buddy. When the remote user requests that a file be played and streamed to a playback device in their own HAN, the FRM ensures that this complies with the local access control policies and the FANAC agent automatically updates the local gateway firewall configuration to allow this media stream to pass through (by default the FANAC configures the firewall to block all potentially harmful interactions, only trusted parties are given access).

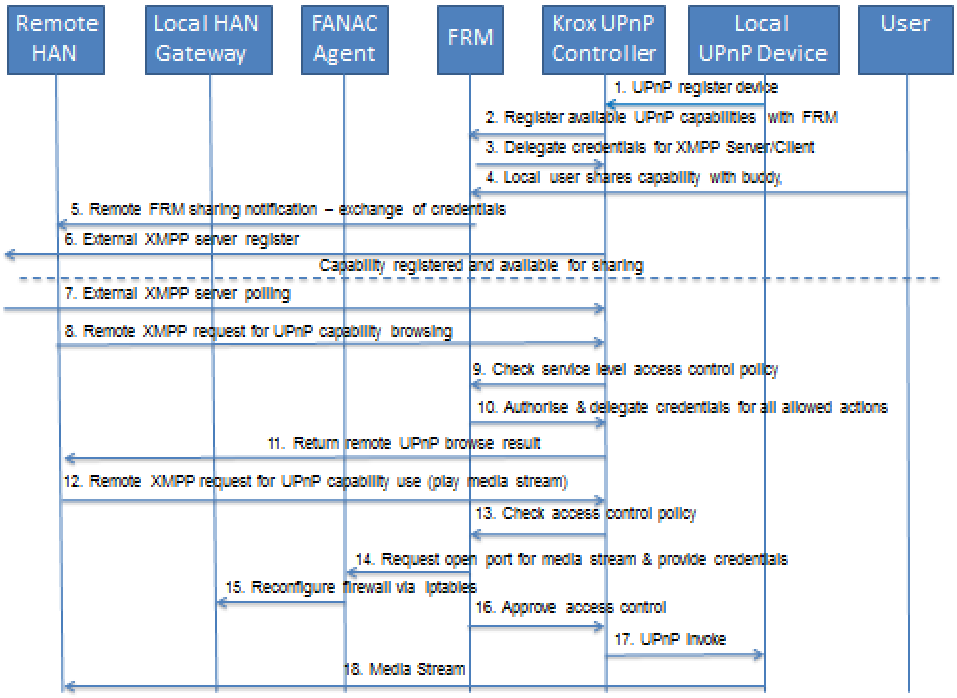

Remote HAN
Local HAN Gateway
FANAC Agent
FRM
Krox UPnP Controller
Local UPnP Device
User
1. UPnP register device
2. Register available UPnP capabilities with FRM
3. Delegate credentials for XMPP Server/Client
4. Local user shares capability with buddy,
5. Remote FRM sharing notification – exchange of credentials
6. External XMPP server register
Capability registered and available for sharing
7. External XMPP server polling
8. Remote XMPP request for UPnP capability browsing
9. Check service level access control policy
10. Authorise & delegate credentials for all allowed actions
11. Return remote UPnP browse result
12. Remote XMPP request for UPnP capability use (play media stream)
13. Check access control policy
14. Request open port for media stream & provide credentials
15. Reconfigure firewall via iptables
16. Approve access control
17. UPnP invoke
18. Media Stream

Figure 5: Message Sequence Chart for Capability Registration and Sharing

6. Evaluation

The goal of the performance evaluation is to assess the different performance aspects of the Krox system with between 5 and 15 remote HANs and up to 300 remote services represented in the local HAN. For inter-HAN performance aspects of Krox system architecture, several parameters needed to be evaluated: CPU utilisation, Memory utilisation, Bandwidth utilisation, Responding to local HAN's search requests, Discovery delay, Remote invocation delay, Remote description delay, Event notification delay. In this article due to space considerations, we just present results related to CPU utilisation.

The evaluation setup consisted of a testbed consisting of 5 emulated HANs each running on a desktop PC (Intel Pentium 4 machines, 2GHz, 100Mb/s network card, 512KB cache, with memories varying between 1 and 2 GB) that each run the Krox system, a single emulated control point, and a set of emulated devices. The XMPP server, installed on the 6th machine (Macbook Pro with OS X 10.6.7 operating system, Intel Core 2 Duo, 2.6GHz, 6MB cache, 4GB Memory running XMPP OpenFire server 3.6.4), is accessible to all of the Krox system instances. In order to evaluate the performance of Krox system implementation with a growing number of services shared from remote HANs, the experiment included 10 steps such that each step is run for an hour. In every step of the experiment, the number of emulated devices in each HAN is increased by 5. Each emulated UPnP device has 3 services; therefore 20 remote devices correspond to 60 remote services shared with each of the HANs, added during each step of the experiment. For consistency, each step of the experiment is separate and involves restarting the Krox system and the emulated UPnP devices and control point followed by an hour of execution. The experiment was repeated twice with different mixes between stationary and mobile devices. The first iteration of the experiment was performed with 80% stationary devices and 20% mobile devices. The second iteration was performed with 60% stationary devices and 40% mobile devices. Each iteration repeated the 10 steps described above such that the number of devices starts from 5 per HAN in the first step, and reaches 50 devices per HAN in the last step. The purpose of running two iterations with different mobile to stationary devices ratio, was to validate the assumption that the impact of the proportion of mobile to stationary devices on the overall performance is negligible despite the increase in signalling traffic that mobile devices incur on the network infrastructure. The results show that the differences are indeed insignificant, therefore for presentation purposes the averaging of the two iterations is used, in order to focus on the significant performance issues.

In order to measure the CPU utilisation of the Krox system, the CPU utilisation was sampled every 30 seconds. Figure 6 shows the increase in CPU utilisation (per cent) of the Krox system with the increased number of services shared with the local HAN. It can be seen that the CPU with 300 services shared with the HAN (which is the maximum required) in all of the desktops is below 4%. Even with 600 remote shared services the CPU grows linearly to less than 7% for all of the desktops in the setup.

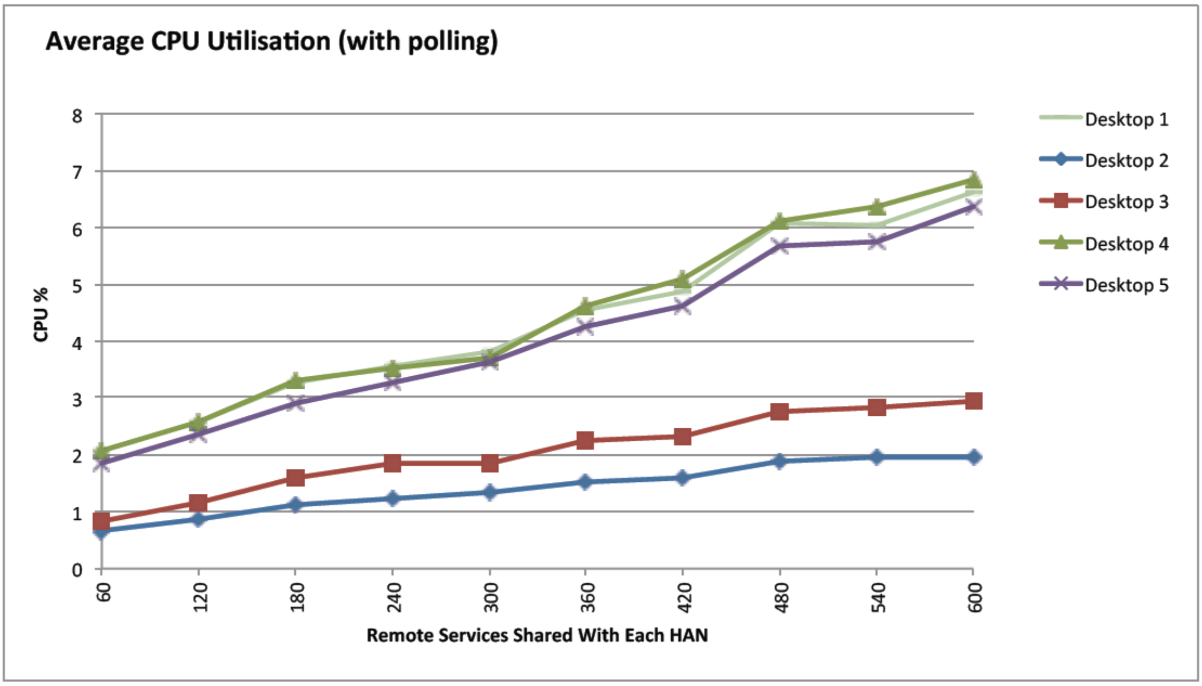


Figure 6: Krox System CPU Utilisation with Polling

7. Conclusions

Soon we will share our devices and home services as easily as we now share files; however there are much greater risks for mis-use and attack. One approach to minimising these risks will be to remain within an operator's or service provider's vertically integrated walled garden of users, providers, services and content. This approach leads to vendor lock-in, a drip-feed of functionality and overwhelming threats in the face compromised security on the part of the operator. Additionally consumers have increasingly opted to move to over the top service providers and best of breed third party solutions in the hope of maximising the value of their information processing and communications networks. There is no indication that they will take a different approach for the next generation of federated homes, devices and services. Thus, secure decentralised models of heterogeneous device-sharing, based on trust-management, usability and HAN protocol independence are important to realise that future.

Acknowledgements

This work was partly funded by Science Foundation Ireland via grant 08/SRC/I1403 ("Federated, Autonomic Management of End-to-End Communications Services") and grant 12/CE/I2267 the Centre for Next Generation Localisation (www.cngl.ie).

References

[1] D. Díaz-Sánchez, F. Almenarez, A. Marín, D. Proserpio, and P. A. Cabarcos, “Media cloud: an open cloud computing middleware for content management,” IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 970–978, 2011.

[2] Z. Etzioni, J. Keeney, D. Lewis , "Inter-HAN service interoperability with Krox," IEEE International Conference on Consumer Electronics (ICCE), 2012, 13-16 Jan. 2012, pp.441-444, doi: 10.1109/ICCE.2012.6161935

[3] K. Feeney, R. Brennan, J. Keeney, H. Thomas, D. Lewis, A. Boran, and D. O’Sullivan “Enabling decentralised management through federation,” Computer Networks, vol. 54 no. 16, 2010, pp. 2825–2839.

[4] S. N. Foley, W. M. Fitzgerald, W. MacAdams, “Federated Autonomic Network Access Control,” 4th Symposium on Configuration Analytics and Automation (SafeConfig), October, 2011, doi: 10.1109/SafeConfig.2011.6111668.

[5] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Engineering Task Force RFC 3920, October 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3920.txt. 29 November 2012 [date accessed].

[6] M. Blaze, J. Feigenbaum, and M. Strauss, “Compliance checking in the policymaker trust management system,” in FC ’98: Proceedings of the Second International Conference on Financial Cryptography. London, UK: Springer-Verlag, 1998, pp. 254–274.

[7] S. N. Foley and W. Fitzgerald, “Management of security policy configuration using a semantic threat graph approach,” Journal of Computer Security, vol. 19 no. 3, 2011, pp. 567–605.

[8] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis, “The KeyNote Trust Management System, Version 2,” ," Internet Engineering Task Force RFC-2704. September 1999.

Biographies

ROB BRENNAN (rob.brennan@cs.tcd.ie) is a senior research fellow in the Knowledge and Data Engineering Group (KDEG), Trinity College Dublin (TCD), Ireland. His research interests include semantic interoperability, data curation, intelligent distributed systems, and the application of linked data to systems management. He has contributed to 3GPP, TMF, IETF, and OMG standards. He has a Ph.D. (2004) from Dublin City University. Prior to TCD he worked in the Ericsson network management research center and several startups.

ZOHAR ETZIONI has over 15 years of R&D experience in academia and industry. He completed a Ph.D. in Computer Science from Trinity College Dublin in 2011. His research focused on sharing and composition of home network services. His main research interests are distributed systems, network management, swarm intelligence, machine learning, and software engineering. He has extensive software development experience as a tech lead across multiple domains including algorithmic trading, telecom network management, and medical imaging.

KEVIN FEENEY (kevin.feeney@cs.tcd.ie) is a research fellow in the KDEG in the School of Computer Science and Statistics at TCD, Ireland. His research interests include cliodynamics, federation, inter-organizational management and applying collective intelligence to management problems. He has a Ph.D. in computer science from Trinity College Dublin.

DECLAN O'SULLIVAN (declan.osullivan@cs.tcd.ie) has a B.A. (Mod), M.Sc., and Ph.D., all in computer science, from TCD where he is head of the Intelligent Systems Discipline in the School of Computer Science and Statistics. In addition, he has worked in industry for 13 years. His research interest lies in the identification and development of techniques to enable semantic mapping as a means to enhance collaboration in heterogeneous environments

William Fitzgerald (www.williamfitzgerald.net) is a Research Scientist and Senior Technologist at EMC. He carries out cyber security research and standardization within cloud and SDDC domains. In a professional capacity, he is a committee member of the CSA Security SLA WG. William is a conference program committee member of IFIP SEC, AIMSA, SECRYPT, SETOP and CRiSIS. William holds a Ph.D. in Cyber Security from University College Cork.

SIMON FOLEY (s.foley@cs.ucc.ie) is a statutory lecturer at University College Cork where he teaches and conducts research in computer security. He serves on the editorial board of the Journal of Computer Security and has served as Program Chair of the IEEE Computer Security Foundations Workshop and the ACSAC New Security Paradigms Workshop. He has over 70 international peer-reviewed publications on security, and his research interests include trust and risk management, security modeling, and security psychology.

Property/Protocol		UPnP	DPWS	Jini	SLP	ZeroConf	OSGi	HAVi
Scope and Market Uptake	**Application Domain**	Generic, currently focused in consumer electronics	Generic	Generic	Broad TCP/IP services	Broad TCP/IP services	Generic, emerging for set top box	Consumer electronics
	Standardization Body	UPnP Forum	OASIS	Sun (Oracle)	IETF	IETF	OSGi Alliance	HAVi consortium
	Market Acceptance	Very common, promoted by DLNA	Not yet common in HAN	Not common in HAN	Used as part of ZeroConf	Very common	Not common for inter-device interoperability	Not widely used
Service Orientation	**Service Adverts**	Multicast	Multicast	Via lookup service	Multicast	Multicast	Via service registry	Via lookup service
	Service Discovery	Multicast	Multicast	Via lookup service	Multicast	Multicast	Via service registry	Via lookup service
	Service Registry	Not supported	Not supported	Supported	Supported	Supported	Supported	Supported
	Service Description	XML	WSDL	Java API	Not supported	Not supported	Java API	Java API
	Service Invocation	Communication mechanism (SOAP)	Communication mechanism (SOAP)	Communication mechanism (Java RMI)	Service location	Service location	Communication mechanism (Java API)	Communication mechanism (Java RMI)
	Service Composition	Not supported	Compatible with web service composition	Not supported	Not supported	Not supported	Not Supported	Not supported
Generality	**Programming Language**	Any	Any	Java	Any	Any	Java	Java
	Physical Layer	Any	Any	Any	Any	Any	Any	IEEE1394
Non Functional Aspects	**Security**	Available as an add-on	Authentication, integrity, encryption	Authentication, authorization, integrity, encryption	Authentication	Authentication, integrity	Java-based security	Authentication, authorization, integrity
	Performance	Small memory footprint	Small memory footprint	RMI is considered to have better performance than SOAP	Considered scalable because of the abstraction of invocation protocol	Optimised discovery protocol with shutdown mechanisms. Considered scalable.	No specific issues	Designed for small networks
Extensibility	**Multi-home Readiness**	None	None	None	None	Via DNS-SD	R-OSGi/ Distributed OSGi	None

Table 1 Service Protocols and Standards Comparison

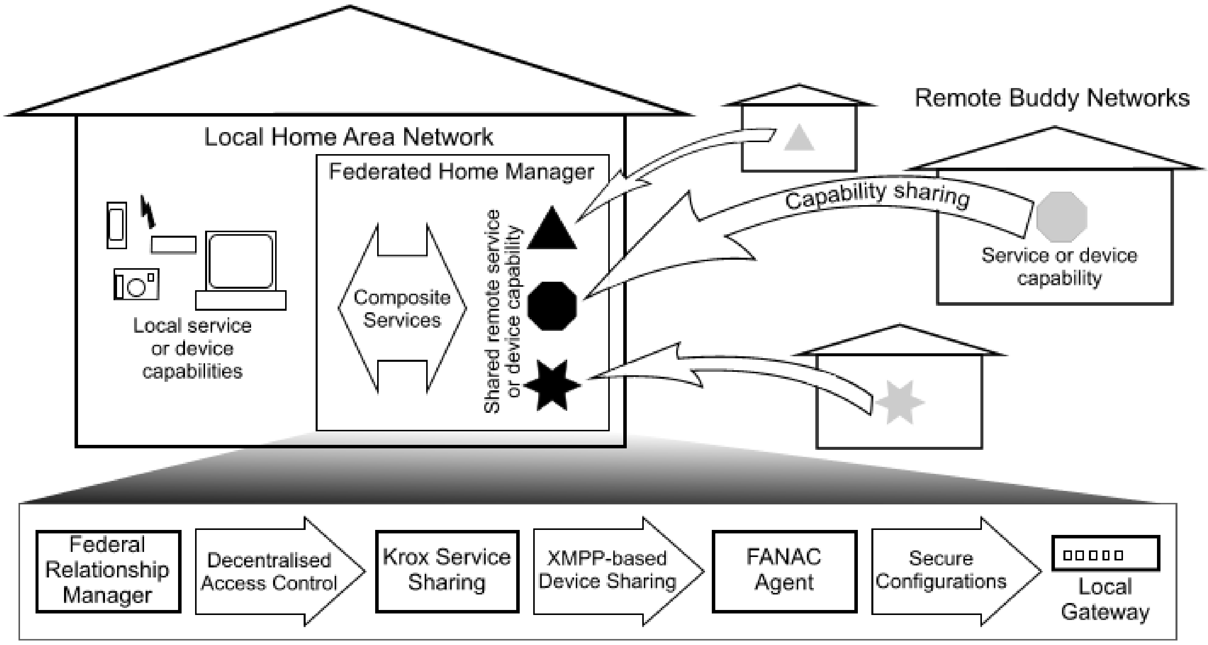

Local Home Area Network
Federated Home Manager
Local service or device capabilities
Composite Services
Shared remote service or device capability
Remote Buddy Networks
Capability sharing
Service or device capability
Federal Relationship Manager
Decentralised Access Control
Krox Service Sharing
XMPP-based Device Sharing
FANAC Agent
Secure Configurations
Local Gateway

Figure 1: Overall System Architecture

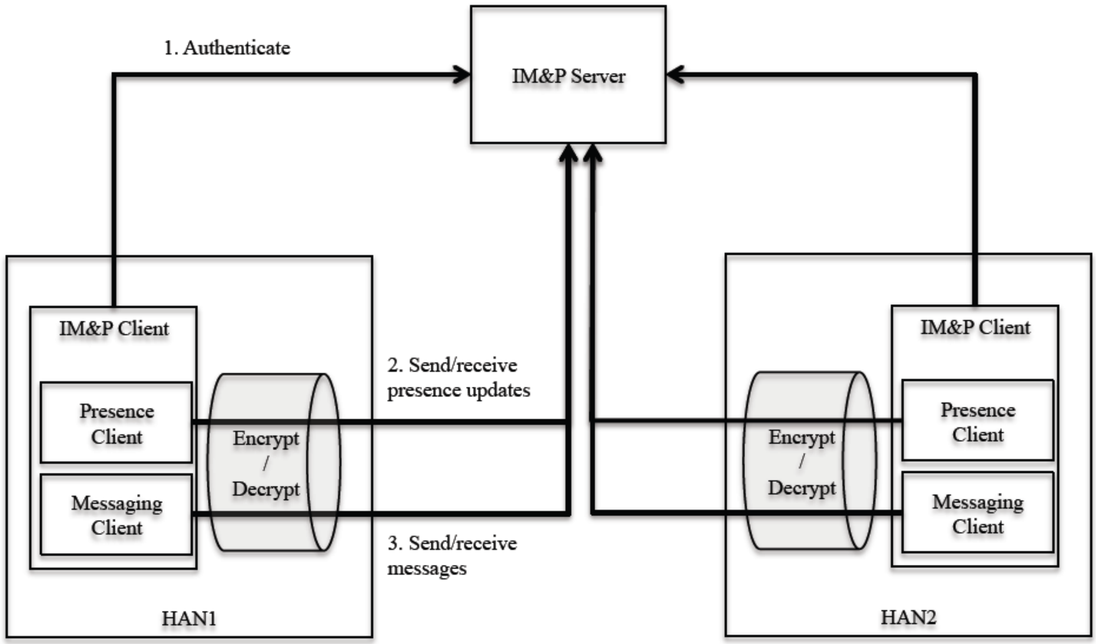
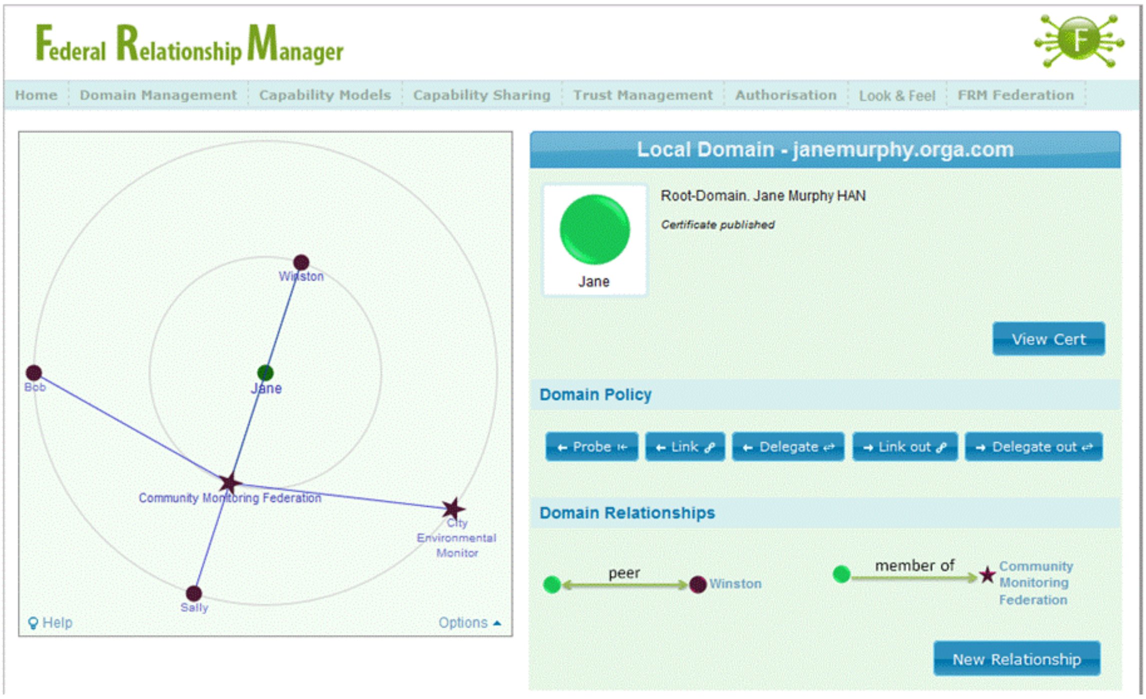


Figure2: Krox Communication Subsystem



Root-Domain. Jane Murphy HAN

Certificate published

Figure 3: Viewing Federations in the FRM Interface

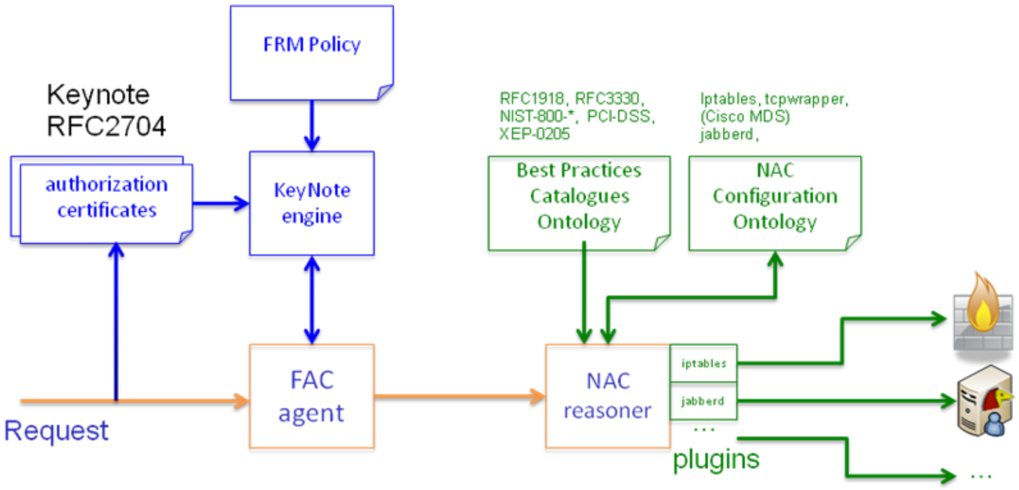

FRM Policy
Keynote
RFC2704
authorization certificates
KeyNote engine
RFC1918, RFC3330, NIST-800-*, PCI-DSS, XEP-0205
Iptables, tcpwrapper, (Cisco MDS) jabberd,
Best Practices Catalogues Ontology
NAC Configuration Ontology
FAC agent
NAC reasoner
iptables
jabberd
...
plugins
Request
...

Figure 4: FANAC Agent Components

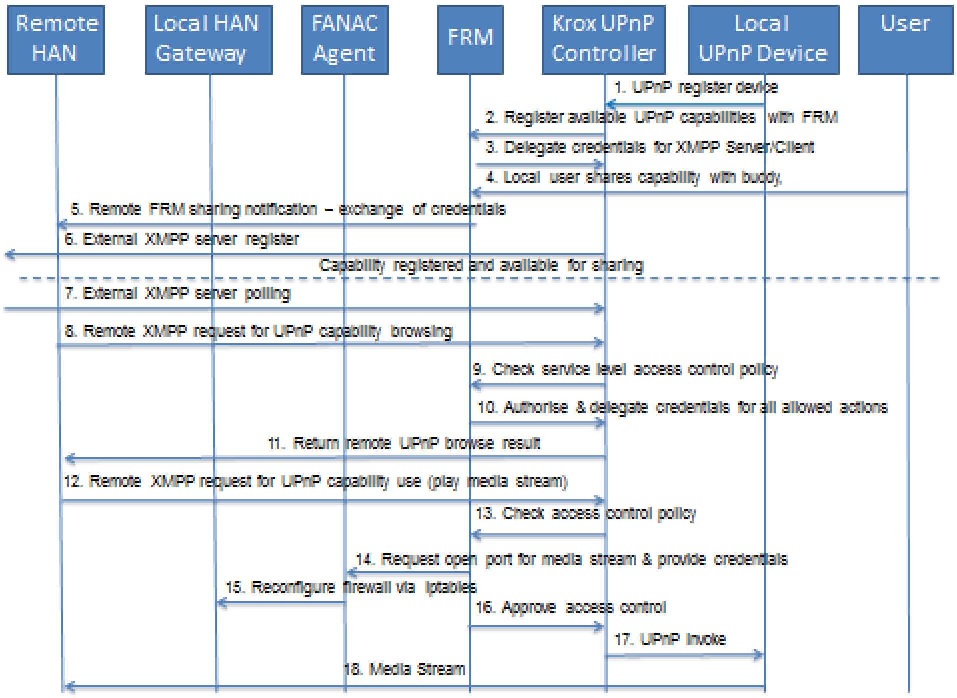

Remote HAN
Local HAN Gateway
FANAC Agent
FRM
Krox UPnP Controller
Local UPnP Device
User
1. UPnP register device
2. Register available UPnP capabilities with FRM
3. Delegate credentials for XMPP Server/Client
4. Local user shares capability with buddy,
5. Remote FRM sharing notification – exchange of credentials
6. External XMPP server register
Capability registered and available for sharing
7. External XMPP server polling
8. Remote XMPP request for UPnP capability browsing
9. Check service level access control policy
10. Authorise & delegate credentials for all allowed actions
11. Return remote UPnP browse result
12. Remote XMPP request for UPnP capability use (play media stream)
13. Check access control policy
14. Request open port for media stream & provide credentials
15. Reconfigure firewall via iptables
16. Approve access control
17. UPnP invoke
18. Media Stream

Figure 5: Message Sequence Chart for Capability Registration and Sharing

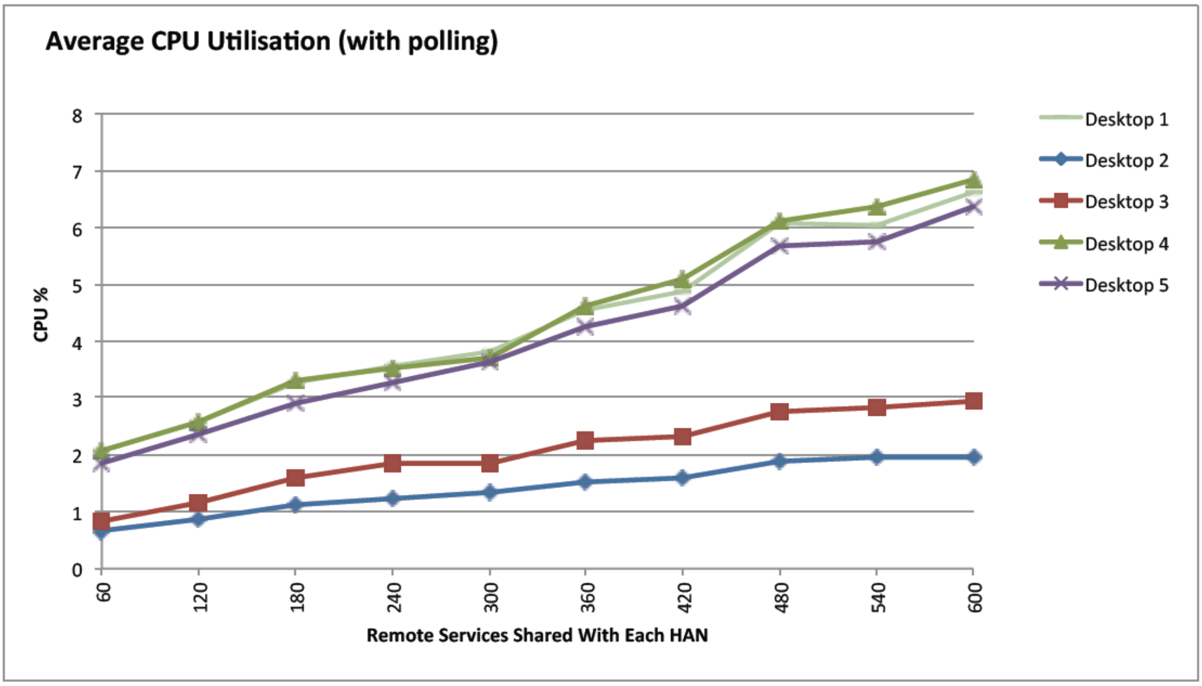


Figure 6: Krox System CPU Utilisation with Polling