NASA’s Secured Advanced Federated Environment

Edward Chow, Ph.D.  David Korsmeyer, Ph.D.  Pat Paterson
Joseph Liu, Ph.D.  Helen Stewart,  Scott Burchell
Pat Chang  Matt Chew Spence  NASA Marshall Space
Conan Viernes  Andy Goforth  Flight Center
Jet Propulsion Laboratory,  Shoshana Billik  Bob Wheeler
California Institute of  Bob Wheeller
Technology

Abstract:

In 1999, a NASA-wide team initially set out to create a collaborative environment to enable NASA’s scientists and engineers to share information and tools across NASA locations and with world-wide partners. This paper describes the team’s development process and solutions in resolving conflicting security issues of building a complex intra/inter-enterprise collaborative system. Based on the federated, hierarchical, compartmentalized principles, the Secured Advanced Federated Environment (SAFE) developed by the team is becoming a foundational element for building a collaborative infrastructure for NASA. This paper also introduces the concept of a Micro Security Domain which can achieve the balance between the need to collaborate and the need to enforce enterprise and local security rules. SAFE’s federated security concepts enables networks to be formed around the functional/security requirements. With the SAFE technologies and approaches, security will not be an afterthought of the enterprise network design.

Introduction:

Like most of the other government agencies, NASA is physically distributed throughout the country at different NASA centers. NASA’s contractors and partners are located throughout the world. Most of the NASA projects and missions involve geographically distributed teams in NASA centers, industry, and universities. In order to improve the efficiency of product development and support electronic collaborations, NASA centers have to provide extensive communication infrastructure to allow sharing of information and services world-wide.

Over five years ago, NASA management recognized that NASA needs a good infrastructure to allow collaboration between NASA engineering design teams. The Collaborative Engineering Environment (CEE) Project was created. Under the leadership of Mr. Doug Craig from NASA Langley Research Center, the NASA CEE project was able to quickly develop a prototype CEE room and deployed CEE rooms in all ten NASA
centers within 1 year. The CEE rooms allow engineering teams from different NASA centers to see and hear each other, to share presentations, design data, view and manipulate CAD drawing together over the network in real-time.

The NASA investment in the CEE Project saved NASA significant travel funds and time, and greatly increased productivity. Much of the improvement in team collaboration and productivity was difficult to measure, however on one of the projects that we supported; we did record some quantitative numbers. This project was a deep space mission between a NASA center and a NASA contractor. The design team was flying people back and forth between the two locations. We invested $70K on equipment for two CEE rooms. The team recorded saving of 70 man-trips in the first two months after they started using the CEE room. By this measure, all the investment in equipment was paid back in just two months.

The CEE rooms turned out to be a huge success. The initial 10 CEE rooms were copied numerous times. It was also adopted as a standard by the NASA video conferencing teams. Similar rooms are still being built today to support NASA mission design teams.

Because of the success of the CEE Project, we started to look at extending these collaborative capabilities to engineer's desktop and NASA's contractors' locations. We learned that building collaborative desktop is very different from building isolated collaborative rooms. Our initial estimate of a short 12 month project turned out to be a four years journey with many twists and turns.

**Collaborative Security Problems:**

What we did not realize was that we were stepping into a mine field full of organizational boundaries, inter and intra-enterprise relationships, differences in priority, and even some fundamental problems with the ways that network security is performed today.

One of the first things we did was to go out to talk to our customers. Through our discussions we detected their frustration with the loss of control over their projects security issues because of their Site or Center security requirements and policies.

One of the fundamental problems is that the people who run the security of an organization, i.e. a NASA Center, are different from the people who run projects/missions. While the project manager is trying to improve collaboration for distributed team members located outside of the local organization, the local security personnel of the project manager's organization are trying to only protect the local organizations networks from outside attacks. Both the project and the local security teams are trying to do a good job from their own perspectives.

The local security personnel are trying to protect the location behind the network firewall where there are many projects co-located together. If a computer used by one of the project behind the firewall is compromised, other projects' computers are also at risk. An intruder may use this computer to attack other resources. In order to protect all the
projects, the security personnel, who typically work for the local organization, not the individual project, has to enforce very strict rules to protect all the projects. These rules create problems for project managers who have team members all over the country and world. This is the reason why there are exceptions to the rules because of the need by certain projects to work with other partners. These rule exceptions or “holes” on the firewall usually take a long time to be negotiated between the company’s security personnel and the project. Because of the difficulty, very often, projects decide to create their own security areas and network connections in order to have better control over the situation. This leads to high cost and duplicate capabilities.

These firewall holes are also very difficult to manage. For example, the last thing on a project managers’ mind when they are closing down their project is to inform the security personnel to close the project’s firewall holes. This leaves many holes on the firewalls that nobody dares to touch due to lack of information about the project status. Many NASA Centers are trying to close all the firewalls holes but this prevents projects from accomplishing their work. Centers are trying to setup special demilitarized zone to host services that need to be shared with outside partners. Project managers do not like it because they lose the flexibility to control their resources in the demilitarized zone. This is another reason why there is friction between the local security team and the project teams.

Another problem for local network security is that each project has a unique set of requirements. One set of security rules may not be able to satisfy every project’s need. It is often necessary to give each project certain control where they can manage the network connections independently. If not, projects often figure out a way to do their job in spite of the security. This is often a reason why there are so many “stovepipes” in a Center when it comes to networks. These stovepipes prevent NASA from efficient management of knowledge. Security is perceived to be an enemy of knowledge.

Many network security technologies such as Virtual Private Network (VPN) and application firewalls are been added to the company infrastructure to handle remote access requirements. But these technologies bandage the networks to handle collaboration requirements and bring additional confusion when VPNs aren’t permitted through the network firewalls. Frequently private extranets and VPNs have been used to handle cross enterprise collaboration issue. A significant security issue is if someone from a partner’s company who has VPN access into our company’s network is fired by a partner’s company. We have no idea that it just happened. The person can still connect into our company and can cause severe damage. It is difficult to decide which company is liable for the damage. This is why most companies take a conservative approach that offers very limited, if any, VPN collaboration capabilities when dealing with partner companies. Projects often built their own VPN systems which make the stovepipe problem worse.

This problem of differences between enterprise securities vs. project collaboration requirements is going to be more significant in the future world of Web-Services and Grid computing. The HTTP tunneling and application firewall mechanism of the Web
Services is assuming that the user application is clean and approved by security people. However, if there is any vulnerability in the application or any user performs an upgrade on an application without getting approval from security. Hackers can get in through this application and threaten other resources in the enterprise. This moves the defense of the enterprise from a single point (firewall) to many servers located throughout the company. It makes it very difficult to defend the company from attack. Enterprise firewalls need to be very powerful to understand the state information of the traffic within the tunnel. This means that enterprise security people need to understand the business logic of all the projects within the enterprise.

The GRID computing Virtual Organization (VO) has a good way of handling the resources sharing across different companies. Resource owners determine how, when, what is available for access. This is a very good model for scientific computing where scientists have control over their server and applications. However, in many organizations, resource owners (project managers) may not have the final say on whether the resource can be available. For example, if the access involves International Traffic In Arms Regulations (ITAR) controlled data, organization security people and the international affairs office will also have to approve the resource access from outside of the organization. The GRID resource owner controlled model needs to be improved to accommodate the hierarchical organizational involvement.

Many government agencies are trying to take the traditional approach by building two separate networks; one for public access and one for private use only. The obvious problem with this approach is the cost of building and maintaining two separate infrastructures. The cost is not just the network but also the secured computers that are attached to the network. We often end up with two computers on our desktop; one for Internet access; one for secured network access. It is very difficult and very costly to maintain this nationwide secured network and enforce security at every desktop. In this day and age of fully connected cyberspace, this old school idea is not going to work.

Firewall plays a critical role in today’s defense against the cyberspace attack. But is it the solution for the future? There are two ways to use a firewall to protect organizational security; perimeter based security and host based security. The perimeter based security uses firewall to create virtual walls where all traffic comes in and out of the organization through the firewall only. The problem with this model is that the technology is surpassing the firewall. Wireless technology is going to be everywhere. Many new notebook and handheld devices come with different wireless access technologies built-in. 3-G wireless Internet access is already happening in Japan and Europe. The traffic of the wireless network is not going to go through the organization’s firewall. It will be very difficult to enforce policy not to use wireless because it is going to be pervasive.

The problem with the host-based defense is that individual users control the host. Because of the inconvenience of the host based firewall software, the person who operates the computer may disable or reconfigured the system. This defeated the purpose of the host-based firewall. The enterprise security cannot and should not rely on individuals. Trained enterprise security personnel should be involved.
The basic problem is that the security is an afterthought of the network design today. Firewalls were added to the organization's network after it's built. This is a fundamental problem that requires fundamental changes to the way the IT infrastructure is built today.

A summary of the collaborative security problems we faced when we started to built our collaborative environment are:

- Firewall blocking collaboration traffic.
- Conflict between organization security priorities vs. project collaboration priority.
- Slow organizational response to project collaborative security request.
- Difficult distributed user authentication, authorization, and management.
- New technology is challenging the effectiveness of firewall based security.

**Objectives**

What we are trying to accomplish is a collaborative environment where NASA project teams can securely share and exchange information, knowledge, and tools with their partners from around the world. A collaborative environment is not very effective if users can not leverage on the knowledge learned by other projects. One of our goals is also trying to prevent "stovepipes" project infrastructure where only one project can use the information generated from the project. The result of our product is a multi-dimensional collaboration grid of knowledge resources where multi-modal information, tools, and domain experts are available to NASA engineering teams when needed. These objectives may sound like a no-brainer. However, anyone who ventured into this will find very little support for what they are trying to do.

The problems are several. First, organizational security teams do not like it because they are doing their job to protect the organization perimeter. They are afraid that the project will do something with people from outside that will compromise the security of the organization. Second, project managers may not support it. This is because most of the project managers have their particular project goals to accomplish within a limited budget and schedule. A collaboration system that allows sharing of information and resources across projects may not contribute directly to the project goals or may not match the typical way the project manager used to do business. This is why project managers may not support an agency-wide system. For example, NASA has over 25 different documentation management systems; it is very difficult to tell a project manager to spend their limited resources to convert years of data into a new system or new sharing format. This makes sharing of knowledge very difficult. Third, partners may not support it. Because partners (contractors, universities, and other government agencies) typically are working on many projects at the same time with different customers. There may be trust between the particular project team within the partners' companies but that trust can not be extended to other projects. So, it is very difficult to get support from partners' organizations. Finally, the higher management may not support it. It is very difficult to support a long term project when both the security people and project people say they want to maintain the old way of doing business. It takes tremendous vision and courage
on the management side to support a project that makes fundamental changes to the way we do business today.

**SAFE - A NASA Solution to Secured Collaboration**

With the support of the Engineering for Complex System Program, Digital Shuttle Program, and NASA Johnson Space Flight Center Mission Control Center Program, we found our support from a NASA research program called Computing Information Communication Technology (CICT). The CICT Program is a visionary program that will make fundamental changes to NASA’s Information Technology (IT). Our goal of making fundamental changes to the way NASA collaborates is a perfect match to the CICT Program. Our project was named Secured Advanced Federated Environment (SAFE) Project. Because of the limited budget for the huge undertaking, we have to limit our task to solving the most common and also the most difficult issue first which is the collaborative network security issue. This is also the focus of this article.

One of the first things we realized was that the current way of putting many projects inside the same organizational security domain is not going to work if projects are going to collaborate with different partners. Instead of one organizational security domain which is based on physical collocation of different projects, the SAFE project proposed a concept called “Micro Security Domain” (MSD). The MSD is logical partition of the network security boundary. For example, a distributed project can form a MSD across enterprise boundaries. A project sub team can form a MSD. A computer can form a MSD. Even services within a computer can form a MSD.

MSD is compartmentalized; i.e. isolated from the rest of the network. The resources within a MSD can communicate but it can not communicate outside the MSD except through the gateway run by the organizational security team.

The purpose for the MSD is to create a network security domain where project managers have maximum control of what they can do within the project. The basic argument is that if they do not need to access organizational resources, the organizational security people do not need to control every detail of what the project does within the project.

Firewalls along with Intrusion Detection Systems serve a critical function in protecting the resources behind it from annoyance from outside. However, we do not think today’s firewalls are being designed and used correctly. Today’s firewall is designed to support many shared resources behind it. An enterprise class firewall not only needs to support giga bit per second speed from multiple network interfaces but also needs to be smart to handle weird protocol such as H.323 video conferencing and Web Services tunneling. This is the reason why firewalls are getting so complicated and expensive. These enterprise class firewalls also require a team of highly trained professional to run it. Even if this is the case; there is no guarantee that the enterprise is free from successful attacks.

However, many of us have $79-dollar firewalls at home that we manage. It does a pretty good job and we don’t need to pay anyone to run it. It is not as powerful as the enterprise
class firewalls but it serves our purpose well. Instead of a complicated firewall, the SAFE project proposes the concept of "micro firewall". Micro firewalls are simplified firewall that serves the purpose of the MSD. A micro firewall is closely associated with the networking layer. It may be manufactured in the same device as a router. The simplicity and close association with an individual network line gives the micro firewall the advantage of matching a very high speed network. A MSD can contain multiple distributed micro firewalls. Distributed firewalls work together under a shared rule set to protect the MSD. It may be connected with encrypted tunnels to other micro firewalls in the same MSD. The micro firewall gives the enterprise security team capability to monitor and control the activities within the MSD across enterprise boundary if policy allows. Because of the limited space, the micro firewall design will be presented in another paper.

Because the MSD serves one project, the rule set for the micro firewall is very simple. External access to servers within the MSD is denied by default. The access to servers within the MSD is granted per application or by default if the policy allows. Because the applications are well known by the project people, it is much easier to allow or deny without the worry of impacting other projects. If the project needs to access services outside the MSD, it has to come through an access gateway which is controlled by the organization security people. So, conceptually the enterprise is composed of many MSDs with a highly controlled gateway.

Another important characteristic of SAFE is automated hierarchical security. Most of the organization has security policy and rules. In order to get approval to collaborate with people outside of the organization a project needs to discuss with the organization security people, write a security plan, get Configuration Control Board approval, and wait for the changes of firewall rules to be implemented. This can easily take six months or longer. Sometime we wonder the value of this process, does it make the project more secure or is it just a process to discourage project from collaborating with outside partner and cover the organization security team just in case something goes wrong. In order to speed up the process, we have seen many projects decide to implement their network infrastructure (stovepipes) which is independent to the organization infrastructure. The problem is that there is no uniform way of managing these stovepipes and enable sharing of knowledge across these stovepipes. The loser is the tax payer who pays for the project.

The SAFE project proposes that we should automate the security approval process. We developed a tool called Security Rule Editor (SRE). The SRE is a graphical user interface tool that allows input of the security rules which automatically configure the micro firewalls. The SRE has inheritance. The organization security people can define security rules which are automatically imposed on the SRE that project people use. Only when exceptions are needed will the project people need to go through the security approval process. Because the MSD creates a independent security domain, as long as the project communication does not leave the MSD, the inherited rule set should be very simple. The responsibility is pushed down to the project manager/security people where the responsibility should belong.
The SRE also serves a very important function of creating a point of discovery of information and tools. Because the project personnel need to enter information in a standard format through SRE, this information is also available to the enterprise directory for discovery purpose. We are currently looking at the ways of producing standard format so that we can work with standards such as UDDI.

Another key element to the hierarchical security approval is the LDAP joint technology. Security right revocation is more important than security approval. The rules defined in the SRE are combined with the capability to read and verify from multiple LDAP directories in real-time. For example, if a person is just fired by the organization, the Human Resource Department takes this person out of the Human Resource LDAP directory. Even the person may still be in the project directory, this person is denied access because the SRE rule requires LDAP joint use of the project directory and the HR directory. This offers instant revocation of access rights.

The third important characteristic of SAFE is group based federated user management. In order to support real-time collaboration across enterprise domains, we need a way to manage users across enterprise boundaries. The first question that comes up is the issue of trust. How can we trust a user from a different enterprise if we do not know the person? We believe the answer is to look at how people work today. When a person calls up and requests access, we typically ask the person’s boss if this person is trustworthy. If we can automate this group based trust process (or capability based trust) where A trusts B, B trusts C so A trusts C, we may be able to achieve real-time collaboration.

To enforce the group based trust across enterprise, we need a common trust infrastructure. It is hard enough to built trust within a company. Building trust across companies requires careful agreements. A more important issue is the penalty if one of the parties does not follows the common agreement.

There are a lot of discussions on what is the best trust model. The SAFE uses a centralized trust model within an enterprise. This is mainly because the ease of implementation within a large enterprise such as NASA and with NASA’s primary contractors which include many of the largest corporations in the country. The model is based on a common trust infrastructure called Federation Proxy Server (FPS). The FPS provides functions such as publishing and exchanging legally binding security policies and rules to collaboration partner’s corresponding FPS, enforcement of rules within the company, and serves as the access proxy to remote services if granted by policy of the common MSD. The FPS enforces the rule set defined by SRE to ensure the security for MSD that crosses the organizational boundary. This can be intra or inter enterprise access.

The SAFE project created a unified architecture model to give project managers the maximum flexibility to run their project, give organization security teams a unified way to manage collaboration security, give NASA a unified way to shared services and knowledge across the agency, and give NASA partners a way to limit collaboration with trusted teams only. The SAFE provides a foundation where trusted distributed services
can be offered easily across NASA center organizational boundaries. NASA can put different types of agency-wide services in different Common Services MSD. Depending on the security requirement, NASA can dynamically allow or deny access to common services. These Common Services MSD will play an important role in the long term knowledge management for NASA.

**Putting It Together**

The SAFE project is a multi-center collaborative research project. Three NASA centers are involved in the project: Ames Research Center, Jet Propulsion Laboratory, and Marshall Space Flight Center. The pilot SAFE system includes a rack of equipment called SAFE Rack. There are six SAFE racks located in six NASA centers: Ames Research Center, Jet Propulsion Laboratory, Marshall Space Flight Center, Johnson Space Center, Langley Research Center, and Kennedy Space Flight Center. The first phase SAFE implementation is being used to support the Digital Shuttle Program and the Mission Control Center at JSC. The following figure shows the network connection of SAFE racks.

The following figure shows the SAFE logical architecture. The SAFE rack is connected with encrypted tunnels across NASA centers. The SAFE rack uses a COTS software called AppGate to provide front-end user interface and application firewall function. The SAFE rack serves as proxy to servers within MSD. Users can access services through the SAFE proxy.
One interesting characteristic is that SAFE resources are “cloaked”. Unless a user can authenticate into the MSD, the services within the MSD can not be seen by the user. User cannot even “ping” the server. User connection to the SAFE is through a Java based Secured Shell tunnel which works on most platforms.

When users obtain a SAFE account, the user can not do much with SAFE. The SAFE MSD access is delegated to a project account manager. The project manager has to put the user into the project group before the user can see the services offered by the project MSD. Once logged-in, the SAFE AppGate downloads a personal firewall software on the users’ machine. This personal firewall software limits the user access to other resources when connected to the MSD. The policy for the personal firewall software is defined for the MSD and it can not be changed by the user.

This SAFE user account is good no matter where the user is located. If the user travels to different NASA centers, he/she can login and work exactly the same as in his/her office.

We are currently working on the FPS with integrated SRE. Once completed, NASA projects can dynamically create or destroy collaboration groups. NASA enterprise security teams can enforce security policy automatically. NASA engineering teams can provide common engineering tools and services across NASA. NASA knowledge teams can deploy NASA-wide common services securely. The implication to NASA is significant.
The Future

Security has been an afterthought of the network design. Typically, a security domain is created on top of the existing network based on physical organizational boundary. The key to security is trusted inside vs un-trusted outside. Because of different requirements and defense in depth, an enterprise often needs to build several network layers with different level of trust.

SAFE promotes just the opposite. In SAFE, there is no inside or outside of an enterprise security domain. The SAFE network is designed based on the functional security requirements. The SAFE MSD requires a project or a team to form one or more MSDs before the network is connected logically. If the project is distributed then the MSD is going to be distributed. Thus the SAFE decoupled the security domain from the physical restriction. The SAFE MSD is a logical collocation of the project and enterprise resources.

We envision the enterprise will change into a logical structure where the enterprise IT team's job is to maintain SAFE gateway, common services MSD, and FPS. This allows true virtual enterprise.

We also envision SAFE micro firewalls will be designed into networking chips. These simple micro firewalls will be so cheap that it will be provided for every network link. The following is a block diagram of a possible networking chip with SAFE capability built in.
Conclusion

The SAFE technology is an important step toward functional based enterprise security. It allows an enterprise to achieve the balance between the need for collaboration and the need to protect enterprise security.

Acknowledgement

This work was partially performed at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautic Space Administration.