Interim Operational Security Plan

Goals & Scope

GENI, being the large cooperative effort that it is, will rely upon the collaboration of several stakeholders (including, but not limited to the GENI Project Office at BBN, the NSF, the aggregate providers at many GENI-affiliated research organizations and campuses, the researchers developing GENI's infrastructure and many other partners) to provide a secure and stable research environment for scientists and engineers. The goal of this document is to lay down the structure of an operational security team and the basic processes for incident response as GENI begins rolling out significant infrastructure for experiments and research, namely the WiMAX and OpenFlow meso-scale build-outs. This is necessarily a living document as GENI is both changing and growing rapidly, and there has not been enough time to complete a full threat and risk assessment for GENI.

Roles & Responsibilities

In order to even talk about the processes to follow in the event of a security incident, it will be necessary to talk about roles and entities that do not yet exist. In this document we make recommendations about the creation of new positions within the GENI community, keeping in mind that these may or may not be created, at which point this plan will need to be revised. In the following we talk about the roles of these different groups and people.

GENI Computer Security & Incident Response Team (GENI-CSIRT)

Presumably, there will be a team with primary responsibility for investigating and responding to security incidents within the GENI community, which we will abbreviate as the *GENI-CSIRT*. If there is no such team, then tickets created around security issues will likely be passed around like a hot potato. There needs to be some party responsible for security who will take ownership of these issues and provide the very necessary role of coordination between organizations within the GENI community.

It is vital, for redundancy, that there be more than one person on this team. GENI will not take a vacation, and so we must have backups. It is also important for at least one person on this team to be funded more than 50% on GENI if they are to take ownership of security and give GENI priority. This team should be created with members from multiple stakeholders in GENI. For projects such as GENI is evolving into, a security team (in aggregate hours) should consist of at least 3 full-time employees (FTEs). However, GENI is still ramping up and may not need so many resources dedicated to incident response in Spiral 3.

The leader of this team, which we will call the *GENI Security Officer (GSO)*, needs to be at least 50% dedicated to GENI, and they need to have prior incident response experience. **The GSO will be responsible for assigning investigation leads for security incidents and also reporting back to the project office**. While the incident response team will collaborate closely with GENI Meta-Operations Center (GMOC) at times, it is not necessary that members of the GMOC be on the team. However, communication with the GMOC and a clear point of contact with the GENI Project Office (GPO) will be necessary. The security team will likely also rely on the GMOC for services like an incident investigation wiki and a network filesystem (for incident response data), email lists for users to report abuse and incidents, as well as a some sort of ticketing system, which the GENI-CSIRT will probably share with the GENI help desk.

In addition to the GSO role, there should be a *Deputy GSO* (DGSO) funded at at least 25%. The DGSO will fulfill all the duties of the GSO when the GSO is unavailable, but otherwise act as regular member of the GENI-CSIRT. During Spiral 3, GENI may be able to get along with just a GSO and DGSO on the GENI-CSIRT, depending upon the percentages funded.

GENI-CSIRT Responsibilities

The GENI-CSIRT will be responsible for resolving all help tickets related to security. The details of the incident response process for investigating such events will be described later in more detail. Because of the decentralized nature of GENI, much of this effort will be coordinating between organizations, ensuring security problems have been resolved before bringing equipment back online and making sure issues are followed-up upon and resolved. In the end, though, it will often be the individual sites providing aggregates which will have to make changes to their systems and provide evidence that they are ready to bring systems back into production. For centrally owned GENI resources, such as those at the GMOC, the GENI-CSIRT may be involved at a lower-level, e.g. hardening hosts, providing monitoring and developing security architectures.

The GENI-CSIRT will also have longer term responsibilities of planning and auditing. They will be responsible for maintaining and updating security policies, auditing compliance with policies and providing appropriate security training and education to the GENI community. Lastly, if GENI is to run a Certificate Authority (CA), the GENI-CSIRT will at a minimum develop policies regarding its administration and configuration and need the ability to revoke certificates. Actual day-to-day system administration of the CA could fall to the GMOC or GENI-CSIRT.

Aggregate Owners and Campus IT

Those providing resources to GENI, the aggregate providers who are mostly on university campuses, have responsibilities to ***prevent, report and***

respond.

Prevention

For major resources, especially those common across many campuses, the GENI-CSIRT may provide specific hardening guidelines. However, it is always the responsibility of the providing organization to protect their own aggregates and components. At a minimum, this means keeping systems up-to-date and patched against security threats, running the minimal number of services, keeping good system logs, giving administrative access to only those who need it and using strong authentication for administrative accounts. This is important not only as their components have trusted connections to others, but credentials and certificates from GENI users will likely exist, if only ephemerally, on their systems. They have a responsibility of due diligence to protect those credentials and experimental data.

Reporting

It is expected for those providing GENI resources to report when there are incidents on their equipment, if that equipment is a GENI resource. This follows as the problems may affect other parts of the GENI infrastructure, but also it will help the security team see the bigger picture and trends. For example, an incident at one site may just be the first of a new exploit being tried out on many other pieces of GENI infrastructure or a piece of a larger attack.

Reporting a problem to the GENI-CSIRT (through the help desk at the GMOC most likely) does not preclude a site from reporting to their own security team or CERTs. In fact, it is expected that security teams at their own institutions will lead the investigation on their side. What aggregate owners are precluded from doing is sharing information they may learn about a similar incident at another GENI affiliated organization (usually in the course of an active investigation) with either the media or any external entity. The privacy of individual organization must be respected in the course of investigating incidents, and both the GENI-CSIRT and individual organizations have the responsibility to protect that privacy.

Response

If one expects to maintain resources in the GENI ecosystem, they must be responsive to requests from the GENI-CSIRT as they agreed to in the Aggregate Provider Agreement. Response here may just mean acknowledging an issue, or it could mean shutting down slices, slivers, components or whole aggregates temporarily. It could also mean proving that a host has been cleaned-up and properly recovered.

Part of being responsive is providing up-to-date contact information for the person(s) responsible for the aggregate and providing a contact at the institution's incident response team. Acknowledgment to requests from the GENI-CSIRT are expected within 24 hours, but that does not preclude the GENI-CSIRT from disconnecting a resource from GENI in the case of an emergency even sooner.

GENI Project Office (GPO)

The GPO gives the GENI-CSIRT the necessary authority to do their job. They provide oversight and clarify the requirements for security and operations. The GPO is also the connection back to the NSF who will expect to hear about major incidents from the GPO before any back-channels. To achieve all of this, there needs to be a clear chain of command from the GSO to a specific person at the GPO up to the NSF program officer.

The GPO representative is also the only one who is to talk to the media about a GENI incident, and they will do so protecting the privacy of individual organizations. Of course, individual organizations can talk about their own site in isolation, but if they are talking about an incident involving a GENI resource they must not make mention of GENI or anything they learn about the incident at other sites.

Others

As mentioned, their are numerous stakeholders and most any of them could be pulled into an investigation. Security is a collaborative effort, especially in GENI. For example, an incident involving an exploit of the control framework found in the wild would require then help of one of the developers of the control framework. Therefore, it is possible in any large incident that a special team may have to be formed from a diverse group of GENI participants.

Incident Classification

High

The incident could lead to exploitation of the trust fabric, i.e. user and host identities; or the incident could lead to instability or misuse of the overall GENI ecosystem. This type of incident will require the GSO to assign an investigation lead and likely require members external to the GENI-CSIRT to be pulled into the investigation. This type of incident must also be reported to the GPO immediately and to the NSF from there.

Medium

The incident affects an instance of a GENI service, but GENI stability is not at risk; or a denial-of-service affects one replica of a given GENI service; or a local attack compromised a privileged user account. This type of incident may require an investigation lead if wide-spread enough. It

must also be reported to the GPO immediately.

Low

A local attack comprised an individual user, non-privileged credentials exposed; or a denial-of-service attack or compromise affects only local GENI resources. This type of incident does not require an investigation lead. It also need not be reported to the GPO out of the normal reporting schedule.

Information Classes

Sensitive Personal Information

This type of information has challenging security requirements and is incidental to planning, provisioning or using GENI. Examples are user names, passwords, social security numbers, and credit card numbers.

Some of these, like SSNs and credit card numbers, are legally protected. While users are prohibited from intentionally storing legally protected personal identifying information on GENI systems, it is always possible that such information could end up on an aggregate due to the activities of a cyber criminal compromising the host.

GENI Restricted Data

This is any non-public GENI information that is not personally identifying. Most information generated as part of an incident investigation will be of this type until the final, public report is made.

GENI Public Data

This is data that has no privacy requirements. Data that is not explicitly classified is presumed to be public.

Data Classification Process

The GSO will determine the classification of any information from a security incident based upon the definitions above. These same definitions could (with some modification) be used by other groups in the GENI community, but it is up to the GPO to decide who has the responsibility to determine the classification in domains other than security.

It is also expected that most everything done in GENI will be public, and that should be the default level for information not otherwise classified. The exception is that the default for an *active* GENI security incident is *GENI Restricted*. This is important to encourage cooperation and information sharing that is critical to prompt incident response.

Incident Response Process

The incident response process used to investigate all GENI security incidents has 7 steps: *Discovery and Reporting, Initial Analysis & Classification, Containment, Notification, Analysis & Response,* and *Post-incident Analysis*

Discovery & Reporting

Incidents will be discovered through a variety of means including users, system administrators, engineers, and peers; operations center monitoring of infrastructure, services, and resources; and through monitoring of intelligence channels.

When an incident is discovered that relates to GENI resources, services or identity, it MUST be reported to the local institution incident handling process AND the discovering/reporting party MUST ensure that the incident is reported to the GENI Meta-Operations Center (GMOC). This can be done through special *security* or *abuse* email lists, presumably run by the GMOC. The help desk at the GMOC must then create a ticket which will alert the GENI-CSIRT to the new incident. Secure internal communication can then be made through the ticketing system.

Initial Analysis & Classification

It is critical to understand the scope and severity of an incident. Therefore, as a new ticket is received, the GSO will evaluate the incident and classify its severity by the 3 definitions discussed above for high, medium and low severity incidents.

Classification will likely require some discussion between the reporter, the GENI-CSIRT and the sites involved. Also, the classification may change as more is learned about an incident. Still, it is important to try to classify the incident early to know the amount of attention to give it and

whether or not it must be reported to higher levels.

The second goal of this step is to create the right team if necessary (it may only be necessary to decide which GENI-CSIRT member to assign a *low* incident to). For example, if it is clear that a GENI software or firmware vulnerability is being exploited in an attack, then team being setup for this investigation needs to include GENI developers as well as some sites who will beta test the patch or remediation solution.

Containment

As a general matter, the level of response must take into account a number of factors, including, but not limited to:

- the resource/service has been compromised or is it just under attack?
- the kind of attack — DOS or user or privileged user compromise?
- the importance of the resource/service locally?
- the importance of the resource/service to the operation of the GENI test bed?
- the importance of the resource/service to various PIs and projects?

As an operational principle for an aggregate *under* attack, the normal response should be to block access from GENI during the initial stages of dealing with an intrusion – only opening access as is prudent and justified, without extraordinary risk. Of course, aggregate owners SHOULD inform the GMOC of actions they take affecting GENI resources/services.

If it is determined that the attack comes from a specific user account or slice, the more reasonable response would be to temporarily deny access to the resource or service through the appropriate local control for authorization. Again, such action should be reported back to the GENI-CSIRT (through the GMOC) who will follow up the appropriate PI corresponding to the offending slice or user.

We must also consider what to do about an aggregate from which an attack is *launched*. A problematic aggregate or service might be reported by another GENI aggregate, an aggregate or ISP on another test bed federated with GENI, or might be discovered by the monitoring capabilities of the GMOC or GENI-CSIRT.

One would like to believe that the GMOC would generally have the ability to block a site or service that was misbehaving, and while that might be true in cases for specific centrally controlled services, it will not be true for the vast majority of services on GENI nor will it be true for federated GENI-like testbeds that have their own operations centers.

Depending on the severity of the attack and based on the other aggregates and slices potentially affected, the GENI-CSIRT will attempt to notify the affected aggregate providers so they can take appropriate action to protect themselves. The GENI-CSIRT may ask the offending site to disable specific slivers, whole components or in extreme cases (when an emergency stop is required) disconnect sites from the GENI backbone.

The second phase of containment is the process of narrowing down the things that are blocked to the specific componets, resources, services and users which were compromised. Incident response teams at the aggregate providers, in communication with their peers, are expected to restore normal operation as quickly as the problem areas can be identified and isolated.

Notification

Any incident requiring a team leader MUST be reported to the GPO. Furthermore, a report on the incident SHOULD be sent to the GPO upon resolution of the incident.

Any incident rated as *high*, must be reported back to the appropriate NSF program directors through the GPO. It is important that the NSF first hear about an incident though the GPO rather than the media.

Analysis & Response

This is the step where an in-depth analysis is done and a path to resolution is established.

Resource Tracking

Since the total cost of the incident is often important for legal action, the GENI-CSIRT and any aggregate owners involved should track:

- the number of man-hours spent on response;
- the extent of the damage;
- what resources where made unavailable; and
- how long said resources were offline.

This is also a good time to assign attributes to incidents for categorization in annual reports. In addition to just the severity of an incident, it is usefully to track the organizations involved, the type of exploits used, and the types of vulnerabilities used for entry.

Evidence Collection

All supporting data for an incident MUST be treated consistent with the aggregate owner's rules for maintaining and storing such materials in non-GENI incidents. Collection and coordination of evidence between aggregate owners is expected to be handled by the appropriate law enforcement agencies.

Removal & Recovery

Determine the extent of known and potential compromise of user and host credentials and passwords. Did the initial containment step treat the entire scope of the compromise? Work with contacts to revoke/suspend credentials, keys and passwords.

Point of entry should also be established, and if a vulnerability was exploited to gain access, that vulnerability must be patched. If this vulnerability is likely to affect other aggregates, they MUST be notified by the GENI-CSIRT. If applicable, any IDS or log monitoring system SHOULD have updated rules to detect this threat automatically the next time.

Any malware installed must be removed, and components must be shown to be clean before the GENI-CSIRT authorizes their reconnection to GENI.

Post-Incident Analysis

At the end of an incident, the investigation lead (if applicable) schedules a conference call to review the lessons learned and formulate feedback to appropriate groups (e. g. GENI participants, management, developers). A close-out report MUST be completed within 1 month following the incident. This report will be given to the GPO but also made public in a sanitized form to protect the identity of individual persons and organizations. This will help prevent the same mistakes from being repeated.

Auditing

Any security plans developed and monitoring infrastructure rolled out by the GENI-CSIRT needs to be audited and evaluated regularly. Reviewing security plans is especially important as GENI is very dynamic in these formative years. Therefore, security plans MUST be reviewed and updated annually.

The audit schedule for the security systems (whether preventative, detective or reactive) must be developed as such infrastructure is rolled out. Currently, there is no security team nor security infrastructure to monitor. In addition to services managed directly by the GENI-CSIRT, they will also want to regularly audit the future GENI authentication and authorization systems. These systems have yet to be standardized at this point, though.

GENI will be relying upon services provided by many parties, and it is prudent to test the security of the major aggregate providers. The GENI-CSIRT SHOULD, with approval, randomly test the security of major aggregates, developing reports and recommendations from their findings. Furthermore, the GENI-CSIRT SHOULD perform exercises to test incident response procedures ahead of time and before a real major incident occurs during GENI's future production phase. Exercises involving several different parties will help to discover cracks in the system and potential problems or bottlenecks.

Recommended Threat Countermeasures

Based upon the draft Threat & Vulnerability Report **(scoped to OpenFlow & WiMAX)**, there are several recommendations we would like make for handling potential threats. As Spiral 3 progresses, and we develop a more general threat & risk assessment, these recommendations will broaden in scope and may in fact change individually. This part of the security plan, much as any other, will have to change and adapt as GENI develops, re-emphasizing the point that the security plans must be regularly reviewed and updated.

High Priority Threat Mitigations

Here we discuss policies, procedures and technologies that MUST be implemented to protect GENI's assets in the near term.

Communication between aggregate owners and GMOC

As the team at the GMOC has been developing the Emergency Stop Procedure, they correctly realized the importance of having up-to-date contact info at each aggregate provider. They have been collecting this info, and we have included it as part of the draft Aggregate Provider Agreement. In addition to having contact info for the person in charge of an aggregate, we are also requesting a security contact at that organization. This would be a person to whom they report a local security incident. This information is important to have as the GENI-CSIRT would want to be in contact with the local institution's security team when coordinating any sort of investigation. Furthermore, the admin of the aggregate will probably not be a 24/7 on-call person, but someone from the security team at the aggregate provider's institution should be.

In addition to having contact info so the GMOC can contact an aggregate, the aggregate needs contact info for the GMOC, both via phone and email. It is important for the GMOC to have a callback number known to all aggregates so that they can verify the GMOC's call, should someone try to impersonate the GMOC with a fake request. The GMOC is providing such a number to aggregates as they collect contact information from them.

Law Enforcement Requests

The GMOC needs to have policies for handle requests from law enforcement, especially when the requests involve multiple GENI-affiliated organizations such as aggregate providers. If there is only one affected organization, it may be as simple as passing on the request to the

appropriate parties. The aggregate providers also need to know what to report back to the GMOC and GPO should they receive any legal or law enforcement request regarding a GENI resource. The GMOC will be interested because at a minimum, it may affect the availability of that site's aggregate and in the worst case such a request may pull in researchers and aggregate providers from many other institutions.

Therefore, it has been planned to develop such a set of policies and procedures for presentation at the GEC 9.

Log Retention

If there is a security incident on GENI infrastructure, it will be important to have good logs at the aggregates for both their internal investigation and any incident analysis done by the GENI-CSIRT. We expect the individual aggregate owners to follow their own institutional policies for log retention, and if possible, they should retain security relevant logs for GENI components for a year. It is also imperative that logs have accurate timestamps and that they are archived with the relevant time zone information to make cross-correlation possible.

Hardening Guidelines for GENI aggregates

Significant trust is put into the ability of the WiMAX base stations and FlowVisor hosts (including the E-GENI aggregate manger) to provide isolation between experiments on different slices. There are security, privacy and stability reasons to ensure strong isolation via their different virtualization techniques. Furthermore, these hosts are critical infrastructure for this meso-scale build-out in Spiral 2 and must be protected.

Because we do not have access to the WiMAX kits and the E-GENI aggregate managers, we can only speak in generalities about the hardening of these hosts (not down to the level of specific files to be monitored by a file integrity checker). Furthermore, these devices are under active development and any low-level guidelines would quickly become out of date. Therefore, specific configuration guidelines should come from the teams developing these kits.

With this in mind we recommend the following:

- A separate interface (whether virtual or physical) should be used for administration of these hosts and connectivity to GENI.
- Administrative accounts should use two-factor authentication.
- Any local accounts on these hosts must use unique passwords, not shared across other unrelated devices or hosts.
- Unnecessary services and accounts should be disabled.
- Security patches must be kept up-to-date. **The developer of the WiMAX kits and the E-GENI aggregate manager are in the best position to monitor for updates to the software and should utilize email lists to notify the appropriate aggregate owners when they need to update software.** The aggregate owner must of course also monitor for any updates for additional software they may add.
- The number of setuid programs should be minimized as they can be used for privilege escalation along with new zero-day exploits.

Education and Policy Adoption

It is vital in a federated community like GENI to get buy-in from all the major stakeholders for any security policies or plans. This can be achieved by allowing all stakeholders to provide input into the process. The regular GECs are one of the only opportunities to bring people together to discuss these issues, and we should use the GECs to gain consensus on all security plans and policies.

Education of security policies and procedures are a major component of any good plan. Simply posting documents on the web and having aggregate providers and users sign agreements that they have read them is not enough. The GECs should also be used as a venue to disseminate this information, as broadly as possible to all relevant parties. A security track at these meetings could be used to achieve this, but that would give too many the opportunity to miss the presentations. Rather, it is probably better to integrate security into other major discussion topics.

At this time, there are no teeth to the security policies. This makes consensus all the more important, but still some clear consequences will have to be spelled out for abuse. The only organization with any "power", is the GPO as the holder of the proverbial checkbook. Therefore, the GPO must make clear the importance of security to the project and ensure that there are real consequences to non-compliance. Furthermore, if they are to delegate any responsibilities for enforcement, that must be clear to the GENI community.

Medium Priority Threat Mitigations

These policies, procedures, and technologies SHOULD be implemented within the next year to protect GENIs assets.

OpenFlow firmware update distribution

When there are security vulnerabilities addressed in OpenFlow firmware updates, it is critical that they reach all the OpenFlow deployments. Furthermore, it is desirable to coordinate these updates for the stability of GENI as multiple OpenFlow versions could create interoperability problems. Therefore, we recommend that the GMOC be involved in coordinating important updates and ensuring that they are distributed securely to all parties. This could mean that they actually host secure update servers, or it could mean that they simply maintain an email list to which they submit signed messages when important updates are available with instructions as to how to get the update. Regardless, the GMOC will need policies and procedures in place that define their responsibility, such as, whether or not they will verify that updates have been installed at the different aggregates.

Secure communication for the GENI-CSIRT

The GENI-CSIRT will need a way for its members to communicate securely. This could be through a help desk ticket system, though they will likely need more than that. They will need a wiki to collaborate on documents as well as some sort of content repository to store things like exploit code and malware discovered. If this content repository could utilize WebDAV in a way that they could link from the wiki to specific files, that

would be ideal.

If email lists are used, they must be private and unlisted. Furthermore, encryption through PGP or some other means should be used. Forcing communication through a secure ticketing system would likely be simpler than trying to secure email, though.

Related to this, the GENI-CSIRT must have a way to communicate securely with the aggregates, PIs and other users. Therefore, they must have both a publicly available callback number and an S/MIME certificate for official emails.

Configuration Checklists

The developers of the WiMAX kits and the E-GENI aggregate managers used for OpenFlow need to provide the aggregate owners with good documentation about configuring their resources securely. If possible, they should produce simple checklists for proper configuration of the base stations and E-GENI aggregate managers. This should be especially practical for the WIMAX kits which will be deployed in almost the exact same way across all sites. OpenFlow may be trickier as there is more customization.

File Integrity Checkers

The WiMAX kits, E-GENI aggregate managers and any other FlowVisor setups should use file integrity checkers (e.g., Sam Hain, Tripwire or Monit) to monitor for changes in key configuration files. The developers of the E-GENI and WiMAX kits should identify a list of files to monitor. In conjunction with a proper change control process at the aggregate owner sites, this could detect both malicious and accidental misconfigurations.

In addition to the configuration files, those sites using FlowVisor to separate production traffic from research traffic will want to ensure that those rules are not changed. Assuming that the production traffic rules are somewhat static, those rules should be monitored for changes by a file integrity checker if technically feasible. This will help protect the separation between production and research traffic.

WiMAX Interference

It is likely as WiMAX becomes more popular outside of research circles, that there will be problems of interference from time to time. Each aggregate owner should have its own internal policies for how to deal with complaints of interference. GENI does not need a federation-wide policy on how this is handled, though.

All of this presumes that there is a way to detect WiMAX interference. Such a capability would be useful at the aggregates to detect a DoS attack, but probably not necessary because (1) the attack is unlikely and (2) it would likely be noticed by the problems it would generate for experimenters and the peculiar measurement numbers such an attack should generate.

Since little can be done if there is interference in many situations, the most appropriate action is preventative. Therefore, aggregate owners deploying WiMAX kits should carefully plan the placement of WiMAX on their campuses to avoid future problems of interference. The GPO can do little to help them with this, though.

Low Priority Threat Mitigations

These policies, procedures, and technologies should be considered and debated as to their utility. The costs of many of these are unclear, and they would need to be determined to decide if these countermeasures are worth implementing.

Code Audits

Many of the threats against OpenFlow discussed in the threat and risk report could be realized if the OpenFlow firmware on routers and switches was exploited or subverted. This raises the point that this is important and trusted software that needs a high level of assurance. Unfortunately code prototyped and developed by academic research groups often have a poor track record of security, and without an external code review, we may not be justified in putting that much trust in this critical software component. Therefore, we recommend a professional code review of the OpenFlow firmware.

Similarly, FlowVisor is a critical part of providing privacy, security and isolation between experiments. For all the same reasons as above, we recommend a professional third-party code review of the FlowVisor software.

WiMAX encryption for experimenters

Just as WiFi has WPA, WiMAX has PKM (Private Key Management). Using PKMv2 to manage keys along AES encryption provides robust protection against eavesdropping and integrity checking that will detect any packet manipulation. While an experimenter should in theory be able to implement PKM, it is wasted effort for each experimenter to re-invent the wheel and figure out a way to do this. It would be more ideal to provide tools that allow an experimenter using the WiMAX base station to simply and transparently turn on encryption in a single config file.

This would encourage more experimenters to use encryption for purposes such as protecting the privacy of opt-in users. However, another project may need to be funded for this work to happen.

Stronger virtualization

The current WiMAX base station kit uses UML (User Mode Linux) to provide separate virtual base station interfaces to the experimenters in different slices. UML guarantees significantly less isolation and non-interference from VMs as compared to VMware or Xen. This increases the risk of (1) interference and exposures between slices and (2) the risk of one experimenter breaking out of the VM "jail" and controlling or affecting

the host OS on the base station.

For these reasons, we recommend migrating towards stronger virtualization solutions. In fact, some of the reports and documents from the WiMAX kit project indicate that they would like to head in that direction eventually.

GENI Intrusion Detection System

As GENI grows, in the future it would be helpful to utilize a distributed IDS to detect threats that could not be noticed easily with the perspective of an individual aggregate. Such an IDS would ideally be administered by the GENI-CSIRT. The appropriate configuration and architecture is not obvious at this early point in GENI's evolution, though it would likely involve some standard type of sensor being deployed at all major aggregate providers to monitor traffic and perhaps consume other types of system logs. These sensors would forward data to a central location for correlation and analysis.

Development of such an IDS would likely require an entire GENI project devoted to its creation. Further, the GENI-CSIRT would likely first need some operational experience with GENI to develop the requirements for such an IDS.

Key Managment

While SSH public keys and certificates have overcome many issues with passwords in the grid community, they still suffer from the problems associated with users managing these credentials insecurely. In particular, users tend to store the associated private keys in the clear on their workstations and many remote hosts. This makes them very susceptible to harvesting attacks.

Such issues can be mitigated by removing control of managing these credentials from the user. However, this must usually be architected into the authentication system early on with proxies being setup to mange credentials. It is hard to implement after the fact without hacking protocols or drastically changing user behavior.

Therefore, we suggest that as GENI's authentication and authorization system is being developed that consideration of this type of attack be given along each step of the way.

Flowvisor audit logging

In performing a threat and risk analysis of the OpenFlow deployment, we realized the necessity of being able to identify who creates any OpenFlow rules directing traffic. This is important after the fact for incident investigation, and it could be very helpful in the future for detecting abuse with an IDS.

Therefore, we recommend incorporating a robust and detailed logging mechanism into FlowVisor which would help to determine the origin of any new rules created on OpenFlow devices managed by FlowVisor. The most flexible way to do this would be to send events to syslog. That would allow audit logs to be forwarded to a remote server to preserve against deletion as well as to integrate with a future IDS more easily.