Threat & Vulnerability Report for OpenFlow & WiMAX Deployments

Document Name: Threat & Vulnerability Report for OpenFlow & WiMAX Deployments
Author: Adam Slagell
Version: 0.1
Date: May 31, 2010

This is an early, internal version, of the *Threat and Vulnerability Report* scoped to the current and upcoming WiMAX and OpenFlow deployments. It is the 4th milestone/deliverable in Spiral 2 and lays the foundation for the *Interim Operational Security Plan* due 5 weeks later.

This document makes two primary contributions. First, it lists the threat agents, i.e. the types of individuals or organizations that would seek to exploit vulnerabilities that would compromise some GENI asset. Several types are listed, but the ones that seem very*un*likely for GENI to have to contend with at this time, or in the foreseeable future, have been "grayed out".

Second, potential threats and incident types are identified. For each item, corresponding assets, which are affected, and potential vulnerabilities that would be exploited are listed. Where appropriate, commentary is made on the type of attacker (or threat agent) with capabilities to pose such a threat.

1. Related Documents

These related documents and resources all contributed to the development of this report, some of them indirectly as input to previous milestones upon which this document has been built.

Document ID	Document Title and Issue Date
GENI-SE-SYSO-02.0	"GENI System Overview", September 29, 2008. http://groups.geni.net/geni/attachment/wiki/GeniSysOvrvw/GENISysOvrvw092908.pdf
GDD 06-23	"GENI Facility Security," by Thomas Anderson and Michael Reiter, GENI Design Document 06-23 Working Group, September 2006. http://groups.geni.net/geni/attachment/wiki/GENISecurity/GDD-06-23.pdf
GDD 06-10	"Towards Operational Security for GENI," by Jim Basney, Roy Campbell, Himanshu Khurana, Vor Document 06-10, July 2006. http://groups.geni.net/geni/attachment/wiki/OldGPGDesignDocuments/GDD-06-10.pdf
GENI-FAC-PRO-S1-OV-1.12	"GENI Spiral 1 Overview", September 29, 2008 http://groups.geni.net/geni/attachment/wiki/SpiralOne/GENIS1Ovrvw092908.pdf
GENI-SE-SY-TS-UC-LC-01.2	"Lifecycle of a GENI Experiment", April 30, 2009 http://groups.geni.net/geni/attachment/wiki/ExperimentLifecycleDocument/ExperimentLifeCycle-v0
GENI-SEC-ARCH-0.55	"GENI Security Architecture", July 31, 2009 http://groups.geni.net/geni/attachment/wiki/GENISecurity/GENI-SEC-ARCH-0.55.pdf
GENI_Concept_of_Operations-final	"GMOC: GENI Concept of Operations", Oct. 1, 2009 http://gmoc.grnoc.iu.edu/uploads/8i/Gu/8iGu80-LqQB37VU4ZE1i5g/GENI_Concept_of_Operation
GENI-Security-Use-Cases-and-Stakeholders	"GENI Security Use Cases & Stakeholders", Jan. 15, 2010 http://groups.geni.net/geni/attachment/wiki/ComprehensiveSecurityPgm/GENI-Security-Use-Case
Asset-Valuation-and-Risk-Assesment-Report	"Asset Valuation and Risk Assessment Report", Apr. 12, 2010 http://groups.geni.net/geni/attachment/wiki/ComprehensiveSecurityPgm/Asset-Valuation-and-Risk
NIST SP 800-30	"Risk Management Guide for Information Technology Systems", Jul. 2002 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
CISSP	"CISSP All-in-One Exam Guide, Fifth Edition", Jan. 2010 http://www.logicalsecurity.com/

2. Threat Agent List

Below is a list of threats agents or adversaries considered, their capabilities and their potential motivations. Threats agents that seem unlikely to affect GENI at this time or in the foreseeable future have been grayed-out.

Old School Cracker

Motivation: The classic hacker/cracker is typically motivated by the challenge and bragging rights. They are mostly ego driven, and often do not consider themselves as unethical because their goals aren't theft or vandalism. However, they often cause harm if only collaterally through their mischief. A prime example of unintended consequences from an "old school" cracker is the Morris Worm that brought down the early Internet

Capabilities: The skill level of this type of attacker is quite varied. She could be a basic "script-kiddie" just getting started or a very skilled attacker with in-depth knowledge of network protocols, kernels and low-level programming. However, such attackers typically work alone or in small groups, thus limiting their effectiveness to some extent.

Hacktivist

Motivation: The hacktivist is an attacker motivated by ideology, usually political or religious. They want their attacks to be highly noticeable and typically perform defacements often with some sort of Denial-of-Service (DoS). One typically knows if they have been subject to such an attack, though not necessarily the extent of it. Sometimes there is intellectual property theft involved as well, but this is not likely in the case of GENI. In fact, GENI is not likely to be a very attractive target to this kind of adversary. Though it is "possible" that by virtue of being a high-profile federally funded project, it could be the target of general anti-American sentiment.

Capabilities: The skills of a hacktivist vary similar to an "old school" hacker. However, hacktivists are often parts of larger groups, potentially giving them more resources. Also, they engage in riskier behaviors since they usually reside in foreign countries.

Computer Criminal

Motivation: The cyber-crinimal is perhaps the most common threat on the Internet and is motivated almost exclusively by monetary gain. These attackers are typically collecting hosts for botnets that can be sold as a commodity on the Internet black market and used for spam, extortion, phishing, DoS attacks and hosting illicit materials.

Capabilities: This type of attacker usually seeks generic hosts that are treated as a commodity. They go after the low-hanging fruit, and thus are typically not the most sophisticated adversaries. While some more advanced cyber criminals may make targeted attacks to go after specific intellectual property, these types of attackers are unlikely to go after GENI which will have not have any commercial IP to steal.

Terrorist

Motivation: Like the hacktivist, terrorists are motivated by an ideology. However, they are looking to be much more disruptive or cause much more monetary damage. Simple defacements or attention grabbing is not enough. To be effective in the "cyber world", they would either have to destroy a costly piece of infrastructure, or affect the systems tied to some sort of critical infrastructure.

Capabilities: Terrorist organizations typically do not have grand hacking skills, but rather they physically destroy infrastructure. GENI is very decentralized and not as visible to the public as other cyber resources, and hence it would make a poor target. The terrorists who would have skills in hacking would most likely focus on espionage or bringing down critical infrastructure through cyber attack. Again, GENI does not lend itself to this kind of threat.

Industrial Espionage

Motivation: The motivation of this kind of attacker is to gather intellectual property as covertly as possible. GENI, being used for open scientific and engineering research is not likely to be a target of this sort of threat.

Capabilities: Such an adversary is usually very skilled, especially at being stealthy.

Nation State

Motivation: Nation states would typically be interested in espionage, denial of service in "cyber war" (particularly against critical infrastructure), and destruction of resources or infrastructure. By definition, this sort of adversary is always politically motivated. Fortunately, GENI has no classified information and is not critical national infrastructure. Therefore, it is not an attractive target for this kind of attacker.

Capabilities: The capabilities of a large nation state are almost limitless, constrained mostly by what they could accomplish unnoticed. It is unlikely that GENI, with its bottom up construction and decentralized control could ever operate in a way to protect against this sort of threat. It is incongruent with how it is managed and the purpose of open scientific research.

Insider

Motivation: An insider could technically be any stakeholder motivated by monetary gain, revenge or just curiosity. However, there is not really any intellectual property or opportunity for extortion within GENI. Hence, monetary gain is an unlikely motivation. The most likely stakeholder to be

an insider threat would a researcher or experimenter, possibly motivated to consume more than their share of resources or just trying to go beyond their authorization out of curiosity.

Capabilities: An insider is usually not a skilled hacker, but they posses special "inside" knowledge about how the system works making them potentially more of a threat. Further, an insider is already a valid user, and hence they do not need to brake any authentication system. This makes them more difficult to detect.

---

3. Threat List

Below, several types of threats are described, broken up into categories of *WiMAX specific*, *OpenFlow specific*, *GENI specific* and *Generic* threats.

3.a. WiMAX specific threats

The following are threats that would not be realized without the WiMAX deployments.

WiMAX licensing rules broken

The threat would be the use of bands by GENI infrastructure for which they are not licensed.

Vulnerabilities: Since the base station's only R6+ connection is to the controller, any misconfiguration (malicious or not) will be done through the Linux workstation controller. The vulnerability could either be procedural, in the case of an accidental misconfiguration by the aggregate owner, or there could be some remote vulnerability in the WiMAX kit. For example, the Linux host may not be well-hardened, kept up-to-date, or have a software vulnerability in the custom software stack (perhaps in OMF). It could also fall prey to weak authN/Z mechanisms or stolen credentials.

Threat agents: In the case of a misconfiguration, the threat is most likely an insider at the aggregate. A computer criminal just collecting hosts for a botnet could certainly compromise the Linux controller, but would likely affect the radio frequencies only by accident. The same is also most likely of any "old school" cracker, except that such a person may be more curious and hence slightly more likely to affect the base station radio.

Assets: The assets affected are the base station, Linux controller host, the frequency spectrum GENI owns or uses, any GENO-owned WiMAX handsets within range of the base station and GENI's reputation.

Potential Countermeasures: The most effective countermeasure for a misconfiguration is good documentation and checklists for those deploying the WiFi kits. These seem to be in place already. Additionally, it could be made standard practice to *regularly* audit or check the configuration, to make sure it is operating in the correct bands. **An alternative to a regular external audit is the use of a host-based file integrity checker like Tripwire**. This would best be configured by the creators of the WiMAX kit who would know all the relevant configuration files to monitor for change.

Protecting the Linux controller can be realized with good **hardening guidelines** that also specify authentication and authorization requirements for any system logins or administrative accounts. Preferably, access from GENI researchers through the OMF API would be on a separate interface than the SSH daemon which would be on an administrative interface. Policies and procedures for **maintaining the controller's security patches** are also important. Since these are all nearly identical as part of a "kit" with special software, it would be pragmatic to develop an update mechanism specific to these WiMAX kits, potentially run by the same project that develops the kits.

WiMAX interferes with other equipment

In this case, we are talking about a very similar threat to GENI operating within a band that it is not allowed to. However, in this case the aggregate owner may be doing everything correctly, but some other device has appeared within range, which GENI's equipment is not allowed to interfere with due to FCC regulations. In this case, as opposed to a misconfiguration, there is little that can be done to prevent such a problem besides some due diligence before determining where the base station will be placed. If such an incident occurs, someone on site will need to investigate and confirm. There is likely no suitable pre-determined formula for how to resolve such incidents, and they will need to be handled on a case-by-case basis, likely between the aggregate owner and complainant. If the GPO has paid for the WiMAX kit deployment, they too will have an interest in the resolution process.

If this is just a case of misconfiguration, malicious or accidental, then the discussion for the threat above applies equally well here. If it is actually a WiMAX handset, then chances are that it is not GENI infrastructure and owned by an opt-in user. In that case, GENI would have no role in the dispute.

Potential Countermeasures: Besides those for the threat above, there should be a **process in place to investigate such complaints** at each WiMAX deployment site. It is not immediately clear whether or not the policy must come from the GPO or if it can be different at each site.

WiMAX handsets interfere with experiments

The primary consideration here is that some third party WiMAX device, not part of a GENI experiment, is interfering with an experiment through the radio medium. This could be an opt-in user, too.

Vulnerabilities: The vulnerability is that the radio medium is subject to interference from anyone within proximity, and unless the experiment is using something akin to WPA2 for WiMAX, the experiment is subject to eaves-dropping and data pollution.

Threat Agents: The threat agent in this type of incident is someone local to the aggregate most likely (it is in principle possible to remotely hijack a WiMAX handset) because of the need to be within radio range. The threat agent may be malicious (e.g., Old School Cracker), or just accidentally causing interference.

Assets: The assets affected are this particular aggregate, the relevant experimenters' data, the radio spectrum or communication channels themselves, and any GENI handsets that are a part of this wireless testbed.

Countermeasures: Denial-of-Service through interference is not something that can be prevented, but it should be easy to detect with the proper measurement instrumentation. Data pollution and eaves-dropping can be prevented through **appropriate encryption techniques**. Ideally, such encryption solutions would be provided in a way that abstracts their setup and configuration away from the GENI experimenter.

WiMAX used by opt-in user for illegal activities

The threat here is that opt-in users, whom GENI may have little if any control over, would perform illegal actions while on the WiMAX testbed.

Vulnerabilities: The vulnerability being exploited here is that there is little to no vetting of opt-in users, and many illegal activities cannot be detected in an automated fashion. For example, users could be sharing copyright protected materials, downloading child pornography or using the WiMAX test bed as the first hop in an series of SSH sessions used to obfuscate the origins of an attack.

Note that a similar threat could occur from an active attacker, and not an official opt-in user. But this would be very similar to threats already discussed which would try to exploit weaknesses in the WiMAX kit, and hence its discussion here will not reveal new vulnerabilities or countermeasures.

Threat Agents: By definition, this person would be a cyber criminal. However, they may not be a professional criminal seeking money, but a fairly unskilled individual just using the WiMAX test bed as an ISP to obfuscate their identity. They could also be a more skilled "old school" cracker, as well.

Assets: The main asset affected is GENI's reputation. Any major incident of this type would not bring the kind of attention GENI wants.

Countermeasures: It is unclear that GENI has any more responsibility than that of the corner coffee shop in this case. Certainly, the aggregate provider's institution would be most culpable in this situation. The main thing is that GENI must have **procedures to follow in response to law enforcement requests**. This is a part of the Spiral 3 milestones. A **distributed IDS** run by GENI operations with sensors at the wireless testbeds could be used to detect some suspicious activities, like file-sharing protocols, and rouge ftp/http servers being connected to through WiMAX.

Opt-in user privacy compromised

Opt-in users are likely to have some expectations of privacy and would have growing levels of discomfort with their activities being shared with researchers of other experiments, other GENI personnel, or the outside world. It is assumed that they would at least expect their behaviors to be monitored by the creators of the particular experiment to which they are opting-in.

Vulnerabilities: While privacy could be exposed at any part of the GENI infrastructure hosting slivers for the experiment, we are focused on WiMAX at this point. The clearest privacy threat to opt-in users of a WiMAX experiment is that their behaviors could be monitored over the air by any party within radio range. We also put a lot of trust in the virtualization of the WiMAX kit to keep experiments from interfering and providing security/privacy guarantees between experiments. However, the virtualization boundary is rather soft in this case, utilizing Linux UML instead of a lower-level hypervisor like Xen or VMWare. It is thus conceivable that parties (e.g., experimenters) sharing a WiMAX base station could eaves drop at that layer even without radio proximity.

Threat Agent: Certainly curious crackers, cyber criminals monitoring WiMAX traffic for credentials and even other opt-in users could enter promiscuous mode and monitor unencrypted traffic or traffic that uses a shared key. This would be the easiest sort of attack as it is likely that many experiments will not use any sort of encryption. If we consider other GENI experimenters or opt-in users from other experiments as insiders, there is an insider threat that someone could break through the UML virtualization barriers and monitor other experiments.

Assets: The assets most directly affected are experimental data and GENI's reputation. Exposures like this could sour GENI's reputation and dissuade new users from opting-in to experiments.

Countermeasures: It would be ideal if those developing the WiMAX kit and working with OMF could make it simple for experimenters to enable **something like WPA2 but for WiMAX**, so that the details of this implementation could be abstracted away from the experiment setup. If it was as simple as another option in a config file to setup, that would encourage experimenters not to broadcast in the clear.

Moving away from UML to virtualization like **VMWare or Xen** would give stronger guarantees of non-intererance between experiments and make such assumptions more realistic. It does appear that the WiMAX kit developers are interested in going that route in the future.

DoS against WiMAX base station

The threat here is someone actually DoSing the radio spectrum. Of course, the base station kit itself could potentially fall prey to cyber attack and be brought offline, but that scenario has already been dealt with in previous threats (e.g. attacks against the Linux controller).

Vulnerabilities: The vulnerability being exploited here is the fact that the radio spectrum is a shared medium that is susceptible to interference from anyone within several miles of the WiMAX base station.

Threat Agents: The most likely threat is not from an active attacker, but interference being caused accidentally. This is especially likely in the unlicensed spectrums. A malicious adversary flooding the WiMAX radio spectrum would need equipment quite local to the region, though it could

in theory be activated remotely.

Assets: The assets are the particular aggregates within range of the interference, the radio spectrum the aggregate owner may have purchased, and the experimental data which could be polluted by such an attack.

Countermeasures: There is little prevention that can be done. A careful **planning of base station placement** could reduce the likelihood of accidental interference. Malicious interference is unlikely and difficult to prevent. However, aggregate owners can have **measurement equipment to detect** such an attack, and GENI could provide procedures for investigating such incidents.

3.b. OpenFlow specific threats

Threats unique to the OpenFlow deployments are described below.

Experiment rules affect production traffic

The purpose of OpenFlow is to allow research on real production networks without interfering with non-research traffic. It is key to have this assurance if we are to convince more universities and labs to deploy GENI OpenFlow devices.

Vulnerabilities: We discuss two ways this type of interference could happen. First, there could be an exploit discovered in the OpenFlow firmware. It is a fairly new protocol, and it hasn't seen the attention that more established protocols have received from the security community. If there is an exploit discovered in the future, it could easily be used to affect production traffic going through the same router or switch.

The second type of vulnerability could arise from how OpenFlow is used specifically within GENI. FlowVisor is not only providing all the security and isolation between experiments, but in some configurations FlowVisor is also being used as a mux between experimental and production OpenFlow controllers. In those setups it is responsible for protecting the production traffic from interference. Of course, if the OpenFlow routers and switches are only being used for research traffic, this is no longer a vulnerability for this specific threat of interference with production traffic.

Threat Agents: Certainly the "old school" cracker would be the most likely attacker here. A computer criminal couldn't make much money unless she were to extort it from the institution (a research university is not a good target though) or some how use the control of the OpenFlow routers to effect a better DoS elsewhere. In all likelihood, a computer criminal's involvement would be from gaining control of the OpenFlow controller and only accidentally affecting OpenFlow substrate. An insider is even less likely, as the aggregate owner does not want to negatively affect its own traffic, and there is little gained by another GENI experimenter from affecting production traffic. Lastly, there is the insider threat of misconfiguration which could allow such interference if the FlowVisor is not setup correctly.

Assets: The GENI relationship with the research institutions involved in the meta-ops rollout would be the most affected asset. If the GENI deployments expose aggregate providers to more risk, they are less likely to contribute aggregates to GENI, thus reducing the amount and diversity of resources available to experimenters. The other assets considered here are the aggregates themselves which would likely be pulled offline if production traffic was being adversely affected.

Countermeasures: In the first case, where the OpenFlow firmware is exploited, there is a little prevention that can be done. While time-consuming, it may be worthwhile to have an **external security audit of the firmware source**. Since, this firmware is very dynamic and bugs are constantly being fixed, it will be important for aggregate owners to deploy updates with security patches. GENI operations should **inform all aggregates when such updates come out** and perhaps even host some of the infrastructure to deliver those updates. Timely and well tested updates are an important defense along against threat vector.

The other major path to realize this threat is to exploit FlowVisor or the broader E-GENI host. Depending on the deployment configuration, compromise of the E-GENI aggregate manager may not allow one to do more than just affect multiple experiments. Regardless, any host running **FlowVisor should be hardened** much like the base station controller for the WiMAX deployments. The GPO should produce hardening guidelines to this effect. Strict configuration **guidelines and checklists may help reduce the chance of misconfigurations** that would allow this threat to be realized, but it would be much more difficult with the OpenFlow deployments which are much more heterogeneous than the WiMAX deployments. Lastly, because FlowVisor is responsible for enforcing much of the security policy to isolate experiments from each other and production traffic, it would be good to do an **external security review of the source code** and software architecture. Lastly, while the flowtables may be dynamic, the rules that separate production from experimental traffic should be rather static. If possible, **integrity checkers should be used** to alert admins of any changes to those rules.

One experiment affects another's flows within an OpenFlow device

This threat assumes there are two separate experiments running on the same aggregate. One experimenter is able to control or interfere with another's traffic by either editing their flowtable or creating rules that affect their traffic in their own flowtable.

Vulnerabilities: Technically, this threat is very similar to the one prior. For such an attack to be successful, one must affect the flow tables on the OpenFlow devices. This can be done by attacking the OpenFlow router itself, perhaps through an OpenFlow exploit (discussed above). It could happen by attacking the host OS running FlowVisor on the E-GENI device (also discussed above), or it could be accomplished from within an experiment by breaking the enforcement of policy by the FlowVisor which is acting as a sort of hyper-visor between the virtual controllers of the different experimenters. This last case is what we are mainly giving consideration here.

Threat Agents: This threat could be realized either through a misconfiguration of the FlowVisor or by an active attack from one experimenter. By definition, an experimenter is an insider to GENI. However, not all insiders are equal. An experimenter does not have the same privileges to FlowVisor and E-GENI that the aggregate owner running the E-GENI device would have. The aggregate owner is also a threat, as she could misconfigure the FlowVisor. However, it seems unlikely that the aggregate owner would purposely make two experiments interfere.

We should also note that an experimenter in this context could also be a cracker that has taken over a slice, but they are still an insider as they

have the additional advantages of a GENI experimenter at this point, and they would be almost indistinguishable from a valid user. However, their motivations for such an attack would likely be very different.

Assets: Clearly the affected aggregate and OpenFlow substrate are affected as well experimental data.

Countermeasures: Ignoring for the moment the more general issue of an adversary taking hostage a slice and the technical counter-measures to prevent that, any such attack from one experiment on another is likely to happen through a compromise of the FlowVisor. This could certainly be through an attack on the E-GENI host OS, and a countermeasure to that is hardening of that host as discussed earlier. However, it could happen by exploiting vulnerabilities in FlowVisor itself from within an experiment. FlowVisor is the service that is enforcing all the policies that restrict experimenters and isolate them. If one cannot change the policy by attacking the E-GENI host OS, there is always hope that they could break out of this virtualization. The main countermeasures to prevent that would be to add code to FlowVisor to help detect violations and to do a **professional software security audit** of FlowVisor itself. The simplest addition to the FlowVisor would be **detailed audit logs** to assist incident investigation. These logs would record what user/host initiated the creation of any rule. Further, knowing that these things are being audited acts as a deterrent to experimenters that might wish to adversely affect flowtables.

OpenFlow used to create a mixer or anonymizer network

The threat is that GENI could be used by a cyber criminal to create some sort of anonymizer network to hide their actions, like ToR.

Vulnerabilities: Any experimenter could already do this, so one path would be to consider ways that an attacker could hijack a slice or steal a GENI user's credentials. This is outside the scope of this report which is focused upon OpenFlow and WiMAX. Alternatively, an attacker could exploit vulnerabilities in the OpenFlow firmware or controllers to try and control the OpenFlow substrate. Such vulnerabilities have been discussed already.

Threat Agents: The most motivated attacker would be the cyber criminal in this case, but they already have ToR and their botnets which could be used to obfuscate the origins of attack. A curious cracker or GENI user (a type of insider) could do this as well, however, this is pretty risky for most GENI users if they are doing anything illegal or anything that affects experiments outside their slice. Making an anonymizer network within their slice could be perfectly acceptable research, though. In all, this seems an unlikely threat.

Assets: Clearly the specific aggregate and OpenFlow substrate are affected as well experimental data.

Countermeasures: Countermeasures to the types of vulnerabilities (e.g., firmware flaw of controller compromise) that could allow such a threat to be realized have already been discussed, and this threat would not expose any new types of vulnerabilities.

3.c. GENI-specific but not OpenFLow or WiMAX specific threats

The following are the threats that are unique to GENI, and not just any host on the Internet, but are not really tied to OpenFlow or WiMAX. Because our focus in this report is on OpenFlow and WiMAX, we only considered the threats in this category that could not be ignored during this first major infrastructure rollout.

Research traffic sets off IDS on campus network

Some GENI experiment falsely triggers a local IDS alert.

Vulnerability: The types of traffic that may be generated from an experiment are varied and unpredictable. This means it is quite plausible that anomaly-based IDSs could be triggered from time-to-time at the research institutions and universities hosting aggregates.

Threat Agents: Technically the GENI experimenter is the threat agent and hence it is an insider.

Assets: Besides relationships with campuses, which are needed for GENI to grow and expand, the specific experiments running on the aggregate setting off an alert could be affected. This is particularly true if the campus incident response teams start blocking traffic in response.

Countermeasures: This example brings home the point of good contact info with the aggregates. Not only should the GMOC have the info of the person running an aggregate,**but also of the security team** that would be alerted locally if there was a problem. Furthermore, the campus networking and security teams should be aware of GENI hosts and have contact info for the GMOC.

If campus IT departments knew about the GENI aggregates, they could put them on a separate virtual network and ignore their traffic. Or they could tune their IDSs to be less sensitive for those hosts.

Lastly, if GENI can create a**distributed IDS** across many of the larger aggregates, they could perhaps detect these problems before they occur and work with campus IT departments.

3.d. Generic Threats

Several threats are just the consequence being online or being a federated entity like the GENI community.

Incident investigation hampered by inability to coordinate

Almost any security related incident in GENI will involve multiple organizations and will require coordination among several parties. The GMOC or another entity will be taking a coordinating role, but relies on communication with the aggregate owners and other stakeholders. The threat is that

something or someone will prevent such coordination.

Vulnerabilities: There is potentially a very long list of things which *could* impede coordination, many of the problems social and not technical. However, in this early rollout, one vulnerability stands out as more likely than any other. Any coordination, which would happen through the GMOC at this time, requires up-to-date contact information with all the aggregate owners and affiliated research organizations. If that information is incomplete or out-dated, then future incident investigations can be affected.

Threat Agents: Any threat agent or attacker could take advantage of this vulnerability, though likely without knowing. A targeted attacker may seek ways to get the list of contact information and specifically attack places with incomplete records, but this seems unlikely.

Assets: Being such a generic threat, any asset could be affected.

Countermeasures: As part of the development of the Emergency Stop Mechanism, the GMOC has realized the importance of this kind of list and is creating it, though not without some difficulty. It is important this list be maintained, and the upcoming **aggregate provider agreement should stipulate that up-to-date contact information** for both campus security and the person managing the aggregate will be provided. It is important that these points of contact are full-time employees and not students which can be quite ephemeral. Another critical counter-measure is the creation of a GENI-wide incident response team. This team would serve as a single point of contact and a coordinator between aggregates.

Private email lists compromised or DOSed

At the moment, GENI operates no private email lists. However, if there will be a team providing operational security services, this will likely change. Furthermore, as the GMOC's role in operations expands, they will likely begin hosting some private lists.

Vulnerabilities: Email lists generally are not very secure and rest upon security through obscurity. Normal email is sent in the plain, and verification of group membership is usually as simple as checking "from" addresses. Also, the email list server itself is a single point of failure and can be DOSed. Though that type of attack much less common than snooping a private list as a DoS draws attention, and people usually fall back to other means of communication if the list is not too large, anyway.

Threat Agents: Any of the threats agents listed so far could use this tactic, especially to monitor incident response or perform reconnaissance. It does not take a very skilled adversary, especially to mount a DoS attack. People within GENI operations have little motive to perform such an attack as they will not get any new information, but a GENI user that is engaging in some malicious behavior that is being scrutinized by the security team would have motivation to read their emails.

Assets: The direct assets are the communication channels and list server platform itself. Indirectly, any asset could be affected because monitoring or disruption of such lists could allow the attacker some advantages.

Countermeasures: Protecting against a DoS attack on the list server can best be handled through redundant hardware or communication channels. However, not much should be invested in this if there are fallback channels of communication. Fallback methods will be likely as any private GENI email list is probably going to be small.

To protect the confidentiality of the list, one-to-many encryption techniques exist, but none appear ready for production use on a LISTSERV. As standard procedure, these lists should **not have their existence revealed or noted in any public forums**. Without using encryption and authentication technologies, the only protection is obscurity and a well-maintained list server.

Alternatively, GENI could prohibit the use of email lists for anything sensitive, using a hardened wiki server for communication and collaboration.

E-GENI, WiMAX base-station or other aggregate host OS compromised by non-targeted attack

Just by virtue of being online, these aggregates and aggregate managers are exposed to constant threats such as SSH brute force password guessing. This threat concerns that and dozens of common types of attack aimed at collecting hosts for a botnet and not targeted attacks.

Vulnerabilities: Perpetrators of these sorts of attacks rely on open services that are poorly configured, out-of-date or have weak authentication mechanisms.

Threat Agents: The main threat agent is the cyber criminal collecting bots. However, one cannot discount the "old school" type cracker that could, for example, be a student of the university where an aggregate resides.

Assets: The assets are the aggregates and aggregate managers themselves.

Countermeasures: The countermeasures to this type of threat are nothing beyond what has already been discussed to protect the WiMAX basestation or OpenFlow controllers. Consistent hardening guidelines for these resources, strong authentication for administrative interfaces, and regular updates (perhaps served by GENI infrastructure) would all be very useful. If GENI ever funds the development of a collaborative IDS between major aggregate providers, that would help detect these attacks more quickly, as well.

Credential harvesting of remote user

This threat could be realized in a couple of ways. First, a credential could be harvested elsewhere and used to get onto GENI. This is possible if GENI is federated with any other system or if that stolen credential (e.g., a university password) could be used to get a GENI credential. In addition to GENI user credentials, there will be local administrative accounts on the aggregate managers. These, too, could be stolen or reused.

Vulnerabilities: The vulnerability is that most common credentials can be stolen and reused by an attacker. Furthermore, attackers are often successful at utilizing user accounts to gain root access and setup new SSH daemons to harvest even more credentials.

Threat Agent: The grid community has seen significant attacks of this sort from the "old school" cracker type, seeking fame or notoriety. Rarely, it is an insider, one user trying to steal the credentials of another. The typical "bot-herder" goes after the low hanging-fruit and does not do the work to understand a host in relation to others at an organization and thus capitalize on credential re-use. However, this does not mean that more advanced cyber-criminals will not utilize this technique to help maintain a foothold in an organization.

Assets: Given the right credential, any asset could be affected. However, at this time we are focused on the WiMAX and OpenFlow deployments. The assets most affected in that regard are the aggregates and the GENI users' experimental data. Of course, the credentials themselves are an asset, too.

Countermeasures: In the case of local administrative accounts on the aggregates and aggregate managers, there are several things aggregate providers should do. **Basic hardening of servers**, as discussed previously, will remove unwanted services and default accounts that could be exploited towards this end. The aggregate owners should strongly consider **two-factor authentication** of any of these interfaces and definitely should **not reuse the same password or key** from another machine on these hosts.

When considering GENI user accounts, there are also many things that can be done. The best option is to **move away from more common authentication solutions like passwords and public key SSH authentication**. Most of the proposed GENI authentication solutions are certificate-based, and it is reassuring that NCSA has never seen stolen grid certificates used to access an HPC system. There is some security through obscurity by using gsissh. If possible, **GENI should try to handle the management of keys** and certificates for users to prevent them from storing unencrypted private keys.

User profiling can also be helpful in detecting compromised user accounts. Many users have a regular usage pattern coming from a particular type of machine, IP address block and time of day. NCSA has had success profiling SSH logins to capture this kind of threat. As GENI matures and usage patterns stabilize, this approach should be investigated.

No matter what authentication technology is used, if a user can leverage one account (like a university login ID) to get a token or credential that can access GENI, GENI operations must worry about this other credential outside their control being harvested. While there is little they can do to prevent such a threat, without giving up the benefits of out-sourcing authentication, they can still use mechanisms like the profiling discussed above to detect compromised user accounts. It will also be important to establish a good relationship with those institutions so that GENI would be informed of account compromises that could affect them.

Social Engineering

Social Engineering is a broad term that covers nearly all non-technical parts of an attack, parts which involve trickery. The "social engineer" is most akin to a con artist.

Being so broad, social engineering could be involved in almost any attack. For instance, it could be used to acquire a user's password. In this report we are most focused upon the WiMAX and OpenFlow deployments.

In particular, we are concerned with whether or not an aggregate owner knows they are talking with the GMOC.

Vulnerabilities: The main vulnerability is that the GMOC must maintain a relationship with dozens of institutions so that when an incident does occur, they can securely contact the appropriate people at those institutions. However, many of these people have never met, and would not recognize each other by voice on a phone call. Furthermore, there is no trusted email list service, or CA issuing S/MIME certificates to these parties.

Assets: The WiMAX and OpenFlow aggregates, their aggregate managers, the communication channels between the GMOC and aggregate providers and potentially the clearing houses are at risk (since impersonation could go both ways).

Countermeasures: As part of the plans for the emergency stop mechanism, the GMOC has considered this problem and how they will "prove" their identity to an aggregate provider should they need to call them. They will utilize a **callback number**, which is a good solution for proving the GMOC to the aggregate owner. The aggregate owner does not "prove" themselves to the GMOC, though. This is less of an issue as a fake aggregate owner could not get the the GMOC to do much except perhaps change entries about their resources in the clearing house.

For email communication, there does not seem to be a current solution. Since the number of major aggregate providers is still so small, PGP keys and email could be used. In fact, PGP key fingerprints could be part of the contact information collected, but it would have to be updated annually. Furthermore, not all aggregates would likely get on board.

If GENI later sets up a CA for certificates, it could also issue S/MIME certificates that the aggregate providers and GMOC would use to authenticate email. This scales better as GENI grows and supports more mail clients, though mobile phones and web-based email clients won't work.

Failure to follow security policies or procedures leads to compromise or reduced service

As security policies, procedures and guidelines are being developed, there is always the risk that parties are unaware of them or ignore them. This can lead to increased risk of incidents or increased cost of incidents. [This will always be the most likely and most common security breach....]

Vulnerability: GENI is very decentralized, and there is a vocal group of participants that are very against any top-down authority or rules. This means it is even more likely than in an enterprise-like organization that security policies will be ignored.

Threat Agents: The threat agents here are of course insiders, though this is not the typical insider threat of sabotage.

Assets: Technically, any asset could be affected. But most directly considered here are the aggregates as this report focuses mostly on the

WiMAX and OpenFlow deployments. In particular, the concern is that aggregate owners will ignore security policies.

Countermeasures: One vulnerability is ignorance of policy, and this can be addressed through **education and training**. In particular, such policies will be important to present to all involved stakeholders at the GECs.

Policies must also be created which balance usability and security. Making them overly onerous will increase the chances they are ignored. Therefore, it is important to get **input from all stakeholders and consensus at the GECs**.

Lastly, policies that have no authority backing them will be ignored. The aggregate provider and user agreements should **describe specific consequences** to breach of policies.

---

4. Threats & vulnerabilities not yet considered

As this is an early analysis, focused mostly on the meso-scale deployments of WiMAX and OpenFlow, there are several threats and vulnerabilities that have not been evaluated at this time but we would like to make note of for the future when this document is expanded in scope. These additional threats are listed below.

- GENI web site or wiki DoSed or defaced
- GENI certificate authority, or that of one of the aggregate providers, is compromised
- Experiment is out of control and must be halted (being addressed by GMOC)
- Several kinds of insider threats should be defined and evaluated
- DoS against documentation resources
- Experiment templates DoSed or experiment data corrupted
- Software update servers DOSed or lose integrity
- Private or proprietary data exposed (may not be an issue with any GENI experiments)
- GENI used as a DoS agent like a botnet
- Log hosts DOSed or compromised and lose integrity
- Backups DOSed or lose integrity
- Web portals compromised and prevent experiment management
- Collaboration tools DoSed
- IDS compromised (if there is one)
- Measurement framework exploited (more vulnerability than a threat)
- Control framework exploited (more vulnerability than a threat)
- AuthN/Z framework exploited (more vulnerability than a threat)
- Optin user software installed on desktops is vulnerable and leads to compromises