Requirements Document for GENI Wireless Security

GDD-06-16

GENI: Global Environment for Network Innovations

September 15, 2006

Status: Draft (Version 1.0)

Note to the reader: this document is a work in progress and continues to evolve rapidly. Certain aspects of the GENI architecture are not yet addressed at all, and, for those aspects that are addressed here, a number of unresolved issues are identified in the text. Further, due to the active development and editing process, some portions of the document may be logically inconsistent with others.

This document is prepared by the Wireless Working Group.

Editors:

Wade Trappe, *Rutgers University*

Wenyuan Xu, *Rutgers University*

We'd also like to acknowledge comments and suggestions from Tom Anderson of GENI Planning Group.

1. Introduction

GENI will provide a global platform for the development of the next generation of networking protocols, and networked applications. Due to its inherently large-scale, its planned resource abundance, and its high-profile, GENI will likely face risks that are greater than the generic corporate network. Further complicating the protection of GENI is the fact that there will be many types of machines spread across hundreds of geographically diverse locations. GENI equipment will be comprised of state-of-the-art equipment with a very high degree of mutability and programmability—making such resources an even more desirable target for attacks, misuse and abuse.

Although there will be many points of entry into GENI, perhaps some of the most susceptible are those that constitute the wireless components of GENI. The wireless subnets that will constitute GENI represent a broad spectrum of wireless platforms, ranging from the most meager sensor networking device to highly versatile cognitive radio devices. Although securing other components of GENI will itself be difficult, ensuring the trustworthy operation of the wireless platforms will be more even more challenging. One of the most basic reasons for this is the fact that wireless devices operate in an easily accessible broadcast medium—it will be a simple matter for adversarial entities to eavesdrop on GENI communications (e.g. transmissions associated with a particular experiment, or even control information being sent to administer such experiments) and even inject messages into the medium to interfere with GENI operations (e.g. an adversary may transmit forged packets to disrupt GENI control and management, or transmissions may simply jam GENI wireless subnets to prevent correct execution of wireless experiments). Further complicating matters is the fact that wireless devices are more easily accessible than many other network components: wireless devices are commodity items that can be easily purchased, providing adversaries an easily acquired attack platform; and wireless devices are generally portable devices that can be easily pilfered, making issues associated with physically protecting GENI wireless devices from theft even more pronounced.

Protecting the wireless components of GENI will require many of the same mechanisms that are being recommended for protecting the broader GENI facility [1], but will also require additional security mechanisms. In this document, we will outline the current plan for the wireless portion of the GENI facility, provide a threat analysis that will cover additional threats facing the broader GENI facility as well as a more detailed focus on GENI's wireless components, discuss a collection of defense strategies for protecting GENI's wireless subnets, and present a list of recommendations that should be considered during the design and construction of GENI's wireless components. In order to support our discussion, we will examine the cognitive radio testbed as a case study, and point to security challenges arising in preventing abuse of this highly-programmable platform.

2. Threat Analysis: Revisiting the Broader GENI Threats

Prior to commencing with full-scale construction of GENI, it will be necessary to involve security analysts in the planning of the GENI facility. An essential input into integrating security into the design is a thorough analysis of threats and risks that will be faced by the facility. Although threat analyses, such as the one provided in this document, in the GENI Facility Security document [1], and in GDD-06-10 [2], are essential as initial input to GENI planning, in actuality such threat analyses will have to be continually conducted throughout the implementation of the system—before new components are added to GENI, it will be necessary to evaluate whether these new components would constitute new point of weakness.

Using the current GENI draft documents, and discussions with WWG members, we have cataloged a variety of threats that we believe will be faced by different components of GENI, including GENI's wireless components. In this section we shall revisit the threats that will be faced by the broader GENI facility, and in the subsequent section we shall focus on threats that will be faced by GENI's wireless subfacilities.

2.1. Characterization of System Threats

GENI will be a large-scale, distributed system with components that are administered by different organizations, while under the supervision of a single GENI management team. In general, when considering the security and protection of a large-scale computer system or network, it is useful to identify the potential attackers, the threats that they might present, and the risks associated with these threats. We now briefly survey these different factors for general systems in order to provide a frame of reference for the rest of the document.

Attackers can generally be categorized according to their motivation and methods employed when conducting an attack. There will be many points of entry for launching an attack, and these points of entry might be susceptible to a variety of different vulnerabilities. Further, these vulnerabilities can allow the adversary to inflict different types of damage upon the system, its resources, or its users. The motivations for conducting attacks on a system can range from recreational to financial to ideological. Examples of types of attackers include external attackers who naively try to guess user accounts and passwords; or external attackers who use more sophisticated attack strategies; or internal users who seek to abuse their access rights; or internal users who seek to elevate their privileges (e.g. through the installation of keyboard loggers).

Threats may be considered to be the collection of tools that an adversary uses to achieve their nefarious plans. There are many threats that attackers may pose for computer and communication systems. Typical examples of threats on networks include: eavesdropping; masquerade/impersonation attacks; the replay, modification, destruction of information; injection of traffic or interference into the system; and the denial of services tendered.

These threats may be used individually or together to cause damage to the system. Such damage represents a risk for the system. For example, an attacker that can successfully masquerade as legitimate user could use such an attack to acquire personal information about that user. Some risks that are generally faced by systems include risks to the system's availability (i.e. denial of service); the loss of system confidentiality (e.g. theft of user information); and the unauthorized use of system resources or services.

2.2. Revisiting Broader GENI Threats

We begin by returning to the broader GENI facility and providing additional discussion regarding a variety of attacks that may be launched against the broader GENI facility.

Cross-slice Resource Consumption Attacks: At the heart of the GENI architecture is the notion of devoting different portions of GENI's resources (called slices) to different experimenters. Supporting this is platform virtualization, whereby each GENI node has virtually partitioned its resources and allocated these resources to processes/experiments operating on that node. Although virtualization allows for more effective usage of GENI's collective resources, without complete/perfect virtualization (a very challenging and daunting research task), slicing may be exploited to launch attacks on GENI experiments. The basic attack would unfold as follows. An adversary obtains a slice consisting of resources on a GENI node. The adversary can then proceed to direct an attack at the node's resources that aren't partitioned. For example, the adversary might write to the hard drive, filling the hard drive and preventing other experiments from using the hard drive's storage for virtual memory or data recording. Or, as another variation, the attacker might launch a recursive shell script, consuming all available OS processes and preventing other experimenters from running their experiments. Of course, the likelihood of such attacks can be mitigated by carefully configuring the device (e.g. by partitioning the hard drive into blocks for each experiment, or by ensuring that simple attacks like recursive shell scripts are monitored for). Nonetheless, perfectly configuring each device requires careful planning and insight into likely exploitation scenarios.

Experimenter Privacy Breaches: GENI will be a common, shared resource for the networking and computing community. The management and experimental support infrastructure represents a source of information that can be monitored and exploited by adversaries. For example, an adversary may monitor GENI management and control information to learn about which users are requesting which resources. Further, it may be possible for clients to monitor each other's usage. For example, since GENI will be used by academic and industrial researchers, it is easy to envision cases where users use GENI resources to monitor experiments being conducted by other rival organizations. Although it will be impossible to completely prevent users from learning about each other's experiments, some level of precaution and *experimenter separation* is warranted. This privacy issue must be carefully considered and weighed against the innate need of the GENI facility to represent a collaborative facility that furthers the advancement of the community's science and engineering knowledge. In particular, it may be more desirable to allow for experimental visibility in order to support more collaboration between researchers and developers, as well as allow for a distributed means to monitor GENI's operations.

Theft of GENI Operational and Management Information: GENI's control and management information must be carefully protected so as to prevent information associated with GENI's operation, management, and state from extending beyond those entities that explicitly require that information. For example, adversaries can monitor GENI management messages to infer information regarding the status of GENI's equipment (e.g. resource outage reports). Further, management logs and security audit data must be protected from intruders, who might use such information to discover weaknesses in GENI's infrastructure. It will be necessary to identify

different classes of information, and associate appropriate levels of protection with each of these data types.

General Family of Operational Denial of Service: There is a broad array of denial of service attacks that could be launched against the general GENI infrastructure. At the most basic level, users may submit bogus resource requests in order to prevent GENI from responding to legitimate resource requests. Limitations on the amount of resources that can be requested, and resource scheduling fairness methods (e.g. randomized resource allocations) might be used to alleviate such threats. As another example of a denial of service attack, adversaries may attempt to block or disrupt management messages, thereby causing GENI to incorrectly allocate resources (for example, not allocating enough resources to correct problems, such as facility outages).

3. Threat Analysis: Wireless GENI

Much like the rest of GENI, the threats that GENI's wireless components will face can be broadly categorized as arising from external threats, and internal threats. We have thus broken down our discussion along these lines. However, before we examine the threats, we shall briefly touch upon the current plans for GENI's wireless subfacilities.

3.1. Overview of GENI's Wireless Components

The GENI Wireless Working Group is pursuing the development of five distinct styles of subfacilities as part of the GENI initiative [3][4]. These five facilities include: a collection of wireless emulation testbeds, similar in spirit to the current Emulab [5], ORBIT [6] and Kansei testbeds[7]; an urban mesh/ad hoc network testbed that will be deployed in a major metropolitan area; a wide-area suburban network that will broad-coverage technologies, such as WiMax or cellular; a variety of indoor and outdoor sensor network testbeds, which will be further extensible through clearly defined sensor kit specifications; and cognitive radio testbeds that will include wireless devices with highly programmable lower-layer interfaces.

In order to secure the wireless components of GENI, a first step is to identify the assets that constitute the wireless subnets. This information can serve to assist in conducting risk analysis, security planning and asset prioritization. The wireless subfacilities will be populated by a variety of different hardware devices and software components [3]. We now enumerate several of these components.

	Emulator Testbeds	Urban Mesh/Ad hoc Testbed	Wide-Area Wireless Testbed	Sensor Network Testbeds	Cognitive Radio Testbeds
Experimental Hardware					
Static Computing Device	Yes	Yes	Yes	Yes	Possible

COTS Radio Node	Yes	Yes	Yes	Yes	No
Fully Programmable Radio Node	Possible	Possible	Possible	No	Yes
Mobility-enhanced devices	No	Desirable	Desirable	Possible	Possible
Environmental Sensor	Possible	No	No	Yes	Possible
Dual Interface Network Nodes	Yes	Yes	Yes	Yes	Yes
Software Components					
FDMA Virtualization/Slicing	Yes	Yes	No	No	Yes
TDMA Virtualization/Slicing	Yes	Yes	Yes	No	Yes
SDMA Virtualization/Slicing	Yes	Yes	Yes	Yes	Yes
Secure Log in (authentication mechanism)	Yes	Yes	Yes	Yes	Yes
Control command signaling mechanism (such as reboot)	Yes	Yes	Yes	Yes	Yes
Audit/Monitoring software	Yes	Yes	Yes	Yes	Yes
Admission Control software	Yes	Yes	Yes	Yes	Yes
Experiment measurement framework (collecting relevant performance statistics)	Yes	Yes	Yes	Yes	Yes

3.2. Wireless Threats: External

There are many threats that will face GENI that are particular to the wireless components. One class of these threats is those that originate from adversaries that are external to GENI's infrastructure. Such external threats are generally characterized by an enemy seeking to exploit the broadcast nature of the wireless medium, or attempting to physically vandalize/destroy/obstruct the correct operation GENI's wireless edge sites. We now enumerate a list of such threats.

Eavesdropping: Although eavesdropping is a general threat that can be applied to wired systems, this threat is more pronounced for wireless systems as the medium can be easily and invisibly monitored. Conventional wired systems can be monitored for eavesdropping or wiretapping by monitoring impedance mismatch. However, such mechanisms are not available for radio systems. Adversaries may simply place a wireless device in a monitor mode, record traffic, and use this data to infer valuable information that might facilitate other attacks.

Traffic Injection: Another attack that applies to general networked systems but represents an enhanced source of security risks is traffic injection. The broadcast nature of the medium, plus the availability of easily programmable wireless platforms means that external adversaries can attempt to inject false GENI traffic in order to cause a disruption of GENI's services. The risks that traffic injection presents are many. One consequence can be the false measurement of experimental data, which might arise due to additional (non-experimental control) traffic on a slice causing protocols to respond differently than expected. As the primary purpose of GENI is to support scientific research, the threat to the validity of the experiment is more than a mere nuisance, but instead could undermine the important scientific objectives that GENI is meant to support. Further, traffic injection can be used to spoof or alter GENI control and management messages.

RF Interference: Whether intentional or not, interference/jamming from external factors will be a serious threat to the availability of GENI's wireless services. Traditional approaches to coping with radio interference (e.g. spread spectrum) will have limited utility in the context of the GENI facility. In particular, it is likely that the platforms that will be used for GENI's wireless testbeds will be chosen from commercial wireless platforms, such as 802.11 or Zigbee, which utilize carrier-sensing for medium access. Consequently, these systems will be extremely susceptible to radio interference attacks whereby an adversary can prevent the transmission or reception of legitimate experimental traffic [8]. An adversary may raise local RF energy to cause the energy-thresholding mechanisms to declare the channel is always occupied, or may prevent the reception of packets by monitoring the medium and emitting short blocker packets to cause CRC checking to fail [9]. Further, it should be realized that beyond the problems of adversarial interference, unintentional interference might arise in cases where GENI testbeds are located in highly trafficked areas (the usual near-far problem of communications).

Physical Threats: One of the most basic security threats to the wireless GENI will be the risk of physical damage to GENI nodes. Unlike the core of GENI, most of the wireless subnets will be located outdoors in communal areas and hence subject to the risk of being damaged, vandalized, tampered with, etc.

3.3. Wireless Threats: Internal

Beyond the threats that GENI's wireless components will face from external sources, there are many additional threats that will be possible when adversaries manage to become (apparently) legitimate GENI users/devices, and use these privileges to cause havoc on the rest of GENI's wireless components.

Ephemeral Rogue Networks: The GENI facility will be a highly-resourced network with interfaces to the broader Internet. These resources should be used for legitimate experimental purposes, rather than for unintended, rogue purposes. A prime example of how GENI could be misused arises if we consider one of the municipal wireless mesh networks that are planned as a GENI wireless testbed, and attempt to turn a portion of that mesh network into a temporary non-experimental access network. An adversary that gains access privileges to a slice of the mesh network may use a subset of nodes to provide service to non-experimental processes. For example, by requesting a spatial slice for a few hours in order to conduct a supposed experiment, the adversary may instead use GENI's resources to host a LAN party, or even provide business services (e.g. cheap internet access, which could harm the business of wireless service providers).

Greedy user/experimenter: Most lower-layer wireless network protocols, such as the 802.11 MAC, handle multiple users sharing the wireless medium through carrier sensing and collision avoidance mechanisms. For wireless testbed scenarios consisting of multiple users running in overlapping (or even adjacent) spatial regions, users will contend for the wireless medium. The consequences of the open and shared nature of the wireless medium will become even more pronounced as GENI opens up lower layer interfaces for experimentation. If GENI provides experimenters the means to tune lower layer parameters, then users might seek to greedily exploit this to their advantage, while at the disadvantage of other users. As a simple example, users might seek to decrease the back-off window size in 802.11, and as a result obtain a larger fraction of the channel utilization [10][11].

Unintentional User Misuse/Interference: As the GENI testbed is intended to support experimentation, it should be realized that the researcher might not necessarily consider all of the consequences of his/her experiment. Often, by focusing on one aspect of a research problem, they might ignore the side-effects. For example, wireless security experiments that involve the study of wireless worms and their propagation might be able to cross-infect other experiments or other GENI nodes.

Administrator Misconfiguration: GENI testbed will be comprised of heterogeneous networks that could belong to multiple management groups. As a result, there may be different security policies need to be manually configured to reflect the best interests of different entities. A misconfiguration can cause partial network failure. For example, a misconfigured wireless network access point can refuse packets coming from a legal wireless device, causing unintentional denial of service.

Rogue Component Threats: (e.g. Rogue Access Points Operated by Attackers) Wireless networks are susceptible to attacks where adversaries introduce rogue components that appear as if they are legitimate components. As an example, it is well known that WLANs are prone to rogue AP attacks—attackers can install access points with the same ESSID as the authorized AP. Clients receiving stronger signal from the attacker operated AP would then attract legitimate

clients to associate with it. Traffic and commands issued through this rogue AP would be susceptible to a variety of attacks, the least of which is denial of service. In the context of the wireless portion of GENI, it may be possible for adversaries to imitate legitimate GENI wireless nodes, for example by using a wireless-enabled laptop and freely-available attack tools to disrupt wireless service. Generally, it should not be possible for adversaries to imitate or introduce components that appear as if they are legitimate GENI devices, in whatever appropriate context that might imply.

4. Solutions and Defense Mechanisms

There are several approaches that can be taken to defend GENI. In our analysis, we have considered the following protection mechanisms that GENI systems can utilize:

- *Prevention/Impairment:* Mechanisms that stop or lessen the likelihood of an attack
- *Detection:* Methods for detecting an attack or anomalous activity
- *Forensics and Characterization:* Methods to pinpoint the attack and characterize the attack
- *Repair and Immunization:* Methods that allow the system to recover, and protect the system against future attack instances.

We shall now present various defense strategies that might be employed to protect GENI and its wireless components. It should be emphasized that these mechanisms will work in concert with each other. For example, diversion techniques are often used to help characterize attacks, while detection is necessary prior to any response or repair taking place.

4.1. Defense: Prevention/Impairment

By far the largest category of defense mechanisms for GENI and its wireless systems should be prevention. Prevention mechanisms ensure that the facility never succumbs to an attack, or at the least make an attack less likely to occur.

Security Policies: At some point, it will be necessary for the management of GENI to specify what is allowed and not allowed. This is a rather serious undertaking. At the first level, it is a specification of access control policies: which user/process is allowed to access which resource. But, it is also a specification of what forms of external events might be considered benign and what events might be considered a threat. It should be noted that there might be other policies/restrictions that come down to GENI from external organizations (e.g. FCC spectrum rules).

Social Engineering: One low-tech approach for lessening the likelihood of an attack against GENI is to make the GENI network less attractive for attack through social engineering, e.g. by advertising or not advertising. Further, for outdoor deployments, it may be generally wise to follow the practice of the telephone and cable industries by encasing deployed equipment in dull, unimpressive containers (e.g. a gray utility box).

Tamperproof Hardware: In order to make it difficult for adversaries to capture GENI nodes and turn them into attack platforms, it is necessary to have some level of tamperproof components. Further, tamperproof hardware will help protect the storage of cryptographic material, such as keys used in encryption and authentication [12].

Authentication: All wireless GENI nodes will need to have authentication mechanisms built-in in order to prevent network intrusions. One question here will be whether this will affect wireless security experiments, and how much GENI security mechanisms should be accessible to the user. Generally, this suggests that it will be necessary to separate a baseline set of GENI facility security mechanisms from the mechanisms utilized/accessible by experimenters. A subsequent question, then, is how much performance overhead is consumed by requiring authentication. Related to this is the idea that there should be some non-mutable way for the policing infrastructure to identify GENI wireless nodes, perhaps to distinguish them from generically available commercial platforms. As part of the access control mechanisms, the GENI Facility Security document [1] proposes the provisioning and operation of a distributed Public Key Infrastructure (PKI) and Certificate Authority to allow strong identities for facility users. In the context of the wireless GENI, it may be possible to use a similar approach. However, it should be emphasized that this would have a correspondingly higher cost for wireless nodes due to their potential resource constraints.

Confidentiality: All traffic streams (including control and experimental packets) should be encrypted to the maximum degree possible. Ideally, all traffic leaving a GENI node should be encrypted to prevent eavesdropping and possible privacy breaches. As in the case of authentication, an important issue that comes up is how much performance overhead is consumed by requiring encipherment, and whether this would have impact on experiments.

Trusted Operating Systems: The operating system issues needed to ensure trustworthiness on an experimental wireless node are fairly complex. In the realm of "slicing" we need to guarantee that one slice does not (and cannot) access another slice's resources. Further, as many experiments will involve modifying the kernel, we need to make certain that what is done to a node's OS is benign (e.g. no rootkits installed). In many cases, it may be desirable to deploy wireless components that employ a trusted computing base with tamper-resistant memory [12].

Frequent Re-Imaging: In order to prevent nodes from becoming too unhealthy (e.g. infected by malware), one simple approach to handling this is to require that GENI nodes undergo frequent re-imaging. In particular, for outdoor scenarios, where nodes do not constitute a regularly-refreshed testbed, as is the case of the emulator testbeds, it will be necessary to stagger the scheduling of equipment maintenance and re-imaging.

Design consideration: It is desirable to take security into consideration during the initial system design and deployment. Different designs that can achieve the same (non-security) system goal with comparable performance should then be selected based upon their security capabilities. In general, security, performance and overhead should be jointly considered during design. For example, in the GENI-WWG Management and Control document [3], there are two ways to address the issue of overbooking network resources: one way is to blindly accept all requests and let the network attempt to filter and provide a best-effort service to all; or, the other approach is for the management and control software to maintain the state of network and admit according to that state requests for resources. Although the latter approach has larger management overhead, it may be able to better defend against DoS attacks if appropriately employed.

Diversion Techniques: Diversion is a less popular defense strategy, but could possibly be a useful strategy for assessing the security of GENI's systems. The general motivation behind

diversion is to make another device or component more desirable to attack than other, higher-value components. This has two primary effects: first, attackers might not end up attacking the important GENI components; and, second, it provides a means to gather information about attacks (discussed later), i.e. it helps drive characterization. Such diversion strategies are often referred to as honeypots.

4.2. Defense: Detection

Another essential step to protecting GENI will be the detection of attacks, which can in turn be used to initiate response mechanisms. It should be noted that both forms of detection can take advantage of the GENI monitoring services that are being proposed as part of the GENI Management and Control. In particular, monitoring an experiment, and monitoring the security/health of the facility are intimately connected, especially in the case of wireless subnets.

Non-experimental Wireless Monitoring Infrastructure: In order to facilitate intrusion detection, as well as identifying when wireless nodes have been compromised, it will be desirable to have an infrastructure that is not part of the experimental facility that monitors the health of the facility. Although such a mechanism will be useful for the rest of the GENI facility, it will be particularly useful for the wireless portion of GENI as the wireless medium allows for more general forms of attack that can originate from almost anywhere. As an example described earlier, RF interference can be a serious threat for the wireless GENI, and having an external infrastructure detect the presence of interference would lead to more robust system adaptation. Further, since the wireless medium is a shared medium, a monitoring infrastructure would facilitate non-fair usage of the medium (e.g. as might occur when greedy experimenters violate proper etiquette).

Experimental Wireless Local Assessment: Wireless GENI nodes may employ a collection of intrusion detection and attack detection mechanisms in order to detect the local occurrence of attacks. Nodes, at the least, should be installed with a collection of common attack signatures, and the detection should initiate appropriate response mechanisms.

4.3. Defense: Forensics and Characterization

Forensics involves the localization of threats, while characterization represents learning about threats that have successfully penetrated other defense mechanisms.

Emitter Localization: As part of the monitoring infrastructure, it would be beneficial to employ techniques (e.g. localizations software, or sophisticated hardware) that can localize a wireless emitter that is responsible for an attack. It should be possible to reuse the wireless monitoring components that are being recommended in the GENI-WWG Management and Control document [3].

GENI Wireless Honeynets: One possible technique that GENI operations members should consider is the merit of deploying fake wireless networks, along with data collection mechanisms to facilitate attack characterization. Data collected from honeypots can be used to describe (either statistically or through specific signatures) a variety of attacks that can be integrated into intrusion detection mechanisms. Although honeypots represent an important data-collection technique, their utility in the greater GENI scheme should be carefully considered as they are a separate facility that requires active management and monitoring.

Wireless GENI Security Audit Framework: The GENI Facility Security document identifies the need for auditing mechanisms in the general GENI facility, and this requirement will extend down to the wireless subnets. As the wireless components represent a heterogeneous collection of devices with varying roles and purposes, it will be necessary to define a common framework for generating service reports, and sufficient storage on each wireless device must be reserved for the delivery of audit logs—especially as wireless nodes might experience periods of disconnection from the main components of GENI. It is only when sufficient data is collected and successfully delivered that security analysis can identify violations and lead to changes in existing security policies.

4.4. Defense: Repair and Immunization

Repair and immunization represents the feedback in the security cycle, and involves closing the loop in the GENI facility design.

Response Policies: Complementing security access control policies should be the specification of policies governing response and countermeasures.

MAC Address Filtering: When packets or traffic flows are falsely injected into the wireless medium, and this anomalous behavior has been detected by the monitoring mechanisms, a first response is to employ light-weight MAC-layer filtering of such traffic. In such a defense mechanism, the MAC address of packets arriving at a GENI node is checked against a list of approved (or, contrarily, against a blacklist) and correspondingly allowed or denied to enter the GENI network. MAC address filtering is a very light-weight defense mechanism as, for wireless NICs, MAC addresses can be changed. However, such a mechanism also places minimal burden on GENI nodes, which may be desirable from a performance perspective.

Fully-authenticated Communications: A more powerful response to anomalous traffic is to initiate full-scale authenticated filtering of traffic entering wireless GENI nodes. This mechanism will necessitate key management, and further will require that GENI nodes perform additional cryptographic computations at lower layers. The effect that this additional computational and communication cost might have on wireless experiments should be carefully weighed when securing the wireless experimental infrastructure.

Human Response: The detection and localization of an intruder, or a rogue wireless transmitter should initiate warning messages to the GENI security administration. In cases where the intruder appears persistent and is localizable, it might be necessary to administer the physical capture of the wireless intruder, or initiate patrolling of the wireless environment. More generally, warning messages should prompt security administrators to more carefully monitor GENI, and manually alter security policies as needed.

Authenticated Deactivation: Malfunctioning or misbehaving GENI nodes may be equipped with an authenticated control channel by which nodes may be deactivated, or reclaimed by GENI management.

5. Case Study: Cognitive Radio Testbeds

In this section, we examine the cognitive radio (CR) testbeds as a case study to support the above discussion for securing wireless GENI. The fact that cognitive radios represent a highly-programmable platform (and hence perhaps the most dangerous of all of GENI's devices), suggests that using the cognitive radio testbed as a case study will provide insight that will be most general and applicable to GENI's other wireless testbeds.

The cognitive radio wireless network is intended as an advanced technology demonstrator. The cognitive radios themselves will be able to scan the available spectrum, select from a wide range of operating frequencies, adjust modulation waveforms, and perform adaptive resource allocation– all of these in real time. It is easily conceivable that the public-accessible cognitive radio testbeds could become an ideal platform for abuse since the lowest layers of the wireless protocol stack are accessible to programmers. It is therefore essential that GENI have methods to ensure that the cognitive radio device and the implementations of their lower layer protocols are trustworthy, and that all cognitive radios (and their users) are held accountable for not following spectrum access policies defined by GENI administration and management. In order to manage the rules that cognitive radios should follow, it will be necessary to have an entity within the GENI organization act as the "Spectrum Law Maker," who must follow regulations, e.g. as specified FCC. In particular, the GENI facility must ensure that the usage of its equipment is compliant with local and federal regulations.

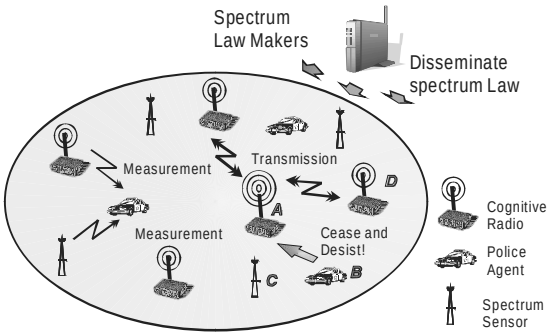

Figure 1: GENI spectrum access enforcement architecture

In order to enforce spectrum access control policies, the GENI cognitive radios should be deployed with a secure on-board trusted computing base (TCB). The operating systems that operate on these cognitive radios should be able to ensure trustworthy radio operation by restricting any attempt to change the CR configuration that is in violation of GENI-issued spectrum laws. As an example of how this process might work, consider a situation in which an experimenter (or his/her protocol) seeks to adjust the operation of a CR to transmit information over a non-licensed spectrum band (or, more generally to transmit with too much power). To block this adjustment, we would require that the user/process must send a spectrum access request, which includes information about the target radio frequency band, the transmission power, transmission duration, etc. to the TCB of GENI CR node. The TCB in turn would validate the request against the spectrum access policies available to it (which should be stored in secure memory on the CR), and would allow the request to go through only if it does not violate any of those laws.

On-board TCB law enforcement can, in general, secure the spectrum access. However, at some point GENI must confront the possibility of truly greedy or even malicious users/processes that circumvent the on-board safeguards. In order to cope with these more serious threats, the GENI CR testbed should enforce spectrum policies through means external to the cognitive radio itself. One means to accomplish this is to deploy a monitoring network, aka. "spectrum police", which

monitor the local radio environment by collecting geographically distributed radio measurements from the population of cognitive radios as well as auxiliary spectrum sensors, as shown in Figure 1. Of course, since we are operating in an adversarial setting, some measurements could be supplied by potentially corrupted CR devices. It is therefore necessary that the GENI CR testbed should filter out inaccurate data, reliably assess an interference environment, and detect violations by comparing with "spectrum laws" (e.g. issued by FCC). Once a violation is detected, corresponding local punishments, which must be specified by GENI security management policies, would be enacted. To enforce proper spectrum law, GENI could shutdown offending CRs via an authenticated kill-switch located on each cognitive radio. In some extreme cases, where the kill-switch located on the cognitive radio is disabled by a malicious user, GENI should be able to conduct a further level of enforcement by utilizing RF-localization techniques and seizing rogue transmitters.

6. Recommendations and Requirements

It is commonly accepted that in order to secure corporate enterprises it is necessary to integrate security into the design and management of the enterprise from the beginning. This process begins by conducting a thorough risk analysis across the components of the system. Additionally, it requires carefully defining policies as to the usage/operation of system components, the rules by which facility employees should follow, and the consequences for employees/users for not following guidelines. Further, it is necessary for the management to outline roadmaps for evolving the system's security mechanisms as new threats are identified, or systems are changed/upgraded are necessary.

As a starting point, the GENI security management team needs to construct an enumeration of GENI assets, classify their importance and identify costs associated with their repair. Related to this is the need to conduct a risk analysis where the threats are categorized, and their risks, likelihood and defense/prevention costs are used to arrive at a prioritization. As an example of such a risk analysis, we present a preliminary tabulation of several threats that have been discussed earlier in this paper.

Threats	**Risk**	**Likelihood**	**Defense Mechanism**	**Cost to Defend**	**Priority**
Cross-slice Resource Consumption Attacks	It could harm the availability of GENI testbed to other legitimate experimenters.	Depends on the payoff of the attacks	Virtual partition enforcement mechanism	Build on top of virtualization mechanism.	High
Experiment Privacy Breaches	Breach experimenter's privacy	High if the information is easy to get	Experimenter separation mechanism	Complete prevention can be costly	High
Theft of GENI Operational and Management Information	Leakage of valuable GENI information to the advantage of adversaries	Possible, as GENI could be the symbol of the US	Comprehensive mechanisms, such as authentication, encryption	Medium	Medium
Operational DoS	It could	Easy	Monitoring and	High	High

	jeopardize the availability of GENI testbed		suspending partial GENI testbed		
Eavesdropping	Variable	Easy	Encryption	Medium	Medium
Traffic Injection	Variable	Easy	Authentication	Medium	Medium
Protocol Specific Vulnerabilities	Variable	Variable	Variable	Variable	Low
RF Interference	Will prevent the wireless part of GENI testbed from working properly	Unintentional interference is very likely	RF environment monitoring and cooperation among wireless devises	Need Monitoring infrastructure	High
Physical Threats	Severe	High	Low-tech solutions	Variable	High
Ephemeral Rogue Networks	Waste the resources of GENI testbed on illicit activities.	Easy	Monitoring and analyzing users' operations	Involve large amount of auditing data recording and processing	Low
Greedy user/experimenter	Cross experiment interference	Easy	Monitoring and experiment separation	High	Medium
Unintentional User misuse/interference	Variable	Medium	Monitoring and suspending the experiments	high	Low
Administrator Mis-configuration	Variable	High	Good human-machine interface designed to assist operations	variable	Medium

One recommendation that seems important to make builds upon the creation of a GENI Cert, as recommended in GDD-06-10 [2]. As we have noted in this document, the threats facing the different GENI subsystems will vary, and the defense mechanisms/responses might differ. Further, GENI components will be highly geographically distributed, spanning global and cultural distances. Although many facility security issues can be addressed by members of host organizations (e.g. by network administrators at a university or GENI participating site), there will be threats that can span multiple organizations, and addressing such threats will require a coordinated response effort. Therefore, the GENI Cert should be hierarchically organized, with individual response teams located within the vicinity of key edge sites. Such response teams might, for example, follow an organization similar to volunteer fire departments, where task force members are on-call to respond to both "local" problems (e.g. threats being faced by a single site), as well as part of multi-community responses to larger-scale disasters (e.g. threats that span multiple GENI locations).

In support of the GENI Cert teams, there must be a sufficient security monitoring infrastructure that can feed detection, security alarm, and response processes. Many aspects of the security monitoring functionality can be shared with experimental infrastructure. For example, records of background RF readings might both be useful to an experimenter who wishes to calibrate protocol performance, as well as to anomaly detection schemes. However, in spite of this possible overlap, there may be scenarios where it is desirable to have a measurement infrastructure that is completely inaccessible to GENI users, and is only accessible to GENI administrators.

Repeated security drills (i.e. penetration studies) and evaluations should be scheduled at regular intervals in order to ensure that the wireless security systems are up to date. This recommendation complements the recommendation of the GENI Facility Security document that GENI operations and governance should perform test runs to evaluate procedures for handling security breaches [1]. It should be further noted that such security drills will not only allow for the improvement of security tools and mechanisms, but will also ensure that that apparatus used to perform monitoring is properly calibrated.

In addition to the general recommendations listed above, there are several key requirements that must be integrated into the design of security components for the wireless portions of GENI:

1. *Compartmentalization of Security Material:* Although the GENI management and control functionality will treat wireless components in much the same way as other GENI components, the heightened risk for compromise of wireless devices necessitates that parameters and material used for the facility's security be localized to mitigate impact upon other portions of GENI. In particular, compromising a GENI wireless node should not provide an adversary access or the ability to gain privileges in other parts of GENI.

2. *Support Wireless Security Experiments:* GENI's wireless components will be used to develop the next generation of wireless security protocols, and therefore the wireless components must be configurable in a manner that allows for security experimentation, while also ensuring that several absolute security requirements are upheld (e.g. slice separation).

3. *Minimal Performance Impact of Security Mechanisms*: Security mechanisms can have a significant impact on the performance of protocol experimentation. Even basic mechanisms, such as encryption and authentication, necessitate additional computational and communication overhead. The security mechanisms that are selected for the wireless components of GENI must be carefully selected so that the resulting impact on experimental validity is minimal. In particular, sensor nodes, which represent the most light-weight of all wireless components, should be able to operate without security mechanisms, while compensatory security functionality should be placed at the aggregate component at the sensor net and GENI interface.

Lastly, we recommend, during the planning of the GENI facility, that GENI's architects contact or involve representatives from the telecommunications industry who have experience in securing large-scale, high-value communication networks (e.g. telephone networks). It should be pointed out that protecting GENI will be different from protecting comparatively smaller

corporate enterprises, or from sanitizing the extremely distributed Internet. Unlike the broader Internet, there will be a single organization that is responsible for GENI and, at the same time, most of the equipment that will make up GENI will be owned by this organization. Whereas the Internet lacks any central authority, the presence of GENI management and specified points-of-entry (which should be monitored by suitable firewalls and policies) will make protecting GENI more tractable than defending the broader Internet. In essence, it should be feasible to provide a safe environment for experiments to be performed by using the separation that the GENI facility provides.

Acknowledgements:

This document is a compilation of the discussions that have occurred within the GENI Wireless Working Group regarding security issues, recommendations, and requirements. Further, the authors of this document would like to acknowledge valuable input from Tom Anderson, of the GENI Planning Group.

Bibliography

1. T. Anderson, M. Reiter, GENI Facility Security (DRAFT), version 0.1, August 2006.
2. J. Basney, R. Campbell, H. Khurana, V. Welch, Towards Operational Security for GENI, GDD-06-10, July 2006.
3. S. Paul et al., Requirements for Management and Control of Wireless Networks in GENI, September 2006.
4. D. Raychaudhuri and M. Gerla (eds), Report of NSF Workshop on New Architectures and Disruptive Technologies for the Future Internet: The Wireless, Mobile and Sensor Network Perspective, GDD-05-04, August 2005.
5. Emulab Testbed, www.emulab.net
6. ORBIT Wireless Testbed, www.orbit-lab.org
7. Kansei Sensor Testbed, http://ceti.cse.ohio-state.edu/kansei/
8. AusCERT, AA-2004.02- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices
9. W. Xu, W. Trappe, Y. Zhang, T. Wood. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pg. 46-57, 2005.
10. P. Kyasanur, N. Vaidya. Detection and Handling of MAC-layer Misbehavior in Wireless Networks. In *Proceedings of the IEEE Internation Conference on Dependable Systems and Networks*, pg. 173-182, 2003.
11. M. Raya, J. Hubaux, I. Aad. DOMINO : A System to Detect Greedy Behavior in IEEE 802.11 Hotspots. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services*, pg. 84-97, 2004.
12. Trusted Computing Group, https://www.trustedcomputinggroup.org/home