ISEAGE Testbed Overview

1.0 Problem Statement

The **Internet-Scale Event and Attack Generation Environment** (ISEAGE) (pronounced "ice age") security testbed is designed and dedicated to creating a virtual Internet for the purpose of researching, designing, and testing cyber defense mechanisms.

Many researchers and vendors are working hard to provide products and services to help defend against cyber attacks. Users of these technologies often do not have any mechanisms to test or even try out these defenses. Researchers and vendors are in need of a facility to test ideas against real world attacks. The ISEAGE testbed provides provide a controlled environment where real world attacks can be played out against different configurations of equipment. It contains a vast warehouse of attack tools that are able to simulate point-to-point and distributed attacks against test configurations. The ISEAGE testbed represents a new paradigm in the area of security research and will enable new and innovative research needed to solve the current security problems facing the world today.

As discussed in the report from the NSF workshop on network research testbeds the need for testbed networks is well documented. We believe this is especially true in the area of security research, where too often security research is based on either data from the internet directly or from artificial data. Either way this can lead to results that are hard to recreate or may not apply to the real world. By recreating the internet for the purpose of launching controlled attacks in the presence of known background data the investigators are confident that higher quality research results will be obtained. ISEAGE provides this environment and facilitates a level of research well beyond the current state of the art.

2.0 ISEAGE Overview

The goal of ISEAGE is to provide a world class research and education facility to enhance the current state of the art in information assurance. This one of kind facility will be the catalyst for bringing together top researchers from several disciplines for a common goal of making computing safer. We currently have over 30 faculty members affiliated with the ISU IAC. The ISEAGE testbed provides an integrated environment to work on synergistic research projects in information assurance. The research areas in information assurance at Iowa State University deal with overlapping problems and can benefit from a common laboratory. For example, the group working in intrusion detection and the group working in survivable networks often utilize the same attack data and are concerned about the same types of attacks. The ISEAGE is a critical element needed to elevate the research efforts and to help provide solutions to these complex problems. We have already had numerous discussions with government agencies, business, and industry about the potential benefits of the ISEAGE, and we have received over $3,000,000 in support to fund the ISEAGE testbed. The following is a summary of the current and potential impact of the ISEAGE testbed:

- **Critical Infrastructure protection:** While we depend on the stable operation of the network for many parts of our daily lives, several parts of the network control critical parts of the infrastructure. This infrastructure can be federal, state, local or corporate. The ISEAGE can be used to recreate critical components of an infrastructure on an ongoing basis. These live models of the infrastructure will be subjected to constant attacks to probe for weaknesses and to try the newest attacks before they become a threat to the actual infrastructure. Any detected weakness will be used to strengthen the actual infrastructure. The goal would be to develop algorithms and methods to harden the networks and computers used to support the critical infrastructure. We have started a project to model the State of Iowa cyber infrastructure with the goal of being able to determine interdependencies between systems and any weakness in the system. We will also be able to study "what –if" scenarios and help

the state develop contingency plans in case of a cyber attack. Once deployed on ISEAGE the State of Iowa will not only be able to test the infrastructure, but will be able to use ISEAGE to provide training of the staff and to try out new protection systems in a controlled environment. Lessons learned from the research will be exported to other states.

- **End-users of security:** End users of security are often forced to deploy technology without field-testing. The ISEAGE provides a place for to test out security configurations prior to deployment and to try equipment and configurations from different vendors. Many of the distributed attacks rely on the inherent weaknesses in the end user systems. By looking at the security of end user systems we can develop new methods to provide increased security for all systems. We have used ISEAGE to conduct product testing for Network World magazine.
- **Developers of security:** The ISEAGE facility provides a test environment for developers to deploy versions of their products. We envision working on jointly funded research projects to create new methods, processes, and algorithms to provide security.
- **Academic and industrial Researchers:** The ISEAGE testbed has designed to provide an excellent environment to conduct state of the art research in computer security and security tool development. Four tightly coupled research efforts involving over 30 faculty members will be the initial focus of the laboratory. We envision additional faculty and research efforts will utilize the facilities.
- **Law enforcement agencies:** The IAC faculty members have worked with several local law enforcement agencies to provide computer forensics support, advice, and training. The ISEAGE testbed has been used to create new tools and methods to support law enforcement.
- **Course Support:** Iowa State University offers several courses in information assurance and networking that have greatly benefited from access the ISEAGE testbed. One course in particular has a synergistic relationship with ISEAGE. We teach a course in information warfare where the students learn how to attack and defend computer systems. One of the experiments in the course is to have students break in to a fake company and then detail both how they did it and how they could stop it. We envision using this class experiment as a way to test out new security concepts and to provide a controlled environment to test out new theories and methods. We have already used this class to test a couple of new ideas in attack tolerant networks. In the spring of 2005 Iowa State University hosted its first cyber defense competition using ISEAGE as the battle ground. Student teams are given a set of operational criteria and then asked to develop a security system to protect an organization. The student teams then spend a weekend defending their organizations against security professionals trying to break into the systems. By using ISEAGE Iowa State University is able to provide the most comprehensive and realistic environment for a cyber defense competition. Our students are better equipped to protect the cyber infrastructure because of these competitions. We have held over 15 competitions to date including a national competition.
- **Security training:** The ISEAGE testbed has been used to support hands-on security training for various groups and organizations. Starting in 2010 we will start to offer regularly scheduled training events to various groups including law enforcement.

3.0 ISEAGE Description and architecture

This section will describe the ISEAGE testbed and will provide an overview of the ISEAGE architecture and what makes ISEAGE different from conventional testbeds.

3.1 ISEAGE architectural overview

There have been several successful network testbeds, but ISEAGE is designed specifically for use in security research and offers many advantages over a conventional network testbed. The primary advantage is the architecture and tool set that will be designed for ISEAGE. These tools and an overview of the ISEAGE architecture are outlined below.

The Figure 1 below illustrates the functional components of the ISEAGE. The primary design goal is to provide a highly configurable environment than can model any aspect of the Internet. The ISEAGE to be designed such that configuration can be changed quickly and that multiple research experiments can be carried out at the same time. The lab will consist of multiple copies of each component, which will allow either multiple simultaneous experiments or for very large single experiments. Each of the key components is described below along with an anticipated equipment list.

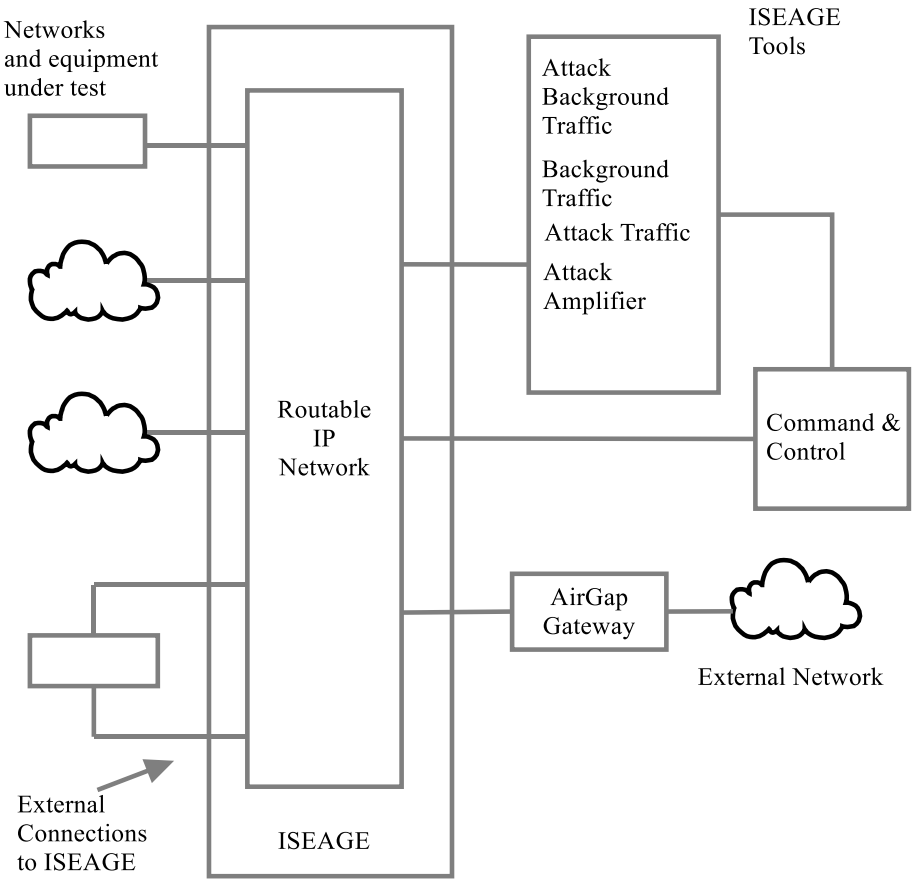

Figure 1 ISEAGE Architecture

Routable IP Network

The core of the ISEAGE testbed is a routable IP network. The routable IP network supports the traffic to and from the networks and systems under test. It also supports connectivity to the custom tools used to generate and monitor traffic. The routable IP network is accomplished using a custom program called ISEFlow. The ISEFlow is a modified router that creates virtual networks that can be interconnected to create a large virtual network. The ISEFlow can act as a set of virtual routers so that traffic appears to have routed through the Internet. ISEFlow is at the heart of the unique ISEAGE architecture and is described in more detail in a later section.

Networks and equipment under test

The external interface to ISEAGE is through an Ethernet connection. This interface is used to connect devices or networks under test and creates a network connection which can support up to 50 subnets. The external interfaces connect to ISEFlow or to other ISEAGE tools. As shown in Figure 1 devices can be placed between two external interfaces which allows for the testing of network infrastructure components.

Command and control network

The command and control network consists of two networks, one used to management of ISEAGE and the other used to control the attack generation. The monitor control network is a separate network used to monitor the core ISEAGE functions and the virtual networks. By using a separate network for monitoring and control of the network any traffic generated will not affect the performance of ISEAGE. This can also allow remote control of ISEAGE via the Internet, while still maintaining isolation between the virtual Internet and the real Internet. The control network consists of several command consoles connected to data collection tools and to various control points. Data and control information will be routed through the monitor control network to the individual devices.

The attack control network is a separate network used to manage then monitor the attacks and the attack tools. By using a separate network for monitoring and control of the attacks any traffic generated will not affect the laboratory. This can also allow remote control of the laboratory via the Internet, while still maintaining isolation between the virtual Internet and the real Internet. The attack control network will be identical to the Monitor Control Network.

Air Gap Gateway

The air gap gateway is designed to allow ISEAGE to interact with the Internet. The current interaction is limited to DNS requests and HTTP GET requests. This allows users of ISEAGE to access web information and to also allow a mapping of actual host names to their IP addresses, thus allowing ISEAGE to mimic parts of the actual Internet.

ISEAGE Tools

There are multiple tools that are designed to support ISEAGE. The tools use a common command and control protocol to allow easy integration into the virtual internet command and control network. Below is a brief description of the tool set. Not all tools are fully operational. We currently have a team of students working on completing several of the tools.

Attack Amplifier & Condenser

The attack amplifier is used to convert an attack launched from a single computer into an attack that appears to be launched from multiple computers. This tool will allow researchers to study distributed and flooding based attacks. With this tools research can create attacks that appear to come from thousands or even tens of thousands of computers.

The attack condenser works with the attack amplifier. Often distributed attacks create a large number of responses back to the attacker or responses that have been redirected to another target. The attack condenser will take the responses and condense them into a small number of responses. It can also be configured to respond to the messages. For example if there is a redirected distributed attack pointed to a machine, the attack condenser can become that machine and absorb the attack and respond when necessary. This tool is described in more detail as part of the discussion on ISEAGE routing.

Packet changer/responder

The packet changer/responder can be used to modify packets in real-time as they flow through the network. This tool can be used to create man-in-middle attacks or can be used to generate traffic in response to certain incoming packets.

Data Collection system

In order for ISEAGE to be used as a research tool a network of devices must be in place to monitor and capture the results of the research being conducted. Since the nature of the data to be collected depends on the research being conducted a separate data collection system must be designed.

Lab Extender (in design)

The lab extender is used to extend the ISEAGE across the actual Internet, by placing a lab extender in a remote location connected via the Internet to a lab extender connected to the ISEAGE. The extender will use compression and special protocols to increase the effective bandwidth between two extenders. The lab extender can be used to provide remote testing of infrastructure components. The lab extender will also be used to setup remote virtual Internets for collaboration on research projects with other universities, agencies or businesses.

Attack Collector/Watcher/Replayer

These three tools are used to collect information to be replayed within the virtual internet. The attack collector is a honey pot / honey net that will be used to collect host based attacks. The attack watcher is an intrusion detection system that will capture network attacks. The attack replayer is used to replay the attack inside the virtual internet. The attack collector and watcher are connected to remote sites via the internet using encrypted connections.

Attack Tool Repository

An extensive library of attack tools will be maintained. The library will allow the researchers to launch a wide array of attacks, and by feeding the attacks through the tools described above the testbed network will provide researchers a mechanism to design and test defenses against real attacks

Traffic collector/replayer

A tool is needed to capture traffic patterns from the actual internet at particular locations so they can be replayed with ISEAGE. This will often be used to gather information about traffic patterns at a client's network so that ISEAGE can recreate those patterns. The collector will need to capture traffic patterns without capturing the data. The replayer will then reconstruct traffic from the captured data to recreate as close to possible the background traffic seen at a given location on the actual internet. A possible extension would be for the remote collector to send data back to the replayer in real-time to allow for a more dynamic recreation.

3.2 ISEAGE architecture

At first glance ISEAGE appears to be no different than conventional Internet testbeds. The next two figures below provide insight into why ISEAGE is different and why these differences enable us to model very large scale networks. The figure below shows the hardware implementation of a multiple node ISEAGE testbed. It should be noted that we have deployed smaller versions of ISEAGE for some of the cyber defense competitions and have even ran a short course off site with a single node version. Figure 2 shows the multiple node clusters interconnected with a high speed backplane. Each node in ISEAGE can run the ISEFlow application as well as additional tools.

The layer 2 interconnect on the high speed backplane allows ISEAGE to implement unconventional routing that is described in the next section. The layer 2 interconnect also supports the connection of ISEAGE tools and traffic generation.

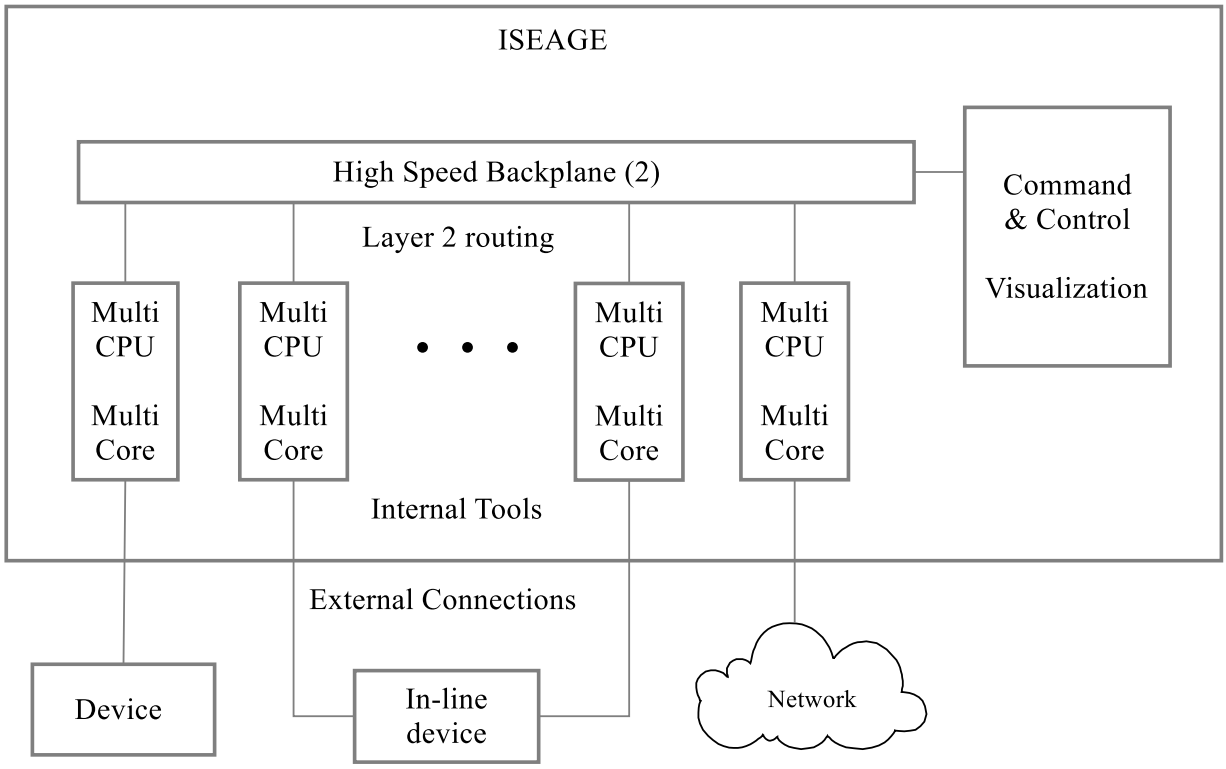

Figure 2. ISEAGE hardware configuration

Figure 3 shows the software architecture of a single node running the ISEFlow application. The ISEFlow application creates the external subnets as well as a large number of internal networks. As was mentioned earlier the ISEFlow tool creates a routable Internet. Unlike conventional testbeds where each router represented by either a real router or a software router running on a computer, the ISEFlow application can create up to 100 routers per board and these routers can be configured to create arbitrary topologies. ISEFLow currently supports the concept of an internal cloud network where the cloud represents a cluster of routers. If an external computer preformed a traceroute it would see a number of hops between itself and server as if there were real routers between it and the server. The TTL field in the IP header would also indicate the traffic traversed multiple routers. This is useful for scenarios where we are interested in a large network but are not interested in the internal components. The next set

in the development of ISEFlow is to implement internal router modules which will respond to router messages like SNMP or BGP. The ISEFlow architecture is designed to support additional modules as needed.

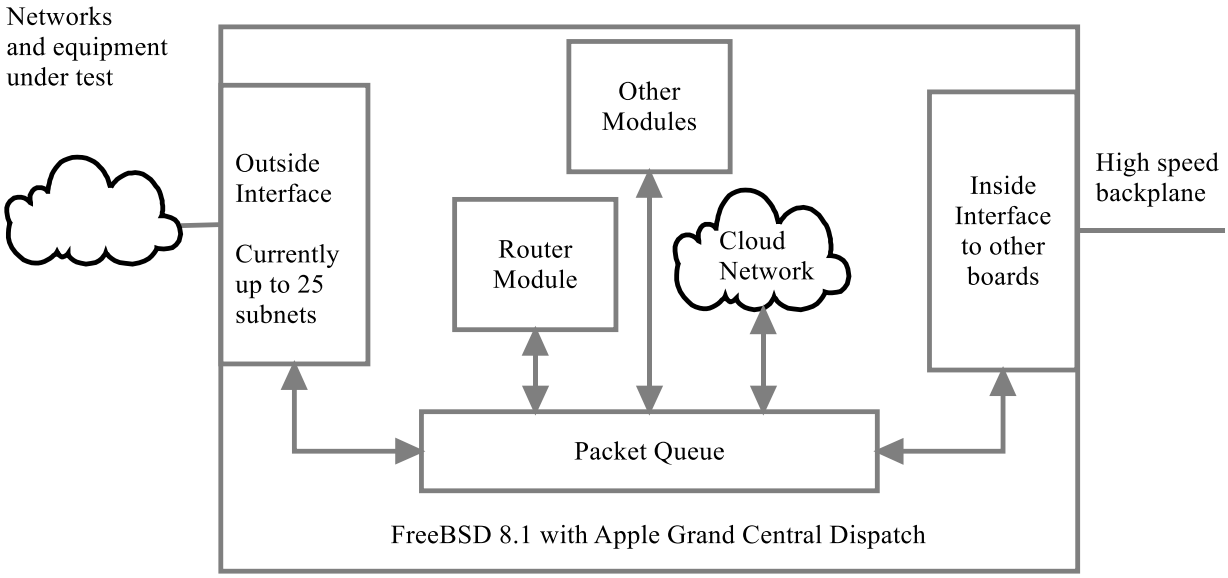

Figure 3 ISEAGE board with ISEFlow

3.3 ISEAGE Routing

Figure 4 shows a logical view of a possible network configuration using ISEAGE. In this figure we see that each board represents a number of routers and these clusters are then interconnected by the devices of interest for the test. The cluster of routers will alter the traffic as if the traffic traversed the routers. As we see in the figure the systems under test are either attached as endpoints and view ISEAGE as an Internet connection or they can be devices that are inserted in the data flow through ISEAGE to test routers, firewalls and other devices that interconnect multiple networks. The large dark line represents normal traffic through ISEAGE.

A more interesting and useful feature of the ISEAGE architecture is its ability to create and route distributed attacks. The problem with modeling a distributed like the DOS attack that was launched in July 2009 against multiple web sites is that it is difficult to create routable traffic that looks like it has originated from multiple sources. ISEAGE lets you create traffic from a single source and using the Attack Amplifier it will take each packet and replicate it as if it came from numerous different sources. The real issue comes when the packets are returned from the victim computer. The victims will response with the destination address equal to the fake address supplied in the attack packet. In a conventional testbed that packet could not be routed back to fake address. ISEAGE supports a concept called the attack plane which will route the packets back to the real device that sent the attack packet independent of the IP destination address. The condenser code will then take the rely packets and return them to the device that sent the original attack packet that was amplified. This is shown in Figures 4 and 5. In Figure 4 the red lines shows a distributed attack being launched from a single host. The attack plane allows the traffic to be returned to the machine that generated the traffic. Figure 5 shows the traffic flow through the boards to and from the attacker. The grey lines represent normal traffic flow and the red lines show the traffic being return via the attack plane.

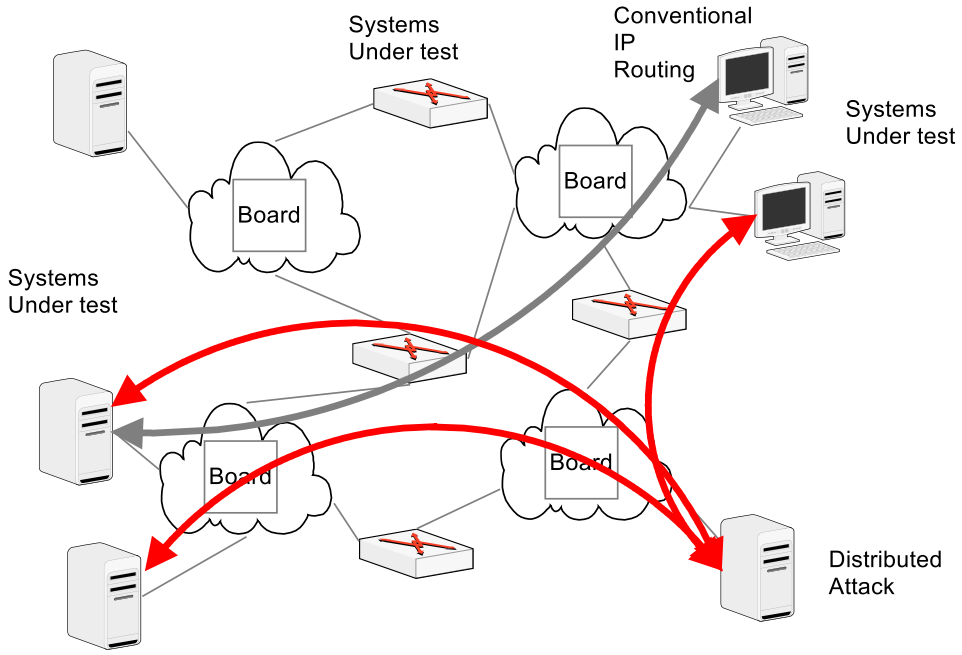

Figure 4. ISEAGE routing

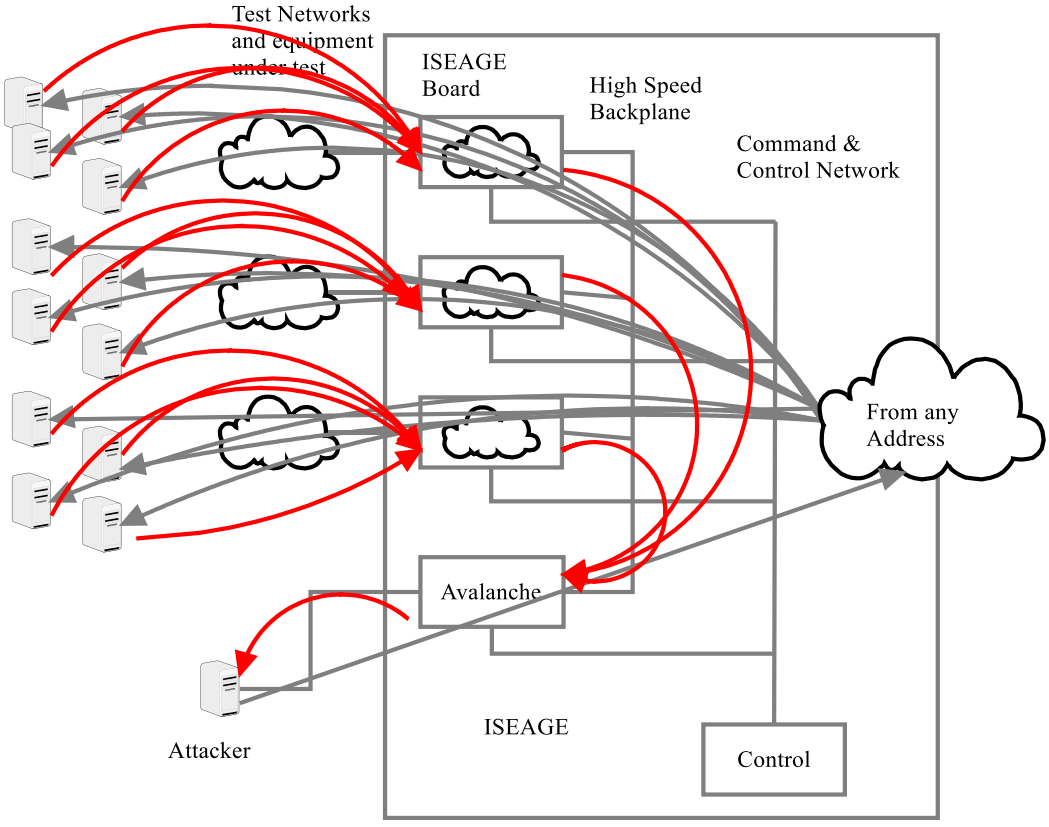

Figure 5 Attack amplifier and condenser

3.4 Other ISEAGE Versions

In addition to the full scale ISEAGE testbed several smaller versions have been developed. ISECube is a small version of the full scale ISEAGE that is designed for smaller applications and can be located at the user's location. ISECube can be connected to ISEAGE to create a larger testbed. ISEBox is a version of ISEAGE that is designed to support cyber defense competitions. ISEBox has supported cyber defense competitions with over 100 students. This is a single node version of ISEAGE can be delivered as a software only solution to be installed on the user's hardware. ISEBerg is a version designed to support training.

4.0 ISEAGE Use Cases

The next few sections briefly describe some of the issues that could be addressed by using the ISEAGE testbed.

4.1 Product and device testing

ISEAGE has already been used to test data loss prevention devices for a major networking trade magazine. As part of that process we developed the testing methodology and the testing metrics. We have entered an agreement to carry out additional tests of other products. The testing of commercial-off-the-shelf (COTS) products in a controlled environment is one issue that can be addressed as part of this project.

4.3 Cyber Infrastructure modeling

‘‘Map Iowa" models the state's critical cyber infrastructure. "Map Iowa" is built upon the Internet-Scale Event and Attack Generation Environment (ISEAGE) testbed network housed at Iowa State University and its portable counterpart ISECube. Both the ISEAGE and ISECube testbeds simulate the Internet with real computers and networking hardware, not just programming software. "Map Iowa" adds traffic generation to the existing testbed's to simulate normal traffic (or usage) of each of the critical pieces in the state's infrastructure. Through parameterization, loads on the critical asset can be pushed upward to induce stress to or failure of the mode. The critical assets could be targeted singularly or could part of a multiple failure situation. The Map Iowa project will allow the state of Iowa to plan and react to failures in the critical infrastructure and will serve as a proof of concept to model other regional infrastructures.

4.3 Critical Infrastructure modeling

Emergency Planning, Emergency Preparedness. Disaster Response. Disaster Recovery. All of these terms describe local, regional, state and national planning efforts that have been undertaken to protect resources and people in case of a disruptive event in a region. The seemingly more frequent occurrence of natural disasters such as ice storms, blizzards, floods, wild fires and hurricanes or man-induced incidents such as power black outs, bridge failures and even terrorism have heightened awareness of the need for such planning. These types of events have damaged physical structures, harmed people, destroyed personal property, caused lost worker productivity and created lengthy interruptions in basic services such as electricity, water, communication, transportation and sanitation in the affected areas.

Ideally the critical infrastructures would be modeled in a single, unified, comprehensive system that could be used for training and preparedness, as well as real-time decision-making in response to real-time disaster data streaming into the model. This unified approach would not only depict real-time physical events as they happened, but would allow responders to model outcomes in the physical world based upon potential response decisions. This thrust of this work is to develop a meta framework that allows modeling of critical infrastructure and assets with physical data which can be used for training, preparedness, and real-time reaction.

This unified model is the Critical Infrastructure Modeling and Response Environment (CIMoRE) [pronounced “see more”] which represents a new paradigm for disaster planning and response.

CIMoRE accounts for all critical infrastructure components such as roads, bridges, rail systems, water treatment facilities, power grids and telephone systems, cyber networks, as well as their interdependencies, in its single, unified framework. It operates in two modes; it provides options to run in both a simulated mode for preparedness training and in real-time mode for reporting of the health of critical infrastructure components as a disruptive event occurs. Additionally, it provides for a varying level of complexity in the inclusion or exclusion of critical infrastructure components. CIMoRE gives emergency planners and disaster responders the opportunity to view the physical locations of the critical infrastructure components, assess their interconnectedness, identify their failing health state, determine and avoid congestion, visually play out mitigation options, document analysis decisions and record the recovery of the critical components. CIMoRE is designed to use the ISEAGE testbed.

4.4 Training

ISEAGE is used to support the Cyber Defense Competitions and security short courses.

