NGI/CE/03

Wireless and Public Network Gateway Security Server

FY 2003 Proposal to the NOAA HPCC Program

August 19, 2002

| Title Page | Proposed Project | Budget Page |

Principal Investigator:	**John P Hernandez**
Line Organization:	OAR
Routing Code:	R/OM/62
Address:	NOAA/OAR/OED 325 Broadway Boulder, CO 80305
Phone:	(303) 497-6392
Fax:	(303) 497-6005
E-mail Address:	John.Hernandez@noaa.gov

Other Investigator 1
Michael.T.Knezevich@noaa.gov

Proposal Theme:	**The Next Generation Internet (NGI)**
Funding Summary:	FY 2003 $ 22,000

John P Hernandez	Jerry Janssen	Kent Groninger
Network Specialist	Network Manager	Executive Director, Boulder Operations
NOAA Boulder NOC	NOAA Boulder NOC	NOAA/OAR/OED

Wireless and Public Network Gateway Security Server

Proposal for FY 2003 HPCC Funding

Prepared by: John P Hernandez

Executive Summary:

As demand for wireless LANs and visitor networks grows at NOAA sites, the security concern posed by these networks often hinders our ability to deploy and utilize new technologies. One method that has been used successfully to contain the security exposure of wireless and roaming networks at organizations such as NASA and the University of Oregon is the concept of an "Authentication Gateway Server." This method is very simple to deploy and manage, and it offers arguably better security than distributed Wired Equivalent Privacy (WEP) keys, which are proven to be insecure.

The principal investigators will develop and deploy a software and hardware solution for wireless (and wired public access) network security based on the Authentication Gateway Server concept. The basic premise is to allow routing, or basic inter-network connectivity, to and from the local network only after a user has established her identity to the gateway (router). This method offers the distinct advantage over WEP and Ethernet address-based (MAC) authentication of being very scaleable and accountable. It effectively sandboxes unknown users on an untrusted network until such time as they are identified as either authorized guests or NOAA staff.

No special client software is needed. Any client equipped with a modern Web browser can interface with the authentication gateway and be given the opportunity to provide user credentials.

This topic is identified in the FY '03 NGI proposal guidelines as one of the primary areas of interest. It is vital that NOAA's networks be secure, while also providing high levels of accessibility and performance.

Problem Statement:

At many of NOAA's facilities, there is a desire to offer wireless LAN services and the ability for pre-approved guests to use our networks in a secure, accountable way. The security risks of wide-open networks are unacceptable, and the expense (in terms of dollars and employee hours) of implementing traditional solutions is prohibitive.

An authorized roaming user should have the ability to plug in (or associate with a wireless device) and painlessly supply her credentials for network access. This procedure should not require special client software or pre-configuration of network parameters by staff. The authentication system should provide details to interested NOAA IT managers about who is using the system in the form of logs and reports.

A potential user needs to be made aware of the consequences of using an unencrypted network for transmitting sensitive data and advised to use end-to-end encryption such as secure shell (SSH) or virtual private networking (VPN) when confidentiality is necessary. The user should be sheltered from inbound connections and internet scanning activity to the extent possible, and they should be treated as residing in an untrusted demilitarized zone (DMZ) even after authentication has taken place.

Proposed Solution:

A Unix workstation with dual network interfaces will serve as the only gateway (router), domain name server (DNS), dynamic network configuration (DHCP) server, and web server for the "roaming" network. This network will be associated with a site virtual LAN (VLAN) on which wired ports and wireless access points will be positioned. WEP can be optionally enabled on the wireless devices.

Standard operating system firewall software will be utilized to sandbox unknown clients and redirect any attempted Web access by unauthenticated clients to the authentication gateway homepage. In this manner, a client whose machine has been configured by DHCP only needs to navigate to a web page to become aware of their unauthorized, or "sandboxed", network state. At this point, after an appropriate warning (as described above) has been displayed, the client will be offered the opportunity to authenticate to the gateway.

The NOAA NEMS directory offers the perfect database of staff credentials to use for this application. The combination of HTTP and LDAP over SSL offer a robust and convenient method for secure transmission of user credentials. In addition, staff with NEMS credentials will be given the ability to create temporary accounts for potential visitors that do not have NEMS accounts.

Once authenticated, a user will retain routing ability until their machine is no longer visible on the LAN (as checked by automated probes at 5-minute intervals) or 24 hours has elapsed, whichever comes first. This limited authentication window is necessary to avoid security threats such as connection hijacking.

Analysis:

The elegance of this solution lies in its scalability and ability to keep records of roaming users who have accessed network resources. Other existing solutions cannot match this level of utility at an equivalent cost.

WEP is insecure and is not scaleable. MAC address authentication is insecure and not tied to individual users. 802.1X (port-based network access control) is not mature, not widely available in existing network hardware, and expensive to license. Other available authentication gateway software such as NoCat has multiple problems, for example, the inability to securely link with existing NOAA credentials (LDAP), and the inconvenient requirement that a client web browser window remain open. Other authentication gateway solutions depend on secure shell (SSH) connectivity, which requires a login account on the gateway machine.

The proposed solution will not be a dead-end technology due to its basis on open standards and the availability of well-written source code and script. In addition, it will be inexpensive enough

for deployment at smaller sites. The system will be largely self-maintaining, and administrator intervention should be infrequent. A system disk image can be provided to make recovery from any disk failure very rapid and painless.

Performance Measures:

This project can be successfully accomplished according to the following timetable:

Milestones

Month 02 – Obtain rackmount Unix servers with dual network interface cards.

Month 04 – Deploy basic routing, firewall, DHCP, and DNS functionality on the gateway

Month 06 – Write the web interface for the authentication routines

Month 08 – Develop the CGI (Perl) programs for LDAP-based authentication and temporary account management

Month 09 – Develop the sweep algorithms and accounting/reporting routines

Month 10 – Gather a group of beta testers for a limited deployment

Month 12 – Finish debugging the gateway and plan a final site deployment

Deliverables

The following is a list of deliverables from the project:

- Authentication gateway application, written in Perl/CGI
- Functional wireless and public visitor network deployments in Boulder and Seattle
- A software package and documentation explaining how the application can be deployed at other sites