September 10-12, 2007
Los Angeles Convention Center
Los Angeles, California

TMC INTERNET TELEPHONY® Conference & EXPO
Our 15th Event!

www.ITEXPO.com

Securing Enterprise VoIP

VoIP Vulnerabilities
Patrick Young
CEO Arlinx Inc.

Patrick Young
CEO Arlinx, Inc.
http://www.arlinx.com
(954) 344-7665

Arlinx manufactures a telecom carrier grade application specific IP Telephony and IP Security Linux open platforms. Ultra reliable (20 year MTBF and 85º C operating temperature) with hardware encryption and strong authentication with certified cryptographic storage. Very energy efficient (6 Watts*), executes 1.33 Billion instructions per second. Best performance per Watt and lowest Total Cost of Ownership. No fans or moving parts, two GigE ports (copper and fiber-optic), four USB 2.0 ports, immune to most malware, strong Administration, Maintenance and Provisioning features. Great alternative to a commercial grade PC.

www.arlinx.com

Enterprise VoIP Security

- **Arlinx Secure IP Optimized VoIP Platform**
  - Strong Authentication
  - Accelerated Encryption
  - Certified Cryptographic Storage Module
  - Dual Fiber and Copper GigE ports
  - No Moving Parts, 20 year MTBF
  - Amazing Performance per Watt (6 Watts)
  - Dual Power Supplies
  - 1 GB Low Voltage DDR2 RAM **with ECC**
  - Mini-ITX Form Factor, Open Platform with API and SDK
  - Speech and Video Media Processors

Enterprise VoIP Security

- Reasons for VoIP Security
  - Financial Loss
  - Regulatory Penalties
  - Civil Damages
  - Repair and Maintenance Cost
  - Breach of Customer Trust
  - Thwart Espionage and Eavesdropping
  - Data Theft
  - Toll Fraud
  - Career at Risk

- **VoIP Infrastructure**
  - IP-PBX
  - IP Phones/End Points/User Agents
  - HTTP and Media Servers
  - Gatekeeper
  - Registration Servers
  - Redirect Servers
  - Media Gateways
  - Firewalls and Application Gateways
  - Proxies
  - IP Switches and Routers
  - AAA Servers, LDAP, DNS, SNMP, NAT, DHCP

Enterprise VoIP Security

- **Basic Vulnerabilities Prevention**
  - Physical Security
  - Strong Authentication on Entire Infrastructure
  - End to End Media and Signalling Encryption
  - Voice and Data Segregation
  - Prevent Loss of Power
  - Prevent Loss of Data (Backups and Error Correction)
  - Stateful Firewalls and Packet Filters
  - Perimeter Security
  - Vulnerability Assessment and Torture Stress Testing
  - No Softphones, No WiFi

Enterprise VoIP Security

- Physical Security
  - PBX secured in locked room
    - Access Control, Access Card, Biometrics
    - Video Surveillance
    - Entry Point Alarms
    - USB ports disabled
    - Strong Authentication, with No Remote Access
  - Theft of System, Hard Drive, or Data
  - Access to Authentication Keys and Certificates
  - Reset Passwords through BIOS
  - Alter OS, Plant Spyware
  - Fire and Flood Prevention
  - 2-5 Hours Battery Backup

- **VoIP Attack Methods**
  - Footprinting
  - Scanning, Host and Port Discovery
  - Enumeration
  - Espionage and Eavesdropping
  - Hijack and Redirection
  - Signaling Attacks
  - Denial of Service
  - Exploit OS Vulnerabilities, Virus, Worms, Spyware
  - Infrastructure Attacks

- **Footprinting the Attack Target**
  - Research Target Web Site
  - Enterprise Structure and Locations
  - Help and Tech Support intended for internal use
  - Job Listings
  - Phone Number and Extensions
  - Default Auto-Attendant Messages
  - Press Releases
  - User Groups and Support Forums
  - Search Engines
  - DNS Whois

- **Scanning Host Discovery and Device ID**
  - Hack Tools
    - **Nmap**
    - **SMAP**
    - **Sip-Scan**
    - **Superscan**
    - **SolarWinds**
    - **Nessus**
    - **Port Scanner**
    - **Hping**
    - **SIPVicious Suite**
    - **VLAN Ping**
    - **VoIP Audit**

Enterprise VoIP Security

- **Ping Sweeps**
  - IMCP Ping, Easily blocked by Firewall
  - ARP Ping, reveals MAC addresses
  - TCP Ping finds active hosts and open ports
  - SNMP Ping, find active network devices & configuration

- **Port Scanning Device Discovery**
  - UDP Scan
  - TCP SYN/ACK
  - Stack Fingerprinting, OS detection
  - Server Detection, DNS, LDAP, RADIUS etc.

Enterprise VoIP Security

- **Enumeration**, User Name and Extension Discovery
  - Hack Tools
    - **Netcat**
    - **Nessus**
    - **Retina**
    - **Saint**
    - **VoIPShield**
    - **Scapy**
    - **SiVus**
    - **Sipsak**
    - **SIPSCAN**
    - **SCTPScan**
    - **SFTF (SIP Forum Test Framework)**

- **Enumeration Methods**
  - SIP Register
  - SIP INVITE
  - SIP OPTIONS
  - TFTP Servers, used for configuring IP Phones
  - SNMP, Reveals IP Phone Configurations

- **Eavesdropping Sniffer Hack Tools**
  - Cain and Able
  - Vomit
  - VoiPong
  - Oreka
  - Wireshark, formerly Ethereal
  - Etherpeek
  - ILTY
  - RtpBreak
  - NetDude
  - PSIPDump
  - SIPomatic
  - SIPv6Analyzer
  - WIST

Enterprise VoIP Security

- **Espionage and Eavesdropping**
  - Conversation Eavesdropping & Recording
  - Call Tracking
  - Number Harvesting
  - Network Sniffing
  - DTMF Capture
  - TFTP Configuration Sniffing

- Denial of Service Hack Tools
  - INVITE Flooder
  - RTP Flooder
  - UDP Flooder
  - SIP Bomber
  - AuthTool
  - SIPp
  - SIPNess
  - Seagull
  - Scapy

- **Denial of Service**
  - Distributed Flooding (Botnets)
  - UDP Flooding
  - TCP SYN Flooding
  - ICMP Flooding
  - SIP Phone Flooding
  - UDP Flood INVITE
  - Application Flooding

- **Targeted Flooding**
  - QoS Manipulation
  - RTP Flooding
  - Malformed Packets
  - INVITE Flood
- **SIP Proxy Flooding**
  - Invalid SIP Phone
  - Invalid IP Address
  - Invalid Domain Name
  - Invalid SIP Phone In Valid Domain
  - Authentication Requests

Enterprise VoIP Security

- Media Hack Tools
  - AuthTool
  - RTP InsetSound
  - RTP MixSound
  - RTPInject
  - RTPProxy
  - SteganRTP
  - Vo²IP

- **Hijack Redirection**
  - **Man in the Middle**
    - Spoof User Agent/Phone
    - Spoof SIP Proxy
    - DNS Spoofing
    - DHCP Spoofing
    - ICMP Redirection
  - **RTP Manipulation**
    - Blocking Media Packets
    - Inserting Media Packets
    - Encrypt Packets

Enterprise VoIP Security

- Signaling Attack Tools
  - BYE teardown
  - RedirectPoison
  - Registration Adder
  - Registration Eraser
  - Registration Hijacker
  - SIP-Kill
  - SIP-RedirectRTP
  - SIPRogue

- **Signaling Attacks**
  - Registration Removal
  - Registration Addition
  - Registration Hijacking
  - SIP Phone Hijack
  - Reroute Calls
  - Reroute Phishing
  - Teardown Conversations
    - SIP Proxy/ SIP BYE
    - SIP Phone/ SIP BYE
    - SIP CANCEL
    - SIP Phone Re-Boot

- **Infrastructure Attacks**
  - OS Vulnerabilities
    - Virus Worms Spyware
  - Firmware Vulnerabilities
  - Network Availability
  - Resource Consumption
  - Infrastructure Attacks
  - DHCP Exhaustion
  - DNS Cache Poisoning
  - DNS Flood

- **References**
  - *Security Guidance for Deploying IP Telephony Systems* from Systems and Network Attack Center (SNAC) of the United States National Security Agency
  - *Security Considerations for Voice Over IP Systems*,Recommendations of the United States National Institute of Standards and Technology
  - *Internet Protocol Telephony & VoIP Security Technical Implementation Guide*, Developed by United States Defense Information Systems Agency (DISA) for the United States Department of Defense (DOD)
  - **The above documents are available in PDF format at arlinx.com VoIP Security**
  - *Hacking Exposed VoIP: Voice Over IP Security Secrets and Solutions,* Authors: David Endler, Mark Collier, Publisher: McGraw Hill, 2007
  - How to Cheat at VoIP Security, Syngress Publishing, 2007 Authors: Thomas Porter, Michael Gough
  - **Additional and detailed information: www.arlinx.com VoIP Security**

Enterprise VoIP Security

- **References**, continued
  - Internet Telephony www.tmcnet.com
  - VOIPSA http://www.voipsa.org/
  - IETF, Internet Engineering Task Force
  - VoIP-News.com
  - SearchSecurity / Information Security Magazine
  - Network World
  - Computer World
  - eWeek
  - CNET
  - Ziff Davis
  - SC Magazine
  - Black Hat and Defcon
  - www.hackingvoip.com

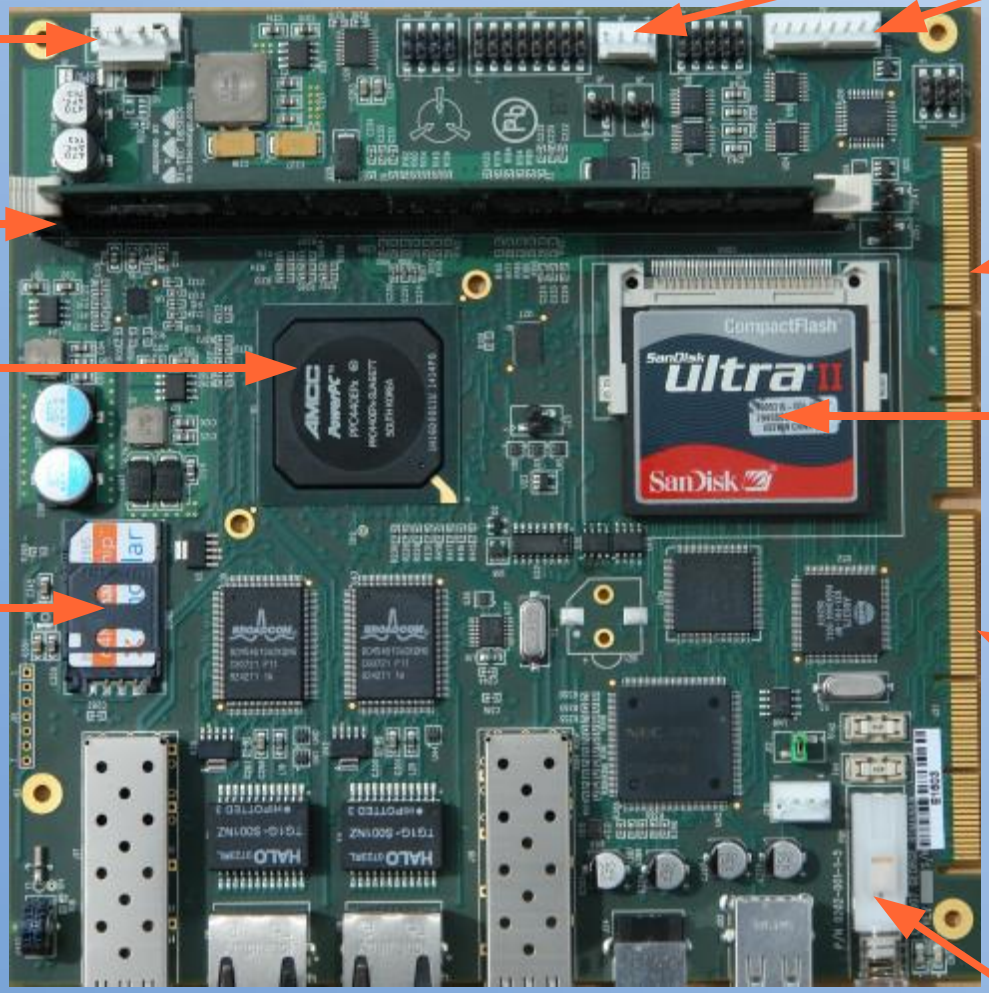
ARLINX

Embedded Linux mini-ITX

6.7” x 6.7”

5 VDC
Input Power

Enclosure Interface
Connectors



1GB DDR2 w/ECC
64 bit data 8 bit ECC

Local Bus Expansion

IP Optimized Power PC
1.3 Billion Instruction/Sec.
Encryption Engine
2 Watts

CompactFlash

Certified
Cryptographic
Storage

PCI Expansion
2 Full Length Slots
in 1U chassis

Blue Locater
LED & Switch

2 GigE Ports, 4 Connectors
2 Fiber-Optic & 2 Copper

3 USB 2.0
2 Type A
1 Type B

20 Year Life Cycle
Military Grade
85ºC Operating Temp
Immune to Malware
Best Performance per Watt
Lowest Total Cost of Ownership
Open Hardware Platform, Linux, and APIs

Editors' Choice
Best of Best of Show

BEST OF SHOW EAST
INTERNET TELEPHONY CONFERENCE & EXPO
2001

www.arlinx.com (954) 344-7665