

DNP

Distributed Network Protocol

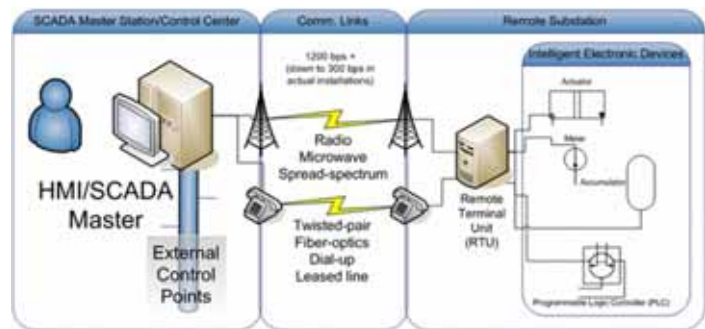
- Connects Components of Process Automation Systems; Crucial in SCADA Systems
- Active in Diverse Facilities from Utilities, Chemical and Power Plants to Shopping Malls
- Mu-4000 Identifies DNP Vulnerabilities in SCADA

Where are DNP and DNP3 Used?

The Distributed Network Protocol (DNP) (also known as DNP3 when used over TCP/IP networks) defines communications procedures for components of process automation systems. Primary beneficiaries are Supervisory Control and Data Acquisition (SCADA) systems for process automation in the electric, water, oil and gas, and transportation industries. However, recent government reports point to more than 1,700 vulnerable private and government facilities ranging from chemical plants and shopping malls to dams and bridges. SCADA master stations (also called control centers), remote terminal units (RTUs), and intelligent electronic devices (IEDs) use DNP3 to perform process automation work.

Automation tasks include opening and closing circuit breakers, measuring line voltages, starting or stopping a motor, or opening and closing a valve. The humans and computers in the master station remotely control a myriad of such distributed and automated tasks. DNP3 is used only for intra-SCADA communications between a master station and devices in remote substations. As needed, master stations use the Inter-Control Center Protocol (ICCP) to communicate.

DNP3 performs multiplexing, data fragmentation, error checking, link control, prioritization, and addressing services for user data, operating at the Data Link Layer (layer 2) of the OSI Reference Model. Many process automation systems operate in harsh physical conditions, which can trigger substantial noise in communications systems. DNP3 compensates for these noisy lines by using checksums within the data frames.¹



DNP3 CONTROLS INTRA-SCADA COMMUNICATIONS IN PROCESS CONTROL SYSTEMS

Source: <http://en.wikipedia.org/wiki/DNP3>

Mu-4000 Identifies DNP3 Vulnerabilities

When operating over TCP/IP transport, security for DNP3 includes limited measures for confidentiality and integrity through Transport Layer Security (TLS) encryption. TLS is the standard that evolved from the Secure Sockets Layer (SSL) encryption protocol. Vulnerabilities resulting from bad implementations of TLS can expose DNP3 networks to attack. The Mu-4000 can identify these and other DNP3-related vulnerabilities, including spoofing, modification of frames, message relay, and some levels of denial of service.

DNP Primer

DNP was created in 1993 by GE-Harris Canada (formerly Westronic, Inc.) to enable multivendor interoperability between SCADA components for the North American electrical power grid. Usage of DNP has spread to adjacent industries using similar kinds of process automation systems. DNP supports the SCADA master station (control center) and remote substations, which consists of remote terminal units and intelligent electronic devices such as programmable logic controllers (PLCs), actuators, meters, and accumulators.

¹See the "Basic 4 Document" at www.dnp.org/About/Default.aspx

ARC Advisory Group reports the worldwide market for SCADA systems for the electric power industry alone is estimated to be \$1.6 billion in the year 2005 and \$1.7 billion throughout 2006. The report also states that SCADA is moving towards knowledge management and is evolving to serve more diverse clients. The worldwide SCADA systems market for the oil and gas, and water and wastewater industries will reach \$780 million by the end of 2005, growing at 3.5% per annum, also according to ARC. European SCADA systems market revenues are expected to reach \$1.16 billion in 2007.

Potential Weaknesses of DNP3

Early SCADA systems for the electric industry were closed to external traffic so security was not a big design consideration for DNP. Newer DNP3 systems carry link layer DNP frames over TCP/IP, which allows utilities to tap the economic and performance benefits of transporting SCADA communications over the Internet. Internet public transport exposes attached devices to attack, thus most of the current work on DNP3 has focused on strengthening its security, currently limited to TLS and SSL encryption. Vulnerabilities resulting from bad implementations of TLS and SSL can expose DNP3 networks to attack.

DNP frames within the TCP payloads can maliciously confuse or disable the target. Mu Security sends mutated DNP3 traffic to SCADA endpoints regardless of the transport stack, be it TCP over IPv4 or over IPv6, with or without TLS.

The clear evolutionary direction is that TCP/IP will eventually be used natively for transporting DNP, and that cryptographic key exchanges will work on an out-of-band network, but deployments of IEC 62351-5 will persist that employ serial and LAN connections. Security improvements are targeted for publication in the first quarter of 2007, but the new measures will not address eavesdropping, traffic analysis or repudiation that uses encryption.

About the Mu-4000 Analyzer

The Mu-4000 analyzer is a security analysis platform that delivers the industry's first systematic and repeatable process to identify unknown and published vulnerabilities in any IP-based system, application or network device without requiring access to source code. The process, known as "mutate, monitor and manage," easily integrates with existing security controls. The Mu-4000 subjects the target under analysis to a virtually unlimited number of attack vectors (the "mutations"). It monitors the target and captures results in a database while managing the process in a reproducible and actionable manner. Results include detailed reports and utilities to speed fault remediation. This lifecycle approach enables the creation of security-enabled processes in all phases of product development and deployment. The extensible security analysis platform also enables organizations to integrate their own suites of attacks. The Mu-4000 analyzer is a self-contained, 2U rack-mountable appliance that is easily configured, operated and managed.

POTENTIAL DNP3 WEAK SPOTS

BENEFITS OF MU-4000

DNP3 is carried over TLS, which has its own set of weaknesses	Rich set of TLS mutations ensure that DNP3 is carried safely over the Internet, either with IPv4 or IPv6 transport
DNP3 was designed assuming a closed network environment so implementations are not expecting to receive improperly formatted frames	DNP3 mutations help SCADA vendors improve the robustness of their DNP3 implementations
SCADA protocols weakness in security exposes SCADA systems vulnerable to manipulation of operational data that could result in serious disruption to public health and safety	Mu Security operationalizes the discovery and expedites the remediation of DNP3 and other key SCADA protocols

Table-1.

OTHER PROTOCOLS SUPPORTED BY THE MU-4000 (partial list)

ARP	PIM-SM
BGP4	POP3
CDP	RADIUS
DHCP	RTSP
DNP	SIP
FTP	SMTP
HTTP	SNMP
ICMP	SNMP Traps
IGMP	SSL-TLS
IMAP	SSDP
IPv4	SSH
IPv6	Sun RPCTCP
ISAKMP	TCP
LDAP	TFTP
MGCP	TLSv1
PIM-DM	UDP

Table-2.



web: www.mudynamics.com | email: info@mudynamics.com
 address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317