ICS-CERT has recently issued a number of advisories that report flaws in the DNP3 interface of various control system devices.

Some Users Group members have asked, "What suddenly went wrong with DNP3?"

The DNP Users Group's Board of Directors and Technical Committee have been monitoring and investigating these reports. Our determination is that all the ICS-CERT advisories issued to date that mention DNP3 have reported issues with implementations (i.e. bugs), not issues with the protocol itself. There has been no change in IEEE Std^{TM} 1815-2012 (DNP3) that has resulted in a lowering of security. If anything, the reverse is the case, with the introduction of DNP3 Secure Authentication adding security functions to a previously unsecured protocol. The emergence of a number of these reports in a fairly short time frame is due to increased focus on the cyber-security of control systems devices through the use of "negative tests" (tests that involve unexpected input).

It is the Board of Director's understanding that the majority of the advisories are coordinated disclosures resulting from investigations performed by independent security researchers. The researchers have followed a procedure of responsible disclosure of the faults to the affected vendors and to ICS-CERT. Subsequently, the individual vendors developed mitigations to resolve the identified faults. The researchers then tested and verified the fixes, which are now available from the specific vendors. In one case that did not follow this sequence, an ICS-CERT advisory was published when it was found that a third party had independently identified and published information about one of the issues.

The DNP Users Group committees are not aware of the specific details of each individual issue, except for the published descriptions. Some members of the DNP Technical Committee have been involved in the testing that has identified the reported issues, but, prior to publication of the advisories and in fairness to all parties involved, no other committee member has been advised of the identity of vendors or devices that have been tested. A subcommittee of non-affiliated Technical Committee members (those not employed by vendor organizations) has reviewed raw DNP3 data traffic captured by the researchers, which demonstrates faults. Again, there was no identification of the devices that had problems with these messages. The purpose of this review was to determine how the messages did and did not comply with the DNP3 specification in order to verify if the faults were due to non-conformance or due to errors in the specification. The conclusion of this review has been that the faults are due to implementation errors, primarily incomplete validation of incoming messages, and are not a result of flaws in the DNP3 specification.

The review has identified some recurring errors (the same or similar fault appearing in more than one device). The Users Group has a responsibility to act in the interests of the DNP3 Community (users, integrators, and vendors) to improve the integrity of systems using DNP3. To assist this, a set of recommendations is being developed that will provide guidance to vendors, integrators, and end users regarding particular conditions that should be verified. These recommendations can be used by vendors to improve their product implementation and testing, and can be used by integrators, end users, and other researchers as guidelines for device evaluation and system validation testing. There will also be recommendations for vendors to provide support for some optional features of DNP3 (e.g. Secure Authentication), as well as recommendations that users include such features when compiling a list of requirements for the purchase of new devices. It is anticipated that these guidelines will be published by the end of 2013 and will be discussed at the DNP Users Group meeting which will be held in conjunction with DistribuTECH in San Antonio in January 2014.

In summary, the DNP Users Group Board of Directors emphasizes that the vulnerabilities reported to date identify issues with software implementation in particular devices and not issues with the DNP3 protocol itself. In addition:

- SCADA protocols were designed for use on trusted networks. On untrusted networks, these protocols must be deployed within a system that uses adequate security measures.
- The current DNP3 specification is IEEE 1815-2012, and is available from the dnp.org Document Library.
- DNP3 is one of the few SCADA protocols that already includes built-in security features.
- DNP3 devices should be certified for interoperability, but these certification tests do not necessarily verify robust behavior in all circumstances.
- No single security feature can defend against all types of attacks. Experts suggest using a defense-in-depth security methodology.

For further information on this topic, please contact directors@dnp.org, or post a question to the dnp.org Discussion Forum.