

Understanding Trust and Security in SCADA systems

*Dr. Clifford Neuman
Information Sciences Institute
University of Southern California
bcn@isi.edu*

Today's SCADA systems are critically dependent on the proper functioning of computing and communications technologies. The management and functional needs of such systems often require connection to public network infrastructure. Even where such systems run isolated from public networks, the growing size of such proprietary networks creates increased opportunity for successful attack. To effectively protect such networks we need to re-architect the security that has been added over the years to these systems. We must go back to the basic principles of least privilege, to understand the roles of all participants in the system, and we must prevent the compromise of less critical components of the system from affecting the critical functions of such networks.

An important step toward improving the security of SCADA systems is to stop thinking of them as monolithic systems. Today we think of these systems monolithically, with privileges assigned to different users, but with rights managed by "the system" which either grants access or not. Instead we need to think of these systems as segregated by function, with the critical functions isolated from the effects of the important but non critical functions.

Both critical and non-critical functions may share physical infrastructure, but the systems and network must, at their lowest levels, provide the separation needed by the critical functions to prevent compromise or denial of service by the less critical functions, or to contain the effect of a compromise of a critical function from spreading to other parts of the system.

The Most Important Challenges

In deploying security for SCADA systems, it is most important to understand the critical functions and consequences of compromise or loss of those functions as contrasted with the loss or compromise of routine functions of the system. The system must be designed to segregate the protection function for critical functions from interference by all other functions, and should seek to contain compromise of even a critical function to as small a region of the system as is possible. Computing, network, and protection mechanisms must be designed to support this segregation, and a management mechanism must be put in place that can support such segregation, without itself becoming a single point of attack or failure.

Important IT research needs

A core research need is to better understand issues of trust in distributed computing systems, and in particular, to develop models of trust that support segregation of dependence for different functional components of a system. These trust models must not be monolithic, or even hierarchical, as different parts of a system must be able to achieve protection and provide availability for themselves, without a central point of failure or vulnerability. These trust models must also be understandable to designers and users of SCADA systems, providing simple abstractions that parallel the physical and organizational dependencies that apply to such systems.

The SNAIR Architecture

At USC's Information Sciences Institute we are investigating such models of trust. We are designing a trusted secure networked architecture based on interlocking rings

(SNAIR). This architecture starts from the premise of traditional ring based architectures like Multics, but extends the concept to recognize that in today's networked environment we no longer have a single "ring zero" trusted by everyone. Instead there exist multiple perspectives on trust. Each protected function has its own "ring zero" and the entities with which it communicates will hold different ring assignments in different "virtual systems".

Within the SNAIR architecture, isolation is provided at a particular level between those components that do not share ring membership in common with functions of other virtual systems, up to the ring of interest.

While initially envisioned to utilize trusted computing architectures to provide mutual protection of end users and content providers from one another (instead of the more common view where the protection is one sided), this architecture is also well suited to visualize, understand, and enforce the protections that are needed in federated SCADA system.

Roadmap for the next 10 years

In the first five years of focus on improvements to SCADA systems several activities can proceed together. We need an analysis of trust and dependence issues in SCADA systems, including an analysis of cross system dependence (e.g. the communications network vs. the power grid).

Simultaneously, work is needed to understand issues of trust and dependence in distributed systems, and to develop architectures that provide strong isolation between different functions that run on common physical (hardware and network) infrastructure.

1. REFERENCES

[1] M. D. Schroeder and Jerome H. Saltzer. *A hardware architecture for implementing protection rings*. Communications of the ACM, 15(3):157-- 170, March 1972.

Finally, work is needed on mechanisms for providing such isolation at the lowest level of the network and in computing systems. These mechanisms must be as simple as possible so that they can be easily analyzed and validated. They should be relatively inflexible so that it is not easy to reconfigure them in a way that eliminates the isolation, though this requirement might need to be balanced to allow some limited reconfiguration that might be useful to recover a system from failure while preventing the compromise of other critical parts of the system that remain operational.

Much of the work just described would continue beyond the initial five years of such an effort, but there would be enough advances by the fifth year that we could start to redeploy critical components of SCADA systems using the new architectures.

Biography

Clifford Neuman is director of the Center for Computer Systems Security at the Information Sciences Institute (ISI) of the University of Southern California (USC), and a faculty member in the Computer Science Department at USC. He earned a Bachelor's degree at the Massachusetts Institute of Technology and subsequently worked for Project Athena. He received M.S. and Ph.D. degrees from the University of Washington. Dr. Neuman conducts research in distributed systems, computer security, and electronic commerce and is the principal designer of Kerberos authentication system, the NetCheque and NetCash systems, and the Prospero Directory Service. Dr. Neuman's current research is focused on trusted computing architectures that support multiple views of trust.

[2] B. Clifford Neuman, *The Virtual System Model: A Scalable Approach to Organizing Large Systems*, Ph.D. Thesis, University of Washington, Department of Computer Science and Engineering Technical Report 92-06-04, June 1992.

[3] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Xen and the Art of Virtualization (2003) .Proceedings of the ACM Symposium on Operating Systems Principles. 2003.