Title

Penetration Tester and System Analyzer for Control Systems

Introduction

With the adaptation of common IT standards like TCP/IP, Windows, wireless, etc. to the domain of process control systems, Supervisory Control And Data Acquisition (SCADA) systems, and control devices, the inherent cyber-security risks also become a threat to the controls domain. Today's control systems usually do not deploy standard security protections (firewalls, anti-virus and intrusion detection systems) as do office IT systems. Therefore, they are an easy target for viruses and worms, but also for hackers and intruders. The lack of security and the actual threat situation has alarmed the controls community, the corresponding manufactures as well as the governments in the US and in Europe, since this situation poses a direct risk, amongst other, to today's oil & gas production, electricity grids and water distributions.
Within the CERN openlab collaboration, CERN's Information Technology (IT) Department and Siemens Automation & Drives (AD) Department are aiming at improving the security of controls devices, i.e. mainly Programmable Logic Controllers (PLCs), but also others.

Tasks

1. Development of an open program suite that employs a novel series of robustness and vulnerability tests and that allows for the security certification of automation devices. The work includes a review of currently existing test procedures as well as a market survey and evaluation of currently available test suites. The development will be conducted in close collaboration with Siemens and several other parties worldwide. This final program suite and the certificate must be accepted by an external review process.
2. Improving Siemens automation devices by developing and deploying hardened and robust firmware versions. After the deployment, the devices must be able to withstand the Robustness & Vulnerability Tester developed in 1. The work includes security assessment and reporting. The development will be in close collaboration with Siemens personnel.

Required qualifications and skills

Required qualification

University or equivalent in computer science or/and automation & controls, or a related field.

Experience and knowledge

Up to 5 year's knowledge and practical experience in information technology, in particular the following areas:

- Equipment control, SCADA systems, Field Buses, and PLC's.
- Computer security, penetration testing, hacking;
- Programming, preferably in C, C++, Perl, Visual Basic;
- In-depth knowledge of the Windows XP operation system.

Flexibility and the capability of learning new tools and techniques rapidly.
Good communication skills and the ability to liaise effectively with third parties are essential, as is the ability to work as part of a team.
Good knowledge of English or French; basic knowledge of the other language or an undertaking to acquire it rapidly.