SPE Digital Security in Oil & Gas

London, December 2005

Those, like ourselves, who thought that security was a 'horizontal,' generic IT issue, were in for a surprise at the Society of Petroleum Engineering's Conference on Digital Security in Oil and Gas. Information sharing across joint ventures, complex data types and a 'nomadic' population make for rather special security requirements. And the field of SCADA[1] and Process Control Systems (PCS) as deployed in productions facilities, pipelines and refineries has its specific security issues, even though these are shared with other industries like manufacturing and utilities.

The extreme sensitivity of many oil and gas installations means that their protection is a national issue. Oil and gas security initiatives roll in government organizations such as the US Department of Homeland Security (DHS), and academic institutions. Oil company presentations included Chevron's work on a pipeline security test with the DHS, BP's approach to SCADA security, Shell on smart cards for access control and Oxy's frank presentation of the harsh reality of a true (near) disaster (Hurricane Rita).

Over the last couple of decades, the process control industry has been caught up in a massive migration to WinTel-based systems. Old timers (especially from the former PCS incumbents) regret the move to COTS, and the increased connectivity, which is considered responsible for many security issues. Both PCS and corporate IT systems are also moving from a 'China Wall' kind of security with an 'impenetrable' exterior and a 'soft inside' to 'security in depth.' The idea is that security at a very detailed level of granularity is what is required for modern systems – especially if they are to connect and share entitled data with other organizations. This 'trend' is known as 'deperimeterization'. Of course many companies are reticent to breach their Chinese Walls. One subtext here is the degree of access that will be afforded to vendors and contractors who may be pushing harder for deperimeterization than some CIOs.

Enterprise security is about firewalls, patches and anti virus software. With deperimeterization, the same issues are appearing on the plant floor. Various techniques that can be used to probe and test the security of a desktop or server may put peoples' lives in danger if applied to a plant. Patching and updating software in a live plant requires a different approach.

We'd like to take this opportunity to thank the SPE for inviting us to this informative conference and in return, offer Technology Watch readers a small plug for what will likely be another worthwhile event – the SPE Intelligent Energy 2006 Conference to be held in Amsterdam next April – more from www.ie2006.com.

Highlights

[1] *Supervisory Control and Data Acquisition – a widely used protocol to control utilities, manufacturing plants and other infrastructure.*

Contents