Abstract

Attack Trees are very important in the effort to secure Industrial Process Control Systems (ICS), because they aid directly in indicating the presence of vulnerabilities in network and how attackers use the vulnerabilities to implement an effective attack. Attack Tree design and analysis provide clues for the network security professionals on how an attacker exploits the vulnerability on the network to achieve goals. In this paper it will be illustrated for designing attack tree in Offshore Oil and Gas Process Complex SCADA System to identify various vulnerabilities. Using the vulnerabilities it presents how an attacker can take control of the SCADA system network and eventually affect hydrocarbons production.

References


**Index Terms**

Computer Science

Security

**Keywords**

ICS, SCADA, MTU, TDMA, RTU