Detecting Cyber Intrusion in SCADA System

by Edvard

Detecting Cyber Intrusion in SCADA System

How to recognize intrusion?

One of the axioms of cyber security is that although it is extremely important ***to try to prevent intrusions*** into one's systems and databases, it is essential that intrusions be detected if they do occur.

Scada intrusion prevention

An intruder who gains control of a substation computer can modify the computer code or insert a new program. The new software can be programmed to quietly gather data (*possibly including the log-on passwords of legitimate users*) and send the data to the intruder at a later time.

It can be programmed to operate power system devices at some future time or upon the recognition of a future event. It can set up a ***mechanism*** (*sometimes called a "backdoor"*) that will allow the intruder ***to easily gain access at a future time***.

If ***no obvious damage*** was done at the time of the intrusion, it can be very difficult to detect that the software has been modified.

For example, if the goal of the intrusion was to gain unauthorized access to utility data, the fact that another party is reading confidential data may never be noticed. Even when the ***intrusion does result in damage*** (*e.g., intentionally opening a circuit breaker on a critical circuit*), it may not be at all obvious that the false operation was due to a security breach rather than some other failure (*e.g., a voltage transient, a relay failure, or a software bug*).

For these reasons, it is important to strive to detect intrusions ***when they occur***. To this end, a number of IT security system manufacturers have developed intrusion detection systems (IDS).

These systems are designed to recognize intrusions based on a variety of factors, including primarily:

1. Communications attempted from unauthorized or unusual addresses and
2. An unusual pattern of activity.

They generate ***logs of suspicious events***. The owners of the systems then have to inspect the logs manually and determine which represent true intrusions and which are false alarms.

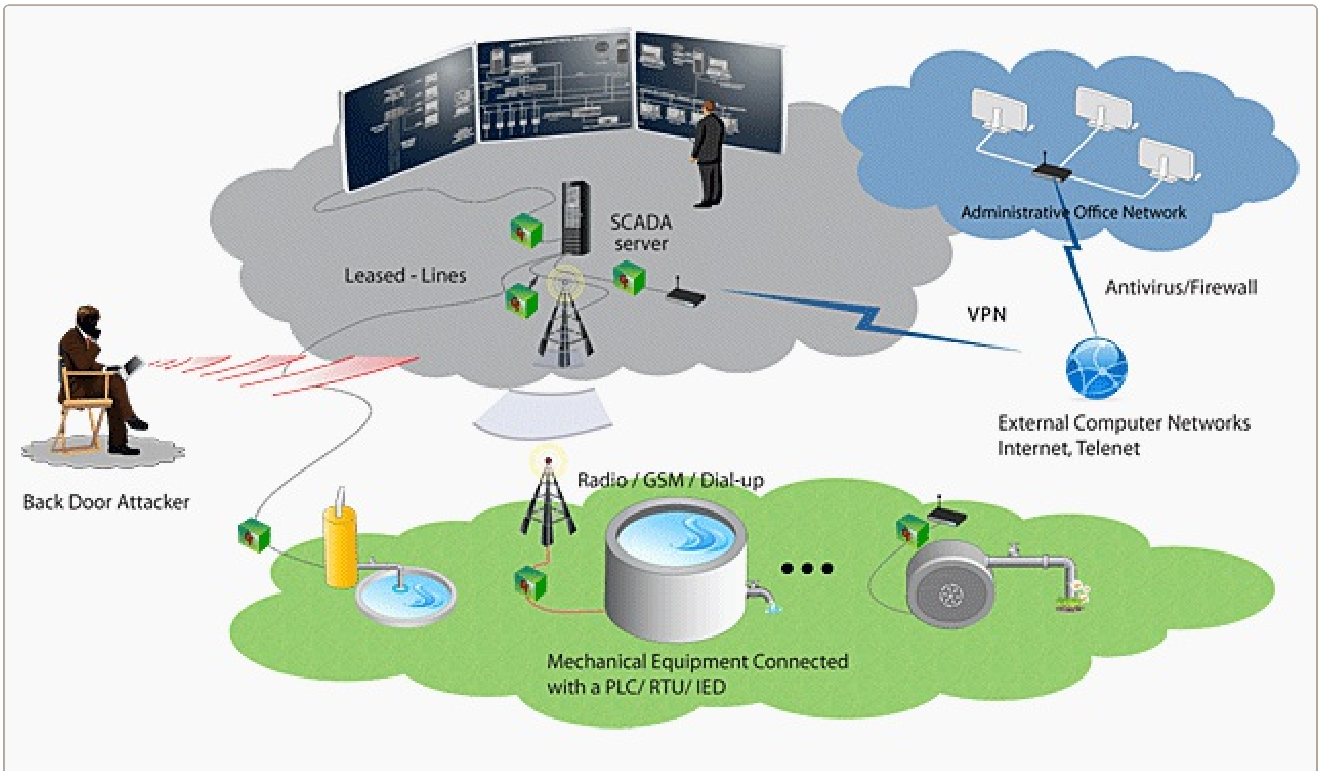

Photo by Cryptango - securing industrial communications

Unfortunately, ***there is no easy definition*** of what kinds of activity should be classified as unusual and investigated further.

To make the situation more difficult, hackers have learned to ***disguise their network probes*** so they do not arouse suspicion.

In addition, it should be recognized that there is as much a danger of having too many events flagged as suspicious as having too few.

Users will soon learn to ignore the output of an IDS that announces too many spurious events.

(There are outside organizations however that offer the service of studying the output of IDSs and reporting the results to the owner. They will also help the system owner to tune the parameters of the IDS and to incorporate stronger protective features in the network to be safeguarded.)

Making matters more difficult, most IDSs have been developed for ***corporate networks with publicly accessible internet services***. More research is necessary to investigate what would constitute unusual activity in a SCADA=SA environment.

In general, SA and other control systems do not have logging functions to identify who is attempting to obtain access to these systems. Efforts are underway in the commercial arena and with the National Laboratories to develop intrusion detection capabilities for control systems.

Summary

In summary, ***the art of detecting intrusions*** into substation control and diagnostic systems is still in its infancy. Until dependable automatic tools are developed, system owners will have to place their major efforts in two areas:

1. ***Preventing intrusions*** from occurring, and
2. ***Recovering*** from them when they occur.

Resource: *Electric Power Substations Engineering – J. D. McDonald (Get it from Amazon)*

Source:
http://electrical-engineering-portal.com/detecting-cyber-intrusion-in-scada-system