Turbine Monitoring and Diagnostic Threats and Solutions

Lior Frenkel
CEO and Co-Founder
Waterfall Security Solutions

April, 2014

Introduction

A variety of turbines are used routinely in power generation: steam turbines, water turbines and combustion/gas turbines. Wind turbines are used as well, but tend to be smaller. Regular monitoring, preemptive maintenance and comparatively small adjustments can often prevent otherwise costly, catastrophic failures which might even require the replacement of entire turbines. Many vendors provide remote services for turbine monitoring and diagnostics. These services are generally accomplished through remote access using firewalls, often with Virtual Private Network (VPN) and other security measures.

Persistent, Targeted Attacks

In the last half decade, targeted attacks have emerged as a new pervasive threat. A targeted attack is an attack where a team of one or more professional-grade attackers assaults a specific site or organization on more or less a full time basis over a period of days, weeks, or months, using continuous, interactive remote control tools. Targeted attacks routinely defeat classic IT-style cyber protections, including anti-virus systems, security update programs, encryption, and firewalls. This class of attack was once attributed only to so-called "advanced persistent threats." In recent years though, the attack techniques used in targeted attacks have been thoroughly documented. Training in these techniques is now part of most intermediate or advanced security training programs and is easily accessible. These very effective attack techniques are now widely understood and routinely practiced.

Attacks via Remote Turbine Service Centers

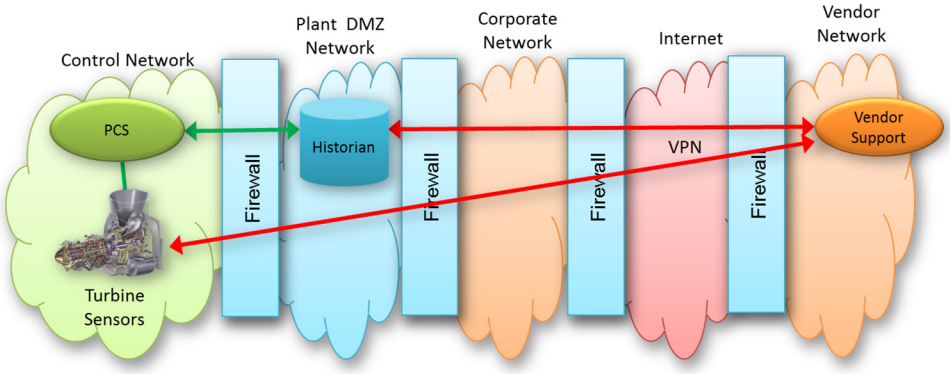
There is an emerging realization that central turbine monitoring and diagnostics sites are extremely attractive targets for persistent attacks, and that such attacks can have devastating consequences.

These central sites maintain continuous connectivity with hundreds or thousands of similar turbine control systems, world-wide. The compromise of any one of these sites rewards an attacker with on-line connections to hundreds or thousands of generation sites. From this vantage point, the attacker can engage in a 'fleet-wide' attack on all connected sites, either indiscriminately, or by selecting sites for specific customers, or geographies. This attack can even be tailored specifically to the control systems common to the targeted sites.

With an infrastructure of back doors established by the attacker during the 'attack preparation period', an attacker is in a position to disable, damage or destroy all of the turbines and sites connected to the monitoring and diagnostic center, on a moment's notice.

Unidirectional Security Gateways

Generation sites are turning to Waterfall's Unidirectional Security Gateways to address the failures



Conventional Turbine Monitoring and Diagnostics

of firewalls. Waterfall's Gateway hardware permits data to flow out of control system networks without permitting any communication at all, or any attack back into those protected networks. The Unidirectional Gateway software produces real-time replicas of control system servers for the central monitoring sites, available to the turbine vendor systems and personnel. Together, Unidirectional Gateway hardware provides absolute protection from attacks from central monitoring sites, and Unidirectional Gateway software makes the gateway products plug-and-play replacements for firewalls.

When occasional remote adjustment of turbine vibration parameters, heat distribution parameters or other parameters is needed, unidirectionally-protected sites turn to Waterfall's Remote Screen View product. Remote Screen View send real-time screen images through the Unidirectional Gateways. The screen viewing product allows vendor personnel to how turbines are being adjusted, and to provide turbine site personnel with advice, without ever introducing the risks of interactive remote control. No action on the part of vendor personnel or possibly-compromised vendor equipment can penetrate the Unidirectional Security Gateways to influence or compromise turbine control systems.

Unidirectionally-protected sites have other remote adjustment alternatives as well, ranging from temporary manual overrides of the unidirectional gateways, to on-site support.

Waterfall FLIP™ – A Reversible Gateway

Advanced turbine monitoring vendors are incorporating the Waterfall FLIP™ into their monitoring and diagnostic systems designs. The FLIP is a single Unidirectional Security Gateway which can be configured to reverse direction from time to time. With the FLIP, turbine management tools can create batch-mode instructions at the central monitoring site, and the FLIP can push those instructions automatically into the control system site, without ever introducing the risks of interactive remote control.

The Bottom Line

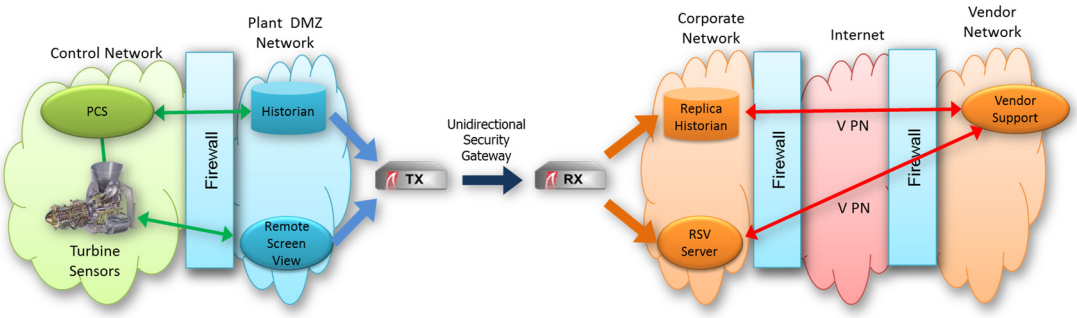
Diligent monitoring and timely adjustment of large turbines are essential to maximizing operational efficiency and the effective life of this equipment. Turbine vendors are uniquely positioned to provide these required services, and the most costs-effective access to vendors' expert personnel is often by remote services. Conventional firewall-based remote connections are vulnerable to a variety of cyber-attacks, and especially to targeted attacks. Firewalls do not provide sufficient security for this sensitive application.

Waterfall's Unidirectional Gateways provide absolute protection from attacks originating on external networks. Turbine vendors can monitor and adjust equipment at customers' sites, via Unidirectional Gateways without introducing any risk of compromise of protected networks. Advanced turbine vendors are incorporating the Waterfall FLIP into their designs, to enable secure batch-mode remote adjustment of turbines, without manual intervention from site personnel.

For More information

Please contact Waterfall directly for additional information on any topic related to Waterfall products.

Waterfall Security Solutions
1133 Broadway, Suite 708
New York, NY 10010
+1 212-714-6058
info@waterfall-security.com



Remote Monitoring with Unidirectional Gateways