Securing the Industrial Internet of Things

A Machfu Security Solution

Tim Winter & John Geiger, Machfu

MACHFU

Current Landscape for Industrial Cybersecurity

> **In October 2017, the U.S. Department of Homeland Security and the Federal Bureau of Investigation issued a rare warning that sophisticated hackers were targeting energy and industrial firms.**

Some of the attacks against nuclear, energy, aviation, water, and critical manufacturing industries had successfully obtained credentials for accessing the computer networks of their targets.

Cyberattacks have primarily targeted companies with large customer databases or high volumes of online transactions, but a recent Kaspersky Labs report found that manufacturing companies now account for a third of all attacks. The implications of cyberattacks on industrial infrastructure are wide-ranging and costly. For example, a Lloyds study conducted with Cambridge University estimated that an attack on the U.S. power grid could cost more than $1 trillion in an extreme scenario.

Industrial infrastructure in every sector is at risk from common cyberattacks, including:

- **Disgruntled Insider Attacks**, where someone with access to passwords and other sensitive information can negatively impact operations;
- **Ransomware and Malware Attacks**, where malicious software is accidentally downloaded to a workstation and spreads to the rest of the network; and,
- **Spear Phishing Attacks**, where attackers send highly customized emails to a few recipients to compromise a network.

Protecting Industrial Assets with Baked-in Mechanisms

Machfu's platform is a solution that helps secure industrial assets with baked-in mechanisms that can be customized as needed.

- **Multi-zone firewall** that can be precisely configured to allow the smallest set of data flows to meet functional requirements;
- **Secure bidirectional communication** between remote SCADA backend and grid devices via a private virtual network;
- **Non-VPN approac**h using public static IP addressing on cellular interfaces coupled with the configuration of various NAT firewall rules;
- **Secure switch/router functionality** to extend network access to only certain legacy devices;
- **Physical ports enable/disable** by configuration;

- **Device-specific protocol stacks** allow contextual awareness even in pass-through modes of operation;
- **Network security model** that can be applied differently for every application;
- **Role-based access controls**; and,
- **Managed software** – policy controlled signed/countersigned.

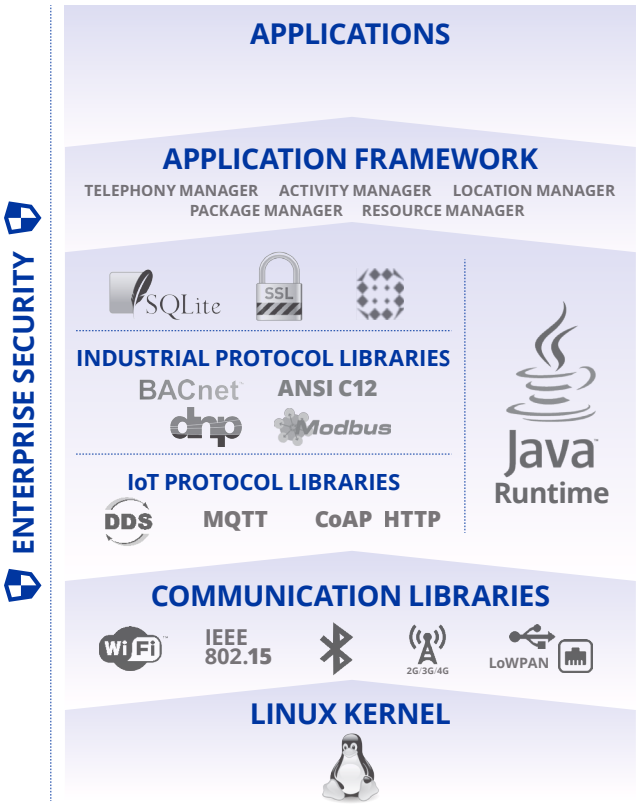

Figure 1: Machfu's platform has defense-in-depth security implementation across all the layers of the OSI stack.

Future of Industrial Cybersecurity

Inevitably, new security threats will continue to emerge that put industrial devices at risk. By connecting industrial devices to a Machfu gateway, companies have access to the latest applications that are designed to protect against new threats and manage cybersecurity risks.

Authors:

Tim Winter

Chief Technology Officer

Tim Winter is the CTO of Machfu and the architect of the Machfu device platform. He has over 20 years of experience in the IoT & M2M space developing strategy and architecture to realize wireless networking platforms. He has expertise in IP networking, protocol stacks, embedded Linux and Android. As network architect at Eka Systems he guided the development teams in an Agile environment. In a consulting role at Captiva he led the implementation of end-to-end embedded communication systems for GE, AT&T and Mueller Water using cellular and private wireless technologies. Tim was the editor at the IETF standards body for the RPL routing protocol and for IPv6 networking for large-scale Smart Grid and other device networks. Tim has a Bachelors degree in Computer Engineering from the Pennsylvania State University.

John Geiger

VP of Business Development, Machfu

John has 20 years of experience and subject-matter expertise in developing innovative solutions for Utility, Oil & Gas, Water/Waste Water, Traffic, Rail, Heavy Industrial and Commercial markets. He is credited multiple patents associated with the application of communication technologies in the industrial scape and actively participates in the SGIP and IEEE802. Previous positions include Wireless Center of Excellence Leader for GE Digital Energy and VP of Engineering for MDS.

MACHFU

Germantown Innovation Center
20271 Goldenrod Lane, Suite 2004
Germantown, MD 20876

301-540-5372
info@machfu.com
www.machfu.com