Deployment of Kaspersky's Industrial CyberSecurity (KICS) Solution, Leveraging on iTrust's Test Bed

Kaspersky Lab today announced the deployment of Kaspersky's Industrial CyberSecurity (KICS) solutions at the Singapore University of Technology and Design's (SUTD) Centre for Research in Cyber Security, iTrust's Secure Water Treatment (SWaT) test bed. The solutions deployed aim to support Kaspersky engineers to detect and deter cyber attacks in real world and real time environments.

SWaT, Singapore's first water treatment test bed for cyber security research is a collaborative project headed by researchers from SUTD, international consultants, and stakeholders. It is managed by iTrust, and aims to provide a real world environment for developing advanced tools and methodologies to ensure the security and safety of current and future large scale infrastructure against cyber attacks in Singapore.

The test bed is a unique and sophisticated facility that mimics the functions of a water treatment system in a live setting. The test bed allows multi-disciplinary researchers to conduct live simulations and testing that will enhance their understanding of the strengths and weaknesses of new and existing defence mechanisms intended for the cyber security industry. SWaT will serve as a valuable platform for researchers in Singapore and globally, who are planning to design secure Cyber Physical Systems (CPS) for water treatment, power generation and distribution as well as oil and natural gas refinement.

Industrial control systems have been known to be a target of malicious and sophisticated cyber attacks worldwide. One such attack was the Ukrainian power grid attack in 2015 that left hundreds of thousands of residents in the Ivano-Frankivisk region in the dark. Another example was the anonymous regional U.S. water utility hack, where cyber criminals managed to gain access to the valve and flow control systems and manipulated the settings, handicapping water treatment and production capabilities.

It is evident that the repercussions of such attacks can be devastating, not only in financial losses but affecting citizens' lives as well. According to the Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT), every third industrial control systems (ICS) computers worldwide has been targeted by cyber threats in the first half of 2017 .

Protection of industrial systems requires a different approach and technologies – a security that keeps availability of process on top of all. Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMIs, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and consistency of the industrial process.

Engineers from Kaspersky Lab will be able to conduct a variety of realistic offensive and defensive experiments on the test bed with KICS. The experiments are aimed at verifying whether what is learnt in simulation applies to the physical testbed. Also, it aims to help engineers to understand the

security gaps that a CPS has, enabling them to build effective designs in a real world setting.

Stephan Neumeier, Managing Director, Asia Pacific at Kaspersky Lab said, “Cyber threats to industrial environments are fundamentally different to traditional ‘office’ threats in terms of the scale of their potential damage, they can be disastrous. We want to play an active role in helping mitigate cyber attacks in this sector and ultimately help build a more secure infrastructure.”

“We are glad to have industry stakeholders such as Kaspersky Lab. We hope to improve our understanding of cyber threats to CPS and to develop and experiment with strategies to mitigate such threats,” said Ivan Lee, Deputy Director of iTrust, SUTD.

For more information about the demonstration of the KICS solution, please visit (https://ics.kaspersky.com/).