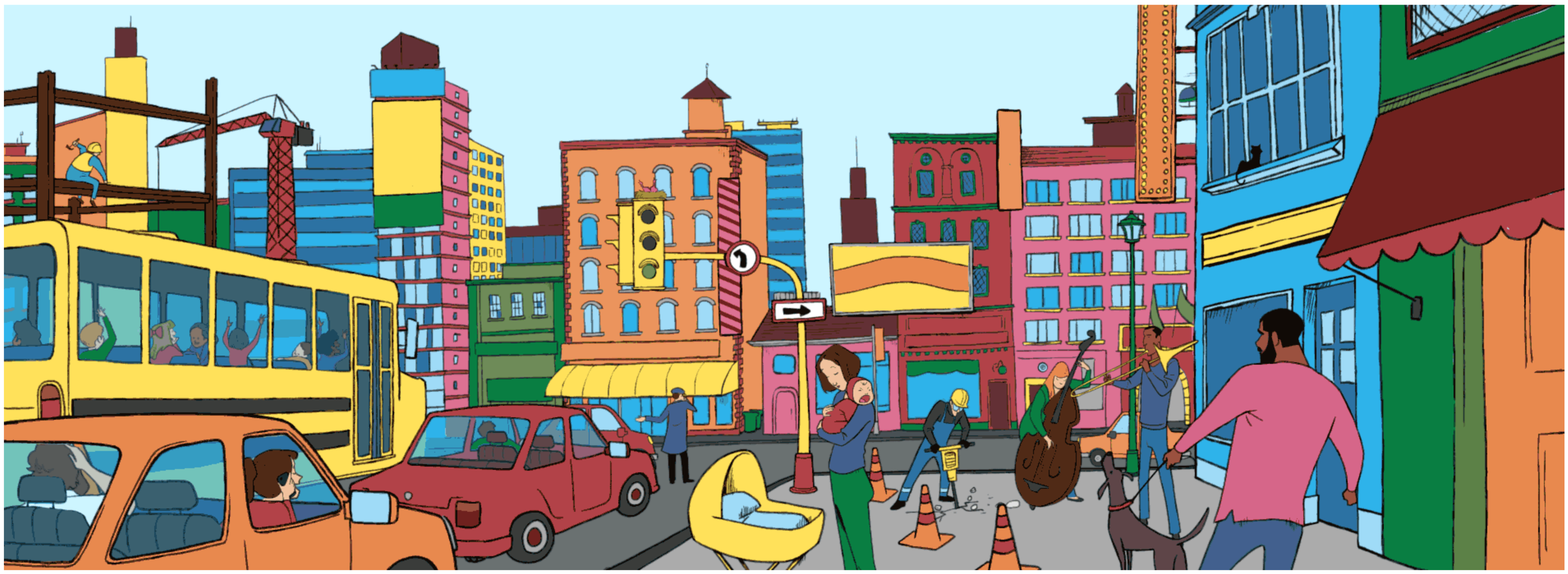
Knock knock! “Who’s there?”

Enabling organizations to better protect their control systems by gaining deeper insights into their network traffic.



Background

The increasing number of IoT devices in Industrial Control Systems (ICS) provides greater risk to Critical Infrastructure. Kaspersky estimates that one industrial computer in five (20.1%) is attacked by malware every month.

Since 2001, FireEye’s iSIGHT Intelligence has identified nearly 1600 publicly disclosed ICS vulnerabilities to help organizations protect their networks. As cyber-criminals enhance their capabilities, cyber-security professionals need to improve their threat detection.

What is Industrial Control Systems?

Industrial Control Systems (ICS) allow operators to monitor and control complex industrial processes, such as those found in oil, gas, and nuclear power transmission and distribution, manufacturing, hospitals, and other Critical Infrastructures. Interruption of these services can have severe consequences.

Organizations incorporating emerging technologies such as ubiquitous computing, cloud, and internet-connected devices, enlarge the attack surface of their network with every device.

Improving FireEye’s existing service capabilities

Scrape data from publicly available sources

Aggregate statistics and metrics to programmatically automate confidence level

Redesign and simplify the report for FireEye’s clients

Using improved capabilities, companies can have increased visibility into their ICS environment, helping them make the decisions necessary to keep their infrastructure secure.

by Gosuddin Siddiqi, Justin Petelka, & Siddharth Naik

FireEye™

Information School
UNIVERSITY of WASHINGTON