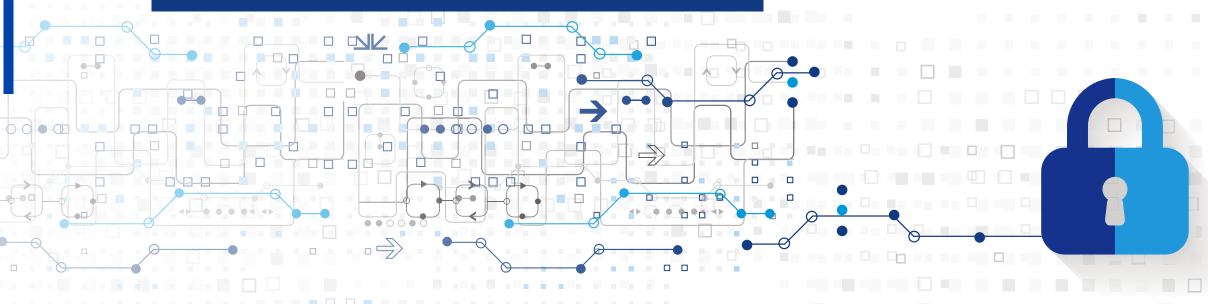
The Software Alliance
BSA

ENCRYPTION BACKGROUNDER



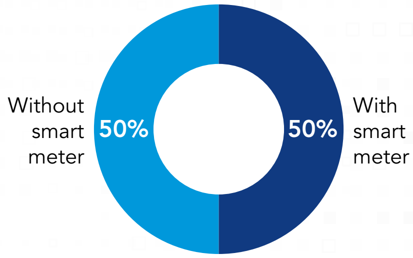
Critical Infrastructure Cybersecurity Depends on Strong Encryption

Increasingly, critical infrastructure relies on internet-connected industrial control systems and internet-enabled distributed operations. Industrial control systems, such as Supervisory Control and Data Acquisition (SCADA), which control and automate core industrial processes, are central to the operation of infrastructure in electricity, transportation, oil and gas, water, manufacturing, and other critical infrastructure sectors. These systems and other technologies communicate constantly with sensors, actuators, meters, and enterprise devices through communications channels that, if compromised, can lead to catastrophic disruptions to essential services.

Encryption is critical to the security of industrial control systems and the communications channels through which they send and receive sensitive data to keep critical infrastructure functioning. It protects the integrity of data in transit, enables secure installation of security updates, and enables secure authentication to defend against compromise by malicious actors. For example, encryption is used to protect data in transit across the electricity grid, including communications to and from operations centers, power generation systems, distribution stations, and home "smart grid" networks.

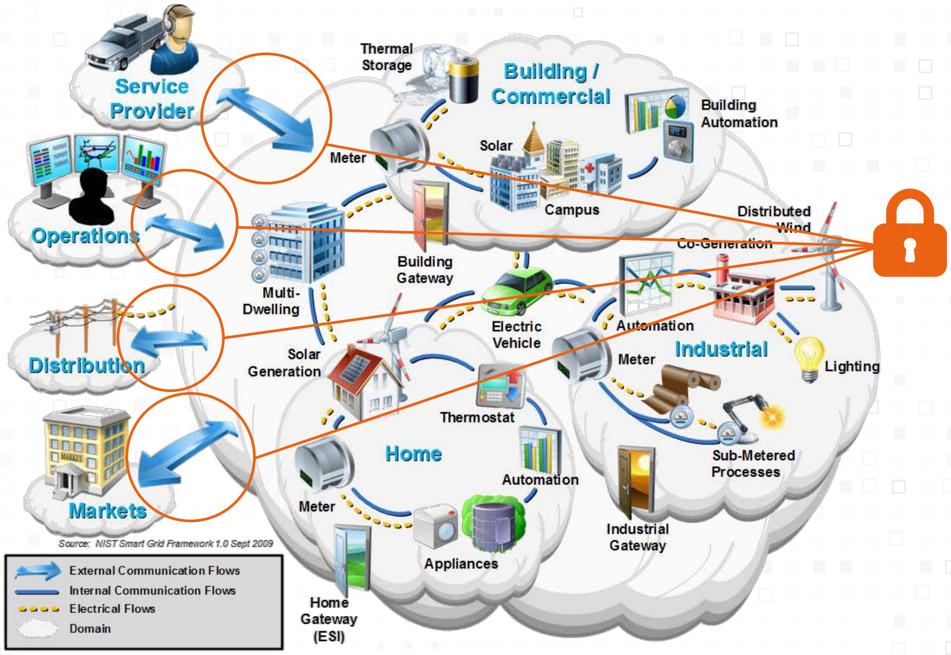
Critical infrastructure is under attack like never before. In March 2018, the Department of Homeland Security warned that a nation-state actor had "targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors" for sophisticated cyber attacks.[1] The potential disruption of such attacks has already been demonstrated when, on two separate occasions, hackers shut off power for hundreds of thousands of citizens in Ukraine.[2] In the face of such threats, strong encryption is a critical element of strong security.

Percentage of Homes With Smart Meters



Source: "1 in 2 American Homes Rely on Smart Meters," *Popular Science* (January 18, 2018), available at https://www.popsci.com/hackers-are-attacking-electric-grid#page-4.

Secure, Encrypted Communications Are Critical to Smart Grid Cybersecurity



Adapted from NIST Framework and Roadmap for Smart Grid Interoperability Standards (September 2014), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf.

[1] Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (March 16, 2018), available at https://www.us-cert.gov/ncas/alerts/TA18-074A.

[2] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (June 20, 2017), available at https://www.wired.com/story/russian-hackers-attack-ukraine/.