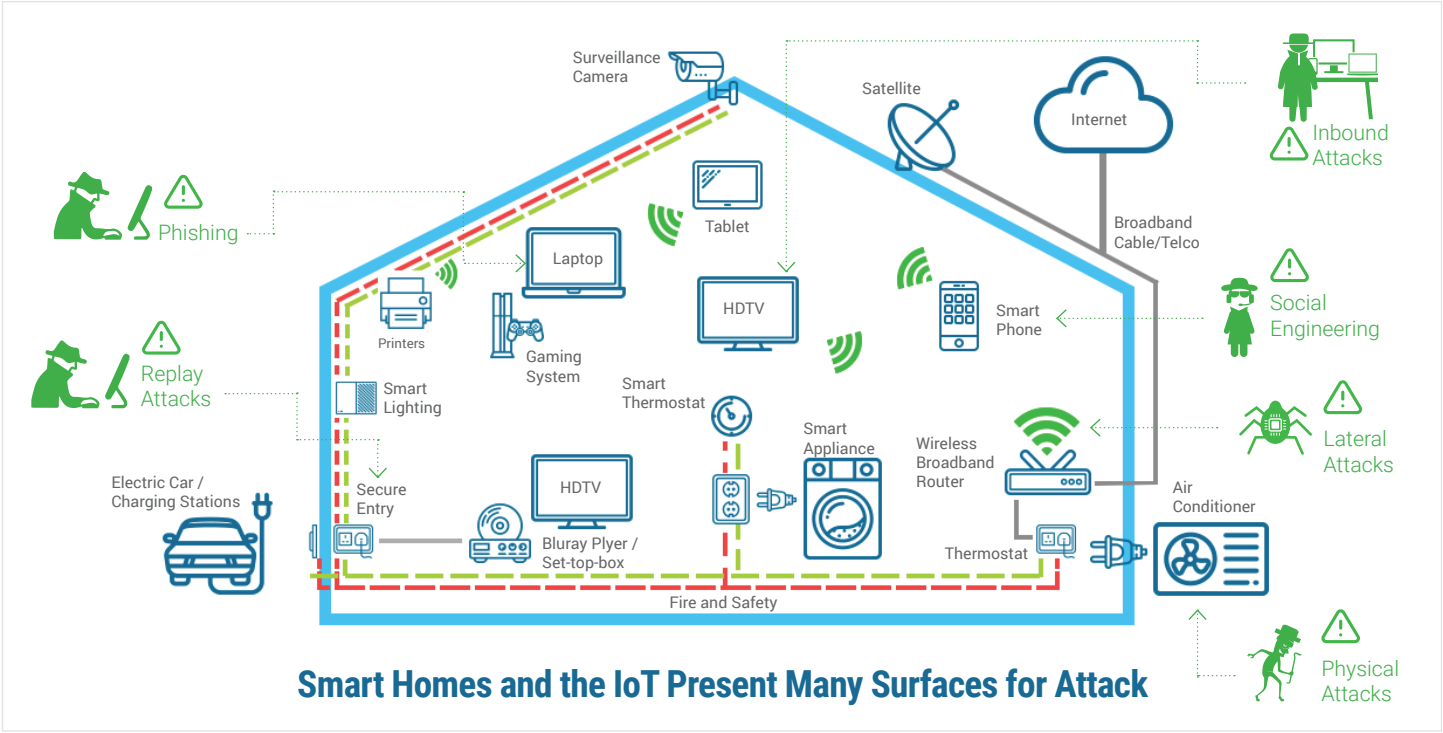
Industry Brief: Smart Home and Connected Internet of Things (IoT) Devices

MOCANA



Smart Homes and the IoT Present Many Surfaces for Attack

Ensuring Safety, Reliability and Compliance

Home networking and threat detection technologies are not enough to defend the connected home against modern cyber attacks. Many surveillance cameras, entry and safety systems, thermostats, home appliances, multi-function printers, smart lighting, and Internet of Things (IoT) devices are vulnerable due to a lack of strong cryptographic controls, including: multi-factor authentication, secure boot, secure update, and secure, encrypted communications.

Smart home technology manufacturers and IoT device companies must ensure compliance with cybersecurity standards such as NIST 800-53, Revision 4, IEC 62443-3-3, and FIPS 140-2. Keeping up with these standards as well as emerging standards from the Industrial Internet Consortium (IIC) and Industrie 4.0 can be challenging. New regulations such as GDPR in Europe raise the stakes for non-compliance to more than €20 million per incident.

Ensuring data privacy in homes with connected devices that are vulnerable to physical compromise is critical. Compromised IoT devices could be used to launch lateral attacks onto home computers to steal private data or deploy Ransomware. Additionally, home computers that have been hit by a phishing email or Ransomware may unleash malware that takes over home appliances, surveillance cameras or fire and entryway systems.

Mocana's Proven Cybersecurity Solution

Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications by giving manufacturers and OEMs an easy way to:

- Harden surveillance cameras, lighting, safety systems, thermostats, printers, gateways, and home appliances with multi-factor authentication using X.509 certificates and trust chaining
- Secure the boot process to validate the firmware, OS and applications
- Enable secure, cryptographically-signed over-the-air (OTA) and over-the-web (OTW) firmware updates
- Integrate hardware or software-based roots of trust such as TPM, SGX, TrustZone, HSMs, SIMs, and MIMs
- Replace open source crypto software such as OpenSSL.

For more information on Mocana's comprehensive IoT Security Platform and how it can help you secure your critical infrastructure, visit our website at mocana.com or send us an email via sales@mocana.com.

A: 20 California Street, 4th floor San Francisco, CA 94111 W: www.mocana.com T: 415-617-0055