SECURANCE CONSULTING

the advantage of insight

www.securanceconsulting.com

THE FUTURE of IOT SECURITY

The Future of IoT Security

The Internet of Things (IoT) is a vast network of interconnected devices. Its mission: to make life more convenient for individuals and businesses alike. To date, there are 35.82 billion IoT devices worldwide, with projections for 75.44 billion by 2025.[1]

Many industries, such as food production, healthcare, finance, manufacturing, and energy, benefit from IoT devices. However, as these devices become more prevalent, their attack surface increases, and it becomes exponentially more important for government, manufacturers, enterprises, and users to focus on their security.

IoT Security Risks

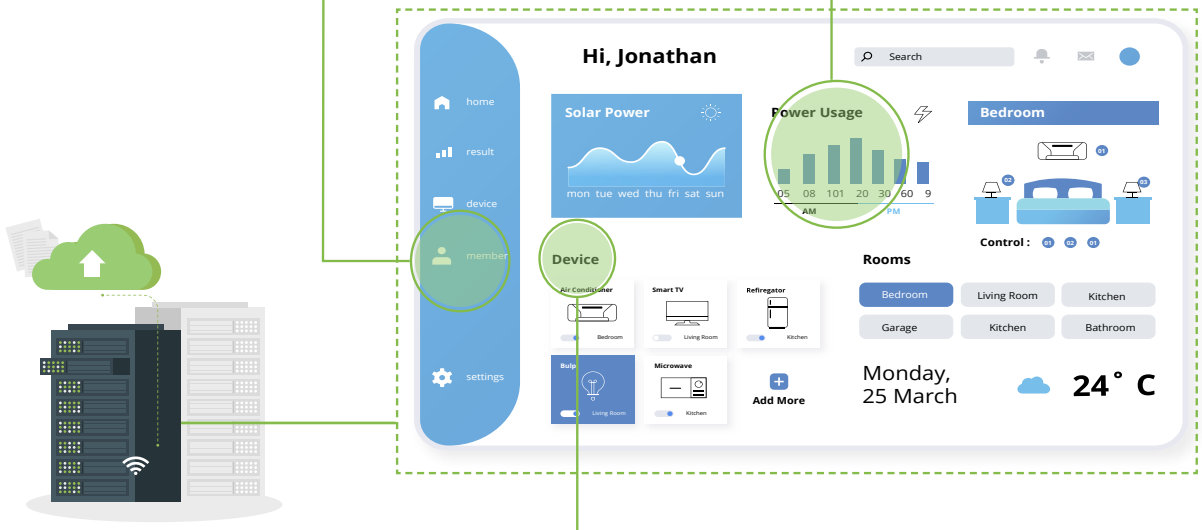
IoT devices have certain characteristics that can lead to security risks. These underlying vulnerabilities lead to not only the device becoming compromised, but potentially any device or system connected to it. These characteristics include:

A bridge between physical and virtual

Connected devices can allow digital exploitation to manifest as physical threats. Without separation between virtual and physical networks, cyber attacks can have larger impacts to people, infrastructure, and operations.

Data collection

IoT devices can collect and store highly detailed environmental and user data that is not necessarily integral to their functionality. Because of this, an unsecured device can freely offer data to any enterprising criminal.



Centralized architecture

A multitude of connected devices amassing data in one place, such as a station or database, creates a wider attack surface to gain access to the single point at which all data is collected.

Complex environment creation

The more connected devices, the wider the attack surface. While users might enjoy the novelty and convenience of diverse and widely available devices, cyber criminals will enjoy more the multiple opportunities for exploitation.

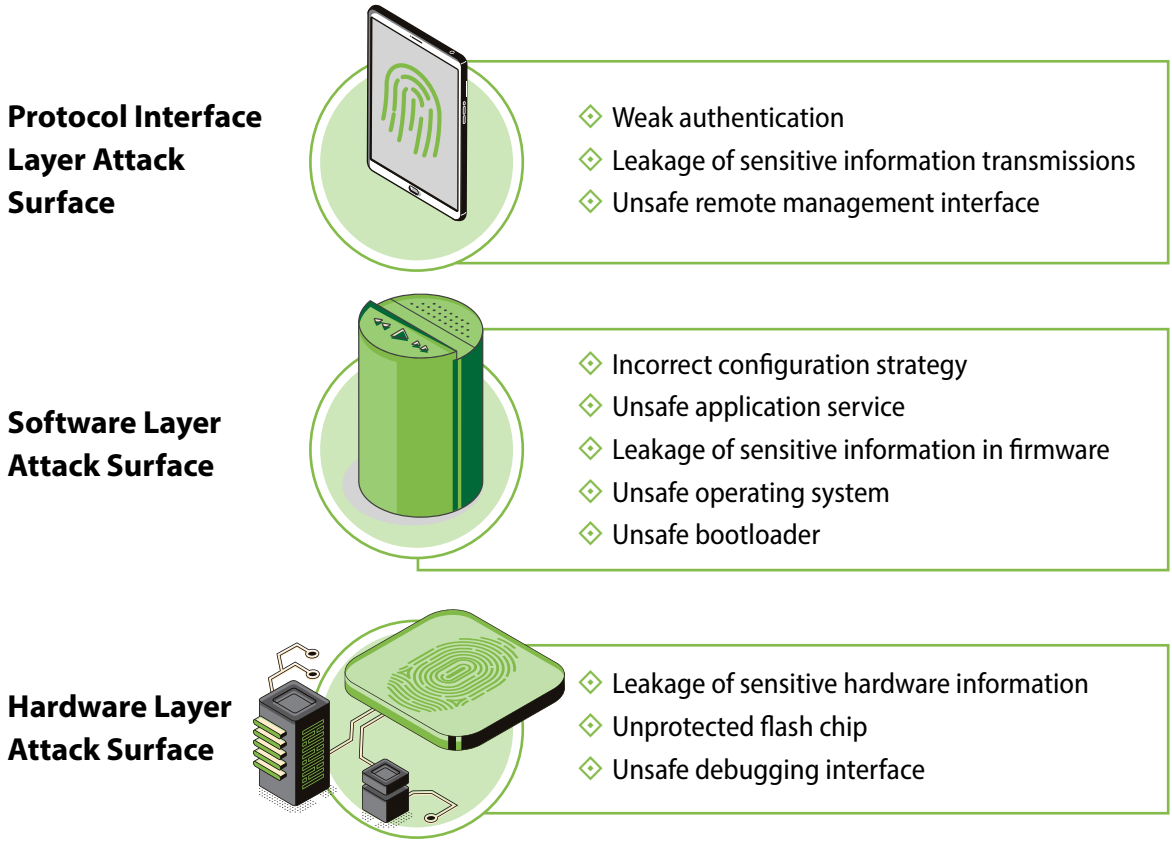
> The industrial sector, including manufacturing, retail, and agriculture, will account for **70%** of all IoT connections by 2024.[3]

The IoT Attack Surface

An attack surface is the total security risk exposure that these connected devices create. In isolation, IoT devices are relatively secure (at least in terms of an attack having far-reaching consequences). But when connected in a larger ecosystem, they can form an exploitable chain that leads into other systems or networks that would otherwise be able to block cyber attacks.

The below graphic depicts vulnerabilities within an IoT device. If an attacker gains access to a device, they could access data stored locally. However, if the device is segmented from the non-IoT network, the damage will end at the device— permitting the data accessed doesn't contain credentials for other systems, devices, or networks.

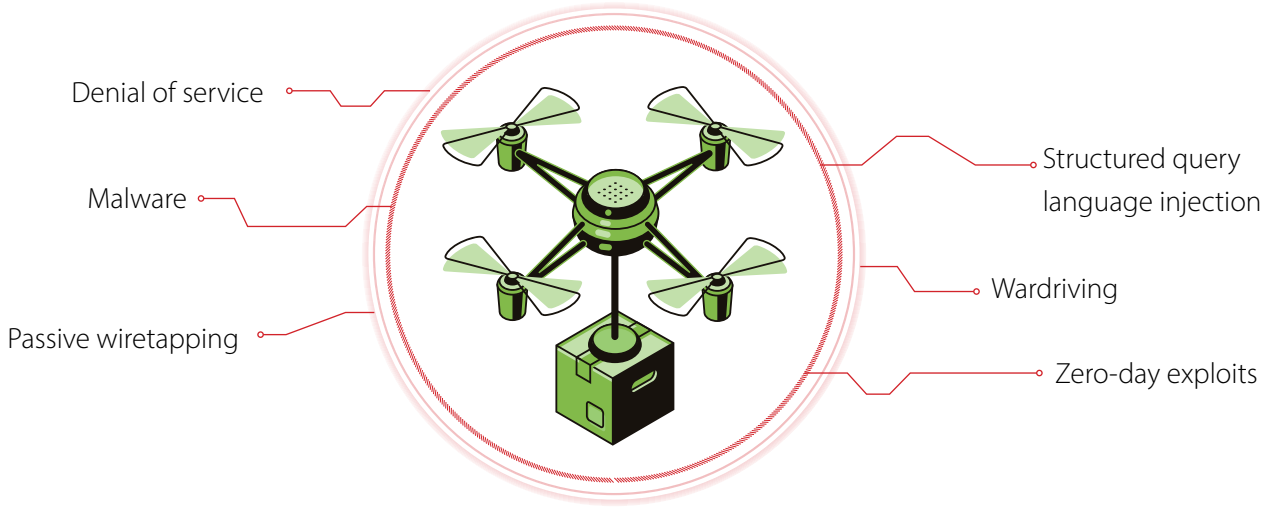
Attack Surface of an IoT Device



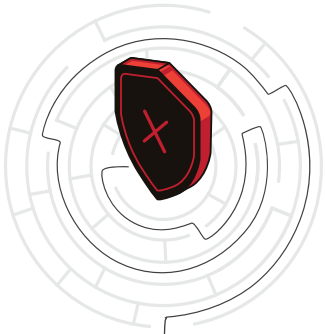
Yu, Miao, et al. "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices." (2020)[4]

If an unsecured IoT device exists within a traditional centralized architecture, hackers can exploit the device to gain access to any other unsecured devices or the main database to which all connections feed their collected data.

According to the U.S. General Accounting Office, the following attacks are the primary threats to IoT:



Challenges and Solutions



Weak password protection

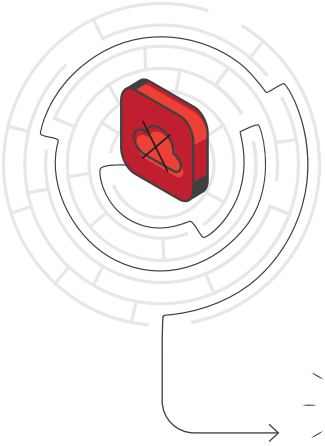
Many IoT devices come with hard-coded default passwords, which are easy for cyber criminals to hack. Manufacturers and consumers learned this the hard way after the Mirai attack in 2016 that compromised over 400,000 devices using just 61 common default usernames and passwords.

One would think this practice of hard-coding weak credentials would have been rectified by now; however, in January 2020, ZDNet reported that a hacker had published a list of Telnet credentials for more than 500,000 servers, routers, and IoT devices on the dark web— all gained by using factory-preset usernames and passwords.[5]

Until manufacturers ensure devices are secure out of the box, large-scale IoT attacks will continue to take consumers and businesses by surprise.

Secure out of the box

IoT devices' native programming should allow for the creation of complex passwords, password expiration, and account lock-out. When appropriate authentication measures (i.e., IoT identity and access management solutions) are in place, device exposure— and the chance of compromise— greatly diminishes.

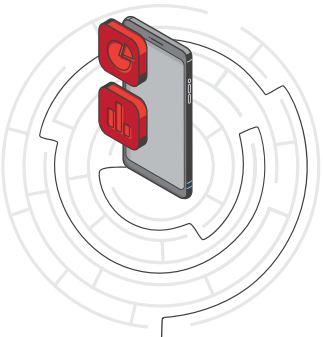


Lack of regular patches and updates

Even if the device is secure out of the box, it doesn't mean new vulnerabilities and bugs won't be found by hackers later. Without routine patches and security updates, existing IoT devices can grow into larger problems over time.

Patch, Update, Secure

Manufacturers should secure the embedded software or firmware in their devices and release regular security updates and patches as vulnerabilities are discovered. They should also be able to guarantee that only authenticated sources are able to push these updates and patches. Otherwise, an attacker would be allowed to run malicious code on a device.



Insecure interfaces

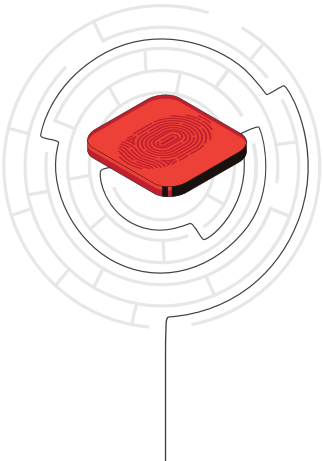
IoT devices handle and communicate data by design. All devices need apps, services, and protocols to communicate, which means all those components' interfaces must be secured. For the most part, issues arise in this area due to insufficient device authentication and authorization.

Authentication and authorization

Authentication and authorization are fundamental to good security. They allow organizations to ensure only certified users and devices are allowed to access certain data and applications. Authorization methods include:

- One-way
- Two-way
- Three-way
- Distributed
- Centralized

Digital certificates are also used to verify digital entities and securely transfer data to authorized parties. For example, X509 certificates are standard certificate formats typically signed by a trusted certificate authority.

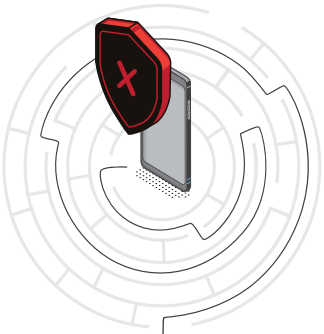


Insufficient data protection

A top concern for IoT devices is insecure communications and data storage. Because IoT devices handle significant amounts of data, data protection is critical. The higher the data visibility, the more likely the theft.

Secure data storage and network segregation

Separating IoT devices from the main network can help reduce the risk of cyber criminals moving laterally and escalating privileges in an organization's network. Data encryption is also effective because it prevents data visibility in the event of theft. It also protects against eavesdropping attacks.

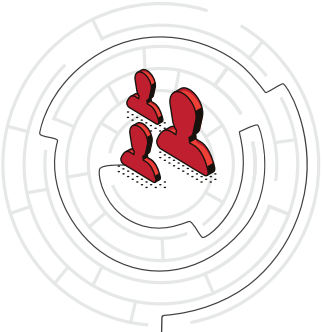


Poor IoT device management

According to a 2020 study, 51 percent of IT teams are unaware of what types of devices touch their networks. Unfortunately, the other 49 percent isn't in a better place. Instead of gaining more visibility into their devices, they tend to guess what's there or use a solution that isn't fit to their needs. This can create additional security issues on top of the challenge of shadow IoT (devices in use without the knowledge of the IT team).[6]

Device management

Gaining visibility into IoT devices on a network helps organizations appropriately tailor their cybersecurity measures. IoT device management platforms help manage devices across their entire lifecycle, including deploying, monitoring, maintaining, and updating IoT devices. They can also aid asset provisioning, security patches, alerts, firmware upgrades, and metric reporting.



Skills gap

Cybersecurity has been facing a general IT skills gap for the past decade, and IoT management suffered for it. Without trained experts, companies who invest in IoT devices will not achieve the full advantages and opportunities of them.

Training

To combat the skills shortage, organizations must take it upon themselves to train employees in effective IoT management. Providing workshops, hands-on activities, and educational materials will help employees understand how IoT devices function and their security requirements.[7]

44% of organizations are recruiting IoT security specialists and 46% are actively training existing staff on IoT security.[2]

Current Laws

Surprisingly, the U.S. did not have an IoT cybersecurity law until December 2020. The IoT Cybersecurity Improvement Act (CIA) mainly deals with governmental IoT technology procurement; however, it is poised to set a standard of security for the IoT industry at large.[8]

The law covers three main points:

1. The National Institute of Standards and Technology (NIST) is required to develop new standards and guidelines to regulate IoT cybersecurity.
2. NIST must also develop guidelines for third-party reporting of issues related to IoT devices.
3. Each federal agency will have until December 2022 to ensure all IoT contractors meet the minimum standards set forth by NIST.

Improvements from this law will potentially affect both the public and private sectors. Currently, 58 out of 80 federal agencies utilize IoT technology, requiring any governance to be expansive in its consideration of cybersecurity. Each agency has many contractors who will have to abide by the new law. If IoT devices are not compliant with the IoT CIA, the government will not be able to purchase them, hurting any potential vendors. On the other hand, if the vendor is compliant, the benefits of improved IoT cybersecurity measures will extend throughout the public sector and help mitigate the risk of cyber attacks.

> IoT attacks more than doubled from the last half of 2020 through the first half of 2021, totaling **1.5 billion**, according to Kaspersky.[12]

As for the private sector, the IoT CIA is not directly meant for it. That being said, the improved minimum standard for IoT device security will almost certainly help private organizations manage cyber risks just like their public sector counterparts.[9]

California was the first state to pass an IoT security law, aptly named the Internet of Things Security Law. The intent of this law is to provide IoT device users with more comprehensive security, including requiring manufacturers to actively promote the security of the devices they create.

The law has two important factors:

1. Manufacturers must equip the device with a reasonable security feature or features that are:
   a. Appropriate to the nature and function of the device.
   b. Appropriate to the information it may collect, contain, or transmit.
   c. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

2. If a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if either of the following requirements is met:
   a. The preprogrammed password is unique to each device manufactured.
   b. The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.[10]

Critics of the California law say it is too ambiguous and does not define penalties for noncompliance. This was likely the motivation for Oregon to include this language in its own IoT security law, passed several months after its predecessor. The Oregon IoT law states that a violation will be considered "an unlawful trade practice" under Oregon's consumer protection law (ORS 646.607), which comes with a hefty fine of $25,000. With Oregon's law as the new precedent, we can expect more of its kind to pop up around the country. Time will tell how impactful these mandates will be.[11]

> **84%** of companies reported IoT had ensured business continuity for them during the pandemic.[2]

Securing the Future

If we don't want our fixation with convenience to lead us to ruin, we must continue to focus on IoT security. Having network visibility, segmenting devices from other networks, and monitoring, inspecting, and enforcing security policies are all necessary for the safe and practical use of these technologies.

Organizations should also have an iron-clad incident response program, in the event that an exploited device leads to a security incident, and look into implementing zero trust architecture (ZTA). ZTA is a cybersecurity concept focused on role-based access. No user or device has access to anything by default, giving organizations tighter control over who has access to what. For IoT, ZTA can authenticate endpoints and devices to maintain control and network visibility.

Like many technologies, IoT devices can help improve our lives and businesses, but we must protect them to protect ourselves.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
2. https://www.iotjournaal.nl/wp-content/uploads/2020/10/vodafone-business-iot-spotlight-report.pdf
3. https://www.juniperresearch.com/researchstore/devices-technology/internet-of-things-iot-data-research-report/subscription/consumer-industrial-public-services
4. https://www.researchgate.net/figure/Attack-surface-of-IoT-device_fig3_339097837
5. https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/
6. https://ordr.net/pr/ordr-releases-2020-enterprise-iot-report/
7. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats
8. https://www.govtrack.us/congress/bills/116/hr1668
9. https://www.nabto.com/us-and-california-iot-security-laws-guide/
10. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
11. https://olis.oregonlegislature.gov/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled
12. https://threatpost.com/iot-attacks-doubling/169224/

The Future of IoT Security

SECURANCE CONSULTING
the advantage of insight

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com