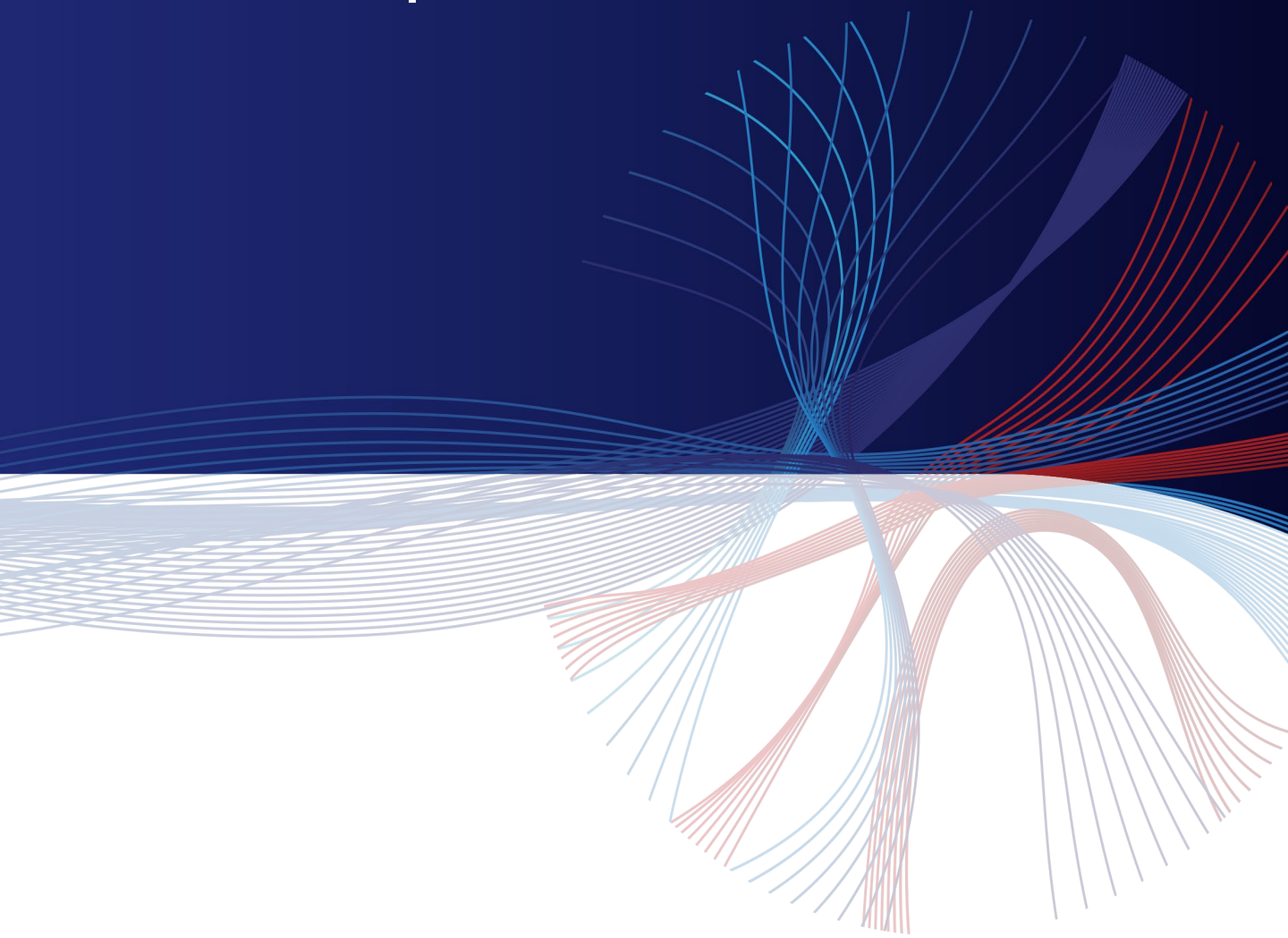
SCADAfence

Whitepaper

Attacks on IoT Devices and the Risks they Pose for Enterprises



July 2020

SCADAfence

Whitepaper

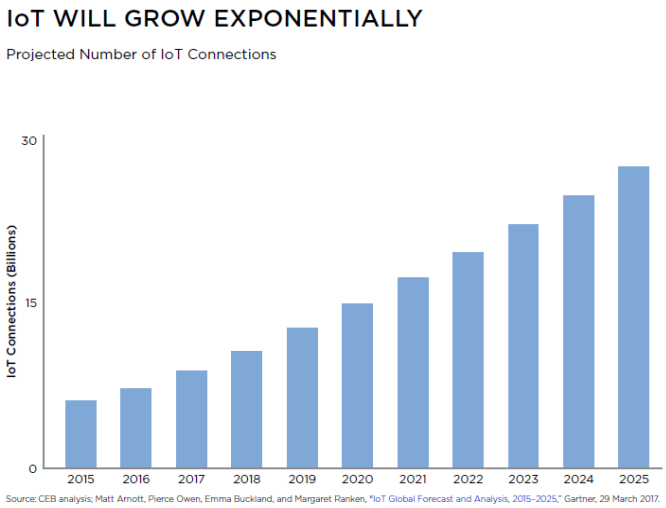
Attacks on IoT Devices and the Risks they Pose for Enterprises

An average enterprise network consists of hundreds of IoT devices, accounting for 15%-25% of the IT networks. According to Gartner, the amount of IoT devices in enterprises is growing at 21% per year (doubling every 4 years).

IoT devices pose a huge and growing management challenge. Many of them were not designed with enterprise policy and management in mind and were not intended to be centrally managed. They use proprietary management interfaces, often designed to be only human-readable or with an API that requires per-device development. A large portion of IoT devices have no proper management tools, while others are managed by a large number of independent (local or enterprise) management systems.

This decreases the IT departments' ability to regularly keep track of all IoT devices connected to the network, to control their policy, and to keep them secure. Usually this results in leaving the IoT devices in an unsecure state and, as a result, the entire IT and IoT network. Here are some of the numerous security issues for IoT devices:

- Old, weak or default passwords.
- Out-of-date firmware with critical CVEs.
- Insecure configurations.
- Lack of monitoring for malicious activity or anomalous behavior.
- Violations of internal policies and external regulations.



IoT connections are poised to grow exponentially and surpass 25 billion in 2025.

Enterprise IoT Devices Include:

- IP Cameras & NVRs
- Wi-Fi Access Points
- Printers / scanners
- VoIP equipment
- Access control systems
- IoT gateways
- Smart sensors
- Smart TVs
- Network-attached storage (NAS)

Why are IoT Devices More Susceptible to Security Flaws?

There are multiple reasons accounting for the insecurity of IoT devices:

Lack of Manageability – According to Gartner, "IoT Manageability is a throwback to IT of 20 years ago". In comparison to servers, PCs or cloud instances, IoT devices are either unmanaged or have a limited support for centralized management - with each vendor providing its own systems. When devices are unmanaged, there is hardly any way to control and standardize policies across all devices, which in turn increases their risk without the knowledge of the enterprise.

Inherent Insecurity – Many IoT devices contain vulnerabilities in their built-in firmware, which in many cases there are no available patches for, or that cannot be applied at scale. In many cases, the end-users are not even aware that they have a vulnerable device.

Diversity – IoT devices are far from being identical – There are thousands of different products with different kinds of hardware, from CPUs to chipsets, as well as different firmware and different underlying operating systems since requirements are different for each device. It is therefore difficult to find one solution to fit them all.

Cloud-Connectivity – Many IoT devices have an optional or mandatory cloud connection, which creates an additional attack vector.

Price & User Friendliness – Secure products tend to be more expensive because they're more difficult to develop and support. Secure products can be more difficult to install and maintain, and many features present a tradeoff between security and user-friendliness, at which many vendors prioritize the latter.

Legacy Equipment – While the issue of IoT devices' security has only become a considerable problem recently, IoT devices have already been in use for many years, with many large scale deployments already in place. Achieving inherent security requires radical changes to the entire ecosystem, which has taken years to decades in the case of PCs and servers, and are likely to require a similar time scale in the case of IoT devices. It is bound to happen eventually, but we still have a long way to go.

Attacks on Enterprise IoT devices

The lack of management and lack of security, significantly increases the risk to IoT and IT networks, and exposes the organizations to previously unknown attack vectors. These risks have been materialized by attackers in multiple attacks against IoT devices in the last years.

An Enterprise IoT device is an embedded computer system designed to run a specific application, using a customized OS. However it is still a computer, containing a CPU (usually ARM, MIPS or PPC), RAM and flash disk space.

Attacks on IoT devices can therefore be categorized into two major categories: **code execution attacks** and **IoT application-level attacks.**

Code Execution Attacks

These attacks take advantage of IoT devices since they're small "computers" connected to the enterprise network. The attackers attempt to exploit their vulnerabilities in order to run malware directly on the IoT devices. The type of devices targeted (Camera, IP Phone etc.) are irrelevant for this type of attack, as it only uses the devices for their CPU and network connectivity.
Cases of generic, wide-spreading malware have been recorded using IoT devices (instead of regular computers) in order to perform DDoS attacks (e.g. Mirai botnet) or to send spam.
However, IoT malware can also be used as part of a targeted attack on an enterprise, in which it is used as a hidden access vector to the enterprise's network, possibly in addition to traditional malware on the enterprise's workstations and servers. As the software running on IoT devices cannot be easily inspected, and as IoT devices are often unmanaged and unmaintained, such malicious agents running on IoT devices can remain undetected for long periods of time.

This serves two main purposes:
Maintain an dormant, undetected presence in the enterprise network in preparation for a future, large-scale attack on the enterprise.
Combined with traditional malware, IoT malware can be used as a fallback, maintaining the attackers' presence in the network and allowing the execution of a second wave of an attack even if the traditional malware is detected and removed.

Code execution attacks are traditionally detected by passively monitoring the network traffic generated by the IoT devices and detecting anomalies compared with similar devices or past behavior, possibly isolating IoT devices that misbehave. This approach suffers from high operational cost due to the downtime in isolation of production devices, limited visibility into the IoT device, and costly, manual incident response procedures that require a human to physically find, inspect and reset or replace the supposedly compromised unit. Furthermore, in the case of a targeted attack, as a malicious agent on an IoT device will remain dormant and low-profile for as long as possible, it might not be caught by passive detection until it is already too late.

When attackers attack an IoT device for the purpose of running malicious code, they attack devices that are either unpatched or have an unprotected administration interface that allows installation of custom firmware or running scripts. This can be done by utilizing the device's default password, or by using stolen credentials.

SCADAfence IoT Security not only monitors the network for attacks on IoT devices, but also pulls the device's state and configuration, allows matching potential IOCs with threat intelligence sources, and analyzes the firmware version and configuration in order to detect vulnerabilities that can result in a successful code execution attack. Users can also use SCADAfence IoT Security to perform management actions such as password changes, firmware updates, and bulk configuration changes, to proactively reduce the attack surface, before the devices are compromised by malicious actors.

IoT Application-Level Attacks

Unlike code execution based attacks, these attacks take advantage of the nature of the specific IoT device by changing its configuration in a way which gives the attacker access to sensitive information or impairs the functionality of the device. Access to the device configuration is usually gained by using weak or default passwords, though vulnerabilities and vendor backdoors can also be used. These attacks do not involve the execution of malware on the device and are therefore significantly easier to mount.

The following list explains the methods in which an IoT device can be used for malicious purposes, using only configuration changes. The list is sorted by device type.

General Attacks

These are relevant to virtually all IoT devices:

Flash Firmware - The attacker can access the built-in firmware upgrade mechanism to flash their own firmware, containing a malicious agent, which turns this attack into a code execution type attack without the need to find and exploit a vulnerability. Alternatively, the attacker may intentionally flash corrupt firmware in order to put the device out of service ("brick the device"). Using a custom firmware, the attacker can directly control the hardware of the IoT device and use any sensors or actuators that are connected to it. In some cases, attackers are able to flash the device in a way that even a factory reset will not be able to revert.

Password Change - After changing a device's configuration in a malicious manner, the attacker may also change the administration interface's password, therefore preventing the administrator from reverting the changes without performing a physical factory reset.

Denial of Service - The attacker may intentionally corrupt the device configuration in order to put it out of service. Reverting the changes may not be trivial if the original configuration values were not backed up.

VoIP Phones

Wiretapping - An attacker can configure an IP phone to route its Session Initiation Protocol (SIP) traffic through their own malicious SIP proxy server, allowing the attacker to wiretap calls.

Call Hijacking - By interfering with SIP signaling using the said malicious SIP proxy, or alternatively using the call forwarding and/or dial plan configuration settings, the attacker can route phone calls (both incoming and outgoing) to themselves, allowing them to impersonate either side of the conversation.

Room Bugging - By combining certain configuration settings, such as the auto-answer feature together with ringer mute, an attacker can use the phone's microphone to eavesdrop on conversations in the surrounding area. A short demo video of this attack in action is available from SCADAfence Research.

Sending Spam - Many IP phones have a built-in SMS feature, which can be abused to send a high volume of spam messages.

Application level attacks on IoT devices:

General Attacks:
Flash Firmware
Password Change
Denial of Service

VoIP Phones:
Wiretapping
Call Hijacking
Room Bugging
Sending Spam

IP Cameras:
Direct Feed View
Alert Capture
Disabling Alerts
Disabling Recording / Streaming
Reducing Camera Resolution

Printers / Scanners / Fax Machines:
Reading Printed Documents
Reading Scanned Documents
Reading Faxes

Wi-Fi Access Points:
Hidden Networks
Weaken Security
Malicious Radius Server
Disruption

IP Cameras

Attacks on cameras can be categorized into two main types. The first is pure espionage:

Direct Feed View - The administration interface of most cameras includes a live view of the camera feed, which the attacker can capture (the view may or may not include audio as well). If the administration interface does not include a live view, the attacker can still add and/or set the credentials needed to access the feed.
Alert Capture - The attacker can change the location of servers used by the camera to send notifications and alerts (e.g. FTP server for video uploads, SMTP server for mail alerts) in order to route the notifications and alerts to themselves.

The second category of attacks on cameras involve the disruption of the correct behavior of the camera in order to weaken the physical security of the monitored area. Examples include:

Disabling Alerts - The attacker may disable functions such as motion detection, in order to prevent the camera from alerting security officers of physical incidents.
Disabling Recording and/or Streaming - The attacker can stop the camera from recording the video and/or detach it from the enterprise NVR. Later, physical attacks can be performed without leaving evidence, unless caught in real time. A short demo video of this attack in action is available from SCADAfence Research.
Reducing Resolution - An attacker can reduce the video resolution to an extremely low value, preventing the identification of burglars. Furthermore, this may not be noticeable from an NVR main split-screen and therefore may go undetected for a long period of time.

Printers / Scanners / Fax Machines

Reading Printed Documents - The attacker may configure the printer to save or send copies of printed documents to themselves.
Reading Scanned Documents - The attacker may change the location of servers handling scanned documents in order to capture them. For instance, changing the outgoing SMTP server value allows an attacker to capture all documents scanned using the “scan to email” function, regardless of the destination address specified by the user.
Reading Faxes - Most fax machines include the ability to automatically forward incoming and/or outgoing faxes, which the attacker can use to capture faxes going in and out of the enterprise.

Wi-Fi Access Points

Most attacks against access points are intended in order to gain unauthorized access to the enterprise network.

Hidden Networks - An attacker can create a new Wi-Fi network with a hidden SSID (which, for that reason, will not show up in network scans), and connects it to the main enterprise network.
Read the Network Password - Many access points display the current password in the configuration. Attackers can use the password in order to connect to the enterprise network without the need to perform any configuration changes. Attackers can also use the password to capture and decrypt network traffic of other users (this is mitigated by WPA3, however WPA3 is still not widely adopted. Furthermore, the attacker can disable WPA3 in the access point configuration).
Weaken Security - The attacker may change the network security scheme to an old, vulnerable method, such as WEP encryption (which is regarded by security professionals as being equivalent to no security at all).
Malicious Radius Server - If the network uses WPA-Enterprise authentication, the attacker can change the Radius configuration to point to their own malicious server, allowing them to decide who can connect to the network, as well as to capture the password hashes of all users who connect. This allows the attacker to not only connect to the enterprise network but to also log-in to the network resources as an enterprise employee.
Disruption - Other than unauthorized access, attackers can also disrupt the Wi-Fi network in a way which is not immediately recognizable, e.g. by changing Quality of Service (QoS) settings to significantly reduce the network bandwidth.

As these methods do not involve code execution, the device will not exhibit behavior which is unexpected for the specific device type. While some of the mentioned attacks may leave a fingerprint big enough to be detected by comparing the device's behavior with a past baseline, many will not.

SCADAfence IoT Security overcomes the problem by directly querying the configuration from the IoT devices, allowing the administrator to instantly notice a change in the device configuration, and revert it to the original values if it is deemed to be malicious.

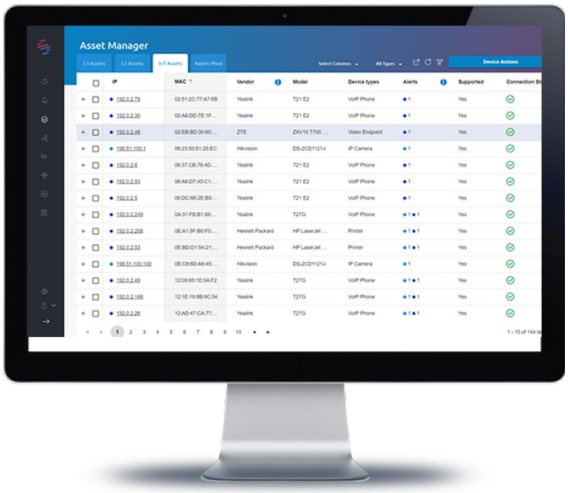
What Can You Do to Secure Enterprise IoT Fleets?

Isolation is Not the Silver Bullet

Traditional IoT security solutions mitigate attacks by integrating with firewall and Network Access Control (NAC) products in order to isolate compromised devices from the network. While this approach is effective in the sense of preventing further breach and/or spread, it has the side effect of disrupting the normal operation of the device. In some cases, such as security cameras, such disconnection might be the intention of the attackers to begin with, and such attackers may intentionally attempt to trigger a false positive identification of an attack.

Dealing with the Manageability and Enforcement Challenge

SCADAfence IoT Security brings a new approach to the table: protect devices before any incidents occur and reduce the need of using isolation for incident response. In case that incidents do occur, detect them quickly and react instantly. This significantly reduces the disruption to services and the manual recovery work needed.



SCADAfence IoT Security Solves Today's Biggest Problems in IoT Security.

The SCADAfence routine methodology for the protection of IoT devices includes:

Asset and Configuration Management - SCADAfence IoT Security uses both passive and active probing to automatically create a complete inventory of all IoT devices connected to the network. The inventory includes detailed information for every device, including the device vendor and model, firmware version, configuration details, users list, logs and others.

Vulnerability Assessment - SCADAfence IoT Security analyzes the collected information in order to create a comprehensive security assessment for each device. The platform alerts on risky configurations such as cameras that allow unauthenticated viewing, out-of-date or vulnerable firmware, and the use of weak or default credentials. The platform also alerts on suspicious network activity such as unauthorized connections, scanning, application level attacks, and many others.

Automate Attack Surface Reduction - SCADAfence IoT Security allows system administrators to perform operations at scale, such as upgrading to the latest firmware, as well as changing passwords and configurations. This proactive protection method allows the discovery and addresses risk exposure as it arises - before it materializes into an actual threat by adversaries. This approach significantly reduces both the total amount of incident responses, and the cost of each incident.

Incident Response Automation - SCADAfence IoT Security automates the incident response procedure to allow scalable incident recovery.

- **Reverting Configuration Changes** - If the attack involved the change of configuration values on the device, SCADAfence IoT Security can automatically revert all of the changes on all affected devices back to a restore point set by the user. This may be followed by a global password change in order to prevent further attacks.
- **Reflashing Firmware** - In the case of code execution type attacks, SCADAfence IoT Security can reinstall the original firmware on all affected devices, removing the malicious agent while keeping the device operational with minimum downtime. A new version of the firmware may be installed if one is available from the vendor, potentially addressing the initial vulnerability.

These proactive measures can detect and prevent most of the attacks on IoT devices before they happen. For the rest of IoT related attacks, SCADAfence IoT Security uses multiple mitigation measures and does not disrupt the normal operation of the organization's IoT devices.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, go to www.scadafence.com