SECURITY AND THE INTERNET OF THINGS

THE STEPS TO SECURE YOUR CONNECTED NETWORK NOW

aimetis | WHITE PAPER

> *“The biggest issue is not the security of the cloud, but the lack of security on the devices themselves.”*

SECURITY GAPS IN THE INTERNET OF THINGS

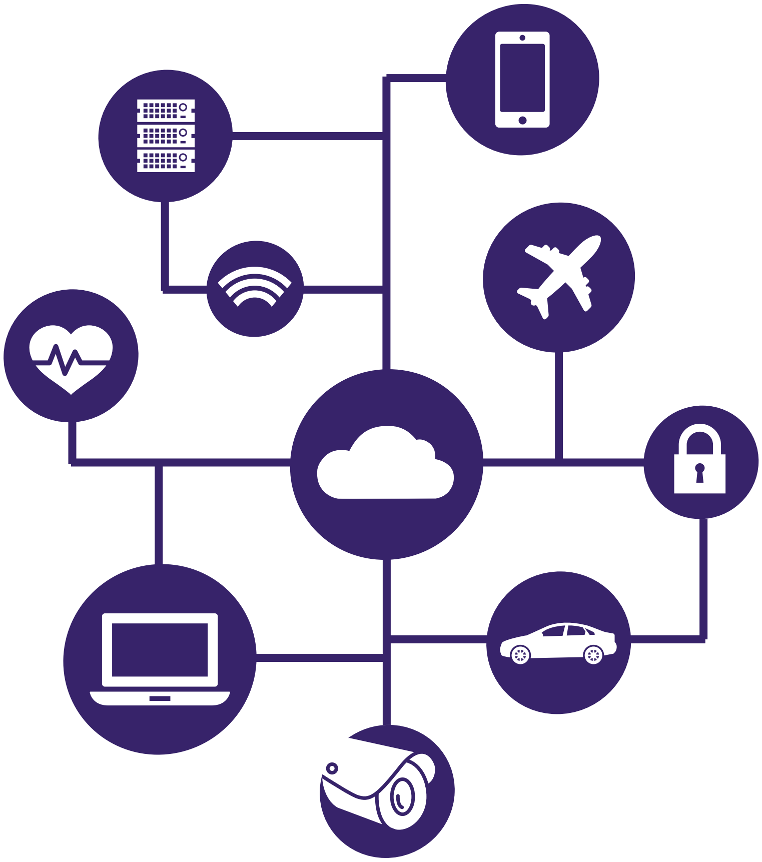
The Internet of Things (IoT) is quickly taking over the technology world. Physical devices from cars to HVAC systems, and even refrigerators, are communicating and interacting with one another either over an internal network or the internet.

BY 2020 THERE WILL BE 25 BILLION CONNECTED SYSTEMS IN THE WORLD

A recent Gartner study estimates that by 2020 there will be over 25 billion embedded and intelligent systems interacting with one another over the IoT[1]. Obviously, there is a tremendous amount of hype around our growing interconnected world of devices, but where does the security of the IoT fit in?

The problem with any new, and much talked about technology, is that adoption and use typically out paces the need for truly secure design, leaving most IoT devices and software a security risk.

The biggest issue is not the security of the cloud connecting these devices, but the lack of security on the devices themselves. Whether it’s old software sold with new devices, or users simply failing to change default passwords, there are countless ways your IoT systems are vulnerable right now.



[1] “Connected Cars Will Form a Major Element of the Internet of Things”, last modified January 26, 2015, http://www.gartner.com/newsroom/id/2970017.

WHAT CAN YOU DO TO ENSURE YOUR CONNECTED SYSTEM IS SAFE AND SECURE?

Vulnerable systems can be found anywhere and can happen to anyone in the IoT world. That doesn't mean you can't take the time to make the adjustments and updates needed in order to prevent unwanted hackers from accessing your system.

Interconnected devices in the IoT are becoming more complex every day. To keep your systems secure, you should focus on: device lifecycles and updates, password control and authentication, data encryption, and overall network security.

4 STEPS TO SECURING YOUR IoT SYSTEM

LIFECYCLE AND UPDATES

It might seem too simple, but start by ensuring your devices have the latest firmware updates. Without it, your security devices could have critical known vulnerabilities. For those devices no longer receiving firmware updates from the manufacturer, it may be time to replace your hardware with a new system in order to close the security gaps.

PASSWORD CONTROL AND 802.1x AUTHENTICATION

Passwords and secure access controls are obvious steps to implement, but it is surprising how many devices have never had their default passwords changed. Did you know your device's default password is most likely posted online right now? That opens you up to an intrusion at any time. Take it a step further, implement IEEE 802.1x authentication, which provides authentication to devices attached to a LAN port. This protection is useful as cameras that are located in public spaces and openly accessible network jacks that can pose a security risk.

DATA ENCRYPTION

When data privacy is of the utmost concern, encryption is the only way to maintain strong security of that data. By using persistence-based encryption that encrypts data when it is stored on a particular device, you can add a key layer of protection. SSL communication can also be used to encrypt data that travels over a network. Using SSL is integral to preventing intrusion attacks such as "man in the middle attacks" and "network traffic sniffing."

NETWORK SECURITY

Strong network security should be maintained. This means implementing a properly configured firewall within the network at all times and securing all ports of access. You should also adhere to operating different VLAN on your network to limit and control access to the overall local area network (LAN). Finally, you should regularly audit, test, and update your IT security policies to ensure constant security.

MOVING FORWARD

The Internet of Things market is not going to stop growing. It continues to expand and evolve as more uses for interconnected devices are created. As the hardware side of the IoT matures, security will begin to improve, but the market is not there yet. Until then, make sure you continue to make updates of your devices or evaluate their lifecycle, maintain password controls, implement data encryption, and continue to assess overall network security in order to reduce the risk of your system being compromised.

QUESTIONS

For any questions on the security of your Internet of Things network or content in this white paper, please contact us at Aimetis anytime.

aimetis.com
info@aimetis.com

ABOUT AIMETIS

Aimetis Corp. simplifies the management of network video for security surveillance by offering smart solutions with the lowest total cost of ownership for our connected world. Combining an industry leading video management system with integrated analytics and centralized management in the cloud, Aimetis delivers the most scalable and easiest to use video management platform on the market. Founded in 2003, Aimetis has established itself as a global leader in intelligent video management from its headquarters in Waterloo, Canada. Aimetis has distributors and certified partners in over 100 countries and serves a variety of industries, including retail, transportation, and others.

The information researched to create this whitepaper was obtained from sources considered to be reliable. Aimetis Corp shall have no responsibility for errors, omissions or inadequacies of this information.

All opinions expressed in this white paper are those of Aimetis, except where original author is credited. The opinions expressed in this white paper are subject to change without notice.