PlantWeb University – Wireless 206

Wireless Security

15 minutes

In this course:

Overview

Security is by far the most frequently cited concern about wireless communication in process automation.

A common myth is that wireless networks are not as secure as wired networks. Because a wireless system can be attacked without *physical* intervention, it's often considered to be less secure than a wired system. But in fact, wired and wireless networks are both vulnerable.

Because these vulnerabilities are well understood, responsible vendors and others have already developed technologies and practices for protecting against them. Choosing and using the right security measures will result in a safe, secure, and easy-to-use network – whether it's wired or wireless. It's not difficult if you understand the risks and how to guard against them.

In this course you will learn about the basics of communications security, including how a wireless network can be attacked. You'll also get an introduction to technologies and best practices that can help you implement an effective security strategy for your wireless solution.

Because in-plant, self-organizing field networks are an important new application for wireless technology, they tend to generate a lot of discussion about security. So although the security principles discussed in this course are applicable to all wireless technology in process automation, we will use in-plant, self-organizing networks for the examples.

At the end of the course you'll find a short quiz to help you confirm what you've learned.

Hint

As you go through the topics in this course, watch for answers to these questions:

- What is the definition of communication security?
- How is wired security different from wireless?
- What are the key components of an effective wireless security strategy?
- What best practices can make your wireless network more secure?

Communication security

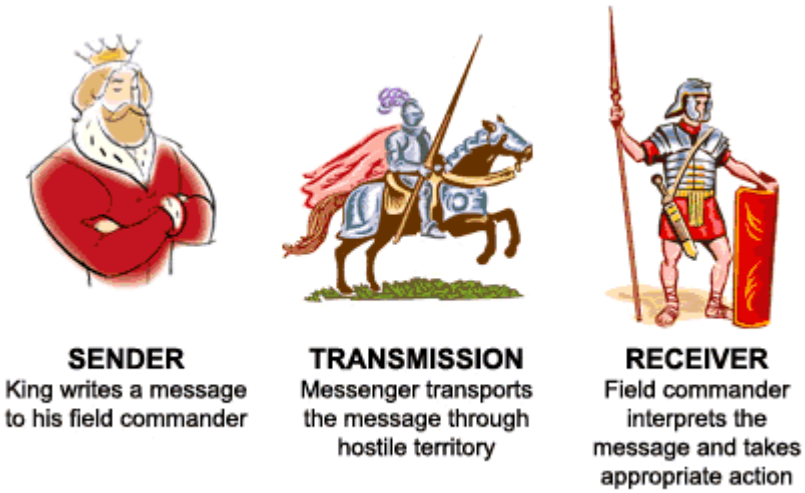
Communication security is **the ability to pass verifiable data from a trusted source to a trusted recipient without third party interference**.

A secure communication system enables you to

- **Authenticate** both the sender and receiver – in other words, confirm that they are who they say they are
- **Verify** that the message is valid – that the information received is the same as what was sent.
- **Encrypt** the data – so it's unreadable if accessed by an unintended party

These are not new concepts. Authentication, verification, and encryption have always existed, in some form, as a way of making communication secure.

Before we discuss how they affect wireless security, let's look back in history when, for example, kings used messengers to carry instructions to field commanders in times of battle:



First, the king *encrypts* a message, or writes it in a code that only he and the field commander understand.

Then the king seals the letter with wax so the receiver can see that the message was not tampered with, thus *verifying* its contents.

Finally, the king, messenger, and commander use pre-arranged passwords to *authenticate* the person who's giving or receiving the message.

The field commander then decodes the message, and carries out the instructions.

Modern communications use similar (but more sophisticated) security techniques, which we'll examine later in this course.

But first, what happens when the king's enemies (or yours) try to interfere with a communication?

Types of attacks

Despite encryption, authentication and verification, your communications may still be attacked – and the attack may succeed if you haven't implemented those security measures properly.

Common types of attacks include

- Denial of service
- Spoofing
- Man in the middle
- Replay

We'll use the same analogy of the king, the messenger, and the field commander to show how each attack works.

A ***denial of service*** attack floods the communication channels with unwanted messages to prevent the system from functioning. This includes ***jamming***, or creating interference on message pathways. For example, the king's enemies might block the road with trees and rocks to prevent the messenger from getting through in time to deliver his message.

Spoofing occurs when someone assumes the identity of another in an attempt to gain access to a system. In this instance, someone pretending to be the king might send his own messenger to deliver incorrect information to the field commander.

A ***man in the middle*** attack provides a way for an attacker to intercept, change, and/or control messages without the sender or receiver knowing that the link between them has been compromised.

An example might happen if the king gives the message to his trusted messenger, who, it turns out, cannot be trusted. This messenger gives the message to someone else, who modifies the message. The messenger then delivers the new message to the field commander.

Replay is a form of network attack in which information is stored without authorization and repeatedly transmitted without the knowledge of the sender.

For example, the untrustworthy messenger could deliver the king's message to the field

commander, then deliver the same message again the next day – and the next. If the order was to move the field commander's troops 5 miles to the west, then each time the order is obeyed the troops will be farther out of position.

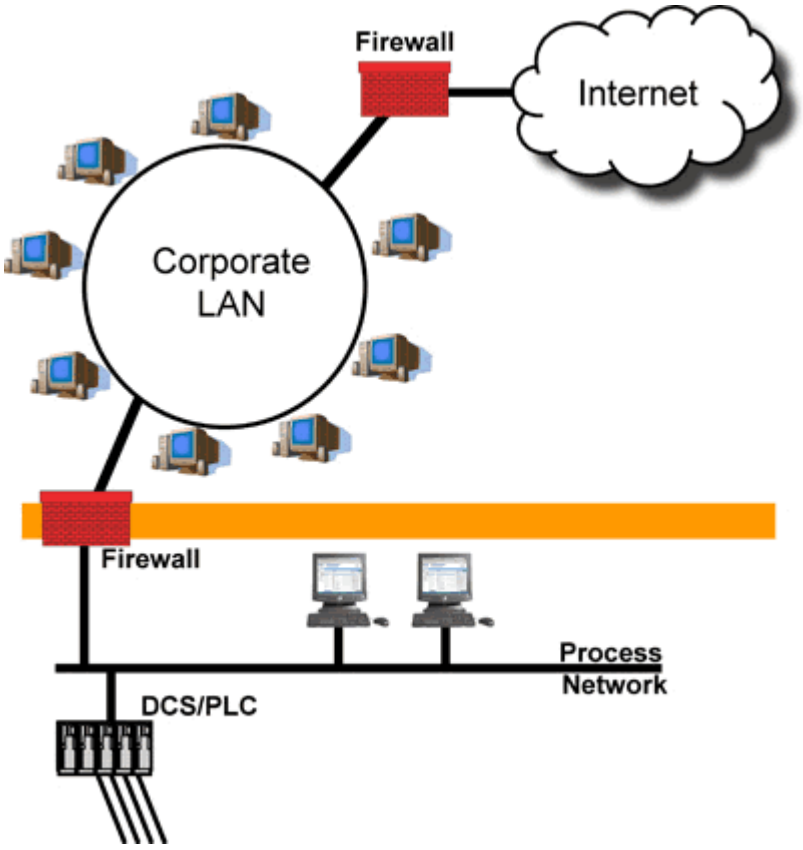
Modern forms of these attacks (and other devious schemes) use electronic means, but they can be just as disruptive to your communications and the process operations that depend on them – unless you know how to effectively protect your network.

Security in process automation

A disruption in e-mail or telephone communications is annoying, but an attack on process-control communications can be much more serious. Imagine the possible effects of bad data on process operations – from poor product quality to unplanned downtime, labor inefficiencies, and health, safety, or environmental incidents.

While most plants have active plans for maintaining physical security, electronic security of process control information traditionally has received very little attention. That's changing as process control networks and systems are increasingly linked to other plant and business systems – and from there to the external Internet.

To protect data under these circumstances, plants today typically use a ***layered*** approach to communication security.



Firewalls can be part of a layered security approach to protecting process data and systems from external attacks.

In this illustration, for example, the first layer of security is a high-quality, industrial-grade firewall between the Internet and the corporate local-area network (LAN). The second layer is a second firewall that connects the corporate LAN to the process control network where the DCS/PLC, automation and optimization packages, historians, and databases are located. Each firewall provides an electronic security barrier between the two networks it connects, blocking unauthorized or potentially dangerous messages.

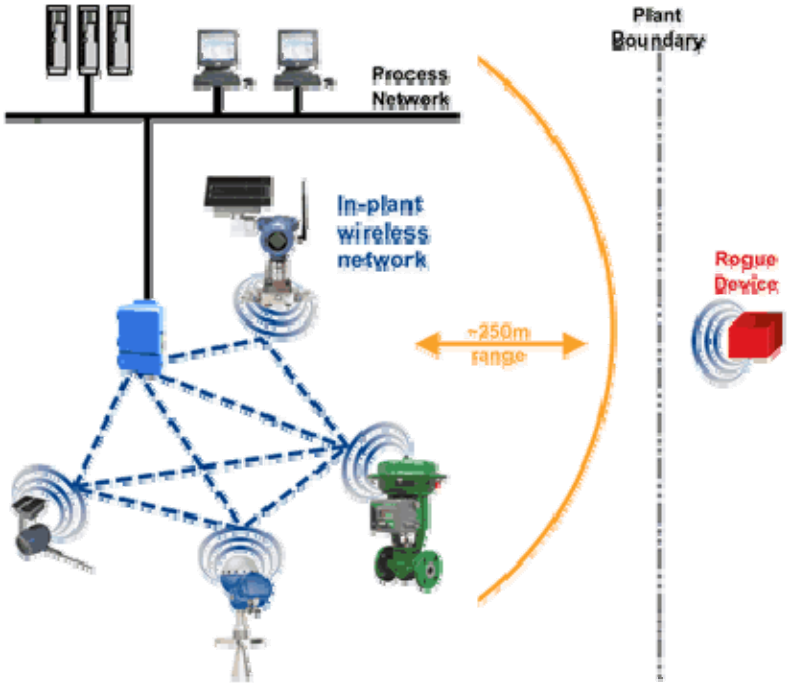
However, commercial firewalls are usually designed to work with Internet protocols rather than control-system communications. And in this scenario no firewall exists between the devices in the field and the process control network. That makes people nervous because they're concerned that the devices could be attacked through the network – or the network could be attacked through the devices.

But is this situation any less secure than a similar wired network?

Wired vs. wireless

Because a wireless system can be attacked without *physical* intervention, it's often thought to be less safe than a wired system. But in fact, wired and wireless networks are equally vulnerable.

A common misconception about wireless is that a rogue device within range of a wireless network can simply connect to the attached process control network. This simply isn't true, as is discussed in more detail later in this course. In addition, these low-powered wireless devices generally have to be within close proximity (about 750 feet or 250 m) to communicate. This limited range makes it difficult for outside devices to interfere with in-plant wireless networks.



The limited range of wireless networks helps make successful attacks unlikely.

Even if an outside device *is* able to access the network, emerging wireless standards will define a number of measures (discussed in the next section of this course) to protect communications. Products built to these standards will make process automation networks very robust and protected against these types of attacks.

In fact, because of heightened awareness of security issues, security-conscious vendors of wireless devices and networks have designed their offerings with security in mind. These products are therefore usually not the primary security problem in process control operations. Instead, the **real problems** often come from antiquated distributed control systems (DCSs) and proprietary protocols that were not designed with today's security considerations.

Making wireless more secure

Wireless-equipment vendors have carefully studied potential security risks and concerns, and have taken steps to incorporate security into their products.

The most effective wireless security strategies include three capabilities we learned about earlier in this course:

- ***Authenticating*** sender and receiver
- ***Verifying*** that the data is valid
- ***Encrypting*** the data

Plus two more that have become more important in the time since our example king and field commander exchanged messages:

- ***Key management*** to periodically change the secret codes
- ***Anti-jamming*** to avoid interference and blocked communication spaces

Let's take a closer look at each of these.

Making wireless more secure
Authentication

As we learned earlier in this course, **authentication** establishes that a sender and receiver are who they say they are. In the case of a wireless network, it proves that a device communicating on the network is the authorized node that its messages say it is.

Authorized devices authenticate each other by exchanging "keys" (the digital equivalent of a password) programmed into the devices and host. This prevents rogue devices or hackers – who don't have the right keys – from gaining entry through an access point and communicating as if they were valid nodes on the network.

Some vendors build authentication capabilities into their wireless-network gateways. (A gateway collects data from devices in the wireless network, then passes the information to the process control network.) Just as in wired networks, such gateways allow only authorized devices to join the network – and you define which devices those are during installation and commissioning.

For example, you can program the gateway to allow connections only from a known set of

transmitters. Any transmitters not on the list fall into the “rogue” category and are denied access. The transmitters, in turn, will accept messages only from a previously identified gateway or from another device that the gateway recognizes as authorized.

Another way a rogue device can try to disrupt the network is by posing as an authorized device and intercepting and modifying a message (called "spoofing"). In this case, a gateway using **message integrity codes** can still prevent the rogue device from communicating with your network. This is explained in more detail in the following section.

Making wireless more secure
Encryption

Encryption techniques used in wireless networks use a digital "key" to mathematically alter or “scramble” data in a message, making it unreadable to anyone other than the receiving device or system (which uses a matching key to unscramble the data).

To minimize exposure of unencrypted data, it's a good idea to do the encryption in the actual device that generates the message.

There are many types of data encryption, but we’ll focus on two common methods:

- **AES** (Advanced Encryption Standard) is U.S. government standard used by many organizations with high security needs – for example, by the Federal Reserve Banks in the U.S to transfer money between banks. While robust and strong, it is computationally very intensive–making it difficult for the small, low-power computing devices that can be embedded in plant equipment such as valves and transmitters. However, the coming availability of ASICs (application-specific integrated circuits) with this capability will enable this level of encryption at the device/gateway level.
- **XTEA** (Extended Tiny Encryption Algorithm) is a less computationally intensive algorithm – but still strong enough to make deciphering the message practically impossible.

Making wireless more secure
Key management

Key management is the process of creating, distributing, authenticating, and storing encryption keys (codes) that are used to encode and decode data.

Poor key management can weaken any security system. It's like losing your bank card – with your password written on the back. Or imagine what could happen, for example, if a disgruntled former employee still had a list of your encryption keys.

One way to safeguard your data is to change encryption keys frequently. Generally, the more often you change the keys, the less vulnerable your system is to a security attack. But the system also becomes more complex unless you have a gateway or other system that can be programmed to do this key “rotation” automatically.

There are three basic levels of key management:

Level 1: Every device from the same manufacturer has the same key. This level is better than nothing but not suggested.

Level 2: Every device on a single network uses the same key. This level of security is generally acceptable for most networks, if the key is changed regularly.

Level 3: A different key is used for each end-to-end communication pair. For example, you might use one key between the pressure sensor and the valve and a different key between the pressure sensor and the gateway.

Complexity of key management increases dramatically with each level. You can work with your security experts and IT team to decide which makes the most sense for your plant, or implement the appropriate level suggested by your wireless vendor.

Making wireless more secure
Anti-jamming

Anti-jamming capabilities decrease the likelihood that radio-frequency or other electro-magnetic signal interference – intentional or otherwise – will disrupt network communications.

One anti-jamming technology is **spread spectrum**, or distributing the message over greater bandwidth to maximize the probability of a successful transmission. There are two common methods: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).

FHSS concentrates the transmission into a particular frequency that changes rapidly over time. If one frequency is blocked by interference or obstructions, the message will get through when it switches to another frequency a few moments later.

DSSS – the method used in Wi-Fi (IEEE 802.11) communications – represents each "0" and "1" in a digital message with a specific sequence of small frequency variations. Even when jamming interferes with part of the transmission, enough of the sequence remains to be recognized by the receiver.

Some wireless networks use both FHSS and DSSS to help ensure reliable communications.

Making wireless more secure
Putting it all together

Because you can't know exactly which type of attack you may face, a strong security system includes protective measures against them all. The chart below shows how each of the techniques we've just reviewed mitigates the risk of some common security threats. (The chart is not meant to illustrate the full range of possible security threats).

	Denial of Service	Spoofing	Man in the Middle	Replay
Anti-jamming	✓			
Authentication		✓	✓	
Verification			✓	✓
Encryption		✓	✓	
Key management	✓			✓

Best practices

Wireless technology offers major cost and performance benefits – as long as you take the proper steps to maintain communication security.

Let’s take a look at some industry best practices you can implement to help secure your network – wired or wireless – and keep your data safe.

- **Stick to open standards**. It's tempting to believe that proprietary software and protocols are more secure because fewer hackers know about them. But even vendor-specific protocols are accessible to someone who really wants to find them – and turn them against you.

  With open standards, however, you'll benefit from the work that others have done – and continue to do – to keep improving stability and security, as well as to add new capabilities.

- **Choose a vendor committed to security**. One of the most important steps you can take to protect your network is to work with a supplier who understands the issues covered in this course. Security should be designed into the network architecture, not added as an afterthought.

  The leading vendors in wireless technology for process automation are committed to providing all aspects of a secure and reliable network architecture, and know how to implement all the components of an effective security strategy – including encryption, authentication, verification, key management, and anti-jamming technology. This makes robust security easy to implement but extremely difficult to compromise.

- **Work with your IT department**. IT groups have well-documented security practices and can help you secure your wireless network. You may have to help them understand the difference between your application and what they're accustomed to with office and business-system applications, but the principles will be the same.

  For more on this topic, see *the course on IT Coordination*

Summary

In this course you learned about the security issues of using wireless technology in process operations, and how you can protect your network from attacks.

Key points covered in the course include

- Wireless networks can be as safe as wired ones when implemented properly. Because wireless equipment has been designed with security in mind, wireless networks may even be **more** secure.
- Potential attacks on communication security include denial of service, spoofing, man in the middle, and replay.
- Security is most effective if it includes encryption, authentication, verification, key management, and anti-jamming measures. You’re not really secure unless you incorporate all these components.
- Security must be designed into the system architecture and not added as an afterthought.

- Knowledgeable vendors can make implementing a security strategy easier, but it's still your responsibility to ensure your communications are safe. Implementing best practices will help secure your network.

The Emerson Advantage

Emerson's approach to wireless security benefits from our familiarity with wireless technology and its applications in process automation.

Because we understand users' concerns about protecting process performance and data, security is **designed into** our wireless offerings. For example, our Smart Wireless solutions include the Rosemount 1420 wireless gateway which comes with automated key rotation and other key-management capabilities – right out of the box.

In short, we make wireless security **easy**.