Wireless Security Measures Part 1 of 2

Table of Contents

Wireless Security Measures 2

Wireless Networking 3

Types of Wireless Networks -1 5

Types of Wireless Networks -2 7

Wireless Hardware 8

Setting Up A Wireless Network -1 10

Setting Up A Wireless Network -2 13

SSID (Service Set Identifier) 15

Wireless Authentication -1 16

Wireless Authentication -2 18

Wired Equivalent Privacy (WEP) 20

WEP Limitations 22

Notices 24

Wireless Security Measures

**005 Nick Flores: And we'll begin with our first topic, which deals with wireless security measures.

Wireless Networking

Has become ubiquitous because of its low cost and convenience, unfortunately it has introduced many security issues along the way

Allows users to access resources without being tethered to a network connection by a cable

Advantages	Disadvantages
Great mobility	Insecure (easy to access)
Cost-effective implementation	No physical protection of network
Easy to connect and network	High risk of data sharing

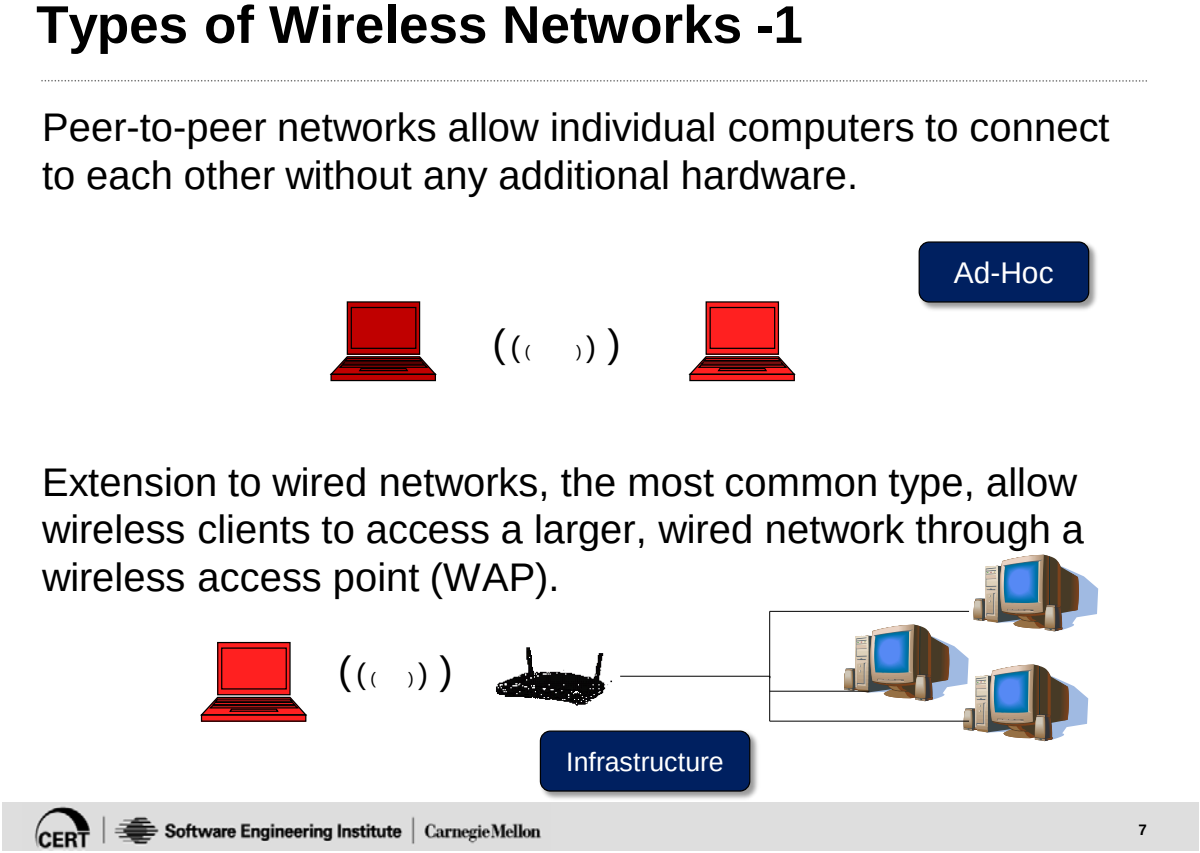
**006 So, wireless networking has become-- Wi-Fi in particular-- has become a very popular form of providing LAN access for individuals. Why is that? Well, there's advantages. It's a lower cost for your wiring expenses. You don't have to run cables everywhere. It makes it very easy to people to connect to and from the network without being near wall jacks or something specific that they need. And most devices nowadays, whether they be laptops, smartphones, tablets, they all come with Wi-Fi capability built in, so it's very easy to connect these devices to the network.

The problem, or the opposite side of that spectrum, is that you have all of these disadvantages to worry about. Wireless networking in and of itself, by default, is insecure. Again, we talked earlier about this idea of a balancing scale, and that the more security you have the less convenient something normally is, and the more convenient something is, the less secure it is. Well, wireless networking is very, very convenient.

So out of the box, it's also very, very insecure. So there are ways we can-- methodologies we can employ to try and secure these networks.

The other problem is that there's no physical protection of the data being transmitted. When we talk about wired networks, in order for me to listen to network traffic on a wired network, in order for me to access that traffic and in order for me to manipulate that traffic, I've got to first physically be connected to that network, which means I normally have to get inside your building or inside your facility; I have to find an area where it's got network capability and then jack into the wall before I can do anything else. With wireless networks, we're talking about an unbound media, bits of ones and zeros floating around in the air. It makes it much easier for me now to intercept those ones and zeros and do different things to them. So physical access becomes much easier for malicious users.

Types of Wireless Networks -1



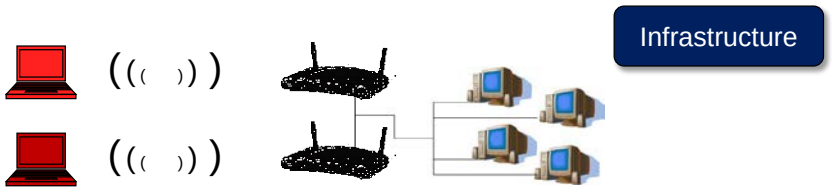
**007 So, what are the different types of wireless networks? We've discussed a little bit in previous topics but we're going to go over it again. How can you set up a wireless network? I've got a wireless access point. In what way can I use that wireless access point? Well, we can set up ad hoc networks. Ad hoc networks generally don't require a wireless access point device. Those are a computer-to-computer Wi-Fi network, often used in LAN parties or gaming parties or for quick data transfers. Normally ad hoc networks are not a permanent solution. It's something that is quick and easy to set up between one host and another

to transfer files or share data back and forth, and then normally when that data sharing is done we kill the network and we go about our separate ways. It allows two individual computers quick access to each other.

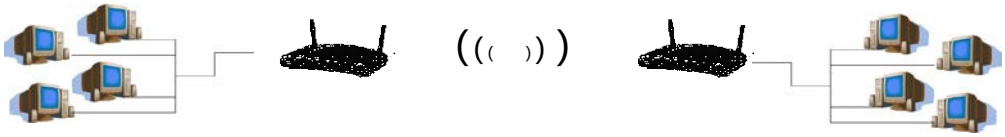
Most of the time when we're working with wireless networks, we're dealing with an infrastructure mode network, where we've got a wireless access point and that wireless access point is connecting our network traffic, or bridging it, into a wired network. An example of that is the diagram you see on the bottom, where a wireless client, the red laptop out there, is connecting to this wireless access point, and that access point is then connected to a wired network. This is the more common architecture we're used to using.

Types of Wireless Networks -2

A multiple access point network uses several access points, usually to cover a wide area or serve many clients.



LAN to LAN (or wired to wired) wireless networks bridge wired networks.



**008 Even more common than that, especially in larger geographical areas, is adding multiple wireless access points or multiple WAPs to that. So still using an infrastructure mode environment, but now I may have wireless repeaters or multiple wireless access points, and so I get a greater surface area coverage, if you will-- a greater geographical area coverage of my wireless signal, which allows me to spread that signal further and further away from my wired network.

You can also use wireless access points to talk to each other. So in earlier topics we discussed maybe I have a wired network in this building,

and I have another building across the street, and there's a wired network there, and I want to connect the two LANs together, but I can't run infrastructure or wires between the two buildings. Well, I can set up a wireless access point on this building, a wireless access point on that building, and have the two wireless access points bridge to each other in a bridge mode, and that allows this wired network to talk to that wired network.

Wireless Hardware

Wireless Hardware

Wireless networks typically use access points.

Antennas are located on both the access point and on the wireless cards and send/receive the wireless radio signals (OSI Layer 1).

- Omni directional antennas radiate signals in all directions.
  - Effective for mobile applications, or where clients may not connect from a specific location
- Directional antennas radiate signals in a more constrained path.
  - Provide higher gain (send / receive stronger signals), but only to clients in the direction they are pointing

CERT | Software Engineering Institute | Carnegie Mellon 9

**009 So, what comprises our wireless hardware? In the picture on this slide you see an example of a traditional Linksys-type wireless

access point. In those wireless access points, whether you can actually see them or not, they do have antennas, and these antennas might be omnidirectional, which is more common-- omnidirectional meaning that the radio waves, the RF, is emanating from those devices in all directions, normally in all directions equally, until of course that RF hits something that interferes with it, like windows or walls or other structures that maybe interfere with the RF.

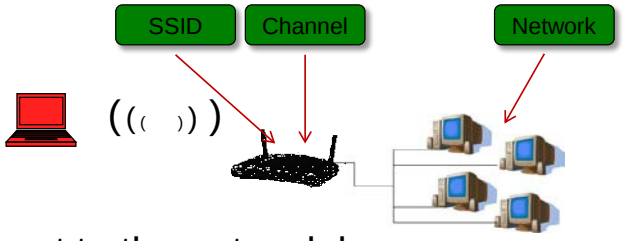
Some wireless access points-- normally used in the example we talked about where we have the two buildings and we want to bridge one to another-- some wireless access points have unidirectional or specific directional antennas. These allow the wireless access points to focus that RF signal in a single direction so that there's a higher gain, which means I can get that signal a longer distance, and there's a greater-- a higher concentration of the signal, if you will-- a louder signal, a stronger signal-- so that the other end receives it without the interference affecting it as much.

Whether your wireless access point uses omnidirectional or directional antennas, either way it is emanating RF. And so when we're emanating RF, we're emanating radio frequency, that's an unbound media and we have a potential for interception there.

Setting Up A Wireless Network -1

Wireless networks require

- A channel
- A SSID
- Network details like IP, gateway, and network mask
- Security and encryption may or may not be configured



Clients can connect to the network by

- Passively listening for broadcasts from an access point
- Actively sending connection requests to an access point

**010 So, when we set up a wireless network, just like when we set up the IP configuration that we talked about in previous topics--when we set up the IP configuration of a host, there are things we need to know in order to configure it. We talked about IP addresses and subnet masks in earlier topics. So too in a wireless network; when you set it up, there are wireless or Wi-Fi-specific information that you have to know or configure in order to set this wireless network up.

For example, you need an SSID. An SSID is the name of the wireless network. So when you open up your

smartphone or you open up your tablet or your laptop, and your laptop says, "Here are six different wireless networks within your range of reception. Which one do you want to connect to?" Well, the names of those networks are the SSIDs being broadcast by those wireless access points.

You also need the traditional network details, like the IP address, the gateway router IP address, the network mask of the network. The wireless access point does work on a Layer 3 part of the stack, just as it also works on Layer 2 for the Wi-Fi component of it. But because it works on Layer 3 to route packets back and forth and to address packets, it needs network information just like a computer would.

So clients can connect to that wireless network in one of two ways. The most common way is to passively listen for a broadcast from that wireless access point. So when we go to Starbucks and we open up our laptop and we see the list of wireless access points we can connect to, the reason we see that list of names is because those wireless access points are broadcasting broadcast packets that say, "I'm here. Here's my beacon." They're called beacon packets. "Here's my beacon. Here's the name of my SSID. Here's the name of my network. And oh, by the way, if I happen to be using some encryption, here's the type of encryption I'm using."

Now, there are ways to make your wireless network-- I won't say hidden, because there are plenty of tools out there that allow you to find networks that aren't broadcasting beacons-- but maybe less-- or maybe more subtle. You can make your wireless network more subtle by turning off those beacon packets. And if you turn off those beacon packets, when you open up your laptop and you see the list of wireless networks to connect to, you won't see that network, because there's no broadcast beacon being transmitted from that WAP saying, "Here I am, here I am. Connect to me."

In order to connect to a network that is not broadcasting beacons, you have to know the information ahead of time, the same information you would get in a beacon broadcast-- things like: What is the SSID of this network I want to connect to? What is the encryption type it's using? Then of course if it's using encryption, what is the shared key to connect to it, or the authentication I need to connect to it? So you can connect to a wireless network that's not broadcasting beacons, but you have to know it's there and you have to know what its name is.

Setting Up A Wireless Network -2

Device placement

- What area do you need to cover?
- Does the signal need to radiate in all directions or follow a specific path?

Signal strength

- If signal exceeds size of space
  - The signal can bleed out causing a security risk
- If space exceeds size of signal
  - A signal booster may be necessary or multiple WAPs must be used

**011 So, when we're setting up a wireless network, we want to think about where we're placing our WAPs. Where physically in the environment are we placing these things?

Because, remember, in most cases, they're broadcasting omnidirectionally from the WAP in all directions, and we have to think about what area do we want to cover, where do we want this signal available from, and are there physical obstructions or electromagnetic interference or other RF interference in the way that's going to reduce the strength of the signal or interfere with the signal, and we need to compensate for that

by either physically moving the wireless access point or by adding repeaters or other wireless access points to get our signal through there.

So, signal strength plays a big part, and your wireless access points, by default, generally are going to come with the signal full-blast. In other words, just like a stereo when you come out of the box, but that stereo's got the volume turned all the way up. So as soon as you plug it in the wall, it's going to blast music because the volume's all the way up.

So too a wireless access point. Normally when you plug it in, it's got its power setting set to its highest possible power because it wants to provide the greatest possible signal that it can out of that access point. But most access point management software will allow you to turn that signal down if you want to. Of course, if you need more signal, because your space is too great or you've got too much interference, then you need to boost that signal with things like wireless repeaters or more wireless access points.

SSID (Service Set Identifier)

SSID (Service Set Identifier)

A unique identifier that wireless networking devices use to establish and maintain connectivity

Defined on a per-network basis

- All clients participating in the network use the SSID

Security concerns arise when the default values are used

- Usually indicates other settings have not been changed either

Beacon frames, sent out by access points and clients, broadcast the SSID helping clients locate and connect to available networks.

- When beacon frames are turned off, the SSID is not broadcast.
  - Usually done in a weak attempt at security through obscurity as the SSID can be easily found through other traffic using the wireless network

CERT | Software Engineering Institute | Carnegie Mellon 12

**012 So let's a little bit more about SSIDs, the service set identifier--again, is the name of that network. Every network, every unique wireless network you want to connect to, has to have an SSID. And all clients that connect on that wireless network have to know what that SSID is. Now, generally they know what it is because the wireless access points are broadcasting that beacon packet, like I said, telling everybody what it is. But if they're not broadcasting the beacon, they can still be connected to if you know what that information is and you set it up in your wireless client first.

So, beacon frames, like I said, are sent out from the access point in order to inform clients in the area, "Hey, I'm here. Here's the name of my SSID. You can connect to me. Here's the type of encryption I'm using."

Wireless Authentication -1

Wireless Authentication -1

Authentication on access points usually uses a pre-shared key (a password that both the access point and the client know), or if none is set, by MAC address.

- Pre-shared key systems are difficult to deploy, manage, and control. They have no accountability and are susceptible to attack.

Authentication may also be done by an external device, such as a RADIUS server.

A client associates with an access point once it passes authentication.

CERT | Software Engineering Institute | Carnegie Mellon 13

**013 So, what if I'm using encryption? Well, encryption involves some type of authentication first. Let's back up a second, because some wireless access points allow you to authenticate without encryption. Is that a good idea? Obviously not. If I'm communicating over an unbound media to a wireless access point, that means anybody

within the listening range of that signal can listen to my traffic going back and forth. So if my wireless access point is now requiring authentication but I'm not using any encryption, then whatever authentication credentials I send to it are going to be easily monitored and easily captured by anybody else listening.

Well, there are really two ways you can authenticate to a wireless access point. You can use some type of shared secret, some type of password-type authentication: Maybe the wireless access point has its own username and password database that it's set up. Maybe it's authenticating off of a third-party server, like a radius server or something. Or that wireless access point can be configured to authenticate via MAC address-- data-link layer, Layer 2 addressing, MAC address that each client has. You can configure that wireless access point to say, "Only allow these MAC addresses to connect to me. And if the client connecting to me is not one of these approved MAC addresses, don't allow it to connect."

Once again, what's the problem with that? MAC addresses, we talked about, can be spoofed. So I can, through the software, change what MAC address my client machine is using and use the same MAC address that I see you using-- because we're talking about an unbound media and I can monitor it-- and I see your MAC address is being allowed to

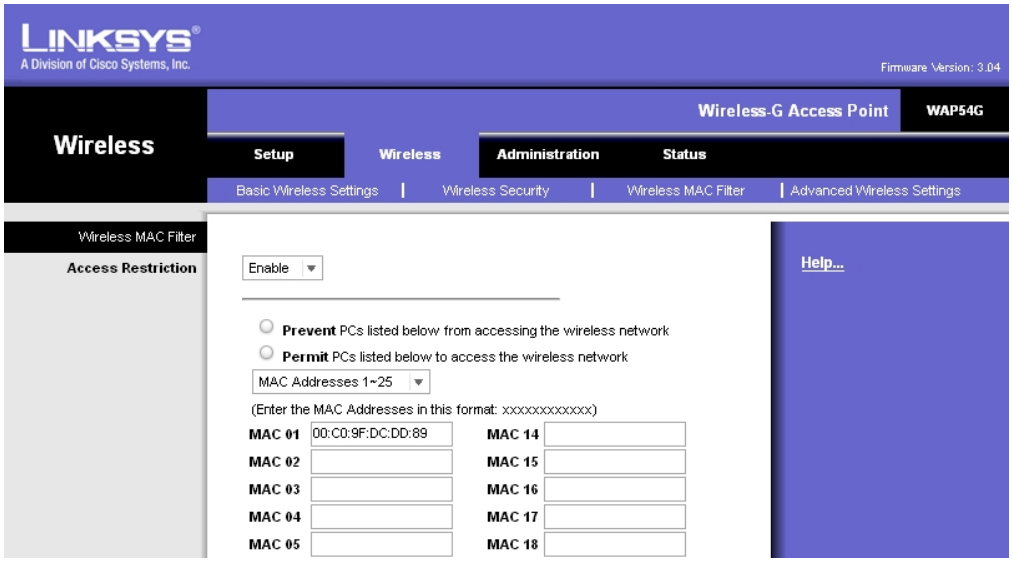
communicate with that wireless access point, so I change my MAC address to use it as well.

So there's no really good reason to authenticate without encryption, so how do we add encryption to it? Well, we'll talk about that later in the topic.

Wireless Authentication -2

Wireless Authentication -2

MAC address filtering with a Linksys WAP



**014 What you see in this example is a screenshot of a Linksys wireless access point and the configuration page for adding MAC-layer authentication. In this screen, you can add the MAC address of a known good client, and then this Linksys wireless access point would only allow that MAC address to connect to it.

This is really good and bad. It's good because at least it's a layer of security. Obviously it's not the only layer of security you'd want to use, but it's a layer. It's bad between it's a management nightmare, especially in a wireless network where you may have people coming on and off your network all the time. You may have guest users that you want to allow to have access to it, but you don't know what their MAC address is. You may have machines that leave the environment and will no longer use it, and now you've got to go into this list and take out those old MAC addresses so they don't get stale. So every time you've got a new device, a new client that wants to connect to the network, you've got to update this list. So that becomes a bit of a management nightmare. But, again, it's a layer of security.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP)

Sep. 1999, referred to as static or manual WEP

Created in attempt to give wireless users same security as wired users

RC4 stream cipher (2 flavors)

- 64-bit WEP: 40-bit key + 24-bit initialization vector (IV)
- 128-bit WEP: 104-bit key + 24-bit IV
- Does not include a key management protocol
  - Single key shared amongst users

CRC-32 checksum

CERT | Software Engineering Institute | Carnegie Mellon 15

**015 So we said that we don't want authentication really without encryption. Well, what type of encryptions are available to me in the wireless world? In 1999 they came out with the first iteration, if you will, or the first try and putting an encryption on top of Wi-Fi signals, on top of wireless authentication. And the first try at it was called WEP, the Wired Equivalent Privacy. The idea was that they wanted to provide the same level of security in a wireless environment that you use in a wired environment, that wired users enjoyed. The problem they didn't implement it very well. It didn't take very long for WEP to be cracked.

And what I mean by cracked is the ability to-- because we're talking about an unbound media-- the ability to listen to users attempting to authenticate to this WEP-enabled wireless access point, and from what I'm listening to and what I'm hearing to them be able to reverse-engineer or figure out what that password is to connect to it.

So WEP used a shared key, a shared secret-- basically a password-- where if you knew what the password was for that wireless network and you typed it in and you connected to the wireless network, and now you had an encrypted signal back and forth.

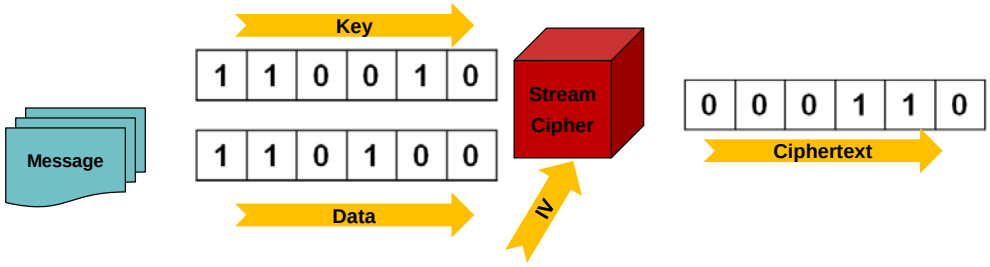
WEP Limitations

Pre-shared keys are used to encrypt packets; either 40 or 104 bits depending on pre-shared key setup.

An “initial value” (IV) of 24 bits is sent in plaintext.

Susceptible to plaintext attacks where the RC4 keystream can be reconstructed based on the IV and a known packet.

With about 24GB of space, an attacker can build a decryption table to decrypt WEP protected packets in real-time.



**016 But the problem was it had some limitations with it. It used a very, very limited set of what's called IVs, or initial values. And those initial values were supposedly a randomly-generated set of characters that was used as a key to encrypt the information before it was sent back and forth. Well, let's say I've got a key ring with 24 keys on it. How long is it going to take me to figure out which one of these keys opens that door? I only got to try 24 different ones. Shouldn't take me too long, even as a human. Imagine how fast a computer could crack that, right?

So with computers, you got to the point where I don't even need to try every key on the door anymore; I can create a data map, if you will, or a decryption table, that basically says, "If the key looks like this, it opens this lock. If the key looks like this, it opens this lock." And for every possible combination of IVs and keys, I could have an equivalent table that showed what the password actually decrypted to. And in 24 gigabytes of space, which-- come on, nowadays, what do our laptops come with? Five hundred gigabytes of space at least minimum-- 250 at least? So with 24 gigabytes of space, I could have a large table file that had every possible WEP password already decrypted. So all I had to do was turn on my wireless sniffer tool, watch for 5-10 seconds any traffic going across that wireless network, capture a couple of those initial values going across, compare it into my list of already-decrypted values, and know exactly what the key was in seconds.

So WEP was fairly easily cracked and cracked fairly quickly, and became really a joke. It was to the point where, "Why bother using it?"
So they tried to do a little bit better, and they came out with WPA.

Notices

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.

CERT | Software Engineering Institute | Carnegie Mellon