2011-08

Wireless (Security) Self-Test for fun, Presentation

Fulp, J.D.

Monterey, California: Naval Postgraduate School.

https://hdl.handle.net/10945/39509

Wireless (Security) Self-Test for fun

Presented by:
J.D. Fulp, CISSP-ISSEP
jdfulp@nps.edu
Senior Lecturer of Computer Science
Naval Postgraduate School (NPS)
Monterey, CA USA

Late Addition to the Workshop!

- Hey... I just want to attend and listen/learn!

Late Addition to the Workshop!

- Hey... I just want to attend and listen/learn!
- Idea: Review a few related docs in order to be a more "sophisticated" listener/attendee

Late Addition to the Workshop!

- Hey... I just want to attend and listen/learn!
- Idea: Review a few related docs in order to be a more "sophisticated" listener/attendee
- New Idea (thanks John!): Present on what you found in these docs

Late Addition to the Workshop!

- Hey... I just want to attend and listen/learn!
- Idea: Review a few related docs in order to be a more “sophisticated” listener/attendee
- New Idea (thanks John!): Present on what you found in these docs
- Modification to the New Idea: The docs mostly read with the excitement of an encyclopedia, and are likely known by these “select” attendees, so...

Late Addition to the Workshop!

- Hey... I just want to attend and listen/learn!
- Idea: Review a few related docs in order to be a more “sophisticated” listener/attendee
- New Idea (thanks John!): Present on what you found in these docs
- Modification to the New Idea: The docs mostly read with the excitement of an encyclopedia, and are likely known by these “select” attendees, so...
- Present in a Q&A form to assess knowledge and perhaps “incite” discussion

Which “related docs” ?

- DoDD 8100.2
  - Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
- NIST SP800-124
  - Guidelines on Cell Phone and PDA Security
- DISA STIG
  - Wireless Overview
- DISA STIG
  - Mobile and Wireless Device Addendum to the Wireless STIG

What KIND of Questions?

- Miscellaneous Wireless Terms/Technology
- Security: Threats
- Security: Vulnerabilities
- Security: Security_Controls
- Security: Policy
- Security: Best Practices
- Security: Technology

- By the way... don’t expect any special “ordering” of any of this!

Misc Wireless Terms/Technology

- ✂What does WiFi stand for?

Misc Wireless Terms/Technology

✂What does WiFi stand for?

Wireless Fidelity

Misc Wireless Terms/Technology

- ✂Which term applies to Bluetooth?
  a. WMAN
  b. WGAN
  c. WPAN
  d. WLAN

Misc Wireless Terms/Technology

✂Which term applies to Bluetooth?

a. WMAN
b. WGAN
c. WPAN
d. WLAN

Misc Wireless Terms/Technology

- Which operates at 5GHz?
  a. 802.11a
  b. 802.11b
  c. 802.11g
  d. 802.11n

Misc Wireless Terms/Technology

- Which operates at 5GHz?
  a. 802.11a
  b. 802.11b
  c. 802.11g
  d. 802.11n

Misc Wireless Terms/Technology

- What is IEEE 802.16 ?
  - a. WiMAX
  - b. ZigBee
  - c. EDGE
  - d. Bluetooth

Misc Wireless Terms/Technology

- What is IEEE 802.16 ?
  a. WiMAX
  b. ZigBee
  c. EDGE
  d. Bluetooth

Misc Wireless Terms/Technology

- Who uses CDMA based cell tech.?
  a. Verizon
  b. AT&T

Misc Wireless Terms/Technology

- Who uses CDMA based cell tech.?
  a. Verizon
  b. AT&T

Misc Wireless Terms/Technology

- Which is the shortest range RF tech?
  a. 802.11
  b. Vicinity RFID (smart card/chip)
  c. WiMAX
  d. Proximity RFID (smart card/chip)

Misc Wireless Terms/Technology

- ✂ Which is the shortest range RF tech?
  a. 802.11
  b. Vicinity RFID (smart card/chip)
  c. WiMAX
  d. Proximity RFID (smart card/chip)

Misc Wireless Terms/Technology

- The two main 802.11 “modes” are Ad Hoc mode and...

Misc Wireless Terms/Technology

- The two main 802.11 “modes” are Ad Hoc mode and...

Infrastructure mode

Misc Wireless Terms/Technology

- The “Evil Twin” threat is aka...
  a. A promiscuous eavesdropper
  b. An RF-jammer box
  c. “War-driving” setup
  d. a rogue wireless access point

Misc Wireless Terms/Technology

- The “Evil Twin” threat is aka...
  a. A promiscuous eavesdropper
  b. An RF-jammer box
  c. “War-driving” setup
  d. a rogue wireless access point

Misc Wireless Terms/Technology

- Which is THE DoD IA Directive?
  a. 8200.1
  b. 8500.1
  c. 8510.01
  d. 5200.40

Misc Wireless Terms/Technology

- Which is THE DoD IA Directive?
  a. 8200.1
  b. 8500.1
  c. 8510.01
  d. 5200.40

Misc Wireless Terms/Technology

- Which is the correct ordering for typical operating range?
  a. IrDA—Bluetooth—802.11—WiMax--GSM
  b. 802.11—IrDA—GSM—Bluetooth—WiMAX
  c. Bluetooth—802.11—IrDA—WiMAX—GSM
  d. GSM—IrDA—Bluetooth—802.11--WiMAX

Misc Wireless Terms/Technology

✂ Which is the correct ordering for typical operating range?

a. IrDA—Bluetooth—802.11—WiMax--GSM

b. 802.11—IrDA—GSM—Bluetooth—WiMAX

c. Bluetooth—802.11—IrDA—WiMAX—GSM

d. GSM—IrDA—Bluetooth—802.11--WiMAX

Misc Wireless Terms/Technology

- ✂Most Cell phones operate in the...
  a. HF range (3-30MHz)
  b. HF and VHF range (3-300MHz)
  c. UHF range (300MHz-3GHz)
  d. SHF range (3-30GHz)

Misc Wireless Terms/Technology

- Most Cell phones operate in the...
  a. HF range (3-30MHz)
  b. HF and VHF range (3-300MHz)
  c. UHF range (300MHz-3GHz)
  d. SHF range (3-30GHz)

Misc Wireless Terms/Technology

- Which is the closest to typical longest operating range of WiMAX?

a. 1 mile

b. 5 miles

c. 30 miles

d. 100 miles

Misc Wireless Terms/Technology

- Which is the closest to typical longest operating range of WiMAX?
  a. 1 mile
  b. 5 miles
  c. 30 miles
  d. 100 miles

Misc Wireless Terms/Technology

- Which is the closest to typical longest operating range of Bluetooth?
  a. 1 meter
  b. 10 meters
  c. 100 meters
  d. 1 mile

Misc Wireless Terms/Technology

- Which is the closest to typical longest operating range of Bluetooth?
  a. 1 meter
  b. 10 meters (most often seen/quoted)
  c. 100 meters (mentioned in Wireless STIG)
  d. 1 mile

8100.2

- What's a PIM, PED, PDA?

8100.2

- What’s a PIM, PED, PDA?

  Personal Information Mgr

  Personal Electronic Device

  Personal Digital Assistant

8100.2

- Which does 8100.2 apply to?
  a. Receive-only pagers
  b. GPS receivers
  c. Implanted medical devices
  d. RF energy between RFID tags

Section 2.5

8100.2

- ✂ Which does 8100.2 apply to?

None of these

Section 2.5

8100.2

- Exceptions/deviations from required security controls usually (always?) require the approval of the DAA. What is a DAA?

Section 4.1.2

8100.2

- Exceptions/deviations from required security controls usually (always?) require the approval of the DAA. What is a DAA?

Designated Approving Authority

Section 4.1.2

8100.2

✂ Which pub is heavily referenced for security issues related to crypto-graphic module validation?

a. FIPS 199
b. DCID 6/9
c. FIPS 140-2
d. NSTISSI 4009

8100.2

- Which pub is heavily referenced for security issues related to cryptographic module validation?

a. FIPS 199

b. DCID 6/9

c. FIPS 140-2

d. NSTISSI 4009

8100.2

- Measures taken to mitigate DoS attacks should address?

a. Only external threats

b. Only internal threats

c. Potential “friendly interference”

d. All of the above

Section 4.1.4

8100.2

- Measures taken to mitigate DoS attacks should address?
  a. Only external threats
  b. Only internal threats
  c. Potential “friendly interference”
  d. All of the above

Section 4.1.4

8100.2

- The term (title) CTTA pops up often when discussing wireless *emissions* and security. What is CTTA?

a. Certified TEMPEST Technical Authority

b. Communications TecSec Tech. Auth.

c. Counter-technical Transmission Analyst

d. Consolidated TEMPEST Testing Agency

Section 4.3

8100.2

- The term (title) CTTA pops up often when discussing wireless *emissions* and security. What is CTTA?

a. Certified TEMPEST Technical Authority

b. Communications TecSec Tech. Auth.

c. Counter-technical Transmission Analyst

d. Consolidated TEMPEST Testing Agency

Section 4.3

8100.2

- ✂What is the DITSCAP?

Section 4.5

8100.2

- What is the DITSCAP?

DoD Information Technology Security Certification and Accreditation Process

Section 4.5

8100.2

✂(T/F) DoD component must actively screen for wireless devices [including] active e-m sensing at the premises to detect/prevent unauthorized access of DoD ISs... to ensure compliance with DITSCAP ongoing accreditation.

Section 4.5

8100.2

- (T/F) DoD component must actively screen for wireless devices [including] active e-m sensing at the premises to detect/prevent unauthorized access of DoD ISs... to ensure compliance with DITSCAP ongoing accreditation.

Section 4.5

8100.2

- ✂PEDs that are connected directly to a DoD-wired network (e.g., hot-sync to a workstation) (shall / shall-not) be permitted.

Section 4.7

8100.2

- PEDs that are connected directly to a DoD-wired network (e.g., hot-sync to a workstation) (shall / shall-not) be permitted.

Insufficient input... what additional info do you think we need to answer this?

Section 4.7

8100.2

- PEDs that are connected directly to a DoD-wired network (e.g., hot-sync to a workstation) (shall / shall-not) be permitted to operate wirelessly while directly connected.

Section 4.7

8100.2

- ✂ PEDs that are connected directly to a DoD-wired network (e.g., hot-sync to a workstation) (shall / shall-not) be permitted to operate wirelessly while directly connected.

Section 4.7

Wireless STIG Overview

- When discussing/categorizng vulnnerabilities, the term CAT is used. What is CAT short for?

Section 1.4

Wireless STIG Overview

- When discussing/categorizng vulnerabilities, the term CAT is used. What is CAT short for?

Severity Category Code

Section 1.4

Wireless STIG Overview

- If analysis of your system reveals a CAT I severity...

a. You can still receive an ATO

b. To get an ATO, this must be mitigated.

c. You may have <= 1 CAT I and still get an ATO

d. You cannot get an ATO with even a single CAT I severity

Section 1.4

Wireless STIG Overview

- If analysis of your system reveals a CAT I severity...

a. You can still receive an ATO

b. To get an ATO, this must be mitigated.

c. You may have <= 1 CAT I and still get an ATO

d. You cannot get an ATO with even a single CAT I severity

Section 1.4

Wireless STIG Overview

- CAT codes are also used to characterize attackers/threats. How is each defined?
  a. CAT 1
  b. CAT 2
  c. CAT 3

Section 1.4

Wireless STIG Overview

- ✂CAT codes are also used to characterize attackers/threats. How is each defined?

a. CAT 1-no special skill/resource required

b. CAT 2-some sp s/r or mux-exploitations required

c. CAT 3-requires unusual expertise, additional information, and/or mux-exploitations

Section 1.4

Wireless STIG Overview

- Two types of WLAN APs may be used in a DoD network: enclave-NIPRNet Connected, and Internet Gateway Only Connected. What's the difference?

Section 2.2.1

Wireless STIG Overview

- Two types of WLAN APs may be used in a DoD network: Enclave-NIPRNet Connected, and Internet Gateway Only Connected. What’s the difference? Enclave provides connectivity to the inside network, whereas Gateway provides a connection to the Internet only

Wireless STIG Overview

✂Which WAP devices are currently apvd for class'd WLAN comms?

a. SecNet11 (Harris Corp.)

b. SecNet54 (Harris Corp.)

c. KOV-26 Talon (L3 Communications)

Section 2.2.4

Wireless STIG Overview

✂Which WAP devices are currently apvd for class’d WLAN comms?

a. SecNet11 (Harris Corp.)

b. SecNet54 (Harris Corp.)

c. KOV-26 Talon (L3 Communications)

Section 2.2.4

Wireless STIG Overview

- To what level of classification?

a. SecNet11 (Harris Corp.)

b. SecNet54 (Harris Corp.)

c. KOV-26 Talon (L3 Communications)

Section 2.2.4

Wireless STIG Overview

- To what level of classification?
  a. SecNet11 (Harris Corp.) **- S**
  b. SecNet54 (Harris Corp.) **- TS**
  c. KOV-26 Talon (L3 Communications) **- TS**

Section 2.2.4

Wireless STIG Overview

- What's a WIDS?

Section 2.2.4

Wireless STIG Overview

- What’s a WIDS?

Wireless Intrusion Detection System

Section 2.2.4

Wireless STIG Overview

- ZigBee is closest in “mission” to?
  a. RFID
  b. Bluetooth
  c. 802.11
  d. WiMAX

Section 2.5

Wireless STIG Overview

- ZigBee is closest in “mission” to?
  a. RFID
  b. Bluetooth
  c. 802.11
  d. WiMAX

Section 2.5

Wireless STIG Overview

- Which best describes the difference between ZigBee & Bluetooth?
  a. ZigBee uses less power (better battery life)
  b. ZigBee has lower data rate
  c. ZigBee used for device-device comms whereas Bluetooth is used for human interface devices
  d. ZigBee is not used by DoD

Section 2.5

Wireless STIG Overview

- Which best describes the difference between ZigBee & Bluetooth?
  a. ZigBee uses less power (better battery life)
  b. ZigBee has lower data rate
  c. ZigBee used for device-device comms whereas Bluetooth is used for human interface devices
  d. ZigBee is not used by DoD

Section 2.5

Wireless STIG Overview

- Cellular...are generally considered (more / less) secure than public WLAN or WiMAX...and should be preferred by DoD sites for wireless remote access to DoD networks.

Section 2.7

Wireless STIG Overview

- Cellular...are generally considered (more / less) secure than public WLAN or WiMAX...and should be preferred by DoD sites for wireless remote access to DoD networks.

Section 2.7

Wireless STIG Overview

- A recent study reported over ____% of wireless devices identified during a wireless scan at several U.S. airports to be illegitimate (i.e., not part of the airport sanctioned wireless network)

Section 2.7

Wireless STIG Overview

- A recent study reported over **50** % of wireless devices identified during a wireless scan at several U.S. airports to be illegitimate (i.e., not part of the airport sanctioned wireless network)

Whoa!

Section 2.7

SP800-124

- ✂Basically, what is 1G cellular?
    a. < 100kbps
    b. Analog
    c. Digital (voice only, no data)
    d. TDMA (vice CDMA)

Section 2.5

SP800-124

- Basically, what is 1G cellular?
  a. < 100kbps
  b. Analog
  c. Digital (voice only, no data)
  d. TDMA (vice CDMA)

Section 2.5

SP800-124

- ✂Which are the two dominant digital cellular networks in the U.S.?

a. iDEN
b. TDMA
c. CDMA
d. GSM

SP800-124

✂ Which are the two dominant digital cellular networks in the U.S.?

a. iDEN

b. TDMA

c. CDMA

d. GSM

SP800-124

- Indicate GSM or CDMA regarding these “evolutionary” enhancements

   a. EDGE
   b. 1xRTT
   c. EV-DO
   d. UMTS

Section 2.5

SP800-124

- Indicate GSM or CDMA regarding these “evolutionary” enhancements
  a. EDGE -- GSM
  b. 1xRTT -- CDMA
  c. EV-DO -- CDMA
  d. UMTS -- GSM

Section 2.5

SP800-124

- What does SIM stand for, and in which cell system (GSM or CDMA) do we find it?

Section 2.2.2

SP800-124

- ✂What does SIM stand for, and in which cell system (GSM or CDMA) do we find it?

Subscriber Identity Module, GSM

Section 2.2.2

SP800-124

- ✂What is the primary purpose of the SIM?

Section 2.2.2

SP800-124

- ✂ What is the primary purpose of the SIM?

Authenticates the phone to the netowork

Section 2.2.2

SP800-124

- The IMSI is the # in the SIM which uniquely identifies the phone. What is IMSI?

Section 2.2.2

SP800-124

- ✂The IMSI is the # in the SIM which uniquely identifies the phone. What is IMSI?

International Mobile Subscriber Identity

Section 2.2.2

SP800-124

- ✂ Is SIM-like functionality on the horizon for CDMA networks?

Section 2.2.2

SP800-124

- ✂ Is SIM-like functionality on the horizon for CDMA networks?

Yes, one such reference is to a R-UIM (Removable – User Identity Module)

Section 2.2.2

SP800-124

- ✂With respect to the discussion of keys and key strength (entropy), what is the distinction between an *on-line* and an *off-line* attack?

SP800-124

- With respect to the discussion of keys and key strength (entropy), what is the distinction between an *on-line* and an *off-line* attack?
  - *On-line*: attacker is "bruting" via the device's primary/intended secret entry interface
  - *Off-line*: attacker is "bruting" directly to the device; bypassing the normal/intended interface

SP800-124

- Short (4-8 digits) PINs are often criticized as insufficient to thwart a guessing attack. What added security mechanism can mitigate the risk of such small PIN spaces?

SP800-124

- Short (4-8 digits) PINs are often criticized as insufficient to thwart a guessing attack. What added security mechanism can mitigate the risk of such small PIN spaces?

For on-line attacks, only permit a small number of incorrect guesses

Mobile & Wireless Device Addendum

- When discussing IA security controls, we typically chose them based upon the confidentiality level and MAC of the information on the system in question. What is MAC?

Section 1.2

Mobile & Wireless Device Addendum

- When discussing IA security controls, we typically chose them based upon the confidentiality level and MAC of the information on the system in question. What is MAC?

  Mission Assurance Category

Section 1.2

Mobile & Wireless Device Addendum

- How does the MAC relate to the CIA Triad of Confidentiality, Integrity, and Availability?

Section 1.4

Mobile & Wireless Device Addendum

- How does the MAC relate to the CIA Triad of Confidentiality, Integrity, and Availability?
  - It’s a combination of the Integrity and Availability (MAC1=HH, MAC2=HM, and MAC3=BB)

Section 1.4

Mobile & Wireless Device Addendum

- 7 areas are addressed in this addendum for security guidelines

1 OS Security

2 ___________ Security

3 Transmission Protection

4 ___________ (emanations) Security

5 Access Control

6 Data Protection

7 User Training

Section 4.1

Mobile & Wireless Device Addendum

✂ 7 areas are addressed in this addendum for security guidelines

1 OS Security
2 Application Security
3 Transmission Protection
4 TEMPEST (emanations) Security
5 Access Control
6 Data Protection
7 User Training

Section 4.1

Mobile & Wireless Device Addendum

- One big issue with OS security is the notion of a separation kernel. What is the purpose of a separation kernel?

Section 4.1.1

Mobile & Wireless Device Addendum

- One big issue with OS security is the notion of a separation kernel. What is the purpose of a separation kernel?

  Basically; a) protect against possible high-to-low (data flows) and b) separate subjects and objects so that access must be granted IAW a policy-enforcing mechanism

Mobile & Wireless Device Addendum

- When the topic of access control arises, we often see a reference to AAA. What is AAA?

Section 4.1.5

Mobile & Wireless Device Addendum

- ✂When the topic of access control arises, we often see a reference to AAA. What is AAA?

  Authenticate, Authorize, Audit

Section 4.1.5

Mobile & Wireless Device Addendum

- Regarding the area of data protection, we often hear about DAR and FDE. What is each of these?

Data-At-Rest and Full-Disk Encryption. The idea is that we are beginning to pay attention to encrypting data at-rest in addition to data in-transit; which we have been doing for quite a long(er) time.

Mobile & Wireless Device Addendum

- What is the necessary precursor to access control?
  a. authorization decision
  b. audit solution
  c. I&A
  d. object classification

Section 2.5

Mobile & Wireless Device Addendum

- What is the necessary precursor to access control?

a. authorization decision

b. audit solution

c. I&A (Identification & Authentication)

d. object classification

App. D (Security Mechanisms)

Mobile & Wireless Device Addendum

- What are the 3 methods used to authenticate (i.e., prove and identity claim)?

a. What you _________

b. What you _________

c. What you _________

App. D

Mobile & Wireless Device Addendum

- What are the 3 methods used to authenticate (i.e., prove and identity claim)?
  a. What you know
  b. What you have
  c. What you are

App. D.1

Mobile & Wireless Device Addendum

- When you get down to brass tacks... they're all have forms. The real distinction is...

a. ______________________________

b. ______________________________

Mobile & Wireless Device Addendum

- When you get down to brass tacks... they’re all have forms. The real distinction is...

  a. whether it’s a unique & permanent part of you (biometric), or

  b. whether it is a secret (in which case it will either be one of public or private)

Mobile & Wireless Device Addendum

✂As usual (INFOSEC) we are ultimate-ly concerned with protecting the CIA of the wireless information. What are the two main tools to protect the C and I ?

a. ____________ Security (think low tech)

b. ______________(hashing and encryption)

Mobile & Wireless Device Addendum

- As usual (INFOSEC) we are ultimate-ly concerned with protecting the CIA of the wireless information. What are the two main tools to protect the C and I ?

  a. Physical Security (think low tech)

  b. Cryptography (hashing and encryption)

Mobile & Wireless Device Addendum

✂What are the 3 primary encryption algorithms approved for use (2 are symmetric and 1 is asymmetric)?

a. ______

b. ______

c. ______

Mobile & Wireless Device Addendum

- What are the 3 primary encryption algorithms approved for use (2 are symmetric and 1 is asymmetric)?

a. DES (Date Encryption Std, older)

b. AES (Advanced Encryption Std, newer)

c. RSA (the asymmetric one)

Mobile & Wireless Device Addendum

- ✂What are the 2 primary hash algorithms approved for use to support integrity check mechanisms?
  a. ______
  b. ______

Mobile & Wireless Device Addendum

- What are the 2 primary hash algorithms approved for use to support integrity check mechanisms?
  a. MD5 (Message Digest 5, 128 bits)
  b. SHA (Secure Hash Algorithm, comes in 160, 224, 256, 384, and 512 bit versions)

Mobile & Wireless Device Addendum

- For secret-based authentication that's easier to setup, we generally employ _____; whereas for secret-based authentication that's more scalable, we generally employ _____.

Choices are: a) PKI, b) biometrics, or c) pre-shared (symmetric) secrets

Mobile & Wireless Device Addendum

- For secret-based authentication that’s easier to setup, we generally employ ___a_; whereas for secret-based authentication that’s more scalable, we generally employ _c_.

Choices are: a) PKI, b) biometrics, or c) pre-shared (symmetric) secrets

Mobile & Wireless Device Addendum

- AES has three key lengths, 128, 192, and 256. Which are appropriate for secret information, and which for top secret?

a. Secret: ___________

b. Top Secret: ___________

Mobile & Wireless Device Addendum

- AES has three key lengths, 128, 192, and 256. Which are appropriate for secret information, and which for top secret?
  a. Secret: all three
  b. Top Secret: only 192 and 256

Mobile & Wireless Device Addendum

- Which of these 3 WiFi security technologies (protocols) is approved for DoD use?

  a. WEP

  b. WPA-TKIP

  c. 802.11i

App. D

Mobile & Wireless Device Addendum

✂Which of these 3 WiFi security technologies (protocols) is approved for DoD use?

a. WEP
b. WPA-TKIP
c. 802.11i

App. D

Mobile & Wireless Device Addendum

- 802.11i is perhaps more commonly know as ________?

Mobile & Wireless Device Addendum

- 802.11i is perhaps more commonly know as WPA2, and also RSN (Robust Security Network)?

  This uses the stronger (and FIPS 140-2 approved) AES cipher whereas WEP and WPA(1) use the weaker RC4 stream cipher

Mobile & Wireless Device Addendum

- Two methods of “RF Monitoring” (for wireless networks) are discussed. One is to employ a “roving” sniffer; what do you think is the other?

Mobile & Wireless Device Addendum

- Two methods of “RF Monitoring” (for wireless networks) are discussed. One is to employ a “roving” sniffer; what do you think is the other?

  Install wireless sensors at various locations (to cover all RF “space”) on the network and have them report back to a central management/monitor console

Mobile & Wireless Device Addendum

- Which attack is the most serious in terms of potential for damage?
  a. sniffing/observation
  b. data modification (blind)
  c. data replay (or impersonation)
  d. denial of service
  e. man-in-the-middle

Mobile & Wireless Device Addendum

✂ Which attack is the most serious in terms of potential for damage?

a. sniffing/observation

b. data modification (blind)

c. data replay (or impersonation)

d. denial of service

e. man-in-the-middle

Mobile & Wireless Device Addendum

- EAP comes in several different "flavors" and is an important security tool for wireless environments. What does EAP stand for?

Mobile & Wireless Device Addendum

- ✂EAP comes in several different “flavors” and is an important security tool for wireless environments. What does EAP stand for?

  Extensible Authentication Protocol (basically a “meta-protocol” that employs secrets to authenticate via a dedicated authentication server)

Mobile & Wireless Device Addendum

- Most/all wireless security best practices say to disable SSID. What is SSID and why should it be disabled?

Mobile & Wireless Device Addendum

✂IPSec is a popular layer-3 VPN. Which mode should be used if the tunnel endpoints should begin and end at/on two communicating hosts?

a. Tunnel mode

b. Transport mode

c. AH mode

d. ESP mode

Mobile & Wireless Device Addendum

✂IPSec is a popular layer-3 VPN. Which mode should be used if the tunnel endpoints should begin and end at/on two communicating hosts?

a. Tunnel mode

b. Transport mode

c. AH mode

d. ESP mode

Mobile & Wireless Device Addendum

- Which mode of IPSec should be used if we wish to provide confidentiality?

  a. Tunnel mode

  b. Transport mode

  c. AH mode

  d. ESP mode

Mobile & Wireless Device Addendum

✂ Which mode of IPSec should be used if we wish to provide confidentiality?

a. Tunnel mode

b. Transport mode

c. AH mode

d. ESP mode

FINISHED