




# WIRELESS SECURITY

Rupam Bhattacharya



# Whoami?

- Security Researcher
- Head of Offensive Security Practice at Spectrami
- Twitter – ru94mb

# Wireless Security?

- Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks.
- The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).
- The current standard is WPA2.
- For organization WPA2 Enterprise is recommended.

# WEP?

- Wired Equivalent Privacy
- Developed in the late 1990s as the first encryption algorithm for the 802.11 standard.
- Weaknesses identified in 2001.
- PCI DSS prohibits using WEP in 2009 after large scale attacks.
- Easily hacked due to its 24 bit initialization vector (IV) and weak authentication.
- RC4 stream cipher.
- Stream Cipher – It converts plaintext into cyphertext in a bit-by-bit fashion.
- The standard originally specified a 40-bit, preshared encryption key.



# WPA

- Wi-Fi Protected Access
- In 2003, the Wi-Fi Alliance released WPA as an interim standard
- Two modes - WPA-EAP and WPA-PSK
- Also based on the RC4 cipher but with Temporal Key Integrity Protocol (TKIP) still a stream cipher.
- Use of 256-bit keys, per-packet key mixing
- Generation of a unique key for each packet
- Automatic broadcast of updated keys
- Message integrity check
- A larger IV size (48 bits) and mechanisms to reduce IV reuse

# WPA

- Was designed to be backward compatible with WEP
- The security provided was not robust enough
- Weak passwords can be easily cracked





# WPA2

- Wi-Fi Protected Access v2
- Introduced in 2004.
- Like its predecessor, WPA2 also offers enterprise and personal modes.
- WPA2 replaces the RC4 cipher and TKIP with Advanced Encryption Standard (AES) and Chaining Message Authentication Code Protocol (CCMP).
- CCMP checks for Authorization along with authentication.
- Uses cipher block chaining message authentication code to ensure message integrity.
- Block Cipher – It operates on the fixed-size blocks of data.
- Current Standard.
- Can still be hacked if weak passwords are used.



# References

- [https://www.w3schools.com/xml/xml\\_what\\_is.asp](https://www.w3schools.com/xml/xml_what_is.asp)
- [https://www.w3schools.com/xml/xml\\_dtd.asp](https://www.w3schools.com/xml/xml_dtd.asp)
- [https://www.owasp.org/index.php/Top\\_10-2017\\_A4-XML\\_External\\_Entities\\_\(XXE\)](https://www.owasp.org/index.php/Top_10-2017_A4-XML_External_Entities_(XXE))
- [https://www.owasp.org/index.php/XML\\_External\\_Entity\\_\(XXE\)\\_Processing](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)
- [https://www.owasp.org/index.php/XML\\_External\\_Entity\\_\(XXE\)\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet)