Security Overview of IEEE 802.11

Mrudula Putcha

Department Of Electrical Engineering & Computer Science
EECS 780 Term Paper Presentation

mputcha@eecs.ku.edu

http://people.eecs.ku.edu/~mputcha

Security Overview of IEEE 802.11

Abstract

Wireless LANs are replacing wired LANS almost everywhere. This is very natural because minus all the wires, they are much less cumbersome. However, being wireless, they have serious security issues, which are not associated with the wired medium.

In this presentation, I intend to cover the initial security measures provided for Wireless LANs, the significant flaws that were eventually discovered and how they were fixed, both temporarily in form of TKIP and permanently in form of the IEEE 802.11i standard.

Security Overview of IEEE 802.11
Outline

- The IEEE 802.11-1997
- Temporal Key Integration Protocol
- The IEEE 802.11i standard
- Security association with IEEE 802.11i
- Conclusion

Security Overview of IEEE 802.11

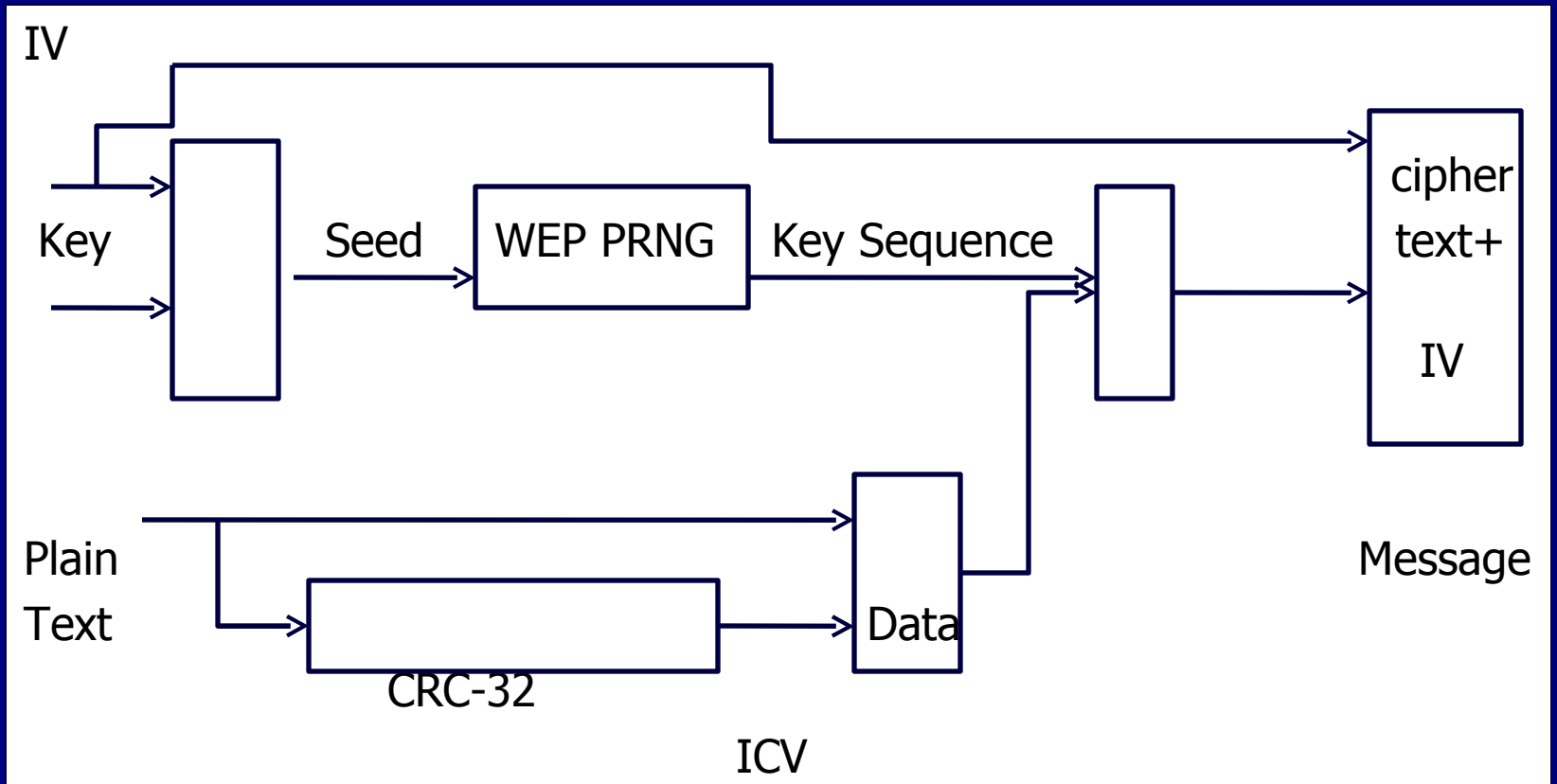
- The IEEE 802.11-1997
  - Authentication Procedures
  - Wired Equivalent Privacy
- Temporal Key Integration Protocol
- The IEEE 802.11i standard
- Security association with IEEE 802.11i
- Conclusion

Security Overview of IEEE 802.11

- Authentication in IEEE 802.11-1997 was either
  - Open System authentication which was the default
  - Shared key authentication
    - The distribution of keys was done using WEP
- Wired Equivalent Privacy
  - Privacy on par with wired medium subjectively
  - An attractive option because
    - Reasonably strong
    - Efficient and exportable
    - Optional

Security Overview of IEEE 802.11

Wired Equivalent Privacy



cite:The IEEE 802.11-1997 standard

Security Overview of IEEE 802.11
Wired Equivalent Privacy

- Weaknesses in WEP
  - Implementation of WEP was optional
  - The use of a 24 bit IV
  - The use of RC4 stream cipher
    - The FMS attack clearly demonstrated the weakness in WEP.

Security Overview of IEEE 802.11

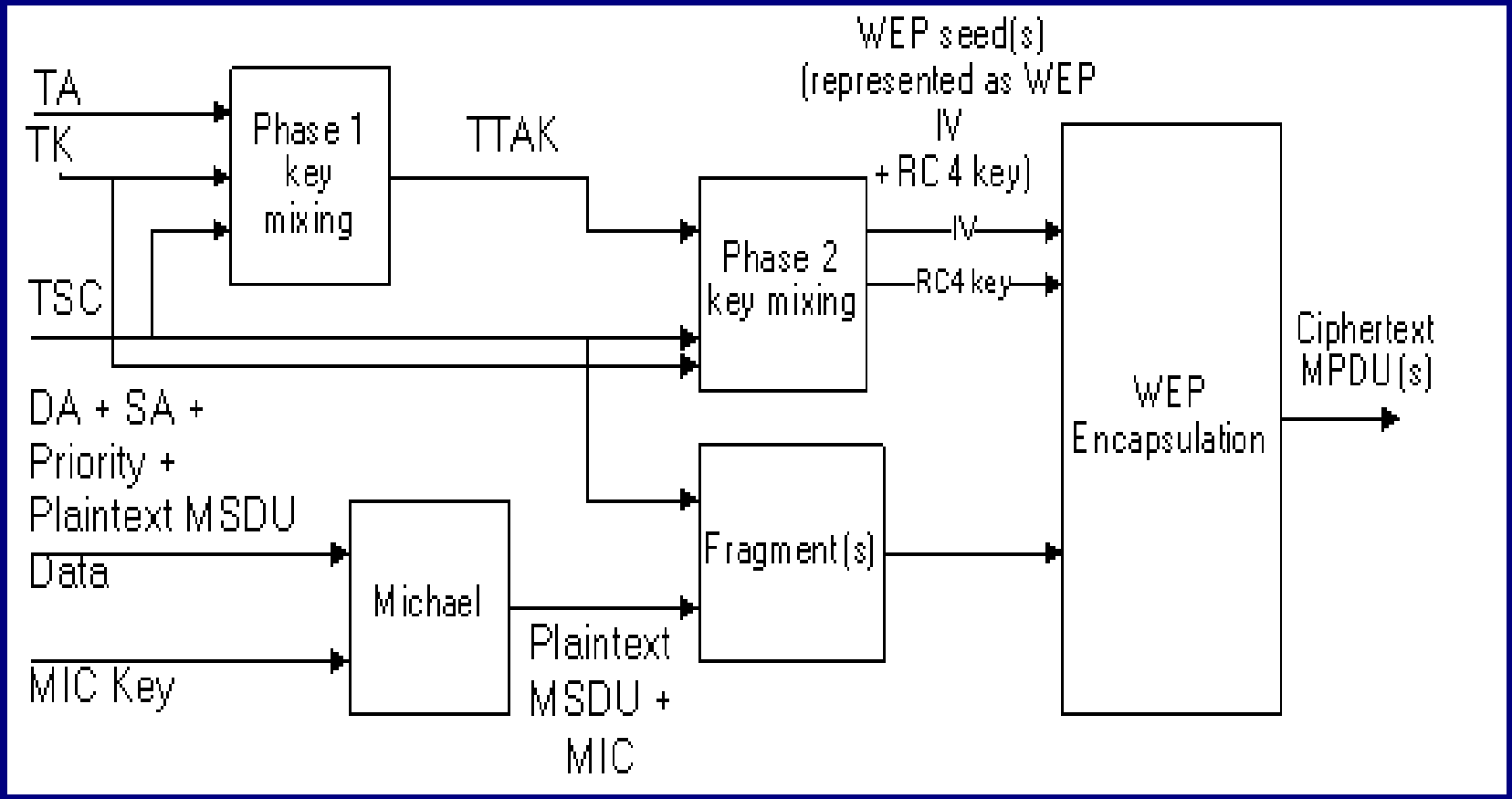
- The IEEE 802.11-1997
- Temporal Key Integration Protocol
  - Enhancement in security after TKIP
  - Weaknesses in TKIP
- The IEEE 802.11i standard
- Security association with IEEE 802.11i
- Conclusion

Security Overview of IEEE 802.11
Temporal Key Integration Protocol

- MIC calculated over SA, DA as well
- 48 bit sequence number used
- Fresh key generated for each message
- Countermeasures used when MIC faulty

Security Overview of IEEE 802.11

Temporal Key Integration Protocol



Security Overview of IEEE 802.11
Temporal Key Integration Protocol

- Weaknesses in TKIP
  - Knowledge of a few RC4 keys of consecutive packets
  - The temporal key can be computed using these
  - TKIP allows less than two faulty MICs in two min
  - Countermeasures come into play after this
  - All reception is stopped for sixty seconds
  - Ideal scenario for DoS attacks

Security Overview of IEEE 802.11

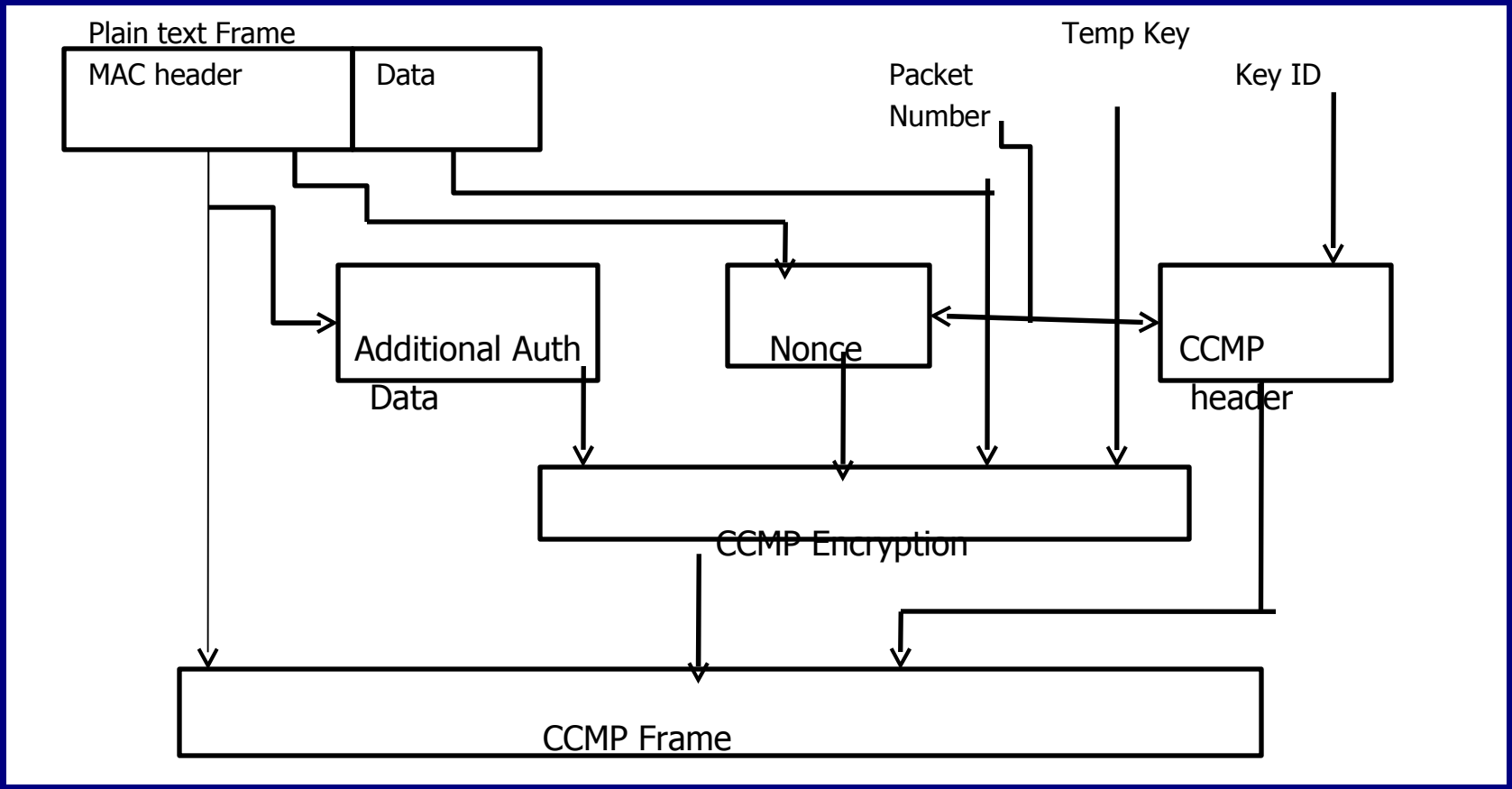
- The IEEE 802.11-1997
- Temporal Key Integration Protocol
- The IEEE 802.11i standard
- Security association with IEEE 802.11i
- Conclusion

Security Overview of IEEE 802.11
The IEEE 802.11i standard

- CCMP is used to protect data privacy
- Based on CCM of AES algorithm
  - Counter with CBC-MAC
  - CTR used for data integrity check and privacy
  - CBC-MAC for authentication
  - Encryption based on 128 bit AES algorithm
  - No weak keys identified with AES

Security Overview of IEEE 802.11

The IEEE 802.11i standard



Security Overview of IEEE 802.11

- The IEEE 802.11-1997
- Temporal Key Integration Protocol
- The IEEE 802.11i standard
- Security association with IEEE 802.11i
- Conclusion

Security Overview of IEEE 802.11

Security Association with IEEE 802.11i

- Setting up a secured channel to communicate
- Set of policies to protect information
- Port based network access control used
- EAP framework called EAPOL used
- Four different ways of authentication possible
- IEEE 802.1X is one of them

Security Overview of IEEE 802.11
Conclusion

- While WEP was considered a very attractive option initially, significant security flaws were discovered in it by 2001
- To support the legacy hardware TKIP was designed to be backward compatible and was an interim solution. By 2004, the IEEE 802.11i standard was ratified
- The Wi-Fi alliance markets the security measures based on this standard as WPA2 and they are a mandatory part of any device certified by the alliance

References

- Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. Security aws in802.11 data link protocols. *Commun*. ACM,46(5):35–39, 2003.
- Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of rc4. In *SAC '01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 1–24, London, UK, 2001. Springer-Verlag.
- Matthew S. Gast. 802.11 *Wireless networks-The Definitive Guide*. O'Reilly, 2005.
- S. Glass and V. Muthukkumarasamy. A study of the tkip cryptographic dos attack. pages 59–65, Nov. 2007.
- Russ Housley and William Arbaugh. Security problems in 802.11-based networks. *Commun*.ACM, 46(5):31–34, 2003.

References

- IEEE std 802.11-1997 information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specfic requirements-part 11: Wire-less LAN medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-1997*, pages i–445, Nov 1997.
- IEEE standard for local and metropolitan area networks port-based network access control. IEEE Std 802.1X-2004 (*Revision of IEEE Std 802.1X-2001*), pages 01– –69; 2004:
- IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE Std 802.11-2007 (*Revision of IEEE Std 802.11-1999*), pages C1{1184, 12 2007.

References

- VebjMoen, Havard Raddum, and Kjell J. Hole. Weaknesses in the temporal key hash of wpa. *SIGMOBILE Mob. Comput. Commun. Rev.*, 8(2):76–83,2004.
- A.E. Standard. FIPS 197. *National Institute of Standards and Technology*,2001.
- D. Whiting, R. Housley, and N. Ferguson. RFC 3610{Counter with CBC-MAC (CCM), IETF, 2003.

Questions?

Thank you!