

Week Four

Assignments

Prior to the next class, be sure to complete the readings specified in Table 1-1.

Source	Reading
Google Scholar	Intercepting Mobile Communications: The Insecurity of 802.11 [1] or Weaknesses in the Key Scheduling Algorithm of RC4 [2]
Fundamentals of Secure Computer Systems	Ch 9 Network Security Ch 10 Network Security Threats
Cryptography Decrypted	Ch 13 Hashes Ch 14 Message Digest Assurances Ch 15 Comparing Secret Key, Public Key, and Message Digests

Table 1-1 Readings Week Four

Download and read either of the above two papers concerning wireless communications. For your chosen paper:

Make a table of the WEP vulnerabilities that are reported in your chosen paper. In the first column, place the name of the vulnerability. In the second column, explain the vulnerability. Once you have completed the table, research a particular vulnerability. Then, briefly present and explain an attack or an exploit that would take advantage of that vulnerability.

Create an electronic version of the assignment. Post the assignment online. Later, it will become part of your online class project.

In your online journal, you have been reporting cryptographic related incidents. This week, please reflect upon those incidents and identify a cryptographic area that interests you. Reflect upon that area and compose a cryptographic express your interest in terms of a problem statement.

Please realize that your class project will propose a solution to that problem. Solutions are expected to utilize a FOSS cryptographic application. Specific solution software may be found on other LiveCDs.

Your essay should be brief. At a minimum, one paragraph should be devoted to a problem statement. Also write, at least, one paragraph explaining how appropriate use of cryptography could successfully mitigate that type of problem.

If possible, your journal should also include several annotated links to references to either the solution or the solution application utilized in your solution statement. Better assignments will include several references.

References

[1] Nikita Borisov, Goldberg, David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, download from:
<http://scholar.google.com/scholar?cluster=8004886276818658089&hl=en>

[2] Fluhrer, Mantin, and Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, download from:
<http://scholar.google.com/scholar?cluster=8935484402887010066&hl=en>