

Name:

Information Assurance: Homework 9 answers and comments

No due date. Answer key will be posted December 7. (or so).

1. One problem with WEP is that a linear CRC is used to detect changes to the packet. The CRC is encrypted with RC4.
 - a. Assume an attacker has changed the first byte of the packet. He does not know the key sequence. Show how the attacker can compute the new CRC without having knowledge of the key or the plaintext.

The CRC is the xor of the words in the message. Say the i 'th word is changed

$$CRC1 = \text{original CRC} = W1 \text{ xor } W2 \text{ xor } \dots \text{ xor } Wn$$

$$CRC2 = \text{new CRC} = W1 \text{ xor } W2 \text{ xor } \dots \text{ xor } Wi' \text{ xor } \dots \text{ xor } Wn$$

The xor of the original and new CRC is the delta

$$CRC1 \text{ xor } CRC2 = \text{delta}$$

We xor the CRC's with the key stream k to get the cipher text version. To get the plaintext back, we xor with the key stream again.

$$C2 = CRC2 \text{ xor } K = \text{new encrypted CRC}$$

$$C1 = CRC1 \text{ xor } K = \text{original encrypted CRC}$$

$$C1 \text{ xor } K = CRC1 \text{ xor } K \text{ xor } K = CRC1$$

$$C2 \text{ xor } K = CRC2 \text{ xor } K \text{ xor } K = CRC2$$

$$C1 = K \text{ xor } (W1 \text{ xor } W2 \text{ xor } \dots \text{ xor } Wi \text{ xor } \dots \text{ xor } Wn)$$

$$C2 = K \text{ xor } (W1 \text{ xor } W2 \text{ xor } \dots \text{ xor } Wi' \text{ xor } \dots \text{ xor } Wn)$$

Say only the i 'th word has changed. In that case, the CRC delta is more specifically. (While we make this single word restriction to illustrate the case, this argument is true in general).

$$\text{delta} = Wi \text{ xor } Wi'$$

If we look at it from the perspective of changing the cipher text, the delta is

$$\text{delta}' = (Wi \text{ xor } Ki) \text{ xor } (Wi' \text{ xor } Ki) = Wi \text{ xor } Wi' = \text{delta}$$

The keys cancel out, so the changing the cipher text will result in the same delta to the CRC as changing the plaintext.

The attacker knows $C1$ and $C2$. He changed bits in the cipher stream.

$$(CRC1) \text{ xor } (CRC2) = (C1 \text{ xor } K) \text{ xor } (C2 \text{ xor } K) = C1 \text{ xor } C2 = \text{delta}$$

The delta is the same for the plaintext and the cipher text.

Therefore, the attacker can update the cipher text version of the CRC directly and it will be the same effect as for the plaintext.

Name:

- b. If the packet and CRC had been encrypted using AES in electronic code book or cipher block chaining mode, could the attacker fix up the CRC to hide changes without knowledge of the key? Why or why not?

The same delta can be calculated on the plaintext.

$$CRC1 = CRC2 \text{ xor } \text{delta}$$

CRC's are encrypted as part of a block encryption using the same shared key (not a key stream).

$$C1 = \text{Enc}(CRC1, K)$$

$$C2 = \text{Enc}(CRC2, K) = \text{Enc}(CRC1 \text{ xor } \text{delta}, K)$$

The keys do not cancel out in this case as they do with the xor operation.

$$C1 \text{ xor } C2 = \text{Enc}(CRC1, K) \text{ xor } \text{Enc}(CRC2, K)$$

Therefore, the attacker cannot fix up the CRC encrypted using a block cipher in the same way they could with an xor stream cipher.

2. Suppose you are performing an investigation on a computer of someone who has recently left the company. Your boss suspects he had been selling information to your company's competitors, and he would like you to look for evidence.
 - a. What two things should you do to preserve the chain of custody, and make it more likely that the evidence you find would be admissible in court?
 1. *Make a bit by bit copy of the hardware before starting investigation. Store the original hard disk in secure storage and perform your investigations on the copy.*
 2. *Take copious notes on the operations you perform in your investigation, so it is very clear how you found the information you find.*
 - b. Identify three places you would look for information on the computer.
 1. *Look for NT streams if this is a Windows system.*
 2. *Look at the file slack space.*
 3. *Do not restrict searches to files with traditionally suffixes.*
 4. *Look for the presence of steganography tools.*
 5. *Look for information in non-standard portions of the disk.*
3. Your boss is concerned about having information leak through emanations scanning. He wants you to analyze option of buying shielded computer monitors and cables for the security sensitive systems vs building a shielded room for all of your organization's computers. Which option would you recommend and why?

Name:

In the shielded component case you would need to examine your system architecture and identify the components that transmit, store, process, and display sensitive information. You would need to shield them from access by non-trusted components (either under your control or not).

In the room case, everything in the room would be shielded. Hopefully, you only have high integrity, highly trusted equipment in this room. If you have untrusted equipment and the potential for physical access by non trusted personnel, you lose some of the benefits of shielding. In theory, your attacker could launch one of the EMSEC virus attacks discussed in the Soft Tempest paper.

A truly paranoid organization would probably both build a shielded room and by shielded equipment. In less paranoid organization could do a cost trade off between the cost of buying enough shielded equipment versus building a shielded room. However, even in the shielded room case, the organization should be aware of trusted vs untrusted systems and maintain separation.

4. Explain one problem with the standard SQL view-based security model that Oracle's Virtual Private Database (VPD) attempts to solve.

There are a couple options here.

- *Reduce the multiplication of views.*
- *Make the relationships between views and users and tables more explicit.*
- *Enable the expression of a wider variety of access policies.*
- *Easier to update policies than views.*