Final Exam

ITIS 6010/8010: Special Topics on Wireless Network Security

Handout time: Dec 16th, 11:00am, 2011

Due time: Dec 17th, 10:59am, 2011

Question 1. Please prove the following propositions.

(a) If the point M is inside triangle ΔABC, when M is shifted in any direction, the new position must be nearer to (further from) at least one anchor A, B or C.

(b) If M is outside triangle ΔABC, when M is shifted, there must exist a direction in which the position of M is further from or closer to all three anchors A, B and C.

Hint: we cover this topic when we discuss the paper "Range-Free Localization Schemes for Large Scale Sensor Networks" by T. He et al.

Question 2. In the radio resource testing mechanism to detect Sybil nodes, a wireless node will randomly assign communication channels to its neighbors and then eavesdrop on one of the channels to detect the Sybil nodes. Let us assume that the node has n neighbors. Within these n neighbors, there are s Sybil nodes, m malicious nodes, and g good (correct) nodes. Because of the communication channel configuration, the node can only test c neighbors at one time. Here c is smaller than n. Now please derive out, if the node conducts r rounds of detection, what is the probability that at least one Sybil node is identified? Please provide detailed explanation of the parameters in your equations.

Hint: we cover this topic when we discuss the paper "The Sybil Attack in Sensor Networks: Analysis & Defenses" by J. Newsome et al.

Question 3. In the physical layer network coding based Sybil detection mechanism, the receivers must distinguish three states of the system: no signal, one signal, and two colliding signals. If the senders are using a Phase based modulation mechanism (such as MSK) to modulate the signals, please describe the mechanism that the receivers can use to distinguish from the three states.

Hint: We cover this topic when we discuss the paper "Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding" by W. Wang et al.

Question 4. When we introduce the mechanism to defend against Sybil attacks via social networks, we define a restricted random route scheme: a node *A* with *d* neighbors will uniformly randomly choose a permutation "*x*1,*x*2, . . . ,*xd*" of the neighbors. If a random route comes from the *i*th edge, *A* will use edge *xi* as the next hop. The routing table of *A*, once chosen, will never change. In this way, we actually embed the predictive property into the random routes. Now please prove the following properties of the scheme:

(a) If two random routes ever share an edge in the same direction, then one of them must start in the middle of the other. In other words, it is impossible for two different paths to enter the same node from two different edges, and then the two paths will merge.

(b) Routing loops can only form at the starting node of the path. It is impossible for a routing loop to be formed in the middle of a path.

Hint: we cover this topic when we discuss the paper "SybilGuard: Defending Against Sybil Attacks via Social Networks" by H. Yu et al.

Question 5. A student designs the following self-healing key distribution method without revocation capability. First, we know that the network lifetime can be divided into m sessions, and for session j, we need to distribute a group key Kj to every member in the network. To protect the keys, the student first generates 2m t-degree polynomials: Hj(x) and Pj(x), j = 1 to m. Then he calculates Qj(x) = Kj – Pj(x), j = 1 to m. During the network initiation procedure, every node i will get the values Hj(i), j = 1 to m.

In session j, the group manager will broadcast the following message:

$$H_1(x)+P_1(x),\ H_2(x)+P_2(x),\ \text{---},\ H_{(j-1)}(x)+P_{(j-1)}(x),\ H_j(x)+K_j,$$
$$H_{(j+1)}(x)+Q_{(j+1)}(x),\ H_{(j+2)}(x)+Q_{(j+2)}(x),\ \text{---},\ H_m(x)+Q_m(x).$$

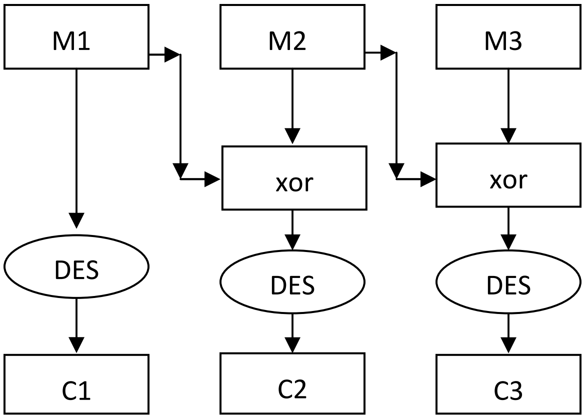
(1) Please illustrate how node i can recover the current key Kj.

(2) Please illustrate how the self-healing property is supported. For example, node i gets the messages in session (j-2) and session (j+2), but not the message in session j. How can it recover Kj?

(3) A malicious node exists in the network. Its identity is z, and it does NOT have any of the values $H_j(z)$, j = 1 to m. Node z can only eavesdrop on the traffic in the network, and it does not have inside colluders or the capability to compromise a good node. Please illustrate how the malicious node z can get K_2 to K_{m-1} in the system by passively listening to the traffic.

Hint: we cover this topic when we discuss the paper "Self-Healing Key Distribution with Revocation" and "Efficient Self-Healing Group Key Distribution with Revocation Capability".

Question 6. Alice is designing a method to chain blocks of DES encryption results together. The encryption procedure is illustrated as below. The ***Mi*** are plaintext blocks, and the ***Ci*** are cipher text blocks. "xor" represents the exclusive-or operation. After encryption, the cipher text blocks ***Ci*** will be sent out. The receiver will try to decrypt ***Ci*** and recover ***Mi*** when it gets the blocks.



Please draw a figure to show the decryption procedure of the three blocks ***C1***, ***C2***, and ***C3*** to recover ***M1***, ***M2***, and ***M3*** at the receiver side.

Question 7. In the DEEJAM paper, the authors propose to use packet fragmentation to defend against the scan jamming attack. Based on equation (2) on page 5 of the paper, the shorter is T_pkt, the lower is the probability that the scan attack will succeed. Therefore, we should use a very short duration of T_pkt. However, in real network environment, we cannot setup the T_pkt to a very small value. Please discuss the reasons from the network efficiency, jamming avoidance, and power efficiency perspectives.

Hint: please refer to the paper "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks" by A. Wood et al. Note that this is an open question and you need to put some thoughts into the answers.

Question 8. In the paper "Non-interactive OS Fingerprinting through Memory De-duplication Technique in Virtual Machines", we use the accumulated access delay to detect whether or not the VM of the attacker and the target VM are using the same OS. Although we need to measure only the delay of the write operation, in the designed approach we conduct four operations: read, read, write, read. Please describe the purpose of each operation respectively.

Question 9. In our class, we discuss extensively the security vulnerabilities caused by the implicit intents of the Android system. Please describe the details of one vulnerability that the attacker is the receiver of an implicit intent and one vulnerability that the attacker is the sender of an implicit intent.

Hint: we cover this part when we discuss the paper "Analyzing Inter-Application Communication in Android" by E. Chin et al.