EECE 512, Fall 2013

Quiz #1 Key

September 26, 2013

This quiz consists of 7 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: _____

Your Given name: _____

Your student ID: _____

#	Points	Out of
1		5
2		5
3		5
4		5
5		5
6		5
TOTAL		30

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. **Explain the differences between isolated flow attacker and chosen flow attacker, as proposed in the paper on attacks on timing-based flow watermarks.**

   The isolated adversary only has access to (possible) outputs of the watermark encoder, while the chosen flow adversary has access to flows before and after they pass the watermark encoder. The chosen flow adversary can also inject flows with a specific timing pattern and observe the distortion possibly added by the watermarker.

2. **Explain the way an adversary who controls femtocell can circumvent IPSec communications with the security gateway to the back-end network, as reported in "Weaponizing Femtocells …" paper.**

   Since the adversary has root access to the femtocell device, there are multiple ways of circumventing IPSec communications with the security gateway and sniffing the subscriber traffic. In the case of the research reported in the paper, a user-space program was in charge of establishing the IPsec connection while a proprietary kernel module encapsulated the network traffic by means of Encapsulating Security Payload (ESP). To allow the kernel to handle encryption of this tunnel, the user-space program had to pass the cipher material (HMAC, Cipher keys, Security Parameter Index) to the kernel. On their test femtocell device, this was performed using the sendto(2) syscall. By hijacking the libc provided wrapper function of this syscall and parsing the message, the researchers were able to grab the key material for circumventing IPSec communications with the security gateway to the back-end network and thus were able to do exfiltration of the subscriber traffic.

3. **Describe the adversary model for the case of Dishonest Display Attack reported in "Security Analysis of India's Electronic Voting Machines" paper.**

(This sample answer is based in part on the answer provided by Jeremy Hewett).

Objectives:

- Manipulate results of votes for individual control units
- Perform the above manipulations undetected

Initial capabilities:

- Ability to create or purchase a replacement display module that has been modified with the ability to change the display counts via a communication channel with the control unit,
- Physical access to EVM control unit (possibly months or years before the election),
- Basic knowledge of electronics if the display module has to be created from scratch.

Capabilities during the attack:

- Ability to communicate to the EVM control unit which candidate is to be favored at any time before votes are publicly counted,
- Ability to get around physical tamper seals.

4.

a) Summarize the idea of the countermeasure that the authors of the *optimistic* acknowledgment (opt-ack) DoS attack ("Misbehaving TCP Receivers …") propose.

The server randomly skips sending the current segment, and instead sends the rest of the current window. A non-malicious client that actually gets all of the packets, except the skipped one, will start re-ACKing for the lost packet, thereby invoking the fast retransmit algorithm. However, an attacker cannot tell where along the path a given packet was dropped, so it cannot tell the difference between an intentionally dropped packet and a packet dropped in the network by congestion. Thus, an attacker will ACK the skipped packet, alerting the server to the attack.

b) Explain why it does not harm much the communications with benign clients and helps detect malicious clients.

Usually, fast retransmission indicates network congestion, so the congestion window is correspondingly halved. However in this case, retransmission was not invoked due to congestion in the network, so the sender should not halve the congestion window/slow start threshold as it typically would. Given that most modern TCP stacks implement selective acknowledgments, this solution is very efficient. The only penalty applied to a conforming client is a single round trip time in delay.

5. Explain the differences between authorization and authentication

Authorization is about enforcing rules on the access of resources by subjects. Whereas, authentication is about binding identity of a user to the subject (e.g., process, network node).

6. **List the names of the 10 principles of designing secure systems that were discussed in the security bootcamp, and briefly explain each one.**

    1. Principles of least privilege (PLP): very program and every user of the system should operate using the least set of privileges necessary to complete the job.

    2. Fail-Safe Defaults: Base access decisions on permission rather than exclusion.

    3. Economy of Mechanism: Keep the design as simple and small as possible.

    4. Complete Mediation: Every access to every object must be checked for authority.

    5. Open Design: Security should not depend on secrecy of design or implementation.

    6. Separation of Duty: Require multiple conditions to grant privilege.

    7. Least Common Mechanism: Mechanisms should not be shared.

    8. Psychological Acceptability: Security mechanisms should not add to difficulty of accessing resource.

    9. Defense in Depth: Layer your defenses.

    10. Question Assumptions: Frequently re-examine all the assumptions about the threat agents, assets, and especially the environment of the system.