Name: _____ UNI: _____

COMS W4180: Network Security — October 2006

1		15
2		10
3		15
4		20
5		15
6		15
7		10
Total		

Rules

- Remember to write your name and UNI on the blue exam book.
- **Important: also write your name on this paper**
- You must turn in *both* the exam sheet and the blue book
- Books and notes are allowed during this examination; computers are not permitted.
- This is a time-limited test. All papers must be turned in 75 minutes after the beginning of the test.
- The total points add up to 100.
- Good luck, and may the Force be with you.

Questions

1. (15 points) Someone has suggested that instead of using firewalls, we should simply encrypt all communications. Is this person right or wrong? Explain.

Encryption protects against eavesdropping and data modification; it also provides for authentication. It does not protect against buggy code. To quote a slide directly, 'The best cryptography in the world will not guard against buggy code."

2. (10 points) I noted in class that it was not possible to resynchronize RC4. Explain why this makes it a poor choice for use with IPsec.

IPsec provide protection at the IP layer. IP packets can be dropped, duplicated, reordered, etc.; this in turn means that all packets have to be treated independently for decryption. In other words, there's no stream. If an out-of-order packet is received, there's no way to handle it, short of going forward until the starting point is reached (if this packet is in advance of where it should be); if the packet is a past packet, there's no easy way to go backwards in RC4.

3. (15 points) Your web server has been attacked successfully in the past by people who send it URLs with strange Unicode characters. You decide to put a firewall in front of it, to sanitize the input. Explain the implications of encryption for this firewall. What could you do to solve the problem?

If we have a firewall between the outside and the web server, and the encryption — say, SSL — is between the user and the web server, the firewall is helpless: it can't see the input. The solution is to use an application firewall for inbound web traffic, and terminate the SSL connection at the firewall rather than the web server. That way, the firewall can do the proper santization. Depending on the operational environment, transmissions from the firewall to the web server can either be in the clear or the firewall can re-encrypt.

4. (20 points) You've been asked to protect a site with a firewall. The are no inbound services. The only outbound service is Web browsing, which of course requires some form of DNS name resolution. There is a lot of concern about people going to improper sites; there is also a desire to filter all web content to remove active content. Describe the best firewall configuration for this site. Justify the purpose of each element.

The most important component is a web proxy server that performs filtering of URLs. All internal machines must route their requests through it. To enforce this, a packet filter should be used to block all outbound TCP traffic from any machine other than the proxy.

By itself, that machine could even be on the inside of a packet filter. However, as noted, it does need to do DNS queries. If no other UDP services run on that machine, outbound UDP access to port 53 from it could be enabled, with all inbound UDP responses permitted. Alternatively, a stateful packet filter could be used, regardless of what other UDP services were enabled.

If there was a threat of unauthorized use of UDP by other inside machines — and the problem didn't say, so you don't have to supply this part of the answer — a DNS server would have to live in a DMZ. Only the Web server — which could live in the DMZ, but doesn't have to — would be allowed to send packets to it. (A DMZ is an acceptable part of any answer, but there's no strong need for it except as explained here.)

DNS filtering alone won't work, since people could browse many sites using just the IP address in the URL.

5. (15 points) Explain why a MAC is needed when encrypting with a stream cipher.

With a stream cipher, it's easy to make controlled changes in the plaintex, by flipping bits in the ciphertext. With a block cipher in CBC mode?

CBC mode is vulnerable to cut-and-paste attacks, though at the cost of one garbage block. In some cases, this can be used to attack confidentiality.

6. (15 points) You are encrypting with AES in CBC mode. You encrypt plaintext blocks A, B, C, D, E. However, the third block is garbled during transmission; in particular, the low-order bit is flipped. What is received?

The third block (C) of plaintext becomes garbage. In the fourth block (D) of plaintext, the low-order bit is flipped. Blocks A, B, and E are decrypted properly.

7. (10 points) SIP uses several different forms of encryption. Why?

Both the trust model and the communications differ among the different players. Signaling messages must be protected hop-by-hop, because they have to be interpreted and perhaps modified at each hop. A SIP endpoint will have a trust relationship with its proxy; it neither knows nor trusts any other proxies. In the general case, two proxies won't trust each other, but may have a business relationship. Some aspects of signaling messages may need end-to-end integrity protection. Voice content needs end-to-end confidentiality protection, where even the trusted proxies don't have the key. Besides, that data may flow over a different path.