Final Exam **COS 432, Fall 2008**

All questions have equal weight. You may use your own lecture notes, copies of the lecture notes of other students in the course, and any summaries you have made of those notes. You may not use any other materials.

Some problems may have more than one correct answer. You will get full credit if your answer is one of the correct ones.

If you can't figure out a complete or perfect answer to a question, tell us what you have figured out. A flawed answer will get more credit if you demonstrate that you know the limitations of your answer.

Please do your work in an exam book.

Undergraduates: Before turning in your exam, please hand-write and sign the Honor Code pledge, "I pledge my honor that I have not violated the Honor Code during this examination."

(Graduate students: No need to sign anything. You are bound by university rules against cheating.)

---

(1) You are designing a VoIP application which lets computer users conduct voice conversations, like a telephone. You are given code that can make a network connection between two computers, and can digitize voice signals and transmit them across the network connections. You're also given code that uses crypto to ensure confidentiality and integrity of communicated data.

All that is left is to provide a key agreement protocol that the two endpoints to a call can use to agree on a shared secret key to use for securing the call. Your protocol should work under the following constraints:

- All copies of the software must be identical; there is no way to "bake in" a unique key to any individual copy of the software.
- Users can trust that they got a legitimate, unmodified copy of your software.
- Your code has access to a hardware-based random number generator that generates bits that no adversary can predict. The random generators on different computers will generate different, independent outputs.
- There is no third party that is trusted by all of your users.
- You may assume that the two speakers on a call will recognize each other's voices. If there is a Man In The Middle (MITM), the MITM will not be able to impersonate either speaker's voice well enough to fool the other speaker.

Describe your key agreement protocol, and explain why it is secure.

(2) In recent years, the MD5 cryptographic hash function has been broken: it is now possible to find collisions for MD5. More specifically, there is an attack algorithm which, given any bit-strings A and B of equal length, can find bit-strings X and Y such that, for all bit-strings C, MD5(A || X || C) = MD5(B || Y || C). (As usual, "||" denotes concatenation.)

For this question, assume that you don't know about any cryptographic hash functions other than MD5. MD5 is flawed, but you have to find a way to accomplish something useful with it anyway.

(a) Can you remedy MD5's weakness by using the HMAC construction? That is, is HMAC-MD5 secure or is it subject to collisions too? Explain.

(b) Can you design another algorithm that uses MD5 as a sub-procedure and is more collision-resistant? You probably won't be able to prove that your construction is more collision-resistant (at least not without extra assumptions about the MD5 collisions), but at least give some justification for why it is likely to be better.

(3) Some products are legal to sell to adults but illegal to sell to kids. Let's call such products "adults-only products". The Prime Minister of Freedonia has announced his nation's intention to protect kids from any emails that mention adults-only products. Freedonia's Ministry of Technology (FMoT) has designed a system to help law-abiding people comply with the Prime Minister's directive. You have been hired to provide feedback on the system.

The system works as follows. Any kid can upload his email address to the FMoT. The FMoT computes the hash of the uploaded email addresses, and publishes on the FMoT's website a big list containing the hashes of all of the uploaded kid email addresses. Citizens can download this list, and before sending an email that mentions an adults-only product, can compute the hash of the destination address, and can refrain from sending the email if the computed hash is on the list.

This system has two goals. First, it should give law-abiding citizens an effective way to avoid sending improper emails to kids. Second, it shouldn't help criminals send improper emails to kids. The FMoT recognizes that criminals can just ignore the system and send whatever emails they want; but the system should at least avoid making criminals' lives easier.

(a) Is this system reasonable, given the goals? Why or why not?

(b) Can you think of a better system, that is, a system that achieves the goals more completely, or achieves them just as completely at lower cost?

(4) LectureVision is a (hypothetical) set-top box that is about to be released by a consortium of universities, to let students watch lectures from the comfort of their dorm room or their parents' beach house. The box will be offered for sale to the public at electronics stores and by mail order. The box will connect to the Internet and will have a video output that can be connected to a TV. To save money, the LectureVision device will have *no input mechanism.*

After receiving the box, a student can engage in a registration procedure (which you will design) that associates the box with the student's identity. From then on, the box will automatically display live streaming video of all lectures from courses that the student is taking.

The registration procedure is designed to prevent random members of the public from viewing lectures, and to prevent students from viewing lectures in courses that they are not taking. The registration procedure need not be absolutely bulletproof, but it should do a reasonable job of balancing security against the convenience of student users.

Describe your design for the registration procedure. You may assume that students have access to an Internet-connected computer, that the universities are willing to cooperate in the procedure, and that the LectureVision set-top box has a way to make secure (confidential, with integrity) connections to the LectureVision servers.. Along with your design, *write a paragraph explaining why your design is good.*

(5) Barack Obama carries a BlackBerry handheld device, which he uses to read and send email. He is very attached to his BlackBerry, but some people say he should give it up when he becomes President on Tuesday. They argue that the BlackBerry is not secure enough for Presidential communications.

For purposes of this question, make the following assumptions about how things work. The BlackBerry hardware and software are manufactured by a private company called RIM. RIM also makes email server software that can be purchased and run by White House technicians on the White House mail server. When email is sent or received by the BlackBerry device, the device makes an Internet connection, via Verizon's cellular network, to the White House mail server. The device also connects to the White House mail server every minute or so to check whether any mail has arrived. The BlackBerry and mail server use a good key negotiation protocol to derive a shared secret session key, which is then used to encrypt and integrity-check the communications using a good cryptosystem.

Assume that the President has access to other communication systems for use with the most highly sensitive data such as detailed intelligence reports. The BlackBerry would be used only for unclassified email.

(a) If you were the government's technology czar, would you let President Obama keep his BlackBerry? Why or why not?

(b) Now assume that the President is going to keep and use his BlackBerry. (If you said no in part (a), assume that the President overruled you.) What measures might you take to reduce the risk attached to the Presidential BlackBerry?