Quiz 2

1. Do not open this booklet until the quiz begins. Read all the instructions first.
2. When the quiz begins, write your name on every page of this quiz booklet.
3. This quiz booklet contains 15 pages, including this one. An extra sheet of scratch paper is attached.
4. This quiz is open-book, open-notes. No calculators or programmable devices (including laptop computers) are permitted.
5. You have 80 minutes to earn 111 points.
6. Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Do not put part of the answer to one problem on the back of the sheet for another problem; pages may be separated for grading.
7. Partial credit will be given. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it. Be neat.
8. Good luck!

Problem	Points	Grade	Initials
1	30		
2	62		
3	19		
Total	111		

Your Name: ____________________________

Academic Honesty: by signing below, I affirm that the work on this quiz is my own, and that I have complied with the quiz policies.

Your Signature: ____________________________

Problem Q2-1. Short Answer [30 points]

(a) For convenience, you set up your email program to automatically decrypt your incoming encrypted mail, and to quote the plaintext in your replies. To what kind of cryptographic attack might you be opening yourself?

Solution: A chosen-ciphertext attack.

(b) In the above scenario, name a cryptosystem that is believed to be secure under such an attack.

Solution: RSA-OAEP or Cramer-Shoup.

(c) Briefly describe two ways a computer program can get access to (some reasonable representation of) its own code.

Solution: Load self from the file system; look at self in memory; use the recursion theorem.

(d) In its next chip, Intel finds a way to make the stack non-executable. Does this solve the problem of buffer-overflow attacks? Explain briefly.

Solution: No. It's still possible to maliciously modify the return address and parameters on the stack, which could cause undesired behavior.

(e) Professor M. U. Lator doesn't believe that Trusted Computing proposals really support attestation. "Someone could just alter the operating system to impersonate the TPM," says the professor. Critique this suggestion.

Solution: The TPM contains secret keys that are tough to extract (due to tamper-resistance), and software cannot emulate the TPM without those keys.

(f) Fill in the blanks: biometric authentication is unsuitable for some security applications, such as 1. ____________ (give one example) because 2. ____________ (give one reason).

1. remote authentication

2. replay attacks are easy

(g) List two technical differences between Palladium/NGSCB and TCPA/TCG (as these systems were presented in class).

1. NGSCB is turned on mid-boot; TCG has a trusted boot process.

2. NGSCB has a trusted I/O path; TCG does not.

(h) List three techniques that virus writers use to make their viruses harder to detect:

1. Putting the virus somewhere other than the head or tail of the executable.

2. Polymorphism (changing the code of the payload with each infection).

3. Detecting whether the virus is being run in emulation.

(i) Give an example of a tamper-resistant technology.

Solution: There are several: a cryptographic coprocessor that forgets its keys when its battery is improperly removed; a TPM/SSC; a PUF.

(j) Finish the following sentence: From a security viewpoint, an advantage of a PUF over MAC with a secret key is that ...

Solution: The key for a MAC can be copied, a PUF (in theory) cannot.

(k) Finish the following sentence: Sebek2 uses a "magic number" in its packet header so that . . .

Solution: Other machines running Sebek2 will filter out those packets if sniffers are run on them.

(l) List two assumptions that a remote server makes when it concludes that it is communicating with an authentic NGSCB client machine.

1. The client's SSC has not had its keys extracted.

2. The SSC's private key has not been computed from the public key.

(m) Give one reason why "simplicity" an important criterion in the design of secure systems.

Solution: There are many: the system will be easier to analyze; implementations will be less likely to have bugs.

Problem Q2-2. True or False [62 points]

Circle **T** or **F** for each of the following statements. No justification is required, but if you think the statement is ambiguous, state your clarifying assumptions.

True **False** A CPUF controls access to a PUF so that to obtain a new valid challenge-response pair for the underlying PUF, you need to either have physical access to the CPUF, or else already have knowledge of an authentic challenge-response pair for that PUF.

Solution: True.

True **False** Fairly good protection against optical tempest attacks can be obtained merely by working in a room with the lights on.

Solution: True.

True **False** Using a laptop with an LCD screen provides good protection against tempest attacks based on RF emanations from the laptop.

Solution: False. It only protects against optical tempest eavesdropping.

True **False** Tamper-resistance techniques have gotten good enough so that one can count on them to reliably prevent access even by an opponent who has a very large budget.

Solution: False.

True **False** With certain physical attack methods, it is not even necessary to have probes on any data lines to find out what values they are carrying while the chip is in operation.

Solution: True.

True **False** Modern hard disks are probably better than older disks at overwriting information so that the overwritten information is no longer inferable.

Solution: True.

True **False** So called "bad blocks" on modern hard disks have no security implications, because they cannot be read.

Solution: False. Bad blocks may contain sensitive data, and still be readable (using special hardware, e.g.).

True **False** It is impossible to design a totally error-proof binary watermarking scheme if two users can compare their copies (even if they are restrained by the Marking Assumption).

Solution: True. See the example from lecture of the "majority word," which cannot implicate any user unconditionally.

True **False** For forward secrecy to be achievable, a party must be able to effectively erase information.

Solution: True.

True **False** It is possible to distribute a secret S to Alice, Bob, and Carol, so that Alice and Bob can reconstruct S, and Alice and Carol can reconstruct S, but Alice can't infer anything about S by herself, and Bob and Carol can't infer anything about S even if they collaborate.

Solution: True. Use Shamir secret sharing with $n = 4$ and $t = 3$, and give Alice two shares, and Bob and Carol one share each.

True **False** It is possible for Alice to prove to Bob that she knows the discrete logarithm x of her public key $y = g^x \pmod p$, *without* giving Bob any new information about x.

Solution: True. Zero-knowledge proofs do this.

True **False** It is possible to fool a fingerprint reader reliably, but only at great expense.

Solution: False. No great expense is needed.

True **False** Before Bob even sees a zero-knowledge proof from Alice, he can generate, on his own, many transcripts that are indistinguishable from what he and Alice would generate during the zero-knowledge proof.

Solution: True. Bob can run the simulator for the proof.

True **False** By publishing the source code of the NGSCB Nexus, as well as the source code of its compiler, Microsoft can allay all fears that the Nexus contains back doors.

Solution: False. See the "Reflections on Trusting Trust" paper.

True **False** It takes roughly twice as long (on the same hardware, using the best known algorithm) to factor a 1025-bit RSA modulus than to factor a 1024-bit RSA modulus.

Solution: False. Because the best known algorithm factors in time exponential in the *cube root* of the modulus length, one would needs a much longer modulus to achieve twice the security.

True **False** For any fixed virus X, it is undecidable to determine, given an input program P, whether P is infected with virus X.

Solution: False. For a virus X that does no trickery to hide itself, a simple scan for P's code would suffice.

True **False** The reason that there are no Java viruses is that the Java byte-code verifier is a highly effective virus detector.

Solution: False.

True **False** A virus V will only be undetectable by a virus detection program D if V is written with foreknowledge of D.

Solution: False. V may be written first, and D may simply not be written to detect V (perhaps because V has not been released, or due simply to negligence).

True **False** Factoring a 500-bit RSA modulus is beyond current computer technology.

Solution: False. See page 151 of the textbook for recent results in factoring.

True **False** In an interactive proof between a prover and a verifier, the soundness property exists for the verifier's benefit.

Solution: True.

True **False** If the committing party is computationally unbounded, Pedersen's commitment scheme is insecure.

Solution: True.

True **False** A 512-bit elliptic curve key is widely believed to offer roughly the same security as a 512-bit RSA key.

Solution: False. Elliptic curve cryptography seems to offer much more security per key bit.

True **False** One advantage of identity-based encryption is that keys are much shorter than in RSA-based encryption.

Solution: True.

True **False** A successful buffer-overflow attack will always result in the attacker gaining "root" access on the victim's machine.

Solution: False.

True **False** To prevent buffer-overflow attacks, it would help significantly to revise the CPU architecture so that the stack grows "upwards" in address space.

Solution: We accepted both answers (we had "True" in mind, but "False" is actually correct).

True **False** It is impossible to write a program A that correctly determines, given a program P, whether P outputs A's source code.

Solution: True. Such a problem is undecidable.

True **False** If the verifier cannot discover the prover's secret from an interactive proof, then the proof is zero knowledge.

Solution: False. Zero knowledge means something much stronger: that the verifier learns *nothing* about the secret (not even a single bit, for example).

True **False** If (as conjectured) SHA-1 is collision-resistant, then there are no two inputs that can hash to the same value.

Solution: False. By the pigeonhole principle, there are an infinite number of inputs that hash to the same value.

True **False** A problem is undecidable if it requires exponential time to solve.

Solution: False. An undecidable problem cannot be solved in *any* amount of time.

True **False** SSL with Diffie-Hellman and AES-128 offers forward secrecy.

Solution: True.

True **False** Forward secrecy requires the use of public-key encryption.

Solution: False. You can have a symmetric-key system in which keys change; the next key is the one-way hash of the previous key. Then, revealing a current key does not reveal previously-encrypted information.

Problem Q2-3. Multiple Choice [19 points]

(a) Which of the following flaws were discovered in the Needham-Schroeder authentication protocol several years after it was proposed? Circle one.

- **I** It relies on RSA keys that were insufficiently long.
- **II** It allows for a server to impersonate a client to another server.
- **III** It allows for a client to impersonate a server to another client.
- **IV** No problems have been discovered with the protocol.

(b) Which of the following flaw were discovered in the station-to-station authentication protocol several years after it was proposed? Circle one.

- **I** It relies on Diffie-Hellman keys that were insufficiently long.
- **II** It allows for a server to impersonate a client to another server.
- **III** It allows for a client to impersonate a server to another client.
- **IV** None of the above.

(c) According to Professor Rivest, if you are designing a new protocol you should avoid MD5 and use SHA-1 instead for which of the following reasons (circle one):

- **I** SHA-1 is faster than MD5.
- **II** SHA-1 provides more security than MD5, even though its output has the same number of bits.
- **III** SHA-1 is the standard, and it's better to use standards.
- **IV** Unlike MD5, SHA-1 is not susceptible to the birthday attack.

(d) Shamir secret sharing has the following disadvantage (circle one):

- **I** Lagrangian interpolation, while polynomial-time, is extremely inefficient.
- **II** Reconstruction creates a single point of failure at which secrecy can be compromised.
- **III** It doesn't protect against extremely powerful adversaries.

(e) Differential power analysis is related to factoring in the following way (circle one):

- **I** Both are attacks that can be used to learn the secret key of a smart card.
- **II** Both are attacks that were invented by Paul Kocher.
- **III** Both attacks work in theory, but they have not been shown to work against actual systems that are typically deployed today with 1024-bit RSA keys.

(f) The "Optical Time-Domain Eavesdropping" attack described by Markus G. Kuhn at the University of Cambridge is not a worry in practice because (circle one):

I If you can see the glow of a computer's screen, you almost always have permission to see the screen itself.

II The equipment that Kuhn used in his demonstration of the attack is not generally available to hackers.

III Since the publication of his paper, CRT vendors have adopted the Silicon Physical Random Functions described by Gassend, Clarke, van Dijk and Devadas, and thus they are now protected against the Kuhn attack.

IV The attack only works certain kinds of phosphors. In particular, red phosphor is not susceptible to the kind of eavesdropping that Kuhn describes. Since white text is displayed by a combination of red, blue and green, this attack is only of theoretical interest.

V The attack does matter and could be widely practiced today, but in a few years it won't matter as much because LCD displays are not susceptible to this particular attack.

(g) The Slammer worm (circle one):

I Was developed by an information warfare laboratory working under contract to either the US government or the government of China; this was proven by a signature that was hidden in the program's code.

II Spread so fast because it required only a single TCP/IP SYN packet to infect a remote computer.

III Infected 90% of the vulnerable hosts within 5 minutes.

IV Could infect both Microsoft SQL server and the open-source DNS server, but fortunately most of the DNS servers on the Internet had already been patched.

V May still be at large on the Internet.

(h) Which of the following is/are true about the Java security model? Circle all that apply.

- **I** The byte-code verifier checks that every operation is allowed by the security policy that is in effect.
- **II** Strong-typing plays an important role.
- **III** A remote server can be assured that a particular applet is running on a client machine.
- **IV** Bugs have been found in implementations of the security manager.
- **V** Java programs are not allowed to read from or write to disk.

SCRATCH PAPER — There is no quiz content on this page.