Information Security:

Theory vs. Reality

Exercise 3

Tel Aviv University

0368-4474-01, Winter 2015-2016

Lecturer: Eran Tromer

Teaching assistant: Tzvika Geft

Submit a ZIP file containing all your work to istvr1516.course@gmail.com by 17 January 2016.

Include your name and ID in the subject and the submitted ZIP file's name.

Submissions are individual and must be done independently of other students and any course-specific reference material. Using reference material that is not course-specific is OK, if you state so explicitly in your code and the body of the submission email; provide a pointer to its origin; and adapt it to precisely and elegantly answer the actual question.

In all questions, you may make reasonable assumptions, as long as you state them explicitly.

Question 1

Using a focused ion beam, an attacker can connect a wire inside a chip to electrical ground, thus forcing it to logical 0. To model this, we define the "single-wire reset" tampering capability as the ability to force a single wire of the circuit to 0. The adversary chooses the wire in advance, and can perform only a single reset throughout the device's operation; the reset persists forever.

A. Explain intuitively how single-wire reset tampering capability can help an attacker. (Think of examples we saw in class.)

The security definition given in class can naturally capture the notion of "tamper-resilience against adversaries with single-wire reset capability". In particular:

- In the real world, initially (before providing the first input to the device), the adversary chooses wire to reset and the device is modified accordingly. Then the attack proceeds as usual.
- In the simulated world, the simulator learns the adversary's choice, but still has only black-box access to the uncorrupted device.

Consider the masking scheme using a global mask, described in class (leakage-resilience against single-wire probing). Consider the simplified case of stateless circuits C with a single input-to-output evaluation (no iterations and state update).

B. Show that this scheme is not tamper-resilient against an adversary with single-wire reset tampering capability and no leakage.
   (Hint: consider the quantifiers in the security definition, and focus on simple, concrete cases. Show how an adversary can extract some secret with some probability. Explain why this contradicts the definition of tamper-resilience.)
C. Show how, moreover, an adversary with both single-wire probing and single-wire reset capabilities can extract some secrets with probability 1.
D. Suggest a circuit transformer for converting any circuit *C* into *C'* that is tamper-resistant against a single-wire reset. Prove its security. In *C'*, Use only NOT and two-input AND/OR/NAND gates.
   (Hint: Some critical systems run 3 computers in parallel, for protection against cosmic rays.)

After learning your new circuit, the attacker developed powerful electromagnetic waves which can instantly reset all transient values in circuits (wires, values on gates, DRAM, SRAM, flip-flops etc.) Non-volatile storage (flash etc.) is, however, unaffected by the waves.

E. Give an example that shows how the attacker can use the waves to extract information from the circuit.
F. Suggest a circuit transformer that protects the privacy of the device from the attacker's waves.

Question 2

You are given a device consisting of a microcontroller containing 32 16-bit registers, a DRAM memory chip, and an input/output interface. The device assumes that its inputs are encrypted under 4096-bit RSA, and decrypts every incoming message using an embedded RSA secret key. The decryption uses plain square-and-multiply exponentiation, without the Chinese remainder theorem (CRT method).

The device uses a highly protected implementation for the microcontroller, which resists all side-channel attacks (available to you) on that particular chip. To also protect the memory stored on the DRAM chip, the manufacturer used a full implementation of Oblivious RAM, including the path-based ORAM shown in class "protecting memory content from leakage", "protecting memory content from corruption", and even scheduling memory instructions at regular intervals to hide timing. To store the small trusted state needed by the above memory protection mechanism, the manufacturer added a small fast non-volatile memory to the microcontroller chip.

You discovered that whenever you lower the power supply voltage to the device from the intended 5V to 2V, it still operates correctly, except that writes to the microcontroller's non-volatile memory will fail silently (the value does not change). This is the only control you have over the device, other than its nominal inputs, and there is no side-channel leakage from the device.

RSA encryption gives a restricted form of homomorphic encryption, where the $Eval$ algorithm supports only programs that contain only multiplications over Z_n. It turns out that the device is utilized in an application that uses such RSA-based homomorphic encryption. The application may operate in Client Mode or in Server Mode.

A. In Client Mode, the device receives data from a remote server and decrypts it (but does not produce any output). Can you gain knowledge of the plaintext? Explain.

B. In Server Mode, the device receives ciphertexts, public key and desired program from a remote client, runs the Eval function on these inputs, and returns the result to the client. Can you gain knowledge of the plaintext? Explain.

As elsewhere in this homework, you may make reasonable assumptions, as long as you state them explicitly.