Monash University
FIT 5124: Advanced Topics in Security
Week 9 Tutorial Sheet

Ron Steinfeld, 22 April 2015

In this week's tutorial we will look at side channel attacks.

Problems

1 **Timing Attacks.** Consider the timing-based attack on password verification presented in the lecture. We consider two variants/extensions of it here.

a Suppose the following countermeasure was used in an attempt to defend against the attack: instead of always comparing $\tilde{P}[i]$ to $P[i]$ in the order $i = 0$ to 7, a random order of comparison for the 8 bytes is used each time, i.e. for each verification, a random permutation s of the integers $\{0, \ldots, 7\}$ is chosen, and the comparison is done in the order $s(0), s(1), \ldots, s(7)$ (again, stopping as soon as a mismatch $\tilde{P}[s(i)] \neq P[s(i)]$ is detected. Can you give a modified timing attack to break this variant? What is the attack cost?

b Suppose now the verification is done with stored password hashes $H = f(P)$, where f is some password hashing function. To verify a login password $\tilde{P}$, the system computes $\tilde{H} = f(\tilde{P})$, and then compares $\tilde{H}$ to H (say they are both 8-byte hash values) using the original timing-vulnerable method. Suppose further that the attacker suspects that P belongs to a dictionary of about 1 million common passwords. Show how the attacker can use a timing method and expect to reveal P using less than 1000 trial logins.

2 **Differential Power Analysis on AES.** An attacker wishes to use a differential power analysis (DPA) attack on a smartcard executing the AES-128 algorithm with unknown key K on inputs $x_1, \ldots, x_6$, where the least significant bytes of $x_1, \ldots, x_6$ are $0x2b, 0xc3, 0x19, 0xf7, 0xde, 0x3a$ respectively (in hexadecimal notation). The attacker measured the values $2, 4, 8, 5, 5, 3$ for the smartcard power consumption for those 6 inputs respectively, all at the instant when the smartcard computed the output of the least significant byte of the AES state after the first AddRoundKey and SubByte operations. Basing the attack on the value of the most-significant bit of the AES state at that point, which of the following two candidates k_1, k_2 for the least-significant byte of K would the attacker consider more likely to be the correct one: $k_1 = 0x64$ or $k_2 = 0x35$? Why? (Note: the number of samples 6 in this example is artificially small to make hand computations feasible).