CS 5435:
Security and Privacy Concepts in the Wild
Homework #2

Due: Before class on 8 Oct. 2014

55 points (+ 15 bonus)

Instructor: Ari Juels TA: Sid Telang

Problem 1: VeriChip was a kind of "synthetic biometric," an RFID tag that could be surgically implanted under the skin and used to authenticate users by emitting a secret key. See http://en.wikipedia.org/wiki/VeriChip for an overview. Verichips could be used, for example, to pay for drinks at the Baja Beach Club in Barcelona. See http://news.bbc.co.uk/2/hi/technology/3697940.stm.

Explain in what ways VeriChip was probably a bad idea as an authentication mechanism. Apart from its perhaps being the Mark of the Beast, what security and/or privacy vulnerabilities would authentication using the Verichip give rise to? [10 points]

Problem 2 Oklahoma Otis's 39-slot roulette wheel became an internet sensation (after he got a cryptographer to fix his gameplay protocol). He even expanded his business by introducing a poker game with 53 cards, instead of the usual 52. A security problem arose, though: A hacker (Eve) kept breaking into the accounts of Otis's customers because they choose weak passwords.

Mississippi Mabel recommended to Otis that he distribute one-time passcode tokens to his customers to secure their accounts.

Otis immediately designed his own authentication token. It's a printed token that works like a real product offered by a company called Deepnet Security (see http://bit.ly/1D7qenE), except that for extra security, of course, Otis's has an extra row. (It has 9 rows instead of 8, but 10 columns, just like Deepnet's.) On Otis's card, characters are selected uniformly at random from the set $\{0, 1, \ldots, 9, a, b, \ldots, z\}$. An example card is given in Figure 1.

	A	B	C	D	E	F	G	H	J	K
0	w	g	r	d	f	8	a	v	s	j
1	v	w	d	g	5	9	x	s	n	8
2	8	q	7	j	4	u	4	b	o	x
3	g	l	e	f	k	v	2	t	g	q
4	q	h	s	a	1	r	s	6	k	3
5	9	3	6	p	8	v	w	e	l	z
6	s	2	d	6	b	6	k	h	5	2
7	f	n	m	e	0	f	x	4	m	w
8	3	q	j	8	u	t	s	q	d	a

Figure 1: Otis's printed "one-time passcode token"

Passcodes in Otis's system are of length five. A user gets three tries to submit a correct passcode before her account is locked.

In this homework assignment, you'll play the role of an attacker and figure out how to break Otis's various authentication schemes.

Question 2.1: Otis starts by using a "one-time passcode" with a "free navigation" option for his authentication token (analogous to the Deepnet option). His system allows a user to authenticate by choosing an arbitrary starting position and then moving through a sequence of arbitrarily selected adjacent squares without visiting the same square twice. A pair of squares are considered adjacent if their letter coordinates and their number coordinates differ by at most one. (So diagonal adjacency counts.) To generate a passcode, the user reads off characters from the five squares she traverses. To prevent eavesdropping attacks, Otis's system will not allow a user to submit an identical path twice.

Suppose that for some customer X (with a random card different from the example above), you've captured the passcode "y9ahe." Briefly describe an attack in which you use this passcode to try to impersonate X. Give an example of a passcode you might use in this attack. [5 points]

Suppose the character 'e' is not incident on an edge, i.e., isn't in row 0 or 8 or column A or K, and that it is adjacent to a square containing the 'h' of the captured passcode, but not to any of its other characters. Give an estimate of the probability that your attack succeeds and show how you arrived at it. (Assume for simplicity that this is user X's first authentication attempt, and make the simplifying assumption that no character is adjacent to two identical ones.) [10 points]

Question 2.2: After your attack on his first scheme, Otis switches to the Deepnet "password protected" variant scheme. In this variant, the user may start from an arbitrary position, but must follow a predetermined sequence of four transitions (e.g., "move down," "move to the upper left," etc.) to obtain her full sequence of five characters. This sequence of transitions is the user's secret "password."

Does the password-protected variant help protect against your attack in the previous question? Why or why not? [5 points] Suppose that X's password is a diagonal line (e.g., "move lower right" four times). With what probability can you impersonate X after eavesdropping just once on X's submitted passcode? How did you arrive at this result? (Again, assume that X chooses a sequence that does not terminate in a character incident on the edge of the card. You may assume for simplicity that this is X's first authentication attempt and that you know X's "password" in addition to the captured passcode.) [5 points]

Question 2.3: In desperation, Otis finally switches to the Deepnet "challenge-response" variant. In this variant, the server presents the user with a sequence of five card positions, selected uniformly and independently at random. The user must return the corresponding sequence of characters from the card as her passcode.

After eavesdropping once a day for a month (30 days) on challenges and the passcodes with which X responds, what is the probability that you can learn the characters in at least 75% of the squares in X's card? You may code up a simulation and use it to provide an (accurate) approximation of the answer. [10 points] Assuming that you've learned exactly 75% of the squares, what is your success probability in attempting to impersonate X? [5 points]

Question 2.4 (Bonus): Devise and simulate a full attack in which you eavesdrop once a day for a month (30 days), as above. Give the probability, via simulation, that you can successfully impersonate X. [5 points]

Then devise a different "challenge-response" scheme that yields a lower probability of impersonation of X in the 30-day eavesdropping scenario. Describe your scheme and show using your attack simulation that your scheme is stronger than Otis's in this particular setting. [10 points]

Question 2.5 (Bonus): Otis set up his service so that the only way for a customer to remove money from an account is to wire it into the customer's pre-registered bank account. Without modifying bank account numbers, compromis-

ing customers' bank accounts, or otherwise wiring money directly from a user's account, how might you steal money from hacked accounts? [5 points]