Authentication grid

Dr Alexei Vernitski

Aims

- Reuse the standard password-based authentication as much as possible
- Reduce the danger of shoulder-surfing
- Keep the authentication process usable
- Use modern touch-screen technology

Authentication

- To keep the grid simple, the password consists of upper-case letters and digits
- Split the password into pairs of consecutive characters
  For example, if the password is DRAGON, split it as follows: DR, AG, ON.
- For each pair, prove to the authenticator that you know the pair, by using a grid challenge.

Grid challenge

K	4.	6.	F	W	H
P	U	1.	8.	Z	S
R	V	E	5.	Q	A
N	0.	B	L	M	G
I	3.	X	D	O	7.
T	C	Y	2.	J	9.

- You are shown a randomly generated grid
- Note that each time you need to enter your password, a new grid is generated

Grid challenge

K	4.	6.	F	W	H
P	U	1.	8.	Z	S
R	V	E	5.	Q	A
N	0.	B	L	M	G
I	3.	X	D	O	7.
T	C	Y	2.	J	9.

- Find the row containing the first character of the pair and the column containing the second character of the pair.
- Press (or click) the character on the intersection of this row and this column

Grid challenge

K	4.	6.	F	W	H
P	U	1.	8.	Z	S
R	V	E	5.	Q	A
N	0.	B	L	M	G
I	3.	X	D	O	7.
T	C	Y	2.	J	9.

- If you want to prove that you know the pairs DR, AG, ON, press on I, A, I.

Shoulder-surfing

- Suppose that the attacker observed you. Then he has some information about your password.
- How successful will he be impersonating himself as you?
- Let us look at a specific randomly chosen example.
- Let us concentrate on the first pair of characters DR.

Attacker’s analysis

K	4.	6.	F	W	H
P	U	1.	8.	Z	S
R	V	E	5.	Q	A
N	0.	B	L	M	G
I	3.	X	D	O	7.
T	C	Y	2.	J	9.

- To enter the pair DR, you press on I.
- Then the attacker knows that
  - The first character is one of I, 3, X, D, O, 7
  - The second character is one of K, P, R, N, I, T

Attacker’s attempt at log in

F	A	C	9.	X	8.
W	R	L	S	B	D
Y	3.	H	2.	U	Q
N	I	7.	6.	4.	M
P	T	5.	V	O	1.
J	K	E	G	0.	Z

- The attacker is shown a random grid
- The red characters are the ones which might be the first character of the password
- They are spread over five rows

Attacker's attempt at log in

F	A	C	9.	X	8.
W	R	L	S	B	D
Y	3.	H	2.	U	Q
N	I	7.	6.	4.	M
P	T	5.	V	O	1.
J	K	E	G	0.	Z

- The green characters are the ones which might be the second character of the password
- They are spread over two columns

Attacker’s attempt at log in

F	A	C	9.	X	8.
W	R	L	S	B	D
Y	3.	H	2.	U	Q
N	I	7.	6.	4.	M
P	T	5.	V	O	1.
J	K	E	G	0.	Z

- Thus, any of the ten orange cells might be the valid response to the challenge
- The attacker is not likely to guess it correctly.

For discussion

- What are the advantages and disadvantages or this authentication scheme?
- For example:
  - Hardware requirements?
  - Cost?
  - Reusing existing password technology?
  - Brute force attack?
  - Time and stress level?
  - Authentication situations?