Security evaluation of the Access Key in Qtech Hide&View program

According to "READme-QtechHV-v011.pdf" information, you are suggested to set up your Access Key (i.e., embedding/extracting key) as "1 to 16 length alphanumeric characters." However, the program was designed to admit much longer and various keys. For example when embedding, if you want to set a 25-character key, it is okay. If you want to have a 32-character key, that's no problem. The longer the key, the safer the embedding.

Qtech HV actually accepts any Access Keys consisting of "1 to 32 printable 8-bit characters."

A typical computer keyboard is equipped with 47 keys having upper and lower case or other shift key variant.

One more special key, i.e., space key, is also available in Qtech HV for an access key (but need some technique when placing it on top).

So, the number of possible Access Keys of length 32 characters (including spaces) amounts to 95^{32} combinations. Let x be the equivalent length of a binary Access Key. Then the equation

$$2^x = 95^{32}$$

holds. From this equation you can easily calculate x=210.7188・・・.

This is to say that Qtech Hide&View program maintains 210 bits password equivalent security.

<Discussion>

How long time will it take to complete an Exhaustive Search for the Access Key?

The total number of 32 length access keys for Qtech HV is

$$95^{32} \approx 1.9371 \times 10^{63}.$$

In order to know if a given key is correct or not, you must run the extracting component of Qtech HV on a PC. Let the average extracting time (i.e., check up time) for a single key be 1 second, or around. You may organize one million PCs to check keys in a parallel way with no-overlapping manner. Then, its overall performance is equivalent to a high-speed computer that can check one million keys in a second, and can check

$$10^6 \times 60 \times 60 \times 24 \times 365 = 3.1536 \times 10^{13}$$

keys in one year.

So the total time, in years (K), needed for the system to complete the key-searching is

$$K \approx (1.9371 \times 10^{63}) / (3.1536 \times 10^{13}) \approx 6.1425 \times 10^{49}.$$

According to "Big Bang Theory", the Universe is only 1.382×10^{10} years old. So, it is absolutely impossible to find a correct key by way of exhaustive search on the current Universe.

Even if you reduce the key-length to only 10, it will still take almost **2 million years**.

In the case the characters for Access Key is limited to alphanumeric (i.e., 62 characters), it will take,

1.5117×10^6 billion years for a 16 length Key, and

6.9235 years for an 8 length Key.

(Updated on Nov. 27, 2019 by Eiji Kawaguchi)