MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Cracking SHA1-hashed passwords

Author: Chair for Cryptology and IT-Security

March 2011

SHA1

The *Secure Hash Algorithmus 1* has been standardized by the National Institute of Standards and Technology in 1995 and is besides MD5 the most commonly used hash algorithm in practice. An example for its usage is password-based authentification. In that case, the server does not store the user password in plain text but instead the SHA1 hash value of it. Once the user enters his password and after its received at the server, its hash value is computed and compared to the value stored on the server in order to verify its correctness.

Scenario

A vulnerability of a surveillance system's webserver leaked the SHA1 hash value of the password of the administrator account. The password's hash value is

```
67ae1a64661ac8b4494666f58c4822408dd0a3e4
```

Furthermore, the keyboard of the login terminal shows clear signs of the entered password since after a successful login navigation in the software is only done via arrow keys.

What is the password?

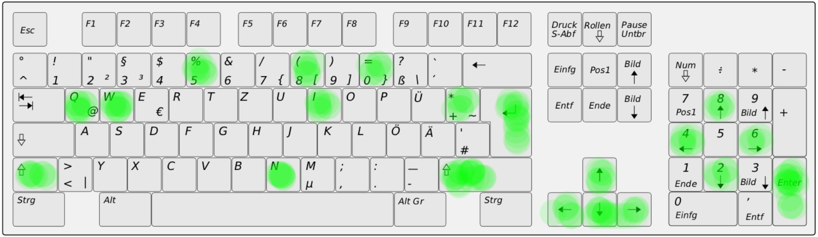
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
Druck S-Abf Rollen Pause Untbr
° ^ ! 1 " 2 ² § 3 ³ $ 4 % 5 & 6 / 7 { (8 [ ) 9] = 0 } ? ß \ ` ´ ←
Einfg Pos1 Bild ↑
Num ÷ * -
Q @ W E € R T Z U I O P Ü * + ~
Entf Ende Bild ↓
7 Pos1 8 ↑ 9 Bild ↑ +
A S D F G H J K L Ö Ä ' #
4 ← 5 6 →
> < | Y X C V B N M µ ; , : . _ -
↑
1 Ende 2 ↓ 3 Bild ↓ Enter
Strg Alt Alt Gr Strg
← ↓ →
0 Einfg , Entf

Figure: Fingerprints on the keyboard

Remark: Note the German keyboard layout!