Google Authenticator

OTP *open* a *basso costo* per piattaforme mobili (e non solo)

Luca Carbone – INFN Mib

Workshop CCR INFN – Genova, 27-31/5/2013

GA in sintesi

- Implementazione di generatori di codici one-time per piattaforme mobili (Android, Apple, Blackberry, *Symbian*) e di un modulo PAM open-source (Apache 2.0) per l'autenticazione sotto linux;
- Tecnicamente parlando: vengono implementati gli standard open definiti e sviluppati da **OATH** (*Initiative for Open Authentication*); supporta sia **HOTP** (*HMAC-based OTP*, RFC4226) sia **TOTP** (*Time-based OTP*, RFC6238);
- E' il sistema utilizzato da Google per implementare l'accesso via *two-step verification* a suoi servizi, il che fa ben sperare per quanto riguarda affidabilita' e supporto nel tempo.

HOTP vs TOTP

- Entrambi gli algoritmi usano un seme pseudocasuale come chiave segreta nota sia al server sia al client; a tale seme e' concatenato un fattore variabile (un contatore nel caso di HOTP, una timestamp nel caso di TOTP) e cio' che ne risulta e' (grossomodo) la chiave one-time (monouso).
- TOTP e' piu' recente e considerato piu' sicuro di HOTP (oltre che meno suscettibile di disallineamenti catastrofici), ma l'implementazione di questo algoritmi in software piuttosto che in hardware ha sollevato in ogni caso piu' di un dubbio sull'effettiva sicurezza di questo approccio low-cost.

libpam-google-authenticator

- Provato con successo (ssh) sotto Fedora 13, Centos 6.3, SLC 5.5; binari disponibili per Fedora 15-18 e Centos/SL 6 (EPEL).
- Configurazione: una linea nel modulo PAM, varie opzioni:
  - `auth required pam_google_authenticator.so`
  - `nullok`
  - `echo_verification_code`
  - `skewadj`
  - `secret` (utile per SELinux)
  - `...`

google-authenticator

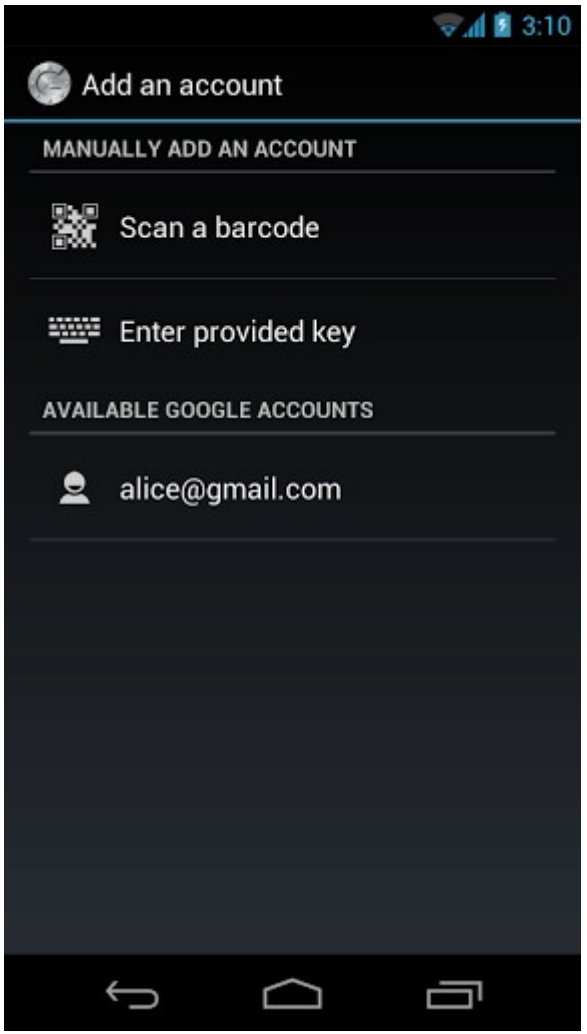
configurazione interattiva account

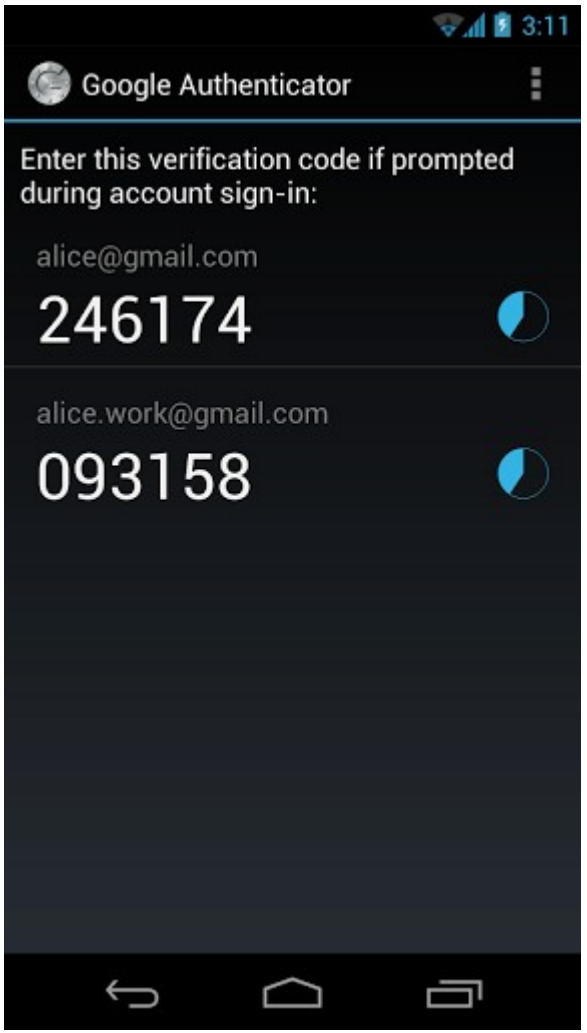
```
ssire.mib.infn.it:22 - tamigi@ssire:~ VT
File  Edit  Setup  Control  Window  Help
[tamigi@ssire ~]$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/tamigi@ssire.mib.infn.it%3Fsecret%3DICPA5F43MEXOXUXO
```

```
Your new secret key is: ICPA5F43MEXOXUXO
Your verification code is 782698
Your emergency scratch codes are:
  24114906
  93313838
  81427533
  49958382
  44369290

Do you want me to update your "/home/tamigi/.google_authenticator" file (y/n)
```

```
Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
size of 1:30min to about 4min. Do you want to do so (y/n) n

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting (y/n) y
[tamigi@ssire ~]$
```

GA mobile

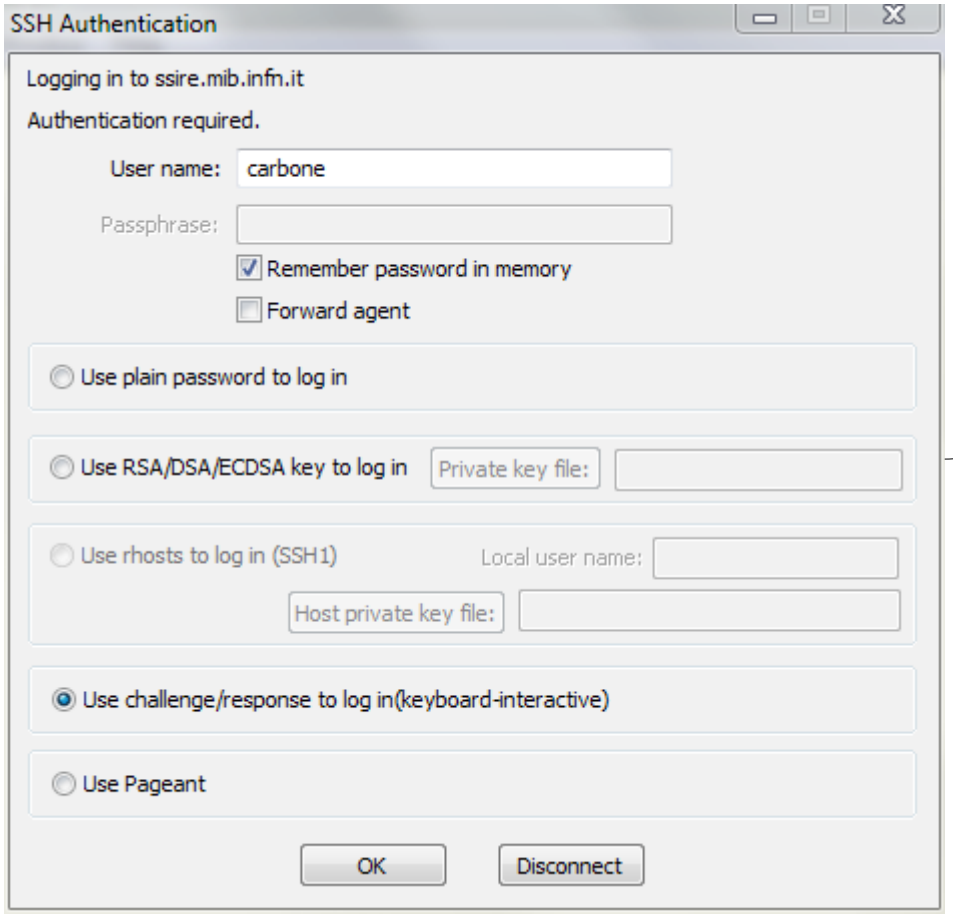

3:10
Add an account
MANUALLY ADD AN ACCOUNT
Scan a barcode
Enter provided key
AVAILABLE GOOGLE ACCOUNTS
alice@gmail.com

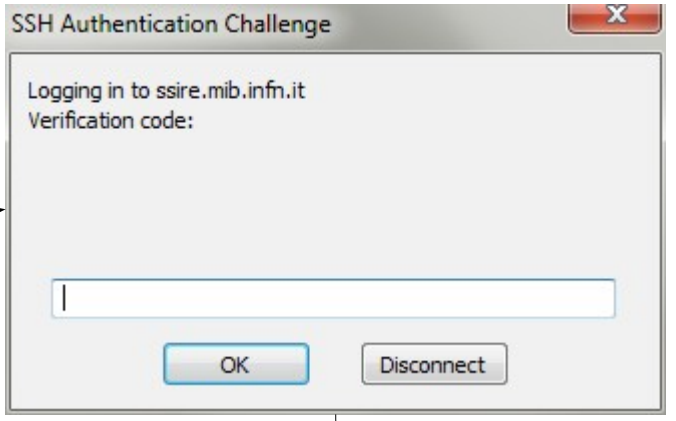

3:11
Google Authenticator
Enter this verification code if prompted during account sign-in:
alice@gmail.com
246174
alice.work@gmail.com
093158

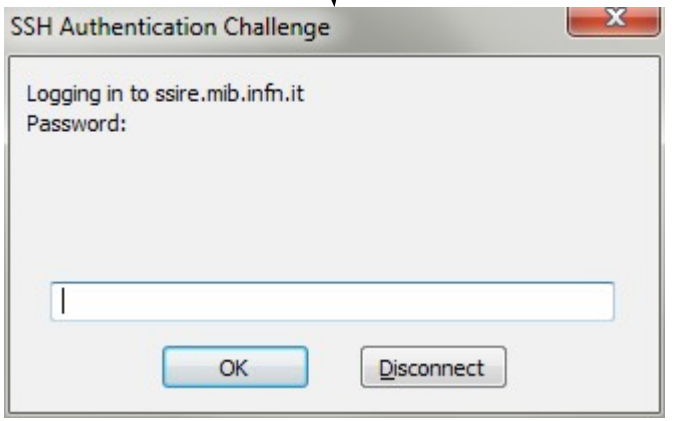
client compatibili

- **ssh**, **slogin**, **scp**; *da notare che una chiave privata o un ticket krb validi hanno la precedenza sulla verifica a due fasi;*

- **teraterm**, **winscp**, ...:







conclusioni

- Facile da installare e configurare (compatibile anche con SELinux con un po' di lavoro), economico, potrebbe rappresentare un salto quantico per quanto riguarda la sicurezza degli accessi ad alcuni servizi, ma l'impatto sull'utenza e' piuttosto robusto;
- e' possibile, essendo basato su open standard, che sia portabile su soluzioni H/W piu' sicure (chiavi dedicate); se c'e' interesse si puo' indagare ulteriormente;
- alcuni servizi/applicativi sono allo stato attuale sicuramente incompatibili (thunderbird, per citarne uno), e non e' dato di sapere se mai diventeranno OTP-aware.