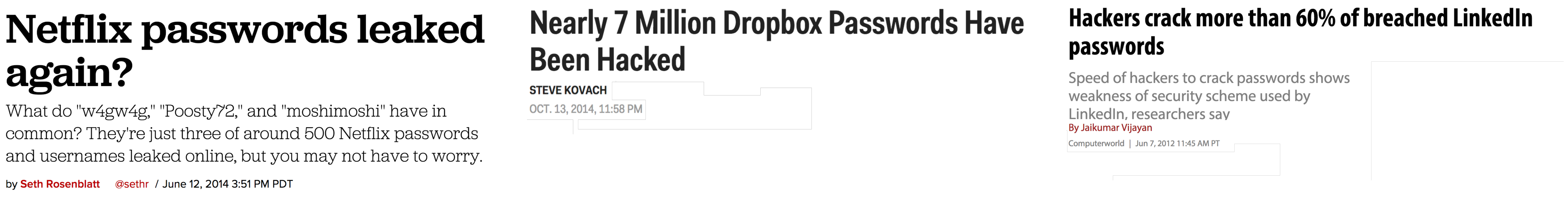
CERIAS

The Center for Education and Research in Information Assurance and Security

ErsatzPasswords - Ending Password Cracking

Christopher N. Gutierrez, Mohammed H. Almeshekah, Mikhail J. Atallah, and Eugene H. Spafford

PROBLEM



Netflix passwords leaked again?

What do "w4gw4g," "Poosty72," and "moshimoshi" have in common? They're just three of around 500 Netflix passwords and usernames leaked online, but you may not have to worry.

by Seth Rosenblatt @sethr / June 12, 2014 3:51 PM PDT

Nearly 7 Million Dropbox Passwords Have Been Hacked

STEVE KOVACH

OCT. 13, 2014, 11:58 PM

Hackers crack more than 60% of breached LinkedIn passwords

Speed of hackers to crack passwords shows weakness of security scheme used by LinkedIn, researchers say

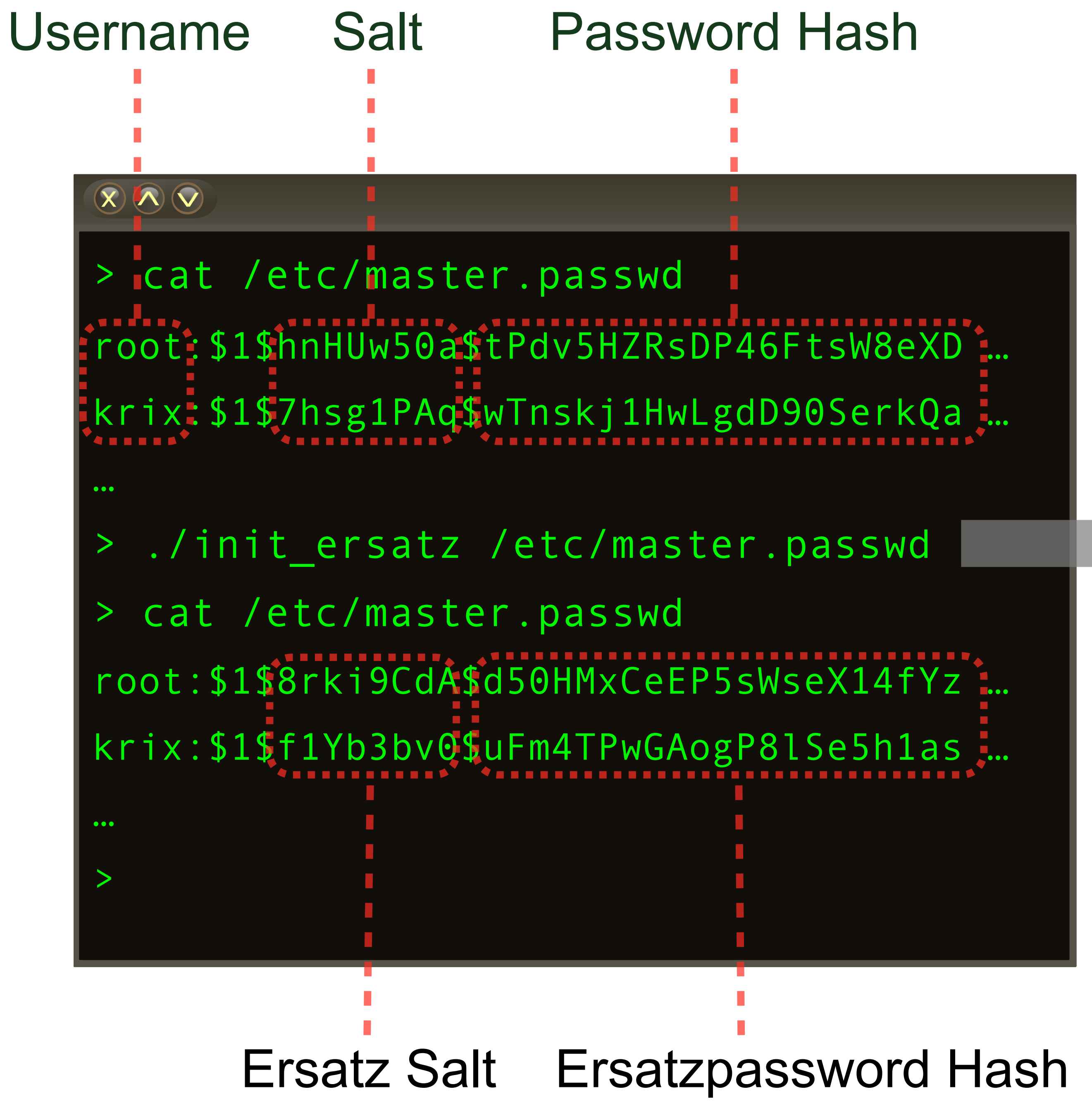
By Jaikumar Vijayan

Computerworld | Jun 7, 2012 11:45 AM PT

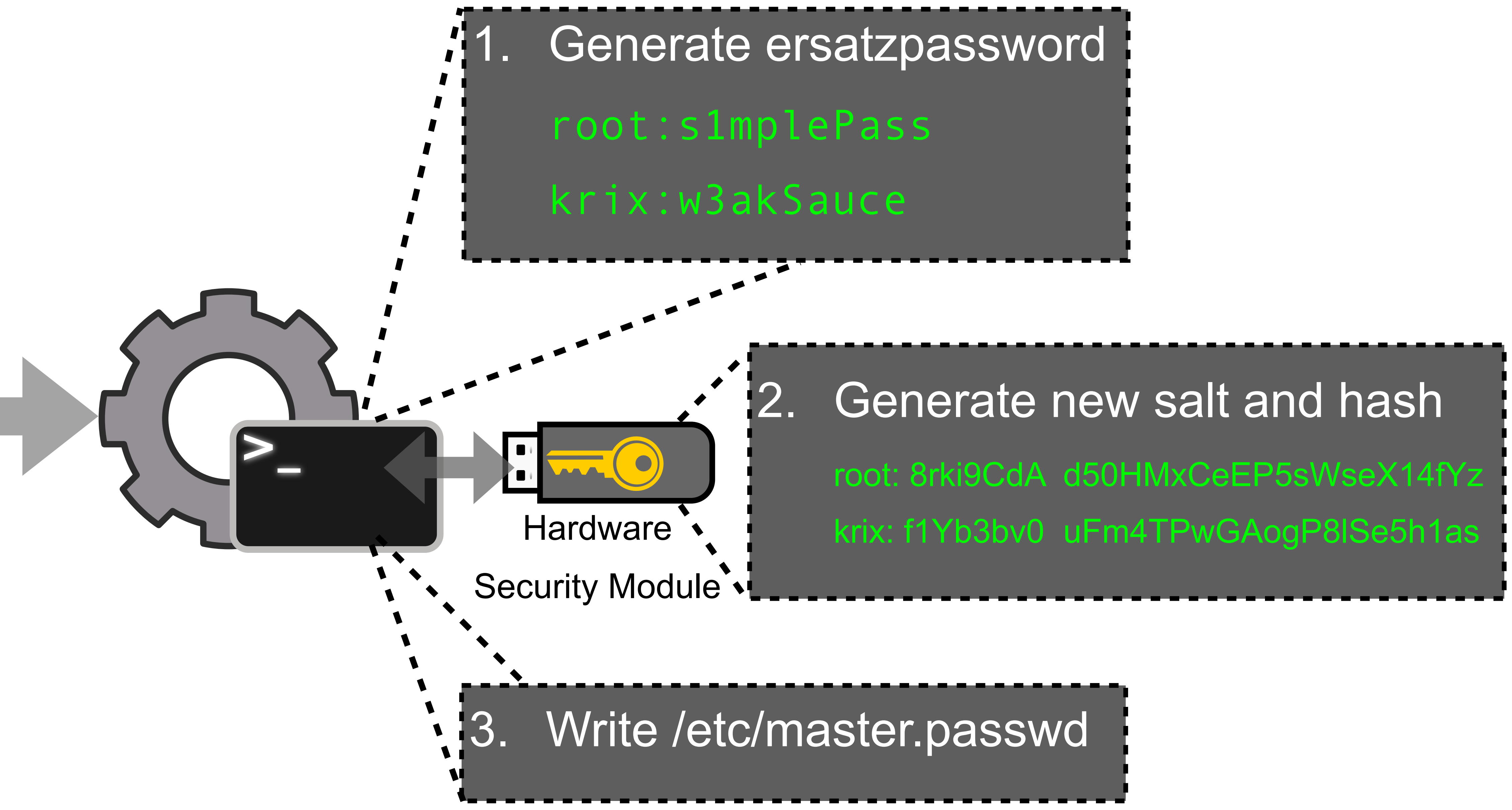
```
/etc/master.passwd
root:$1$hnHUw50a$tPdv5HZRsDP46FtsW8eXD …
krix:$1$7hsg1PAq$wTnskj1HwLgdD90SerkQa …
…
```

```
root: sTr0ngIshPW
krix: Cmplx1tY$
```

SOLUTION



```
> cat /etc/master.passwd
root:$1$hnHUw50a$tPdv5HZRsDP46FtsW8eXD …
krix:$1$7hsg1PAq$wTnskj1HwLgdD90SerkQa …
…
> ./init_ersatz /etc/master.passwd
> cat /etc/master.passwd
root:$1$8rki9CdA$d50HMxCeEP5sWseX14fYz …
krix:$1$f1Yb3bv0$uFm4TPwGAogP8lSe5h1as …
…
>
```



1. Generate ersatzpassword

```
root:s1mplePass
krix:w3akSauce
```

2. Generate new salt and hash

```
root: 8rki9CdA  d50HMxCeEP5sWseX14fYz
krix: f1Yb3bv0  uFm4TPwGAogP8lSe5h1as
```

3. Write /etc/master.passwd

If an attacker gets ahold of master.passwd …

```
/etc/master.passwd
root:$1$8rki9CdA$d50HMxCeEP5sWseX14fYz …
krix:$1$f1Yb3bv0$uFm4TPwGAogP8lSe5h1as …
```

```
root: s1mplePass
krix: w3akSauce
```

No noticeable difference in password hash file

Reveals ersatzpassword instead of true user password

This work was supported, in part, by a grant from the Northrop Grumman Corporation

CERIAS

PURDUE UNIVERSITY