CERIAS

The Center for Education and Research in Information Assurance and Security

ErsatzPasswords - Ending Password Cracking

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

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 …
```

→ John the Ripper →

```
root: RootPwrd1
```

SOLUTION

Username Salt Password Hash

```
> cat /etc/master.passwd
root:$1$hnHUw50a$tPdv5HZRsDP46FtsW8eXD…
…
> ./init_ersatz /etc/master.passwd
> cat /etc/master.passwd
root:$1$8rki9CdA$d50HMxCeEP5sWseX14fYz …
```

Ersatz Salt — Ersatzpassword Hash

Hardware Security Module

1. Generate ersatzpassword
   `root:s1mplePass`
2. Generate new salt and hash
   root: 8rki9CdA d50HMxCeEP5sWseX14fYz
3. Write /etc/master.passwd

If an attacker gets ahold of master.passwd

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

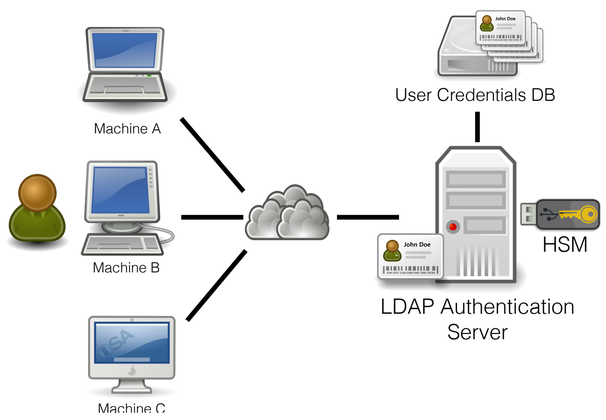
→ John the Ripper →

```
root: s1mplePass
```

No noticeable difference in password hash file

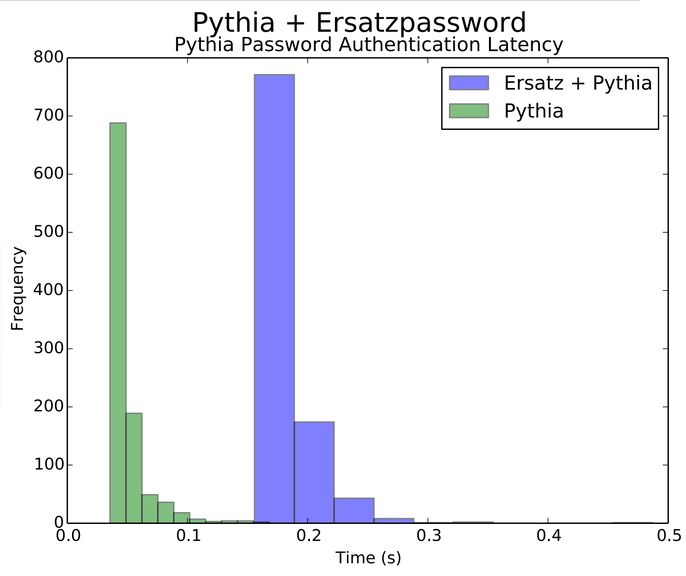
Reveals ersatzpassword instead of true user password

RESULTS



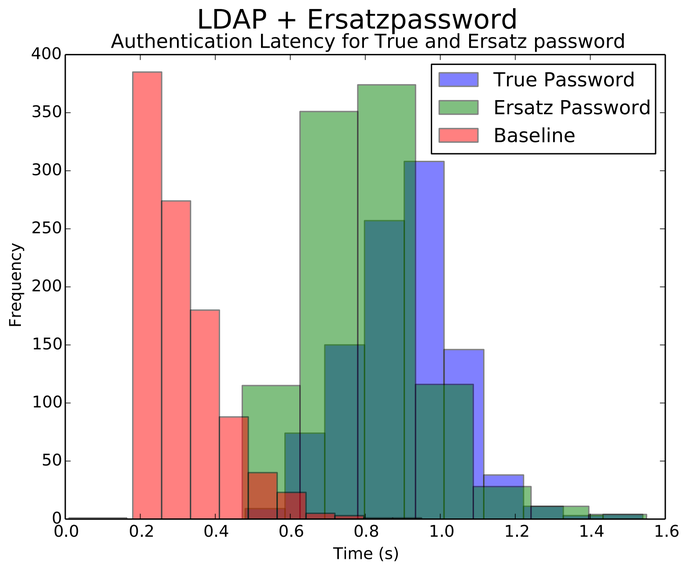
Integration	Filename	Original	ErsatzPassword	Difference
pam_unix	pam_unix.c	338 LOC	393 LOC	55 LOC
LDAP	passwd.c	893 LOC	926 LOC	33 LOC
Pythia PRF	safeid.py	61 LOC	124 LOC	64 LOC

ErsatzPassword Integration LOC



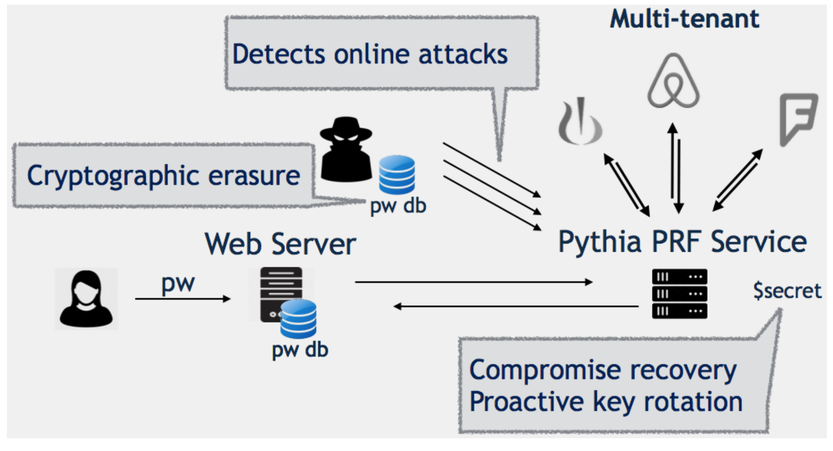
Pythia PRF [1]

LDAP



Library	Language	LOC
pam_unix, LDAP	C	255
Pythia PRF	Python	103

ErsatzPassword Library LOC



This work was supported, in part, by a grant from the Northrop Grumman Corporation, National Science Foundation Grants CPS-1329979, Science and Technology Center CCF-0939370, and EAGER-1548114.

[1] Everspaugh, A., Chatterjee, R. , Scott, S., Juels, A., and Ristenpart, T. 2015. The pythia PRF service. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15). USENIX Association, Berkeley, CA, USA.

CERIAS

PURDUE UNIVERSITY