redhat

AUTHENTICATION USING ONE-TIME PASSWORD TOKEN AND SMART CARD

AN EASY WAY TO PREVENT IDENTITY THEFT

THIERRY BORDAZ - FLORENCE RENAUD

Senior Software Engineers - Identity Management

PASSWORD THEFT

LILY HAY NEWMAN SECURITY 12.14.16 6:27 PM

HACK BRIEF: HACKERS BREACH A BILLION YAHOO ACCOUNTS. A *BILLION*

CNIL RECOMMENDATION

Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe

NOR: CNIL1702369X
ELI: Non disponible

Cas n° 4. - Mot de passe et matériel détenu par la personne

Si l'authentification s'appuie sur un matériel détenu par la personne, la commission considère que :

- la taille du mot de passe doit être au minimum de 4 chiffres ; et
- l'authentification ne peut concerner qu'un dispositif matériel détenu en propre par la personne, à savoir uniquement les cartes SIM, cartes à puce et dispositifs contenant un certificat électronique déverrouillable par mot de passe (token) ; et
- un blocage du dispositif doit être mis en œuvre après un nombre d'authentifications échouées consécutives au plus égal à 3.

PHISHING

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

PASSWORDS ARE NOT SECURE.
WHAT SHOULD I DO, THEN?

TWO FACTOR AUTHENTICATION

- OTP (TOTP/HOTP TOKENS, SOFT TOKENS, MOBILE PHONE...)
- PKCS#11 (SMART CARD READER + SMART CARD, USB KEYS...)

IDENTITY MANAGEMENT

MAIN FEATURES

- **CENTRALIZED AUTHENTICATION**
  - Source: IDM or Active Directory
  - Credentials: passwords, certificates, Smart Cards, OTP tokens
  - Single Sign-On: Kerberos, SAML, OpenID
- **CENTRALIZED AUTHORIZATION**
  - Resources: systems, services, applications
  - HBAC, sudo rules, privileges
- **CENTRALIZED MANAGEMENT**
  - Policy
  - Certificates and Keys
- **DNS**

BASED ON A COLLECTION OF OPEN SOURCE COMPONENTS:
KDC, LDAP, PKI, DNS, FREEIPA

DEMO #1:

OTP AUTHENTICATION WITH FREEIPA

Phase 1: Sharing a secret

Soft token
(freeOTP)

Secret

user 1

Secret / SR

user 2

Serial number XXX

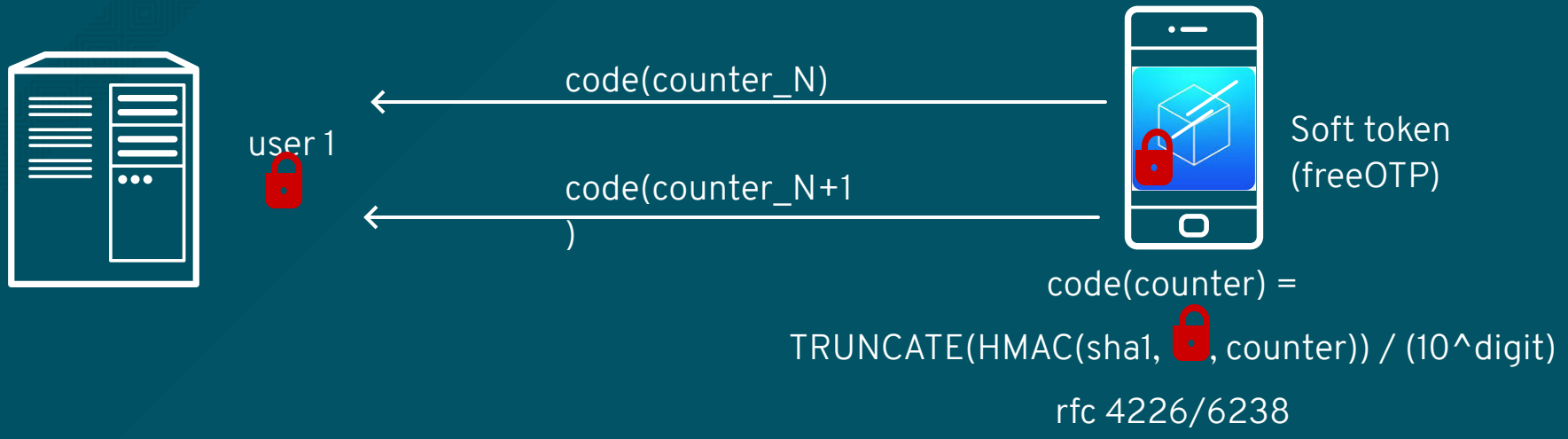
Hardware token
(gemalto)

user 3

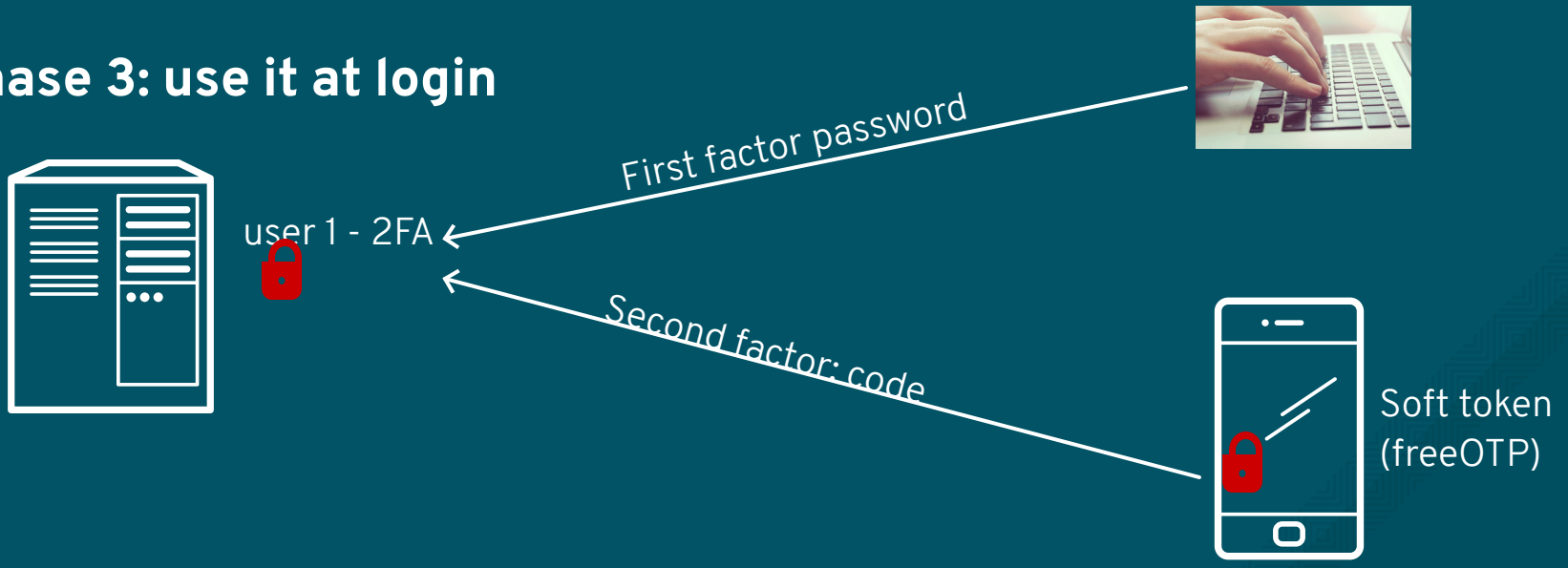
Write secret

Programmable Hardware
token (yubikey)

Phase 2: Synchronize counter



Phase 3: use it at login



DEMO #2:

SMART CARD AUTHENTICATION WITH FREEIPA

SMART CARD AUTHENTICATION

FREEIPA SERVER

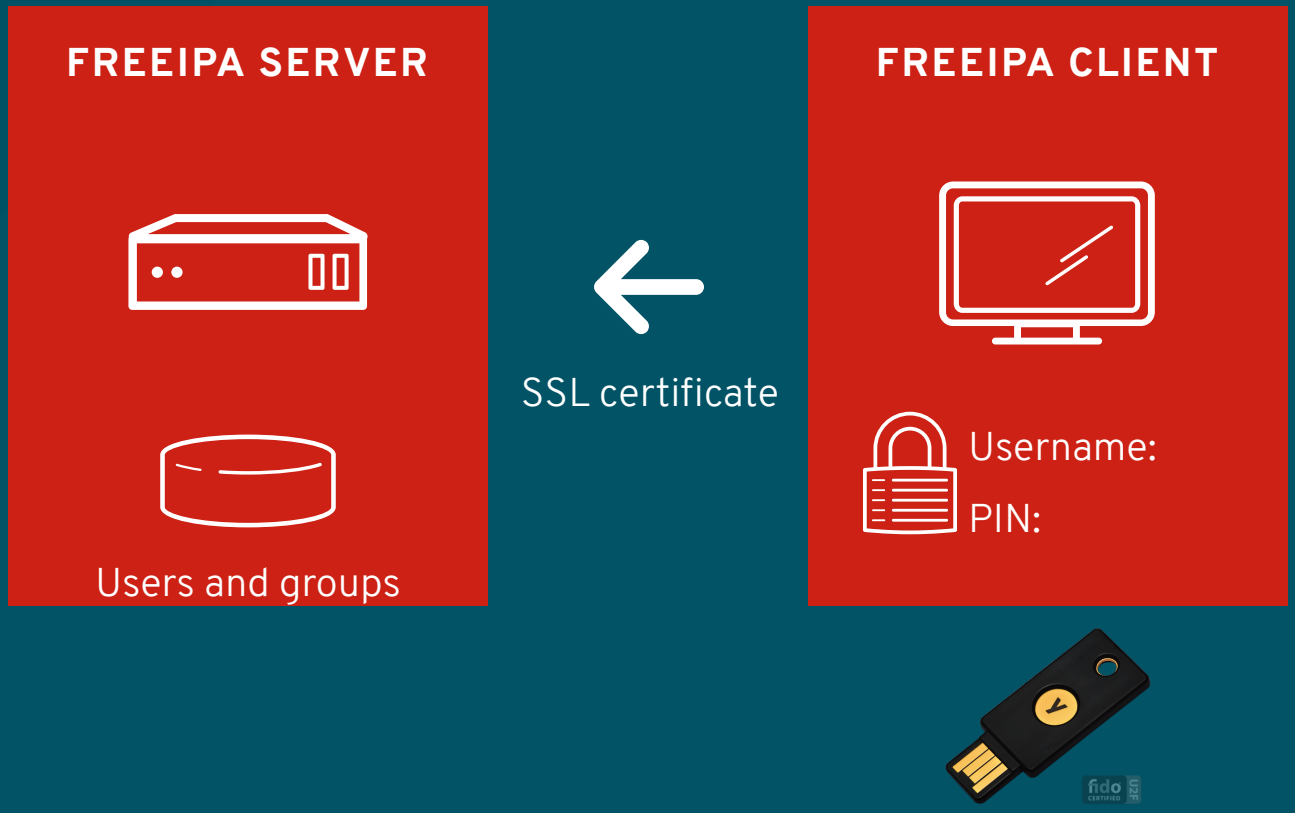
Users and groups

FREEIPA CLIENT

Username:

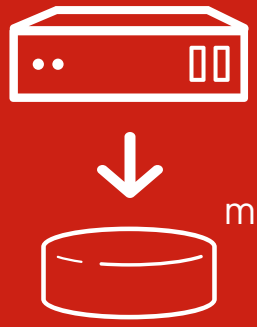
PIN:

SMART CARD AUTHENTICATION



SMART CARD AUTHENTICATION

FREEIPA SERVER



Look for matching user

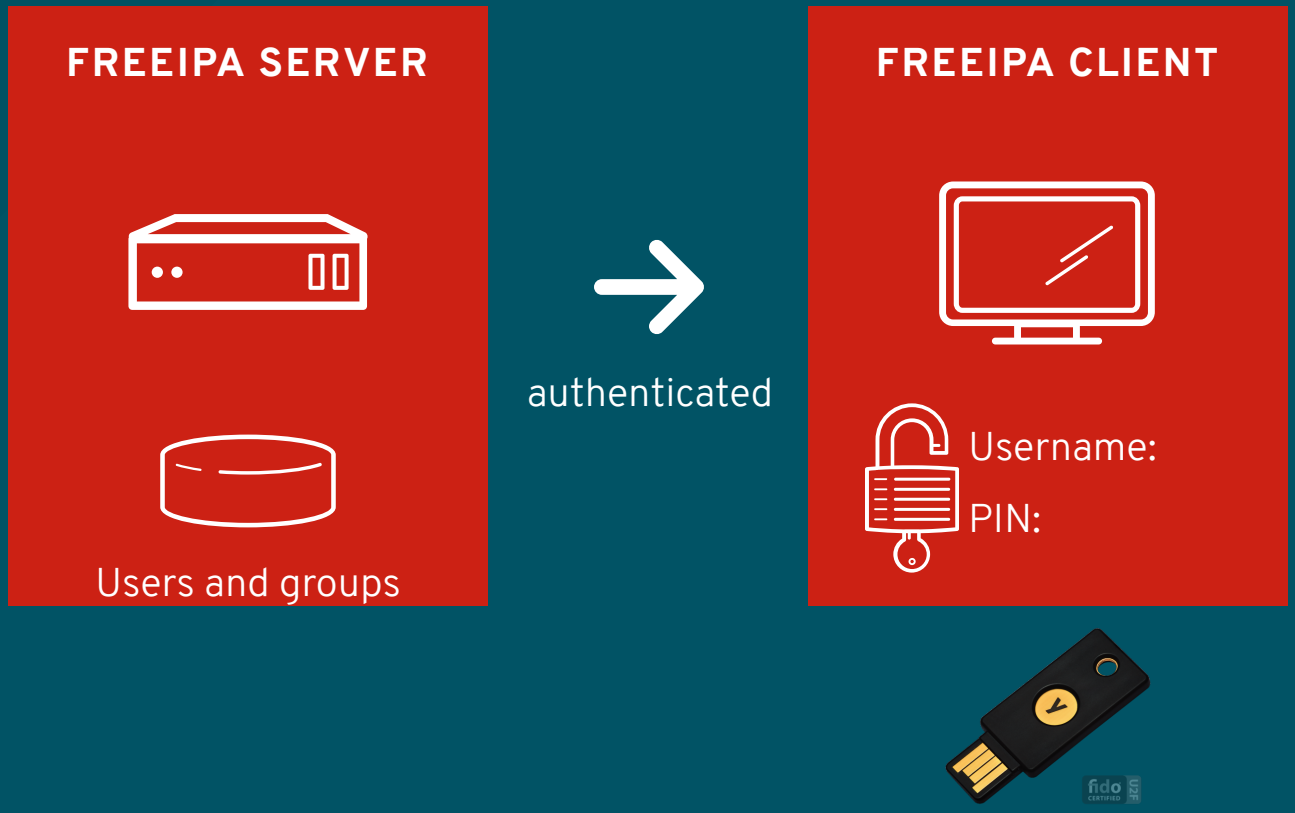
Users and groups

FREEIPA CLIENT

Username:

PIN:

SMART CARD AUTHENTICATION



RESOURCES

FREEIPA

- Project wiki: http://www.freeipa.org
- Project trac: https://fedorahosted.org/freeipa/
- Code: https://git.fedorahosted.org/cgit/freeipa.git/
- Blog aggregation: http://planet.freeipa.org/
- FreeIPA demo instance in the cloud: http://www.freeipa.org/page/Demo
- Mailing lists:
  - freeipa-users@redhat.com
  - freeipa-devel@redhat.com
  - freeipa-interest@redhat.com

redhat®

THANK YOU!

linkedin.com/company/red-hat

twitter.com/RedHatNews

facebook.com/redhatinc

plus.google.com/+RedHat

youtube.com/redhat