FAST OTP for MIT Kerberos

There is more than one password

Linus Nordberg, NORDUnet A/S

2011 Kerberos Conference & Interop Event

NORDUnet
Nordic Infrastructure for Research & Education

Outline

1. Intro
2. One-time passwords
3. OTP pre-auth rundown
4. The OTP plugin
5. Current status
6. Try the OTP plugin

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

About

- FAST is the "flexible authentication secure tunneling" padata type
- OTP is one-time passwords
- This presentation is about a FAST factor, implemented as a preauth plugin, authenticating users using one-time passwords

This work

- This work was funded by the internet fund of .SE, the fine people running the swedish top level domain .se
- The work is based on FAST (RFC 6113) and draft-ietf-krb-wg-otp-preauth
- The goal of this presentation is that some of you play with the OTP plugin
- Focus on how to configure and run the OTP plugin

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

OTP models

- Event-based – press a button to generate the next OTP
- Time-based – wait some and the next OTP is generated
- Add a challenge
- A PIN can be used to protect the token and also for strenghtening the generated OTP

Problems

- Short password – need protection against guessing
- Synchronous operation – makes backend service redundancy harder
- Synchronisation – a token might get out of synch with the server

An OTP standard, HOTP

- OATH is the open authentication initiative, see `http://www.openauthentication.org`
- HOTP is an HMAC-based OTP algorithm by OATH, see RFC 4246
- Pick a secret, get a counter
- Calculate the HMAC-SHA-1 of the secret and the counter
- Truncate the result and turn it into six (or more) decimal numbers
- The Oath-toolkit package and the Yubikey are two implementations

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

2-pass or 4-pass?

4-pass

- Client sends an AS-REQ
- Kdc sends a KRB-ERROR with a nonce in padata
- Client sends another AS-REQ, with encrypted nonce in padata
- KDC sends an AS-REP

2-pass or 4-pass?

2-pass

- Client sends an AS-REQ with encrypted timestamp
- KDC sends an AS-REP

Using the OTP for key generation or not

The must-encrypt-nonce variant

- The client and the KDC bot calculate the next OTP and generates keys (client key and reply key) using this shared secret
- If the nonce decrypts correctly, the client has proved knowledge of the client key and by that knowledge of the OTP
- The KDC uses the reply key to encrypt the AS-REP and proves its identity by knowledge of the key and thus the OTP

Using the OTP for key generation or not

The other alternative – the OTP is not available to the KDC

- The FAST armor key is used as both client key and reply key
- No authentication of the KDC is provided

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

OTP plugin outline

- Plugin system with "otp methods", f.ex. basicauth or yubikey
- OTP tokens configured for principals by the new key/value tl_data type mechanism (set_string/get_strings)
- A principal has zero or more tokens configured
- A token in the kdb consists of an identity, a method and an optional opaque blob which is passed to the method

Implementation details

- The verification backend system might be blocking – solved by libverto
- XXX
- XXX

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

Feature set

- A FAST plugin ‘otp’ implementing draft-ietf-krb-wg-otp-preauth
- The FAST plugin implements a plugin framework for ‘OTP methods’
- OTP methods ‘basicauth’ and ‘ykclient’ implementing HTTP/HTTPS basic authentication and Yubico mode

Tested OTP systems

- Oath-toolkit/oathtool –> Apache + mod_authn_otp
- Yubikey in OATH mode –> Apache + mod_authn_otp
- Yubikey in Yubico mode –> Yubiserve

What's missing

- Support for 2-pass variant
- Support for OTP systems where the client does not include the OTP in the PA-OTP-REQUEST
- Support for connected tokens
- Support for PIN change

In the pipe

- Moving verification backend methods out of the KDC process
- kinit prompting for password
- Policy for expressing what's required for authenticating – OTP or static, OTP and static, one OTP or another OTP, one OTP and another OTP?

Outline

1 Intro
2 One-time passwords
3 OTP pre-auth rundown
4 The OTP plugin
5 Current status
6 Try the OTP plugin

Innstall, configure, run

See
`https://www.nordu.net/~linus/INSTALL-krb5-fast-otp.`