A Talk about MS-SFU Kerberos Extensions:

Protocol Transition (S4U2Self) & Constrained Delegation (S4U2Proxy).

Isaac Boukris

SambaXP 2019

Agenda

- Why S4U2Self is important for Samba.
- How does it work in local and cross realm.
- Recent CVEs related to S4U2Self.
- A couple of words on S4U2Proxy and RBCD.

What is S4U2Self and why you should care

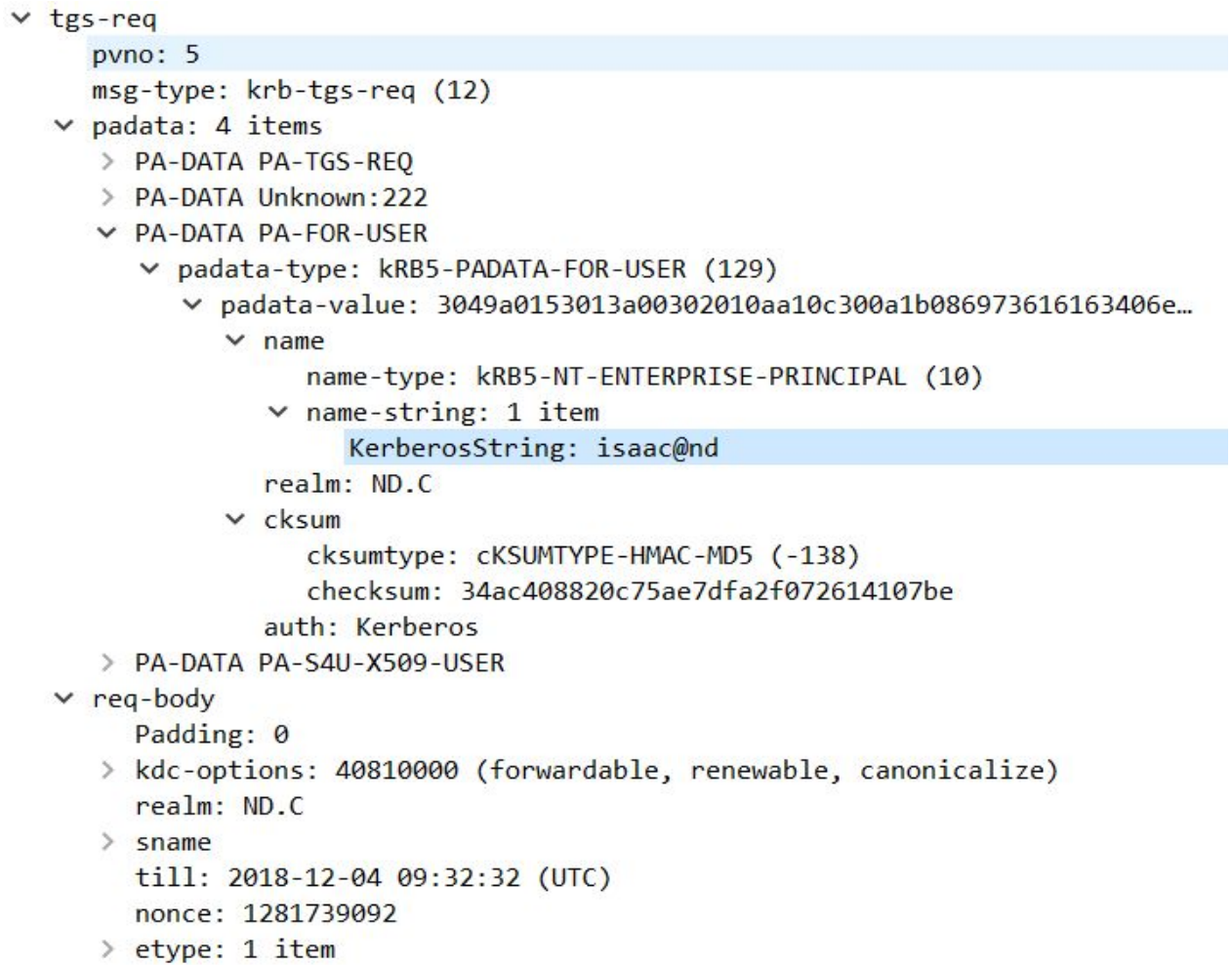
- Any server providing resources needs to have a mean to authenticate the user and to get a the list of groups the user is member of for authorization.
- Usually user’s password is required to get user’s token (Kerberos or NTLM).
- Any other authentication schemes (TLS, OTP, name it) can’t get us a token.
- LDAP is the problem - not the solution.
- The consensus on Samba ML is that the best solution is S4U2Self.
  - Supports enterprise-names and and X509 certificates.
  - We can and should implement S4U2Self within winbind!

How does it work

- PA-FOR-USER.
- PA-S4U-X509-USER - only implemented in MIT.
- Cross Realm S4U2Self - only implemented in MIT.
- TODOs:
  - Porting S4U code from MIT to Heimdal.
  - Add test coverage to Samba MIT build.

MS-SFU 2.2.1
PA-FOR-USER:

The PA-FOR-USER padata value is protected with the help of a *keyed* checksum, as defined below...



CVEs related to S4U2Self

- Samba **CVE-2018-16853:** A user in a Samba AD domain can crash the MIT KDC by requesting an S4U2Self ticket.

  https://github.com/samba-team/samba/commit/6ab51b2af90f5dca11b8587b2a16215ab4497069

  https://github.com/samba-team/samba/commit/6c453aeb0c771d14fe501e9a37d9f51b9403872b

- MIT Kerberos **CVE-2018-20217:** Reachable Assertion. If an attacker can obtain a krbtgt ticket using an older encryption type (single-DES, triple-DES, or RC4), the attacker can crash the KDC by making an S4U2Self request.

  https://github.com/krb5/krb5/commit/94e5eda5bb94d1d44733a49c3d9b6d1e42c74def

- Samba **CVE-2018-16860** / Microsoft **CVE-2019-0734:** S4U2Self with unkeyed checksums.

  https://github.com/samba-team/samba/commit/43958af1d50f0185e21e6cd74110c455ee8996af

  A python tool for intercepting and manipulating Kerberos packets, can be used to test KDC handling of unkeyed S4U2Self requests:

  https://github.com/iboukris/S4U/blob/master/kintercept/kintercept.py