Negotiating FAST

Sam Hartman

Painless Security, LLC

IETF 75

November 11, 2009

THE PROBLEM

- `draft-ietf-krb-wg-preauth-framework` provides a way to protect the Kerberos exchange.
-
- We need a way to securely determine whether a KDC supports FAST.
- We need to secure the process used to obtain the armor ticket.

GOALS

- ➜ Protect the list of enctypes the client sends when obtaining an armor ticket
- ➜ Determine whether a KDC supports FAST without opportunity for an attacker to force a downgrade

PROPOSAL

Proposal Overview

- ➜ Include integrity-protected checksum of AS-REQ in AS-REP
- ➜ Include integrity-protected indication of FAST availability in AS-REP
- ➜ Provide client mechanism to request this extension
- ➜ Use ticket flag to always indicate availability of extension

Introducing Encrypted Padata

- Windows 2000 introduces a padata field in the encrypted part of the AS-REP.
- This field provides an extensible typed hole for integrity-protected data.
- Currently used to provide security for referrals.
- Propose to standardize this AS-REP extension.

Client Request

- ➜ Include a new PA type in armor ticket AS-REQ
- ➜ New PA-Type indicates support for encrypted padata and requests protected negotiation

KDC Reply

- Include checksum of AS-REQ in encrypted padata
- Include an encrypted padata item if FAST is supported.
- Checksum over AS-REQ protects encryption types and other parameters.

Protecting Against Downgrade

- KDC always sets ticket flag indicating support for this extension
- Client fails authentication if ticket flag is set and encrypted padata not received
- Client stores information on FAST availability; if FAST is indicated as available then client fails if it is later not used.