Supporting IPSec with Legacy Credentials

Steven M. Bellovin

Florham Park, NJ 07932

AT&T Labs Research

973-360-8656

smb@research.att.com

Steven M. Bellovin
The IPSRA Charter

to AH, ESP or IKE protocols.

The WG strongly prefers mechanisms that require no changes
authenticaiton mechanisms.

... authenticaiton to an IPsec device running IKE, using Legacy
authenticaiton to an IPsec device running IKE, using Legacy

to define a standard mechanism to accomplish human user

Rationale

Legacy Credentials
My Goals and Non-Goals

- To demonstrate that there are many ways to accomplish our objectives without touching IKE.
- To build on existing tools and protocols.
- To avoid producing a standards-track RFC. (If this RFC is ever advanced, I've failed.)

Steven M. Bellovin — March 29, 2000
Legacy Credentials

Approach

- Use SSL/TLS.
- Use existing HTTP and HTML syntax.
- Perhaps permit use of Web browsers, with added manual steps or automated plug-ins.
Four Suggestions

- Server-generated shared secrets.
- Server-side key storage.
- Server-side key pair generation.
- Client-side certificate generation.

---

Legacy Credentials

Steven M. Bellovin — March 29, 2000
Server side does nothing — certificates are self-identifying.

- Module
- Application (or user) conveys certificate and private key to IKE
- Server signs and returns certificate.
- Standard HTTP-style authentication is used.
- Client generates RSA key pair; uploads public key via SSL/TLS.
- Server sends (Netscape-standard) <KEYGEN> tag.

**Client-side Certificate Generation**
Server-side Key Pair Generation

Server generates high-quality key pairs in its spare time.

No risk here to server retaining private key — the server controls all access no matter what, and this certificate is used for nothing else.

Client uses HTTP authentication and SSL/TLS to request a certificate.

Legacy Credentials

Steven M. Bellovin — March 29, 2000
The user's long-term certificate and encrypted private key are stored on the server. After HTTP-style authentication, both are returned under protection of TLS. Client decrypts and uses private key.

- Can be used with global PKI or locally-generated certificates.
- Server-side key storage
SSL/TLS required for earlier schemes is expensive; the result is then
discarded, to be followed by an equally-expensive IKE exchange.

Instead, use the authenticated SSL/TLS session to pass back a
transient shared secret.

Authentication server then passes the secret to the IKE server.

Permits use of cheaper IKE variants.
Issues

Legacy Credentials

- Clients MUST verify server-side TLS certificate.
- Must resolve issue of certificate expiration versus SA expiration, and balance against desire for reuse of legacy authentication technique.
- Isn’t standard HTTP, since the user doesn’t return there. Standard Web browsers are a poor match for such cards — but this authentication.
- Designed to permit back-end RADIUS servers, including token card.

Steven M. Bellovin — March 29, 2000
There are many ways to solve this problem.

- A hybrid of the second and third schemes is a big step towards use of a PKI with client-side certificates.
- Existing building blocks are quite sufficient.
- We don’t need to touch IKE.