Proxies in
AAA Key Management

Russ Housley

General Area Director
(Former Security Area Director)

Introduction

- The “Housley Criteria” was first presented in March 2003, and it became RFC 4962
- RFC 4962 offers no guidance on Proxies
- This presentation offers personal opinions on Proxies in AAA key management
  - Not a mandated from an Area Director
  - Not consensus of any group

Proxies

- Proxies behave like servers, yet pass the work on, employing the same protocol
  - Appear as a server to their client
  - Appear as a client to the upstream server

Two Environments to Consider

- Enterprise
  - Client wants to be connected only to their enterprise
- Service Provider
  - Client willing to connect to any service provider that has an agreement with their home AAA server
  - Client just wants their traffic to flow
  - Client does not want to be surprised when the bill arrives

Proxies in these Two Environments

- Enterprise
  - – If Proxies are used, they are operated by the enterprise
- Service Provider
  - – Proxies operated by different service providers
  - – Agreements or contracts between the service providers
  - – Since the Proxy can be invisible to the Client, one must consider the AAA servers and Proxies as a distributed implementation

Server Provider Proxies

- When operated by different organizations, agreements or contracts must be in place to make this situation as secure as possible because:
  - Key sharing cannot be avoided
  - The sharing is invisible to the Client

Interpretation of RFC 4962 for the Service Provider Environment

- Limit key scope
  - AAA Server and Proxies are part of the same key scope
- Authenticate all parties
  - AAA Server and Proxies indistinguishable by the other parties – cannot be authenticated separately
- Keying material confidentiality and integrity
  - AAA Server and Proxies may share keys
  - Confidentiality and integrity on transfer

Questions?