PINT Security Requirements

Steven M. Bellovin

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Basic PINT Security Principle

- If you make a call, you are responsible for it.
  - You pay for it.
  - You are responsible if the call is illegal, immoral, or improper.
- Any other arrangements are by prior agreement.

IN Views

- Whoever makes a request of the IN node is responsible for the call.
- Therefore, the IN node must authenticate the requestor.
- Other responsibility arrangements require *authorization*, based on the authenticated identity.
- Internal relays of the request must be authenticated, too, though (possibly) without cryptography.

Payment Models

- Hop-by-hop — IN authenticates requestor; requestor authenticates customer.
  - From IN's point of view, if the customer disputes the charge, the requestor is responsible.
- End-to-end — customer signs request; requestor forwards it.
  - Again, if the customer disputes the charge, the requestor is responsible.
  - But, if the customer has an agreement with the IN operator, and the request is digitally signed, then the customer might be held responsible.

Authentication Models

- SSL plus a PIN may suffice, for customer-to-requestor or requestor-to-IN.
- SSL with client-side certificates is much better.
- IPSEC is probably good for requestor-to-IN; it is probably not good for customer-to-requestor, unless user-oriented keying and certificates are used.
- Customer requests must be digitally signed, even within SSL, or they aren't forwardable. (SSL here may be necessary for customer privacy.)

Other Aspects

- Customer privacy is important. Encryption of requests SHOULD be done.
- On the IN side, the toll fraud people like to do traffic analysis. Make sure there's an interface that can supply all possible information.