Anomalous Behavior with Anonymous Tickets

Frederick Butler[1], Iliano Cervesato[2], Aaron D. Jaggard[2], and Andre Scedrov[3]

IETF-65

Kerberos WG

20 March 2006

[1]West Virginia University, [2]Tulane University, and [3]University of Pennsylvania

Partially supported by ONR and NSF

Setup of Anomaly

The AS Exchange takes place as usual, producing TGT and k_{TC}:

C ⟷ KRB-AS-REQ ⟷ K

KRB-AS-REP (TGT, k_{TC})

The client C requests a regular and an anonymous ticket (both for S) using TGT:

C → KRB-TGS-REQ (Regular, based on TGT) → T

C → KRB-TGS-REQ (Anonymous, based on TGT) → T

The TGS T replies, but the intruder I switches the tickets (undetected by C):

C ← $\{SK_{Anon}, Anon, ...\}k_S, \{SK_C, ...\}k_{TC}$ ← $\{SK_C, C, ...\}k_S, \{SK_C, ...\}k_{TC}$ ← T

C ← $\{SK_C, C, ...\}k_S, \{SK_{Anon}, ...\}k_{TC}$ ← I ← $\{SK_{Anon}, Anon, ...\}k_S, \{SK_{Anon}, ...\}k_{TC}$ ← T

- **C has wrong beliefs about data**
- Undesirable, but doesn't violate design goals. However, ...

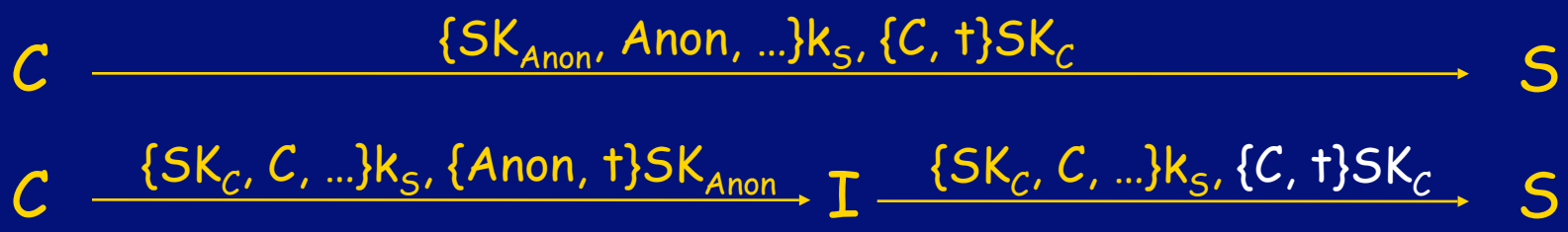
- SK_C and SK_{Anon} are service keys generated for regular and anonymous tickets.
- $\{m\}k$ is the encryption of m with k.

Options for Final Step

1. C's name is leaked when she tries to contact S anonymously:

Intruder actions integral if this message's integrity is protected [Tom].

2. Alternatively, C sends each type of request. The request with anonymous ticket gives error, but I fixes other request by replaying first authenticator.



I then tampers with error message so that it names C. C believes anonymous request accepted (no error), regular request failed; reverse is true instead.

•C's name is leaked or she has wrong beliefs about which type of request succeeded/failed.

Conclusions

- No violations of authentication or confidentiality, but anomalous behavior
  - Possible to leak C's name (even if link to S is integrity protected)
  - Possible for C to have reversed view of which type of request has been accepted
- Are these (or related issues) of practical concern?
- We should be aware of possibility for these types of problems.