

# Analysis of Kerberos 5 Using MultiSet Rewriting

Frederick Butler (UPenn), Iliano Cervesato (ITT Industries), Aaron D. Jaggard (Tulane, formerly UPenn), and Andre Scedrov (UPenn)

Partially supported by the CIP/SW URI "Software Quality and Infrastructure Protection for Diffuse Computing" through ONR grant N00014-01-1-0795

Appeared in part in 2002 IEEE Computer Security Foundations Workshop

## Kerberos Project Goals

- Give precise statement and formal analysis of a real world protocol
  - Formalize and analyze Kerberos 5 using MultiSet Rewriting (MSR)
- Identify and formalize protocol goals
  - What sort of authentication?
- Give proofs of achieved protocol goals
  - Gain experience in reasoning with MSR
- Note any anomalous behavior
  - Consider possible fixes, test these

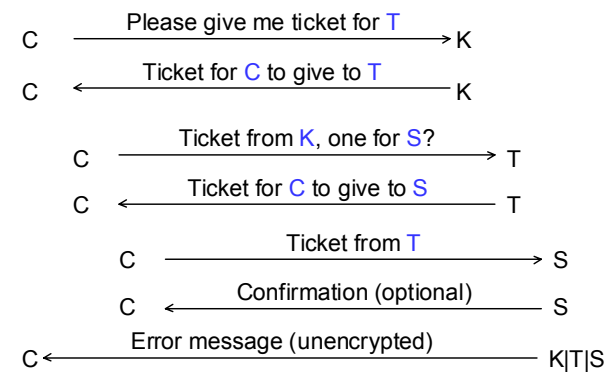
## Achievements

- Formalizations of fragments of Kerberos 5
  - MSR can handle real world protocols
- Formal analysis of protocol
  - Proofs of protocol properties
    - Using rank and corank functions
    - Properties and proofs show parallels between abstract and detailed formalizations
  - Curious behavior seen
    - Doesn't prevent authentication, but slightly weakens properties which hold for Kerberos 4
- Interactions with Kerberos designers

## Kerberos 5

- Authentication
  - Repeatedly authenticate a client to multiple servers
- Client **C** wants ticket for end server **S**
  - Tickets are encrypted – unreadable by **C**
- **C** first obtains long term (e.g., 1 day) ticket from a Kerberos Authentication Server **K**
  - Makes use of **C**'s long term key
- **C** then obtains short term (e.g., 5 min.) ticket from a Ticket Granting Server **T**
  - Based on long term ticket from **K**
  - **C** sends this ticket to **S**

## Protocol Messages



## Formalizing Kerberos

- Use MSR 2.0 + some extensions
  - MSR development supported by ONR MURI
- Abstract formalization
  - Contains core protocol
    - Enough detail to prove authentication and confidentiality
  - Exhibits some curious behavior
    - This is due to the protocol structure, not omitted detail
- Two detailed formalizations
  - One adds options and checksums
    - Authentication and confidentiality properties hold here
    - Exhibits additional curious behavior involving options
  - One adds timestamps (still to be analyzed)

## Proof Methods

- Two classes of functions defined on MSR facts
  - k-Rank
    - Data origin authentication
    - Work done to encrypt a specific message with key k
  - E-Corank
    - Confidentiality
    - Work needed to extract information using keys from the set E
  - Inspired by work of Schneider in CSP
    - Our corank functions parallel his rank functions
- Effects of MSR rules on these functions
  - Find conditions which ensure that rank/corank cannot be increased/decreased by a malicious intruder

## Properties Proved

- Client and Ticket-Granting Server
  - Authenticity of ticket-granting ticket
  - Confidentiality of associated session key
  - For both abstract and detailed (with options) versions
    - The structure of the abstract theorems and proofs can be recovered from the structure of those for the detailed version
- Client and End Server
  - Authenticity of service ticket
  - Confidentiality of associated session key
  - For abstract level
    - Similar theorems appear to be true for detailed formalization

## Sample Authentication Theorem

- For Ticket-Granting Exchange in detailed version
    - Prove this by adding details to abstract level proof
    - Assume long-term keys safe (+ technical assumption)
- If **T** processes the message  $\{TFlags, k_{CT}, C\}_{k_T}, \{C, ck, t\}_{k_{CT}}, TOpts, C, S, n_2, e$  then some **K** created  $k_{CT}$  and sent  $C, \{TFlags, k_{CT}, C\}_{k_T}, \{k_{CT}, n_1, TFlags, T\}_{k_C}$  and **C** sent some  $X, \{C, ck, t\}_{k_{CT}}, TOpts, C, S, n_2, e'$  with  $ck = \{TOpts, C, S, n_2, e'\}_{k_{CT}}$

## Anomalies

- Encryption type anomaly (detailed formalization)
  - Difficult to recover from lost long term key
- Ticket switch anomaly (abstract and detailed)
  - Client has incorrect beliefs about data in her possession
    - Kerberos 5 does not have all properties of Kerberos 4
    - In detailed version, this can involve 'Anonymous tickets'
    - Anonymous option under review
- Ticket option anomaly (detailed formalization)
  - Replay a ticket; effects similar to ticket switch anomaly but for wider range of options

## Conclusions

- Formalizations of Kerberos 5 at different levels of detail
  - Extended MSR to do this
  - MSR can handle real world protocols
- Proofs of properties which hold here
  - Parallel theorems and proofs in two formalizations
  - Authentication and confidentiality throughout
  - Gained additional experience in reasoning with MSR
- Curious behavior
  - Does not prevent authentication
- Interactions with Kerberos designers

## Future Work

- Systematize definition and use of (co)rank functions
  - Need to determine 'public terms' for corank
- Analysis
  - Relationships between properties in our different formalizations
- Extend formalizations
  - Add structure and functionality, perform analysis
- Continue interaction with Kerberos designers
- Connect methods to automated tools