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

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)

Protocol Messages
- Please give me ticket for \( T \) to \( K \)
- \( C \) sends ticket for \( C \) to give to \( T \) to \( K \)
- Ticket from \( K \), one for \( S \)?
- \( C \) sends ticket for \( C \) to give to \( S \)
- Ticket from \( T \)
- Ticket from \( C \)
- Confirmation (optional)
- Error message (unencrypted)
- \( K(T|S) \)

Anomalies
- Encryption type anomaly (detailed formalization)
- Difficult to recover from lost long term key
- Ticket switch anomaly (abstract and detailed)
- \( C \) 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)
- \( C \) sends ticket; effects similar to ticket switch anomaly but for wider range of options

Formalizations 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

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)
  \( T \) processes the message
  \( \{TFlags, C, kCT, C, kT, C, TOpts, C, n1, T\} = \{TFlags, C, kCT, C, kT, C, TOpts, C, n1, T\} \)
  \( X, C, T, C, n'1, T\) then some \( K \) created \( kCT \), and sent
  \( (TFlags, kCT, C, kCT, C, TOps, C, n1, T) \)
  and \( C \) sent some
  \( (TFlags, kCT, C, kCT, C, TOps, C, n1, T) \)
  with \( kCT = \{TFlags, C, kCT, C, TOps, C, n1, T\} \)

Conclusions
- Formalizations of Kerberos 5 at different levels of detail
- \( C \) extends 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