FORMAL SPECIFICATION AND ANALYSIS OF GROUP DOI FOR ISAKMP

Catherine Meadows
Code 5543
Center for High Assurance Computer Systems
Naval Research Laboratory
Washington, DC 20375
meadows@itd.nrl.navy.mil

PURPOSE OF THIS WORK

- Perform a formal specification and analysis of GDOI using the NRL Protocol Analyzer
  - **NRL Protocol Analyzer - specialized formal methods tool developed for security analysis of crypto protocols**
- Perform analysis early on in standards process for maximum impact
- Speed up acceptance of GDOI by use of formal analysis
  - **Finding and removing bugs and ambiguities**
  - **Providing evidence of soundness**
- Learn more about strengths and limitations of the NRL Protocol Analyzer and formal analysis in general

THE NRL PROTOCOL ANALYZER

- Formal methods tool for verifying security properties of crypto protocols and finding attacks
  - **Already used to analyze substantial portion of IKE**
- User submits security requirements to tool
- NRL Protocol Analyzer works by either
  - **Constructing a proof that no attack (violation of the requirement) is possible**
  - **Demonstrating an attack**

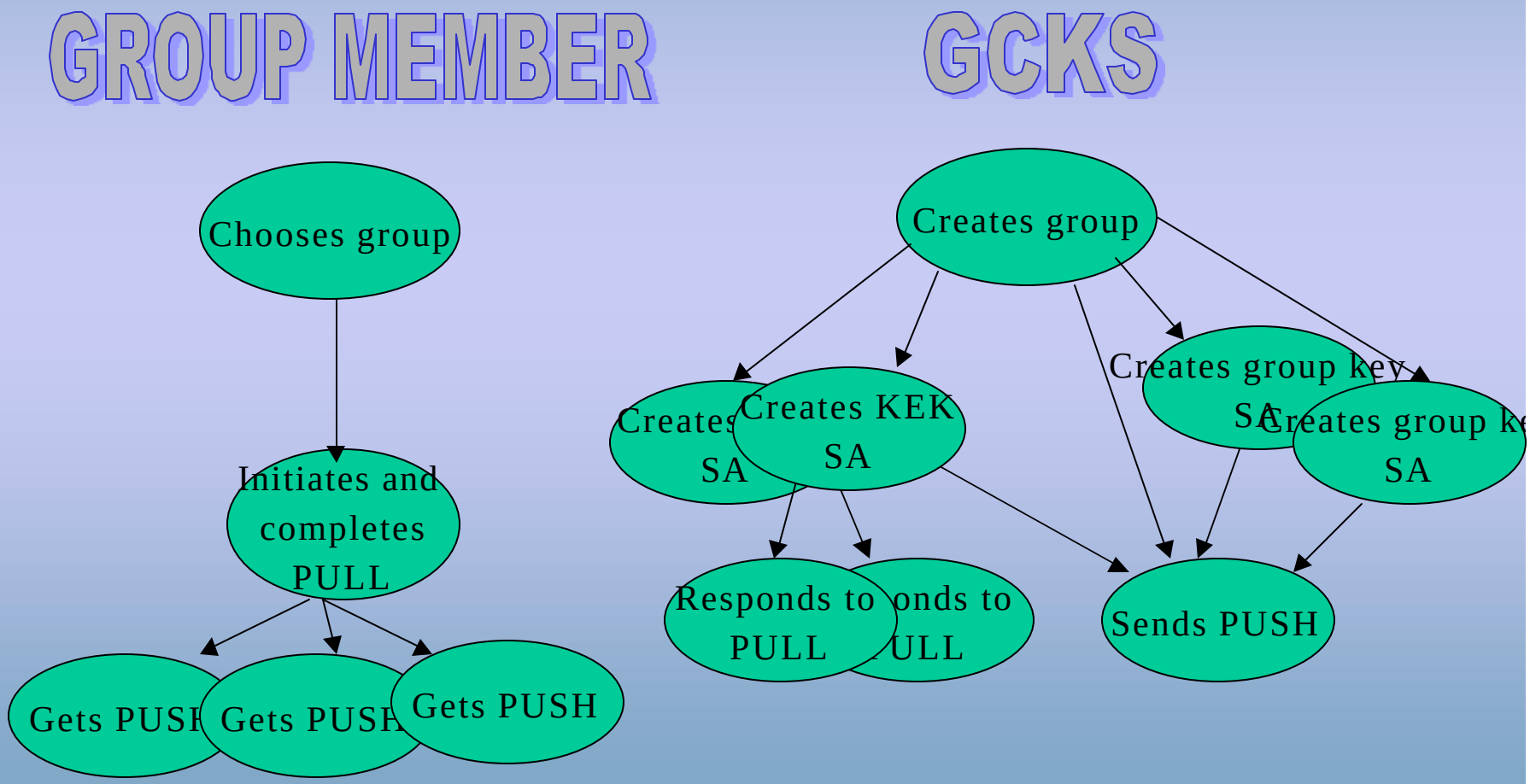
VERIFICATION TO-DO LIST

- Write formal specification
  - **Done**
- Prove initial lemmas
  - **Done**
- Formally specify security requirements of protocol
  - **Have initial list, currently being refined & added to**
- Prove that protocol satisfies security goals

WHAT WE SPECIFIED

- Assume unbounded number of groups and unbounded number of members
  - **One GCKS for each group**
  - **Members may belong to more than one group**
- GCKS starts by creating group & group key
- Group member starts by by initiating a PULL Exchange
  - **GCKS responds by completing exchange**
- GCKS creates new keys when initializing group and preparing PUSH Datagram
- GCKS may send PUSH Datagram at any time after creating group
- Currently not addressing key hierarchies
  - **Investigating feasibility of doing so in future work**

STRUCTURE OF SPECIFICATION



BENEFITS SO FAR

As a result of writing specification:

- Found a number of small errors and ambiguities
- Found one major inconsistency, in handling of sequence numbers
- Timely identification of these problems made it possible to remove them before spec sent to IETF

As a result of writing formal security requirements:

- Suggestion for improving security of POP
- Expect to come up with other insights as we continue

Conclusion

- Although it is only part of the analysis process, formal specification a helpful way to identify potential problems in GDOI early
- What seemed most helpful was
  - **concreteness and unambiguity of the NPA specification**
  - **Still at relatively high level of abstraction, allowing for "rapid prototyping"**
  - **Writing security requirements formally forces one to think carefully about goals**
- Continuing with specification and analysis in consultation with GDOI authors
  - **Will share what we learn from security analysis as we shared what we learned from writing specification**