

# Adaptive Cryptographically Synchronized Authentication (ACSA)

TIS Labs at Network Associates

David M. Balenson and David W. Carman, Principal Investigators

Sponsored by the

DARPA/ITO Next Generation Internet (NGI) Program

DARPA Contract # F30602-98-C-0215

Hilarie Orman, Program Manager

Walt Tirenin, Rome Laboratory, COTR

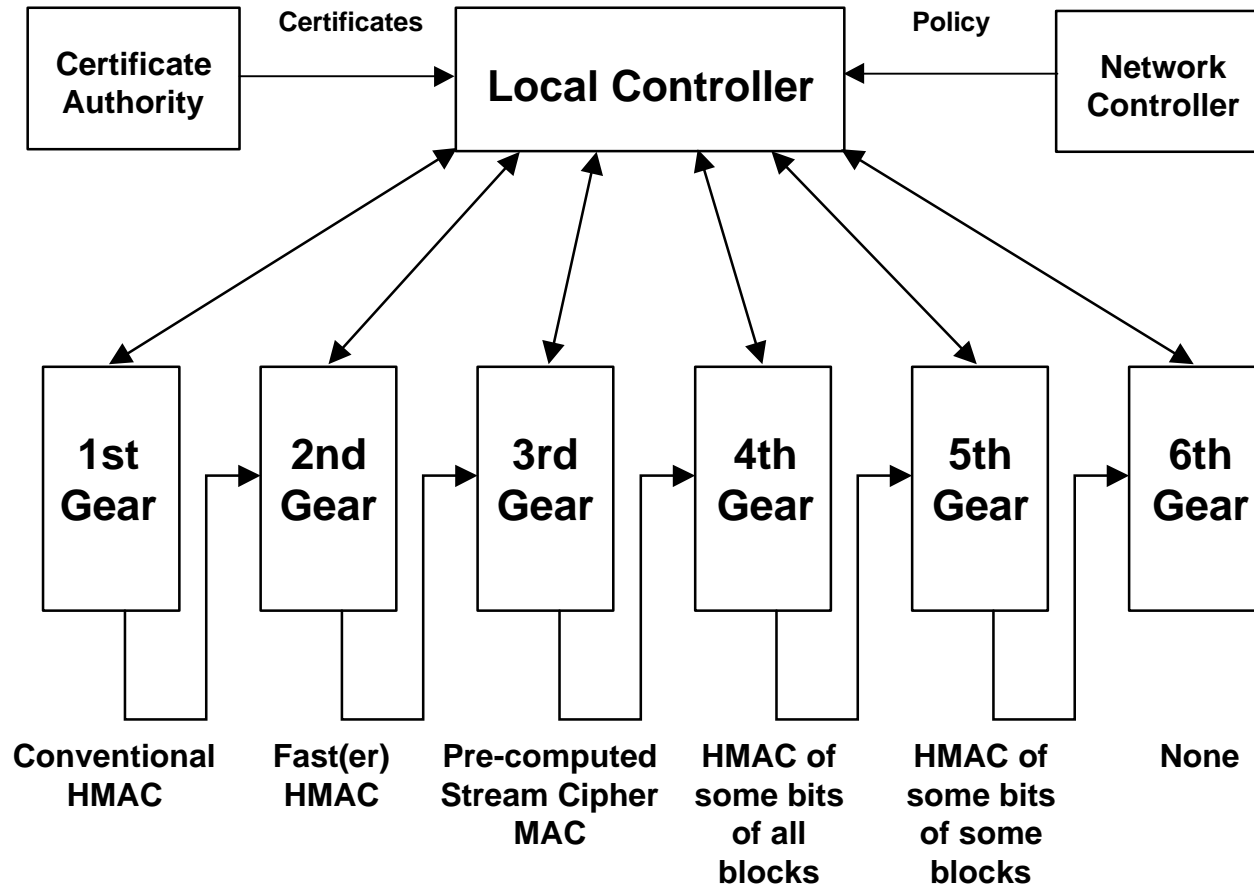
# Overview

- Project Goal and Objectives
- High-Level Model
- Approach
- Discussion Items
  - Scope
  - Other ?

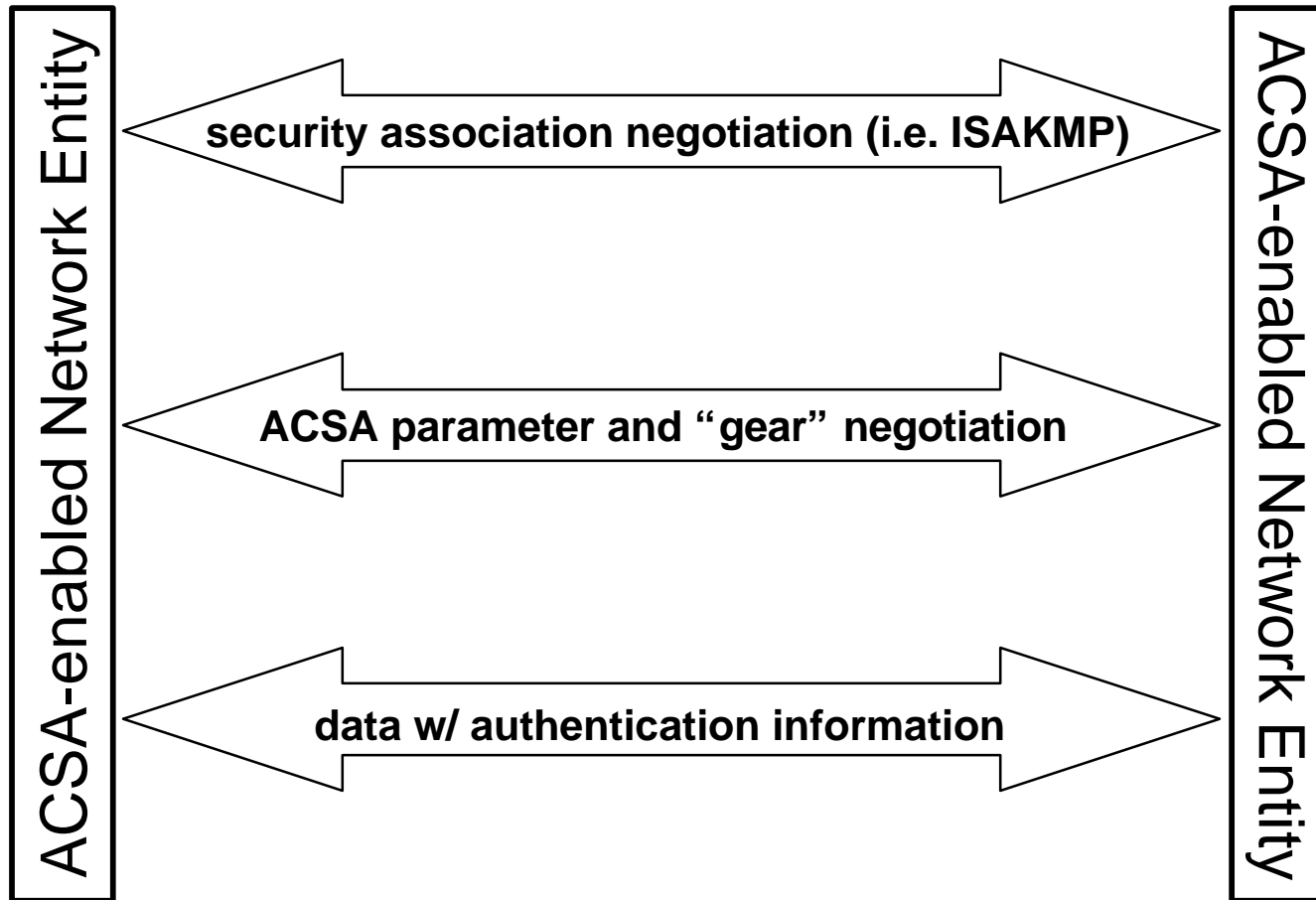
# Project Goal and Objectives

- **Goal:** *Provide a strong authentication solution that meets the demands of ultra-fast networks.*
- **Objectives:**
  - Identify cryptographic mechanisms that can be used to provide various levels of authentication, assuming strong authentication cannot always be provided.
  - Design a control protocol and system that maintains acceptable levels of authentication in a dynamic threat environment.
  - Implement a prototype system that demonstrates effective authentication at various speeds and under various attack scenarios.

# High-Level Model (Local)



# High-Level Model (Network)



# Contract Line Items

- ***CLIN 0001*** - PROTOTYPE SOFTWARE/DEMO
  - Technical tasks as described in the Statement of Work
  - Start date: 07/07/98
  - Completion: 24 months after start date
- ***CLIN 0002*** - DATA
  - Eight CDRL items deliverable to DARPA

# Deliverables - Reports

- Program Progress Reports
  - *CDRL A001* - due quarterly (first report due 100 days after start of CLIN 0001 - 10/15/98)
- Contract Funds Status Reports
  - *CDRL A002* - due quarterly
- Final Report
  - *CDRL A003* - due 30 days after completion of CLIN 0001
- Presentation Material
  - *CDRL A004* - Presentation Material (i.e., Briefing) Slides

# Deliverables - Software

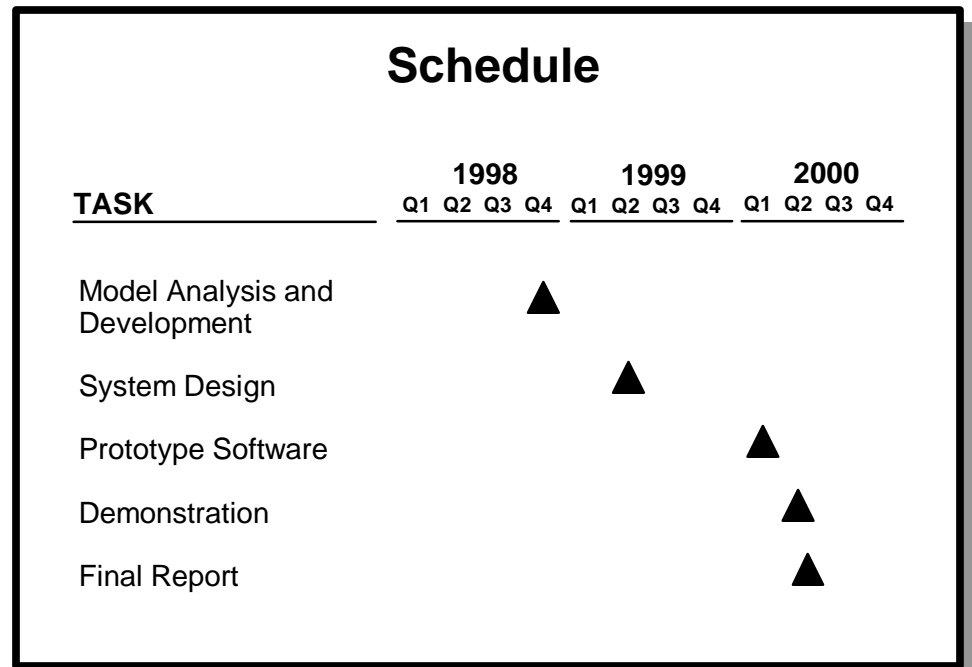
- Prototype Software Product Specification
  - *CDRL A005* - commented prototype software source code due at the completion of CLIN 0001
- Documentation of Prototype Software Product
  - *CDRL A006*
    - draft documentation of prototype software product due 18 months after the start of CLIN 001 (01/07/00)
    - government submits comments within 30 days after receipt of draft copies
    - final documentation of prototype software product due at the completion of CLIN 0001

# Deliverables - Technical Tasks

- Model Analysis and Development
  - *CDRL A007* - Technical Information Report due 5 months after start of CLIN 0001 (12/07/98)
- ACSA System Design
  - *CDRL A008* - Technical Information Report due 10 months after start of CLIN 0001 (05/07/99)

# Project Phases

- System Goals and Requirements Definition
- Model Analysis and Development
- System Design
- Prototype Software Development
- Demonstration
- Final Report



# System Goals and Requirements

- Security
  - “Fall-back” (slow) mode must be as secure as the underlying conventional secure communications protocol
  - ACSA must not expose relevant characteristics of the network entity host (no security “side-effects”)
- Performance
  - Significant performance gains versus conventional ISAKMP for a reasonable risk tolerance
- Implementation
  - Applicability to ISAKMP and other protocols
  - Applicability to various platforms

# Model Analysis and Development

- Investigate candidate authentication mechanisms
- Investigate applicable secure communications protocols
- Further define model components
- Analyze and optimize model components and gear interactions

# System Design

- Design a protocol that facilitates interactions among multiple entities
- Map optimized model into existing protocol(s)
- Define prototype architecture
- Design individual prototype components

# Prototype Software Development

- Design, code and test optimized model software
- Design, code and test secure communications protocol software
- Design, code and test network simulation software
- Integrate prototype system components
- Document software program specification
- Design, code and test demonstration software

**Demo GUI**

**ACSA Model**

**ISAKMP**

**IPSEC**

**Net Simulation**

# Discussion Items - Scope

- Environments
  - Peer-to-peer and Multicast?
    - Multicast environments may often benefit from lower assurance, high-speed authentication
  - Asymmetric relationships?
    - server/client, computation-limited entities
- Prototype
  - Use of licensed components in prototype system?
  - Other communications security protocols?
  - High-speed network components vs. simulation?
  - Operating system: NT vs. Unix?

# Discussion Items - Other ?