

A Formal Analysis of Some Properties of Kerberos 5 Using MSR

Frederick Butler, Iliano Cervesato,
Aaron D. Jaggard, and Andre Scedrov

Supported by ONR URI
To Appear in CSFW 2002

Project Goals

- ◆ Give precise statement and formal analysis of a real world protocol
 - Find a real world protocol - Kerberos 5
 - Pick favorite formalization method - MSR
- ◆ Identify and formalize protocol goals
- ◆ Give proofs of achieved protocol goals
 - Gain experience in reasoning with MSR
- ◆ Note any anomalous behavior
 - Suggest possible fixes, test these

Background

◆ Kerberos 4

- Analyzed using inductive approach (Bella & Paulson)

◆ Kerberos 5

- Simplified version analyzed with Mur ϕ (Mitchell, Mitchell, & Stern)

◆ MultiSet Rewriting (MSR)

- Partially supported by ONR MURI

Achievements

- ◆ Formalizations of Kerberos 5
 - Using MSR + extensions
- ◆ Formal analysis of Kerberos 5
 - Anomalies found
- ◆ Proofs of protocol properties
- ◆ Interactions with Kerberos working group

Introduction

Kerberos Overview

Two Views of Kerberos 5

Anomalies

Formalization

Proof Methods

Protocol Goals and History

◆ Protocol goals

- Repeatedly authenticate a client to multiple servers
- Does not guard against DOS attacks

◆ Kerberos 4 - 1989

◆ Kerberos 5

- Specified in RFC 1510 (1993)
- Subsequent revisions by working group

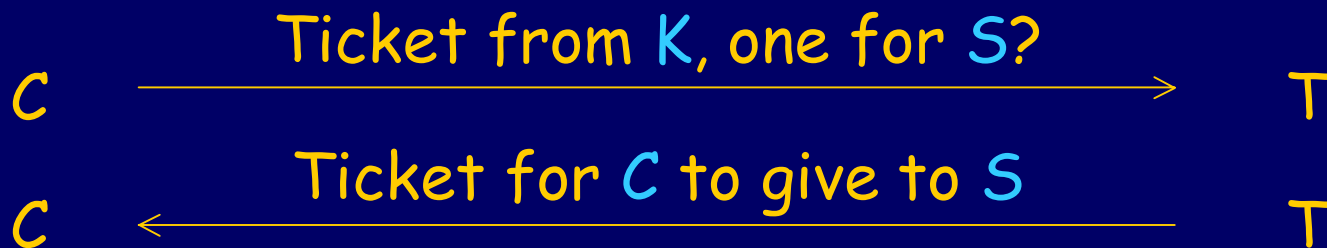
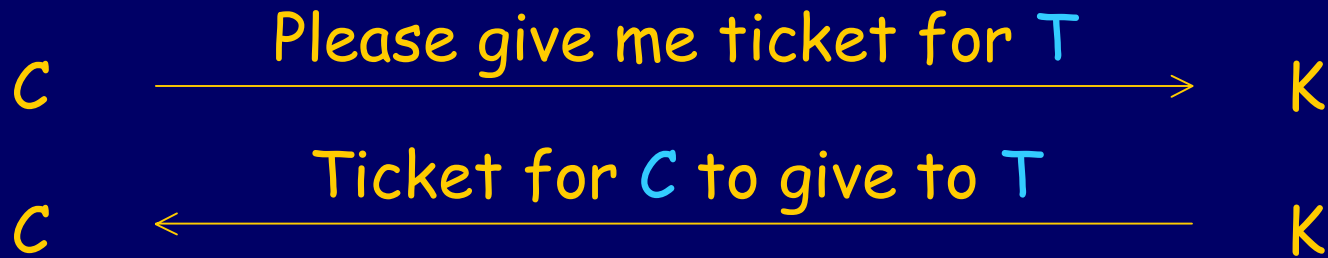
◆ A real world protocol

- Windows 2000 (RFC 1510 + extensions)
- User login, file access, printing, etc.

Kerberos 5

- ◆ 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



Introduction

Kerberos Overview

Two Views of Kerberos 5

Anomalies

Formalization

Proof Methods

Abstract Formalization

- ◆ Contains core protocol
 - Other formalization refines this one
- ◆ Exhibits an anomaly
 - This appears to be structural and not due to omitted detail
- ◆ Allows us to prove authentication results

Detailed Formalization

◆ Uses richer message structure

- Adds some fields for options
- Models encryption type
- Adds checksums

◆ Exhibits anomalies

- Encryption type option specific to this level
- Structural anomaly also seen at abstract level
 - Also variations which use added detail

Introduction

Kerberos Overview

Two Views of Kerberos 5

Anomalies

Formalization

Proof Methods

Encryption Type Anomaly

- ◆ Kerberos 5 allows C to specify encryption types that she wants used in K 's response

C $\xrightarrow{\text{Please give me ticket for } T \text{ using } e_{\text{type}} \text{ (sent unencrypted)}} K$

C $\xleftarrow{\text{Ticket for } C \text{ to give to } T \text{ (other info encrypted using } e_{\text{type}})}$ K

- ◆ C 's key associated with the etype e_{bad} is k_{bad}
 - Intruder I learns k_{bad}
 - C knows this and attempts to avoid $e_{\text{bad}}/k_{\text{bad}}$
 - I can still force k_{bad} to be used

Ticket Anomaly



◆ Kerberos 4:

- Ticket is enclosed in another encryption

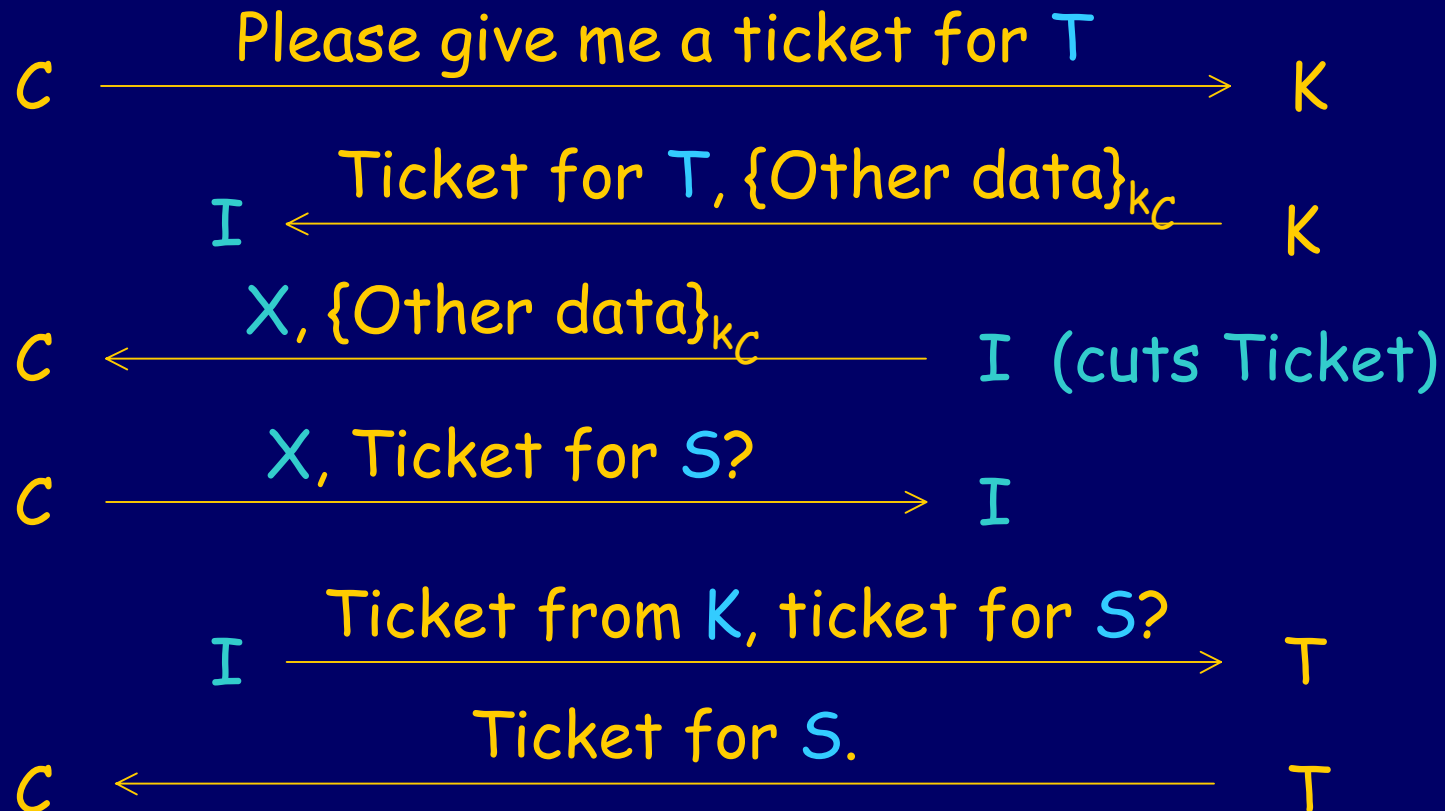


◆ Kerberos 5:

- Ticket is separate from other encryption



Ticket Anomaly



Ticket Anomaly

- ◆ T grants the client C a ticket for S
- ◆ C has never sent a proper request for a ticket
 - C never has the ticket for T
 - C thinks she has sent a proper request
 - C's view of the world is inaccurate
 - Some properties of Kerberos 4 don't hold here
- ◆ Seen in both formalizations
 - Variations possible using added detail
 - Anonymous tickets

Comments from Kerberos Designers

◆ General

- Methods help expose implicit changes and their potential effects
- Would be interested in our analysis of protocol extensions

◆ Encryption type anomaly

- Exists; perhaps more documentation or standardization needed

◆ Ticket anomaly

- Analysis of detailed variations a big help while designing protocol
 - Anonymous option added after RFC written
- Exists, but not of practical concern
- Trying to solve variations of this

Introduction

Kerberos Overview

Two Views of Kerberos 5

Anomalies

Formalization

Proof Methods

MSR Overview

- ◆ Andre's talk yesterday
- ◆ Some extensions added
- ◆ Dolev-Yao intruder

Introduction

Kerberos Overview

Two Views of Kerberos 5

Anomalies

Formalization

Proof Methods

Proof Methods

- ◆ Inspired by work of Schneider
- ◆ Define functions on MSR facts
 - k-Rank - data origin authentication
 - E-Corank - secrecy
- ◆ Proofs
 - State desired property
 - Find applicable (co)rank functions
 - Determine effect of MSR rules on these functions

An Authentication Theorem

◆ If T processes the message

$\{k_{CT}, C\}_{k_T}, \{C\}_{k_{CT}}, C, S, n_2$
then some K sent the message

$C, \{k_{CT}, C\}_{k_T}, \{k_{CT}, n_1, T\}_{k_C}$
and C sent *some* message

$X, \{C\}_{k_{CT}}, C, S', n'_2$

◆ Authenticate data origin using rank

- Show ticket $\{k_{CT}, C\}_{k_T}$ originates with some K
- Show authenticator $\{C\}_{k_{CT}}$ originates with C
 - This makes use of a corank argument for confidentiality

Conclusions

- ◆ Formalizations of Kerberos 5 at different levels of detail
 - Extended MSR to do this
 - MSR can handle real world protocols
- ◆ Anomalous behavior
 - Stated weakened authentication properties which hold for Kerberos 5
- ◆ Proofs of properties which hold here
 - Adapted methods from Schneider
 - Gained additional experience in reasoning with MSR
- ◆ Interactions with Kerberos Working Group

Future Work

- ◆ Investigate fixes for anomalies
- ◆ Give proofs of additional properties
 - Further authentication, confidentiality
- ◆ Continue interaction with Kerberos working group
- ◆ Give additional formalizations
 - Additional structure and functionality
 - Public key extensions
- ◆ Explore use of automated tools

Achievements

- ◆ Formalizations of Kerberos 5
 - Using MSR + extensions
- ◆ Formal analysis of Kerberos 5
 - Anomalies found
- ◆ Proofs of protocol properties
- ◆ Interactions with Kerberos working group