Cryptographically Sound Security Proofs for Basic and Public-key Kerberos

Protocol eXchange

September 2006

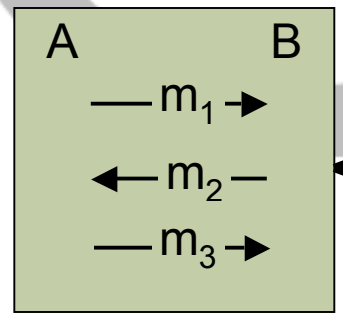
M. Backes[1], I. Cervesato[2], A. D. Jaggard[3], A. Scedrov[4], and J.-K. Tsay[4]

[1]Saarland University, [2]Carnegie Mellon University - Qatar, [3]Tulane University and [4]University of Pennsylvania

Partially supported by ONR and NSF

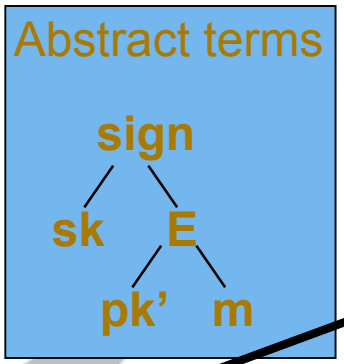
Context

Protocols

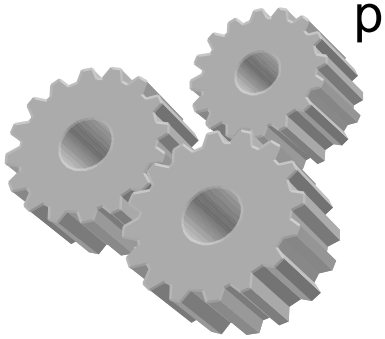


Very hard to get right

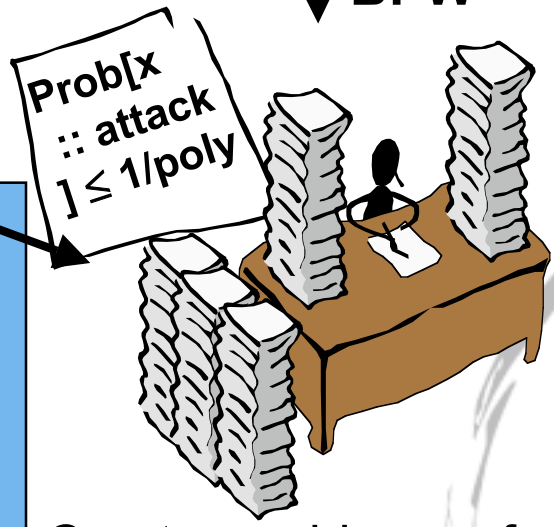
Attacks on e.g. Needham-Schroeder 78, recent Public-key Kerberos, …



Tool-supported proof; but limited adversary



BPW



Cryptographic proof

Want to prove protocols secure in computational model;
So far only for *academic* protocols, e.g. NSL, Otway-Rees, Yahalom [1]

Our work

- First computational analysis of an industrial protocol
  - Analyzed Basic Kerberos 5 and public-key Kerberos
    - Consider authentication and secrecy properties
  - Kerberos is complex
    - E.g. PKINIT uses both public-key and symmetric cryptographic primitives (encryption, signatures, MACs…)
- Proofs were carried out symbolically in the BPW model
  - Proofs in Dolev-Yao style model are cryptographically sound
  - Proofs can be automated (in the future)

Some related work (1)

- Kerberos and other commercial protocols
  - **[Butler,Cervesato,Jaggard,Scedrov'02], [Cervesato,Jaggard,Scedrov,Tsay,Walstad'06]**: Symbolic analysis of Kerberos (basic and public-key) using Multi Set Rewriting
  - **[He,Sundararajan,Datta,Derek,Mitchell'05]**: Correctness Proof of IEEE 802.11i and TLS using Protocol Composition Logic

  ...

Some related work (2)

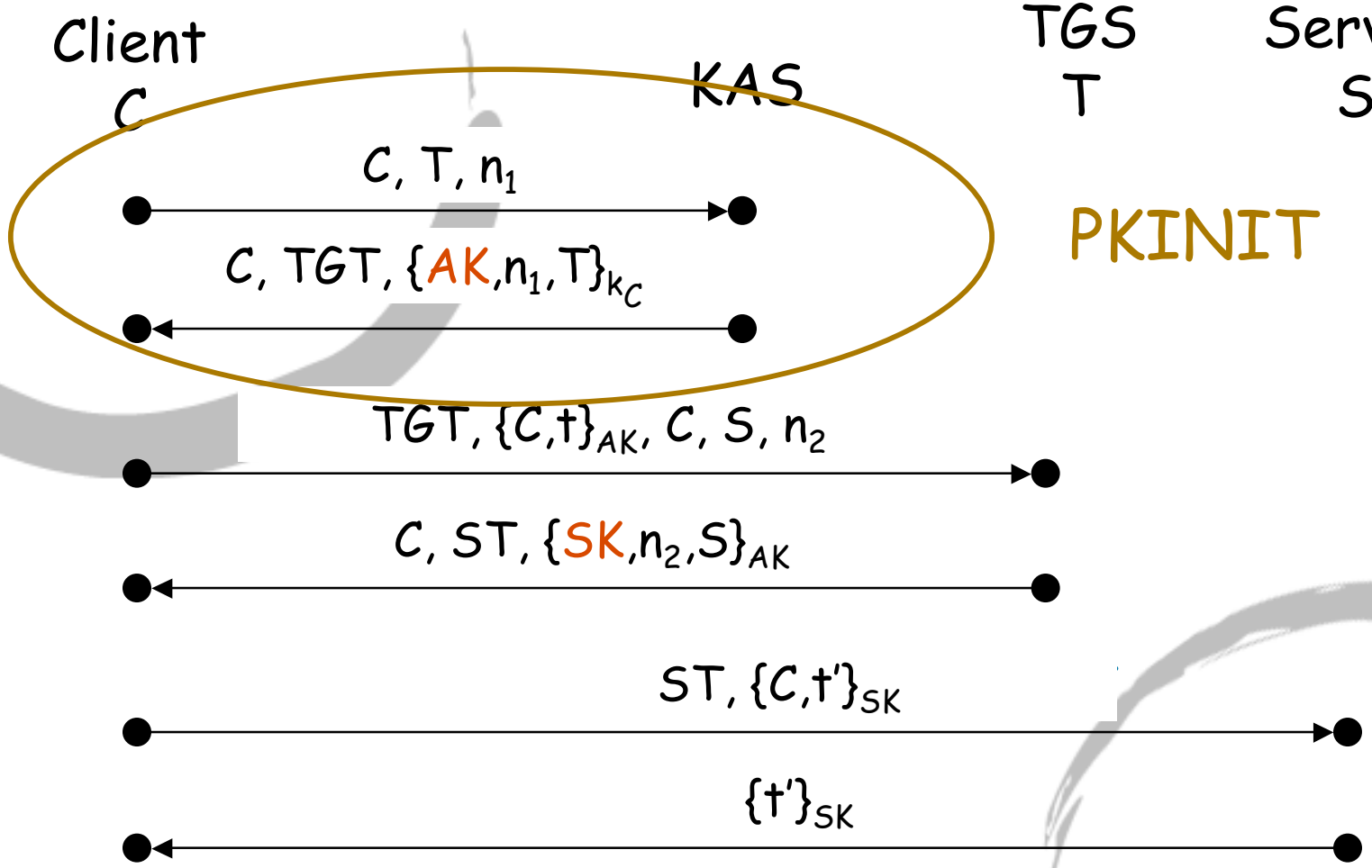
- Linking Dolev-Yao and Cryptography
  - **[Abadi,Rogaway'00], [Laud'04]**: Indistinguishability sound for symmetric encryption under passive, resp. active, attacks
  - **[Backes,Pfitzmann,Waidner'02], [BPW03], [BP04], [BP05]**: Soundness for various security properties under active attacks, for wide range of crypto primitives, within arbitrary surrounding protocols
  - **[Miccancio,Warinschi'04]**: Soundness of integrity for public-key encryption under active attacks
  - **[Canetti,Herzog'05]**: Soundness of key secrecy and mutual authentication for asymmetric encryption under active attacks, within arbitrary surrounding protocols
  - **[Datta,Derek,Mitchell,Warinschi'06]**: Soundness of security properties of key exchange protocols under active attacks

  ...

Kerberos

- Goals
  - Repeatedly authenticate a client to multiple servers on single log-on
    - Remote login, file access, print spooler, email, directory, …
- A real world protocol
  - Part of Windows, Linux, Unix, Mac OS, …
  - Cable TV boxes, high availability server systems, …
  - Standardization and ongoing extension/refinement by IETF (very active --- 10 documents)

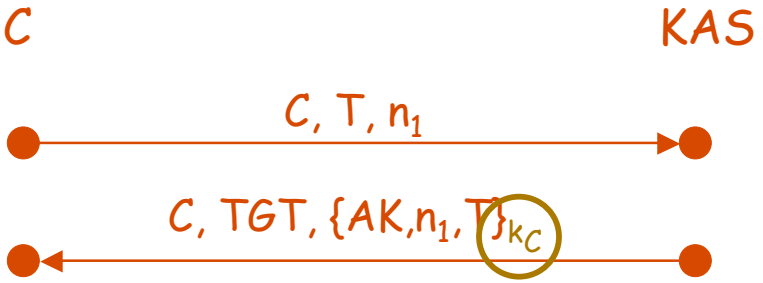
Abstract Kerberos Messages



$TGT = \{AK,C,t_K\}_{k_T}$
$ST = \{SK,C,t_T\}_{k_S}$

Public-Key Kerberos

- Extend basic Kerberos 5 to use Public Keys
  - Change first round to avoid long-term shared keys (k_C)



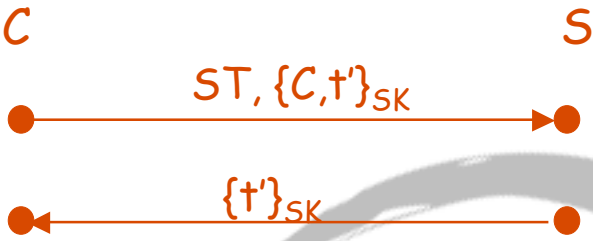
- Motivations
  - Security:
    - Avoid use of password-derived keys
      - Smartcard authentication support
  - Administrative convenience:
    - Avoid the need to register in advance of using Kerberized services

Symbolic Security Properties of Kerberos

- **Property 1 (Key Secrecy):**

  For any honest client C and any honest server S, if the TGS T generates a symmetric key SK for C and S to use (in the CS-exchange), then the intruder does not learn the key SK

last round:



- **Property 2 (Authentication)**

  I. If a server S completes a run of Kerberos, apparently with C, then earlier: C started the protocol with some KAS to get a ticket-granting ticket and then requested a service ticket from some TGS.

  II. If a client C completes a run of Kerberos, apparently with server S, then S sent a valid reply message to C

Computational security of Kerberos (basic and public-key)

- **Theorem (Computational security of Kerberos):**
  If Kerberos is implemented with provable secure cryptographic primitives then Property 1 and Property 2 hold with negligible error probability for all polynomial bounded users and adversaries over the probability space of all runs for a fixed security parameter.
- In particular: Kerberos offers computationally sound authentication
- Proof symbolically using the BPW model
  - Proofs conducted separately for basic and public-key Kerberos; despite its highly modular structure
- Key secrecy in computational model: (later)

The BPW model (1)

- Proposed by Backes, Pfitzmann and Waidner
  - Justifying the Dolev-Yao model
- Pair of detailed system models for cryptographic protocols
  - A **symbolic system** and a corresponding **computational system**.
  - The symbolic system is a Dolev-Yao style deterministic formalism; the computational system the realization of it
- Reactive Simulatability

  - I.e. what a PPT adversary can achieve in the computational system another PPT adversary can achieve in the symbolic system

The BPW model (2)

- Composition Theorem
  - If $s_1 \geq s_2$, then can build system S_2 on s_2, replace s_2 with s_1 to obtain S_1, and have $S_1 \geq S_2$.
- Preservation Theorems
  - Allow us to infer computational results from symbolic proofs for trace properties, various forms of secrecy properties including key secrecy, non-interference, liveness etc.
  - This requires implementation of provably secure cryptographic primitives

The BPW model (3)

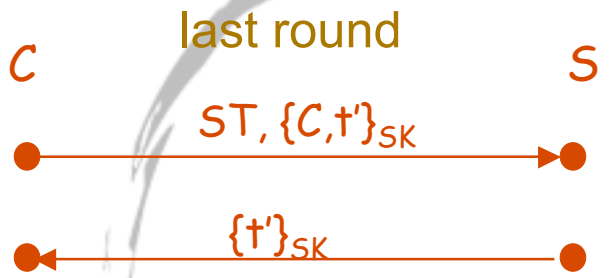
- Only computationally sound symbolic framework comprehensive enough for Public-key Kerberos
  - Both symmetric and asymmetric cryptographic primitives are used
- Some success with automation of BPW model
  - Isabelle theorem prover [BBPSW06]
  - [Backes,Laud'06]: Mechanized tool based on BPW model and type interference

Key Secrecy in Kerberos (1)

- Key secrecy in computational model:
  - Generally accepted notion is Cryptographic Key Secrecy
    - I.e. key must be indistinguishable from random

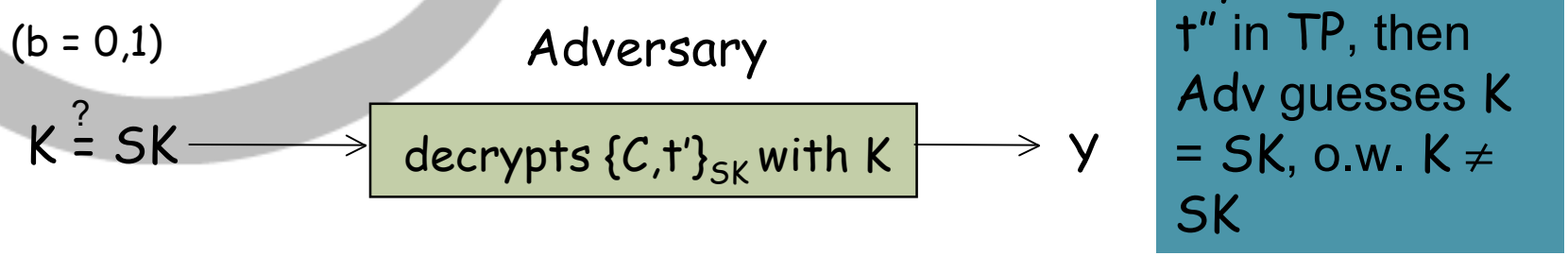
- **Proposition 1:**
  Kerberos does not offer cryptographic key secrecy for the key SK generated by the TGS for the use between client C and server S after the start of the last round

  - SK is used to symmetrically encrypt a message that the intruder partially knows; this leaks partial info about SK



Key Secrecy in Kerberos (2)

- How to distinguish the key SK from a random key:



- Probability that $\{C, t'\}_{SK}$ decrypts to C, t" with t" in TP using K≠SK is negligible

Summary

- First computational proof of authentication for a commercial/real-life protocol
  - Using the Dolev-Yao style BPW model
- Kerberos does not offer cryptographic key secrecy for the key SK shared between C and S
  - Only an optional sub-session key is cryptographically secret

Future Work

- Augmenting the BPW model with tailored protocol logics to further simplify modular reasoning
  - Gives simple and elegant way to integrate numerous optional behaviors of commercial protocols
- Understanding the relation of correctness proofs of (commercial) protocols in MSR and in the BPW model
  - Computationally sound proofs with MSR?

Thank you!