ATIRP Consortium

Advanced Telecommunications/Information Distribution Research Program (ATIRP)

Authentication Scheme for Distributed, Ubiquitous, Real-Time Protocols

David L. Mills, University of Delaware

21 January 1997

http://www.eecis.udel.edu/~mills

Introduction

- **Authentication for ubiquitous, real-time protocols such as Network Time Protocol**
- **Current scheme uses one-way hash functions and private keys**
- **New scheme combines with public-key cryptosystem and certificates**
  - **Avoids public-key computations for every packet**
  - **Requires no per-client state at busy servers**
  - **Requires only occasional verification of server credentials**

NTP capsule summary

- **Network Time Protocol (NTP)**
  - **Synchronizes clocks of hosts and routers in the Internet**
  - **Provides submillisecond accuracy on LANs, low tens of milliseconds on WANs**
  - **Reliability assured by redundant servers and diverse network paths**
  - **Engineered algorithms used to reduce jitter, mitigate multiple sources and avoid improperly operating servers**

NTP authentication - issues

- **Configuration and authentication and synchronization are inseparable**
  - **Clients and servers must require no manual configuration**
  - **Ultimate security must be based on private values known only to servers and public values obtained from directory services**
  - **Must be fast**

NTP authentication - approach

Linking Technology

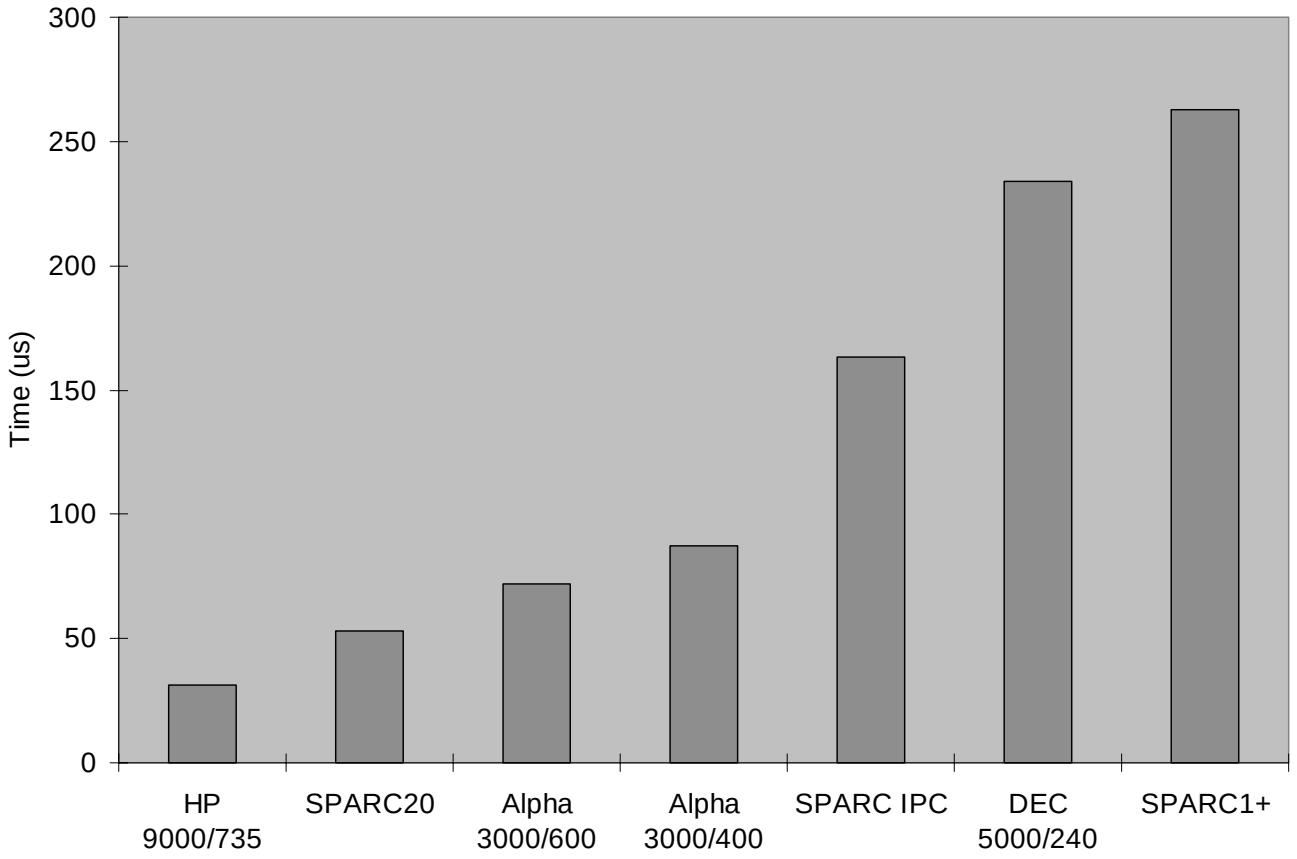
ATIRP Consortium

- **Authentication and synchronization work independently for each peer server**
  - **Public keys and certificates are obtained and verified relatively infrequently**
  - **Session keys are derived from public keys using fast algorithms**
  - **Only when time and authentication are independently verified is the local clock set**

MD5 message digest

Linking Technology

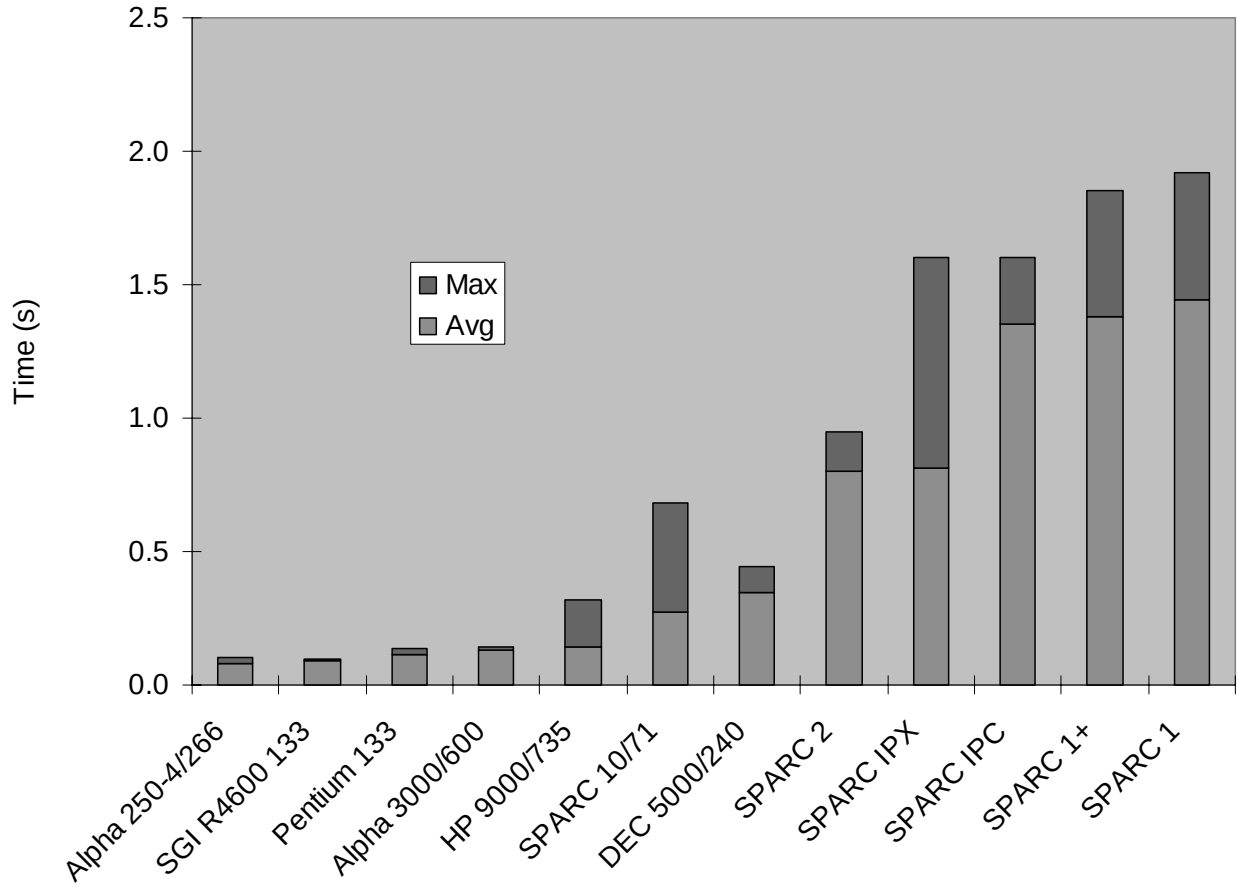
ATIRP Consortium



MD5/RSA digital signature

Linking Technology

ATIRP Consortium



Authentication scheme A (Kent)

Linking Technology

ATIRP Consortium

- **Scheme is based on public key encryption and one-way hash function**
  - **Certificated public values for each server provided by Secure DNS or X.509**
  - **Server computes session key as one-way hash of server private value, server/client IP addresses and key identifier as each client request is received**
  - **On request, server sends session key to client using public-key cryptography**

Authentication scheme B (S-Key)

Linking Technology

ATIRP Consortium

- **Scheme is based on public key encryption and S/KEY scheme**
  - **Server generates list of session keys, where each key is a one-way hash of the previous key**
  - **Server uses keys in reverse order and generates a new list when the current one is exhausted;**
  - **Clients verify the hash of the current key equals the previous key**
  - **On request, the server signs the current key and sends to client**

Current status

Linking Technology
ATIRP Consortium

- **Complete analysis of security model and authentication scheme in TR 96-10-3**
- **Preliminary design for integration in Unix/Windows NTP daemon completed**
- **Implementation plan in progress**
- **Complete set of status reports and briefing slides at: http://www.eecis.udel.edu/~mills**