

PROJECT PROFILE

Adaptive Cryptographically Synchronized Authentication

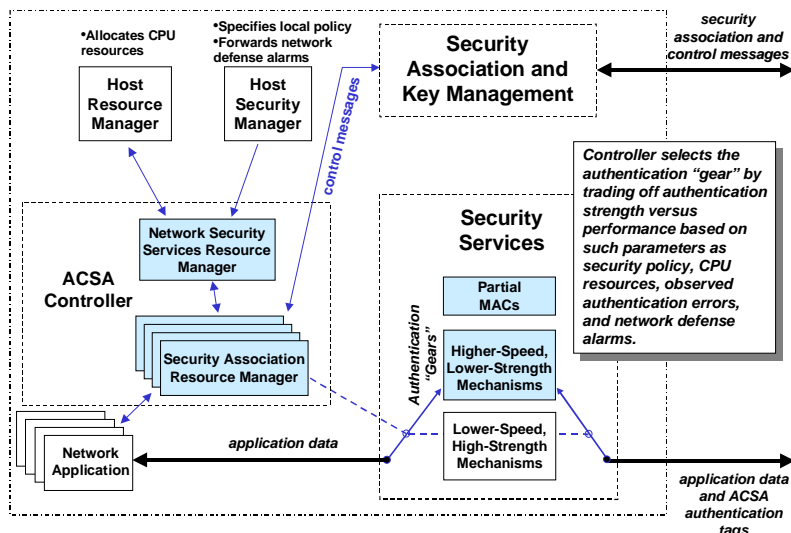
Overview

The overall objective of the ACSA project is to provide an authentication solution that is computationally efficient enough to meet the demands of ultra-fast network applications. The research has three underlying objectives:

- Identify a spectrum of practical cryptographic authentication algorithms that can be used selectively like gears of an automobile transmission in order to provide various strength-performance levels of data authentication under the assumption that strong authentication may not always have to be provided;
- Design a control protocol and system that establishes and maintains acceptable levels of authentication in a high-performance environment where the processor load of participating network devices is dynamically changing; and
- Implement a prototype system that demonstrates effective network authentication at various speeds and under various processor loads.

Approach

The ACSA System embodies a spectrum of authentication mechanisms—like gears of an automobile transmission—that provide various strength-performance levels of network authentication. These authentication gears are organized in the following three classes: lower-speed, high-strength conventional mechanisms; higher-speed, lower-strength mechanisms; and ultra-fast Partial Message Authentication Codes (PMACs) that authenticate only a portion of a message.



ACSA Model

Research Focus

High-Speed Authentication

High-speed authentication is essential to protecting high-speed networks. The ACSA project offers a new approach to achieving high-speed network data authentication by trading off authentication strength and performance.

Our research has shown that in comparison with the conventional high-strength HMAC-SHA-1-96 algorithm, we can achieve authentication computation speedup factors of about an order of magnitude for the higher-speed, lower-strength UMAC-SIMD-15 algorithm, and yet another order of magnitude speedup when partial authentication using PMAC-256 is used.

The ACSA approach is especially suitable for high-speed applications such as real-time high-speed video that can tolerate small amounts of modifications and lower levels of authentication strength.

- David Carman
Principal Investigator,
Cryptographic Technologies
Group

Approach (continued)

The lower-speed, high-strength mechanisms include algorithms such as the hash-based message authentication code (HMAC) algorithms HMAC-SHA-1-96 and HMAC-MD5-96. The higher-speed, lower-strength ACSA gears include other Message Authentication Codes (MACs) such as UMAC and our novel HMAC groups with bit scattering.

A control system determines what gears to use. During a communications session, the control system establishes a suite of authentication gears and shared authentication keys between the sender and the receiver. Security conditions and processor load will cause the control system to dynamically change gears. Furthermore, the sender and receiver will exchange control information that can influence dynamic gear changes.

A collateral benefit of the ACSA approach is that it provides communicants with the option of using multiple authentication tags. For example, with little overhead, the sender can compute two or more authentication tags with different strength-performance levels for the same message packet. Then, the receiver—independently from the sender—can in real time select which tag to verify. This flexibility is especially useful in multicast environments, where there may be many receivers with different processor capabilities, or where the receiver cannot predict future processor loads.

To demonstrate the strength-performance levels achievable by the ACSA approach, NAI Labs built prototype software that includes major ACSA model components and authentication mechanisms. At its highest level, the ACSA prototype software is composed of: (a) an ACSA prototype toolkit; (b) processor-specific optimizations; (c) prototype demonstration software; and (d) third-party network security software. To facilitate the goal of developing freely distributable ACSA prototype software, NAI Labs constructed a modular, portable toolkit that is integrated with the Linux-based FreeS/WAN network security software. Non-portable demonstration software and processor-specific optimizations have also been developed and integrated for demonstration purposes. To more easily achieve portability, NAI Labs has implemented the ACSA prototype in accordance with existing network security standards, most notably the standards encompassing IPsec and IKE.

Results

In comparison with the high-strength HMAC-SHA-1-96, our prototype achieves authentication computation speedup factors of about an order of magnitude for the higher-speed, lower-strength UMAC-SIMD-15, and yet another order of magnitude speedup when partial authentication using PMAC-256 is used.

Total processor costs for protecting and sending IP packets show that authentication is only part of the overall networking cost. For large packets greater than 16 kilobytes, the processor cycles consumed per each message byte communicated on our Pentium-based Linux FreeS/WAN prototype include about 5 cycles for IP processing, about 6 cycles for non-cryptographic IPsec processing, and between 0.1 to 13 cycles for PMAC-256 and HMAC-SHA-1-96, respectively.

Applicability

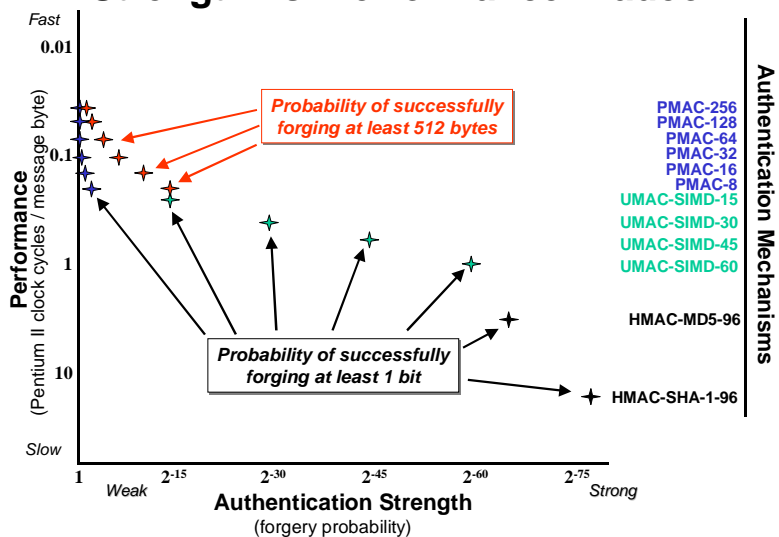
The ACSA approach is suitable for a wide range of high-speed network applications. It is especially suitable for protecting large packets such as video streams in applications that can tolerate lower levels of authentication strength. To maximize the benefit of using the ACSA approach, further reduction of IP layer computations outside of cryptography are also needed.

Additional Information

For additional information about the ACSA project, please email acsa@tislabs.com or visit our Web page at: <http://www.pgp.com/research/nailabs/cryptographic.asp>.

1/5/01

Strength vs. Performance Tradeoff



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

CORPORATE Headquarters

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337*
Fax (888) 203-9258

*Call for additional Worldwide Sales Offices