Application Note

Atmel ATSHA204 Authentication Modes

Prerequisites

- Hardware
  - Atmel® AT88CK454BLACK Evaluation Board
  - Atmel AT88CK109STK8 Kit
- Software
  - Atmel Crypto Evaluation Studio (ACES)

Overview

- Understand which customers the Atmel ATSHA204 device benefits.
- Understand which use cases the ATSHA204 device is useful in.
- Develop an in depth understanding of the ATSHA204 device.

Introduction

This document describes the general application of the ATSHA204 device. Since a minimal amount of system changes are required, the ATSHA204 device is beneficial in securing product accessories. The four basic types of accessory authentication are described more in detail in this document which are:

- Fixed Challenge Authentication
- Unique Challenge Authentication
- Random Challenge Authentication
- Diversified Key Authentication

1. Authentication Types

1.1 Fixed Challenge Authentication

The Fixed Challenge Authentication is an easy way to add security to a product without the added expense of added hardware to the host, interactive testing, or extensive software development.

Host		Client
Same question on each request.	What's the answer to the question?	
	→	
	The answer is...	Same answer to each question.
Compare	←	

With the Fixed Challenge Authentication only, the client requires an ATSHA204 device programmed with secrets. The host is able to use any number of precalculated challenge/response pairs to validate that the client includes a valid ATSHA204.

Utilizing an ATSHA204 device in the client enables the Atmel CryptoAuthentication™ to be off loaded to a secure device with no firmware requirements on the client. The Fixed Challenge allows for the addition of the first level of hardware authentication with a minimal amount of change to the host firmware changes.

Host		Client
Send command to client ATSHA204.	MAC (SlotID, Fixed Challenge)	
	→	
	Response	ATSHA204
Compare	←	

1.2 Random Challenge Authentication

The Random Challenge Authentication improves on the Fixed Challenge by adding a changing challenge to each request. This feature enables the system to defend against replay style attacks.

Host		Client
New question on each request.	What's the answer to the question x?	
	The answer is y...	Different answer for each question.
Compare		

By adding an ATSHA204 device to the host, the system is able to generate a challenge for the client on the fly. This allows a unique challenge to be sent for every validation request. In addition, by generating the challenge internally with the host's ATSHA204 device, the response is unknown to the system allowing the use of an unsecure processor without the threat that an attacker will be able to learn the system secrets. This dramatically limits the ability of an unauthorized device from producing the correct response.

Host		Client
Generate Random Number.		
Send command to client ATSHA204.	MAC (SlotID, Random Challenge)	
	Response	ATSHA204
Compare		

1.3 Unique Challenge Authentication

The Unique Challenge Authentication improves on the Fixed Challenge by adding a unique challenge to each request. This authentication feature enables the system to defend against replay style attacks.

Host		Client
New question on each request.	What's the answer to the question x + time?	
	The answer is y.	Different answer for each question.
Compare		

By adding an ATSHA204 device to the host, the system is able to generate a challenge for the client on the fly. This allows a unique challenge to be sent for every validation request. In addition, by generating the challenge internally with the host's ATSHA204 device the response is unknown to the system allowing the use of an unsecure processor without the threat that an attacker will be able to learn the system secrets. This severally limits the ability of an unauthorized device from producing the correct response.

Host		Client
Generate random number.		
Send command to client ATSHA204.	MAC (SlotID, Unique Challenge)	
	Response	ATSHA204
Compare		

1.4 Diversified Key Authentication

The Diversified Key Authentication enables the host to identify the specific accessory that is trying to authenticate with it. This enable the use of access lists (black lists) by the system.

Figure 1-1. Diversified Fixed

Host		Client
	Who are you?	
	→	
	I am...	
	←	
Same question for you only on each request.	What's the answer to the question.	
	→	
	The answer is	Same answer for me to each question.
Compare	←	

Figure 1-2. Diversified Fixed

Host		Client
Read serial number from client.	Read (Config, Block 0)	
	→	
	Serial Number	ATSHA204
	←	
GenDig (SlotID, S/N)		
Send command to client ATSHA204.	MAC (SlotID, Fixed Challenge)	
	→	
	Response	ATSHA204
Compare	←	

Figure 1-3. Diversified Random

Host		Client
	Who are you?	
	→	
	I am...	
	←	
New question for you only on each request.	What's the answer to the question x?	
	→	
	The answer is y.	Different answer for me to each question.
Compare	←	

Figure 1-4. Diversified Random

Host		Client
Read serial number from client.	Read (Config, Block 0)	
	→	
	Serial Number	ATSHA204
	←	
GenDig (SlotID, S/N)		
Send command to client ATSHA204.	MAC (SlotID, Random Challenge)	
	→	
	Response	ATSHA204
Compare	←	

2. Configuration

Figure 2-1. Shared Key Configuration

Host	Client
Load Key into SlotID	Load Key into SlotID

Figure 2-2. Diversified Key Configuration

Host	Client
Load Master Key into SlotID	Load Master Key into SlotID
	Read Client S/N
	Load Client S/N into TempKey
	DeriveKey (SlotID) with S/N

- The master key is loaded into the client slotID.
- The S/N of the client is loaded into the client TempKey.
- The DeriveKey is run on the client updating the key in slotID with a unique key based on the master key and the client S/N.

3. Examples

3.1 Fixed and Random Challenge

Table 3-1. Fixed and Random Challenge

Host Sends to Client SHA															
29	03	27	08	00	00	00	00	00	00	00	00	00	00	00	00
I2C ADDR	CMD	Count	MAC	Mode	SlotID		Challenge								
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Challenge															
00	00	00	00	00	00	00	BB	97							
Challenge							CRC								

Host Reads from Client SHA															
28	23	CA	9F	60	7C	B7	37	83	AE	D7	93	BF	00	2A	A4
I2C ADDR	Count	Response													
9A	1A	86	06	11	87	90	70	E3	25	24	E4	7E	AD	40	11
Response															
2C	A6	4F	19												
Response		CRC													

3.2 Diversified Key

The host will read the S/N from the client and then load that value into tempkey. This is done to allow the host to match the key stored in the client.

Table 3-2. Diversified Key

Host Sends Read to the Client ATSHA204								
29	03	07	02	80	00	00	09	AD
I2C ADDR	CMD	Count	Read	Zone	Address		CRC	

Host Reads the Response from the Client ATSHA204															
28	23	01	23	4B	88	80	01	02	00	8D	3F	57	7E	EE	00
I2C ADDR	Count	S/N[0:3]				RevNum				S\N[4:8]					Res
00	FF	C9	00	00	00	00	00	00	00	00	00	00	00	00	00
I2C	Res	I2C ADDR	TO	OTP	SM	Slot0		Slot1		Slot2		Slot3		Slot4	
00	00	16	39												
Slot5		CRC													

Host Generates a Key that Matches the Client ATSHA204												
29	03	0B	15	02	00	00	1C	00	00	00	CA	69
I2C ADDR	CMD	Count	Gen-Dig	Mem-Zone	SlotID		Other Data				CRC	

Host Reads Status			
28	00	03	40
I2C ADDR	Status	CRC	

Host Sends MAC to the Client ATSHA204															
29	03	27	08	00	00	00	00	00	00	00	00	00	00	00	00
I2C ADDR	CMD	Count	MAC	Mode	SlotID		Challenge								
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Challenge															
00	00	00	00	00	00	00	BB	97							
Challenge							CRC								

Host Reads the Response from the Client ATSHA204															
28	23	CA	9F	60	7C	B7	37	83	AE	D7	93	BF	00	2A	A4
I2C ADDR	Count	Response													
9A	1A	86	06	11	87	90	70	E3	25	24	E4	7E	AD	40	11
Response															
2C	A6	4F	19												
Response		CRC													

4. Revision History

Doc. Rev.	Date	Comments
8834B	11/2012	Update title from Accessory Authentication to Authentication Modes.
8834A	10/2012	Initial document release.

Enabling Unlimited Possibilities®

Atmel Corporation
1600 Technology Drive
San Jose, CA 95110
USA
Tel: (+1) (408) 441-0311
Fax: (+1) (408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Roa
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Bldg
1-6-4 Osaki, Shinagawa-ku
Tokyo 141-0032
JAPAN
Tel: (+81) (3) 6417-0300
Fax: (+81) (3) 6417-0370