ndn-cxx - Bug #1589

KeyChain::sign is slow with tpm=osx-keychain

05/10/2014 11:32 PM - Junxiao Shi

Status:	Rejected	**Start date:**	05/10/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			

Description

Environment: OSX 10.9 on Mac Mini

Steps to reproduce:

1. in ~/.ndn/client.conf, set tpm=osx-keychain
2. install a self-signed default certificate
3. prepare one Data packet with 4096 octet payload
4. call keyChain.sign(data) in a loop of 1000 times, and observe time spent in the loop

Expected: signing 1000 packets takes less than 5 seconds

Actual: signing 1000 packets takes more than 15 seconds

Related issues:

Related to ndn-cxx - Feature #2488: Asynchronous API for data signing	**New**	
Blocks NFD - Bug #2174: Multiple register prefix gives NFD error "request tim...	**New**	**11/13/2014**

History

#1 - 05/10/2014 11:36 PM - Junxiao Shi

My benchmark results:

OS	CPU	TPM	nIterations	duration
OSX 10.9	2.5G	osx-keychain	1000	19550ms
OSX 10.9	2.5G	file	10000	25227ms
Ubuntu 12.04	2.7G	file	10000	25270ms

#2 - 05/12/2014 06:47 PM - Alex Afanasyev

This is a known issue and I would like to reject this.

For security to be secure, private key should never be exposed to the application, not mentioning be cached in memory. This basically defeats the purpose of security and key protection in the first place (there are well-known "cold boot" attacks, where keys are being extracted from RAM). And as long the key is secured, there is obviously large overhead and we would see extremely slow performance, such the one with OSX keychain.

Separate issue #1204 should address signing performance problem, without sacrificing much of security benefits by clearly separating keys that are used by applications and user keys that can be used to sign application keys. The former keys can be "less secure" (as they are cheap), kept, and used directly from RAM.

#3 - 05/12/2014 09:08 PM - Junxiao Shi

- Target version deleted (v0.2)

You are admitting this is "a known issue", thus it is a bug.

This bug would be fixed when KeyChain is able to sign Data using a Data Signing Key instead of relying on osx-keychain TPM.

#4 - 05/13/2014 06:43 AM - Jeff Burke

I agree with the fix proposed in #1204. This issue may block low-latency / high-throughput applications from using signing in the current security library. Can its priority be increased and example code be provided for how applications should generate derived keys?

#5 - 05/13/2014 10:15 AM - Lixia Zhang

Jeff, I am afraid that this is NOT a priority question.
We do not have a solution at this time, no matter how high the priority one wants to set it.

#6 - 11/18/2014 02:56 PM - Junxiao Shi

- Blocks Bug #2174: Multiple register prefix gives NFD error "request timed out (code: 10060)" added

#7 - 11/18/2014 09:57 PM - Junxiao Shi

One proposed solution to this Bug is Task #1204, although it has design challenges in itself.

#8 - 08/03/2015 03:16 PM - Junxiao Shi

- Related to Feature #2488: Asynchronous API for data signing added

#9 - 08/03/2015 03:18 PM - Junxiao Shi

At 20150803 conference call, Alex classifies this as a "corner case".

However, I disagree with this classification unless the default TPM for OS X is changed to something other than osx-keychain.

#10 - 02/04/2019 08:49 AM - Junxiao Shi

- Status changed from New to Rejected

OSX 10.9 is no longer supported by ndn-cxx.
If a similar issue appears on a supported platform, please open a new bug with test logs.

Files

sign-bench.cpp	1.36 KB	05/11/2014	Junxiao Shi