[33mcommit 32ff4aecb66e5a9530f2aef7d738a94f9b98491d[m[33m ([m[1;36mHEAD -> [m[1;32msinshrptr[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 4 10:28:12 2022 -0700

    added functions to enque/deque jbuffacc to/from jbuffman, updated some documentation, updated fullog

[33mcommit 2fc2696b8e94e5bff03e6776eae396cb8f6f6d10[m[33m ([m[1;36mHEAD -> [m[1;32msinshrptr[m[33m, [m[1;33mtag: protocolppv531_devel_30May2022[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 30 00:53:11 2022 -0700

    move platform check higher, uniquified ENUMs, fixed some resource issues for multiple responders

[33mcommit 734ed6f6fb8effccd5cc88daf59f4d8e39ae6edb[m[33m ([m[1;33mtag: protocolppv531_devel_28May2022[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 28 11:45:22 2022 -0700

    fixe for jwots

[33mcommit e5ec20030af8f95d74c8bb5de5d1e1447dc0028a[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 28 08:50:19 2022 -0700

    added additional unit tests for jbuffacc

[33mcommit ec5ab68072cfefef63a0d0bbf0a7bb549b38ea3d[m[33m ([m[1;33mtag: protocolppv531_devel_26May2022[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 26 19:45:48 2022 -0700

    updated mudsums

John Greninger

Digitally signed by John Greninger
Date: 2022.06.04 12:35:16 -07'00'

[33mcommit afca6c235a0cd473079edc2589f4f6fc6c356004[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 26 19:45:05 2022 -0700

    jbuffacc now fully templated, new constructor from jbuffman

[33mcommit 1992727bfdd2c00c817f8843caf56129d3790bb1[m[33m ([m[1;33mtag: protocolppv531_devel_24May2022[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 24 23:34:07 2022 -0700

    expanded counters to uint64_t

[33mcommit 4b154fee332ce81a4ce6415f18bec7c4033fc2b4[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 24 22:47:39 2022 -0700

    debug of SFMT_MODE for randomizer when using CLang, added copyright notice, expanded period of SFMT

[33mcommit ceb41c3b4d574052b0bac5d8b4209341b1844566   [m   [33m ([m   [1;33mtag:

protocolppv531_devel_21May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 21 23:57:33 2022 -0700

updated mudsums

[33mcommit 12aff419a5a624338b4a0f3834481734dd766a85 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 21 23:57:00 2022 -0700

added simple logger function, fixed some doxygen items

[33mcommit e5dfb355cb9ddcf77254aa81d61eacf4f620adb0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 21 22:51:52 2022 -0700

updated to check generated bytes for zero and discard them

[33mcommit 46115d1cbc2ee5b591b9e0a35bc875a846ce2a47 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 21 21:53:40 2022 -0700

updated

[33mcommit 81cb168e8410675ab87f92fddec95ab27b44622e [m [33m ([m [1;33mtag:
protocolppv531_devel_19May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 19 23:54:32 2022 -0700

updated mudsums

[33mcommit 1b3ab79510e0a18596708d0300ad403049b36eb3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 19 23:11:06 2022 -0700

added methods to retrieve the linked-list from the accessor class

[33mcommit 1a2647dbf560ebd50491177b7770c5973a8e7ebd [m [33m ([m [1;33mtag:
protocolppv531_devel_18May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed May 18 23:26:51 2022 -0700

updated mudsums

[33mcommit 4810824625050f1958055cfea413ca224fe1499c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed May 18 23:20:45 2022 -0700

updated mudsums

[33mcommit a04338fbc3aa1c7dc9e6f69a815098a4c142ebdf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed May 18 23:17:22 2022 -0700

added buffer memory and accessor function for slices of the buffer memory

[33mcommit 3fb9c30dcb962fd214652e299ac6ad36d2241360 [m [33m ([m [1;33mtag: protocolppv531_devel_12May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 12 23:49:19 2022 -0700

code cleanup

[33mcommit 5fe2c5b98675e010270c58661b5823530c536639 [m [33m ([m [1;33mtag: protocolppv531_devel_9May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 9 23:22:49 2022 -0700

additional code analysisi, added jlogger function to return ASCII code

[33mcommit cd5c8380820e9d844ffd62c9721c24448abe5b1f [m [33m ([m [1;33mtag: protocolppv531_devel_8May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 8 20:36:15 2022 -0700

additional code analysis

[33mcommit 4094bd341c51445c1fb8c596670a3f49c78a10ee [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 8 19:23:31 2022 -0700

updated mudsums

[33mcommit ef3de554e12facd83c94baf2f7d70d258fe88619 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 8 19:21:51 2022 -0700

additional cleanup from code analysis tools

[33mcommit ed2b0c280d960f84ec049f45b54d199ebeb7dbcb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 8 18:41:26 2022 -0700

fixed some CLang compile warnings

[33mcommit 49d6eccf8b5d77e59366794c169cf75ce1e80c24 [m [33m ([m [1;33mtag: protocolppv531_devel_7May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 7 17:20:10 2022 -0700

updated mudsums

[33mcommit f45da135793eac55b09f0679f4be886c37e38d2f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 7 17:19:36 2022 -0700

fixed keysize for HMAC in W.A.S.P randomizer, fixed doxygen for jarray, updated CLANG to c++17

[33mcommit 5b978e0b46bf8a1577038747786d85b1a421683b [m [33m ([m [1;33mtag: protocolppv531_devel_5May2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 5 23:12:04 2022 -0700

updated

[33mcommit 2be9492093329590fb5ab347764a1509202e04b5 [m [33m ([m [1;33mtag: protocolppv531_devel_30April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 30 08:24:45 2022 -0700

updated mudsums

[33mcommit b01cfa0a73c97dc4471ec62355c014d4cdede507 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 30 08:24:23 2022 -0700

fixed stack

[33mcommit 5dce7f0ff1b9b3ed19a752ed78c0e7300f920f20 [m [33m ([m [1;33mtag: protocolppv531_devel_29April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Apr 29 19:49:07 2022 -0700

fixed an RLC bug, updated mudsums

[33mcommit bb4ff6ff01051f66e190ae39c8657f528d3f0c94 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 23 11:02:04 2022 -0700

still leak free

[33mcommit a3cb343013747cd48f2917e4757a5bd6d3dc8a62 [m [33m ([m [1;33mtag: protocolppv531_devel_22April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Apr 22 00:08:03 2022 -0700

guardbanding

[33mcommit 82fbd27c02e20e0ab00d151536dbb52c556adb66 [m [33m ([m [1;33mtag: protocolppv531_devel_18April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 18 23:08:42 2022 -0700

uniquified SAID

[33mcommit 8a300026348dc8615117dba840859e0a744cf112 [m [33m ([m [1;33mtag: protocolppv531_devel_17April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 17 18:09:00 2022 -0700

fixed stream collision

[33mcommit 30bc9791b64ab4640eebeab4584001d58973df9c [m [33m ([m [1;33mtag: protocolppv531_devel_10April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 10 16:32:37 2022 -0700

updated mudsums

[33mcommit 6b6e25c0cc0f24ddcece154cb96af94ef029649e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 10 16:29:47 2022 -0700

removed alot of shared pointers in jpacket, jstream, wasp

[33mcommit 84f2ce3aa38ea81598f16d14964f7d779f155dc9 [m [33m ([m [1;33mtag: protocolppv531_devel_4April2022 [m [33m, [m [1;32mreinterpret_fix [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 4 23:54:36 2022 -0700

updated mudsums

[33mcommit b6c0a24d35a64b81605144de56f0ad8facbc5b90 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 4 23:54:05 2022 -0700

code cleanup, added some convience functions

[33mcommit 62bb2b4659d48969854c28ec8a6f3976ab45f49b [m [33m ([m [1;36mHEAD -> [m [1;32mreinterpret_fix [m [33m, [m [1;33mtag: protocolppv531_devel_3April2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 3 22:06:24 2022 -0700

updated mudsums

[33mcommit d6d8ea36fce665bd7af267a753ddc9c17c92db0c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 3 22:05:35 2022 -0700

fixed some debug comments

[33mcommit a81ac38f77a18f5bbe609cb2bf30f7e2c261ef00 [m [33m ([m [1;33mtag: protocolppv531_devel_27Mar2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 27 21:12:54 2022 -0700

fixed after reinterpret fix to make a copy of the security association rather than a shared_pointer to the same one

[33mcommit 0195a1ce8522f7993d1969620391c947d2bf63f5 [m [33m ([m [1;33mtag: protocolppv531_devel_26Mar2022 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 26 17:57:01 2022 -0700

updates for reinterpret

[33mcommit d83f7301f929495997d21d0e61828b165237efad [m [33m ([m [1;32mv5.3.1 [m [33m) [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 26 15:17:21 2022 -0700

    updated to fix bug when passing value to randomizer from XML for jconfident

commit ec5c24205f2cc7ec234be920de8a27465f82fc1e
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Mar 25 00:21:42 2022 -0700

    updated

commit 9569e9e3b3c8770d2436e9636cf49e1167f56158
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 13 15:28:00 2022 -0700

    fixed some memory leaks in zuc256 authentication

commit 1a47400b1bdd180cfa655f07c92cd2569e4a2f7c
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 13 12:57:15 2022 -0700

    fixed a buf in ZUCA-256 in jintegrity

commit f610a70860c2c4abdf0eaa6a08e2fcb8c92906e3
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 13 11:05:51 2022 -0700

    updated version numbers for all tests

commit a71da772cca64d20ce6cbcfd84064921a79ae5c2
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 6 18:34:17 2022 -0700

    fixed some IV length issue in W.A.S.P for jconfident

commit 1e78afff9ba49e942a725a28e4b62ffd050f06a2
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 1 23:52:10 2022 -0700

    fixed zuc256 issue

commit 22030d1eaf0c7f337d55fa26ae0c197025da2895
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 1 23:21:43 2022 -0700

    updated full GIT log and mudsums

commit ab6fe0573057513b1e8aece969c925425dacdce4
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Sun Feb 27 19:00:17 2022 -0700

    bumped version

[33mcommit 8dc55d9145d445d5dce5256269fb171011db2502 [m [33m ([m [1;33mtag:
protocolppv530_final_27Feb2022 [m [33m, [m [1;32mv5.3.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 27 18:46:21 2022 -0700

    updated mudsums and README

[33mcommit f91387045b1b0f9d2dadcce5d346e88a5e96fbbd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 27 18:41:18 2022 -0700

    updated with support for ZUC256-128 to ZUC, LTE, and added unit conformance tests

[33mcommit 8483830a00731bee61414da667994686c5e3301e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 20 16:06:25 2022 -0700

    added 16-byte IV version of ZUC-256

[33mcommit eaed174a6c9d50a7ff8ac573753682b4276745dc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 20 13:45:19 2022 -0700

    updated mudsums

[33mcommit a0fb1d78444f30bc22fabbef62157474c395428c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 20 13:43:37 2022 -0700

    updated windows release area for v5.3.0

[33mcommit e0d71ef63288b24475fba8f646aa45dc41fcb4ae [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 20 13:38:34 2022 -0700

    updated file permissions

[33mcommit 2a8a639001c71fe8c23fa40953ed3161834df021 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 15 22:34:50 2022 -0700

    updated mudsums

[33mcommit ee55f447e048f949ff7335e80a90dd82075e42b6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 15 22:32:35 2022 -0700

    updated version to 5.3.0

[33mcommit bb98640c92bfad539cae42c8e9262df71c706923 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 13 20:35:15 2022 -0700

    test for reverse() method

[33mcommit 67ff7a043f741787047774aac8908c361d96d22c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 13 20:12:27 2022 -0700

    updated mudsums

[33mcommit 3a2995b1e3af36145f930207f2a3f094dc00c03b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 13 20:03:49 2022 -0700

    updated reverse() in jarray to be more efficient

[33mcommit 29714be1790fd59d5404ace96108e7ef51102dca [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 13 19:40:27 2022 -0700

    added endian test

[33mcommit 65d84121d6fe338f6cde783cde6a45b65684d831 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 13 18:32:55 2022 -0700

    fixed unit test after changing jsnowv interface for GCM to match STREAM interface

[33mcommit 1dc26cc8287fe13270047c2b634a9617757b7aff [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 7 08:20:14 2022 -0700

    bumped version

[33mcommit 1aeddacd21bb6c736dacfc9c17dcb6f11d8a6db8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 7 07:56:38 2022 -0700

    removed explicit from initializer list constructor

[33mcommit 9c86ad04674a2fe3263ca4221e07f9337bb98d68 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 6 11:57:47 2022 -0700

    fixed constructor from raw pointer to accept any type not just UINT8_T

[33mcommit 2df03b7a5987a80706f0705852e2277b5c5412c6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 5 01:07:17 2022 -0700

    added SNOWVA to runpp and runprotpp regressions

[33mcommit fb6f4713221fbe67f56ce90ee438e16abde57f64 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 5 01:04:16 2022 -0700

    updated README and mudsums

[33mcommit 8cdcc5d21bac159d67ef8f53c95e2a712af4af4a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 5 00:58:10 2022 -0700

    added SNOWVA to jintegrity, modified jsnowv ProcessData to place aad and aadlen at end instead of middle

[33mcommit 8e1a55b466aeb87999a62f4695486daa5f3b77e8 [m [33m ([m [1;33mtag: protocolppv524_final_30Jan2022 [m [33m, [m [1;32mv5.2.4-final [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Feb 3 23:06:18 2022 -0700

    added template specializations

[33mcommit aec91580e7dee693b32f0f84a1f9019a80cad5ed [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 1 22:13:53 2022 -0700

    updated README

[33mcommit 2201cecd95a0706e20109b9e7f36b12c67f4aa0d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 1 22:12:52 2022 -0700

    updated mudsums and versions

[33mcommit 4963d3527a47c668cc872b92cb65e5b278706090 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 1 22:11:15 2022 -0700

    fixed version number

[33mcommit e275e1b451f026d81f7729a7ae50eeacc0d0a03e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 1 21:55:47 2022 -0700

    updated mudsums

[33mcommit 51d105513647dcf18b033eb847602f0ac7e0898c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 1 21:48:26 2022 -0700

    fixed formatting

[33mcommit 1ddb8d7b4adc5725e97c7889b60e6cc783986cb8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 30 20:54:28 2022 -0700

    updated mudsums

[33mcommit c415e5b6ccb26f8d91100b8222b995f1c442b4b9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 30 20:53:10 2022 -0700

additional pedantic fixes, updated versions in executables and help menus

[33mcommit cd711b35515504c3bff02281b755cbd69e920e7c [m [33m ([m [1;33mtag: protocolppv523_final_26Jan2022 [m [33m, [m [1;32mv5.2.3 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 26 18:23:12 2022 -0700

updated valgrind run after pedantic fixes, updated mudsums, and README

[33mcommit e37babe821f2f29727a45d6e0070a1acab43498e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 26 18:08:28 2022 -0700

fixes for pedantic compile

[33mcommit e69f5fefef3c72c05a5986d47a1012308275l9b0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 24 16:55:56 2022 -0700

updated README

[33mcommit 265f83e0f9b502ac8da530646d259dc01751e369 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 24 16:54:28 2022 -0700

updated mudsums and make

[33mcommit cdd9b83dcee0af3b64bd9783ffb15b925ee52f0b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 24 15:35:29 2022 -0700

changed all seeds to uint64_t from unsigned long for better portability, added initilizer list constructor and append to jarray

[33mcommit ae805ef7a86afce881500f6ccbe024f50705b0ff [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 23 20:51:12 2022 -0700

updated README and mudsums

[33mcommit 917b1c4e9ae6fc847557527393c625cfa4effdd8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 22 23:45:19 2022 -0700

updated mudsums, bumped version

[33mcommit ad76a33955bd564722ba41e3e4c15a64b0805d34 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 22 22:50:38 2022 -0700

added missing tests, specs, dependency script, valgrind log

[33mcommit 065f85e361b2734fdce73b7f666118528e62368c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 22 22:19:41 2022 -0700

fixed missing values in schema for snowv, hmac

[33mcommit 46ed0cbf50e2f5bde7f83d262fa17390d30f890f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jan 21 01:16:40 2022 -0700

updated doxygen to include dependency graph

[33mcommit 302fcc83e10f4f91852cf2dd244854690f4794a5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 19 00:30:33 2022 -0700

bumped version, updated mudsums

[33mcommit a951196423d5eeb04dfa5a1c4b3eaf20e64b495d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 19 00:12:31 2022 -0700

recoded jarray constructor for different size types to reduce reallocations

[33mcommit b00283c2d9d78909630167e907620ecf1f82e2ee [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 17 00:33:44 2022 -0700

updated valgrind run results, mudsums

[33mcommit c41a3cb0b2751a30c831cb824254425b1342cf4d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 17 00:16:32 2022 -0700

added hashing of large keys in jikev2::prfplus, fixed some formatting of error messages

[33mcommit 7f66f2e8aee1aff3983076079ecbd5b4ce83b190 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 15 15:32:02 2022 -0700

additional CLangTidy updates, fixed possible double-free

[33mcommit 3aef8a4320e321b5a35e5cd13108c519e1cd644e [m [33m ([m [1;33mtag: protocolppv522_final_12Jan2022 [m [33m, [m [1;32mv5.2.2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 12 02:11:27 2022 -0700

updated mudsums and valgrind log

[33mcommit 544dc866af45e7cb9b07babca8821f7221f26ab7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 12 01:55:08 2022 -0700

fixed some possible double free issues

[33mcommit 920266ffadde48749634c4f2766976065072ef2e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jan 11 18:13:07 2022 -0700

fixed signature generation for release

[33mcommit 7e324e161b9839a62a5e2b5c99dd9b469459d0d6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jan 11 17:53:16 2022 -0700

fixed paths for install

[33mcommit f0bad498a764d70afb8634fb3fa181bf86a8985a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jan 11 17:13:09 2022 -0700

updated mudsums

[33mcommit 1a466cbb76cf6a119298b12675d9181eaccd8b28 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jan 11 17:11:51 2022 -0700

updated install and makefile to install correctly for i686 or x64

[33mcommit 9d46ea78e25dc8939952a4a4b206d6d8818f450d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 14:19:10 2022 -0700

updated mudsums for final release

[33mcommit e596dd04ddc9ba1309969735caf18012b845a403 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 14:18:47 2022 -0700

updated

[33mcommit 03b54cef4e7ea49ddfa2289f1fb7ab448134a457 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 14:17:44 2022 -0700

updated windows compile area

[33mcommit e685230c7d690fd836a503d608b3d26e0c2c664b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 13:22:11 2022 -0700

updated mudsums

[33mcommit 4f48c2875c16a08b97675d1fba70c0f9cbaffb54 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 13:21:55 2022 -0700

updated copyright dates in all files

[33mcommit b6afcb84f9d434186edac61ae8715c27c2a56b91 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 9 12:47:40 2022 -0700

final CLand-Tidy updates for source and header files

[33mcommit ceba901d68ded6eebad05645f6345b8580e82263 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 2 20:21:39 2022 -0700

updated mudsums

[33mcommit 22614a7091a663b662e68b09759644e58814ab64 [m [33m ([m [1;33mtag: protocolppv522_rc3_31Dec2021 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 31 20:04:34 2021 -0700

updated make file

[33mcommit 12c113cae73092f32da232c956cb7f921d8d0354 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 31 19:08:42 2021 -0700

added WASPDUT platform, updated mudsums and README, fixed GENKEYPAIR in W.A.S.P

[33mcommit ba57960dc61a9913d8471f1d43afd7a0a2e97b86 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 31 16:37:03 2021 -0700

more CLangTidy updates to header files

[33mcommit c5fb6b2728a4258e8eb055be08be6b82bfa86054 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 31 00:30:22 2021 -0700

updated mudsums

[33mcommit 4f920db6ced529e4f77fbfd75f44fbec327b9323 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 31 00:28:57 2021 -0700

added hash, hmac, sha3, snowv, zuc, zuc256 tests to regressions

[33mcommit a08ebb9bdce38f491c76f633d1c892f009097e49 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 30 22:21:44 2021 -0700

restored tests to original

[33mcommit 2eef323717eef773009f9ccc6a797d6015d35cdf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Thu Dec 30 22:14:08 2021 -0700

    fixed formatting issues

[33mcommit 2dbc13f8a512762b555fdd03f717f6016ce4121e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 30 19:58:37 2021 -0700

    updated HMAC_SHA2 enums

[33mcommit 3848dcfddd5c80f59efe1f5900c5120ef5b224a3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 29 01:07:51 2021 -0700

    updated README

[33mcommit cca5947241d925f19abe944a168998f34e2d46ab [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 29 01:04:58 2021 -0700

    debuged ZUC-256 F8 mode, now working, added it to testbench, W.A.S.P, and jconfident

[33mcommit 6d7e5e9d2e845a7d49b5a378ef8b93f9e46ee4fd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 25 16:35:08 2021 -0700

    updated mudsums

[33mcommit 5d890bcfe429b90cde1ad1ccdc222530b9702c2b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 25 16:03:58 2021 -0700

    added hash functions, HMAC functions were always supported, added registered trademark symbol

[33mcommit 5dcd3521b06bc5b8b020a390905aefca143f5050 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 24 01:08:26 2021 -0700

    fixed name

[33mcommit 78c4e2b3c2a63cd443d7121c49241af89e6b3e0b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 24 00:44:32 2021 -0700

    added conformance vectors for SHAKE128/256, added back SNOW3G and SNOWV context and constructors

[33mcommit a0f2e50ae9a2443d2eb6d5d7f4b7d734a2717953 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 21 19:26:38 2021 -0700

    updated README and mudsums

[33mcommit d055cec7d057401a9fa24842d0fc6fced4cb679d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Tue Dec 21 19:09:08 2021 -0700

    updated LaTeX header file

   [33mcommit ab01870122a22f6d66af47443f113df022ee7435   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 21 18:55:58 2021 -0700

    added SHAKE128 and SHAKE256 to the testbench and integrity

   [33mcommit c4d56a85218d385293d07ca4ac0faf93fbb72572   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 21 18:18:42 2021 -0700

    added SHAKE128 and SHAKE256 to jmodes

   [33mcommit 430c418a38bac923ce2b269504ae9f396e4b3a2e   [m   [33m ([m   [1;33mtag:
protocolppv522_rc3_19Dec2021   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 19 20:01:24 2021 -0700

    updated README and mudsums

   [33mcommit 4b162d1274330275b05ddd04d870d246d2331108   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 19 19:49:56 2021 -0700

    updated all files to v5.2.2

   [33mcommit a731d4fa0f9955f96c3b52c4038e9813f7e16b24   [m   [33m ([m   [1;33mtag:
protocolppv522_rc2_17Dec2021   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 17 13:46:50 2021 -0700

    fixed ZUCA for conformance vectors, SNOWV as authentication only (GHASH) so it can be used with other ciphers

   [33mcommit 15bd0ba85cefcade9529a69e0394e5c6f5022d86   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 15 11:31:55 2021 -0700

    fix for 16-bit SN when using SNOWV-GCM

   [33mcommit bc0d1a101e1a5cf84118d0adf41116a65ce6fae8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 15 11:06:14 2021 -0700

    fix for LTE and RLC control plane with 5-bit SN

   [33mcommit 7fe64f8567f67970047314c137881cb26a8b518c   [m   [33m ([m   [1;33mtag:
protocolppv522_rc2_15Dec2021   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 15 01:46:36 2021 -0700

    debug of SNOW-V in LTE, working except for 16-bit SN

[33mcommit 99797eb3c9caba301b3662262a32fdf3c04db8a3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 12 18:46:04 2021 -0700

added SNOWV, SNOWVA, and SNOWV_GCM to LTE

[33mcommit 223e4d10cc1325791783b90d0c46e42b76c7dbad [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 12 16:50:21 2021 -0700

changed SNOWV_AEAD to SNOWV_GCM

[33mcommit ef0b889cb8367e472a4e6d2c7a6c6e93231bfdc9 [m [33m ([m [1;33mtag: protocolppv522_rc1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 11 13:57:02 2021 -0700

updated mudsums

[33mcommit 8b63b61f5ab8df79d3a98a37fba0ad2007ad4ba5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 11 13:54:21 2021 -0700

final debug of SNOWV/SNOWV_AEAD in unit, cipher, and W.A.S.P interfaces with conformance tests, all working

[33mcommit 236768bcabfafa29c11e4e176ce4deee80f0c070 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 9 12:52:16 2021 -0700

updated with static code analysis

[33mcommit 46edf743f14b9c169c7f6b3155af829d5b99a547 [m [33m ([m [1;32mfailme [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 5 22:11:44 2021 -0700

updated mudsums

[33mcommit a61a8ed21de6eae62b5da45fc9b792605024d5a5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 5 22:02:21 2021 -0700

fixed some more testbench status messages

[33mcommit 4f6673db35245dbdd81680202d271d984af4b1e7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 5 21:56:25 2021 -0700

fixed some debug messages in the testbench, added guard-banding for setup phase to only issue packets for initial flows

[33mcommit 749498dd6b5805226328cd6f1f7680c2eb1edd59 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 5 20:12:00 2021 -0800

found a bug in ZUC-F9

[33mcommit 9b31a1fe5347c5dd14319c4340917816187 57dfb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 3 22:41:23 2021 -0800

added new MAC calculation for ZUC-256

[33mcommit 7ca2fe110f070d63ed1c677198b7cbae1b85c1eb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 3 19:19:02 2021 -0800

added ZUCE and ZUCA conformance vectors

[33mcommit 926ef15a8c8ce98cecae0d4c68557c65e6368ab5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Nov 29 19:26:33 2021 -0800

zuc256 debug, keys other than all 0 not initialized correctly

[33mcommit 76f9a9a3201c7fe287ebb850d738215705a758e9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 28 15:39:12 2021 -0800

partial zuc256 debug

[33mcommit ca6aa208cd2fa2b27490c44035ead89cde77367c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 27 23:27:07 2021 -0800

final SNOW-V debug, conformance now passing

[33mcommit 1431e6238cb0e34cafa77206c851de33fa051c06 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 21 08:16:05 2021 -0800

updated serase to erase the memory after scrubbing it with the pattern

[33mcommit fb707e8bd3c3ed71165191956071c4d2d27d1acf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 21 07:24:24 2021 -0800

documentation clean up to fix some tables

[33mcommit d9f24f8d586878c04cb08dfdff8b5a6478d9a8d0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Nov 19 06:42:44 2021 -0800

fixed some documentation syntax errors, added some missing fields

[33mcommit e7dbb8bcc3786e5876fd5778ce4c09d9f62f28e9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Nov 10 00:03:37 2021 -0800

zuc256 separted encryption from authentication, keystream debug

[33mcommit 29096ebddd3900f486df6fb83feff87b92ba2f9a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Nov 9 21:11:15 2021 -0800

moved pretty print back to 24 wide

[33mcommit 1a97e473fad2e59481df293d26672faf43f7bfac [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 7 16:44:47 2021 -0800

updated mudsums

[33mcommit a6a3ede20e4d61287af95ae92e02c6b1ac1ec5cf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 7 16:01:14 2021 -0800

updates for ZUC-256

[33mcommit db470e91310c0a7ec67c4c1aa9d5db4afc50e32b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Nov 1 23:13:00 2021 -0700

updated to separate SNOWV and SNOWV_AEAD

[33mcommit 20ed7713c75ae989de982a8c5460cd969c8a18cd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Oct 29 15:43:53 2021 -0700

added SNOW-V to testbench, support for STREAM and AEAD modes

[33mcommit b090f3f2d9fb689dc5d36b51a29aa6df9055af50 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Oct 29 14:42:38 2021 -0700

fixed ikev2 main for Windows

[33mcommit c6e4fa872b33e350573b01f718a841efc5529e19 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Oct 29 14:20:23 2021 -0700

updated version for licensing software

[33mcommit 693f44445beddd03524346a088633d7dc09f9bbe [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Oct 26 00:33:25 2021 -0700

added conformance vectors for SNOW-V, able to compile without errors

[33mcommit 620f4990a2ea737025c40be287939fd4e52f25bf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Oct 25 19:51:45 2021 -0700

documentation for SNOW-V

[33mcommit f37292c7d07ff7b66ef873cd2807c5a16e5f5836 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 23 21:13:02 2021 -0700

initial checkin for SNOW-V

[33mcommit eae05dadb99f6d13b10b38c062a3b58f5824d788 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 16 10:20:07 2021 -0700

fixed some schema issues

[33mcommit 874382024900e3e976ab31e529911ecb06653613 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 10 14:53:52 2021 -0700

updated conditional make

[33mcommit 0df7b4145ee26a86c568eef74d5f6cdf60a11bb4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 10 14:19:13 2021 -0700

bumped version, streamlined some code in producer

[33mcommit 717c0494cc3aa342dea2be37c0b463730b9b0f60 [m [33m ([m [1;33mtag: protocolppv521_final [m [33m, [m [1;32mv5.2.1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 9 10:49:05 2021 -0700

updated mudsums

[33mcommit 59adf9195c7d8e3c1dee61280dcf2b25133216f6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 9 10:47:37 2021 -0700

updated documentation with trademark for protocolpp and protocol++ in windows area

[33mcommit b02636782a1f03fcb40206cb8ae300bfbb6696b4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 9 10:14:25 2021 -0700

updated mudsums

[33mcommit 138cba38f150e40d63871e63290f6b27d782cfeb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 9 10:12:55 2021 -0700

updated documentation with trademark for protocolpp and protocol++

[33mcommit 13ee24a929d5e35b6761cb86c36e27883cdc0fb8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Thu Sep 30 13:45:18 2021 -0700

    moded to c++14 standard compiler

[33mcommit 5aa3134da981876b7efc16b8a290399847e5188e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 30 11:27:39 2021 -0700

    added SEC files to Windows compile

[33mcommit 4220357e94a3e8f1d3b17bf4f0078f047a5b8f0c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 30 11:25:52 2021 -0700

    updated permissions

[33mcommit 4465cb50acde86f23e8c8ae548fe397195cf8252 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 30 11:24:57 2021 -0700

    updated windows port

[33mcommit 5329c0cadee51bea12de79ca47ad9fc5c5951289 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 30 11:12:16 2021 -0700

    fixes for windows compile, updated CMake for Windows compile

[33mcommit 71489068c78f43776fc4a7221a3c5222a9048a39 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Sep 27 22:53:15 2021 -0700

    final release v5.2.1

[33mcommit 7e12aa57356c7b00667f93c9b1a1401e25809a9d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Sep 27 22:05:50 2021 -0700

    fixed driver code for Windows licensing

[33mcommit 9feecab2d8a3139b50628a3627f3a5d12ab47a44 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 26 19:58:29 2021 -0700

    removed object files form windows compile, added VC++ project and solution files

[33mcommit d36200d1c5108a827198798a81df1770ce952e96 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 26 19:16:27 2021 -0700

    updated with CLang Tidy changes, windows compile debug

[33mcommit 2709ba4c96c496acec90ebabd0f64fee94d4cfdb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Sun Sep 26 19:13:25 2021 -0700

    updated with CLang Tidy changes, windows compile issues resolved

   [33mcommit 0afd73cd93c356fa8094a132c5391b4d700d7cf6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 24 16:28:06 2021 -0700

    updated README with full list of v5.2.1 changes

   [33mcommit 1c6e7b01d5e8793f487f41c3dc247e2d47d409ee   [m   [33m ([m   [1;33mtag:
atQC22Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 22 15:42:21 2021 -0700

    updated windows port

   [33mcommit ddc6c4479993680fd13b5e85bb13aa585852d817   [m   [33m ([m   [1;33mtag:
atQC21Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 21 14:48:55 2021 -0700

    debugged LMS and XMSS length issues

   [33mcommit e1ee440a9f8607605cea2a84c0a53b7faaf87dfb   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 21 08:25:05 2021 -0700

    logging update

   [33mcommit 3ff798131ca335b9233386dfadbd7f9204eeaa71   [m   [33m ([m   [1;33mtag:
atQC19Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 19 19:16:04 2021 -0700

    fixed keylen selection for TLSv13, updated unit tests for DH to use two different key pairs (sender and receiver)

   [33mcommit 40928fdac1a8632872921d89bfbd7884eb165ca6   [m   [33m ([m   [1;33mtag:
atSeattle17Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 17 10:39:09 2021 -0700

    updated mudsums

   [33mcommit f49a23cdb644e800f42829de7331658baa082310   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 17 10:37:13 2021 -0700

    documentation update, added unit tests for Diffie-Hellman with curve25519

   [33mcommit 0234753a45a1ecade37f81087597dd65e06327ba   [m   [33m ([m   [1;33mtag:
atSeattle15Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 16:09:21 2021 -0700

updated mudsums

[33mcommit b2b7389771094cfb6822c375a46ab622c6087ba6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 16:06:12 2021 -0700

updated windows release area

[33mcommit 5b15abc3d008af94182de5f210e7d5da3ee46ad6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 16:04:08 2021 -0700

updated distribution

[33mcommit 88ff3f9bf462a329d47b73706db7d237b99c73dd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 14:25:44 2021 -0700

fixed a doxygen parsing issue

[33mcommit 260f86ecb4a93241896320a393e4881acebdf7ad [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 13:59:06 2021 -0700

consistent code

[33mcommit f26c646b7c07714ec496f0b5f370811971978eba [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 13:40:41 2021 -0700

updated random and all tests to included missing protocols

[33mcommit 2d8aecd33d3806b636a194666d95924700d93cd0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 13:33:43 2021 -0700

removed salt from TLSv1.3 per the specficiation

[33mcommit c9411ccadb05b61821d8b9cfdf44575d0f33e368 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 15 11:00:42 2021 -0700

updated documentation, schema, added jikev2 functions to library

[33mcommit 2d815b862bafdb8c0cdb8e853afd98a38ecaa838 [m [33m ([m [1;33mtag:
atSeattle13Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Sep 13 20:20:38 2021 -0700

fixed some print statements, added new make targets

[33mcommit b3c10752f404adadd3d03c7f536fcb48f1c5e70f [m [33m ([m [1;33mtag:
atSeattle12Sept2021v521 [m [33m) [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 12 19:20:54 2021 -0700

    updated mudsums

  [33mcommit 047fb6959a24874b03243abdb02e433217d21f1e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 12 19:19:23 2021 -0700

    code cleanup

  [33mcommit 6e3dd452b863993f74fadabe36634a65058f23e0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 12 18:18:47 2021 -0700

    added ability to retrieve top of stack without popping it from the stack for XMSS

  [33mcommit 90b6a3000c1db04243a5beecefc172ff04437a66 [m [33m ([m [1;33mtag:
atSeattle11Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 11 11:14:16 2021 -0700

    added SEC testbench to distribution, fixed trial activation

  [33mcommit d664c540a7ce0fb9aa1cdf6ad4b8ed2e51259135 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 11 10:57:24 2021 -0700

    updated trial activation with new product id

  [33mcommit 1dc834796280b4a5f2149e03905814b2fb1317e4 [m [33m ([m [1;33mtag:
atSeattle10Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 10 09:14:23 2021 -0700

    added SEC testbench to distribution, fixed trial activation

  [33mcommit 7848a599c015994fdb1436b1f4ecd866081d2fa5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 9 11:04:45 2021 -0700

    cleaned up Clang compile warnings

  [33mcommit aacf1ea011fa74b632ef809191fa08110e498927 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 8 19:25:52 2021 -0700

    re-enabled licensing code

  [33mcommit 67fae5a2750c8ee7992c6d9b5f453637946c9463 [m [33m ([m [1;33mtag:
atSeattle7Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 7 16:05:44 2021 -0700

updated str_status with missing protocol and error

[33mcommit e67ba4ffd519f0c8feeea0f49046809cb3d48ebe [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 7 14:46:11 2021 -0700

updated mudsums

[33mcommit 0a8c0bfac419254935730949e29645f00429312d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 7 14:23:50 2021 -0700

iv encode for larger IV, mudsum update

[33mcommit 012ffcfd353184b7ed4ee7b5aece79b595340eb8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 7 14:22:21 2021 -0700

updated unit test with conformance from ZUC-256 Stream Cipher document

[33mcommit ad2fcd5f51fb29cfee88814c3cefdabc179582f9 [m [33m ([m [1;33mtag:
atSeattle6Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Sep 6 23:21:38 2021 -0700

added support for zuc256 with all ICV lengths

[33mcommit 6aff974d752277a07e3cb3b08bdf05ca9778fde7 [m [33m ([m [1;33mtag:
atSeattle5Sept2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 5 20:21:11 2021 -0700

updated mudsums

[33mcommit 622199920c2d814f2b167ab82452c2eaf138534c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 5 20:20:09 2021 -0700

updated to removed unused code

[33mcommit d1bfbff9f8984044c5d3db1949e1fb50f4a1d0a6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 5 14:47:54 2021 -0700

updated mudsums

[33mcommit 84eb9164c787fe331b060e06d3312f1bc183b595 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 5 14:47:07 2021 -0700

fixed cut-n-paste issues for key validation

[33mcommit 4f37d43a3f2d45dd1525bc2357d18d1a9cd59466 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Sun Sep 5 13:23:45 2021 -0700

    added PKI key validation

   [33mcommit 601e362115b3c1ca914e5021d372e35a9dbd16ab   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 5 12:59:24 2021 -0700

    code cleanup added F2M and Fp to regressions and unit tests

   [33mcommit a261fa5a9a33cfd5e39b933bfb6545571716c042   [m   [33m ([m   [1;33mtag:
atSeattle4Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 4 18:23:19 2021 -0700

    debug of stack for LMS/XMSS

   [33mcommit ab6f1943a54e019f4ae9dbaae7eafd9cc885f31b   [m   [33m ([m   [1;33mtag:
atSeattle2Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 2 12:41:07 2021 -0700

    update mudsums

   [33mcommit db7df4fcc2db67f6e03eb1ab949162d60c132525   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 2 11:58:46 2021 -0700

    fixed invalid material error for some curves

   [33mcommit 83bf4fcc4026fa914ea1caacb90b8b45cecd6df8   [m   [33m ([m   [1;33mtag:
atSeattle1Sept2021v521   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 1 18:02:16 2021 -0700

    update mudsums

   [33mcommit 4adc6f4aca8f1b50c46331c7a87b1041f07dd76f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 1 18:00:41 2021 -0700

    updated distribution to remove unneeded header files

   [33mcommit ed17f594ea55548913d91dce8f47fae7f0a19fc4   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 1 15:56:00 2021 -0700

    updated documentation for EdDSA

   [33mcommit 859e4338e12ccd6c509702a68c83d0026ea94612   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 1 15:21:25 2021 -0700

    updated DSA and RSA to correctly encode keys

[33mcommit 2f92fa74964359a787c987e517081e97da415096 [m [33m ([m [1;33mtag: atSeattle31August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 31 17:23:59 2021 -0700

updated mudsums 22Aug2021 17:13

[33mcommit 64e432e7fce84b07e144ab792c676e71e32e53df [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 31 17:03:11 2021 -0700

updated regressions with EdDSA, code cleanup

[33mcommit 1c9d2cab1d0f292ba25c0ac978e15993ff168ed0 [m [33m ([m [1;33mtag: atSeattle30August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Aug 30 16:58:01 2021 -0700

added missing status updates for keypair generation and signign in LMS, XMSS

[33mcommit e1e08d5065a924309d57e06d9bb9ab07612eb0d6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Aug 30 16:34:47 2021 -0700

updated with x25519 DH, Ed25519 signatures, fixed indentation issue in W.A.S.P for ECDSA

[33mcommit 19cc661839fcf374b5bbd568695615d35c2c93f1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 29 19:07:25 2021 -0700

added documentation

[33mcommit 567d97cc3bfecd6f00012d115915673d6392c7cc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 29 11:56:31 2021 -0700

added support for Ed25519 signature scheme

[33mcommit 09760e32bd55e974d3ccc1ed9475ef71830026e4 [m [33m ([m [1;33mtag: atSeattle28August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 28 18:41:57 2021 -0700

added additional randomization to the testbench

[33mcommit 05dff2401278de9369bd61953419d16eee19934b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Aug 26 18:40:23 2021 -0700

added 192-bit version of XMSS, changed valgrind run to use multiple responders

[33mcommit 9ab49485025a56e2508cd0cafe6cf58439470157 [m [33m ([m [1;33mtag: atSeattle25August2021v521 [m [33m) [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 25 23:28:16 2021 -0700

    updated README and mudsums

[33mcommit f16633de04257c6def8170da36449273030afe30 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 25 23:14:43 2021 -0700

    removed all shared pointers from jmodes, removed PLAT from WASPPLAT and SECPLAT, fixed randomizer for stream with no children and protocol with no children to correctly generate replay packets

[33mcommit a20985ca83ee92b2bd71b241570c62d01e14805e [m [33m ([m [1;33mtag: atSeattle23August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Aug 23 22:45:04 2021 -0700

    updated GNUmakefile to clean SEC executable

[33mcommit 1d297fc27b5d2a07a9a586adae3cccf3e73f341e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Aug 23 22:43:25 2021 -0700

    debugged SEC testbench

[33mcommit c5be9881bba00efb7d94d9d9fe13002a9778d680 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 22 17:13:50 2021 -0700

    updated mudsums 22Aug2021 17:13

[33mcommit 1d2bd3c63fd974f2e4811dc8f3175b0be2b26898 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 22 16:01:20 2021 -0700

    updated some iterators to use auto, finished jtestcfg coverage

[33mcommit 078cc9d9640a5baa92037cd7e18b54b2431b3b9b [m [33m ([m [1;33mtag: atSeattle22August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 22 11:28:24 2021 -0700

    updated all files with latest copyright for v5.2.1, effective July 17, 2021

[33mcommit 6d3e3aed25b5792f4edab35c5f99c04a38c7b7f2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 21 18:02:17 2021 -0700

    fixed testcfg connection checking for responder

[33mcommit da7711726fe1509556f798a97462c0a4d1b8ae3f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 21 11:07:33 2021 -0700

removed unused code in test configuration parser

[33mcommit fe40e052277107c728faefe6f568e7ccc19317ca [m [33m ([m [1;33mtag: atSeattle19August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Aug 19 11:51:07 2021 -0700

renamed ECDSA classes to reflect Fp and F2M functions

[33mcommit 9bab6e4b9f3af1136b86e683583eb500ee405810 [m [33m ([m [1;33mtag: atSeattle18August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 18 21:14:53 2021 -0700

updated README and mudsums

[33mcommit 8df3ec0fa30c0506006b634ab2fc637efc414c91 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 18 21:11:15 2021 -0700

moved to TinyXML2 v9.0.0, randomized order of patterns for scrub

[33mcommit d5a37251ff1d31765297aa64e8f53154729df018 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 17 13:38:00 2021 -0700

updated README and mudsums

[33mcommit 554713638af26f5971858b3d4c7f4eaa3194967a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 17 13:35:06 2021 -0700

bumped version number

[33mcommit 3a4e0a36dfd3ab7e876dcff2bc5eba73ab7c717a [m [33m ([m [1;33mtag: atSeattle15August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 15 14:41:08 2021 -0700

updated with feature to scrub array. Used to scrub keys, salt, iv, on destruction

[33mcommit 6e064bd4cd674a94ce0962d5b58fbee960e3fb0a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 14 08:31:50 2021 -0700

more updates for W.A.S.P when only passing <stream> without children, nonce clean up for CHACHA20POLY1305 in TLS and IPSEC

[33mcommit fb9a102d2dc8792b0bdf8967fda7c39714e1460c [m [33m ([m [1;33mtag: atSeattle11August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 11 13:17:45 2021 -0700

updated mudsums

[33mcommit 787c48549a7a1b33ef259c5f837aaa21a41e48df [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 11 13:17:25 2021 -0700

additional code cleaup from analysis

[33mcommit 27809829b57a986ced4e3c3976eca3f6b132a1bd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 10 20:15:14 2021 -0700

fix for W.A.S.P when not passing protocol or security objects

[33mcommit 85084b71f33e3ecc456e35255925078f6df10b88 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 10 19:42:05 2021 -0700

code analysis cleanup, fixed a bug when only passing a protocol object to the parser without a security object

[33mcommit 0a9fb1f09538467efec8bb4c4feda2e411c722de [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 10 18:02:31 2021 -0700

added missing variable to initialization list in constructor

[33mcommit 43183ef5fa8f559b67c5377991eeca9b60c4a7ef [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 10 17:21:44 2021 -0700

fixed some missing variables in constructor

[33mcommit 564522f85b8446f69670fd949f6ca1f07d672ac2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 8 11:50:52 2021 -0700

coverage and debug updates, include coverage at 92.7%

[33mcommit 2db3131507dc7dfcec7b31affb93fb01b1a184e6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 7 13:11:13 2021 -0700

documentation updates, added key validation for ECDSA

[33mcommit 7cac72025413c8b49dc1a0e665f591911f1be2eb [m [33m ([m [1;33mtag: atSeattle4August2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 4 10:08:52 2021 -0700

updated ECDSA to load/unload keys with private element and point, updated banner to include number of responders, updated README for v5.2.1

[33mcommit 5084cda69445df78b951db0281438bfc08f14cdd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 4 09:48:08 2021 -0700

updated mudsums

[33mcommit 60ef950a44f0366bf2f1f2f9b4e9fa9370cbfdff [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Aug 2 15:53:41 2021 -0700

cleaned up ECDSA after Fp/F2N split

[33mcommit e59ee19214b4890878371e42f19e4e3551044a1a [m [33m ([m [1;33mtag: atSeattle31July2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 31 22:55:34 2021 -0700

added missing jumbogram IPsec tests

[33mcommit 241b2debc27b340bf8138570db7dca800b3ea933 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 31 22:54:08 2021 -0700

split Fp and F2N ECDSA

[33mcommit b1049f7603e6dc82acadb105e7387ccb97ab0ed4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jul 25 17:46:51 2021 -0700

coverage work

[33mcommit 64bff3fc21cee141b9f9e0430a36e1cfdc4637d3 [m [33m ([m [1;33mtag: preSeattle18July2021v521 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jul 18 17:42:05 2021 -0700

coverage work

[33mcommit 59d033143eaefec64ad1cfcba26da33c90706fed [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jul 16 21:20:45 2021 -0700

added specs, updated mudsums

[33mcommit 93f263b144b770f6500fb029005445f424182f3a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jul 16 21:17:11 2021 -0700

removed debug code

[33mcommit 59f0a3ec5b4a1168af3e39731411879e500d1910 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jul 16 21:12:56 2021 -0700

coverage work

[33mcommit 32ca0bfdb0944b0be3cdd94d428a2599e362c130 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jul 15 14:21:22 2021 -0700

    coverage work

[33mcommit b876b39aabe6f10c03b2976d3305cf7162909216 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jul 14 13:24:10 2021 -0700

    coverage work

[33mcommit a214b1a02a385e2555d338d3faa1a7bb35ad0d01 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jul 8 17:11:03 2021 -0700

    updated log level to removed INFO messages

[33mcommit fe684d1c2851e5568372e4ba74ec17065c54f5f3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jul 8 10:34:00 2021 -0700

    updated all signature interfaces to be consistent (RSA, DSA, ECDSA, XMSS, LMS)

[33mcommit dcdc15c0e8c55aec73e238b3cd8df00cf4c76d4b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jul 7 10:54:25 2021 -0700

    updated for XMSS and LMS to remove bool and update status, added missing XMSS and LMS to flow setup

[33mcommit 40af3782b02c2b0035af840f1316a84c80e683bd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 3 21:22:40 2021 -0700

    code cleanup on tls13

[33mcommit 15749c1001213deb5c38df36c2ab458e23680d5a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 3 20:17:54 2021 -0700

    added tls13 class

[33mcommit 3eeb1d08a99fbbf70e48a807c37649ba26c0e5d3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 3 14:40:27 2021 -0700

    separated TLSv1.3 from legacy, updated signature tests to add more streams and bitsizes

[33mcommit 9ce10793225d296f8af1a88e59daab5758072e07 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jul 2 14:43:59 2021 -0700

    moved utility functions to their own directory

[33mcommit 804afbde25150055512c104c504c1306d993bc59 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jul 2 14:14:52 2021 -0700

    script for converting to PDF for copyright submission

[33mcommit 6183324e62c5cd37a5866d141307c2f68cb13eb0 [m [33m ([m [1;33mtag: release-5.2.0-FINAL [m [33m, [m [1;32mv5.2.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jun 27 21:48:51 2021 -0700

    updated mudsums

[33mcommit ba7cf3fc8a24d40f7e5a3565bdeed0c5f8f5472e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jun 27 09:50:22 2021 -0700

    ruby script for generating test configurations

[33mcommit a778ffe5612edef3a471bb6876e855f91080b0bc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 26 19:40:04 2021 -0700

    updated mudsums

[33mcommit a988ee95613365270c91f6aff8e9d1e81b48d2ab [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 26 19:31:30 2021 -0700

    updated mudsums

[33mcommit 746010d623c128b6b70c903cca61ae07fc0b61cb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 26 19:27:16 2021 -0700

    fix for BER encoding issue

[33mcommit 2ac4172d48ad345006bd4d2a2c7bf8a081fdd3d1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 26 13:39:11 2021 -0700

    fixed signature postprocessing

[33mcommit a05a31f45da6d5c9fa3b14521fc2e1ba7cf306cf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 25 21:23:51 2021 -0700

    updated mudsums and unit tests

[33mcommit c6fff518ed62bb259a447725bc492b7815f87feb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 25 21:16:12 2021 -0700

    updated mudsums

[33mcommit 0b11b46f9ac1952041da060c44ee145a7cb02950 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 25 21:14:15 2021 -0700

updated RSA to be consistent with DSA and ECDSA

[33mcommit 74a3177bba01319f683fc8f4e61d56fe01bd0d79 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jun 24 22:45:46 2021 -0700

updated mudsums

[33mcommit 870c219d4c42d0e7e2399000c671bc6c408edba1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jun 23 19:33:01 2021 -0700

fixed some error comments, added line number to str_status()

[33mcommit 66de237c58e82a3460b2648535f949bbdd415114 [m [33m ([m [1;36mHEAD ->
[m [1;32mv5.2.0 [m [33m, [m [1;33mtag: release-5.2.0-FINAL [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 22:03:25 2021 -0700

updated mudsums

[33mcommit 57d233d2439e00ea8f8c67aafb2270064a5e2e57 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 22:02:59 2021 -0700

updated GIT log

[33mcommit 628f69ae0435da0c6dd13751f964a98b41ea2123 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 21:38:03 2021 -0700

updated mudsums

[33mcommit 3d68268cfa41dbb0e3ffee5f245652d49dbecf3c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 21:37:37 2021 -0700

updated README

[33mcommit 8e400ba5b36ec703fa580a498c12ec600e3f3169 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 21:36:38 2021 -0700

updated mudsums

[33mcommit 4bb210ae9ece82c0a8c45a29a486357b8c9ae7b4[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 18 21:36:09 2021 -0700

update status in signature schemes rather than just a boolean

[33mcommit 3c60eb00744e3835890d80671559a016b001ea66[m[33m ([m[1;32mv5.2.1[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jun 14 22:34:44 2021 -0700

    updated makefile to clean XMSS and LMS directories of coverage files

[33mcommit 1406405b673b3b29a7942dcb6a0550cd45c060e6[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jun 14 22:31:32 2021 -0700

    update for sigantures in testbench

[33mcommit 686487c1db60b115377093c5b3c1fbab3de79a29[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jun 13 19:08:35 2021 -0700

    updated mudsums

[33mcommit a43929644e2413bdece10a56839419694b0e3ede[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 16:51:30 2021 -0700

    updated mudsums

[33mcommit 11382cb457515bccea26eb5e7913ba8a87f00d87[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 16:50:06 2021 -0700

    updated mudsums, added back licensing

[33mcommit 50e1cd2e2df2e3c601e8605fb2fee69f152e5449[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 16:47:37 2021 -0700

    code cleanup from static analysis

[33mcommit e3262261716df1cfc0851056141eda2365c2c8eb[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 13:29:54 2021 -0700

    updated schema with missing field from parser, units

[33mcommit 0cbf34a1fc8be7ea0fb2c9d71c93f5dda32051f1[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 13:24:28 2021 -0700

    updated schema name to be correct with parser

[33mcommit 2d5e5d21ff47b0356afb09125de24ba048359e22[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 00:32:18 2021 -0700

    added back licensing

[33mcommit 074708355c7847903921fba5e50ebabf58ca837a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 12 00:28:05 2021 -0700

added back tests

[33mcommit 0e04a02c24ba0e6d21476c23e554ae52fe065687 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 11 18:38:04 2021 -0700

updated mudsums

[33mcommit d555285c5cb3b4c216600d635ad257bcef09287e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 11 18:36:54 2021 -0700

fixed TLS bug for CCM_8 versions for programming error

[33mcommit 6d5ad339bd72d1c05ab0126c371636d63ce9fa7d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jun 8 20:28:52 2021 -0700

fixed makefile, updated mudsums

[33mcommit 5bb079a4c5e1e7c3afd241e3e5837597daeb966e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jun 8 20:22:00 2021 -0700

updated mudsums

[33mcommit 4e309c014cc9e4f9f62ebd43ac73c421ec33f8bf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jun 8 20:20:32 2021 -0700

code analysis cleanup

[33mcommit 1da4848d993d211a79cc8d7dd548d734f528e8bc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jun 7 22:22:27 2021 -0700

code clean up, static analysis

[33mcommit 4737fa6d2e09a373a6d82e3fc6968a1f184f3a60 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jun 5 22:30:43 2021 -0700

updated mudsums

[33mcommit 08f52770468b1a64c19c4244f679433ba3faee4a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jun 3 12:59:07 2021 -0700

udpated make with new target

[33mcommit b4de89c617fab8c13f15df62f5df3da74d772f35 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jun 3 12:56:40 2021 -0700

split testbenches for SEC and non-SEC

[33mcommit d7f110352ddf8223a8b6f17d74e6e7f26b99f655 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jun 1 23:17:22 2021 -0700

fix for multiple responders, able to run any number as long as there is memory (six tried)

commit d34102b9ed2859a8d2a1a1529f6356d09947283d (HEAD -> 5.2.0)
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 24 23:52:30 2021 -0700

added XMSS and LMS to responder and exec engine

[33mcommit a7335debf1feeda2fc94b8eeb0f6e5c3de0458cd [m [33m ([m [1;36mHEAD ->
[m [1;32m5.2.0 [m [33m, [m [1;33mtag: release-5.2.0-RC2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 23 18:03:06 2021 -0700

added XMSS and LMS to random testbench

[33mcommit bdb862e70176791e8a27c61b0d0b00b5cf058ea8 [m [33m ([m [1;36mHEAD ->
[m [1;32m5.2.0 [m [33m, [m [1;33mtag: release-5.2.0-RC1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri May 21 18:51:41 2021 -0700

updated with licensing data for 5.2.0

[33mcommit ed796627227f24a5cfc62e758682a94e98d40037 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 20 21:57:36 2021 -0700

updated mudsum

[33mcommit ba98cbd66b1337ac9b1fd61d0ac6e471f3808210 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 20 21:56:30 2021 -0700

updated schema, docs, WASP, product DAT

[33mcommit 9e6c7ce11f293ec2473dcabca583406f5977b16f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 17 20:48:18 2021 -0700

updated mudsums

[33mcommit c2b531befb21c81de130744a5aba42222a87778d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 17 20:43:36 2021 -0700

updated XMSS with NIST versions of XMSS_KeyGen and XMSS_Sign

[33mcommit 7a6e504235cf335acad269e791764b68ddd93cae [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 16 18:25:58 2021 -0700

added NIST versions of algorithm 10 and 12

[33mcommit 987823978978ee0e713aa976596d03557afda421 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 11 21:26:02 2021 -0700

updated images for LMS/XMSS

[33mcommit c6a5568a8e199b0ffb0a6ee38c095300c8ec0b33 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 11 21:25:33 2021 -0700

debugged test LMS vector 2 that uses psuedorandom key generation

[33mcommit ee89967721a00bb18e851bcbaea11440b53875fb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon May 10 21:56:44 2021 -0700

updated to allow leaf value to be passed into LMOTS, fixed LMS, updated unit tests

[33mcommit 4dfc6634725e17f17ad584aa7b7fc9b408db61a2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 9 20:22:14 2021 -0700

partial debug of LMS

[33mcommit b098f7c0bbb8959703725fd392fe542096bce679 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 6 21:59:16 2021 -0700

added conformance vectors for LMS

[33mcommit b7dd45eea6d67e7ec9ea6345217767e9e868ddb0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 2 14:29:18 2021 -0700

updated mudsums

[33mcommit c36498167b52255db71b83264a3242ced2fb6c95 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun May 2 14:28:03 2021 -0700

compiling LMS, updated unit tests, updated documentation

[33mcommit aad7f851cf077585621dbfdd497e55085f5a259d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 27 20:58:28 2021 -0700

updated mudsums

[33mcommit 072a72a863d4dfe1f7c601deccd0300e4c2e6362 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 27 20:55:21 2021 -0700

updated LMS documentation

[33mcommit 2041547e492359ed69e42f674897074224e13b5b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 27 07:02:22 2021 -0700

updated mudsums

[33mcommit b5f603282550cd254d6545fab26c3488a2669399 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 27 06:59:57 2021 -0700

removed LMS files that are not needed

[33mcommit 5f21376550d1b92955165f1b493bf9efed2bcf42 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 25 21:23:12 2021 -0700

updated mudsums

[33mcommit 50333d5ac0def00dea6b21fb13c555289ff26317 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 25 21:16:29 2021 -0700

updated mudsums

[33mcommit b7bd7ff586833868b1e76d6098af6c84e14cedda [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 25 21:16:00 2021 -0700

updated schema for protocolpp(protocol++) moved cryptopp

[33mcommit 68b38eda726fa66e0799eafcfe22df9322b37b19 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 25 12:26:12 2021 -0700

finished coding LMS, needs debug

[33mcommit 6a22bb5335af36eb10c1f3cd8a6e343f144f57a8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 21 21:30:22 2021 -0700

updated mudsums, LMS keygen, and signature

[33mcommit 510b14fbea0df1cd1d4b5ea4a4974da0ea9f7e73 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 19 18:08:39 2021 -0700

fixed Wifi PBKDF2

[33mcommit 9a0356d459c95d73fcfa859232809dd2ddca6c00 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 17 22:12:09 2021 -0700

updated versions

[33mcommit 98c4b027944ad01cf10eef3b6460bbe768f921de [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 17 21:48:25 2021 -0700

updated copyrights, licensing banners

[33mcommit 943aaede7516fc076d1e155e789295a2d21eb231 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 17 21:00:38 2021 -0700

crossing t's, dotting i's

[33mcommit 3284fded75dedfca8c95eeeea693ae07cf765891 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 17 00:52:56 2021 -0700

fixed typo for LMS enums, fixed replay prediction bug

[33mcommit 9ed95aa22b22d48ffaa435fdc1836e01a9d4aec3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Apr 16 18:06:13 2021 -0700

finished coding LMOTS

[33mcommit a9df98e15d231a905faa787508e58163fc652a2d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Apr 15 23:01:59 2021 -0700

initial checkin of LMS Signature Scheme

[33mcommit 929c712aa34d61d34680779634b8ba211c285615 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 14 21:16:15 2021 -0700

updated mudsums

[33mcommit 5a8178866f93d290e65e40176e9b74c560550a1d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 14 21:12:37 2021 -0700

updated XMSS documentation

[33mcommit 5bbd2e68d0e63d4a0cea09b50cfe1eac0d2c742a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 14 05:26:06 2021 -0700

updated mudsums, full log

[33mcommit 5065fc565f3af4bfc41faea1821bc583bdb23d6c [m [33m ([m [1;36mHEAD ->
[m [1;32m5.2.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 11 16:15:18 2021 -0700

updated documentation for XMSS classes

[33mcommit a22978c531c469cbcf176e78de07707ca494737f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 10 20:52:54 2021 -0700

added security association for XMSS, debug of new XMSS inteface for protocolpp

[33mcommit e39ccb2aa6faaed53b53feb28251e7a7c9e62de6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 7 20:25:18 2021 -0700

updated to crypto++ 8.5.0

[33mcommit 322a051e69278e0bb8c83cad216e5e1a01cc25fc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 5 23:02:50 2021 -0700

updated Doxyfiles for lastest version

[33mcommit 1634d818995430568d850721d6e650e1380b2c02 [m [33m ([m [1;33mtag: release-5.1.2-
final [m [33m, [m [1;32m5.1.2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 5 21:47:09 2021 -0700

fixed doxygen warnings after moving to newer version

[33mcommit 60437cca90cd4f16cceb232759b6d27a50d7331b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 5 18:48:30 2021 -0700

added params for XMSS and WOTS, cleared out addrbyte except where needed

[33mcommit 4b8772af23c4d02c9ed7b06772fd112b34979670 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Apr 5 18:01:18 2021 -0700

updated with XMSS

[33mcommit b34c792234ae1d513043023fdeae7d0486d61eaa [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 14 21:03:01 2021 -0700

put back removed runs for coverage

[33mcommit 94fa49471f2a4b133f3dd4671420b1bf947ed915 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 14 21:00:54 2021 -0700

    updated ppp files to create more combinations for coverage, added jxmss to interface

  [33mcommit d2f6c51bf66760c2f5e63318cd60602e2b3563ad [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 13 12:56:39 2021 -0700

    updated

  [33mcommit a3b0e22c342c8ae50c656fdb845387e85e7c48c3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Feb 9 00:01:55 2021 -0700

    debug for hi-res timers

  [33mcommit ed246d35c6e61b035123c0f3185ce9d349775c29 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 8 23:29:21 2021 -0700

    updated test.cpp sources to add jexec, added hi-res timer to jexec for latencies, updated jtestcfg to pass units to cfg object

  [33mcommit 9b00f49f2a98e48a095386a5ffb7270ca4906c10 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 7 19:28:27 2021 -0700

    updated with additional test configurations

  [33mcommit fffd078fb9fe9914e6876140e308bc89fdd6141e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Feb 7 19:22:37 2021 -0700

    minor updates for version, formatting, version checking

  [33mcommit 23c83168d7213fe344f67f8576949f1de6c5ea58 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 6 23:34:49 2021 -0700

    updated unit tests

  [33mcommit 45167480c274adba3894e861e7aaf81ac2f43d3f [m [33m ([m [1;33mtag: release-5.1.1-final [m [33m, [m [1;32m5.1.1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 6 17:31:05 2021 -0700

    updated unit tests

  [33mcommit 333afb953e4a9e1cf6c2acdaf7821f052ed48533 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 1 19:39:16 2021 -0700

    fixed boundary checking in array class to check sizes before creating temp array

[33mcommit e5c4cf919f3715617e2a7e041a5f46e2a5d6c78a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 1 19:17:20 2021 -0700

debugged rsa unit tests, generating keypairs, updating fields, etc

[33mcommit dfce6f2a70f6823408f4e75dc08617ff57d79f86 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 31 22:38:37 2021 -0700

added unit tests for jintegrity, jconfident, jrsa, fixed some names in RSA header file doxygen

[33mcommit 58577359b11e52c01ded20bb28b782fe90e1b0d2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 30 23:08:11 2021 -0700

added more unit tests for jconfident and jdata

[33mcommit 318d87a02e7c92739d8510d42b9d9011994911e0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 30 00:18:09 2021 -0700

updated with blob unit tests

[33mcommit 9570e11612ead7465a177aa6f37cfc4532cb9913 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jan 26 01:16:42 2021 -0700

updated default constructor for TLS

[33mcommit 4e0ee089c92716b4eab4d50e342bd55da3e1bee1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 24 02:29:38 2021 -0700

updated usage banner for copyright, fixed finish banner to correctly report seconds of elasped time

[33mcommit 50b4db82cb120347c5c49f9c74aaac51c4f50e5a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 17 17:00:21 2021 -0700

missing files for cryptopp 8.4.0

[33mcommit 134e25268ac388c8680f46fda72fd7890c7678d9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 17 16:56:17 2021 -0700

fixed missing stream flag for BLOB

[33mcommit 05972e698349bddf6a86b64984a4055e8a5f28de [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 17 15:59:41 2021 -0700

fixed some comments from cut-n-paste error, fixed an extraction in BLOB

[33mcommit 9e4bc1be51bcbc9463fce5e753c790edfdd668c7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 17 14:16:45 2021 -0700

removed mtrand from CMake, fixed range issue uncovered by distribution, fixed unit test to no pass NULL pointer

[33mcommit 3005fc5d32487bdc6063d57a3a1ca587dc371029 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 17 13:06:24 2021 -0700

updated to Cryptopp 8.4.0

[33mcommit dcce00737bf2035d2efabdae8f1e883e80eca32d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 11 19:50:27 2021 -0700

updated to use distribution for ranges

[33mcommit c2c7a4ed11558c8a456d6d9c1f31630bd1a01ca6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 10 01:56:48 2021 -0700

removed all shared pointers from security associations to remain persistent

[33mcommit ed50cd29eecf945ef9fc3ce1a94ec7f4af11ca33 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 10 01:55:23 2021 -0700

fixed a range issue for getbyte(), changed to using standard c++ randomizer

[33mcommit 629881bb874758e16fe9e3d8339e94c37045aad5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 9 07:08:31 2021 -0700

added missing documentation

[33mcommit e8a74cf17085b2e640286a2fd71cb3d9d569c445 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 9 06:54:55 2021 -0700

fixed missing jsecass, added post processing for BLOB

[33mcommit 0fcff754236dc3202469a306c14dcd488e4692dd [m [33m ([m [1;33mtag: release-5.1.0-final [m [33m, [m [1;32mrelease-5.1.0 [m [33m, [m [1;32mdev510 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 12 15:51:06 2020 -0700

updated release notes, mudsums, full GIT log (from initial checkin)

[33mcommit 64ccc8facf9acf1fd763f1a25934d7693ea065d4 [m [33m ([1;36mHEAD [m [33m, [1;32mdev510 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 12 15:37:54 2020 -0700

updated parsing of schema, updated schema for security associations

[33mcommit b73e88ddd7ce1e9555d2546b343d87b5e926057a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 8 08:27:17 2020 -0700

updated blob with randomizer, wasp blob debug, release 5.1.0

[33mcommit 63095fc7f5a16a3bce09c8b33cd5065672392761 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 22 14:45:20 2020 -0700

updated with images for BLOB doxygen, debug of WASP for BLOB, add get_blob to protocolpp

[33mcommit 1c31e3b19ba65418fa26d3d84de275333b6f887b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 22 12:36:20 2020 -0700

debugged jmemblob and jmemblobsa, added TCP support for IKEv2

[33mcommit 44a01b4b03b8a54efd21ad25100c03c776262b31 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 22 10:35:35 2020 -0700

updated src files with 5.0.0 copyright, added jmemblob class, documented jmemblob, generated doxygen

[33mcommit 42934dad71c7b94539ff87e6ca0b35f8432151b6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 27 12:36:59 2020 -0700

debug for tls1.3

[33mcommit 293011a6b9123a5fb66696acdc507093cde7c7ae [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 20 17:34:25 2020 -0700

fixed some SA names in W.A.S.P

[33mcommit 0a1b377997dcc73d0b4da3866aaf4f71239f9994 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 20 17:23:00 2020 -0700

added additional assertions in unit tests

[33mcommit d8d3c5b3d98c5d47c9c340e95e277c6fe1919b44 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 19 14:46:55 2020 -0700

fixed parsing issue after rewriting TLS ciphersuite selection and checking for version

[33mcommit b56aafb4707d2d65b74e2b766d90c5a9673de8b5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 17 06:23:03 2020 -0700

HKDF unit tests debugged and passing

[33mcommit 129dbc50a555364cd994dc5cf2beb2195060661e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 16 22:14:45 2020 -0700

partial HKDF debug, conformance vectors 1-4 pass, 5-7 fail (likely a cut and paste error of the conformance vectors)

[33mcommit 860a2be173249ce3fe6c7e208c758952149c51c6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 15 20:33:42 2020 -0700

updated with HKDF conformance vectors

[33mcommit 67889275e4a327da0f4e692b90e4e95267ce4485 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 13 11:54:23 2020 -0700

updated with new HKDF key material function for TLS1.3

[33mcommit 681cf9c6bd79af74be1da8d6cdb2edbe3db480fd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 8 22:09:38 2020 -0700

added TLS1.3 application record code with padding

[33mcommit 618ae12ffe753068bfddfc700b1f005a1b875a21 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 4 21:11:46 2020 -0700

updated mudsums

[33mcommit 920a95c7617184e7e8af00b8eb089263a140aea0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 3 22:40:03 2020 -0700

fixed some parser issues, schema checking

[33mcommit 49bb58c259a835cf1301049100aac96707ee4b02 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Sep 1 22:36:20 2020 -0700

added intersection to jarray, code cleanup on jproducer, jrsa, updated wasp for TLS1.3

[33mcommit f8bd25d1a8f4694a163fffe6be721c9e5a0eb94f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 30 21:23:46 2020 -0700

updated version

[33mcommit a8bcab8f537f45a8cfa41ecb0768074d6b8175b1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Aug 30 21:21:49 2020 -0700

updated constructors, fixed secass lookup

[33mcommit 0ff4f9afbd8753980d382aeda9a39fb6f320b1d4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 29 19:42:38 2020 -0700

fix for zero length array copy construction

[33mcommit 611d0ce0c9b474bd3a25eb697736620345ba61ff [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Aug 27 20:45:54 2020 -0700

updated for WASP

[33mcommit 45e1fbd2f60f3115b331b06d8cfd0160f0172943 [m [33m ([1;32mdev500 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Jun 2 20:47:13 2020 -0700

added Validate function for PKI key pairs, fixed key pair encoding to HEX for XML

[33mcommit ee837a291f35ee140e657cba0e7468b5ad40408e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jun 1 22:00:13 2020 -0700

partial debug of RSA simulation

[33mcommit 2c52e83ff1f82cdf828bc2f123a958c2a80cc62c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 28 21:25:29 2020 -0700

updated for PKI, clean compile

[33mcommit a2ebee851ffc4feec8d408b5a3964873207e1248 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 12 23:57:12 2020 -0700

added DSA and RSA security associations for running standalone

[33mcommit 4e89baa89f19fc6c4e8541bb5f8623623fdbc1a7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 2 20:10:10 2020 -0700

added units to execution units

[33mcommit 5829ff637565f7a4b99942435047c82244d16e81 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 28 18:52:02 2020 -0700

updated mudsums

[33mcommit b3755e348233d4be08561aaa86eca634c9f80c4a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 28 18:43:40 2020 -0700

updated all versions to 5.0.0

[33mcommit f70a10602bd159d8e505d39c895c8ea364dfaf4e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 26 18:32:42 2020 -0700

fixed TLS bug for multiple execution units

[33mcommit 828a23dca90ef45e766b569088c3dfeac755006c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 26 11:21:57 2020 -0700

fixed TLS anti-replay for multiple execution units

[33mcommit 8cc5227aa85bee7aa1a53b915451e1054c62baec [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 26 11:10:51 2020 -0700

fixed WiMAX anti-replay for multiple execution units

[33mcommit 225bd3dd4d7f644ec965088f0ca893084f37f692 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 26 11:04:32 2020 -0700

fixed SRTP anti-replay for multiple execution units

[33mcommit 87b90857ddf532ad347c53c1540777357153eb32 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 26 10:42:18 2020 -0700

fixed MACsec anti-replay for multiple execution units

[33mcommit d70624f7fd7ae9bddecbd9b0ca68e630025a3c21 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 25 18:51:19 2020 -0700

fixed Wifi anti-replay for multiple execution units

[33mcommit 183b1f578c282575b4448cfe89ec479bad635860 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Apr 25 12:21:52 2020 -0700

fixed IPsec anti-replay for multiple execution units

[33mcommit c46266c4911096cf1410c8e1747c9604c2974838 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 22:15:31 2020 -0700

beginning work on multiple threads and responders

[33mcommit 154fdbc16daac262b93e1f85c9da9d73cb148d05 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:57:56 2020 -0700

updated for new test configuration

[33mcommit 5339d7c379ebc28729cdb9c9841849760e19d75a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:57:03 2020 -0700

cleaned some code to be more generic

[33mcommit 0b41d199499c627c0c7839748490f9d4336a6e42 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:55:40 2020 -0700

version bump

[33mcommit f308003580c7e129ef10ec4406056958fb2af3e8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:53:38 2020 -0700

updated

[33mcommit 0b9c7eb7fbabfa307a1d9e1de751f539f33b1656 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:49:44 2020 -0700

moved to TinyMXL2 8.0.0

[33mcommit 508bc963d9fa0463855cd2ff4e0c42d36c207d64 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 8 21:48:34 2020 -0700

fixed epoch to be zero when not DTLS

[33mcommit 58092328c374dc45cbed6349ba1f499d2e542d77 [m [33m ([1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 5 21:45:37 2020 -0700

removed 4.1.0 documentation

[33mcommit 88cfa0964d4182ac268dec7a49efe4be440108f3 [m [33m ([1;33mtag: release-4.1.0 [m [33m,
[1;32mrelease-4.1.0-final [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Apr 2 21:00:44 2020 -0700

updated mudsums

[33mcommit 058b7509a0920bab046b932f1609f258f71efcb2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Apr 2 21:00:28 2020 -0700

updated distribution

[33mcommit b1cf9fe33187452d7b92efec3733ee243adabdfb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Thu Apr 2 20:58:23 2020 -0700

    updated mudsums

  [33mcommit 07dbf79fe46c3b9b6021a749b2f3eb103f04c2e4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Apr 2 20:58:01 2020 -0700

    updated Filelist to add test configurations, distribution install to include test configs

  [33mcommit c0c0ececa743044067e177151b7d1553abc2b48e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Apr 2 20:54:03 2020 -0700

  [33mcommit e5f57ee8eadc35385fd384634469b100907a1757 [m [33m ([1;36mHEAD [m [33m, [1;33mtag: release-4.1.0 [m [33m, [1;32mrelease-4.1.0-final [m [33m, [1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Mar 27 22:18:04 2020 -0700

    updated cppunit tests, mudsums, documentation, and release for 4.1.0 final release checkin

  [33mcommit 17be8873ac50af770084624cc7981f42e66fae74 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 26 23:55:31 2020 -0700

    updated makefile and mudsums

  [33mcommit bb92e96f3acfcc632390c55089f3aaef2e2e3c5f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 26 23:38:13 2020 -0700

    updated mudsums

  [33mcommit ee9eb26bd54436b14c29da62686c46f02daa4e35 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 26 23:37:12 2020 -0700

    updated runprotpp with new configuration files

  [33mcommit e040d9b50de8fccf8fe0cb7b0636f1a0ff83a80d [m [33m ([1;33mtag: release-4.1.0-rc1 [m [33m, [1;32mrelease-4.1.0-rc2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 26 12:52:54 2020 -0700

    updated mudsums

  [33mcommit c33256aaa5e65a1b5111a31b076f45d72a425832 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 26 12:50:20 2020 -0700

    updated product DAT and ID for licensing

  [33mcommit 45dab11dd35c4200af73b9a44028c91f3d29998c [m [33m ([1;33mtag: release-4.1.0-rc0 [m [33m, [1;32mrelease-4.1.0-rc1 [m [33m) [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 23:39:35 2020 -0700

    updated README

[33mcommit 231492ace8cb62e62220059e2cd6b983f9773d28 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 23:37:47 2020 -0700

    added valgrind test configuration, added mudsums to distribution

[33mcommit 20b730daea9f3cda77eab1bbf43c8900439c73e5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 23:29:31 2020 -0700

    updated test configurations with correct version

[33mcommit 6f1aa60b2b00e558efb6c0024e780460f27bcc31 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 23:15:13 2020 -0700

    updated License for distribution, fixed SRTP replay bug

[33mcommit 1759d032909de1d31d7dc82c7a3f23b778ceaae1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 21:13:48 2020 -0700

    turned off debug for replay packets

[33mcommit 691826d868bc93609ccda3f01266e06d10cfd90c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 19:05:35 2020 -0700

    added random replay packets to wimax

[33mcommit f21a758bb1d3298fbda2e447cb78144854a5b66f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 25 18:02:25 2020 -0700

    updated source code legal verbage

[33mcommit 3fe88b5f9ac50825a7fa158a98f58486f828fbc5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 22 23:04:58 2020 -0700

    updated wifi with random replay packets, added testbench configurations for all protocols

[33mcommit 249e5a7ade0aa238cc172a356d75a84c9f059c29 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 22 17:39:27 2020 -0700

    bumped version, added copyright for v4.0.0 to all files

[33mcommit 767f3634bdc49146ac8a42f038c86dc73da3cf6f [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 21 23:57:42 2020 -0700

    replay support for SRTP and TLS

  [33mcommit ee6d701e8fda2250adea9978ad0335cd6e7feb73 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 21 14:53:03 2020 -0700

    removed excess debug logging for antireplay

  [33mcommit 2587d207632963de3a3c4826be33b0bd933cbc70 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 21 14:27:44 2020 -0700

    fixed TLS generated replay packets

  [33mcommit fb4a5c9044f3e2cfb3749a8d0a7dcd3ac9246185 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 17 23:27:13 2020 -0700

    more random replay packet debug

  [33mcommit b4723fa6f2fc363f94f2fa8c8a25f47f546e5b0d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 15 15:50:24 2020 -0700

    added replay feature to protocol

  [33mcommit 9a0fe039150dffc582bf8afab85ebb9480facf02 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 15 05:48:26 2020 -0700

    added random generated replay packets for IPsec (NORMAL, SHIFT, WINDOW, REPLAY, LATE)

  [33mcommit 5c05fd0b158a62e36fd5e0f276fc60d000d0549b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 3 22:21:34 2020 -0700

    checked in reference testbench configuration

  [33mcommit 0e5022a0252c0288e4eb206acafd9cea8323c8b2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 3 21:54:05 2020 -0700

    updated copyright dates, bumped version

  [33mcommit b25439d8ee27008e438c22db7a99845bdf8fa099 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Mar 3 21:00:40 2020 -0700

    fixed reproducibility for new testbench configuration

  [33mcommit 7d305ef87804486c2d98e2ed14d34210da9606c8 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Mar 1 19:41:17 2020 -0700

    added support for testbench configuration with parser, support for multiple responders running in parallel. Needs debug, support for multiple threads per responder, arbitration when running multiple responders (should be configurable for type ROUNDROBIN, ONEHOT, PRIORITY)

  [33mcommit 0f0c5bd68af35a27e182f23a95b2f15ddc262f49 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Feb 26 22:49:11 2020 -0700

    debugging of testbench configuration parser

  [33mcommit b24977407eec8eb4f66065637e6927558e1d5f7a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Feb 19 22:23:42 2020 -0700

    jtestcfg parser debug to remove output from iring

  [33mcommit 5af949df4266a69f8e538906c7dcaecfe585b994 [m [33m ([1;36mHEAD [m [33m, [1;32mdev500 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 15 14:21:34 2020 -0700

    new testbench configuration parser

  [33mcommit 7fd605de408bce09ba17e1fb8a734452a9c5da00 [m [33m ([1;33mtag: release-4.0.0-final-release [m [33m, [1;32mrelease-4.0.0-final [m [33m, [1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 13 21:16:09 2020 -0700

    updated licensing to reduce number of calls to server

  [33mcommit 5a9f03ffba4138af7726d980b3c1d32c43ff0ea2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 13 21:12:44 2020 -0700

    updated licensing to reduce number of calls to server

  [33mcommit f6a33e2f4d9e5f16ff22a3c5e00cfb3290792e0a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 12 20:56:36 2020 -0700

    updated mudsums

  [33mcommit 2c689c83c983384f84d55a4b47516a993bd7ee37 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 12 17:41:18 2020 -0700

    updated mudsums

  [33mcommit 355d513843704d04a09d3a5b3da4eac7ade58469 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 12 17:35:09 2020 -0700

added better status reporting for licensing software

[33mcommit 64158e44bdd172d9b38f89795ca7450b8a84c828 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 12 06:59:51 2020 -0700

updated product data and mudsums

[33mcommit 99e40702f25e81161e1230e54a0668f7afd8fc99 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 11 23:06:11 2020 -0700

updated mudsums

[33mcommit 44222a6654dbb10cfff2c48fc4bd874101372b19 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 11 23:04:54 2020 -0700

updated to active license if none detected before activating trial

[33mcommit 93742d5330a482982effd9c4cafcd6c8b33ab9d8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 1 23:56:04 2020 -0700

updated mudsums

[33mcommit a8740117c407b69970926c2a752621bd0d91cc50 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 1 23:33:19 2020 -0700

fixed CRC to use uint32_t instead of a byte array

[33mcommit 6473720aa3611700d4e08cc971c1f1b688193435 [m [33m ([1;33mtag: release-4.0.0-rc2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 28 21:01:23 2019 -0700

debugged integrity for all modes, fixed distribution to only install library headers, fixed product version

[33mcommit 0c1bf0ec8210071be337c9556e9509ac54c99398 [m [33m ([1;33mtag: release-4.0.0-rc1 [m [33m, [1;32mrelease-4.0.0-rc1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Dec 27 00:17:58 2019 -0700

debug of CRC

[33mcommit 63334e60a3608caa4a2295a842313765d7379871 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 22 16:18:12 2019 -0700

added Serpent documentation, updated install script, finalized distribution

[33mcommit 11ffbb447525dc31b8156b8873db31a170a127a0 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 21 22:40:53 2019 -0700

    debug of ciphers

[33mcommit 3d769e371be3cfd72b8e17e876e88ebb710f8198   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Dec 14 23:08:05 2019 -0700

    added general CRC

[33mcommit 0f311f877eaba245c34d1c4bd0bdef385b3eb892   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 10 22:46:58 2019 -0700

    updated mudsums

[33mcommit 2d6a03dc90cbec5745b8382c1d2a0303f7339d99   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 10 22:34:24 2019 -0700

    Fixed flow count

[33mcommit f13374a9d5101a0c909aa5e35ff405dd0c137ed9   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Dec 10 21:06:32 2019 -0700

    ********** Protocol++ 4.0.0 **********

    Protocol++(Protocolpp) is the property of John Peter Greninger
    and requires the use of a fee based license for ALL use cases
    please see

    www.protocolpp.com
    www.protocolpp.org
    www.protocolpp.net
    www.jpgnetworks.net
    www.jpgnetworks.org

    For license fees, evaluation licenses, and additional information

    The following copyrights have been issued for ProtocolPP(Protocol++)
    (copyright covers both names) and ALL derivative works are owned,
    controlled, and managed by John Peter Greninger under license found
    on www.protocolpp.com. Trademarks and further copyrights are pending

    Copyrights:

    Protocolpp(Protocol++) 1.0.0 - TXu002059872
    Protocol++(Protocolpp) 1.2.7 - TXu002066632
    Protocolpp(Protocol++) 1.4.0 - TXu002082674
    Protocol++(Protocolpp) 2.0.0 - TXu002097880
    Protocol++(Protocolpp) 3.0.1 - TXu002169236
    JPGNetworks   - VAu001334497

Trademark:

JPGNetworks - 87708008

****
********** ALL RIGHTS RESERVED **********
****

JPGNetworks, LLC and Protocolpp(Protocol++) is wholly owned (100%) by John Peter and Sheila Rocha Greninger. If you have received this software from any other source other than www.protocolpp.com, immediately report the offending party to https://www.ic3.gov/complaint/default.aspx for software, IP, and Copyright theft.

ProtocolPP(Protocol++) is NOT the property of Intel Corp. Intel has no rights to sell, distribute, license, or represent JPGNetworks, LLC or ProtocolPP(Protocol++). If you have received this software from anyone representing Intel, please contact Federal authorities immediately as they are infringing this copyright and contact JPGNetworks, LLC at the address found in the license

If your copy of this software has been delivered by Robert W. Santucci or Norma Bettine you have received a fake copy and have paid the wrong distributor and I would suggest you sue to recover you money. If you have received a license from any other source other than www.protocolpp.com, immediately report the offending party to https://www.ic3.gov/complaint/default.aspx for software, IP, and Copyright theft. ProtocolPP(Protocol++) is NOT the property of Bob or Norma and they have no rights to sell, distribute, license, or represent Protocolpp or to represent themselves as employees or managers of JPGNetworks, LLC. Any license from Norma or Bob or Intel will not be honored with support, updates, or new features

JPGNetworks, LLC and Protocolpp(Protocol++) is NOT the property of NXP Semiconductor. NXP has no rights to sell, distribute, license, or represent JPGNetworks, LLC or Protocolpp(Protocol++). If you have received this software from anyone representing NXP, please contact Federal authorities immediately as they are infringing this copyright and contact JPGNetworks, LLC at the address found in the license

Only www.protocolpp.com or this website has the rights to update, modify, license, distribute, sell, or make copies of Protocolpp(Protocol++). Evaluation licenses that last 60-days are available from the website

Full licenses last a year and include support and updates

Protocol++ has several different interfaces and can be configured in different ways. Preview the Makefile to see the target. Descriptions of the different targets are found below. Contrary to some people's opinion, ProtocolPP(Protocol++) is not a "WORK IN PROGRESS". The core library has remained unchanged for several years. Changes have only been added when updating to new versions of tinyxml2 parser or the Crypto++ library. NEW items have been added (drivers, IKEv2, Security Associations) that sit on top of the core library of protocols, ciphers, and authentication

algorithms with randomizers, parsers, anti-replay, and structures necessary for complete functionality

protocolpp - Executable of the full set of protocols, ciphers, testbench, and responders to provide a command line interface for connecting and testing a device under test (DUT). A user can opt to use the jresponder (default) or use QorIQ and Layerscape compatible testbench by setting PLATFORM to SECPLAT. If using the SEC platform, the testbench only reads and writes to the software rings as it is expected that the SEC connected to the other side of the software rings. See the file jbuilder.cpp

libprotocolpp.a - Static library of the protocolpp.h interface, wasp.h, and ciphers.h

libprotocolpp.so.4.0.0 - Shared library of the protocolpp.h interface, wasp.h, and ciphers.h

winprot++.lib - Static library for Windows compiled under VC++ 17

rdriver - Ring driver that for UDP, TCP, TLS, or SRTP. Underlying protocols include ICMP, IP, IPsec, MACsec, Ethernet, LTE, RLC, Wifi, WiGig, WiMax with separate threads that run both the send and receive functions from the rings

ddriver - Same as the ring driver except the input and output are queues rather than rings and have push and pop routines to send and receive packets

driver - Unlike the two previous drivers, the calling program must feed the driver with single packets that are driven onto the socket. The calling program must also poll the receive method continually to obtain packets from the receive socket

ikev2 - Support for Internet Key Exchange (IKE) version 2 for IPsec ESP with CHACHA20 AES-GCM, AES-CCM, AES-CBC, AES-CTR, and Camellia. All Diffie-Hellman curves supported including 448 and 25519. Suppoort for all authentication methods now supported (RSA, PSK, ECDSA, DSA)

test - Runs the CPPUNIT tests for Protocol++. Message outputs are for negative testing

USE CASES

Protocol++(ProtocolPP) can be used for several different use cases in development, software, hardware development, stacks, and testbenches.

* TESTBENCHES - Protocolpp comes with a testbench to allow the interface to be connected to a Device Under Test (DUT) through software rings for test of protocols, encryption, and authentication algroithms, replay windows, randomization, Diffie-Hellman routines, and other items. In addition, Protocol++ can be used to generate XML output for all of the above items that can be read back in to drive Verilog or software drivers for development of hardware accelerators and software

* STACKS - The drivers in ProtocolPP show examples of how to write software stacks that support all levels of the OSI model to allow full manipulation of all features and methodologies of the protocol stack. Want to try out a new retry routine for TCP? Change the code in level 4 of your software stack to try it out. Want to try a new

algorithm for IPsec? Add it to level 3 of the stack. Developing a driver for extended packet numbers in Macsec? Run your software against the Protocol++ testbench to ensure conformance. Additional protocols that do not need need the stack and require direct access to level 3 (IP/IPsec) such as Real Time Protocol (RTP) or its secure version (SRTP)? Disable TCP/UDP and TLS to drive IP/IPsec directly

* HARDWARE DEVELOPMENT - Protocol++ can be used for testing hardware accelerators that support encryption and authentication algorithms. Developing an AES-GCM engine for your hard drive controller? Instantiate AES-GCM using the "ciphers" interface of ProtocolPP in your SystemC testbench to driver your Verilog or VHDL through your UVM driver. Received your silicon back from manufacting and need to verify there are no defects? Read back in the XML files generated during pre-silicon testing that achieves 100% coverage, and execute them through ProtocolPP's driver (or your own driver) and compare to the expected value. Have some conformance vectors from the specification? Enter the conformance data into the XML format specified by Protocol++'s XML schema, read the data into the testbench or driver, and test the silicon and or RTL

* SOFTWARE - The elements of ProtocolPP can be incorporated into larger software projects to encrypt data, authenticate, generate CRC32 values, create Signatures, verify signatures, create PRF material, generate random data over ranges as bytes, words, or double words, enable SMFT mode and generate millions of random bytes from hardware is little or no time

These are the use cases currently being used. Development continues for Internet Key Exchange (IKEv2), additional driver features (ICMP message generation and return), offline key protection, key ring use, etc.

Please see the documentation found above and www.protocolpp.com for all options

INSTALLATION

To install Protocol++, the cryptopp library must first be compiled.
Go to the cryptopp directory and type 'make'. After the compilation
type './cryptest.exe v' to verify the library is correct. Cryptopp
also allows the user to install the library and header files by
typing 'make install'

To compile and install, add the path for libcryptopp and libprotocolpp
to LD_LIBRARY_PATH and type 'make protocolpp'. Once compilation is done
protocolpp will respond as found in the USAGE below. To verify build,
make the directory "logs" then type './runprotpp'

Both libcryptopp and libprotocolpp can be installed by typing
'make install' in their respective directories. This requires
administrative privileges.

USAGE: protocolpp [options]

Options:

```
  --help, -h   Print usage and exit
  --in, -i     Input file (either *.ppp or *.protopp)
  --out, -o    Output file (*.protpp)
  --seed, -s   Seed for reproducibility
```

--log, -l Path to output simulation log
--size, -z Size of the rings in entries
--resp, -r Number of responders
--thread, -t Number of threads per responder
--plat, -p Platform to run (WASPLAT or SECPLAT)
--endian, -e Endiness of the platform (BIG or LITTLE)
--ptr, -q Size of address pointers in bytes (4 or 8 default=8)
--sgt, -g Size of SG entries in bytes (8 or 16 default=16)
--irg, -n Address of the input ring
--org, -z Address of the output ring

Examples:

protocolpp --in file1.ppp
protocolpp -i file1.protpp
protocolpp --in file1.ppp --out file2.protpp
protocolpp --seed 1234567890 -i file1.protpp
protocolpp --seed 1234567890 -i file1.ppp
protocolpp -i file1.ppp -l filelog -z 50
protocolpp --in file2.protpp --log filelog -r 2 -z 40
protocolpp --seed 1234567890 --in file2.protpp --log filelog --resp 2
protocolpp --seed 1234567890 --plat SECPLAT --in file2.protpp --log filelog
protocolpp --seed 1234567890 -i file1.ppp -l filelog

For W.A.S.P usage, see the doxygen section

* New in 4.0.0 (Thu Oct 17 04:22:21 2019 -0700)

-- Bumped version
-- Added jconfident and jintegrity to run one-off jobs
-- Added jconfidentsa and jintegritysa to support one-off jobs
-- Added support for BLOB in SEC platform
-- Fixed RSA encrypt and decrypt
-- Updated DSA, RSA, ECDSA with new constructor for key-pair construction
-- Moved to tinyxml2 7.1.0
-- Moved to ChaChaTLS
-- Added copyright for version 3.0.1 (TXu002169236)
-- Improved coverage
-- Documenation Updates

* New in 3.0.1 (Thu Oct 17 04:22:21 2019 -0700)

-- Bumped version
-- Improved coverage
-- Documenation Updates
-- Updated licensing calls
-- Added format to all protpp and ppp files

* New in 3.0.0 (Sun Oct 14 12:22:21 2019 -0700)

-- Bumped version
-- Fixed ICMP regeneration
-- Updated time logging to be cross-platform
-- Updated drivers to look for destination on local network first

-- Updated drivers to handle IP routing headers
-- Updated drivers to handle ICMP messaging
-- Removed get_prf() and get_skseed() from IPsec and replaced with jikeprf
-- Added new parameters for MacSec (enreceive, entransmit, inuse, protectframes)
-- Fixed time reporting in the testbench to work across multiple days
-- Moved to final version of Crypto++ 8.2.0
-- Fixed missing base class calls in security associations
-- Added ability to change logging colors in jlogger
-- Added licensing calls to libraries and executables
-- Added multiple policies to IKEv2 configuration
-- Improved coverage
-- Fixed parser to reject unknown formats
-- Added ability to request multiple responders, each with it's own software ring
-- Added *.cpp file for jsecass to allow insertion of licensing API
-- Added Wifi key derivation function (KDF) to jwifi with support for IEEE802.11-2016
-- Added KDF use to wasp when generating Wifi keys
-- Added KDF use to cppunit tests
-- Added AES-GCM to Wifi, fixed NONCE generation for AES-GCM
-- Added documentation for AES-GCM to jwifi and jwifisa
-- Added BIP mode to WIFI with AES-CMAC and AES-GMAC
-- Streamlined interface for jdata and jpacket
-- Added VLAN support in Macsec for 1 or 2 tags
-- Added documentation for BIP mode to jwifi and jwifisa
-- Updated licensing and copyright notice
-- Added registration for trademark
-- Documenation Updates

* New in 2.5.6 (Sun Feb 10 23:37:22 2019 -0700)

-- Fixed memory leak in IKEv2
-- Added conformance vectors for SM4, SM3, CHACHA20, and POLY1305
-- Fixed a bug in SM3 key size checking
-- Fixed some EnumString() values for ERR_*
-- Coverage updates
-- Added images for IKEv2 payload format documentation

* New in 2.5.5 (Sun Feb 10 23:37:22 2019 -0700)

-- Moved to Crypto++ 8.2.0

* New in 2.5.4 (Sun Feb 10 23:37:22 2019 -0700)

-- Moved to Crypto++ 8.1.0

* New in 2.5.3 (Sun Feb 10 23:37:22 2019 -0700)

-- Split out signature classes as separate functions
-- Used new classes in IKEv2 to streamline code
-- Updated documentation to fix math symbols and equations using LaTeX math
-- Removed obsolete ciphers, authentication, dh curves from IKEv2
-- Generated PDF from all documentation (901 pages)
-- Updated schema to include restrictions

* New in 2.5.2 (Sun Jan 20 21:30:58 2019 -0700)

-- New class jdsa
-- New class jecdsa
-- New class jrsa
-- Updated copyright to 2019

* New in 2.5.1 (Sun Jan 6 12:45:27 2019 -0700)

-- Moved to Crypto++ v8.0.0
-- Moved to tinyxml2 v7.0.1

* New in 2.5.0 (Mon Dec 31 21:15:03 2018 -0700)

-- Separated IKEv2 functions into separate classes
-- New class jikeparse
-- New class jikev2dh
-- New class jikencrypt
-- New class jikeprf

* New in 2.4.3 (Sat Dec 23 21:39:15 2018 -0700)

-- All encryption schemes for IKEv2 working (CBC, CTR, GCM, CCM, DES, 3DES, CHACHA)
-- All integrity schemes for IKEv2 working (MD5, SHA, SHA2-256, SHA2-384, SHA2-512, AES-CMAC, AES-GMAC, POLY1305)
-- All PRF schemes for IKEv2 working (MD5, SHA, SHA2-256, SHA2-384, SHA2-512, AES-CMAC, AES-XCBC-MAC)
-- 80% of Key exchange schemes working (MODP, ECP, missing curve25514 and curve448)
-- All encryption, integrity, Diffie-Hellman, and Signatures tested against StrongSwan IKEv2 (www.strongswan.org)
-- Added all conformance vectors for CCM, CMAC, XCBC-MAC, GCM, CHACHA20, POLY1305, SM3, SM4, ARIA to cppunit tests
-- Fixed small bug in jrand
-- Added Appendix A from employment agreement to clarify ownership
-- Crypto++ support for curve25519 and curve448 not quite ready
https://stackoverflow.com/questions/50408019/crypto-ed448-unknown-oid

* New in 2.4.2 (Sun Dec 24 15:22:38 2018 -0700)

-- GIT log for all time

* New in 2.4.1 (Sun Dec 24 17:58:22 2018 -0700)

-- Working IKEv2 for AES-CBC, SHA256, MODP1024 (see log files)

* New in 2.4.0 (Mon Nov 26 22:13:39 2018 -0700)

-- Added delete_sa() to IKEv2
-- Fixed SKEYSEED and KEYMAT generation
-- Fixed AUTH payload generation
-- Fixed preshared key authentication
-- Fixed key ring issues
-- Added key ring to drivers
-- Added ability to daemonize IKEv2

* New in 2.3.3 (Tue Oct 30 19:02:06 2018 -0700)

-- Moved from pthread to std::thread
-- Moved to CryptoPP 7.0.0 for SM3, SM4, Poly1305, ARIA encryption engines
-- Documentation updates

* New in 2.3.2 (Sun Oct 21 19:02:35 2018 -0700)

-- Support for all IKEv2 encryption algorithms (CHACHA20, AEAD, Camellia)
-- Support for all IKEv2 Diffie-Hellman curves (including 22855 and 485)
-- Support for multiple IPsec connections

* New in 2.3.0 (Sun Oct 7 17:59:27 2018 -0700)

-- IKE configuration parser working
-- Updated DH parameters with all RFC value except group 31 and 32
-- Fixed gateway lookup of HWADDR
-- Updated to include Ethernet
-- Discard of packet not for this interface

* New in 2.2.0 (Fri Sep 14 22:36:21 2018 -0700)

-- Split SKEYSEED and Key material generation for IPsec and IKEv2
-- Valgrind clean ring and direct drivers
-- IKEv2 initial checkin

* New in 2.1.0 (Fri Aug 31 22:38:31 2018 -0700)

-- Added ring driver
-- Added direct driver
-- Added driver
-- Added function to interpret status word as a string for printing
-- Fixed several testbench bugs
-- Logging levels now configuration from command line with --loglvl
-- Valgrind is completely clean, fixed the remaining issue that left 168 bytes of data in use at simulation end

* New in 2.0.0 (Tue May 15 01:41:28 2018 -0700)

-- Fixed support for SEC/CAAM with new security associations
-- Added new classes and base clase jsecass for security associations
-- Moved to tinyxml2 v6.2.0
-- Removed memory leaks
-- Updated all files and testbenches to use new security associations
-- Fedora28 libraries
-- Re-qualified code

* New in 1.5.0 (Sat Mar 31 20:57:46 2018 -0700)

-- Added namespaces for ProtocolPP, InterfacePP, DriverPP, and PlatformPP

* New in 1.4.2 (Wed Mar 14 19:18:10 2018 -0700)

-- Updated driver
-- Static link of libgcc and libstdc++ in libraries

* New in 1.4.1 (Mon Feb 12 00:52:10 2018 -0700)

-- Moved to Crypto++ 6.0
-- Stripped out dead code
-- Added in template specialization

* New in 1.4.0 (Sun Jan 28 21:12:41 2018 -0700)

-- Fixed several parser and randomization issues
-- Fixed overrun issue in responder
-- updated copyright for 2018 and second copyright
-- added outlen to ringin API
-- Fixed RLC control plane bug
-- Fixes for Windows compile to configuration files VC++
-- Added Phanton colorization theme

* New in 1.3.1 (Sat Dec 23 11:10:19 2017 -0700)

-- Updated copyright with newly granted copyright reference number
-- Added mudsums for all files

* New in 1.3.0 (Thu Nov 30 00:08:31 2017 -0700)

-- Fixed next header processing for IPv6 in IP and IPsec
-- Fixed some randomization issues that were affecting reproduction of simulations
-- Generation of random extension headers for IPv6 when respective NH is selected (IPv6_Frag, IPv6_Route, IPv6_Opts, Jumbogram)
-- Found and fixed segmentation faults related to next header generation and processing
-- Fixed issue with status not being updated when generating descriptors
-- Fixed <data> nodes

* New in 1.2.7 (Fri Oct 20:38:49 2017 -0700)

-- Removed --native compile option, re-enabled SFMT randomizer
-- Fixed memory leaks in the library, still looking in testbench
-- Fixed parser bug when reading *.protpp files for SRTP

* New in 1.2.6 (Sat Sep 16 19:56:44 2017 -0700)

-- Fixed PRF generation issues for AES-CCM
-- Remove shared objects

* New in 1.2.5 (Thu Sep 14 22:28:19 2017 -0700)

-- Added #define for SFMT_MODE to enable use of SFMT Mersenne Twister otherwise uses previous randomizer

* New in 1.2.4 (Thu Sep 14 20:51:00 2017 -0700)

-- fixed makefile to build correctly with given repository structure

* New in 1.2.3 (Sat Aug 29 11:49:09 2017 -0700)

-- fixed formulas in doxygen
-- added back PRF usage for TLS and IPsec in W.A.S.P

* New in 1.2.2 (Sat Jul 29 16:15:55 2017 -0700)

-- Port to Windows VC++ 15
-- Updated header files
-- Linux debug for Windows port

* New in 1.2.1 (Tue Jul 25 19:25:10 2017 -0700)

-- Changed RDSEED to RDRAND in hardware random number generation

* New in 1.2.0 (Sun Jul 23 17:37:04 2017 -0700)

-- Support for IKEPRFv1, IKEPRFv2, TLSPRF1.0, TLSPRF1.2 as static functions in the jipsec and jtls classes
-- Added try/catch blocks in jmodes when calling encryption engines
-- Added generation and usage of PRF material for IPsec and TLS in the W.A.S.P randomizer

* New in 1.1.1 (Sat Jul 22 03:12:49 2017 -0700)

-- updated jrand for SFMT usage

* New in 1.1.0 (Sat Jul 22 03:12:49 2017 -0700)

-- SIMD based random number generation using SFMT
-- New build system to support versioning

* New in 1.0.0 (Sat Jul 15 11:43:00 2017 -0700)

-- First production release of Protocolpp(Protocol++)

* New in beta-2.5 (SUn Jul 2 22:38:00 2017 -0700)

-- Added SEC updates
-- Doxygen Updates

* New in beta-2.3 (Wed Jun 28 20:55:27 2017 -0700)

-- Updates for the SEC platform
-- Updated examples

* New in beta-2.1 (Mon Jun 19 23:14:25 2017 -0700)

-- Doxygen updates
-- Removed submodules

* New in beta-2.0 (Wed Jun 14 11:12:30 2017 -0700)

-- Print packet name when there's an error
-- Fixed randomizer to randomize on each pass
-- Fixed IP/IPSec decap with extension headers

* New in beta-1.0 (Sat Jun 10 12:30:08 2017 -0700)

-- GitHub site secured

-- First working release for Protocolpp(Protocol++) with testbench, all protocols,
all cipher, all algorithms present and working on GitHub
-- Previously for sale on www.protocopp.com

* www.protocolpp.com goes LIVE! (Sat May 6 10:47:35 2017 -0700)

-- Source code for sale
-- Documentation Available
-- Examples Available
-- Testbench Available
-- Able to run regressions with parser, testbench, responders
-- As STC informed me many times, there's no free lunch (so my code isn't free either)
-- No one has ever paid me for my code not NXP or Intel even though I was told I would be
-- I was to be "handsomely rewarded" for it. Still haven't seen a penny
-- There will be no free copies
-- Documented above

* Working testbench before Intel (Mon Apr 23 04:02:03 2017 -0700)

-- Fully working testbench
-- Screenshots taken with date and time
-- Documented above

* Protocol++ genesis (Sun Feb 8 2015 -0700)

-- jrand.h first file created with the IDE (hence the date, see file above)
-- I had been told by someone at STC to "go home and learn how to program"
-- When it was up and running, was told they didn't want my "crap code", ah well
-- I won't let NXP, Courtney McQuien, STC, Secuirty Investigators, or anyone else define me again
-- Documented above

* Additions

-- Added CPPUNIT tests as examples of usage
-- Added test executable to run CPPUNIT tests
-- QorIQ and Layerscape support has been added
-- Enabled input and output ring address pass in
-- removed responder for SEC to allow connection to device/testbench

* Fixes

-- dynamic memory tracking in the testbench
-- Fixed TLS random IV postprocessing
-- minor code clean up
-- Fixed randomization when <protocol> is present to randomize prot and dir with each pass
-- Fixed testbench to print packet name when an error occurs
-- Doxygen updates
-- Added CYGWIN compiled libraries
-- Fixed "free" bug

* Outstanding Issues

-- Arbitration of threads in execution units
-- Realignment of packets in execution units when finished out-of-order

-- See "Upcoming Features" on www.protocolpp.com for additional information
-- AES-XTS mode
-- Reordering of output from jexec
-- Multiple jexec units per responder
-- Support for KEK protection for sensitive information (Keys, IV, Salt)

[33mcommit ebc4d9c13176a28f311ce53f7eb4f7a9494e08c9[m[33m ([1;36mHEAD[m[33m, [1;33mtag: release-4.0.0[m[33m, [1;32mmaster[m[33m)[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 8 17:07:02 2019 -0700

updated with new copyright

[33mcommit 6f4255c08151321ab097b6faa446dbdc6e945d3b[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 8 16:33:49 2019 -0700

Debug for INTEGRITY

[33mcommit dda9a1757cac95f00c7d83e999a020feb8c8b601[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 5 20:29:12 2019 -0700

updated mudsums

[33mcommit 7337934673db078cf4a3bd5ba1715fdc12fc84c0[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 5 20:21:05 2019 -0700

fixed ChaChaTLS and ECB modes in jconfident and randomizer

[33mcommit 8465240225df4a432a6be6245b5e66d37ea97810[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 5 00:00:25 2019 -0700

updated README and mudsums

[33mcommit 4666e98135dd7fb69d142b59a3f0ebbd51ccbcf8[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 4 23:51:42 2019 -0700

fixed confident randomization, fixed blocksize, changed to ChaChaTLS for jmodes

[33mcommit 3d3cf1cbd9c8e38cae55d1c3006cc9033c63fd94[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 2 22:42:35 2019 -0700

updated mudsums

[33mcommit 81a44cc20bf71ed2e04674b96c9bca440714eee6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 2 20:26:18 2019 -0700

fixed m_dir collision

[33mcommit eb2d18d036a405d9567d472d37d28084b52c8ffa [m [33m ([1;32mrelease-4.0.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 1 21:44:43 2019 -0700

update checksum

[33mcommit 1fe97ecd9f548fb7da55945fbfe0ebf44f3781f9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 1 21:44:15 2019 -0700

debug for jintegrity

[33mcommit 378f271de746a59626def7888509bdcaa09f6c45 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 15:44:35 2019 -0700

fixed GCM and CCM for jconfident decrypt

[33mcommit 17f6b08f63cd56f5c2eb6d2a04204b106b24d13e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 15:43:28 2019 -0700

updated mudsums

[33mcommit db9eb1901d2893d8b440493523d8c55d5a21b7e8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 15:42:57 2019 -0700

fixed GCM and CCM for jconfident decrypt

[33mcommit 6523a5ceff8bfd1afe075fc13fc7fdc1af96b695 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 14:05:07 2019 -0700

updated README

[33mcommit 3c7d8f50a3526bd71256d0d6d267a4ec6c214a2c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 14:03:31 2019 -0700

moved to tinyxml2 7.1.0

[33mcommit 7aa3125c209eb6be891e24f5aa377e230d939181 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 30 08:25:31 2019 -0700

updated copyright

[33mcommit 3bfa29df17036e778d81055b2770025cb11b0cc6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Nov 29 22:32:59 2019 -0700

updated checksums

[33mcommit f2b8dcadee28c9d9fe3f8e3d1a658bc42874974a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Nov 29 22:32:15 2019 -0700

updated with Snow3G documentation

[33mcommit 29d959005b5910b74bbbda2da44ed02bcdaf69b6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Nov 28 19:58:12 2019 -0700

updated mudsums

[33mcommit 7c57875e12125e42c4c41f9d63552613eb0ddedc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Nov 28 19:44:53 2019 -0700

updated documentation

[33mcommit 2574f0c95bb9e27058fbcc9225d54543df22d568 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Nov 28 18:49:37 2019 -0700

documentation for ZUCE

[33mcommit 6ff7ad076abe3cba5b78717e83a92cbfb9714ff0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Nov 28 01:14:28 2019 -0700

additional debug for CONFIDENT mode

[33mcommit 9e9d9b2802c29631a52b5b6afe05969226fc048c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Nov 22 22:26:55 2019 -0700

fixed a bug for a missing variable in the initializer list, additional debug for CONFIDENT

[33mcommit 83d9e725138942efeef847ea7b40fc720b0a36a7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Nov 21 23:44:31 2019 -0700

updated with debugged code

[33mcommit 9f3a9c59cf4f55deefcda51832fb8908fbb26ae2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Nov 20 23:11:09 2019 -0700

debugged randomization of jconfident

[33mcommit 45e9be7f4c0ff26cee77866de11a36048606332d [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Nov 18 23:22:18 2019 -0700

debugged integrity protocol with randomization

[33mcommit b421d20828b862c7b21880e572c0855a8f268c06 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 17 22:18:40 2019 -0700

fixed licensing software

[33mcommit 30ede9bd68eb15f29a3a92b7e32da1e435fab9f9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 17 00:53:35 2019 -0700

debugged jintegrity and jconfident

[33mcommit 4645b6d3a05093f1f743e7f6d0344eedd224d773 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Nov 16 00:59:18 2019 -0700

updated jconfident and jintegrity with additional images

[33mcommit 3242d61ac0c60ceaa1767773ab48f873a5503baf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Nov 13 20:52:26 2019 -0700

updated jcipher to include AAD data, fields adde to jenum

[33mcommit 93c97129c43aac64316512346fcf4173cf5cf9b8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Nov 13 20:48:52 2019 -0700

updated jcipher to include AAD data, fields adde to jenum

[33mcommit 78ae4f0978b55d1ad3174a1ee412008d3820aee0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Nov 12 22:10:16 2019 -0700

debugged jcipher and jauth for compilation, fixed some documentation

[33mcommit 85c5c662857b0fa888ab119a3f00c4da310856be [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 20:07:31 2019 -0700

updated full_log for development

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:57:23 2019 -0700

updated mudsums

[33mcommit b2a519bdcdea5fa427edca1e24c928aefe66bbc3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:56:58 2019 -0700

updated README

[33mcommit 7a8fce34dc8181ed0cb7418c44d665385c26249e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:53:18 2019 -0700

update

[33mcommit 37396779422f6ef515639cff3560d68fcbcca7fc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:42:27 2019 -0700

updated

[33mcommit 0f42c60929176ed289a9965c9390e97e371d6a2a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:37:11 2019 -0700

added support for one-off cipher and authentication processing

[33mcommit 081637d793dcb96ae1346994b81b70978b7f8657 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Nov 10 19:36:39 2019 -0700

added support for one-off cipher and authentication processing

[33mcommit 411c7b7a3d0d6abe6e462448fde2d2d4bf0d7c84 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 27 21:15:18 2019 -0700

added regression make target, updated ikev2 and jrsa

[33mcommit 8ca33ba3b99ff64b6a35778150db893395393fd5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 27 20:31:29 2019 -0700

added new constructors for DSA, RSA, ECDSA to construct from keys or key pairs

[33mcommit 81a30a57def8b67a5c9006458428ca066fa7bba2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 26 17:35:08 2019 -0700

documentation updates

[33mcommit c8bc7e1b7a38ae552ac040cb6a35b11bfa2cf3cc [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 20 21:42:15 2019 -0700

fixed RSA encrypt/decrypt functions, added additional set/get fields

[33mcommit e80cbe62438ba52e92c36907bf548dbe83f38dc5 [m [33m ([1;33mtag: release-3.0.1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Oct 14 08:06:44 2019 -0700

updated with license checking fixes

[33mcommit 59ae156c4c149787ab6fe30587cc125608c1474c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 13 12:23:08 2019 -0700

updated licensing terms and copyright notice

[33mcommit a88f5ea4044c507d0f9fb779e2132661ce476c48 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Oct 13 12:21:59 2019 -0700

updated licensing terms and copyright notice

[33mcommit ba096d57a6999664faea6d0e2a523bce8e2b7f0b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 12 19:52:28 2019 -0700

updated documentation for most of the testbench classes

[33mcommit a4fd651efa2fb9171dd2ebfe1e643d6ee4b9176c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 12 00:29:55 2019 -0700

documentation update

[33mcommit 029be64b58848edbe07e93bc6435647b171c85cb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Oct 12 00:12:59 2019 -0700

updated documentation

[33mcommit 9d5b54e9f4a7261b45b60c4cd8f94af0b3e120f1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Oct 11 21:48:59 2019 -0700

documentation updates

[33mcommit c7039d0bf3ac46e1de36670efddf0e991bc0c72a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Oct 7 23:43:12 2019 -0700

updated mudsums

[33mcommit f5b41b4f0ba8431d8e004cc7d807ddc765ba358a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Oct 7 23:42:37 2019 -0700

updated documentation

[33mcommit 5bdb8ac1408c71160008d9e40f025202ce9170d3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Oct 7 23:39:51 2019 -0700

updated documentation

[33mcommit d9edbd300394cf39aea977984e0ab7cbe78923c2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Oct 2 21:19:12 2019 -0700

fixed default value of colors in jikev2 configuration

[33mcommit 7e42dc1b6d53bb40ce0f4c5c6425f54265edb572 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Oct 2 20:28:25 2019 -0700

fixed doxygen issues

[33mcommit ba4e262e82a75fbef36f758417836147472fb9e4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 28 18:17:08 2019 -0700

added cpp files for jpacket, jstream, and jdata

[33mcommit f16003dde826a10a0e128399ff2c6678ce5f3fe4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 25 19:36:52 2019 -0700

fixed logger issue

[33mcommit 60c057f21614d7076f15a233a0849af6b7159578 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 22 20:32:56 2019 -0700

updated mudsums

[33mcommit 92c307f41e6ee0fa8f98790005bc2aaee4c9e665 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 22 20:28:37 2019 -0700

updated mudsums and README, removed man page generation

[33mcommit 88d46aa3e1937c628ba5a2d4851f5122b9f2e239 [m [33m ([1;36mHEAD [m [33m, [1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 22 19:53:34 2019 -0700

fixed some doxygen issues

[33mcommit a33300312476bb2cdea259d5c5e88ad5ee4c186f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 22 19:17:56 2019 -0700

streamlined interface for jdata and jpacket, added VLAN images for documentation

[33mcommit 61264ac5b52f141e0f337481653842537a8a1b74 [m [33m ([1;31morigin/master [m [33m, [1;31morigin/HEAD [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 14 08:26:52 2019 -0700

added VLAN tagging to macsec, support of two tags and CVLAN, SVLAN, and IVLAN tags

[33mcommit c4b6b6bef83b7792bb023a9f7943062d2281ddeb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Sep 14 07:06:55 2019 -0700

fixed missing return values

[33mcommit 88b552aa9f7a460b2ba032020a1afe1b256ba2e6 [m [33m ([1;32mikerecode [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Sep 13 17:12:18 2019 -0700

added specs

[33mcommit 7f5dfda1e41716f1673e6a25232d6292260fda4f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 5 21:14:46 2019 -0700

fixed GMAC/CMAC in WIFI when in decap

[33mcommit 84e64826f2ba3734f374e4b2effbb70951760104 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 5 19:53:29 2019 -0700

fixed some missing items in status to string converter for printing

[33mcommit 715760fadf0b4eb77e3a9bec1322a4c751d3f05b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Sep 5 19:45:23 2019 -0700

fixed randomizer issue when using WIFI

[33mcommit 3957ac8579f789b2d22cd5df2d7d455b5320bbb8 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Sep 4 00:46:13 2019 -0700

added GIB mode to wifi, randomized ciphers, authentication, fixed a bug

[33mcommit de39de70db62325eeb3e3f215fc6a7fd38841f6e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Sep 1 22:27:42 2019 -0700

addes AES-GCM support to Wifi, fixed it's Nonce generation, added AES-GCM documentation to jwifi and jwifisa

[33mcommit 59be7e6ae0241f9534ef0d56b64f4e6b8030a744 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 28 22:06:44 2019 -0700

added WIFI PRF test vectors to unit test, debugged WIFI PRF function

[33mcommit 81627e70b5ff44dc653293739d2ffc2ae763d586 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Aug 28 20:53:23 2019 -0700

updated label length for kdf in jwifi

[33mcommit 96e1c67ce3bf90612313fdb9e962b025d96353d4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Aug 27 23:54:29 2019 -0700

added ability to add logging colors in jikev2 per configuration, fixed PRF and KDF in JWIFI according to the spec

[33mcommit c4bb2b388d14289c6c44810e63b77b5d278d2daf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 24 16:16:37 2019 -0700

added ability to change colors in jlogger

[33mcommit 2e39d7efd442b9c75a9e6e88139ce4b8ecabed5c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Aug 10 23:55:53 2019 -0700

update

[33mcommit 07e23a6ccd8aef817b9cfbccfeff09b155675c1e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jul 27 08:42:04 2019 -0700

updates for wasp coverage

[33mcommit 22879433b307c91d7c88d27d2d24893c8c2f1a7c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Jul 25 20:50:19 2019 -0700

improved coverage in jreplay

[33mcommit 07273d5dda1853cff233c8b1882ef3a965daa1d2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 21 23:20:36 2019 -0700

fixed parser issues in jikeparse

[33mcommit b141960484fffe4d6891f68f77cef76532ffc147 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jun 21 22:50:59 2019 -0700

recoding IKEv2 to handle multiple policies

[33mcommit efc4333e847a6e90d7667d00505acc877648a71f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri May 31 01:08:26 2019 -0700

added cpp for SAs

[33mcommit 1402318464550eee1edda19484d5131cefdcca9f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri May 31 01:06:08 2019 -0700

fixed make file

[33mcommit 7a08adae4a0f0605aa5764539cb651bd5e68e49f [m [33m ([1;33mtag: release-3.0.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 30 12:32:26 2019 -0700

Moved to Crypto++ 8.2.0 final version and fixed missing call to SA base class in four classes

[33mcommit 6cc4ec6b832dc347399228865bad6c7b2566cfe5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 30 12:27:02 2019 -0700

Moved to Crypto++ 8.2.0 final version and fixed missing call to SA base class in four classes

[33mcommit de1479993f76233ada7e611fc4e5f84d8dfa95ad [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 28 10:52:54 2019 -0700

fixed time reporting in the testbench to report correctly across multiple days

[33mcommit 7977e061a2f6fe23cf0c09ca4733919de39ca327 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue May 28 10:51:46 2019 -0700

fixed time reporting in the testbench to report correctly across multiple days

[33mcommit f0685462e4974ead442d4a0e2f852e865be628f3 [m [33m ([1;36mHEAD [m [33m, [1;33mtag: release-3.0.0 [m [33m, [1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 4 16:11:37 2019 -0700

added switch for ETH_P_IP

[33mcommit 38792f6d94ac0f545967be31365aa1a8a0fd24e1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 4 08:45:02 2019 -0700

updated drivers to handle routing headers and ICMP messages

[33mcommit 1d76eb841455f68e815fde6b99f1f0fb04a771fd [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 4 08:31:41 2019 -0700

updated drivers to look for destination on local network first

[33mcommit e789133abd401398acebeb16b5cd9d7253bf3dd7 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 4 08:29:58 2019 -0700

updated drivers to look for destination on local network first

[33mcommit f4bad1def826eb8b16baf64786f528fd2db2aca9 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat May 4 08:28:11 2019 -0700

updated drivers to look for destination on local network first

[33mcommit 481f97e7bb94e286da8bca91d3011fec689c474b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu May 2 22:42:29 2019 -0700

added licensing to executables

[33mcommit e4f8d15c430985fe032f769c861186531b3258af [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 30 17:03:46 2019 -0700

Updated Makefile to fix Latex for overlapping objects

[33mcommit 8d91f3ed1f8c2fdcbb608a3a4db4c188f99518f4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 30 14:25:38 2019 -0700

fixed time logging to be cross-platform

[33mcommit 77dc31f549bb8b6432c70db980a035be734a94ff [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Tue Apr 30 13:44:17 2019 -0700

fixed simulation time to be cross-platform compatible

[33mcommit ce3babd039d653f7a70529b773bda89eed42b1ab [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 28 15:54:23 2019 -0700

fixed ICMP regeneration

[33mcommit 2261ad6df017add3ffd713e4bf023920482035ef [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Apr 28 15:37:32 2019 -0700

fixed ICMP regeneration

[33mcommit e5e75702439e2faa0319827c6480abc64f217108 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 24 20:59:57 2019 -0700

removed get_prf and get_skseed() from ipsec now using jikeprf, added new parameters to Macsec (enreceive, entransmit, inuse, protectframes), documentation updates

[33mcommit 5f26ff83e87e1b0ba92363e2c325518413ef185c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 24 20:23:25 2019 -0700

removed get_prf and get_skseed() from ipsec now using jikeprf, added new parameters to Macsec (enreceive, entransmit, inuse, protectframes), documentation updates

[33mcommit 0cfcd06af6ff865ef49277e0b22b8a8876a82d95 [m

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 24 17:49:34 2019 -0700

    removed get_prf and get_skseed() from ipsec now using jikeprf, added new parameters to Macsec (enreceive, entransmit, inuse, protectframes), documentation updates

  [33mcommit 1405d62c4c1e6e8e1e4bc8b99970031732449761 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Apr 24 15:39:43 2019 -0700

    bumped version, removed get_prf and get_skseed() from ipsec now using jikeprf, added new parameters to Macsec (enreceive, entransmit, inuse, protectframes), documentation updates

  [33mcommit 97206a685d53cd826f27e30d51091e6efe604e2b [m [33m ([1;33mtag: release-2.5.6 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Mar 23 19:45:33 2019 -0700

    fixed memory leak in IKEv2

  [33mcommit e8d81e9b736175b464e9c6d1ba2daeabcfac738f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 21 23:28:15 2019 -0700

    updated coverage

  [33mcommit 4885685fce6d66ff8e1ef6b341e1b2eb2a480174 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Mar 21 18:52:09 2019 -0700

    Updated Makefile

  [33mcommit ef3d32dd953f82c79f700f652ad1b6c8065a1ace [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 20 23:38:29 2019 -0700

    added images for IKEv2 payload formats

  [33mcommit 4dba44a27130780d37aee8b1ae1dc1d2b07f0fa3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Mar 20 23:33:38 2019 -0700

    Added conformance vectors for SM4 and POLY1305, coverage updates for corner cases

  [33mcommit efb009765be5c47b1406c28a06f9909a25c94988 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Mar 8 01:27:19 2019 -0700

    fixed retry and a parser bug for IKEv2

  [33mcommit cc8ff03fea96f5ea9c7b3b43c3272038a1cac96e [m [33m ([1;33mtag: release-2.5.5 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Feb 28 22:30:30 2019 -0700

******** Updated README ********

[33mcommit 21c57154a1e87cdaa559f5b05904c7c7afa69cee [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Feb 28 22:27:18 2019 -0700

moved to Crypto++ 8.2.0

[33mcommit 347cda39457d4722e83c1d66a22500a4ee0a2841 [m [33m ([1;31morigin/master [m [33m, [1;31morigin/HEAD [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Feb 16 12:45:33 2019 -0700

updated protocol++ schema

[33mcommit c659bd5871fd09b1a0235e873bc419a9dc84e0b1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Feb 4 23:50:21 2019 -0700

updated to IKEv2, schema, documentation

[33mcommit 4865b8bab6137141ce8abd519bc75f9afe82b37e [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 23 23:39:29 2019 -0700

debugged jdsa, jrsa, and jecdsa, added them to jikev2

[33mcommit 5716eed703e54a6679f0144c531947fa7c27eede [m [33m ([1;32mdev [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 21 21:05:52 2019 -0700

fixed math equations on signature documentation

[33mcommit 9d19fb8646138423f07d7e8b22f9c40b6007f830 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Jan 21 00:24:59 2019 -0700

added ECDSA signature protocol

[33mcommit 4619f8c25d952ee4796c9ba90a1817579f017bd5 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 20 23:12:13 2019 -0700

bumped version, updated copyright, added signature protocols DSA, RSA

[33mcommit e7a5a87e438bc873bc7faf6d7e2ebb1bbf35f306 [m [33m ([1;32mcheckme2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 20 21:30:58 2019 -0700

added signature classes

[33mcommit 286a7ee86760e25da90eac5ee571c399c57114c1 [m [33m ([1;32mcheckme [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 20 02:06:54 2019 -0700

updated with set and get functions

[33mcommit f8337cbc1b1131a21fc58c8af137f266d1cefeaf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 20 01:54:40 2019 -0700

added Diffie-Hellman class

[33mcommit a9614f3c56c1608f304db01169e6817195690fdb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Jan 16 21:58:48 2019 -0700

added configuration for privateinternetaccess, fixed delete vs free issue

[33mcommit e3987e36b1817598df38edd6cf07c6d8b88773f6 [m [33m ([1;33mtag: release-2.5.1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 6 14:05:04 2019 -0700

bumped version

[33mcommit fa881b76c1b1f462d779c377309d1ca4338398ac [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 6 12:45:27 2019 -0700

moved to tinyxml2 v7.0.1

[33mcommit 03c9744b889eb439f4103d05f0f7fd36a7f40ee1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Jan 6 11:55:32 2019 -0700

Moved to Crypto++ 8.0.0

[33mcommit 8e6a47f636c4ce5546f8ddef1891d810e0cfdb6a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sat Jan 5 00:49:49 2019 -0700

fixed auth method in configuration, added notify for features

[33mcommit 955f85c3ff421c8a9bd63104ccecf915c4d8dbcf [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Fri Jan 4 23:50:38 2019 -0700

added support for all the authentication methods that are MUST or SHOULD

[33mcommit 3c9acae8464177da29266e11ee8f3c051e8573a0 [m [33m ([1;33mtag: release-2.5.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 21:31:45 2018 -0700

added documentation

[33mcommit d209d84eaf785f69337c4d9a0fbe9bf43d94fe22 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 21:20:39 2018 -0700

updated README

[33mcommit a955b5991fa15db2c496e8238931e11a4e42a85b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 21:16:29 2018 -0700

bumped version

[33mcommit 112418e5a89717c13481fa396a77c90b7f174a71 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 21:15:03 2018 -0700

fixed documentation

[33mcommit d38285a7eedab1f6b19f0047ffcf1a6b102a35a1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 21:04:20 2018 -0700

removed extra commands

[33mcommit c79589eef4c8f8cc7c3b88098a39200b56cc9fd6 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Mon Dec 31 00:51:24 2018 -0700

split out Diffie-Hellman functions as a separate class, debugged DECAPSULATION, CREATE_CHILD_SA, beginnings of INFORMATIONAL

[33mcommit 0cb530e179137170ba2c3e174b358c16ae0300b4 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 30 20:01:32 2018 -0700

fixed direction issue, separated out DH functions, need to fix DECRYPT

[33mcommit 95149b1fd64ec4f925f799bdff9990a6f10c4789 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Thu Dec 27 23:21:16 2018 -0700

factored out related functions to new classes in IKEv2 to improve modularity and upkeep

[33mcommit d93089137f0cb73ca5af849f0564d48aaa815724 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 26 22:25:33 2018 -0700

added Specifications

[33mcommit 84cbf44c6001cad5e0a04acc9ca2571050ea07c0 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Wed Dec 26 22:24:53 2018 -0700

fixed cryptopp700 installation with missing data files

[33mcommit 54cf3bfa09b02a85fda5a4ebcd844b78afd76c83 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>

Date: Tue Dec 25 00:04:09 2018 -0700

    added Latex images for PDF generation

[33mcommit 8eab332e2f2ee1df82db477b7d3625800627b3f5 [m [33m ([1;33mtag: release-2.4.3 [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 23 21:39:15 2018 -0700

    updated README and release

[33mcommit 817ccd36c76aa335649c5412b16444b474913d2f [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 23 21:35:17 2018 -0700

    updated documentation, bumped version

[33mcommit c3e7ce9072e717dbf057fd9563b494a849239815 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 23 21:28:30 2018 -0700

    updated schema for IKE to include flags in ESP

[33mcommit 07589e2c22342d9d2d9f0dc55cd764215c26ef03 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date: Sun Dec 23 21:06:19 2018 -0700

    fixed issue with RDRAND

[33mcommit 97c1e453ba6c2418b4c85dbb949cbe52d27ef1d1 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 23 11:32:48 2018 -0700

    added separate salts for IKEv2 security association, added conformance vectors, debugged CCM, GCM, CTR in IKEv2 all are working

[33mcommit a9090d2cd2587536c92cec3e64cf33ce54477357 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Dec 18 22:04:28 2018 -0700

    new curves to test

[33mcommit bf4e27336d0eeeec86fa7d141a77b6701cb41e32 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 16 22:53:55 2018 -0700

    debugging of AEAD modes for IKEv2

[33mcommit 842ea9f8cde7b24d50af6f29767b90f1f8768903 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Dec 15 17:13:46 2018 -0700

    added additional attributes to esp_proposal for TFCLEN, DF, DSCP, RANDIV, and ARWINDOW

[33mcommit 6a5300fc746a322f2e6812a8039eb3527c001833 [m

Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Dec 13 23:24:25 2018 -0700

    split DH out into it's own class, added use_tfc for TFC padding support in IKEv2

  [33mcommit bb34caad615073df2ca4e5b35c060f7a060a6b8b [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Dec 12 00:08:34 2018 -0700

    connection established, CHILD SA not created due to traffic proposal

  [33mcommit 61f30983a45a0852c2138d67ad68a9c54d544a03 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Dec 11 00:37:34 2018 -0700

    fixed some bugs in jmodes for HMAC key size, fixed authentication of packet after encryption, added TFCLEN to IKE configuration, debug

  [33mcommit a272bc9d6156e39cd53a66ffbde9634d3f26a450 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 9 11:59:41 2018 -0700

    working IKEv2 with AES-CBC_SHA256_MODP1024

  [33mcommit 58180af60293cce62dcbcc88613c3333ad2d60ad [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 2 20:43:36 2018 -0700

    added more iterations to IPSEC

  [33mcommit b62bd7ad6d88984411a7bd05070ce3197ec82b40 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 2 20:30:36 2018 -0700

    fixed CHACHA20

  [33mcommit 8d7081d9cf529e03ee3d121b5f10d4838990e15e [m [33m ([1;33mtag: release-2.4.1 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 2 17:58:22 2018 -0700

    bumped version

  [33mcommit 305e7ae0531ca5e6799fc9c3a09d6a04245c40c6 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 2 17:57:09 2018 -0700

    added mudsums

  [33mcommit 2662d1673e8b5479a9688af14dea1b78e70e1daf [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 2 17:55:07 2018 -0700

    updated

[33mcommit 9ada87950ef5c48528c2abb313cc46c9a3e25dde [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Nov 27 19:25:53 2018 -0700

updated to lookup security association from key ring

[33mcommit e4bb338eb00f32c0fb3dd4a5adf23615c8b5253b [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Nov 27 19:20:32 2018 -0700

updated ring driver to include key ring in appropriate places

[33mcommit 943aee3fc4a34e0a1d676f712e75ac3435a7ac52 [m [33m ([1;33mtag: release-2.4.0 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Nov 26 22:13:39 2018 -0700

fixed key ring issues

[33mcommit 4872910ba73566f1b37e3201bfee0b5e05cb98c3 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Nov 25 03:47:18 2018 -0700

updated to add back in the randomizer and keyring, kernel seems to be lagging

[33mcommit 98d4f8e5dc1de3f6c78993bad55dd02b8bec9051 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 23:41:08 2018 -0700

removed windows EFS files

[33mcommit ed56e51356d4c16ae303ae637ed432feb6d4312a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 23:37:02 2018 -0700

added logo with copyright and trademark

[33mcommit 7b833dd09ee33d8c7f36c477360a21549e3818fc [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 23:00:59 2018 -0700

updated release notes

[33mcommit c1fb4fb0c520c786d855c283fedfc2566b8250ec [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 22:55:59 2018 -0700

updated documentation

[33mcommit 6072a0086751253b5a44c061bd519926cb2f79db [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 22:33:28 2018 -0700

Fixed keymat generation, added missing Nonce for AUTH payload, fixed shared secret for AUTH payload, updated

logging for levels

[33mcommit 4e276af3966aadb9d4ba3298660426ff7f230607 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 15:51:25 2018 -0700

added support for parsing all payloads found in RFC7296

[33mcommit 4b8d96597057013baeed56c54ba97571094dddfb [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Nov 23 12:56:22 2018 -0700

added support for parsing all payloads found in RFC7296

[33mcommit 05a98e64db50ccc5dada3022f51ce86cc67e4792 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Nov 18 13:10:12 2018 -0700

cleaned up some code

[33mcommit e2034bef77c5cc15c3c2a4bb384421afd507d275 [m [33m ([1;33mtag:
Nov_18_2018_JPGNetworks [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Nov 18 00:29:34 2018 -0700

fixed a major bug, debugged packet parser in IKE to be more robust (still need a couple payload types)

[33mcommit ffe1851122718ba8ebc5756c1cbc1544c25d9e1c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Nov 13 23:57:41 2018 -0700

added the logger, fixed missing IV in encrypted packet, ICV is failing on remote (using strongswan on remote)

[33mcommit 9567ce88c074eb4421dfb4183214c731eca91c91 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Nov 13 00:11:25 2018 -0700

fixed typos, fixed parsing errors for protected subnets, fixed authentication when key is larger that auth key size, encrypting

[33mcommit fcdf4cd97493bdd97742739ccd979dff37d3b347 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Nov 11 22:19:16 2018 -0700

IKE SA negotiated and created

[33mcommit 13fbd6244e8253a1e450fcb48928e007c5336af5 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Nov 11 03:48:38 2018 -0700

removed unused receive socket

[33mcommit 283e19baac9e606629a250ad4adbcdcdf3b8ed11 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>

Date: Sun Nov 11 03:47:00 2018 -0700

    parsed first received security association

  [33mcommit dea79c299c00eea101444645d87fc3fdfd075e55 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Nov 5 22:42:11 2018 -0700

    fixed some indentation issues with the XML output, fixed CAMELLIA key size bug after move to CrytpoPP 7.0

  [33mcommit 82b090351d856671df75b62926907fbf636913f8 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Nov 1 23:24:38 2018 -0700

    debugging of syntax issue in IKEv2

  [33mcommit b4ced068487656d38fa6d5e3ffaac34225edd46a [m [33m ([1;33mtag: release-2.3.3 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 30 19:02:06 2018 -0700

    moved to CryptoPP 7.0 and std::thread, documentation updates

  [33mcommit 2304e7bedb95883e277cb52a4d87231011b26bea [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 30 02:44:28 2018 -0700

    updates

  [33mcommit 2c5c3b690d531613cf15a61eb2143fbac747002a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 28 20:41:06 2018 -0700

    updates for IKEv2

  [33mcommit be025ba40c0a7946da2857ccabb9cdd20aa1c08e [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 28 00:51:34 2018 -0700

    updated DH groups parameters

  [33mcommit 1034cffe2157401274784601696c3881c80178e8 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Oct 25 23:25:23 2018 -0700

    added CAMELLIA to IPsec, IKE functioning up to initial packet send, packets look good

  [33mcommit fbeb22a2f946618877316e9d9f1ee91741e74ec3 [m [33m ([1;33mtag: release-2.3.2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 21 19:02:35 2018 -0700

    added new images

  [33mcommit cb8521ee53f02ae30946970af254cb3cce3c0dcc [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>

Date: Sun Oct 21 19:01:13 2018 -0700

    fix for key sizes

[33mcommit c63ada7f6d25c55df174a82e8e6f594db5649b7e   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 21 00:19:23 2018 -0700

    fixed some compile issues

[33mcommit bb8e0a59f2c31ab065d4ef90cd71c426b10bf4c5   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Oct 20 21:14:09 2018 -0700

    removed duplicate function

[33mcommit ac6f403657fdb8ceb9aaee0785a949ec06eef2cc   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Oct 20 02:37:23 2018 -0700

    updated with key management

[33mcommit c90f52f9e95d18310280a969c1eee3bb1833f173   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Oct 19 00:50:21 2018 -0700

    updated version

[33mcommit e48e20b8afd566df9482cdc4bb82253e6c1620ec   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Oct 19 00:28:22 2018 -0700

    updated release notes

[33mcommit 4f9b5f3d3e0090f9bd99b8ed75206425cf0f5622   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Oct 19 00:23:38 2018 -0700

    compiled IKEv2 with support for all ENCR ciphers (including AEAD) and DH curves, updated documentation, support for multiple connections

[33mcommit 0cede5355241b0388bbb867e881540eeec3a726c   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Oct 18 21:26:15 2018 -0700

    updated

[33mcommit 339d0721914a062e310442892ad4a7167b2c07f6   [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 16 23:58:03 2018 -0700

    docs update

[33mcommit ec76b83117d1f2ad955f166f757216d1cb6fa15d   [m

Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 16 23:56:57 2018 -0700

    debug

[33mcommit 2f6d481605d7ad3ea5deb51735f77c85649b33b9 [m [33m ([1;33mtag: ike_update2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 16 01:02:07 2018 -0700

    debug

[33mcommit cbcfbf18f694b634023c129b2d04bac2c58f5143 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 14 23:13:52 2018 -0700

    updates

[33mcommit d0baf5f4071e00ece30f85253e6cce5679eb911b [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 14 21:10:11 2018 -0700

    update

[33mcommit 4055b5527e14e00e207146d8058625fe27b41cbb [m [33m ([1;33mtag: ike_update [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Oct 13 22:53:33 2018 -0700

    updated

[33mcommit e6ff231ff157857220d8053ae05bc3459fcd7fd4 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Oct 11 23:47:00 2018 -0700

    updated

[33mcommit 49740f71116d8708f835b148ee879d037bc6bbf2 [m [33m ([1;33mtag: release-
2.3.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 7 17:59:27 2018 -0700

    update

[33mcommit 2e97862e00d434c6a60fec7198907911c234cf0d [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Oct 7 17:52:24 2018 -0700

    update

[33mcommit 1c5764be90377a400a172cb3102413f0f60900c0 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 2 22:22:30 2018 -0700

    updated

[33mcommit a2245411269fd3cba84f7e070e51982c142654f9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Oct 2 22:19:37 2018 -0700

updated

[33mcommit bcf7bb337233f04ce95c215049bf119991bab419 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Oct 1 22:49:11 2018 -0700

update

[33mcommit 5e671151f011c171af373445e518bd3e0bf46e35 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 30 22:45:59 2018 -0700

update

[33mcommit 0e61c7235f281f6e1d8259307da3468fe65c026e [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Sep 29 21:23:17 2018 -0700

IKE configuration parser compiling

[33mcommit 2b7ef2f173b521dd7a00768c0e65ccc3a807f6b9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 28 22:27:20 2018 -0700

update

[33mcommit f3d991e63f441bb25b9f930fe5ddc1926ee18fab [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 28 20:56:52 2018 -0700

updated DH parameters with all RFC values but group 31 and 32

[33mcommit 353288fdfaed771780a4eed526faf620ac77123b [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Sep 26 23:36:28 2018 -0700

work to parse parameter files

[33mcommit e8982fe86417e3981c136392ccde26af3042b047 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Sep 26 01:31:01 2018 -0700

fixes to accept broadcast and reject packets not for this interface

[33mcommit 41a8d2b01bfe42ba811d9d9bf2ff1ca2b19b51da [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 23 23:56:24 2018 -0700

fixed gateway lookup of HWADDR

[33mcommit 648f77c16c9edacebc4e6347ad342f94a3b577b6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 23 20:22:54 2018 -0700

updated to included ETHERNET (no MACSEC)

[33mcommit 0d5c1283f63be7cbaf8be74b534b8f90bb038e5c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 23 19:52:30 2018 -0700

cleanup

[33mcommit 8bfadc4205646c040856c8f074825c317134cf6d [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 23 19:40:47 2018 -0700

removed old documentation

[33mcommit 2cdf0f0c524a807bfd6a5bab89e8cab10498ca12 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 23 19:39:18 2018 -0700

updates to discard ethernet packets what are not for the HWADDR

[33mcommit 4954e2f9a4252395d779f28d2819a48c447646c9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 21 00:05:53 2018 -0700

parser for ikev2 configuration files

[33mcommit 705b0f07cfb64227f0165c22ca3636a1e60b23d1 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Sep 18 21:49:20 2018 -0700

fixed memory leak in resend queue of the ring and direct driver

[33mcommit 1b174780e80512057b6e572e6e96ca1113e702f3 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Sep 17 22:33:06 2018 -0700

updated drivers to lookup local gateway and additions to jikev2 to computer public keys and verify shared secrets

[33mcommit b52f552ff53575e8a10a3fd66300d4109cce5b84 [m [33m ([1;33mtag: release-2.2.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 14 22:36:21 2018 -0700

updated release notes for release-2.2.0

[33mcommit 38013a79107d768d9e9d03cda494cc8527cbdca6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 14 22:21:23 2018 -0700

working and valgrind clean ddriver

[33mcommit 82d177e20916628d1de2a99af26e22b3427836c3 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Sep 13 22:23:58 2018 -0700

updated to debug direct driver

[33mcommit 4058fa85c1ed0f2c398f1506ad20029cb520e735 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Sep 13 00:21:40 2018 -0700

updated documenation for interface change to ipsec

[33mcommit 7eb094d821d14bdc9780e6a10c55a89d6a394634 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Sep 14 22:26:34 2018 -0700

updated README

[33mcommit 76aff43c786afaf4efcc6d01d508617377df22a7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Sep 13 00:15:08 2018 -0700

leak free ring driver, additional IKEv2 work

[33mcommit 83e4acd907bd204157de4b40972d6e0e7d74162f [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Sep 8 20:17:25 2018 -0700

fixed tabs with spaces

[33mcommit 85fab2f17205715dd4bd7708033eb65478aba7a3 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Sep 8 19:55:59 2018 -0700

separated SKEYSEED and key material generation in jipsec see documentation, although this is normally done in IKE

[33mcommit aca2133d138b334ffb0c41a3146e79440389387d [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Sep 8 06:14:33 2018 -0700

updates for IKEv2 implementation

[33mcommit d6596012c6f42225053d461294475eae4a526b45 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Sep 4 23:32:32 2018 -0700

added some work for generating IKEv2 requests

[33mcommit bf6399d6f370079ab7f2a3f9a491ee12fbf52205 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Sep 3 19:43:33 2018 -0700

updated documentation

[33mcommit 575ef6e85dc7825664c4658bf7667d20655f6454 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Sep 2 20:54:09 2018 -0700

added enums for IKEv2, cleaned up ringdriver, added code to lookup IP addresses and gateway MAC

[33mcommit a592c631d9b270da2f5a80ab2cc0d155d4b1c22e [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Aug 31 22:56:49 2018 -0700

removed old documentation

[33mcommit 29b9ee02a69d159ac604c73201ba3e0156860e39 [m [33m ([1;33mtag: release-2.1.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Aug 31 22:38:31 2018 -0700

updated for release-2.1.0

[33mcommit 9336a3c8c977f683a6200de4ee1bd7a89b7a06b7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Aug 30 21:23:58 2018 -0700

fixed memory leaks in rdriver and jlogger

[33mcommit f8b0e872ef641cb419163f116fea746edfc8570e [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Aug 28 23:09:19 2018 -0700

fixes to allow passing both IP address and domain names for destination

[33mcommit 93b2c55bedbb375d543d0b53f7d676b996d9a687 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 26 22:18:29 2018 -0700

debug of directdrive

[33mcommit 6cbef5fe6d34ef61b88fccc62169f0a2ac02f4f6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Aug 22 23:41:59 2018 -0700

updated ringdriver to allow receive to catch up with send

[33mcommit d9d98660f6ef10e7804251c7fcf8571424b359b6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 19 12:47:45 2018 -0700

updated with ability to change logging level from the command line in drivers and executables

[33mcommit 444ebecb25d7a9e9d1187a0088a2959ca1525195 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 19 09:56:19 2018 -0700

reduced logging, added new file_policy, added switches to print to std::cout

[33mcommit 6a2435f4ddfece5b4cd178e127f14f022457d283 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Aug 15 22:55:06 2018 -0700

working direct driver

[33mcommit 132a69b568e1ef96abf5cc98d124ce4deb639289 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 12 21:29:38 2018 -0700

updated README and release notes

[33mcommit 39b389240befc19378e5636bba8b926eea4f4046 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 12 21:18:00 2018 -0700

removed lcov reports

[33mcommit 8387ae3f045ee76a5a476239438b6f95fab92b8d [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 12 21:17:06 2018 -0700

updates for directdriver

[33mcommit 7b94edeb02b6ba0333097aa26828cfa986e75102 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 12 18:48:55 2018 -0700

updated documentation

[33mcommit 4bc46447c0ad3d979e2b36647e0f6ee23dffa727 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Aug 12 18:46:06 2018 -0700

bug fixes for the ring, testbench and responder

[33mcommit 18ab100f89f48b3d9387940326e4f966a24157c9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Aug 11 01:05:21 2018 -0700

updated status values

[33mcommit 4427ae799349c0315f68a3fabcae06e800f5e377 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Aug 11 00:30:00 2018 -0700

working UDP packets in ring driver for both send and receive

[33mcommit 7bb43be465cc1dce3144b062b763071307e00871 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jul 29 23:50:23 2018 -0700

added checking for socket, send error still

[33mcommit 175f7d5881dae64d961d2122f40539bee8f6e850 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jul 29 15:28:39 2018 -0700

working send, debugging receive

[33mcommit 5e9c23e07fe0d6fc00fdc070a444a7da8845d102 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Jul 28 23:12:54 2018 -0700

updates for ring driver, able to open socket with loopback address

[33mcommit a71e6cda7dd4165a7d0f17d5130885be0afabfdd [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Jul 27 22:13:36 2018 -0700

added new copyright for version 2.0.0

[33mcommit 189a59c8a930910beee64420bf70b259a8bbb0f0 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jul 22 23:17:23 2018 -0700

updated coverage

[33mcommit 8c2a4457b45c3af3bb47f902fdde52a5c5527967 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Jul 18 18:04:43 2018 -0700

compiled directdriver

[33mcommit df22d741c7db5187bd0edb499177a277d904a1fd [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jul 17 21:40:39 2018 -0700

directdrive driver

[33mcommit 751b93bf6478ff880f6b7e0dd45d45420d951be2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jul 17 19:01:51 2018 -0700

updated ring driver

[33mcommit 3371b408919f562d65501c72750d61d9b0b1abf7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jul 17 19:01:19 2018 -0700

updated ring driver

[33mcommit a489c6e1d947e1bb35ce59c0dc32468312d902b0 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jul 8 13:31:51 2018 -0700

documentation updates

[33mcommit bf527a33ef3dd04eda94c5c9db433a9117139e8c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Jul 7 16:32:28 2018 -0700

updated documentation

[33mcommit 8ba6e1ff9d0cdd78853969d78dc0e977fae054ba [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Jun 15 23:46:45 2018 -0700

added documentation for using template interface for new security associations, debugging new driver

[33mcommit 153b676ad915ade170b1608a8889b743c2cf9e12 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Jun 2 22:59:09 2018 -0700

updated documentation

[33mcommit b27b05ba396de3f4c8388c67ceda3efc4b4652f1 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Jun 2 22:58:16 2018 -0700

updated documentation

[33mcommit 42907612fd035b99011f68490ce7e635afef3938 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon May 28 23:52:42 2018 -0700

fixed last valgrind issue with buffer overrun

[33mcommit 51e0a3a22699b05e8eda07e65d87cc556a801c3b [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon May 28 23:48:04 2018 -0700

fixes for buffer overrun, last valgrind error in testbench

[33mcommit 33096a6945b7a6177d96ec4ae32c6f82b5c80c86 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat May 26 23:06:58 2018 -0700

updated with new libraries for release-2.1.0

[33mcommit c6120115301482e1e8ddd42691988a115bd7d9a0 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 25 00:04:10 2018 -0700

fixed missing returns in get_field

[33mcommit 6cbb42601ea961e43ce66fc5d97f6061282f77c2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon May 21 22:05:43 2018 -0700

update mudsums

[33mcommit 7767b17111359692bb85121e9c29befbc08e9d0a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon May 21 21:42:42 2018 -0700

added elapsed time for simulation, removed testbench memory leaks

[33mcommit 4718784fcf038975535813bfeea7d349b13c188a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 18 07:37:20 2018 -0700

updated README and mudsums

[33mcommit 76b1df9b1cb545ec44fde33d994409ee4d8ac925 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 18 07:33:27 2018 -0700

updated with tinyxml2 v6.2.0, documentation updates

[33mcommit aeaa9398e78443138adb1d066955fc31a6a3facf [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 18 00:06:25 2018 -0700

updated documentation to include DriverPP

[33mcommit b663effa478e6c3bd7ddc3f9a8577210e2bc76ac [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 18 00:01:09 2018 -0700

updated documentation for tinyxml2 v6.2.0

[33mcommit 1d9adbbf7e536168f2baaa5c86dfb24a533c58c6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu May 17 23:56:15 2018 -0700

updated to tinyxml2 v6.2.0

[33mcommit 855675af778fb3aca320e64c0b839d9183c49508 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu May 17 21:27:04 2018 -0700

fixed some documentation issues and added back CAAM/SEC support

[33mcommit 877569e4a49a3882c70c16cd5633b9d65c8842e8 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu May 17 21:26:37 2018 -0700

fixed some documentation issues and added back CAAM/SEC support

[33mcommit 7288e37d7ae8b7fe4168d261fe990580dd50f130 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue May 15 01:46:16 2018 -0700

updated mudsums

[33mcommit e5e43afa7478b3a81c14cd750d244fa62cbfb2ca [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue May 15 01:41:28 2018 -0700

rebuild for release-2.0.0

[33mcommit 670c6e9f71846dee821e320008567b0df585d9e9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue May 15 01:16:29 2018 -0700

fixed post-processing for TLS and IPSEC

[33mcommit 5bdce7a40050e7149fda932d26195a4c1755fb63 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue May 8 03:05:41 2018 -0700

updated tests

[33mcommit 2fddbc31bbaed86b8fcb310ba7ecfc78b8adde30 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun May 6 23:59:05 2018 -0700

updated mudsums

[33mcommit fee9e9dae6dcfe071368b54cde5b94bba720817c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun May 6 23:56:09 2018 -0700

fixed a type made while converting to new security associations

[33mcommit d3651ce11ab04c89465ec0e0f530946818496395 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun May 6 23:26:40 2018 -0700

fixed typos introduced by conversion to new security associations

[33mcommit c1fc519089430643696b11fe764c8ab0edde5a91 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 4 01:11:29 2018 -0700

updated mudsums

[33mcommit 57a8057db34ee0e4bff3b7c286741e946f09fd70 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 4 01:08:43 2018 -0700

updated README

[33mcommit 6bcbb76ce72671d64d31fd8ae6fcfff5c11fcce7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri May 4 01:07:15 2018 -0700

debug and documentation updates for new security associations

[33mcommit 70ceea5be87012873a2079450ee262dc3ec19714 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed May 2 21:30:18 2018 -0700

updates for new security associations

[33mcommit b5d79c64b79d45b3c644f7364092be060d898e7c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Apr 30 23:16:09 2018 -0700

fixed some documentation and added back more cppunit tests

[33mcommit 4857dfd960c6b29318e0ac040e15527557e7c360 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 29 23:42:56 2018 -0700

debug of new secass classes

[33mcommit f94a6d6764f61847e10cb8248115dd3726b44a29 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Apr 26 07:20:44 2018 -0700

continued debug

[33mcommit 17ed52111363304fe98600870760d123fad0acf4 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Apr 25 23:43:43 2018 -0700

debug of classes for jsecass while updating cppuint test

[33mcommit a6f218ca7d2cdc5fc20b6dee746a0aac04c0e698 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Apr 23 23:01:15 2018 -0700

continuing conversion

[33mcommit 63edfa0745c267f800e8e7e53ade834a05d907c4 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 22 19:07:50 2018 -0700

debug for new secass borecleaner tests

[33mcommit 08b4c67659732b65b68f36bbb23958b2e32779e5 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 22 02:03:53 2018 -0700

updated documentation

[33mcommit ece0ed16becdc370e1ddb0c7627854bd3776c10f [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 22 02:03:24 2018 -0700

debugging with new secass classes

[33mcommit 65850664fd3bbe04b42636776d1b2cb3da24cba4 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Apr 20 00:30:41 2018 -0700

debugged except for last lines of wasp

[33mcommit 1fa57de8662db39472c73d509572f63faa0d9147 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Apr 17 22:40:54 2018 -0700

fixes for documentation generation

[33mcommit 3366d984a28b84c2c054a24b95b01f632a379854 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Apr 17 22:06:11 2018 -0700

finished converting to jsecass

[33mcommit 2eabc966bf92622bdc54a437002cbb1e358673e3 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Apr 16 23:08:05 2018 -0700

updated with TLS secass

[33mcommit dc58c473656de6b7c79ee41968e50d4a6cf78d7c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 15 22:24:05 2018 -0700

updates for new jsecass and namespace

[33mcommit 0a86b434922312fb27c97880fb42e5b8547f7e24 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Apr 11 23:04:25 2018 -0700

done converting jwifi

[33mcommit ff0f86f52c4c1f873e57d250d7a30c1a47104b32 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 8 23:35:43 2018 -0700

finished recoding WASP, updating SRTP

[33mcommit 37e8cef8d64ac6d014ad2556eef615c5df189640 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Apr 7 23:44:18 2018 -0700

update to wasp.cpp for non-leaky security associations

[33mcommit f233697da56d1a948222662bad74b64b5ea93672 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Apr 4 22:44:16 2018 -0700

updated responder for new secass

[33mcommit 167083e119b6ecfcc69783f345d61a25a59785d6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Apr 1 22:12:25 2018 -0700

finished converting JLTE

[33mcommit 5702779af68e76f63d5ec5e42c26143c58014580 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 31 20:10:19 2018 -0700

more work on memory leaks

[33mcommit 55f79d5145b2452d381f9521579005800d7361ff [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Mar 26 00:32:10 2018 -0700

more work on removing memory leaks

[33mcommit 371946302ae0a384a36620b6710114ee23215df2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Mar 22 21:14:04 2018 -0700

added jipsecsa

[33mcommit f4f87f331188fe3b7e02df5d6c7fd4bf979c88cb [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Mar 20 23:36:45 2018 -0700

updated jip with jipsa class and functions

[33mcommit ed2fa932f61d8d90a875d72782b056bd299f00bf [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Mar 20 23:36:21 2018 -0700

updated jip with jipsa class and functions

[33mcommit 2a4ac7346644caca31a068ff420b79e4d063fde2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Mar 20 00:13:54 2018 -0700

updates secass

[33mcommit 4b9c4f57f7a9d65572d10129921101fe1c34f60c[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Mar 18 22:08:53 2018 -0700

adding new security association

[33mcommit d888d7466a961111766cc19f59b4872460f4e9c3[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Mar 18 19:00:38 2018 -0700

helper functions for new security association class

[33mcommit 2442066add3244f4e64f62fd964dc1fd2fb725c8[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Mar 18 18:48:18 2018 -0700

new base class

[33mcommit 96682f70463fc2e7ff1875c76e55762289d2971c[m[33m ([1;33mtag: release-1.5.0[m[33m)[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 31 20:57:46 2018 -0700

update for Windows compile

[33mcommit 7f7dda91b7b7751d3ebf564449c06d591aa89b0f[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 31 20:41:13 2018 -0700

fixed headers for Windows compile

[33mcommit 8bd560ab8977f5c765beb9225581fc6d3dc289ec[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Mar 22 22:34:05 2018 -0700

fix for new image

[33mcommit b45212ea1e7b0111a57b3e04ca7a982f5dad3aa2[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Mar 22 21:41:13 2018 -0700

updated documentation

[33mcommit 60bd60d2f8600c5c80ca179946cd970cef773b59[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Mar 22 21:39:01 2018 -0700

fixed version in Doxygen

[33mcommit a4f834dca7fd35e7b72e32501e6fda5bd08f5033[m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Mar 22 21:37:16 2018 -0700

updated release 1.5.0

[33mcommit ae40243232a6cabd67e60fd4890e293d953f644b [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Mar 18 18:00:28 2018 -0700

added back config.h

[33mcommit a5be703d83e42662d1118c1b7965da98b3f71478 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Mar 18 17:58:28 2018 -0700

updated version

[33mcommit 1ab1e9fb801c6a23957ec925984ba78c6be6b68f [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 17 18:30:10 2018 -0700

working namespaces ProtocolPP, InterfacePP, DriverPP, PlatformPP

[33mcommit a828717ce5cf3fb6b59fcf64a7956baba8e54802 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 17 18:26:28 2018 -0700

working namespaces ProtocolPP, InterfacePP, DriverPP

[33mcommit 0bbe06792400a834201bccdf5f6070f124e5f1a0 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Mar 16 00:27:46 2018 -0700

namespace debug

[33mcommit 4b3f46d132951025a70ee1696ce69e553e1e3d2a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Mar 14 23:39:36 2018 -0700

namespace work, library compiles, test and jbuilder do not

[33mcommit 6aff2a15ace78a04fb03d00da3b7c61c8c9cada6 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Mar 14 19:22:13 2018 -0700

namespace file

[33mcommit 54a75d0b2dbaf129457993438e9a25dbd6ce1b7e [m [33m ([1;33mtag: release-1.4.2 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Mar 14 19:18:10 2018 -0700

removed

[33mcommit 5c0b244693036c2b1ac6c33803e44d1de5408093 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 3 06:49:14 2018 -0700

updated mudsums

[33mcommit 47a7fb04c4ccb73af6d714e6bf3d56cb6079cadf [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 3 06:46:49 2018 -0700

updated examples

[33mcommit c9eeeed9a470fb76947306dbffb828e69ee1fa12 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 3 06:39:46 2018 -0700

updated with static libgcc and libstdc++ builds

[33mcommit e65c79ccd55fcfa0cadb295dadbece22622383b2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 3 06:23:02 2018 -0700

updated with static-link of libgcc and libstdc++

[33mcommit 8bcaec1233c35b2e53048e97e8741e2218ab9929 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Mar 3 06:22:02 2018 -0700

updated with static-link of libgcc and libstdc++

[33mcommit a40782909fd421fd69ce906be39a26811d19a663 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Mar 2 23:29:51 2018 -0700

compiled with static libc and libc++

[33mcommit 57186d34a266698e365e3dbdbcde5150d5165cef [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Feb 17 19:13:55 2018 -0700

added missing images

[33mcommit 124ae7fed0a7b000461c56289955b4377f3b010f [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Feb 17 19:07:05 2018 -0700

update driver and documentation

[33mcommit f7df8d8b8bcf91b6da790c138125c1e209a65948 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Feb 12 23:45:00 2018 -0700

recompile for cryptopp565

[33mcommit b15f65353bce20cfdf9f3628178d93be8604e2a5 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Feb 9 20:17:28 2018 -0700

Crypto++ 5.6.5

[33mcommit 16e59922b2103d8d07f5c97faf38ceedad8a668a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Feb 7 19:40:12 2018 -0700

fixed issue in aria where variable names were masking each other

[33mcommit 5c173e6f78040b9230c13d5028e88a73f4f7b685 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Feb 4 22:53:12 2018 -0700

changed version

[33mcommit 2f7e06ed4837f814a0ba054813c40c8855730450 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Feb 4 21:47:10 2018 -0700

release update

[33mcommit e3db8ec071f6ed9e1b7867e4473d8e669de62c62 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Feb 4 21:34:25 2018 -0700

added library paths for different distros

[33mcommit b67afb2970df48d44985a0c24dc0ca9c9a78087a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Feb 3 22:37:20 2018 -0700

update

[33mcommit ff01176be45d0a2ea6dc7c267e41fba7846921f7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Feb 3 22:33:39 2018 -0700

moved to Crypto++ 6.0

[33mcommit 3ce286863ce129fa05bf7e590039f7953d814435 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Feb 3 22:31:40 2018 -0700

reduced code bloat

[33mcommit 4ac7f8cfdd35b09c09aaed0b1941d54eb971e914 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 29 00:31:16 2018 -0700

mudsum update

[33mcommit 773b30219496cf6829e5510580d9508e5e34a435 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 29 00:30:27 2018 -0700

rebuild with LTE and RLC debug, copyright updates

[33mcommit 06a7a0969584949f5c72b911b04f7d3b01a2bd1c [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 22:29:05 2018 -0700

added second copyright

[33mcommit 1baf3aa180b4c4f44f11e6797c9c68eb4800832d [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 21:54:34 2018 -0700

update for 2018 copyright

[33mcommit 135e8f1f77accd52409a6a74b3ab6af68b0e2a28 [m [33m ([1;33mtag: release-1.4.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 21:12:41 2018 -0700

i686 and x64 fix in test.cpp

[33mcommit 3ad0c32a72c77bb43ffa5eddd3de5f44a830eb41 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 18:19:02 2018 -0700

update for 2018 copyright

[33mcommit a0ebe72cd44ab0ac3fedcea1198bd24003630ba2 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 18:15:43 2018 -0700

updated copyright and RLC control plane debug

[33mcommit 62b272f8816fd016038a309fa8697eedb0449abe [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 28 18:12:56 2018 -0700

updates for copyright, debug of RLC and LTE for control packets

[33mcommit 24cdbc3fd69ab6dfb5f88369d5da326fce8039fa [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 21 23:39:15 2018 -0700

debug for LTE, still need RLC and ICMP

[33mcommit 3d4be42abf0cac6e411dc3125c43b63c4eca25f8 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sun Jan 21 04:21:43 2018 -0700

updates for Windows compile

[33mcommit b1c55e08bbafc64d8cf456660aa9fe5056e42a50 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Fri Jan 19 23:20:10 2018 -0700

added Phantom theme

[33mcommit 76a2fa234c6403d76366fff5a7db1254bc6333a5 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 15 22:09:25 2018 -0700

coverage updates

[33mcommit ba4aa47277c12dbcda2b3322ced7f3a9e795d478 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 15 12:40:36 2018 -0700

updates for coverage

[33mcommit 70dbf248f2703cecfc6686e4e89961c160cf77c7 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 15 01:50:08 2018 -0700

new files for coverage

[33mcommit 9d3f8583451b2215cbd13ae4bc60ad9e549a10af [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 15 01:46:18 2018 -0700

improved coverage

[33mcommit 1937c965503aa509c5578ca3d49b64a0a2750ccb [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jan 9 22:20:35 2018 -0700

updated examples

[33mcommit f29184c10c48d6890e87785cd956d5832c0015e3 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jan 9 22:17:35 2018 -0700

added mudsums

[33mcommit e3e293c27ed30e3872985bb3ba9eafcd333c9264 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Tue Jan 9 21:57:18 2018 -0700

debugged issues, now running both random and from generated files

[33mcommit d33a4ff62bcaf5024e7406a519d0fc5dc50a5237 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Jan 4 23:10:53 2018 -0700

new build

[33mcommit 18df28b6fe945d7781ba12bbba9d05dad6d5c389 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Jan 4 23:06:59 2018 -0700

fixed some parser issues when writing out the XML file

[33mcommit 20ef5d88a5af85ea4f4263ef388a66a5da37ac1e [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Jan 4 02:50:56 2018 -0700

updated version

[33mcommit 0d3091148cea11ac5e6164210e7a5982d3588d4a [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Jan 4 02:47:51 2018 -0700

fixed several parser bugs, overrun in the responder

[33mcommit b5d2688f9fbf97787922098211ba7239959b1736 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Jan 3 06:41:55 2018 -0700

fix for improperly constrained randomization for IPSec/IP payloads

[33mcommit 7fabab2adfcaf60f4c6571de8568e504517e82c4 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Mon Jan 1 16:37:51 2018 -0700

fixed several segmentation faults for next header processing and zero length data

[33mcommit a2a0d0eba04de035821c163fbc5d5c354f45dc38 [m [33m ([1;33mtag: release-1.3.1 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Dec 23 11:10:19 2017 -0700

updated readme

[33mcommit f5af59d971206da575d2f23f08824adf126ddcd9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Dec 23 11:07:57 2017 -0700

added libraries

[33mcommit a4dd4992fda149611a7c5aa3b0b8770ad494fdb9 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Dec 23 11:07:24 2017 -0700

updated examples, added mudsums file

[33mcommit 8f17ad1b7332d3492f2662a7f635a7363621df60 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Sat Dec 23 10:50:29 2017 -0700

updated copyright

[33mcommit 52e351385c88a09851c5c788381149950301be36 [m [33m ([1;33mtag: release-1.3.0 [m [33m) [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Thu Nov 30 00:08:31 2017 -0700

update

[33mcommit 724ce3a3ec9560f59de1b7ceda6ee30883b06c12 [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>
Date: Wed Nov 29 23:50:50 2017 -0700

updates for bugs

[33mcommit 56e35b8a91ab11ec673fc78f5f2eec9553da99af [m
Author: John Peter Greninger (JPGNetworks) <jgreninger@hotmail.com>

Date: Wed Nov 29 23:22:10 2017 -0700

    smaller compile

  [33mcommit 6ce8e90d42d45e8987d0d2ac92547cf2fc99c642 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Nov 29 23:15:02 2017 -0700

    fixes

  [33mcommit fbc308ca6b35be9b128f62f47c611a66a3548fce [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Nov 28 00:23:20 2017 -0700

    fixes for jresponder

  [33mcommit 91ffb6f5a1fe79cca643a8539bb50d253542bd50 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Nov 27 23:35:27 2017 -0700

    fixed status issue for IPV6_NONXT in IP

  [33mcommit 38b06c6fc1040d01aa770c68edc6ebae560340f1 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Nov 27 00:51:22 2017 -0700

    documentation updates

  [33mcommit e4b4aed6e1b0356a867276a3088b002431ee2e81 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Nov 27 00:50:51 2017 -0700

    added coverage report

  [33mcommit 50c078da55ca8016074049d336a1ff9f26719c97 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Nov 26 23:40:12 2017 -0700

    doxygen updates for NH processing

  [33mcommit 4320c01dc958812cd52eb0c5ac467c817cbb202b [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Nov 26 23:36:52 2017 -0700

    updates for release-1.3.0

  [33mcommit 776c2762fcaf86e6d15aedeb61d5066f54f7d5fe [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Nov 26 23:14:38 2017 -0700

    updates and fixes for release-1.3.0

  [33mcommit 09f0bdecc4f7e970ad839a4109bf4ed59b457669 [m [33m ([1;33mtag: release-1.2.7 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>

Date: Fri Oct 27 20:38:49 2017 -0700

    fixed parser bug when reading in *.protpp files that have SRTP

  [33mcommit eb0838fcd6b5e6ab68fec7b3247ea99d030b00ea [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Oct 27 20:18:16 2017 -0700

    fixed parser bug when reading in *.protpp files that have SRTP

  [33mcommit 72341bcfbf8c7cae7c425147c13c451bbb90dadc [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Oct 24 23:10:32 2017 -0700

    fixed parsing error when *.protopp file is read in

  [33mcommit 486e8869acdf814d6aea7d847bef26608bb2833b [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Oct 23 01:21:23 2017 -0700

    added specifications

  [33mcommit b127d6def62a0f05f7d9c70b390ac78dad6e4064 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Oct 23 01:12:39 2017 -0700

    fixed various memory leaks, shadow variables

  [33mcommit c8e263b55d04806cdfbac21f10b0164a3f720100 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Sep 20 22:01:24 2017 -0700

    updates for release-1.2.7

  [33mcommit 9ae58a9dea83ebac963255d516da34c742b5ab38 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Sep 20 22:01:05 2017 -0700

    removed --native compile option, re-enabled SFMT randomizer

  [33mcommit 3b9e6c0fcd4bf11c90027c594884fd9d5cc3f114 [m [33m ([1;33mtag: release-1.2.6 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Sep 16 19:56:44 2017 -0700

    fixed AES-CCM PRF generation, removed shared objects for release-1.2.6

  [33mcommit b85f8145b6ecb2fd05057891c5330d44b9cf34a9 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Sep 16 19:53:38 2017 -0700

    fixed AES-CCM PRF generation, removed shared objects for release-1.2.6

  [33mcommit 99ece2fafca822a97e4e2825584a9e14ebeaa444 [m [33m ([1;33mtag: release-1.2.5 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>

Date: Thu Sep 14 22:28:19 2017 -0700

    updates

  [33mcommit 6797b9ae9c0bf984333a750408f28ef83ab6beb4 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Sep 14 20:55:36 2017 -0700

    updates for release-1.2.5

  [33mcommit 2ae6f7dd9765688716412e04bf60d4a7a857bdd1 [m [33m ([1;33mtag: release-1.2.4 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Sep 14 20:51:00 2017 -0700

    updates for release-1.2.4

  [33mcommit 1fdf84ac695c94fd84747fe52012cda0fb508829 [m [33m ([1;33mtag: release-1.2.3 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Aug 27 11:49:09 2017 -0700

    updates for release-1.2.3

  [33mcommit 23907f1a576e65dda3bdbd2d5f0953fa79c0c77b [m [33m ([1;33mtag: release-1.2.2 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jul 29 16:15:55 2017 -0700

    Linux debug of Windows port

  [33mcommit 6a14ad614a5c2502275ef1cde4e0a0215ce5cd71 [m [33m ([1;33mtag: release-1.1.1 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jul 22 03:12:49 2017 -0700

    updates examples

  [33mcommit 58b74800f6ebca9af49c3d7d97cbce7bee871cb2 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jul 22 03:11:36 2017 -0700

    updates for release-1.1.1

  [33mcommit 5d6da4d4aee5a12d33f93bbf73a60fd0006f44bf [m [33m ([1;33mtag: beta-2.6 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jul 6 23:31:11 2017 -0700

    new examples

  [33mcommit f16526ecf4834834a679bc2e58a7aa852485eeed [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jul 6 23:30:14 2017 -0700

    added support to pass in address for input and output ring for SEC

  [33mcommit 612cdc059d9fdaab6ef4b80848df1fd3651fdb32 [m

Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jul 6 00:33:38 2017 -0700

    updates for SEC

commit 986424123ecb9c360499e39f7d6059595bb110ed [m [33m ([1;33mtag: beta-2.5 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 2 22:38:00 2017 -0700

    updates

commit 1afda7fceea75d6f997460b631daa80530f54f16 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 2 22:34:14 2017 -0700

    updates

commit fa24e9b0e3f001b583c662488ec3ca46adcec6b6 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 2 22:28:37 2017 -0700

    added SEC updates, doxygen updates

commit 3e82a595286a4e6fac8a89ae41e5b12344c3282c [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 2 22:24:58 2017 -0700

    updates for SEC platform

commit fb37a05845d4d8bdfbb3288c2f410cf98a71d2d0 [m [33m ([1;33mtag: beta-2.3 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 28 20:55:27 2017 -0700

    updates

commit f478ba866bc7ebc11ca1d15c6ea9affe3a38b225 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 28 20:54:13 2017 -0700

    updated examples

commit feb44c1e24e6c9e0831070d5d28f12ca769e98e2 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 28 20:48:18 2017 -0700

    updates

commit 72ab0922c0192bb0df17488dcbb462a7aeca56a4 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 28 20:43:47 2017 -0700

    updates

commit 8b2d3f2ffb57e9001be978abcc4b244a0af1308e [m [33m ([1;33mtag: beta-2.1 [m [33m) [m

Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 23:14:25 2017 -0700

    doxygen updates

[33mcommit 317dc4f67d3e94f6056c87c7d237c7f84cd9a54f [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 23:07:10 2017 -0700

    updates

[33mcommit e48fee3e3d15be852391d28e5f4b9886e740afc7 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 22:59:52 2017 -0700

    removed submodules

[33mcommit 0f01df78f1ea73ca21884dd63afa27fe0f1d1bd2 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 22:56:34 2017 -0700

    updates

[33mcommit 45ce149102b8d4083bcdbd8ef8cb4b6f4aec3ea1 [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 22:53:19 2017 -0700

    updates

[33mcommit 2ac2e9f8af897c1e659643b438f83e883da0c08b [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 19 22:50:10 2017 -0700

    updates

[33mcommit 23a2e3bfd22d56821cadff373ec0e21a08410de2 [m [33m ([1;33mtag: beta-2.0 [m [33m) [m
Author: John Peter Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 14 11:13:34 2017 -0700

    updates

[33mcommit 2e3682a3d8c79c59dcfd97661d7f7fe64dbc063b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 14 10:50:58 2017 -0700

    updates

[33mcommit 0f40c95f49ad5299a9a8207f935397ec048f4757 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jun 14 09:58:11 2017 -0700

    updates

[33mcommit 7565d93822dd7bab1c93e6a708ad5511bc48ee95 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Jun 13 22:13:55 2017 -0700

    updates

[33mcommit a1cdb11a149774a25d25db64bab3f4144f71fc26 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 12 09:10:47 2017 -0700

    added examples

[33mcommit bd4e3fc7b609ebeb630c9ad90529ee1940bbb35f [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 12 09:02:34 2017 -0700

    updates

[33mcommit 6cd132446e7003f4ebb18ba10b1d8b0e824bd56f [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jun 12 09:01:10 2017 -0700

    updates

[33mcommit 780a4b9f70c206a4041ce02f0dfb380e6535593f [m [33m ([1;33mtag: beta-1.0 [m [33m) [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jun 10 11:42:06 2017 -0700

    release text

[33mcommit bb784fd82118126810c079c369603a4526dbfaff [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jun 10 11:06:27 2017 -0700

    initial checkin for release area

[33mcommit 3149c56abad0a7138d71932700eef7f3ed8b5742 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jun 10 10:39:00 2017 -0700

    updates for make

[33mcommit bba2ac7c113d0ad45d7129112a03e2398bf49d5a [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 9 12:36:33 2017 -0700

    doxygen updates

[33mcommit 1ad9fb924d5dbb6147977e28df9cdbb5dea95f6e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 9 12:33:33 2017 -0700

    fixed TLS and WIMAX anti-replay

[33mcommit 7531d008fa29c2d40080af37a466e3f8c36d9a05 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 9 03:19:48 2017 -0700

    added new window when only arlen is supplied

[33mcommit 71b59e264938717dd21af8f1b1110f8212487b90 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 9 02:59:06 2017 -0700

    removed some debug code

[33mcommit 6b521eaebccfcd108f484597923a22a69a5c70de [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 9 00:11:04 2017 -0700

    fixed MACsec decap

[33mcommit b11bc64e78ecfeef3c211333a77347a69bf92f9b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jun 8 15:28:36 2017 -0700

    added this back

[33mcommit 0434b5a518fee89a75ea9d27f5b342e8b939c70f [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jun 8 15:23:35 2017 -0700

    fix to allow constructors to make empty replay window, doxygen updates, wasp updates, LTE decap debug

[33mcommit 3553bd645de34ef2129289201ae5432a2748e544 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jun 4 15:19:36 2017 -0700

    added copyright

[33mcommit 37524efaeea8f0f4d6242f455f0d48179d895025 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jun 4 15:18:03 2017 -0700

    missing file

[33mcommit 9f21346c3292de3a3afabb83d76a3a8267076965 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jun 4 15:15:50 2017 -0700

    fixes for headers for control plane in LTE

[33mcommit ccd02cd7299c173b496198ada87e45947e3fc161 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 2 22:27:41 2017 -0700

    doxygen updates

[33mcommit a903af5b85b5f56c02542d7e1a4c8833bd023c7e [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 2 13:41:26 2017 -0700

    added guard banding to extended header parsing

[33mcommit bb4e1ad60fb9ef56140005ec864f1142bb876213 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jun 2 08:39:10 2017 -0700

    code cleanup, JUMBOGRAM format error updates

[33mcommit a695c2fd560c0f61584540758b59573f68475e4c [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jun 1 23:16:19 2017 -0700

    doxygen updates

[33mcommit 901137934a2d9d9a50f06fa748d6d395c60a28d8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jun 1 22:57:41 2017 -0700

    doxygen updates

[33mcommit 32c7963cb1ac70bdd3175a6008fdbc89cc8eec8e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Jun 1 22:54:11 2017 -0700

    added TRANSPORT, debugged RANDIV and TFC PAD in encap to support postprocessing in IPSEC

[33mcommit 977f5f9b96f54eb88fa317b9aa31da2f8c51e864 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed May 31 12:16:03 2017 -0700

    added copyright notices to *.cpp files

[33mcommit 9d1f4b4f94c7c76be9d08d9b33f9f3b76065687b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 30 00:20:10 2017 -0700

    updates for unified fields, fix for IPSEC when NH is TCP UDP ICMP or IP to correctly make a valid payload

[33mcommit 0373b0d2410c096e8379b93934e6b12dd4d24d85 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 28 21:54:35 2017 -0700

    fixes for TCP/UDP checksum after decap in IPSEC

[33mcommit bff3ced5a8d45dd5ed8dc8cbd8cba6a8077fd12c [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 28 10:30:52 2017 -0700

    updated copyright verbage

[33mcommit 454a05b367defb918229bad26d74f8773eda3858 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat May 27 19:15:19 2017 -0700

    doxygen updates

[33mcommit 283466e4b39ef1cbe15e192d7d66f59394bea09e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat May 27 18:48:15 2017 -0700

    tightened randomizer for TLS, fixed NULL_CIPHER and NULL_AUTH in TLS

[33mcommit 2a04b1ef37392e378532fd729ae336063116d0af [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 21 12:21:49 2017 -0700

    fixed jwifi for NULL_CIPHER

[33mcommit 9d34b78764fd6545e0cfb367990b3e015c6cc466 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat May 20 00:37:29 2017 -0700

    constrained randomization for WIFI a little better

[33mcommit c4d2c81b6bb4ab5307bc60948c363fa40315f188 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed May 17 18:19:04 2017 -0700

    fixes for SRTP decap nonce construction in CTR mode

[33mcommit fb2105d13fb8e58cd898a400add79e3809279c50 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 23:53:58 2017 -0700

    fix

[33mcommit 56547b3fd617fa3fd102b6c5c6ba4c020a2875a8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 23:49:47 2017 -0700

    doxygen updates

[33mcommit d41974c9693e51d5ffd985a73ecabb63fb20ab95 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 23:48:26 2017 -0700

    forgot missing initial values

[33mcommit d612e4003d893f0de105ae763295082ffa861cce [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 23:45:25 2017 -0700

    additional cleanup

[33mcommit c1897d7915b0492dcb0b1b91472788c98dde0f81 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 11:12:40 2017 -0700

    added other extension header formatting

[33mcommit 77973f9d4be201cf76161ce3568a92e6763dcde5 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue May 16 00:38:47 2017 -0700

    updates for next header processing

[33mcommit 8aa026b4c843e413effcbbd4f5fa981e3d38b6fc [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 15 22:14:44 2017 -0700

    fixed small decap bug

[33mcommit 1ab83368ca8b1ce0577a3cbf4b22401e2206f732 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 15 00:24:40 2017 -0700

    doxygen updates

[33mcommit 6a04a7e755ca2dda44e63b4158438fbd4cbcb0fb [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 15 00:23:50 2017 -0700

    fixes for decap in SRTP, fixed missing extension header

[33mcommit f225e214e3c85c0b48f5999360a4d98f457f1502 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 14 20:19:06 2017 -0700

    fix for srtp

[33mcommit 38bf58a331fe357e30ceaefa0408c27617d4425d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 14 18:39:11 2017 -0700

    fixed some randomization issues

[33mcommit 17bbf775c02cd0aa047ab1acbf98c763eea87c68 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 14 18:37:31 2017 -0700

    updates for testbench

[33mcommit 6abf259733f0d4a6b918a855ced6df113c4c467d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 14 18:35:39 2017 -0700

    guard banding

[33mcommit cdf019b574ed53dafa35721f1e96716b96725864 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu May 11 22:47:17 2017 -0700

    fixes to to_xml() for decap

  [33mcommit 6617922b56dac7f11ecb3ceb2971a2f70b70e643 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 8 23:50:19 2017 -0700

    additions

  [33mcommit 462873b0b0ae4eb0ed62025339b2e6cc640f8ffe [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 8 23:49:52 2017 -0700

    name change

  [33mcommit 5b2b0c570ac0a98cf2030fd04c08b507b86bd3c0 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 8 23:46:28 2017 -0700

    updates

  [33mcommit 4ca01e482a9620d49294b043766908319 91a50a1 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 8 20:51:09 2017 -0700

    added PLATFORM command line option

  [33mcommit b71e36c768c6f52d9c835ea94b4912be4c9d7d18 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 7 23:17:56 2017 -0700

    doxygen updates

  [33mcommit f97c0c5fd0532127c850de6fddad00247a54fb47 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 7 23:17:28 2017 -0700

    updates for TCP decap

  [33mcommit 3253d3dd0bde08bda533a232565c89da2b44edaf [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun May 7 19:44:40 2017 -0700

    updates to logger and remove extra header files

  [33mcommit 4e8e959f8ce795c808fd32dcf30ef2197615e8ac [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon May 1 23:43:04 2017 -0700

    fix to WiMax counter modes

  [33mcommit c8ab9776e62851d484ab0a9e3d2e33235506bf65 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Apr 30 18:18:58 2017 -0700

    guardbanding for SA copy constructor to avoid seg faults

[33mcommit 8adf4b6fe7d75ad5bc14924df8e2e420865c10cb [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Apr 30 09:44:15 2017 -0700

    fix for copy constructor in jsrtp

[33mcommit 8e220c855693f4018fa2977935491aaaa4c79bc6 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Apr 30 01:12:21 2017 -0700

    fixed SA copy constructors to make copies of data pointed to by shared pointers

[33mcommit 605724bfad304077af57bdea1aa8bb6b9ed69634 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Apr 29 22:55:59 2017 -0700

    added postprocessing infrastructor for random IVs and TFC padding

[33mcommit 3ab5e8b4841cf70142c64fafa748ac59b9810a92 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Apr 29 16:42:42 2017 -0700

    updates for parsing, doxygen, logging

[33mcommit b08e8d25a5eb290602635cd65338b9c469f80f7e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Apr 28 15:32:23 2017 -0700

    parsing debug for IP, fixed double free for WASP

[33mcommit 981c3b079952b5f2adff233aec9ec587c7fd15e2 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Apr 26 11:44:17 2017 -0700

    options parsing added for command line

[33mcommit c589bf46b7170a9dee167686b6a14417a5e0d669 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Apr 23 16:01:42 2017 -0700

    updates for schema

[33mcommit 96b54adb5d56a5e9d30be23420aa010eda553477 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Apr 22 21:51:28 2017 -0700

    testbench updates

[33mcommit 2387f40c7f865ed0497b26d2f9b83b8da3fc7f01 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Apr 20 00:25:32 2017 -0700

    copy constructors for security associations

[33mcommit 13b1a6ef42f42de394df0099a7cf4e176d15ec80 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Apr 14 00:27:15 2017 -0700

    updates for testbench

[33mcommit 4ee2485795f5ed567e243b294e99f237704f91af [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Apr 12 22:59:31 2017 -0700

    random packets for IPsec have well formed NH packets for IP, TCP, UDP, ICMP

[33mcommit 9193b1e9a14ebf824875b781f787f5d1c193e60e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Apr 8 02:00:22 2017 -0700

    doxygen updates, debug of testbench and responder

[33mcommit 4439040aeea74f701f4f8edea2e08e0c3041c96b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Apr 3 23:22:13 2017 -0700

    doxygen update

[33mcommit 29edb458fe554e8ba73820da3c75abdc08d2ebfd [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Apr 3 20:58:34 2017 -0700

    added back ivlen in IPsec

[33mcommit 7c9311a1c19b4835319f6cce0a67005a55011329 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Apr 2 21:18:54 2017 -0700

    fixed some set/get parameters in Wifi

[33mcommit 459493a32d077924000ec781731c1756d5df5638 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Apr 1 13:38:33 2017 -0700

    debug of reading *.ppp *.protpp and generation of packets and flows

[33mcommit b224df2f280c243ec6821fea5472e5a85cba15f6 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Mar 31 19:19:40 2017 -0700

    additional full randomization debug

[33mcommit 04e8f71b0c8796a38060517cc802d7b24c398078 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Mar 31 00:32:39 2017 -0700

    debug for randomizer after turning on full randomization

[33mcommit 2e715f29b06610a48044c86aa6e85082c0748027 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Mar 29 15:26:28 2017 -0700

    fixes for NULL_CIPHER in JTLS and WASP, doxygen updates

[33mcommit 1f15a50df6af087ae6000f0083c18e79b2397c26 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 26 19:10:16 2017 -0700

    doxygen updates

[33mcommit 85f92cd79abdb1a10788e602ec7fe83b51323cf8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 26 19:04:39 2017 -0700

    refactored m_pkts to use a map to map packets to their associated flow

[33mcommit cf97519852456f792692a1557cd5105f8ebb8a29 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 26 18:50:59 2017 -0700

    refactored m_pkts to use a map to map packets to their associated flow

[33mcommit d5f01c8359aa90ed86cedb5d6b9ab918be209ca7 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Mar 25 16:31:22 2017 -0700

    fixed a missing initializer

[33mcommit 8fb3b5d20d42933ae0b3dc96d112f6b7907c7da0 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Mar 23 16:48:18 2017 -0700

    debugging of testbench and it's components

[33mcommit 90da027aa24d85bcbf5ed44f5dbd53144e479786 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Mar 23 00:56:58 2017 -0700

    updates

[33mcommit 540340d9d60b193f14c13758efedb12a285b13ca [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Mar 23 00:27:52 2017 -0700

    fixed an bug, still working on AH

[33mcommit 022ed9df08e34d0c1c5223fc6443c962fb474f54 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 21 22:53:56 2017 -0700

    doxygen updates, fix to sm3 pointer arithmetic

commit 356b3c97e14d31cb5a83697bc75bc8db935cb4ec
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Mar 20 21:25:03 2017 -0700

    doxygen updates

commit 7ff014d8fd7216e4e7dc249815f391b9ca05efe0
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Mar 20 21:13:38 2017 -0700

    doxygen updates

commit b97f210482852ab5e33bd5c1152da2ef15320246
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Mar 20 21:07:21 2017 -0700

    sm3 conformance debug

commit 3ff86a6a39374290b83ea132bc95d81e67d47615
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Mar 20 01:05:29 2017 -0700

    debugged SM3

commit 55be531af0af89ca3a6a9e525a17dcafff15bfd0
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Mar 18 19:17:51 2017 -0700

    SM3 code and doxygen update, needs debug

commit 8d39155bbbe981680c7363f18b980ea289c5a4b1
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Mar 18 00:30:36 2017 -0700

    Fixed a bug in 15-bit LTE-AES

commit bf723743f8ceb630bd581686a37ed42f37e404e4
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Mar 17 13:35:59 2017 -0700

    doxygen updates

commit a209ac43afedadbeb68aacbd6d2a4d13d9e634c4
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Mar 17 13:13:06 2017 -0700

    working LTE/RLC debugged and wasp working

commit 9e05195484b5cbfe4ced9302751244b8742334ac

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 14 18:11:25 2017 -0700

    doxygen updates

[33mcommit 525777534288bf67ebed5de5f61ba12cece48a1b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 14 18:04:12 2017 -0700

    added RLC mode to jlte

[33mcommit 2de661dcf295dd922badbf2ea3ace2039e7cb20d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 14 00:17:21 2017 -0700

    working AES-CTR and AES-CMAC for LTE

[33mcommit 8274aca640cea53f906e10535eb81adb3dea5654 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 12 00:13:33 2017 -0700

    working LTE with doxygen updates

[33mcommit 32fed761e0b9eee79a563f0277d2b8a5bb06970d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Mar 9 00:25:36 2017 -0700

    added LTE

[33mcommit 5c318e1fdefb15d4e8bc60f289bae2fa2c5c30ee [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 7 15:26:04 2017 -0700

    updates for LTE

[33mcommit b8baa9c40aa00ca838e2913c81346fdd6e304e4d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Mar 7 10:43:22 2017 -0700

    updated to remove copy constructors

[33mcommit 7dcc8162b81500f596c019ae477f310c7403b861 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 20:47:15 2017 -0700

    fixes for zuc and snow3g to use raw pointers and process the byte inputs directly

[33mcommit 91cf6b54c11a371ec6069402b05ca965a98b5828 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 20:41:42 2017 -0700

    fixes for zuc and snow3g to use raw pointers and process the byte inputs directly

[33mcommit 857715b051d754bc2905022000319a6bf92516c4 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 17:45:38 2017 -0700

    reconfigure zuc and snow3g SBOX and constants

  [33mcommit d374248617a355283e8c2be70e526cfde8b3eaf1 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 15:54:25 2017 -0700

    jdata class to hold create data for testbench or driver

  [33mcommit 6dbd1d2c49dc0027ede91afc84c871dadf373fcc [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 15:47:03 2017 -0700

    reconfigured chacha20 to remove the structure

  [33mcommit 39c9a58afa6d8cc35ec52cf854ca08ba83114bbf [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Mar 5 12:15:05 2017 -0700

    fixed ARIA for chunking

  [33mcommit 636aa32e49338541c8fa1570ce58ac25f29fa705 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Mar 4 14:53:18 2017 -0700

    updated poly1305 to be able to chunk data

  [33mcommit 32cb996e405e15f245c8f26a06393de79b94b9eb [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Mar 3 22:44:34 2017 -0700

    cleanup and addition of testbench items

  [33mcommit 17769cc158c195c06f4632bb4be87d2e43431e37 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Mar 2 20:24:06 2017 -0700

    cleanup to simplify and remove duplicate code

  [33mcommit e8f9b7f18a6bf0472f7d8dc4d5dc38c90661e428 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Mar 1 15:11:13 2017 -0700

    updated AEAD mode to remove vectors and use byte arrays with raw pointers to improve performance

  [33mcommit a3b63504fda5d2273ed5b83c1b44563f164e9aab [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Mar 1 00:02:25 2017 -0700

    moved aead_chacha20_poly1305 into jmodes

  [33mcommit 9ec93aa6b7cea92fb778f2ee3a7ab56052245eb3 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Feb 24 21:29:13 2017 -0700

    new images for macsec

[33mcommit 8a58ddc7c78bb8adefb82f3e2f21a40bfc6b9e30 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Feb 24 21:28:32 2017 -0700

    fixed some TLS1.3 bugs

[33mcommit ad0a5ddf6b952a9b585ea7d37297c24c88da0b26 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Feb 20 22:17:52 2017 -0700

    added method to retrieve roundkeys from aria

[33mcommit 706d9235a0294548eae03c4972aaec54c166e165 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Feb 20 21:30:08 2017 -0700

    added SM4 cipher

[33mcommit c65413d8594aa9478d01362d4b3c3a6ef0e93523 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Feb 7 00:46:57 2017 -0700

    doxygen updates

[33mcommit 78ef92a7d3eb4026144971df909e7c1f70bd3934 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Feb 6 00:55:29 2017 -0700

    doxygen updates

[33mcommit b6c5a020c2c8cdbe45956021cf492b8bc0160944 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Feb 6 00:45:43 2017 -0700

    updates for reading protpp files and running packets

[33mcommit 3f6ac9fe88c0119484518b6bc18469c0fa53add8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Feb 4 00:57:40 2017 -0700

    updates for wasp to print correct direction for protpp files

[33mcommit 5a20eff9cd5a120197a406e6ddebc029fab1149f [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Feb 1 17:21:15 2017 -0700

    updates for CryptoPP 5.6.5

[33mcommit b2296dfa937aeb207fc56f615031bb3a9d1bfed2 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jan 30 01:13:58 2017 -0700

    new logo, updated jreplay with function to return seqnum based on type and window

  [33mcommit 07f9b68361d08cf19d9ed34c9d459baaacfdb55e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jan 28 21:14:38 2017 -0700

    added range interfaces for jrand

  [33mcommit d805b251d3d077da1b83a60d13aceff8eea25fdf [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jan 28 20:44:14 2017 -0700

    updated jwifi to use homegrown GCM/CCM modes

  [33mcommit 0c99a15487b76782e8ca034313fd4f03fda0d310 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jan 28 19:54:16 2017 -0700

    Documentation updates

  [33mcommit 2f95508beeb9c2b1758d637a4751ae5a06b08190 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jan 15 03:02:54 2017 -0700

    updated jrand to use std::mt19937 when compiler is C++11, test updates

  [33mcommit 47b6c5325140f13a376dc07902759beaceca1e50 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jan 8 23:05:27 2017 -0700

    changes m_flows to map to lookup by name

  [33mcommit 76d2166474f2c3b378ea20e5f4ef4c83bea23385 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jan 2 00:18:55 2017 -0700

    added testout directory, GCOV output

  [33mcommit 2a92292b2119880821d3a8a056b1db33403d3adf [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Jan 2 00:15:02 2017 -0700

    fixed parser to support security associations for all protocols

  [33mcommit d33a0c9c9b742a1a217d214cafc2d524c48d5753 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jan 1 00:50:24 2017 -0700

    updates for code coverage

  [33mcommit 9e7343b3b6145e10d6658d2b97d2ba45ff4d6a8e [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Dec 24 22:42:38 2016 -0700

    finally got back to macsec, fixed IV creation, added extended packet numbers, added new support to WASP

[33mcommit 4284ee5d54d84f3bb9981171851fda87d534cd0b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Dec 24 00:15:43 2016 -0700

    fixed bug when mkidata is not present

[33mcommit 34dc53b354b46755cef5c0901ca4ff22339829c9 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Dec 4 13:25:36 2016 -0700

    updated TLS with original jmode code with CryptoPP ECB core

[33mcommit 47783f8e468993fc86f637ac9b6a11e95ca6568d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Dec 3 21:10:24 2016 -0700

    updates to cppunit test, parsing, sequencing

[33mcommit 7434162c962cc9c044596e63ea558109b69f23e2 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Nov 15 16:44:14 2016 -0700

    added parsing exception to wasp

[33mcommit 8037e86ece26722bcfd3ea33c6f8d313a38a3214 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Nov 3 11:36:10 2016 -0700

    doxygen updates, randomization updates

[33mcommit 508752a50c26ecba507c1d7e2e3c06741a01d26a [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Nov 3 01:31:27 2016 -0700

    removed debug code

[33mcommit df4a066f92ad2228abffe2804c2380c5f06c22c3 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Nov 3 01:22:50 2016 -0700

    updates for parsing errors due to ENUM conversion

[33mcommit e4ac0a46285acfcd38f078abfc0e5f97e3d51d92 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Nov 2 01:38:41 2016 -0700

    added security associations for UDP, ICMP, TCP, IP

[33mcommit 867e99482758e7b867451f7ef647be676eff3d80 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Oct 31 23:29:19 2016 -0700

    still a bug in void pointer of engine

[33mcommit 8c58fefb4ece5b9c4db7cb82e63f02939fb4bc6e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Oct 31 20:26:28 2016 -0700

    revamp to eliminate m_engines

[33mcommit d25ba6bd9cd839a51cf3be1333ebbfd5263ff1dd [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Oct 31 14:09:23 2016 -0700

    wasp random test files

[33mcommit a0a04602ebbef0bd17f420ceff304d4093240388 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Oct 30 19:04:38 2016 -0700

    doxygen updates

[33mcommit 88c213d8ff66876321f9cf127b48518d4aa1089d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Oct 30 18:59:47 2016 -0700

    doxygen updates

[33mcommit a1a7ebc69ee394b88335f0d93db74cc0a8a8a217 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Oct 30 18:57:18 2016 -0700

    doxygen updates and images

[33mcommit 6c511b6847aeaae1a823601f20a968fefd2d6716 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Oct 30 18:56:06 2016 -0700

    debug of CMAC mode, added random tests for parser

[33mcommit b62d792104fa0cebbd669a2406057c3631504f48 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Oct 29 23:35:50 2016 -0700

    cleanup

[33mcommit 69c8852d3230e1223b8fddeca3d19f63ceb33c17 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Oct 29 23:33:20 2016 -0700

    coverage updates

[33mcommit 0473fe4b4e5b0f07bb91be936a305240acf76e18 [m

Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Oct 29 20:29:37 2016 -0700

    updated to reflect standardization of src and dst across all protocols

[33mcommit 20947bfc1641abbeb29a526b0e9514178825cb6d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Oct 29 20:16:49 2016 -0700

    added schema checking to parser, cleaned up some code

[33mcommit 7d4a8716a9abe28a233625031821e2a3c77f70db [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Oct 27 01:55:40 2016 -0700

    doxygen updates

[33mcommit f0f7b5657d2d2b7e5d88884f7d5282b3e37dedc1 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Oct 25 23:09:04 2016 -0700

    added support for WiGig, fixed bit ordering issues in Wifi, moved all init routines to *.cpp files

[33mcommit 1d7f932313ebdc66fd35f2084499e6323bd43ba4 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Oct 20 21:06:26 2016 -0700

    fixed SALT values to be independent of the cipherkey, added AES-CTR with CMAC for Wifi, randomization fixes for default values in wasp

[33mcommit 6e9ac97964743c14159fa596520a821b3f3d30ed [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Oct 14 23:59:26 2016 -0700

    added stream class, worked on randomization and parsing as well as testbench interface

[33mcommit e19977fd7c7b5262699c4de530a052fc817c936a [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Oct 13 23:19:28 2016 -0700

    fixed stream issue during descriptor generation

[33mcommit 346fb73511babe6e54ba43dc804f06d5d6c1810d [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Oct 8 22:40:19 2016 -0700

    finishing touches to W.A.S.P

[33mcommit a03d0e8970f4958aaedb6bf24aa68514c47ab7e8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Sep 29 20:17:08 2016 -0700

    parser debugged for all protocols with output, needs debug for different modes

[33mcommit 02b6261251e94c475078e30d8a3671b14591ca02 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Sep 29 02:12:39 2016 -0700

parser debug for SRTP

[33mcommit f04319a8081ea68fda13e77e6c48d5b9abde233a [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Sep 26 02:35:45 2016 -0700

working parser and generator, needs a little more debug

[33mcommit c2817c5992974ced96daddbd3ba3dfac5a96dd8b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Sep 25 21:59:23 2016 -0700

fixed formatting

[33mcommit 126f0612082d68115e4bce7f68392fbe48a066d4 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Sep 25 21:57:43 2016 -0700

added jpacket, added regex to jarray to strip out underscores and whitespace, parser debugging

[33mcommit 287d10651fa34c0cbeed39433aa76cb29da71a2b [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Sep 23 17:56:20 2016 -0700

fix for doxygen

[33mcommit 374bd20bb8762f949920cbc913b398ccf5bb2ee1 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Sep 23 17:44:59 2016 -0700

updates for front end and doxygen

[33mcommit 79a2c0a3d361bd0cc5cc3fba285b275d35a607ec [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Sep 13 00:59:12 2016 -0700

second pass debug front end

[33mcommit 66e4a066ccb6b7a62f10312ae935a3100aee8506 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Sep 11 22:52:33 2016 -0700

first pass debug on front end

[33mcommit 7f5c97f9104b7253c22ba2188433711990ee33f5 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Sep 11 18:14:39 2016 -0700

updates for front end

[33mcommit 5fca907c24469c7d34416f41a874e8de9be6b7bb [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Sep 5 21:38:09 2016 -0700

updates for protocopp interface to use base class for all pointers, doxygen updates, XML parser beginnings

[33mcommit 78b54998b5bb705097a202ced842da0013a25766 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 27 20:26:37 2016 -0700

doxygen updates

[33mcommit 58095114ce09d91d695f00b3d7dd7576e8cec525 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 27 19:05:23 2016 -0700

fix for replay, removed multiple copies of HEX

[33mcommit 4b25fbb40868a9772393610954669aec0921e110 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 27 17:46:30 2016 -0700

updates to schema for all protocols, enum to randomly choose a value, replay to fix masking issue

[33mcommit fc4e40e1913d7de64f205235645f659607561ec8 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Aug 24 20:39:41 2016 -0700

updates for anti-replay

[33mcommit b12491a3d5ce47d8202134bcfe1d4ffcf6011613 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Aug 23 23:54:15 2016 -0700

update for replay window

[33mcommit ed742c1177a1e079d5a4e370163369747a5a7540 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Aug 25 21:13:24 2016 -0700

doxygen updates

[33mcommit c1aafd6473b3168f867f89d8e089520af0c70a7e [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 20 15:43:54 2016 -0700

updated TCP to include the TCP state diagram for setting up sessions

[33mcommit 4e93566bef4a9453aae5fc55e3dbfaff019c04c2 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Aug 16 23:28:12 2016 -0700

fixed some memory leaks

[33mcommit 1792246935769ce1b6dc208135ad14c3d4d1dbdb [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Aug 15 19:29:47 2016 -0700

fix for anti-replay

[33mcommit 307e1d386d5c1d810f95e7c8cae14b34b3b0cb09 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Aug 14 23:47:59 2016 -0700

added ICMP protocol, fixed documentation, added TTL detection

[33mcommit f0a7adb9d355d881fbf08040767279f73b989639 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 13 23:22:56 2016 -0700

update

[33mcommit 4e642d5dbe74fd40e4d0ac0f2171c943295fc9c3 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 13 23:11:37 2016 -0700

updated coverage reports

[33mcommit ce0a39cfe902829707ef0f002d22d0fa6bc10895 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 13 23:06:09 2016 -0700

added missing images

[33mcommit efc44f05189697ffcb765222a319a83f5a62acfc [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Aug 13 22:59:18 2016 -0700

added ICMP protocol support for extension header processing in IPsec, doxygen updates

[33mcommit 03d42d1fad8fdd6ec6c72c7e143811e02136e9ab [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Aug 12 20:09:37 2016 -0700

added NAT-T UDP encapsulation

[33mcommit 6b801a6c61836525b6bbfc03a9da58f70cdf8796 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Aug 12 15:58:05 2016 -0700

fixes for SRTP header bits

[33mcommit b6ebed802d23e1ab965a49728f6c3f57cec26be1 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Aug 12 00:23:19 2016 -0700

added constructors for security associations

[33mcommit 9d5961ee5c718e8ac661c2795a0f7f1205c94608 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Aug 8 23:13:46 2016 -0700

doxygen updates, fix to CHACHA20

[33mcommit 1ab4eed68d2324d1d6aa00f7cba92ae904a7d0cc [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Aug 4 23:47:11 2016 -0700

added JUMBOGRAMS, merged some modes, added format checking for IPv6, new audit mode 'FORMAT'

[33mcommit 1ca783b509f5fbb25057f748c468136c5da9a8e2 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Thu Aug 4 18:56:23 2016 -0700

not sure but it's a bug

[33mcommit 055fb2e44d67fdf682592adbce77f77905a48a32 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Aug 3 22:35:05 2016 -0700

updates for CCM

[33mcommit 9fd1b2b47af1b1eb2542ee753e748fc0eef25916 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Tue Aug 2 21:54:21 2016 -0700

updates to add SEED Korean cipher to TLS

[33mcommit 1e43ed5295676ac409d8afb493ae9a88ac0827f9 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Aug 1 21:10:46 2016 -0700

doxygen updates

[33mcommit 4eb0c252eb6df22629fa9f0ad6aaba53e717f1d2 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Mon Aug 1 21:07:36 2016 -0700

added ARIA to jmodes, TCP/UDP over IPsec

[33mcommit e3434d6c904b12325906e92f68ad52d38ace62c7 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 31 22:14:04 2016 -0700

added psuedo header computations for TCP/UDP

[33mcommit ef0c52d7d9a860b6e69a79f3c662861bea96fa80 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 31 16:02:46 2016 -0700

final debug of CCM mode in jmodes, added to ipsec, reduced spacing for debug in jarray

[33mcommit 5a90b9c25163dbfccc71a83364113ccb4f5bbc12 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jul 30 18:30:44 2016 -0700

update to the aead_chacha_poly1305 interface

[33mcommit 04d242def4cd12058df9be33fd7773aab8ef22b3 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sat Jul 30 18:06:45 2016 -0700

debug of IPsec AES-XCBC mode, randomized datalen in tests

[33mcommit 6dc5bcbd9de9a24db32b796dad231c1bb9816672 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Fri Jul 29 21:18:51 2016 -0700

added new warning

[33mcommit 0d77f00005bb7659166ec1dde4b1fcc9dbe07438 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jul 27 20:23:45 2016 -0700

working CCM, added conformance tests for different modes

[33mcommit 6348cea347d6e7a6c7bb533765e73eca4204912a [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Wed Jul 27 00:19:32 2016 -0700

CCM mode debug

[33mcommit 354e6ed3adf970a76879131706786eb33ba26452 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 24 22:51:43 2016 -0700

report updates

[33mcommit cf1926967cb5fc0c5133d71cc85ca9b3b809f319 [m
Author: John Greninger (JPG Networks) <jgreninger@hotmail.com>
Date: Sun Jul 24 22:39:46 2016 -0700

added reports

[33mcommit a3b4348d2bea1bdef8c8fc7040506e0e1d4c37c7 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 24 22:11:34 2016 -0700

added images for doxygen

[33mcommit a27da654c423d1e575cabcbb00849a02fa27e6ab [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 24 22:06:46 2016 -0700

updates for doxygen

[33mcommit d29be171a451b9821b707ff82de20782c1ab96ee [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 24 18:47:00 2016 -0700

debug of new GCM mode in jmodes

[33mcommit 97602fd63682af28220970ae65c96ae8121131f6 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jul 22 00:04:23 2016 -0700

Debugged GCM in jmodes, fixed debug() in jarray

[33mcommit 77a9a5a9a00a5cbaf4ffe7f9395e00dfdd2e7b85 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jul 20 22:33:24 2016 -0700

added missing code to copy header values from outer IPsec to inner IP, still need flags in SA

[33mcommit d698daaf3178b5bde5bc1a69a7b2317ba0265560 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jul 20 18:54:46 2016 -0700

debugged AES-XCBC-MAC and added to IPsec

[33mcommit d3b7f9c76e4a1f69081d84e9382d10831ffdeac1 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 19 22:56:46 2016 -0700

doxygen updates

[33mcommit 10b83e3254e3aba0ba78818825569f45d4434e3a [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 19 22:33:24 2016 -0700

added AES-XCBC-MAC to jmodes, needs debug for non-block size messages

[33mcommit 07f79a20710713bc648f0d188a2a60da02fb6f8b [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jul 18 23:34:23 2016 -0700

added back non-random IV for IPsec

[33mcommit 203db4e1dac68e9b3cc83e0c579f343ede5a3eff [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jul 18 23:32:10 2016 -0700

added AES-CTR mode to IPsec

[33mcommit 8540fcae4e21ca7029eee9b009dfb7bcbc4bdedb [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 17 22:57:18 2016 -0700

added Encrypt-then-MAC to TLS, some doxygen updates

[33mcommit da8a765775ac7ee27a9efa1d989da629e786ddc4 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 16 20:16:51 2016 -0700

removed stand along ARIA files

[33mcommit b5210da1e909e50390610bdf9768846f80a40356 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 16 20:13:54 2016 -0700

check in of stand alone ARIA files

[33mcommit 69bdf99d9f559a86596707e7c59dc4d95c189e6f [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 16 18:39:20 2016 -0700

fixed pretty print in jreplay

[33mcommit a8c8b4442b52432d82873be97c3236b1753a8873 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jul 15 01:44:50 2016 -0700

updates

[33mcommit fd4f171f104132d438e49be0c91a57467451c29f [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jul 14 21:05:32 2016 -0700

debug of new modes class

[33mcommit bfae9eb0f1d46772063b83f0e7b219222bfd8a79 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jul 14 20:53:59 2016 -0700

updates for guard-banding in modes

[33mcommit a465bc21ddca1989a99672de686aa3bed136a8a6 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jul 14 00:36:30 2016 -0700

work in progress

[33mcommit f214dfc31539ede14c6e3e25d5418323e2b520bd [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jul 13 21:28:58 2016 -0700

moving to original modes

[33mcommit 342c670df2612b84f482a3c736df926baf6af7bb [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jul 14 00:39:39 2016 -0700

added logging function for debug

[33mcommit 897a14a0f4bde80d43d5bb8934cee876d7997b3f [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jul 13 06:56:29 2016 -0700

removed some unnecessary code in modes

[33mcommit 5bd89958c9980e0d3181c3e762d66ae2741da998[m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 12 23:55:36 2016 -0700

added CCM to modes, added AEAD_CHACHA20_POLY1305

[33mcommit 30e2ea1d398ffe072a67a71b1405d88ea36cae63[m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 12 23:51:55 2016 -0700

added CCM to modes

[33mcommit efb6a35c51ad88bea1b6e56d4784458d5e4091e4[m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 12 00:05:43 2016 -0700

added MODE class for block cipher modes

[33mcommit 7f1d0f90c84dcddbdfc1b43151ae2ccf0865fddb[m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 10 23:23:17 2016 -0700

fix to IV in ARIA code, debugged ARIA-GCM and ARIA-CBC in TLS

[33mcommit cfa9cb6e5bb6eb748b3120b32518e732b1dbf71b[m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 10 23:20:44 2016 -0700

fix to IV in ARIA code, debugged ARIA-GCM and ARIA-CBC in TLS

[33mcommit f188634f6779125bcffac494484fa26744dd7a8c[m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jul 10 16:11:59 2016 -0700

updates for TLS CHACHA and ARIA

[33mcommit 07dc68ccdc0b62a7c64d8276ebd7d49422c94f21[m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 9 21:33:00 2016 -0700

updates for SRTP-ARIA GCM and CTR

[33mcommit 172348f70ed05f7110fcff653cf8cbbf50bcfd18[m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 9 08:53:25 2016 -0700

updates for SRTP-ARIA mode

[33mcommit 7ee2e84c30df9ab21dc4f6dd349cd27dfc5e2eef[m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 9 01:20:58 2016 -0700

    updates for CCM mode

[33mcommit 9f3eac5ba375fefe75c661e35a8c52a208b0be10[m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jul 7 22:38:55 2016 -0700

    updates to ARIA for different modes

[33mcommit bdf84adfdb4eb8b7363e689b3910d4540cc1fd37[m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jul 6 22:26:09 2016 -0700

    debug of ARIA modes, ECB, CBC, CTR working

[33mcommit 5fd0c1e2ae101bd3ad64974b8b82d32e7557cd00[m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jul 5 21:14:46 2016 -0700

    debug of ARIA GCM mode

[33mcommit a26da7c42295de55fdb30bbc5d850592685d31b1[m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jul 4 23:10:40 2016 -0700

    added AEAD functions for CHACHA20_POLY1305, debug

[33mcommit eb83bd93a9e99fab9992d817c5c5085c38165a05[m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jul 4 00:43:13 2016 -0700

    debug of AEAD chacha/poly1305 in IPsec and TLS

[33mcommit 6436202d14e7d9a5055144a24e6f4cc02abc42ae[m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jul 2 16:24:41 2016 -0700

    added ARIA and CHACHA suites to TLS

[33mcommit 9b159b24f736f83d83ee5411f2dd284b33134597[m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 30 20:38:40 2016 -0700

    updates for tls authentication

[33mcommit 7c08437ee940d0c824ec2f4f56c8c25f6ca307c0[m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jun 29 08:26:59 2016 -0700

    updated doxygen

[33mcommit 0e10385ea0ddabbd1cbf0e88af9757329102ff7a [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 28 21:45:52 2016 -0700

debug of TCP/UDP over IP checksum

[33mcommit a95119ae7420e3d5772b067e9db7a3f40655bebf [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 28 20:10:26 2016 -0700

updates for IPv6 addresses

[33mcommit 32b2c09a14d0f067c8ab9b0755245a2c8d1a8643 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 28 01:25:52 2016 -0700

updates

[33mcommit 427213e028d7a476cd3c4fb892c0922b7124cdfc [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 28 01:22:55 2016 -0700

debugged checksums, update for IPv6 addresses

[33mcommit 8d133e2542265c7244f80f38f0b07c579ac17750 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jun 27 22:35:46 2016 -0700

added psuedo header documentation for UPD and TCP

[33mcommit 474590d488cdfcebacdea514bb08142ab3f81942 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jun 26 23:14:48 2016 -0700

updates for doxygen

[33mcommit 7f30e82dae903f2c4a50b8e0d7916c3244885b4e [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jun 26 02:09:28 2016 -0700

debugged wimax, fixed replay pretty print function

[33mcommit e3993717c3097a53147cc591c3aa4a3616abb691 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jun 25 01:08:21 2016 -0700

added wifi to protocolpp interface

[33mcommit 1718c47889fb01b6bd49ad1d908787be0c58af23 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jun 24 23:35:52 2016 -0700

updates for anti-replay

[33mcommit d0074cea3ad7092aa48c14b03db9f56fe626f05f [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 23 23:41:43 2016 -0700

WiMAX debug, doxygen updates

[33mcommit f89e35f5d9eda733ca0373bdef03533060f09f00 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 23 16:23:14 2016 -0700

added wifi and wimax with doxygen updates

[33mcommit c98ce89df05c8931bd19af3a98136b7f6a603b1d [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 23 16:19:08 2016 -0700

updates for doxygen, wifi working, replay support

[33mcommit 2ea49434b4c046f64122e3b835c6309637a4c4e0 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jun 22 23:26:00 2016 -0700

updates to create Poly1305 AAD and key according to RFC7634, updated CHACHA20 interface to pass the counter value, updated IPsec to always use a random IV

[33mcommit f6ea20a6c3796f5cf94241eadde73c7ebf41cd83 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jun 19 21:00:12 2016 -0700

debug of Wifi and doxygen updates

[33mcommit 1225372f7eab739e64093bcad967a7d481949ae9 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jun 17 21:34:56 2016 -0700

doxygen updates for wifi and wimax

[33mcommit fed659c5cbf37bad0a77a2fa71a98b05e627e829 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jun 17 21:34:15 2016 -0700

doxygen updates for wifi and wimax

[33mcommit 63b4a6881ad25962ff72f57940e941cfe57c1691 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 14 19:58:20 2016 -0700

doxygen updates

[33mcommit 02cd99808352d4c1120013b8e882189be329b51b [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 14 19:57:03 2016 -0700

simplified the interface, added some missing fields

[33mcommit c00fd28be4b2f3e8081e1d5a46193f86280a0d2c [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jun 13 21:02:04 2016 -0700

updates for ciphers interface

[33mcommit 44fc2242fa8bd1775a49a8aca130133bf757f9b8 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jun 12 23:33:28 2016 -0700

updates for wrapper to cryptopp engines

[33mcommit ab1ace17973853a57c13c28fce87f15e04c2f051 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jun 10 20:26:46 2016 -0700

updates

[33mcommit 014d1227ac4595d3d7b885b4932390d0fa85ca1e [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Jun 10 20:04:21 2016 -0700

updated TLS with Camellia encryption

[33mcommit ee9aa8124361f01710c54e2695132ecbfb1d3655 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 9 22:34:01 2016 -0700

debugged GCM and CCM in jtls

[33mcommit 4332bf004ef9d5514b49fd35241b50d414a59a1a [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jun 8 22:43:19 2016 -0700

updates

[33mcommit 56a8caf3c4d8200667719047a3a862f9dc557094 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jun 8 21:13:56 2016 -0700

updates

[33mcommit 23e4434b17efb22f2a16b2ce42e62c3b00a0f600 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Jun 8 19:12:34 2016 -0700

fix for zero padlen calculation

[33mcommit 27d185ecd98aae81e827a58b3f3f301a511968c7 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue Jun 7 22:34:55 2016 -0700

TLS debug

[33mcommit 5696c6ae055cc0cb7c360b8403a6e3be114b99c8 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jun 6 23:38:44 2016 -0700

TLS debug

[33mcommit fd3de8389b3b3e0ba481a34e465c0e3411dab7e4 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Jun 6 22:00:45 2016 -0700

debug for JTLS

[33mcommit a2f8d2bba44548fceb1ef1435648ffa6de789247 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Jun 5 21:42:46 2016 -0700

debug of GCM and CCM in IPsec

[33mcommit a29a8b5dc42b3a6a78cce53ba9c8f8d498c7f5e9 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jun 4 21:06:28 2016 -0700

doxygen updates

[33mcommit b31ff67e4bcae41f7987a59b882ff4e05a63b5a7 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jun 4 20:47:16 2016 -0700

doxygen updates

[33mcommit 30b51f350bdb507aab0ca84df2b1ac37d800c210 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jun 4 14:23:37 2016 -0700

doxygen updates for SRTP to add LaTex formulas

[33mcommit 3dac1a791111c320de3aa97c4410a8f0b156f8eb [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Jun 4 12:30:34 2016 -0700

debugged GCM and CCM modes in SRTP

[33mcommit 9c469aa903659ac11c5eb1f35bc7cc4f35274a0d [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu Jun 2 23:29:04 2016 -0700

updates to add GCM/CCM to SRTP

[33mcommit bdc1630c0ae0c74c0799aeec46a9c3ff2a413264 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon May 30 15:19:01 2016 -0700

doxygen updates

[33mcommit 1d44145f03a5f64037312f9a88fbdccd2555d8af [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon May 30 10:05:29 2016 -0700

updates for string constructor

[33mcommit 9f2447e6e2df06279d90f6fa5f84fde90c0c4a8f [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon May 30 06:58:49 2016 -0700

fix for string constructor to allow either encoded or simple strings to be passed

[33mcommit 9782ee9f8eacbdd066e4d0164d9dbcaf6c943c51 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun May 29 13:54:00 2016 -0700

added SRTP to test harness

[33mcommit 6af75302060245056dbbf2508a6aed373c8cfbbe [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun May 29 12:12:08 2016 -0700

debugged SRTP and jarray conversion constructor

[33mcommit 2ba94a061a30452f04f8085fe15b0c817a560ddb [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu May 26 22:20:01 2016 -0700

Doxygen updates

[33mcommit ffa08ff248a7a7fd74fee8b8067fe3f4f2e8a2a9 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu May 26 22:14:32 2016 -0700

SRTP debug

[33mcommit 0a758f8f12b5346a34af332bc8dec41574603b0e [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu May 26 21:45:32 2016 -0700

updates

[33mcommit 809b6e33064a1244c2267727b6e1017f0cfc6e58 [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu May 26 21:18:31 2016 -0700

SRTP debug

[33mcommit 100e24330077ddbf5a8656ba3e5fba7975439db4 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 25 22:29:23 2016 -0700

added SRTP protocol

[33mcommit cf362f963ef1b70d8a6dd4d289d1e6e64b5364c8 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 25 22:07:26 2016 -0700

added SRTP protocol

[33mcommit 85eb5f3baf5bececccc2570d02e387e9e554fd27 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon May 23 22:24:32 2016 -0700

updates

[33mcommit 3f98add6dcd19663368d91d64427e38887af30cc [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon May 23 19:51:50 2016 -0700

makefile for different targets

[33mcommit 55fc1b0889a15f5a39607309abf90995d4b49269 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat May 21 21:03:26 2016 -0700

fixes for status

[33mcommit 392dd15795b67b82a969aea56cd92a4dac47230c [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat May 21 20:58:18 2016 -0700

fixes for status

[33mcommit 9de5e1d228623a6649f8ef81dae0db36b1c4f586 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 18 23:34:39 2016 -0700

SImplified interfaces

[33mcommit 37b225c52bf7bf86eb6212f8677a1cd252face9a [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 18 23:29:22 2016 -0700

SImplified interfaces

[33mcommit 511bd346d1a6cbff7c11576c05de8791b0d78cb2 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 18 23:28:41 2016 -0700

SImplified interfaces

[33mcommit 92843b7e508929ab564936334623bf5762672eec [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed May 18 20:40:30 2016 -0700

Fixed IP to work correctly with templated source and destination

[33mcommit a60d296d88291b941221808b167320b442c22df5 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue May 17 22:05:38 2016 -0700

FIxed IPsec bug that was writing past the end of the output buffer

[33mcommit c850ad8deedb82725ad17bf386c6b9c5eada5065 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue May 17 20:34:54 2016 -0700

Added HTML Doxygen

[33mcommit 86f926d0aa8901a93cb7c2021f1d0c6309f20909 [m
Author: jgren <jgreninger@hotmail.com>
Date: Tue May 17 20:07:40 2016 -0700

Added set/get functions to reduce interface

[33mcommit 58319ca3d76cade0eaa39430299c9b10bf15f41c [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun May 15 22:37:43 2016 -0700

Added unit testing with cppunit

[33mcommit 6f404e6fb3259e08ec6cee859c1d79dcaf93c16c [m
Author: jgren <jgreninger@hotmail.com>
Date: Thu May 12 21:50:39 2016 -0700

Doxygen updates, interface simplifications

[33mcommit 920ecd6ed7d24d38ff402d14711717c1cf994075 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun May 8 14:23:24 2016 -0700

simpllified protocolpp interface

[33mcommit 564905908c55afbd4f7fedf1260f853c746ddbf1 [m
Author: jgren <jgreninger@hotmail.com>
Date: Wed Mar 23 21:19:44 2016 -0700

encryption support

[33mcommit b61f6db3c05a09fff5ce0a51d667b5361eb21b53 [m
Author: jgren <jgreninger@hotmail.com>
Date: Mon Mar 21 13:14:54 2016 -0700

encryption support

[33mcommit 3f555bfa349e289286c9cb5f636189443ffecb9b [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Mar 20 20:12:08 2016 -0700

Updated copyright

[33mcommit 5e4e1aaa23dca5022d0d9cd211db16ba642b877d [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Mar 20 18:10:33 2016 -0700

Updated doxygen

[33mcommit f0ac4bda0df981044d60599a0dc45206c8866f9b [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Mar 19 18:08:47 2016 -0700

changed some names

[33mcommit 573b5e8ae037ff2da5332cea69a8d0e4b3869b3f [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Mar 19 18:03:36 2016 -0700

Add POLY1305 and CHACHA20 to TLS

[33mcommit efdea4d465e01f1c96aac9ca63ef4b4870fa35b0 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Mar 18 21:13:26 2016 -0700

Add POLY1305 and CHACHA20 to TLS

[33mcommit 98a533a4a304f0156f5b99560584e6006f4e1120 [m
Author: jgren <jgreninger@hotmail.com>
Date: Fri Mar 18 21:05:47 2016 -0700

Add POLY1305 and CHACHA20 to TLS

[33mcommit 819131b41c8abeea0bd1fced580c4fc953a33c19 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sun Mar 13 16:26:10 2016 -0700

Debugged TLS

[33mcommit 9e543cf09ffb0e9c2c383de16f9496b92ab61fa3 [m
Author: jgren <jgreninger@hotmail.com>
Date: Sat Mar 12 23:59:29 2016 -0700

Debugged TLS

[33mcommit 2d754ae0b76b0517a2591ba06cb77494fee775e1 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Fri Feb 19 03:33:53 2016 -0700

Added factory class protocolpp

[33mcommit cf9a156e3fd0231fb8b98539d0a822cfc46c2f3c [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Wed Feb 17 21:10:08 2016 -0700

fixed function toarray write files to include status and convert directly from the input byte

[33mcommit e41e6786495f74616b1b60b58e63860b2381f87d [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Wed Jan 27 00:40:59 2016 -0700

Added GCM and CCM modes

[33mcommit 79f4b5a842c625198ee923b5eb11d181a65394db [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Tue Jan 26 22:11:29 2016 -0700

fixed function to write files to include status and convert directly from the input byte array

[33mcommit 3e9c4806c9558342d1de476c07a032bd8199d82f [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Tue Jan 26 22:01:50 2016 -0700

Added additional modes

[33mcommit 7dbe65b025b9c70d09b756d7e8940c21863af958 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Jan 17 20:34:09 2016 -0700

fixed function to write files to include status and convert directly from the input byte array

[33mcommit cdbced3cf89f80d9c770fc529e9f20a731c1f1a0 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Jan 17 17:20:57 2016 -0700

fixed function to write files to include status and convert directly from the input byte array

[33mcommit d6fc2ab665430e2b243b79b76170f1294c6291e1 [m
Author: John Greninger <sage4rplg>
Date: Sat Jan 16 23:56:12 2016 -0700

updated file functions to use shared pointers

[33mcommit f5a62ae89d64f3a266124311e7fcaeaf11826c6a [m
Author: John Greninger <sage4rplg>
Date: Sat Jan 16 22:54:23 2016 -0700

updated file functions to use shared pointers

[33mcommit 77357717c0605858a2c4f6708e5331458b30c199 [m
Author: John Greninger <sage4rplg>
Date: Sat Jan 16 20:46:58 2016 -0700

fixed bug when writing to file

[33mcommit 971b410d603030e2e3d153e6c3ca75218bb5161a [m
Author: John Greninger <sage4rplg>
Date: Thu Jan 14 23:21:15 2016 -0700

updated write function for file

[33mcommit 64046c18dc9814b12f162c67e649b6d5e4302436 [m
Author: John Greninger <sage4rplg>
Date: Sun Jan 10 01:13:55 2016 -0700

updated IPsec

[33mcommit 4a42de2e1cd94d67408444308acba33a77a0f8da [m
Author: John Greninger <sage4rplg>
Date: Sun Jan 3 21:50:06 2016 -0700

update

[33mcommit 8102c4256c5065dc3523356754da9197a66ec529 [m
Author: John Greninger <sage4rplg>
Date: Sun Jan 3 21:45:14 2016 -0700

updated IPsec

[33mcommit eecc0a7064d0467bc502b2a576c456785abe2c6b [m
Author: John Greninger <sage4rplg>
Date: Sat Jan 2 19:26:30 2016 -0700

updated IPsec

[33mcommit 82b854c021c80e5af2963fe9ce1f798bf0370d02 [m
Author: John Greninger <sage4rplg>
Date: Sat Jan 2 19:14:40 2016 -0700

Added IPsec

[33mcommit 2ffc8e3fe646b8f74a9892da2d8de4275dfa6cfa [m
Author: John Greninger <sage4rplg>
Date: Fri Jan 1 21:50:37 2016 -0700

Added ZUC and SNOW3G

[33mcommit febcb2576cfc8e8d20ea34f09053700ba46adf83 [m
Author: John Greninger <sage4rplg>
Date: Sun Dec 27 23:08:45 2015 -0700

updates to add Snow3g because Crypto++ doesn't have it

[33mcommit da52af1ece54eabec56f6e57a36a6191f3087638 [m
Author: John Greninger <sage4rplg>
Date: Sun Dec 27 22:59:09 2015 -0700

updates to add Snow3g because Crypto++ doesn't have it

[33mcommit 488ab205369bb310e1a5777e0913845c7cce951c [m
Author: John Greninger <sage4rplg>
Date: Fri Dec 11 21:01:52 2015 -0800

updates

[33mcommit 69742f7f4a9b3fefe503dddf4207cd1be7292104 [m
Author: John Greninger <sage4rplg>
Date: Sun Dec 6 01:18:44 2015 -0800

working with libcryptopp linked in

[33mcommit 581372fb65fb80232bb76078f0914f47a0cfd2a7 [m
Author: John Greninger <sage4rplg>
Date: Sat Dec 5 13:13:22 2015 -0800

MacSec AR debug

[33mcommit cc1c1e347db44d2ecf21c10d66436f87ce278dbc [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Tue Dec 1 01:16:46 2015 -0700

Doxygen updates

[33mcommit acc33ccbc314ece298c17df80b5c5f4daaca9cf9 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Mon Nov 30 23:37:41 2015 -0700

code clean up from static analysis

[33mcommit 2a398996d9ee7bd4771c37ab35aecae4528a847b [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Nov 29 20:38:47 2015 -0700

working macsec

[33mcommit fd07fb9ff56c8fec44e22bf5c2c233a9b310b07f [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Nov 29 01:33:44 2015 -0700

MACSEC debug

[33mcommit c29e35eee064ce482e0998bbec7687aadd408ff5 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Fri Nov 27 18:22:57 2015 -0700

added Doxygen configuration file

[33mcommit 111f36bf44d4b7b8eaab1f2aaa5d4fe34acd3511 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Fri Nov 27 00:07:53 2015 -0700

working with crypto++ linked in

[33mcommit 8e729521eb564c10daab24110ed148bbc109444f [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Thu Nov 26 21:33:45 2015 -0700

Further debugging

[33mcommit e7317176822fb1e9a9f4d7965e1901baef95434a [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Tue Nov 24 00:08:08 2015 -0700

anti-replay class

[33mcommit 0d75d0fa4755672cc39841ee0736aab639f746fb [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Mon Nov 23 22:27:44 2015 -0700

anti-replay class

[33mcommit 9d4a052c945b9ca1a63df270ef7a1482a76118a5 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Nov 22 11:47:42 2015 -0700

Debugged

[33mcommit d8700030cea94a822e12c2781d76e6776b930432 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Nov 15 00:33:13 2015 -0700

Debugged

[33mcommit 2914adeb452cb1e3a158125b020028c51c615fc8 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Wed Nov 11 21:27:14 2015 -0700

Debugged ENUMs

[33mcommit 68df87f67b40f1547ad99b0b5bb7eba1f7e32652 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Wed Nov 11 21:25:28 2015 -0700

Debugged TCP, UDP, IP

[33mcommit 786469f2225c907b35f51bfa5bb4f9b2c851e1ab [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Mon Nov 2 19:10:32 2015 -0700

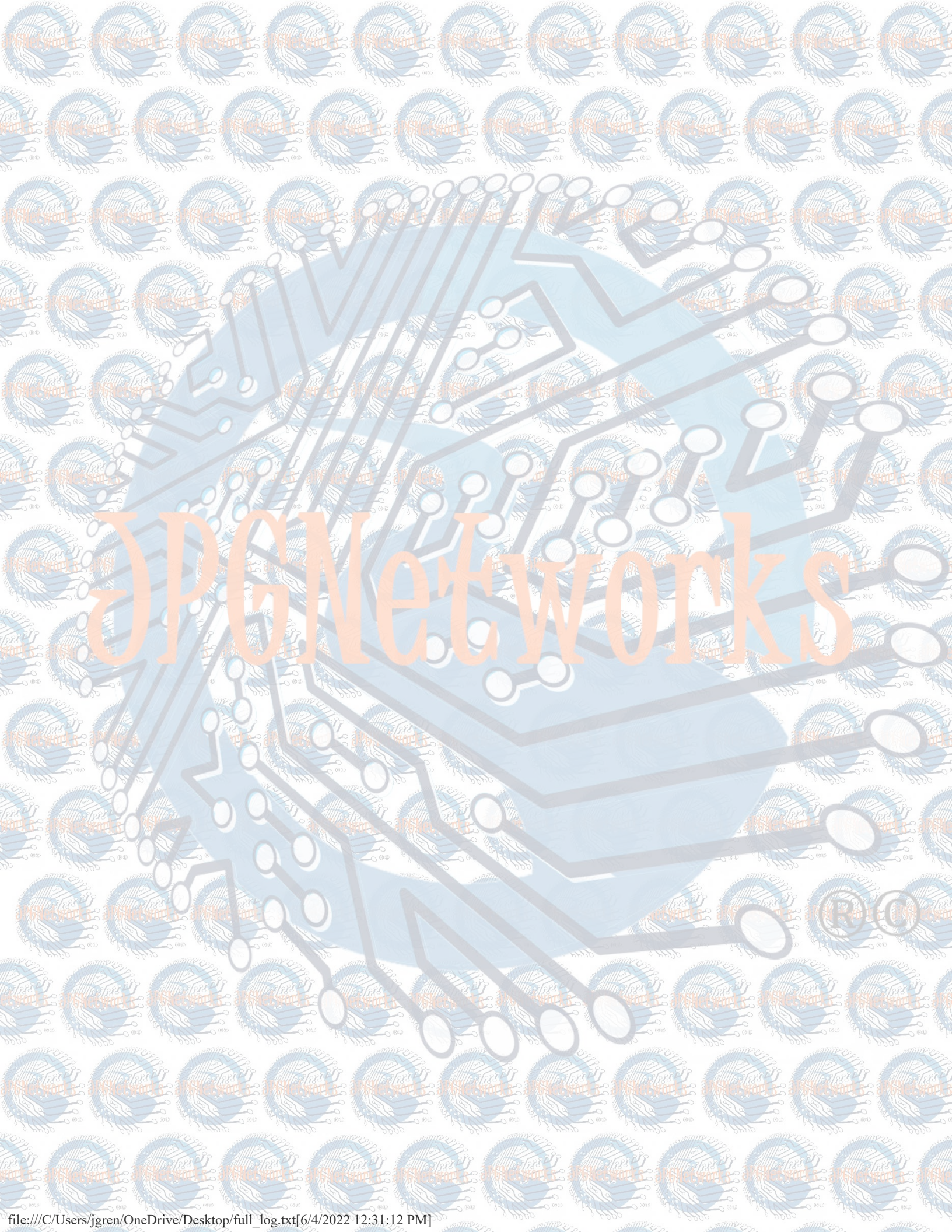
debug

[33mcommit 11a9f5c27f62ecdce6eefc5eda1a8d69de12b42c [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Tue Oct 13 22:29:39 2015 -0700

updates for move to new laptop

[33mcommit eb0f8c197a7c482647fbaee262459f27ecf4e837 [m
Author: John Greninger <jgreninger@mchsi.com>
Date: Sun Sep 20 15:20:06 2015 -0700

Initial checkin for jbuilder on new laptop


JPGNetworks