U.S. DEPARTMENT OF OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE



Automated, Disruption Tolerant Key Management System (ADTKM)

Pacific Northwest National Laboratory (PNNL)

Thomas Edgar, PM/PI

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Project Title

ADTKM

Objective

- Design a Key Management system to meet the unique requirements of EDS
- Disruption-tolerant
- Centrally managed
- Automated key management services for devices
- Self-monitoring system
- Integrated enterprise security

Schedule

- October 2015 January 2019
- Year 1: System design; research grade test kit Complete
- Year 2: Prototype system; component tests Complete
- Year 3: Experimentation/performance testing Complete
- Year NCTE: Open source documentation; Publishing



Total Value of Award:	\$1,900,000
Funds Expended to Date:	94%
Performer:	Pacific Northwest National Laboratory
Partners:	LBNL, ABB, Intel (Alterra), APS



Advancing the State of the Art (SOA)

ADTKM

Current key management architectures:

- Are not designed for machine-tomachine communication
- Are designed around "online" mentality
- Are often burdensome to manage (key distribution, revocation lists, governance, etc.)

ADTKM approach combines ideas from enterprise key management, identification, and authorization protocols:

- Kerberos cached authorization
- 802.1x device identity and authentication
- Self monitoring for attack detection



	1000		-	Let a second	8.97.2
the second second second second			1000	Conception in the second se	
in all of a long straight	117.25.9.1	10.00.00.0	PC I	ar to Linerar	
man-search have beinger	110.28.01.5	10.10.10.1	1.10	19 Mill + 2000 [102] SHOT WE'LL WE'LL WE'LL LINE DISCONTINUE (SHO HILDER)	
WARD-18-26 11(10) 24-11(10)	118.38.26.1	28.04.2.5	196	1/1P/0/11/arCio	
W.R.C. 19-36 1115 M.GOW	116.28.25.1	18.18.9.1	10	20 Rel + 5286 [403] 565-1 80-1655 228-1162 160-6 (200-111209) 567-502003	
102.001-00-00 10235 30 /01235	1.0.20.25.2	38,64[9.3	195	109 Continuation	
172 July 18-36 1725 M 412246	128.28.35.1	18.12.9.8	73.0	20 51205 + 361 (MR) SIG-126 40-125 82+2022 64+9 (Sell-12252) Toto-202000	
THE RESIDENCE BOOK OF 15 (422)	110.28.31.1	18.33.78.8	THET	71 Continuation	
112.001-10-30 10:05 30.00420	139.28.26.2	105.22.79.1	10	75 MG + 52001 [MU] Sec 135 Adv-1279 kth-11072 Lat-0 7540-1108.00 [Sec-000749]	
200 (0040-10-30) (00305 (30) (005250)	100.06.76.0	180.49.79.3	1941	106 Continuation	
704 3045-104-36 10255-36 102590	120.26.25.3	18.33.79.6	712	18 (2006 + aG 14001 Sec.1079 Act 200 kge-30072 Let 0 75wd-200500 There-3000100	
THE MAN TH M. ROOM M. COURSE	115 St 18.1	19.35 W I	1947	Un Continantio	
APR 2414 12 12 12 18 18 18 1911				- 19 A 19 1 19 1	



Challenges to Success

Comparison to 62351

- Worked with Triangle Microworks to update DTM to allow updating certificate expiration
- DTM is only fully implemented testable suite for 62351
- Only provides a CRL style key management and not the OCSP default mechanism
- Bias results for comparison

How to evaluate?

- Execute test cases against ADTKM prototype and IEC 62351 systems to quantitatively evaluate approaches
- Need implementation of IEC 62351 with key management
- Working with Triangle Microworks (DTM software)

Progress to Date

Major Accomplishments

- Open sourced technology developed under this project
 - Code and designs uploaded to Github (links in later slide)
- Created an RTU 61850 application
 - Provides Master and Slave interface between OPC server and relays
 - Necessary to enable test case system
- Executed laboratory testing of solution



Test Design

ADTKM



Phase 1 Baseline Test Setup

Phase 2 ADTKM Test Setup

Phase 3 IEC 62351 Test Setup



Test Setup













Testing

ADTKM

The sets days in provided the sets 1.1.2.1.8.001 5000. Public to connect replaced, enters could not connect to 102.17.6.0 1.1.2.1.8.001 5000. Public to connect replaced, enters could not connect to 102.17.6.01 on po- replaced to the set of	ADTKM emulated Relay device	Pa
CONTRECTOPTE.CONT. Namedice research of 201700.200912.CONT. CON, error lead-time to saw PM-DEC-THESTMPTPW-FK-AS-ID, as cals.[]] put as reg marked put sSD as response put sSD as response TGS reg processed put by lay response to the fill a response to the response to a second of the store store store store to the response to a second of the store store store store to the response store store to the response store store store store store store store to the response store store to the response store store store store store store store to the response store store store store store store store store store to the response store store store store store store store store store to the store (lettrand) (lettsponse store sto	22 Departs How/DE Mag 1 DMIDE (4.8-06.1.8) 32 Departs How/DE Mag 1 DMIDE (4.8-06.1.8) 42 Departs Add Tog 1 DMIDE (4.8-06.1.8) 43 Departs Add Tog 1 DMIDE (4.8-06.1.8) 44 Departs Add Tog 1 DMIDE (4.8-06.1.8) 45 Departs Add Tog 1 DMIDE (4.8-06.1.8) 46 Departs Add Tog 1 DMIDE (4.8-06.1.8) 47 Departs Add Tog 1 DMIDE (4.8-06.1.8) 47 To DMID DMIDE (4.8-06.1.8) 57 To DMID DMIDE (4.8-06.1.8)	Image: Control (Control (Contro (Control (Control (Control (Contro) (Contro) (Contro) (Contro) (C
pol a "42 pol a "42 central solution of the difference of the solutions Central solution of the difference of the solution of the solution of the solution of the solution of the solution of the solution of the solution of the the solution of the solution of the solution of the solution of the solution of the the solution of the solut	Encodestand (1973) Franceston (1974) Encodestand (1974) Franceston (1974) Franceston (1974) Franceston (1974) ADTKM emulated RTU device	Day Day Link Art, Nacht Dir (1.4.8.4.1) Link State Art, Link Art, Dir (1.6.8.4.1) The Link Art, Dir (1.6.8.4.1) Link State Art, Art, Dir (1.6.8.4.1) The Link Art, Dir (1.6.8.4.1) All Hind Art, Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) All Hind Art, Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) Bir Channett, Li The Hind Art, Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) Bir Channett, Li The Hind Art, Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) Bir Channett, Li The Hind Art, Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) Mind Art, Dir (1.6.8.4.1) Dir (1.6.8.4.1) Hind Art, Dir (1.6.8.4.1) Mind Art, Dir (1.6.8.4.1) Dir (1.6.8.4.1) Dir (1.6.8.4.1) Mind Art, Dir (1.6.8.4.1) Dir
Consider the second repropertiesmultipliance is interfaced repropertiesmultipliancemult	ит роф и. 22001.1 оро, к.1/ Норо, 53.12 оно ction	U.S. DEP

acket Manipulation

Det.	Line	Taturity.	destination .	Lypex.	
140	CHERRICHTERN	122-372-01-172-10300	10.1.1.1.1.0.00	100	F
193	10.44:45.155952	172.17.8.604.22	1.02.12.308.37-46918	MILEscryption packet	
1.24	10.44.46.115739	172.17.8.00.22	172.17.100.37:40018	SSH. Encrypted pecket	
195	15.41.45.156340	372.17.300.37.48018	172.17.0.00.12	T	
100	THERE'S AN A TRANSPORT	122.17.390.17:40418	577.17.0.981:37	- XP.	
19/	10145-60. 158.116	1/2 17 8 69-57832	177.17.0.11.0890	102	
100	10:44:40.138504	172.17.8.01.9968	172.17.0.00:37070	TOP	
1.00	10.41.46.117100	10.1.1.13:00	472.17.0.37.18902	UDP	
7.81	18:41:05.375358	107.17.8.882.21	3.07.17.106.50:00910	Shill screpted packet.	
201	10-41-41.171249	172.17-8-681.21	1.77.17.100.11-00410	Well incrumed raciost	
		T THE THE NEW AND AND AND AND	a sea and a second of		The second second second
enc 95 600 90 600 90 600 91 640 92 640 92 650 64 650 64 650 43 610 43	27 18 00 30 71 85, 1 BC 07 74 40 80 37 3 DC 06 08 05 33 85, 1 00 08 08 45 83 60 0 11 08 15 66, 81 61 0 81 57 18 21 84 41 0 84 60 20 84 85 83 84 61 40 45 85	1 10 75 30 44 00 00 4 7 10 157 11 14 20 N 2 10 157 15 14 14 20 N 2 10 25 51 14 15 25 14 15 0 17 14 25 26 26 25 14 15 0 17 14 25 26 26 26 25 36 22 31 0 17 14 26 <	5 60 · · · · · · · · · · · · · · · · · ·	5. Care-e	(1000000) E210002(000)



Collaboration/Technology Transfer

- Open source the project technologies developed under this project
 - Including:
 - ADTKM services: <u>https://github.com/pnnl/ADTKM</u>
 - Bro sensoring additions: <u>https://github.com/lbnl-</u> cybersecurity/dtkm-sparcs
 - BeagleBone Black development platform: <u>https://github.com/pnnl/ADTKM</u>
 - Coming soon:
 - Improved user documentation
 - Tutorials/Walk-throughs
- Comparative study to quantitatively showcase benefits and negatives
 - Contribute test cases and process to community for comparison of other existing or future solutions
- Interaction with DNP3 Secure Authentication
 - Expressed interest in maybe leveraging some of our approach in their Key management process
 - They are trying to get renewed funding for the DNP3 Key Management working group

Next Steps for this Project

- Write Technical documentation
 - User guide for tools
 - 2 papers planned for conference/journal submission
 - Paper documenting ADTKM approach and empirical evaluation results
 - Bro sensing analytics for Key Management

