

Contents

1. Introduction	1
1.1. Cyber Security in Smart Grids and IACS	1
1.2. Motivation	2
1.3. Research Scope and Objectives	3
1.4. Document Structure	4
2. Related Work	5
2.1. Attribute-based Access Control	5
2.1.1. Research	5
2.1.2. Application of ABAC in Smart Grids/IACS	6
2.2. Security Guidelines	8
2.2.1. NIST Framework for Improving Critical Infrastructure Cybersecurity	8
2.2.2. NIST NISTIR 7628 Guidelines for Smart Grid Cyber Se- curity	8
2.2.3. NIST SP 800-82r2	8
2.2.4. NIST SP 800-53r4	9
2.2.5. BDEW Whitepaper	9
2.3. Security Standards	10
2.3.1. ISO/IEC 270xx	10
2.3.2. IEC 62443	10
2.3.3. IEC 62351	11
2.3.4. IEEE 1686	12
2.3.5. NERC Critical Infrastructure Protection (CIP)	12
2.4. Research Projects and Standardization	13

3. Basic Concepts	15
3.1. Public Key Infrastructure	15
3.1.1. Components	15
3.1.2. X.509 Public Key Certificates	16
3.1.3. Attribute Certificates	18
3.1.4. Certificate Validation	20
3.1.5. Certificate Revocation	22
3.1.6. Directories	24
3.2. Access Control	26
3.2.1. Access Control Models	26
3.2.1.1. Commodities	26
3.2.1.2. Mandatory Access Control	27
3.2.1.3. Discretionary Access Control	28
3.2.1.4. Role-based Access Control (RBAC)	29
3.2.1.5. Attribute-based Access Control (ABAC)	31
3.2.1.6. Comparison of RBAC and ABAC	32
3.2.1.7. Hybrid RBAC-ABAC models	34
3.2.1.8. Additional Considerations	35
3.2.2. Access Control Components and Data Flow	35
3.2.2.1. Components	35
3.2.2.2. Credential Distribution	37
3.2.3. XACML	38
3.2.3.1. XACML Context	38
3.2.3.2. XACML Attributes	39
3.2.3.3. Policy Definition	40
3.2.3.4. Policy Evaluation	42
3.3. IACS and Smart Grid Control	44
3.3.1. System Architecture	44
3.3.2. IEC 61850	46
3.3.2.1. Scope	46
3.3.2.2. Data Model	47
3.3.2.3. Abstract Communication Service Interface (ACSI)	48
3.3.2.4. Specific Communication Service Mapping (SCSM)	49
3.3.3. Open Platform Communication Unified Architecture	50
3.3.3.1. Data Model	50
3.3.3.2. Service Definition	52
3.3.3.3. Comparison with IEC 61850	52
3.3.4. Security	53
3.3.4.1. Communication Security	53
3.3.4.2. Access Control	56

4. ABAC - Access Control System	59
4.1. ABAC Security Requirements	59
4.1.1. ABAC Trust Chain	59
4.1.2. Management Systems	60
4.1.3. Attribute Security	61
4.1.4. Access Enforcement	62
4.1.5. Access Control Policies	62
4.2. System Architecture	63
4.2.1. Management Systems and Directory	63
4.2.2. ABAC Module	65
4.3. Management Systems	68
4.3.1. Attribute Certificate Management	68
4.3.1.1. Attribute Certificate Specification	68
4.3.1.2. Data model Representation on Directory	70
4.3.1.3. Configuration of Device Data Models	73
4.3.1.4. Attribute Certificates for Subjects	75
4.3.1.5. Attribute Certificates for Objects	77
4.3.1.6. Attribute Certificate Revocation	78
4.3.2. Policy Management	79
4.3.2.1. Policy Configuration File	79
4.3.2.2. Policy Configuration - Security Aspects	82
4.3.2.3. XML Signatures	83
4.3.2.4. Directory Organization	83
4.3.2.5. Policy Configuration Updates	85
4.3.3. Secure Associations	85
4.3.4. LDAP Access Control	87
4.3.5. Synchronization	89
4.4. Environment Representation	90
4.4.1. Motivation/Background	90
4.4.2. The Environment Engine	92
4.4.3. Different Types of Observed Data Values	93
4.4.4. Situation/Condition Evaluation	95
4.4.4.1. Description Format	95
4.4.4.2. Situation Evaluation	96
4.4.4.3. Condition Evaluation	96
4.4.5. Observing Data Values	97
4.4.5.1. Data Observer Functionality	97
4.4.5.2. System Component Observer	97
4.4.6. Provided Environment Attributes	98

4.5.	Policy Information Point	99
4.5.1.	Functionality	99
4.5.2.	Synchronization of Object Attributes	100
4.5.3.	Synchronization of Subject Attribute Certificates	101
4.5.4.	Attribute Management	103
4.5.4.1.	Attribute Organization	103
4.5.4.2.	Querying Attributes	104
4.5.4.3.	Hierarchical Attributes	105
4.5.4.4.	Attribute Updates	106
4.6.	Policy Retrieval Point	107
4.6.1.	Functionality	107
4.6.2.	Policy Activation and Rollback	108
4.7.	Policy Decision Point	109
4.7.1.	Purpose	109
4.7.2.	PDP Configuration	110
4.7.3.	PDP Services	110
4.8.	Policy Enforcement Point	113
4.8.1.	Functionality	113
4.8.2.	Communication Security	113
4.8.3.	PDU Parser	115
4.8.4.	Enforcement of Access Decisions	115
4.9.	System Operation	117
4.9.1.	Initialization	117
4.9.1.1.	Initialization with available Directory	117
4.9.1.2.	Initialization from local Repositories	118
4.9.2.	Access Request Operation	118
4.9.3.	Connection Management	121
4.10.	Event Logging	124
4.10.1.	Logging of System State	124
4.10.2.	Logging of Transactions	126
4.11.	Static System Configuration	127
4.11.1.	Configuration Content	127
4.11.2.	Security Aspects	128
5.	Implementation	129
5.1.	Software Requirements	129
5.2.	Software and Libraries	130
5.3.	The Application Programming Interface	131
5.3.1.	API Design Aspects	131
5.3.2.	Connection Manager	133

5.3.3.	API of Dynamic Library	133
5.3.4.	Protocol-specific Functionality	134
5.3.4.1.	General API	134
5.3.4.2.	Environment Observer	134
5.4.	Integration of the ABAC Library	135
5.4.1.	General	135
5.4.2.	Implementation as Part of Application	135
5.4.3.	Implementation as Firewall	136
5.4.3.1.	Configuration and Security Aspects	136
5.4.3.2.	Protocol-specific Functionality as Plug-In	136
5.4.3.3.	Sequence Diagram for Firewall	137
5.5.	Policy Decision Point	138
5.6.	System Setups and Deployment	139
5.6.1.	Policy Decision Point	139
5.6.2.	Directory Server	139
5.6.3.	Deployment of an ABAC Module	140
5.7.	Access Control for IEC 61850	141
5.7.1.	Security for IEC 61850	141
5.7.2.	Service Description	141
5.7.3.	Attribute-based Resource Description	144
5.7.4.	Policy Design	146
5.7.4.1.	General Policy Design Aspects	146
5.7.4.2.	Implementation of Roles and Permissions	146
6.	Tests and Results	149
6.1.	Test Setup	149
6.1.1.	Clients and Server	149
6.1.2.	Policies and System Configuration	150
6.1.3.	Considered Scenarios	151
6.1.4.	Measured Times and Data	152
6.1.5.	Platforms	153
6.2.	Performance Evaluation	153
6.2.1.	Total Transaction	153
6.2.2.	Policy Evaluation	154
6.2.3.	Multiple Clients and multiple sub-requests	156
6.3.	Interpretation of Results	158
7.	Conclusion	161
7.1.	Summary of Results	161
7.2.	Future Work	163

