Federal Networking and Information Technology Research and Development (NITRD) Program

Tailored Trustworthy Spaces: Solutions for the Smart Grid

July 18-20, 2011

Arlington, VA

Workshop Report

Table of Contents

Executive Summary

The NITRD workshop on "Tailored Trustworthy Spaces: Solutions for the Smart Grid" was conceived by the Federal government to probe deeper into how Tailored Trustworthy Spaces, a strategic Federal cybersecurity research theme, could provide a framework for addressing cybersecurity challenges in the Smart Grid. Approximately fifty researchers from the power sector, academia, and the government met for three days and discussed critical concepts and challenges. This report summarizes the workshop's findings and puts forth key topics to serve as priority areas to guide further research and development activities.

Among the findings, it is important to note that Tailored Trustworthy Spaces have the potential to drive the development of more secure, trustworthy, and dynamic communications solutions that could allow third-party telecommunications providers to carry a greater range of Smart Grid transactions, instead of requiring the power utilities to build their own telecommunication networks and solutions. Consequently, Tailored Trustworthy Spaces could be an important business and economic driver to enable future Smart Grid capabilities.

The recommended top priority areas for further research are:

- Development of abstractions and methods to characterize Tailored Trustworthy Spaces and its properties in the Smart Grid
- Development of novel models and tools to allow tailoring of the security and trustworthiness properties based on the electrical state of the system
- Development of trust negotiation and the establishment of Tailored Trustworthy Spaces for fine-grained transactions

For further information about this workshop or follow-on activities, contact the National Coordination Office for the NITRD Program, 4201 Wilson Blvd., Suite II-405, Arlington, VA 22230, nco@nitrd.gov.

Report Co-Authors

Sandy Bacik
Principal Consultant
EnerNex

Isaac Ghansah
Professor, Computer Science and Computer Engineering, California State University of Sacramento

Himanshu Khurana
Senior Technical Manager
Honeywell

William Sanders
Professor, Department of Electrical and Computer Engineering, Director, Coordinated Science Laboratory, University of Illinois

Daniel Thanos
Chief Cyber Security Architect
GE Digital Energy

Andrew Wright
Chief Technology Officer
N-Dimension Solutions

Tim Yardley
Assistant Director, Testbed Services,
Information Trust Institute, University of Illinois

Acknowledgments

This workshop was sponsored by the Federal Networking and Information Technology Research and Development (NITRD) Program, the Office of Electricity Delivery & Energy Reliability of the Department of Energy, and by the Information Technology Laboratory of the National Institute of Standards and Technology. The workshop was organized and executed by the National Coordination Office for the NITRD Program, with support from Energetics Inc. For more information on the NITRD Program, visit http://www.nitrd.gov.

Introduction

The "Tailored Trustworthy Spaces: Solutions for the Smart Grid" workshop was organized by the Federal Networking and Information Technology Research and Development (NITRD) Program to examine research challenges in achieving Tailored Trustworthy Spaces (TTS) in the Smart Grid. The workshop took place during July 18-20, 2011 in Arlington, Virginia.

Tailored Trustworthy Spaces is one of the Federal cybersecurity research and development (R&D) themes[1]. TTS is a catalyst for cybersecurity solutions within a range of domains, including the healthcare sector, the financial sector, and the energy sector. These domains have a common requirement for dynamic, customizable, and secure environments in which to share information and conduct transactions. See Appendix A for a summary of TTS.

The TTS workshop convened experts from the power grid sector to pursue the following objectives:

- To review key use cases where TTS capabilities could be a significant factor in improving the delivery of the Smart Grid services and capabilities
- To identify important research needs and objectives to guide the development of TTS capabilities in the Smart Grid
- To identify opportunities for pilot projects
- To inform Federal government planning for R&D activities in TTS

In addition, the workshop contributed to the following outcomes:

- Provided input to help refine Federal cybersecurity R&D agenda to more effectively prioritize TTS research opportunities and challenges
- Supported Federal priorities in Smart Grid cybersecurity and interoperability
- Identified exemplary Smart Grid use cases for future TTS-oriented R&D activities
- Promoted exchange of information on TTS research challenges and goals and explored common TTS needs, requirements, and use cases

The workshop was organized with support from the National Institute of Standards and Technology (NIST) and the Office of Electricity Delivery & Energy Reliability of the Department of Energy (DOE/OE). Both agencies are at the forefront of the Federal government's efforts in modernizing the power grid and assuring its safety, reliability, and security. At NIST, the Smart Grid Interoperability Panel Cyber Security Working Group (SGIP–CSWG) coordinates the development of a framework that includes protocols and standards for information management to achieve interoperability of smart grid devices and systems, while maintaining the reliability and security of the electricity infrastructure. The DOE/OE works closely with the private sector to achieve the vision of the *2011 Roadmap To Achieve Energy Delivery Systems Cybersecurity* that, by 2020, resilient energy delivery systems are designed, installed, operated and maintained to survive a cyber incident while sustaining critical functions. Both agencies seek to understand how TTS capabilities can help achieve trustworthy and secure Smart Grid.

[1] "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," http://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

TTS in the Smart Grid

Background

Sometimes called the world's largest interconnected machine, the electric power system is the most capital-intensive infrastructure in North America.[2] The United States has embarked on a major transformation of its electric power infrastructure. This transformation is commonly known as the Smart Grid. This vast infrastructure upgrade—extending from homes and businesses to fossil-fuel-powered generating plants and wind farms, affecting nearly everyone and everything in between—is central to national efforts to increase energy efficiency, reliability, and security; to transition to renewable sources of energy; to reduce greenhouse gas emissions; and to reduce dependence on foreign oil. As the grid is modernized, and in order to more capably manage energy from a variety of distributed sources, it will become highly automated and leverage information technology more fully. Various industry groups are taking steps to evolve the nation's electric power grid into an advanced digital infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy. Given that over 80% of the physical assets that make up the grid are privately owned, coordination and collaboration between the public and private sectors is essential to securing this vital infrastructure and ensuring safe and reliable delivery of high-quality electricity[3]. This transformation will take place over many years. However, in the process of becoming increasingly "smarter," the grid will expand to contain more interconnections that must, and are, being protected to prevent their becoming portals for intrusions, error-caused disruptions, malicious attacks, and other threats.

The convergence of the information and communication infrastructure with the electric power grid introduces new security and privacy-related challenges. However, this fusion of technologies also presents opportunities to further increase the reliability of the power system and to make it more capable and more resilient to withstand cyber attacks, equipment failures, human errors, natural disasters, and other threats. Greatly improved monitoring and control capabilities should enable better cybersecurity solutions. Cybersecurity is one of the key areas that will benefit from further advanced research to stay ahead of the next-generation functional, reliability, and scalability requirements of the Smart Grid. A case in point is the central focus on cybersecurity in smart grid deployments and pilots being funded by the American Recovery and Reinvestment Act of 2009, which requires that cybersecurity plans must be approved and implemented for each of the projects. In turn, this requirement is motivating research in directions that have the opportunity to provide next-generation cybersecurity capabilities. In this context, TTS has rich potential for further advancing the cybersecurity protections that are currently in place.

Smart Grid systems have a unique set of properties that include complicated, inter-dependent cyber-physical systems with varying combinations of timeliness, safety, and availability requirements. These properties can be more easily, adequately, and economically achieved by pursuing next-generation

[2] Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, *Critical National Infrastructures*, April 2008.
[3] See http://www.eia.gov

research directions, such as TTS. With appropriate research and development, TTS can be a catalyst to drive the necessary security and resilience properties in economically and commercially viable solutions.

Economic Case for TTS in the Smart Grid

TTS focused R&D offers the promise of addressing the need of higher-grade security and reliability while making use of more modern technologies and public infrastructure. The primary benefits of realizing TTS capabilities for Smart Grid systems are economics, safety, security, and reliability.

The wide geographic dispersal of many of the endpoints of Smart Grid systems drives a strong need for secure and resilient communications. However, different subsystems have different security and resilience requirements. For example, smart meter communications require a strong degree of privacy but only modest availability and low timeliness. Substation control communications require a high degree of integrity, availability, and timeliness, as well as resilience both against traditional node or link failures and power supply resilience so that control of substation equipment can be maintained in the face of a power outage, but low confidentiality. Synchrophasor communications used for wide area monitoring and control require high bandwidth, high integrity, low latency, and low jitter, but only low to moderate confidentiality. These varying and in some cases unique security and resilience requirements make it difficult for Smart Grid systems to utilize current broadband, cellular, and other carrier data networks, even in metropolitan areas where such networks are ubiquitous. Carrier networks do not currently offer the ability to control the full suite of end-to-end properties needed for Smart Grid systems, such as confidentiality, integrity, availability, timeliness, latency, jitter, provenance, authorization, etc. TTS could enable carriers to offer communications networks with tailorable security and reliability properties that could provide Smart Grid communications at much lower cost than building special purpose dedicated networks for Smart Grid functions as is done today.

A further economic benefit through TTS would be enabling Smart Grid communications to evolve along with common communications technologies. One of the current challenges in building and securing the Smart Grid is a significant installed base of legacy systems that use older (sometimes proprietary) and often very slow communications. For example, 9600 baud serial radio or leased lines are quite common, but these links are at least two orders of magnitude slower than a typical residential broadband Internet connection. Nevertheless, new equipment operating at these speeds is being installed today. These speeds make security solutions that require greater bandwidth impractical. Many of the new—and proprietary—mesh networking Advanced Metering Infrastructure (AMI) systems are about one order of magnitude faster than legacy serial equipment, but are still one to two orders of magnitude slower than today's typical residential broadband connection. Assuming communications technologies continue to evolve as they have done over previous decades, today's new Smart Grid communications systems will become the legacy systems of the next decade or sooner, operating at speeds far below what will then be available to ordinary consumers, resulting in challenges to security and deployment of new applications. By utilizing TTSs available from carrier data networks, Smart Grid communications could evolve as carriers upgrade networks, and enable security and applications advances for utilities just as for other businesses and ordinary consumers. Hence, TTS-capabilities put Smart Grid systems on the rising side of the innovation and cost optimization curve while offering these needed benefits:

- Decreased costs
- Sustainability
- Increased innovation and capability
- Ability to upgrade
- Scalable interoperability
- Cross-cutting benefits to other critical infrastructures
- Decreased barriers to entry for introducing increased functionality in areas of security, safety, reliability, and resiliency
- More efficient and responsive power markets
- Productivity increases through enhanced and pervasive automation

Smart Grid Capabilities Enabled by TTS

Smart Grid systems provide both the basic infrastructure and advanced communications within the electric utility sector. TTS can drive new solutions in the Smart Grid by advancing capabilities in the following areas:

Security:

- Trust negotiation and data trust models to support transactions between domains and systems within the Smart Grid
- Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path, especially when Smart Grid transactions are transmitted cross-domains
- Enhancing consumer privacy when dealing with Smart Grid applications and devices and how the Smart Grid usage data is created, stored, transmitted, and destroyed after use
- Enabling "Tailored Cyber-Physical Power Space," a new cyber-physical model where the physical (electrical) system state is used as an input to the establishment and operation of tailored trustworthy spaces

Recovery:

- Disaster avoidance such as compensating controls and defining trust domains to prevent or limit a compromise. Such controls should include policies, processes, and advanced intrusion detection systems that can detect both malicious insiders and outsiders.
- Enhanced reliability and redundancy techniques to assure that when operational cybersecurity is affected, actions such as automatic rerouting or islanding of Smart Grid assets can take place
- Enhanced resiliency through compensating controls such as when defining domains of trust the utility has built-in defense in depth within each trust domain to prevent the spread of malware within the Smart Grid assets

Interoperability:

- Platform security mechanisms and trust-in-platform establishment within Smart Grid legacy systems being used with new technology
- Defining migration paths and better integration from legacy technologies to modern paradigms

Challenges and Recommendations for R&D in TTS

A number of topics related to security, tailored trustworthy spaces, and the Smart Grid were discussed during the 3-day workshop. A summary of the topics is provided in the Workshop Proceedings section on page 12. In the opinion of this report's co-authors, the following areas characterize the critical research subjects that should be pursued in order to realize TTS benefits in the Smart Grid:

- Abstractions and Methods to Characterize a TTS and its Properties
- Tailored Cyber-Physical Power Spaces
- Trust Negotiation and TTS Establishment for Fine-grained Transactions

Abstractions and Methods to Characterize a TTS and its Properties

A TTS is a concept of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements in the face of an evolving range of threats. Entities can join a space and leave a space. Entities that violate rules can be denied participation in the space. To achieve these capabilities, users of the TTS need a common set of rules that govern a specific trust environment. Some research challenges include the creation of a common specification language of the rules of engagement, developing a protocol to determine which rules are used for a particular situation (also called tailoring), and developing methods to implement these tailored rules. A common trust model with properties and attributes that can be scaled up or down depending upon the size of the utility is needed to allow utilities of different size to participate. Mechanisms are needed to change the rules to deal with evolving threats. Some questions to be answered include: how are rule violations detected, who changes the rules, and how are rules communicated to participating entities effectively?

Conceptually the Smart Grid consists of a set of TTSs with clear boundaries delineating where each trusted space is required to have different trust properties. The following are examples of spaces with different properties that could exist in the Smart Grid:

- Customer premises (high confidentiality, low integrity)
- Billing data and management of user data (high integrity)
- Supervisory Control and Data Acquisition (SCADA) (high availability, integrity)
- Synchrophasor communication for Wide Area Situational Awareness (WASA) (high integrity, timeliness, bandwidth)

Because end-to-end communication could potentially involve data flowing through multiple spaces, a common language is also needed to deal with cross-space transactions as well as ways to deal with trust negotiations, detection of trust violations, etc. For instance, one objective could be to tailor authentication and authorization mechanisms to specific requirements where the requirements could be high integrity, medium integrity, etc. How is this accomplished? How do we formally describe this to permit machine to machine automation and how do we verify that the requirements are met in a formal way so that any entity can trust it?

Another area where a common language is needed is metrics. Metrics can be used to tailor the trustworthy space to satisfy certain requirements. Metrics involve measurement of attributes. The research challenges are to develop a standard specification language needed to specify attributes, how attributes are measured, and how they are used. For instance, consider resilience which is a measure of availability. Given that availability is an important requirement in the Smart Grid how can resilience be measured in the smart grid system? What meaning can be attached to a specific measure of resilience? Which resilience value is adequate in a specific system? Formal specification methods are also needed to allow TTS entities to understand metrics and to deal with metrics.

When any Smart Grid domain electric utility has a transaction that includes usage data relating to a customer or business, the utility needs to ensure that data at creation, in transit, in storage and finally in its destruction the data are protected in accordance with its level of importance to the utility, and that compliance with applicable federal, state, local, tribal, and territorial laws and regulations is maintained.

Lastly, the abstractions and methods that characterize a TTS and its properties need to be linked to business and operational objectives. Research is needed to define how business and operational objectives can be translated to TTS requirements. When a utility develops business drivers for enhancing their Smart Grid operations, the research into attributes and properties could assist the utility in defining metrics and measurements to target the utility's operational performance to enhance resiliency and improve the protection of the utility's Smart Grid assets. After the business attributes and properties have been researched, the security attributes can be mapped to security properties and attributes to protect Smart Grid information transactions and assets. Areas of research include the following types of business attribute classes and properties:

- User, which relates to the users' experience of cybersecurity within the system, subsystems, and use of personal and business information
- Management, which relates to the governance of the utilities' smart grid assets
- Operational, which relates to the concerns of protecting data during day-to-day operations
- Risk management, which comprises a set of cybersecurity requirements and properties to identify and manage business risks
- Legal and regulatory, which covers current and future compliance issues
- Technical strategy, which addresses the strategic aspect of the technical cybersecurity architecture
- Business strategy, which are the utility's senior management and board of directors objectives

Tailored Cyber-Physical Power Spaces

Electric grid systems are designed to be adaptive in the presence of failures via either feedback loop control or supervisory control. As monitoring and control systems of the grid get "smarter," the computer and communication systems themselves need to be adaptive – but, in this case, to both failures and attacks. Consequently, the dynamic power grid adaptations in the generation and delivery of electricity need to also affect the security posture of the involved components (for example, an idle power source can operate under relaxed security requirements vs. a power-generating source that's critical to meeting the instantaneous power consumption needs, whose security is vital). In the face of

cyber attacks, a complex inter-connected system like the electric grid needs capabilities for dynamically adapting its security policies, associations, and postures so it can effectively detect attacks, contain them, mitigate consequences, and maintain delivery of electricity in the underlying physical network to consumers.

In considering such adaptations there are tradeoffs that must be considered carefully. For example, (a) emergency conditions require overrides of access policies and temporary increases in assigned accesses to users, however, these same overrides can be potential backdoors whereby an adversary can fake the emergency and then use the increased accesses as part of the attack, (b) detection of an attack in one part of the network (say an important transmission substation) may create suspicion about neighboring parts of the network with similar architectures and components, however, traditional approaches that take suspicious components offline for forensics analysis are not acceptable as they can impact the mission of continuous power delivery, (c) presence of exposed embedded components (e.g., substation intelligent electronic devices or field devices in distribution networks) provide opportunities for compromise and malware injection, however, tamper detection solutions must be cost-competitive for commercial viability.

In realizing TTSs for the Smart Grid the above-mentioned adaptation refers to the scope and flexibility of "tailoring" the TTS and includes changes to security policies, associations, and posture. In cyber-physical systems like the electric grid there is an opportunity to leverage measurements and control of the cyber and physical components to address this gap and create novel means of flexible and trustworthy TTS tailoring. For example, if a particular access control system is used for authenticating measurement data streams and the emergency requires that the access control be removed, a certain level of authentication could be achieved by comparing the received data with authenticated streams of neighboring data. Given the well-defined nature of power flow one can calculate expected variation in data in a certain neighborhood thereby allowing certain relaxation of security posture that would not be possible otherwise.

Benefits from utilizing the power grid electrical state to affect the security state will necessitate advancements in our capability to model the dependencies between the physical and cyber, and in securing the interaction between the two. At the time when the security decisions use the physical contextual information, e.g. data obtained from sensors and other devices, the contextual information has to also be trustworthy.

Research is needed to develop novel solutions that take advantage of such cyber-physical interactions to create flexibility in TTSs and address the type of tradeoffs mentioned above. Questions that can be addressed by research in this area include:

- How can we leverage the modeling, characterization and real-time data/measurement analysis of the underlying physical network to detect, contain, and work around malicious activity?
- How can we secure the interaction between the electrical state and the cyber world?
- How can we design flexible security technologies that deal with rare events such as emergency overrides as a seamless component of the overall security solution?

- Can we realize cost-effective end-to-end security taking exposed end points with limited resources into account that provide an equivalent alternative to more costly hardware enabled-trust approaches?

Trust Negotiation and TTS Establishment for Fine-grained Transactions

Today, electric grid transmission systems operate in a highly structured, hierarchical, and monitored environment. Distribution systems, while not so structured or regulated, work on the basis of bilateral (e.g., between a utility and a customer) and multilateral agreements. Emerging Smart Grid applications, such as Demand Response that aim to manage aggregate load of multiple customers, built on these environments use a combination of structure and agreements to achieve their objectives. However, in the future, we see the need to enable scalable and ad-hoc transactions between many different kinds of entities to truly realize the Smart Grid vision. For example, consider extensive use of fast and scalable Demand Response, leveraging distributed storage of solar panels and similar devices across wide geographic locations, efficient use of flexible loads such Plug-in Hybrid Electric Vehicles (PHEVs) whose charging and discharging patterns must be protected from adversarial manipulation, management of Distributed Energy Resources (DERs) where individual customers may generate electricity and sell it to the grid, and scalable renewable integration. All of these capabilities require the existence of a computing and communication infrastructure that can allow ad-hoc messaging and command and control transactions to be established and executed among relevant entities. Ensuring that these transactions are trustworthy is paramount as adversarial actions can lead to significant impact and damage to grid systems.

TTS offers rich potential for advancing today's technology that is currently being implemented in the Smart Grid to mitigate these risks. TTSs enable trustworthy fine-grained and transient transactions. For example, a parking lot with PHEVs should be able to dynamically optimize the charging and discharging of the vehicles in the lot by interacting with local and remote load systems, learn about and analyze market and pricing information, and balance the policies of individual vehicle owners. Properties of importance to TTSs that can help realize such capabilities include authentication and authorization of all relevant grid entities; trust negotiation to establish necessary security associations; secure networking that can support necessary confidentiality, integrity and availability requirements; effective logging, auditing and non-repudiation support; verification of security attributes of transactions; and efficiency and timeliness for transactions. A TTS capability that addresses all these properties goes beyond the type of negotiated security spaces provided by today's technologies and requires an exploration into new mechanisms, security components, protocols and their secure composition. For instance, both authentication and authorization requirements mentioned above requires the use of trusted identities. Providing such trustworthy identification of devices (e.g., PHEV, meter, substation components, etc.) for end-to-end transactions will help to deal with TTS violation incidents more effectively once they are detected.

Research is needed to develop novel solutions that enable trustworthy fine-grained and transient transactions across Smart Grid components and systems. Questions that can be addressed by research in this area include:

- How can we create trusted end-to-end interactions for Smart Grid applications that involve large numbers of devices with limited capabilities, lack of global identities, complex sensing and control applications, and human-in-the-loop decision support?
- Can we develop trustworthy communication systems that allow secure ad-hoc interactions among disparate Smart Grid components and sub-systems to realize scalable participation of consumers and other Smart Grid stakeholders for advanced applications?
- How can we develop new lightweight trust management mechanisms that establish trust relations among Smart Grid components and sub-systems with limited infrastructure support?
- What operational quantitative security and reliability models, metrics, or analytics can be used to optimize tailoring of properties to meet certain trust objectives and to assess the benefits of TTS?
- Can existing frameworks, such as the Security Content Automation Protocol (SCAP)[4], be extended and utilized for TTS establishment in the Smart Grid?

[4] See http://scap.nist.gov/index.html

Workshop Proceedings

This section of the report lists key challenges and R&D objectives identified by workshop participants. The challenges and R&D objectives are provided as further input to shape future R&D directions related to TTS and the Smart Grid. The challenges and R&D objectives below received the highest ranking by the participants during workshop discussions.

Key Challenges and R&D Objectives for Implementing TTS in the Smart Grid

The participants discussed the following questions: What limitations, barriers, and challenges prevent utilizing TTS approaches and scenarios for the Smart Grid? What R&D is needed to address the limitations, barriers, and challenges to achieving TTS?

- Develop business models for TTS
    - Develop appropriate security metrics and language to communicate TTS goals
- Meta language for TTS properties
    - Develop meta-language for characterizing TTS properties
    - Develop light-weight distributed control protocol for negotiation of tailoring capabilities
- Models and methods for TTS properties in the Smart Grid
    - Develop methods to identify and quantify needed trust level for a given space/mission/task. How to identify (quantify) current (actual) “trust” level for the space/mission/task
    - Develop methods to ensure properties of TTS end-to-end
    - Develop capabilities to be able to place different levels of trust in operational data based on different tailorable options for authentication/validation, cryptography, etc.
    - Coordinate types of trust and anchors in (a) public key infrastructure (PKI), (b) trusted computing, (c) virtualization into a meaningful whole
    - Develop models that can describe the effect of TTS choices on the performance of the Smart Grid
- Cyber-physical models
    - Develop methods to use both physical (electrical) and cyber state information to drive tailoring
    - Develop methods to use power flow network’s system management, redundancy, and other existing utility capabilities for meeting TTS requirements
- Key management
    - Scalable, manageable, and trustworthy key management services are currently inadequate for TTS requirements
    - Develop capabilities for compromise reporting and revocation status dissemination that is usable across spectrum of low to high constrained devices
    - Develop PKI methods that address user authentication and device authentication
    - Develop tools and techniques for large scale key distribution and revocation

    - Develop efficient key management schemes for large scale resource constrained systems
- Automatic detection of policy violation within TTS, e.g., privacy policies
    - Develop capabilities to regulate automatic configuration of combinations of TTS spaces based on high level policy goals
    - Develop methods to verify what current TTS configuration satisfies security goals
    - Achieve verifiability: develop methods to validate that desired security objectives have been correctly implemented
- Recovery
    - Develop capabilities to detect, compare, and recover from compromised space
- Visualization
    - Visualization of the domain policy, domain interfaces, interaction to aid with TTS configuration
    - Tools that utilities can use to model environments and visualize changes in trust levels
- Experimentation and pilots
    - Establish a “small grid city” for TTS and build test environments for experimentation with TTS and interoperability
- Legacy devices and systems
    - Develop tools to extract TTS attributes and properties for legacy systems and configurations
    - Elevate the need for interoperability consideration in research

Recommended Smart Grid Use Cases for Further TTS Research

In conjunction with the workshop, three use case areas were identified to help focus further TTS research activities in the Smart Grid. The use case areas were selected from the published NIST cybersecurity use cases (see Chapter 10 of the NIST Interagency Report (NISTIR) 7628, vol. 3, August 2010) by the workshop organizers based on the input from sector subject matter experts. The experts participated in two rounds of reviews, where each expert individually ranked NISTIR 7628 use cases in the order of their relevance and applicability to the vision and goals of Tailored Trustworthy Spaces.

The three use case areas focus on: (a) Transmission Operations, (b) the management of distributed energy resources (including integrating PEVs), and (c) the need that end-user devices communicate with utilities and that utilities have certain means to communicate back to those devices. Each use case area combines two NISTIR 7628 cybersecurity use cases:

Transmission Operations Use Case:

- Transmission Operations / Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data (NISTIR 7628, page 129)
- Transmission Operations / Real-Time Emergency Transmission Operations (NISTIR 7628, page 131)

Distribution Automation Use Case:

- Distribution Automation / Distributed Energy Resources Management (NISTIR 7628, page 121)
- Demand Response / Mobile Plug-In Electric Vehicle Functions (NISTIR 7628, page 105)

Customer Interfaces Use Case:

- Customer Interfaces / Customer's In Home Device is Provisioned to Communicate With the Utility (NISTIR 7628, page 106)
- AMI / Remote Connect/Disconnect of Meter (NISTIR 7628, page 95)

The experts who participated in the use case selection were: Sandy Bacik, EnerNex; Rakesh Bobba, University of Illinois; Bobby Brown, EnerNex; Frances Cleveland, Xanthus Consulting; Mark Enstrom, Neustar; James Ivers, SEI; Himanshu Khurana, Honeywell; Howard Lipson, SEI; Rhett Smith, Schweitzer Engineering Laboratories; Tim Yardley, University of Illinois.

See Appendix B for the list of the use cases.

Workshop Participants

Last Name	First Name	Title	Organization
Bacik	Sandy	Principal Consultant	EnerNex
Bobba	Rakesh	Research Scientist, Information Trust Institute	University of Illinois
Braden	Robert	Supervising Computer Scientist, Fellow, Information Sciences Institute	University of Southern California
Brenton	Jim	Regional Security Coordinator	ERCOT
Cleveland	Frances	President and Principal Consultant	Xanthus Consulting
Coop	Mike	Co-Founder, Managing Director	ThinkSmartGrid
Drummond	Rik	Principal	Drummond Group
Elliott	Karl	CTO	Aunigma Network Solutions
Enstrom	Mark	Product Management Director, Advanced Technologies Group	Neustar
Frogner	Bjorn	Entrepreneur-in-Residence	University of Maryland Baltimore County
Gammel	Dennis	R&D Manager	Schweitzer Engineering Laboratories
Garrard	Ken	Founder/CEO	Aunigma Network Solutions
Ghansah	Isaac	Professor, Computer Science and Computer Engineering	California State University of Sacramento
Greenberg	Alan	Technical Director, Cyber and Information Studies	Boeing
Ivers	James	Technical Lead, smart grid security architecture	Software Engineering Institute
Katz	Jeffrey	Chief Technology Officer, Energy and Utilities Industry	IBM
Khurana	Himanshu	Senior Technical Manager	Honeywell
Kravitz	David	Principal Member of the Technical Staff	Certicom
Kundur	Deepa	Associate Professor, Department of Electrical & Computer Engineering	Texas A&M University
Lindqvist	Ulf	Program Director	SRI International
Lipson	Howard	Senior Member of the Technical Staff, CERT, Software Engineering Institute	Software Engineering Institute

Molitor	Paul	Director of Smart Grid and Strategic Initiatives	National Electrical Manufacturers Association
Montgomery	Austin	Program Lead	Software Engineering Institute
Neuman	Clifford	Director, USC Center for Computer Systems Security, Information Sciences Institute	University of Southern California
Rasche	Galen	Technical Executive - Cyber Security	Electric Power Research Institute
Reynolds	John	Consultant	Drummond Group
Sanders	William	Professor, Department of Electrical and Computer Engineering, Director, Coordinated Science Laboratory, University of Illinois	University of Illinois
Sinopoli	Bruno	Assistant Professor, Electrical & Computer Engineering Department	Carnegie Mellon University
Sorebo	Gilbert	AVP/Chief Cybersecurity Technologist	SAIC
Thanos	Daniel	Chief Cyber Security Architect	GE Digital Energy
Tudor	Zachary	Program Director	SRI International
Wright	Andrew	Chief Technology Officer	N-Dimension Solutions
Yardley	Tim	Assistant Director, Testbed Services, Information Trust Institute	University of Illinois

Government Presenters

Last Name	First Name	Title	Organization
Dodson	Donna	Division Chief Cybersecurity Advisor	National Institute of Standards and Technology/Information Technology Laboratory
Kenchington	Hank	Deputy Assistant Secretary for R&D	Department of Energy/Office of Electricity Delivery & Energy Reliability
Muoio	Patricia	Member, Senior Steering Group	NITRD Cyber Security and Information Assurance R&D
Swanson	Marianne	Senior Advisor, Information System Security	National Institute of Standards and Technology/Information Technology Laboratory
Hawk	Carol	Program Manager, Cybersecurity for Energy Delivery Systems	Department of Energy/Office of Electricity Delivery & Energy Reliability
Ferraiolo	David	Group Manager, Security Research Group, Computer Security Division	National Institute of Standards and Technology/Information Technology Laboratory
Vagoun	Tomas	Cybersecurity R&D Technical Coordinator (Contractor)	National Coordination Office for the NITRD Program
Wagner	Grant	Technical Director, Trusted Systems Research Group	National Security Agency
Weber	Sam	Program Director, Directorate for Computer & Information Science & Engineering	National Science Foundation

Appendix A: Tailored Trustworthy Spaces

The following is a description of Tailored Trustworthy Spaces from "NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) Cybersecurity Game-Change Research & Development Recommendations," available at http://cybersecurity.nitrd.gov/page/federal-cybersecurity-1:

TTS provides flexible, adaptive, distributed trust environments that can support functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats. A TTS recognizes the user's context and evolves as the context evolves. The user chooses to accept the protections and risks of a tailored space, and the attributes of the space must be expressible in an understandable way to support informed choice and must be readily customized, negotiated and adapted. The power of the tailored spaces theme lies in the capability to:

- Articulate and negotiate the security requirements of the situation at hand
- Adjust the assurance level on specific security attributes separately
- Establish trust between systems based on verifiable information that test the limits of traditional trust policy articulation and negotiation methods, raising the bar for highly dynamic human understandable and machine readable assured policies. This necessitates the development of dependable methods of separating and isolating processes operating from small trust islands in a largely untrustworthy system

The primary goal of the tailored spaces theme is to identify and develop a common framework that supports varying trustworthy space policies and services for different types of actions. These policies and services will provide visibility into rules and attributes of the space to inform trust decisions, a context specific set of trust services, and a means for negotiating the boundaries and rules of the space. This framework will offer assurance that user requirements are accurately articulated in the TTS policy, that these spaces are truly separate, and that build-up and tear-down of the space is clean and trustworthy.

The scientific challenge of tailored spaces is to provide the separation, isolation, policy articulation, negotiation, and requisite assurances necessary to support specific cyber sub-spaces. Research is required to develop:

- Trust negotiation tools and data trust models to support negotiation of policy
- Type-safe languages and application verification, tools for establishment of identity or authentication as specified by the policy
- Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path
- Resource and cost analysis tools
- Hardware mechanisms that support secure bootload and monitoring of critical software

- Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments
- Application and operating systems elements that can provide strong assurance that the program semantics cannot be altered during execution
- Support for application aware anonymity to allow for anonymous web access; and platform security mechanisms and trust-in-platform establishment

Tailored Trustworthy Spaces
Vision: Create flexible, distributed trust environments that can support the functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats. TTS supports a variety of operating capabilities across multiple dimensions, including: confidentiality, anonymity, data and system integrity, provenance, availability, and performance.
Why: TTS enables cyber users to make informed trust decisions based on verifiable security properties of their environments and transactions. Today, cyberspace is composed of subsystems that lack mechanisms to ascertain their security conditions and to participate in creating environments with required trust and provenance characteristics. The absence of mechanisms to establish trust has made cyberspace vulnerable to illicit exploitations. A TTS is a vision of transparent secure trust environments suited to users' context. In the future, users and systems will have the means to establish a TTS by invoking and tailoring a set of security attributes to create a work environment within cyberspace appropriate to the task at hand. The establishment of trust between participants and systems in TTS will be based on verifiable information and properties.
Goals: • Develop mechanisms to enable specific trustworthy space policies and services for specific types of actions: a) Allow rules, attributes, and boundaries of the space to be defined to inform trust decisions b) Ensure that requirements for the use case can be accurately articulated in the policy for the TTS c) Establish a context specific set of trust services, supported by a scalable set of tools d) Assure TTS separation so that the build-up and tear-down of the spaces is trustworthy • Enable trustworthy computing in untrustworthy environments

Challenges:

- Develop flexible trust characterization and negotiation tools
- Develop a scalable service framework and configuration decision support capabilities for TTS establishment
- Ensure that users' requirements can be enabled in the policies that control the TTS, and that the policies can be implemented by relevant elements of the TTS
- Assure separation, and prevent leakage, of information between spaces
- Ensure that threat identification and mitigation can be considered in the policy and methods of defining TTS
- Advance the ability to perform informed trust analysis
- Develop capabilities to be able to dynamically tailor (including joining, adjusting, merging, splitting) a TTS

Critical Supporting Technologies:

- Trust negotiation tools: trust negotiation protocol elements, tailored identity establishment and management, transaction attribution mechanisms, reference monitors
- Access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire communication path (limited by the TTS policy)
- Data trust models to support negotiation of TTS policy based on data criticality
- Validation tools to provide the ability to verify application configuration and functions conform to the policy and as expected
- Data encryption and protection tools to support stronger non-repudiation and data attribution
- TTS resource and cost analysis tools
- Hardware mechanisms to establish trusted state and to monitor critical software
- Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments
- Application and operating systems elements (programming languages and compilers) that can provide assurance that the program semantics cannot be altered during execution
- Network and hardware configuration verification of TTS rules to establish trusted paths

Use Case Examples:

- Anonymous health care or employment search web surfing for private purposes where attribution and authentication are not desirable
- Protection of personal medical history or lab reports between individuals with minimal IT infrastructure and medical or insurance providers with substantial IT infrastructure
- Creation of an environment within cyberspace that can be trusted with sharing of information between government agencies as well as with coalition partners and state, and local authorities

- Authenticated, audited government-to-government transactions such as E-Gov or GAO reporting, and interagency sharing of sensitive information
- Capability to leverage TTS for the exchange of controlled and authenticated, high value messages such as those which support large financial transactions, official government dispatches, and military orders
- Demonstration of the ability to handle confidential authenticated citizen-to-government transactions such as submission of tax data, or electronic voting
- Demonstration that a high assurance tailored space suitable for national security requirements can be established in a trustworthy way

Appendix B: Recommended Smart Grid Use Cases for TTS Research

Transmission Operations Workshop Use Case

Transmission Operations Workshop Use Case combines:

- Transmission Operations / Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data, page 129
- Transmission Operations / Real-Time Emergency Transmission Operations, page 131

<table>
<tr><td colspan="3">Category: Transmission Operations</td></tr>
<tr><td colspan="3">Scenario: Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data (NISTIR 7628, pg. 129)</td></tr>
<tr><td colspan="3"><u>Category Description</u>
Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility’s control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include—
Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)
Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions
Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies
Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
Provides power quality
Optimizes asset utilization
Anticipates and responds to system disturbances</td><td><u>Cyber Security Objectives/Requirements</u>
Integrity is vital to the safety and reliability of the transmission system
Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)
Confidentiality is not important</td><td><u>Potential Stakeholder Issues</u>
Customer safety
Customer device standards
Demand response acceptance by customers</td></tr>
</table>

Category: Transmission Operations

Scenario: Real-Time Emergency Transmission Operations (NISTIR 7628, pg. 131)

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

During emergencies, the power system takes some automated actions and the operators can also take actions:

Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery

Operators manage emergency alarms

SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and pre-arming of fast acting emergency automation

SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):

Operators performs system restorations based on system restoration plans prepared (authorized) by operation management

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers

Distribution Automation Workshop Use Case

Distribution Automation Workshop Use Case combines:

- Distribution Automation / Distributed Energy Resources Management, page 121
- Demand Response / Mobile Plug-In Electric Vehicle Functions, page 105

Category: Distribution Automation

Scenario: Distributed Energy Resources Management (NISTIR 7628, pg. 121)

Category Description

A broad definition of "distribution automation" includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected DER, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.

Direct monitoring and control of DER

Shut-down or islanding verification for DER

PEV management as load, storage, and generation resource

Electric storage fill/draw management

Renewable energy DER with variable generation

Small fossil resource management, such as backup generators to be used for peak shifting

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is critical for any management/ control of generation and storage Availability requirements may vary depending on the size (individual or aggregate) of the DER plant Confidentiality may involve some privacy issues with customer-owned DER	Customer safety Customer device standards Demand response acceptance by customers

Category: Demand Response

Scenario: Mobile Plug-In Electric Vehicle Functions (NISTIR 7628, pg. 105)

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

In addition to customers with PEVs participating in their home-based Demand Response functions, they will have additional requirements for managing the charging and discharging of their mobile PEVs in other locations:

Customer connects PEV at another home

Customer connects PEV outside home territory

Customer connects PEV at public location

Customer charges the PEV

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically Availability is not an issue Confidentiality is not an issue, except with respect to meter reading	Customer data privacy and security Retail Electric Supplier access Customer data access

Customer Interfaces Workshop Use Case

Customer Interfaces Workshop Use Case combines:

- Customer Interfaces / Customer's In Home Device is Provisioned to Communicate With the Utility, page 106
- AMI / Remote Connect/Disconnect of Meter, page 95

<table>
<tr><td colspan="3">Category: Customer Interfaces</td></tr>
<tr><td colspan="3">Scenario: Customer's In Home Device is Provisioned to Communicate With the Utility (NISTIR 7628, pg. 106)</td></tr>
<tr><td colspan="3"><u>Category Description</u>
Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.</td></tr>
<tr><td colspan="3"><u>Scenario Description</u>
This scenario describes the process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device, or smart appliance.</td></tr>
<tr><td><u>Smart Grid Characteristics</u>
Enables active participation by consumers
Accommodates all generation and storage options
Enables new products, services and markets</td><td><u>Objectives/Requirements</u>
To protect passwords
To protect key material
To authenticate with other devices on the AMI system</td><td><u>Potential Stakeholder Issues</u>
Customer device standards
Customer data privacy and security</td></tr>
</table>

Category: AMI

Scenario: Remote Connect/Disconnect of Meter (NISTIR 7628, pg.95)

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems, as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

Traditionally, utilities send a metering service person to connect or disconnect the meter. With an AMI system, the connect/disconnect can be performed remotely by switching the remote connect/disconnect (RCD) switch for the following reasons:

Remote Connect for Move-In

Remote Connect for Reinstatement on Payment

Remote Disconnect for Move-Out

Remote Disconnect for Nonpayment

Remote Disconnect for Emergency Load Control

Unsolicited Connect / Disconnect Event

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved Availability to turn meter back on when needed is important Confidentiality requirements of the RCD command is generally not very important, except related to non-payment	Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Acronyms

AMI	Advanced Metering Infrastructure
CSIA	Cyber Security and Information Assurance
CSWG	Cybersecurity Working Group
DER	Distributed Energy Resources
DOE	Department of Energy
DOE/OE	Department of Energy / Office of Electricity Delivery & Energy Reliability
EMS	Energy Management System
GAO	Government Accountability Office
IWG	Interagency Working Group
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NITRD	Networking and Information Technology Research and Development
PEV	Plug-in Electric Vehicle
PHEV	Plug-in Hybrid Electric Vehicle
PKI	Public Key Infrastructure
R&D	Research and Development
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SGIP	Smart Grid Interoperability Panel
TTS	Tailored Trustworthy Spaces
VAR	Volt-Amperes Reactive
WASA	Wide Area Situational Awareness