Smart Grid and the Cloud

Panel Discussion
February 26, 2013

Chair: Dr. Michaela Iorga
NIST Senior Cloud Computing Technical Lead,
Chair, NIST Cloud Computing Public Security Working Group
Co-Chair, NIST Cloud Computing Public Forensic Science Working Group
Panelists:

Dr. Arnab Roy,
Fujitsu Laboratories of America
Top Ten Security and Privacy Challenges for Big Data and Smart Grids

Dr. Sarbari Gupta,
President, Electrosoft Inc.
Key Management Challenges

Marianne Swanson,
NIST, Senior Advisor for Information Security Management
Cloud Computing and Smart Grids
Cybersecurity

Dr. Alvaro A. Cárdenas,
Assistant Professor, University of Texas at Dallas
Big Data Analytics and Security Intelligence in Smart Grid Applications

Chris Knudsen,
CTO, AutoGrid Systems Inc.
How Big Data and Cloud Computing Can Solve Next Generation Utility Challenges
The migration to the cloud is already occurring in various applications within the Smart Grid. As Chair of the Smart Grid Interoperability Panel Cybersecurity Committee, I am leading a team that is researching the roles of cloud computing within the Smart Grid and determining how best to secure them.
Cloud Computing and Smart Grid Cybersecurity

Marianne Swanson, Chair SGCC
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology (NIST)
Smart Grid Cybersecurity Committee
Background

- To address the cross-cutting issue of cybersecurity, NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009.

- Moved under the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the Cyber Security Working Group (CSWG).

- As the SGIP transitions to SGIP 2.0, the group was renamed the Smart Grid Cybersecurity Committee (SGCC).
Cybersecurity Committee Active Sub-groups and Leads

- Architecture Group
  - Elizabeth Sisley
- Cloud Computing and Smart Grid
  - Marianne Swanson
- High-Level Requirements Group
  - Dave Dalva & Victoria Yan Pillitteri
- NISTIR 7628 Users Guide Group
  - Chris Rosen & Mark Ellison
- Privacy Group
  - Rebecca Herold
- Standards Group
  - Frances Cleveland
Cloud Computing Subgroup

- Drafting White Paper on unique Smart Grid issues
- Build upon the large amount of cybersecurity guidance already available
  - NIST Special Publications
  - FedRAMP
  - National Rural Electric Cooperative Association
Tentative White Paper Approach

• Select two Smart Grid use cases, for example:
  – Outage Management System
  – Customer Information Systems
• Describe business goals and business impact
• Depict in depth view of architecture
• Provide recommended security requirements and rationale
Learning More and Getting Involved

• Learn more about the SGCC at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

• Learn more about the subgroups, including meeting times: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo

• To learn more about SGIP 2.0 and join, visit: http://sgip.org/
Contact Information

- For any questions or comments, please contact Marianne Swanson, SGCC Chair, at marianne.swanson@nist.gov
Power infrastructures are increasingly becoming data-driven with the proliferation of consumer devices communicating with the service providers. While there are tremendous advantages enabled by the aggregation and analysis of this data, the increasing granularity and personal nature of the data imply that smart grid application platforms deployed in the cloud inherit the security and privacy challenges of Big Data. The security and privacy issues are magnified by velocity, volume, and variety of big data, such as large-scale cloud infrastructures, diversity of data sources and formats, streaming nature of data acquisition and high volume inter-cloud migration. Therefore, traditional security mechanisms, which are tailored to securing small scale static (as opposed to streaming) data, are inadequate. The CSA Big Data Working Group has identified top ten big data specific security and privacy challenges. I will discuss the challenges in general as well as how they apply to smart grid application deployments.
Top Ten Security and Privacy Challenges for Big Data and Smartgrids

Arnab Roy
Fujitsu Laboratories of America
User Roles and Security Concerns [SKCP11]

Utilities:
- Data Leakage - Consumer trust, Regulatory compliance
- Data Modification - Power billing, Grid operation
- Data Platform Sharing - Pricing/Forecast algorithms

Consumers:
- Data Leakage - Behavior monitoring, industrial espionage
- Data Modification - Power usage measurement, Pricing

3rd Party Service Providers:
- Data/Platform Sharing - Internal algorithms, Data
- Access Diversity - Regulatory compliance, Platform integration
Data Characteristics & S&P Issues [SKCP11]
Top 10 Challenges Identified by CSA BDWG

1) Secure computations in distributed programming frameworks
2) Security best practices for non-relational datastores
3) Secure data storage and transactions logs
4) End-point input validation/filtering
5) Real time security monitoring
6) Scalable and composable privacy-preserving data mining and analytics
7) Cryptographically enforced access control and secure communication
8) Granular access control
9) Granular audits
10) Data provenance
Top 10 Big Data S&P Challenges

- **Infrastructure security**
  - Secure Computations in Distributed Programming Frameworks
  - Security Best Practices for Non-Relational Data Stores

- **Data Privacy**
  - Privacy Preserving Data Mining and Analytics
  - Cryptographically Enforced Data Centric Security
  - Granular Access Control

- **Data Management**
  - Secure Data Storage and Transaction Logs
  - Granular Audits
  - Data Provenance

- **Integrity and Reactive Security**
  - End-point validation and filtering
  - Real-time Security Monitoring
Secure Computation in Distributed Programming Frameworks

Smartgrid Scenario:
Application Computation Infrastructure

Threats/Challenges:
- Malfunctioning compute worker nodes
- Access to sensitive data
- Privacy of output information

Current Mitigations:
- Trust establishment: initiation, periodic trust update
- Mandatory access control
- Privacy preserving transformations
Security Best Practices for Non Relational Data Stores

Smartgrid Scenario:
- Data from Diverse Appliances and Sensors

Threats/Challenges:
- Lack of stringent authentication and authorization mechanisms
- Lack of secure communication between compute nodes

Current Mitigations:
- Enforcement through middleware layer
- Passwords should never be held in clear
- Encrypted data at rest
- Protect communication using SSL/TLS
Secure data storage and transaction logs

Smartgrid Scenario:
Consumer Data Archive

Threats/Challenges:
- Data Confidentiality and Integrity
- Availability
- Consistency
- Collusion

Current Mitigations:
- Encryption and Signatures
- Proof of data possession
- Periodic audit and hash chains
- Policy based encryption
End-point Input Validation / Filtering

**Smartgrid Scenario:**
- Data Poisoning

**Threats/Challenges:**
- Adversary may tamper with device or software
- Adversary may clone fake devices
- Adversary may directly control source of data
- Adversary may compromise data in transmission

**Current Mitigations:**
- Tamper-proof Software
- Trust Certificate and Trusted Devices
- Analytics to detect outliers
- Cryptographic Protocols
Real-time Security Monitoring

Smartgrid Scenario:
Fraud Detection

Threats/Challenges:
- Security of the infrastructure
- Security of the monitoring code itself
- Security of the input sources
- Adversary may cause data poisoning

Current Mitigations:
- Discussed before
- Secure coding practices
- Discussed before
- Analytics to detect outliers

Copyright 2013 FUJITSU LIMITED
Scalable and Composable Privacy-Preserving Data Mining and Analytics

Smartgrid Scenario:

- Consumer Data Privacy

Threats/Challenges:

- Exploiting vulnerability at host
- Insider threat
- Outsourcing analytics to untrusted partners
- Unintended leakage through sharing of data

Current Mitigations:

- Encryption of data at rest, access control and authorization mechanisms
- Separation of duty principles, clear policy for logging access to datasets
- Awareness of re-identification issues, differential privacy
Cryptographically Enforced Data Centric Security

How do we enforce the protection of data end to end?

Smartgrid Scenario:

- Data Integrity and Privacy

Threats/Challenges:

- Enforcing access control
- Search and filter
- Outsourcing of computation
- Integrity of data and preservation of anonymity

Current Mitigations:

- Identity and Attribute-based encryptions
- Encryption techniques supporting search and filter
- Fully Homomorphic Encryption
- Group signatures with trusted third parties

Copyright 2013 FUJITSU LIMITED
Granular Access Control

Smartgrid Scenario:
Data Privacy

Threats/Challenges:
- Keeping track of secrecy requirements of individual data elements
- Maintaining access labels across analytical transformations
- Keeping track of roles and authorities of users

Current Mitigations:
- Pick right level of granularity: row level, column level, cell level
- At the minimum, conform to lattice of access restrictions. More sophisticated data transforms are being considered in active research
- Authentication, authorization, mandatory access control
Granular Audits

Smartgrid Scenario:
Audit of usage, pricing, billing

Threats/Challenges:
- Completeness of audit information
- Timely access to audit information
- Integrity of audit information
- Authorized access to audit information

Current Mitigations:
Infrastructure solutions as discussed before. Scaling of SIEM tools.

Copyright 2013 FUJITSU LIMITED
Data Provenance

Smartgrid Scenario:
- Keeping track of ownership of data – pricing, audit

Threats/Challenges:
- Secure collection of data
- Consistency of data and metadata
- Insider threats

Current Mitigations:
- Authentication techniques
- Message digests
- Access Control through systems and cryptography

Copyright 2013 FUJITSU LIMITED
Thank You
Futuristic Smart Grid architectures demand highly available, scalable, consistent and secure computing environments. Hence, cloud computing is a natural fit for smart grid implementations. In order to provide the security and privacy required for smart grid implementations, it is essential to use cryptographic mechanisms within the cloud. This presentation discusses special issues and challenges that arise in managing cryptographic keys that protect data in the cloud, the approaches that are currently being used for managing such keys, and the areas where there are significant opportunities for improvement.

Key Management Challenges

Dr. Sarbari Gupta
President, Electrosoft Inc.
Key Management Challenges
with Smart Grid and the Cloud

Dr. Sarbari Gupta

Managing Cyber Risk Through Innovation and Engineering

February 26, 2013
Smart Grid and Cloud

• Smart Grid Functions moving to Cloud
  – Collection of Data from Meters/Sensors/Devices
  – Rapid Analysis of Big Data
  – Control and Management of Smart Grid Operations

• Why Cloud Computing for Smart Grid?
  – Supports “Elasticity” needed in Smart Grid Operations
  – Lower Cost and Rapid Deployment
  – Higher Availability and Reliability
  – Connects variety of Stakeholders through Standard Interfaces
    • Providers (Generators, Distributors, Utilities, etc.)
    • Users (Industrial, Commercial, Home, etc.)
Cloud Based Systems – Uncertainties

• Processor
  – Where is my process running?
  – Am I sharing the processor with other users/organizations?

• Data Storage
  – Where does my data reside?
  – Is my data co-resident with other users’ data?

• Communication
  – How does my CSP know who I am?
  – How is my connection to cloud components protected?

• Administration
  – Who administers the Cloud Infrastructure?
  – Who has access to my data? My activity history?

• Key Management
  – Where and how are keys: Generated? Stored?
  – How are keys: Distributed? Protected? Recovered? Destroyed?
Cryptography Integral to Cloud

• Supports strong remote authentication
  — Regular users (1- or 2-factor)
  — Administrators (2-factor)

• Implements strong communication protocols
  — Between user (browser) and cloud (SSL/TLS)

• Partitions User data in co-tenancy environments

• Provides data confidentiality
  — From cloud administrators
  — From Cloud co-tenants

• Supports data integrity
  — Tamper-detection of critical data through MACs and digital signatures

• Strengthens Audit Log Management
  — Signed and time-stamped audit logs
Cryptographic Key Management

• Cryptographic Keys - Core Functions
  – Confidentiality Protection
  – Integrity Protection
  – Source Authentication

• Key Management - Scope
  – Key Generation
  – Key Storage
  – Key Distribution
  – Key Recovery
  – Key Destruction
Use Case 1: Remote Authentication to Cloud

- Key Management from Cloud User’s Perspective
  - Some Visibility
    - Assurance of standard protocols and TTP issued credentials
  - Some Control
    - User may select own Credential Provider, Configure Browser settings
Use Case 2: Secure Communication with Cloud

- Key Management from Cloud User’s Perspective
  - Some Visibility
    - Assurance of standard protocols and TTP issued credentials
  - Some Control
    - User may configure browser settings
Use Case 3: Cloud Data Protection

Key Management from Cloud User’s Perspective
- **SaaS** - little or no visibility; little or no control
- **PaaS** - limited visibility; limited control
- **IaaS** - more visibility; more control

Courtesy of CIO Research Council (CRC)
Wrap-Up and Contact Information

• Summary
  – Smart Grid and Cloud are a Natural Fit
  – Cloud Computing presents unique security challenges
  – Cryptography essential to secure cloud operations
  – Sound Key Management Practices critical

• Contact Information
  – Dr. Sarbari Gupta – Electrosoft
    • Email: sarbari@electrosoft-inc.com
    • Phone: 703-437-9451 ext. 12
Our critical infrastructure systems are being modernized with information and communication technologies to face the operational requirements and efficiency challenges of the 21st century. The smart grid (including building and home automation) in particular, will introduce millions of new intelligent components to the electric grid, buildings, and homes within the next decade. This large-scale instrumentation will also be the source of data collected on an unprecedented scale and granularity.

In this talk I will talk about the advantages of analyzing this data (big data analytics) for better situational awareness, and in particular, for security intelligence. I will exemplify some of these notions with smart grid data being used for electricity theft and anomaly detection.
Big Data Analytics (and Security Intelligence) in Smart Grid Applications

Alvaro A. Cárdenas
University of Texas at Dallas
IEEE ISGT Conference
February 26, 2013
Big Data World

- Growth of Data in Motion
- Growth of Data at Rest

- **Source:** The World’s Technological Capacity to Store Communicate and Compute Information. Hilbert and López. Science 332, 60 (2011)

- 90% of the data in the world today was created in the last two years ([Source: http://www-01.ibm.com/software/data/bigdata/](http://www-01.ibm.com/software/data/bigdata/))
What is new in Big Data?

Traditional Systems

• More rigid, predefined schemas
• Data gets deleted
• Complex analyst queries take long to complete
• Others?

Big Data Promise

• Structured and unstructured data treated seamlessly
• Keep data for historical correlation (e.g., 10 years)
• Faster query response times
• Others?

Hadoop is de facto open standard for big data at rest
Stream processing? Participation welcome!!
A Large Part of this Data is Coming from Sensors and the Internet of Things

Standards: Wireless HART (IEC), ISA SP 100.11a, IETF 6LoWPAN, ROLL, CoRE, Eman, LWIP, IRTF IoT, W3C EIX, IEEE 802.15.4 (g), 802.15.5, etc.
Big Data Analytics in Smart Grid

Massive Smart Meter Data Storage and Processing on top of Hadoop.
D.P. dos Santos et.al. EDF. BigData 2012
Hadoop Energy Databases

• Cost of running a Hadoop cluster is going down
  – It allows business models like Ecofactor to flourish
    • Adam Lesser-GigaOM

• Opower using Hadoop to manage massive energy data streams
  – Katie Fehrenbacher GigaOM

• PJM uses Hadoop to organize energy data coming off synchrophasor sensor projects
  – Katie Fehrenbacher GigaOM
Cloud-Based Big Data Services

• Real-time weather data
• Real-time load
  – Smart thermostats
• Real-time electricity prices
• Real-time state monitoring (synchrophasor)
• Historical data/models
  – Demographics
  – Weather
  – User behavior
Startups

• Players
  – EcoFactor, C3 Energy, Tendril, Stem, AutoGrid, Bidgely, Nest Labs, Opower, EnergyHub, Opower, Noesis

• Goals:
  – Social media for customers to reduce energy
  – Analytics for DR
  – Predict and analyze energy use in commercial buildings
    • Building management
  – Energy disaggregation in SEP 2.0 to help consumers identify appliance loads (e.g., fridge left open, inefficient appliance, etc.)
Old

Utilities
Day Ahead Forecast

Commercial Buildings:
Phone-call to shed load

Residential
No info

New

Utilities
More Complexity: DR and distributed sources
- Real-time info
- Generation optimization
- Maintenance

Commercial Buildings
Real-time forecast and shedding

Residential
Appliance insights and intelligent systems
Security can also be a Big Winner from Big Data
Security is a Hard Business Case in Critical Infrastructures

• Push back in prices
  – Billions of low-cost embedded devices

• Security ROI is hard to see
  – Hard to see advantages of hardening devices, system

• The reason for Executive Order from the President earlier this month!
Business Case for “Data Analytics” is Easier than Security Business Cases

- **Situational Awareness is part of the business case for modernizing our infrastructures**
  - To understand the health of the system
    - Transmission grid, distribution grid, routing protocol in AMI, etc.
    - Wide Area Protection, Monitoring and Control

- **Goal: leverage this data to improve cyber-security situational awareness**
  - We get: Redundancy, Diversity
  - Data Analytics to identify suspicious behavior

Last year > 60% of respondents installed tools to gain a better view of what is on their network
  - McAfee Risk & Compliance Outlook 2012
How Big Data and Cloud Computing Can Solve Next Generation Utility Challenges

Knudsen—who oversaw PG&E’s smart grid initiatives before becoming AutoGrid’s CTO—will explain how advances in predictive analytics and Big Data have created an opportunity for utilities and demand response providers to replace or enhance hardware-based demand response systems with cloud computing services.

Knudsen, as an OpenADR Alliance Board Member and NIST Smart Grid Architecture Committee Member will also provide an overview of industry-wide trends. Come and learn how intelligent system design that leverages technology created in the last decade, can address scalability, reliability and security to meet the pragmatic needs of the utility industry.
How Big Data and Cloud Computing can Solve Next Generation Utility Challenges

IEEE PES | February, 2013

Chris Knudsen
CTO, AutoGrid Systems Inc
The Concept is Simple...

- Define the Problem
- Extract relevant data from existing disparate sets
- Predict outcomes and optimize solution
- Execute in real-time to improve operational decision-making
The Reality is Much More Complex...

Every source of data is different
Cada fuente de información es diferente
每一個數據源是不同的
Ogni fonte di informazione è diverso
データのすべてのソースが異なっている
Jede Quelle von Daten verschieden ist
แหล่งที่มาจากของข้อมูลทุกที่แตกต่างกัน
Chaque source d'information est différent

Utility-scale solutions must be:

• Safe & Reliable: across all variations and unknowns
• Scalable: to millions of end points and Diverse loads (residential to industrial)
• Forward & Backward Compatible: support migration from to legacy systems to open, standards-based solutions
• FERC Compliant: Solve for complex rules around aggregate load shed (ie. > 300MW)
• Complete solution: not just a communication server
And Change is Hard...

- Utilities are bound by their legacy
  - Safety and Reliability are the priorities
  - Current regulatory structure does not reward risk
  - Status Quo is “OK”, no upside for innovation
  - Decades of functioning technology solutions make change problematic
  - 100’s of critical applications in place
- Smaller Utilities need highly cost-effective solutions
- Many large, closed, vertically integrated systems
Entering the 3rd Generation of Cloud, Big Data, and Analytics Companies

Technology Components for Hybrid & Cloud Computing, Data Science & Actionable Analytics are rapidly maturing
The Hype Cycle is Packed with Now and Near Term Maturity

Source: Gartner (July 2012)
Cloud Solutions Provide Great Advantage

Why Cloud Computing?

- Pay As You Use
- Lower TCO
- Reliability, Scalability & Sustainability
- Secure Storage Management
- Lower Capital Expenditure
- Frees Up Internal Resources
- Highly Automated
- Utility Based
- Easy & Agile Deployment
- Device & Location Independent
- 24X7 Support
Traditional Architecture does Not Scale

Utilities need a solution that can scale & grow with the increasing intelligence of their Smart Grids

Relational Databases Expensive at Scale
So What is the Solution...

Apply the last decade of technology innovations to the Utility industry in a way that has never before been done

Build an Energy Data Platform to:

- Know what every resource is doing past, present, & future
- Scale reliably to millions of connections
- Process information in real-time
- Enable Rapid Deployment at extremely low cost
- Disaggregated technology model
- “No instructions Needed” complete, intuitive, easy to use
AutoGrid Energy Data Platform: Big Data for Energy

• Similar to e-commerce recommendation engines and weather forecasting applications
• Analyzes trends, forecast demand by examining millions of variables and petabytes of data
• Optimizes power consumption and system operations
AutoGrid: Turning Big Data into Power

AutoGrid’s Energy Data Platform

- Real time processing of many highly varied data streams
- Applied, actionable, intelligence using the right set of data to make the optimal decisions for specific Utility business needs
Reliable, Scalable, Extensible

AutoGrid Systems Inc. — Confidential
AutoGrid DROMS Benefits

✓ Unified View of All Resources:
  – Across all customer classes, load types and programs
  – More load diversity allows better “yield” optimization

✓ Open Ecosystem:
  – 100% hardware neutral, standards-based architecture;
  – Allows more customer choice, participation and satisfaction
  – Eliminates vendor-lock, lowers cost of deployment

✓ Scalable:
  – Internet scale architecture to support millions of users & petabytes of data
  – Generate 1 Million + forecast every minute for each meter and time series
  – Secure, scalable, fault-tolerant architecture available on public or private clouds
  – Highly Cost effective solution

✓ Rapid Deployment:
  – No Hardware to purchase or software to install
  – Get going in weeks, not months or years - Low risk and low cost
  – Grows with your program - start small & grow to millions of users & multiple programs
Summary

✓ Low Risk
✓ Low Cost
✓ Rapid Deployment
✓ Open and Scalable
✓ Available Today...

for the Future

... Ready
Questions

Thank you!