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
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