Privacy-Enhanced Bi-Directional Communication in the Smart Grid using Trusted Computing

Andrew Paverd, Andrew Martin, Ian Brown
University of Oxford

https://www.cs.ox.ac.uk/people/andrew.paverd/tre
Smart Grid Architecture

NIST Model

- Secure Communication Flows
- Electrical Flows
- Domain

Markets — Operations — Service Provider
Bulk Generation — Transmission — Distribution — Customer

NIST Smart Grid Framework
Smart Grid Architecture

NIST Model

[Diagram showing the NIST Smart Grid Framework with labeled components: Markets, Operations, Service Provider, Bulk Generation, Transmission, Distribution, and Customer.]

- Secure Communication Flows
- Electrical Flows
- Domain

NIST Smart Grid Framework
Information Flows

1. Monitoring
   - Monitoring/balancing specific sectors
   - Unidirectional: smart meters → DNO/supplier
   - Requires high temporal granularity but can be spatially aggregated

2. Billing
   - Facilitates dynamic energy pricing
   - Unidirectional: smart meters → energy supplier
   - Requires individual data but can be temporally aggregated
Demand Response (DR)

<table>
<thead>
<tr>
<th>Incentive Based Programs (IBP)</th>
<th>Price Based Programs (PBP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classical</td>
<td>Time of Use (TOU)</td>
</tr>
<tr>
<td>Direct Control</td>
<td>Critical Peak Pricing (CPP)</td>
</tr>
<tr>
<td>Interruptible/Curtailable</td>
<td>Extreme Day CPP (ED-CPP)</td>
</tr>
<tr>
<td>Programs</td>
<td>Extreme Day Pricing (EDP)</td>
</tr>
<tr>
<td>Market Based</td>
<td>Real Time Pricing (RTP)</td>
</tr>
<tr>
<td>Demand Bidding</td>
<td></td>
</tr>
<tr>
<td>Emergency DR</td>
<td></td>
</tr>
<tr>
<td>Capacity Market</td>
<td></td>
</tr>
<tr>
<td>Ancillary services market</td>
<td></td>
</tr>
</tbody>
</table>

Classification of demand response programs (Albadi et al.)
Information Flows

1. Monitoring

2. Billing

3. Demand Response (DR)
   - Demand-bidding and equivalent protocols
   - “Transactive” energy markets
   - Closed-loop feedback control
   - Requires full bi-directional communication:
     - Consumers ↔ Demand Side Manager (DSM)
Security and Privacy Threats

Security Threats
• Modification or falsification of data

Privacy Threats
• Honest-But-Curious (HBC) adversary
• Inference of private information
  • Non-Invasive Load Monitoring (NILM)

These are applicable to all three information flows
Existing Solutions

1. Monitoring
   - Spatial aggregation (Garcia et al.)
   - Pseudonymization (Rottondi et al.)

2. Billing
   - Temporal aggregation (Danezis et al.)

3. Demand Response
   - Cannot aggregate bi-directional communication
Trustworthy Remote Entity (TRE)
Monitoring

Differential Privacy (Dwork et al.) \[ L \sim \text{Lap}(1/\epsilon) \]
Demand Bidding

- Consumer
  - Publish DR Event
  - Bids/opt-outs
  - Notify successful bidders
  - Verify bid compliance

- TRE
  - Publish DR Event
  - Pseudo-bids
  - Accept pseudo-bids

- DSM
  - Apply incentives to consumer bills
Enhanced Architecture
Establishing Trust
Establishing Trust

**Trusted Platform Module (TPM)**
- Standardized by the Trusted Computing Group (TCG)
- Widely-deployed cryptographic co-processor
  - Over 500 million TPMs deployed
  - FIPS 140-2 certified
- Hardware random number generator
- Secure storage of private keys
- Extend-only Platform Configuration Registers (PCRs)

\[
p_{r0} := 00000000000000000000000000000000 \\
p_{rk} := \text{sha1}( p_{rk} \ || \ \text{new value} )
\]
Establishing Trust

Measured Boot

-  Transfer control
-  Measure and extend PCRs

CRTM  →  BIOS  →  MBR  →  Boot Loader  →  OS Kernel  →  Applications

Trusted Platform Module (TPM) - Platform Configuration Registers (PCRs)
Establishing Trust

Remote attestation

- Cryptographic proof of PCR values
- Scalability challenges on modern systems due to quantity of software.

```
verifier → prover: nonce
prover → verifier: pcrs, signature(pcrs, nonce)
```
Establishing Trust

Trustworthy Remote Entity (TRE)

- Single-function, specialized system
  - Networking, crypto, TPM & protocol logic
  - Uses measured boot and remote attestation

- Orders of magnitude less code than OS kernel
  - Linux kernel 3.10 ~15,000 kLoC
  - TRE ~20 kLoC

- Micro-benchmarks
  - Remote attestation: ~700 ms per operation
  - > 1000 attestations per 15 minutes
Formal Analysis

**Casper/FDR tool (Lowe et al.)**

- Describe protocols in user-friendly script
- Compile description into CSP model
- Analyses secrecy and authentication properties
- Uses the Dolev-Yao adversary model

**Casper-Privacy tool (Paverd et al.)**

- Uses existing Casper/FDR script and model
- Adds privacy properties: undetectability & unlinkability
- Uses the Honest-But-Curious (HBC) adversary model
Formal Analysis

#Protocol description
1. sma -> tre : sma, ma1
1b. smb -> tre : smb, mb1
2. tre -> ut : agg1
3. sma -> tre : sma, ma2
3b. smb -> tre : smb, mb2
4. tre -> ut : agg2
5. tre -> ut : sma, agga
5b. tre -> ut : smb, aggb

#Specification
Secret(sma, ma1, [tre])
Secret(sma, ma2, [tre])
Agreement(sma, tre, [ma1, ma2])
Agreement(tre, ut, [agg1, agg2])
Agreement(tre, ut, [agga, aggb])

#Privacy
Unlinkable( UT, {MA1,SMA} )
Unlinkable( UT, {MB1,SMB} )
Unlinkable( UT, {MA2,SMA})
Unlinkable( UT, {MB2,SMB} )
Formal Analysis - Security

Security properties:

- Only authorized consumers can submit measurements and DR bids [false data injection attacks]

- Consumers cannot submit multiple measurements in a single period [false data injection attacks]

- Unauthorized modifications of measurements or bids are detected [false data injection attacks]

- Consumers cannot impersonate each other [fraud]
Privacy properties:

- Measurements and bids cannot be viewed by external adversaries [confidentiality]

- Only the TRE can detect if a specific consumer has placed a DR bid [undetectability]

- Measurements, bids and DR incentives cannot be linked to individual consumers except by the TRE [unlinkability]
Conclusions

- Demand Bidding requires full bi-directional communication between consumers and DSM.

- Privacy-preserving bi-directional communication is possible with the use of a TRE.

- Trusted Computing remote attestation can provide proofs of trustworthiness for the TRE.

- The security and privacy properties of the protocols can be analysed using formal methods.
Privacy-Enhanced Bi-Directional Communication in the Smart Grid using Trusted Computing

Andrew Paverd, Andrew Martin, Ian Brown

University of Oxford

https://www.cs.ox.ac.uk/people/andrew.paverd/
“Changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized”

- United States Department of Energy
Smart Grid Architecture (GB)

GB Model

Energy Consumers

Data & Communications Company (DCC)

DCC Service Users

Smart appliance
Smart gas meter
Smart electricity meter

Communications hub

In-home display

Communications Service Providers

Data Service Provider

Smart DCC Limited

Energy suppliers
Distribution Network Operators (DNOs)
Other authorized parties

Home Area Network

Wide Area Network
Trusted Platform Module

Cryptographic processor
- random number generator
- RSA key generator
- SHA-1 hash generator
- encryption-decryption-signature engine

Persistent memory
- Endorsement Key (EK)
- Storage Root Key (SRK)

Versatile memory
- Platform Configuration Registers (PCR)
- Attestation Identity Keys (AIK)
- storage keys

"TPM" by This figure was made by Eusebius (Guillaume Piolle).