Security & Privacy in Smart Grid Demand Response Systems

Andrew Paverd

Department of Computer Science
University of Oxford

Supervisors: Andrew Martin *(Department of Computer Science)*
Ian Brown *(Oxford Internet Institute)*

Objectives

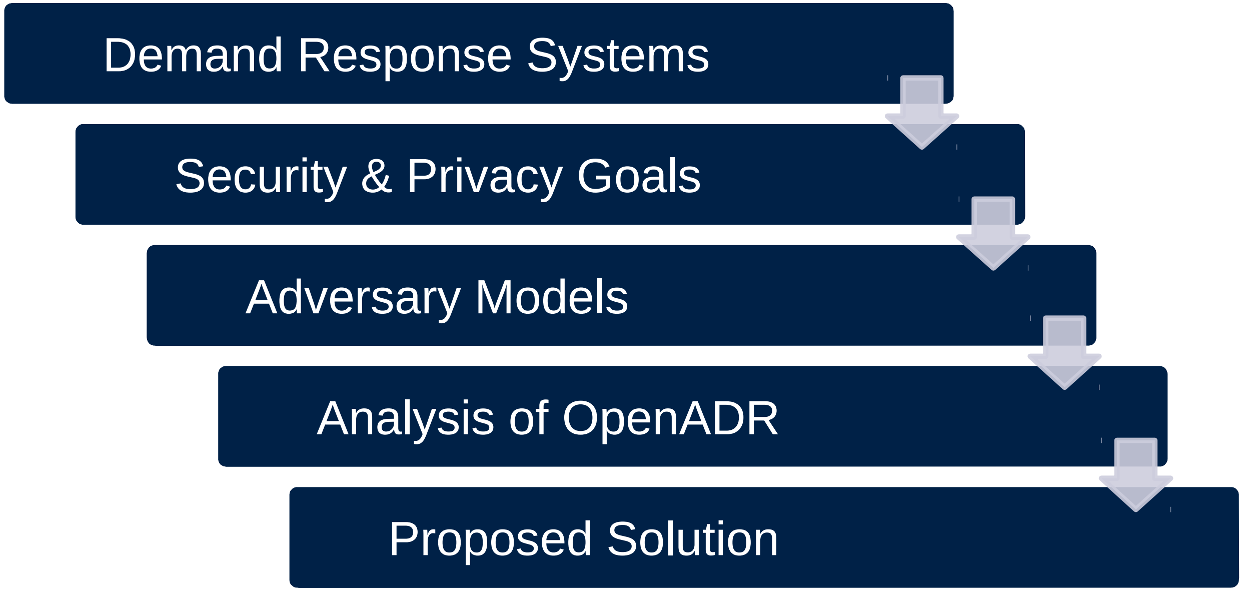
- Highlight security and privacy issues
  - Different from smart metering

- Build on existing research
  - Work by M. Karwe and J. Strüker *(SmartGridSec 2012)*

- Encourage further research

Overview

What are the main security and privacy challenges in demand response systems?



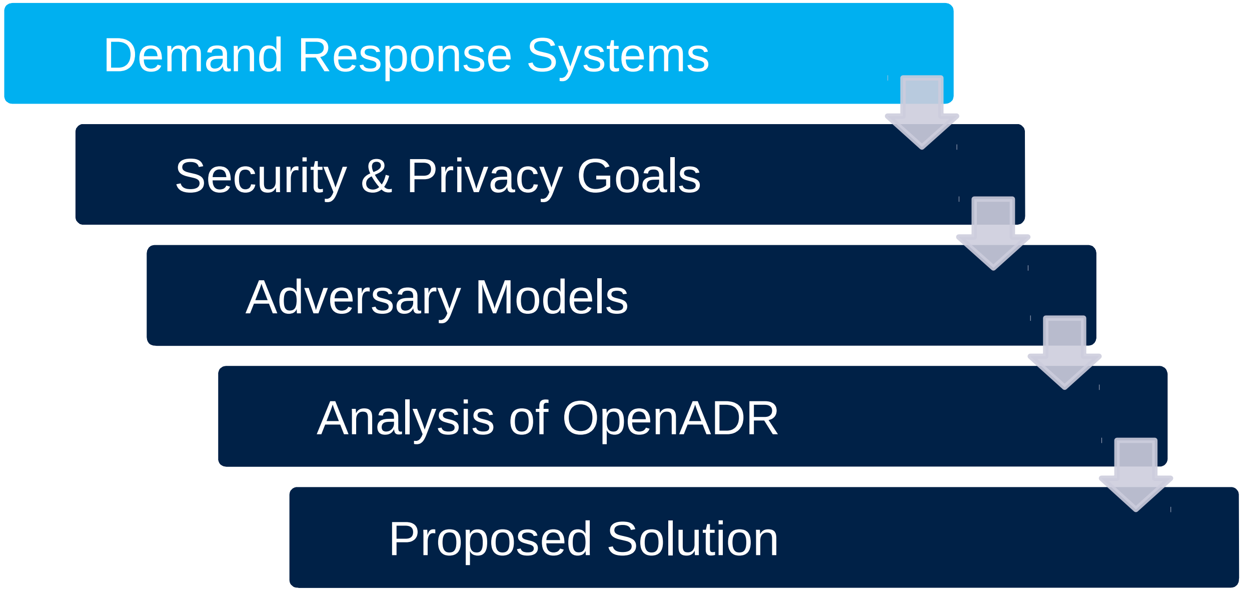
Demand Response Systems

Security & Privacy Goals

Adversary Models

Analysis of OpenADR

Proposed Solution



Demand Response Systems

Security & Privacy Goals

Adversary Models

Analysis of OpenADR

Proposed Solution

Demand Response (DR)

Dynamically reducing energy demand at specific times and in specific locations…

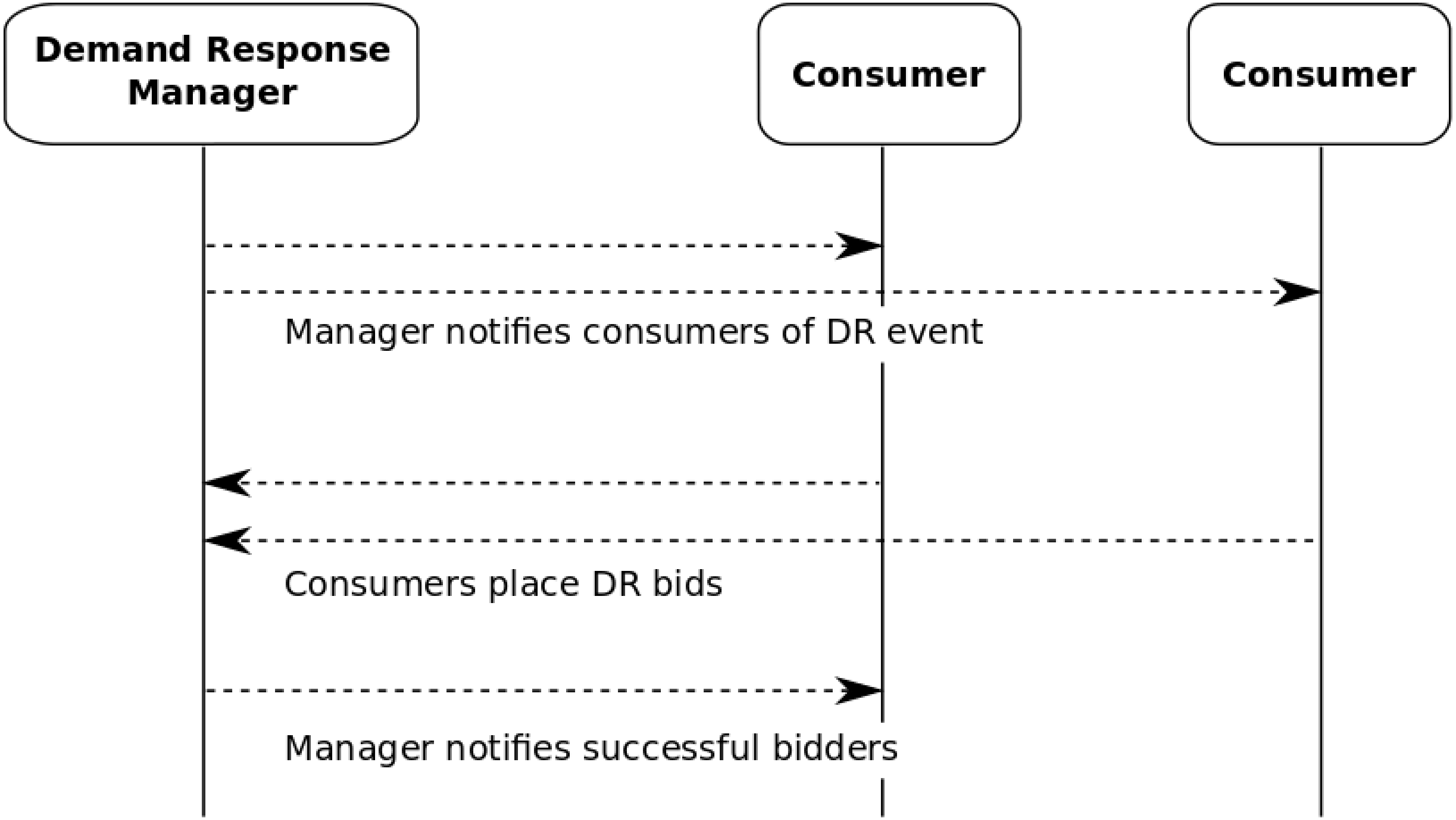
Price-based

- Time of use (ToU) pricing
- Critical peak pricing
- Dynamic pricing
- In-home display or energy management system

Incentive-based

- Consumers bid to reduce or shift demand
- Financial incentives
- Bidding protocol (bidding agents and manager)

Incentive-Based DR



Manager notifies consumers of DR event

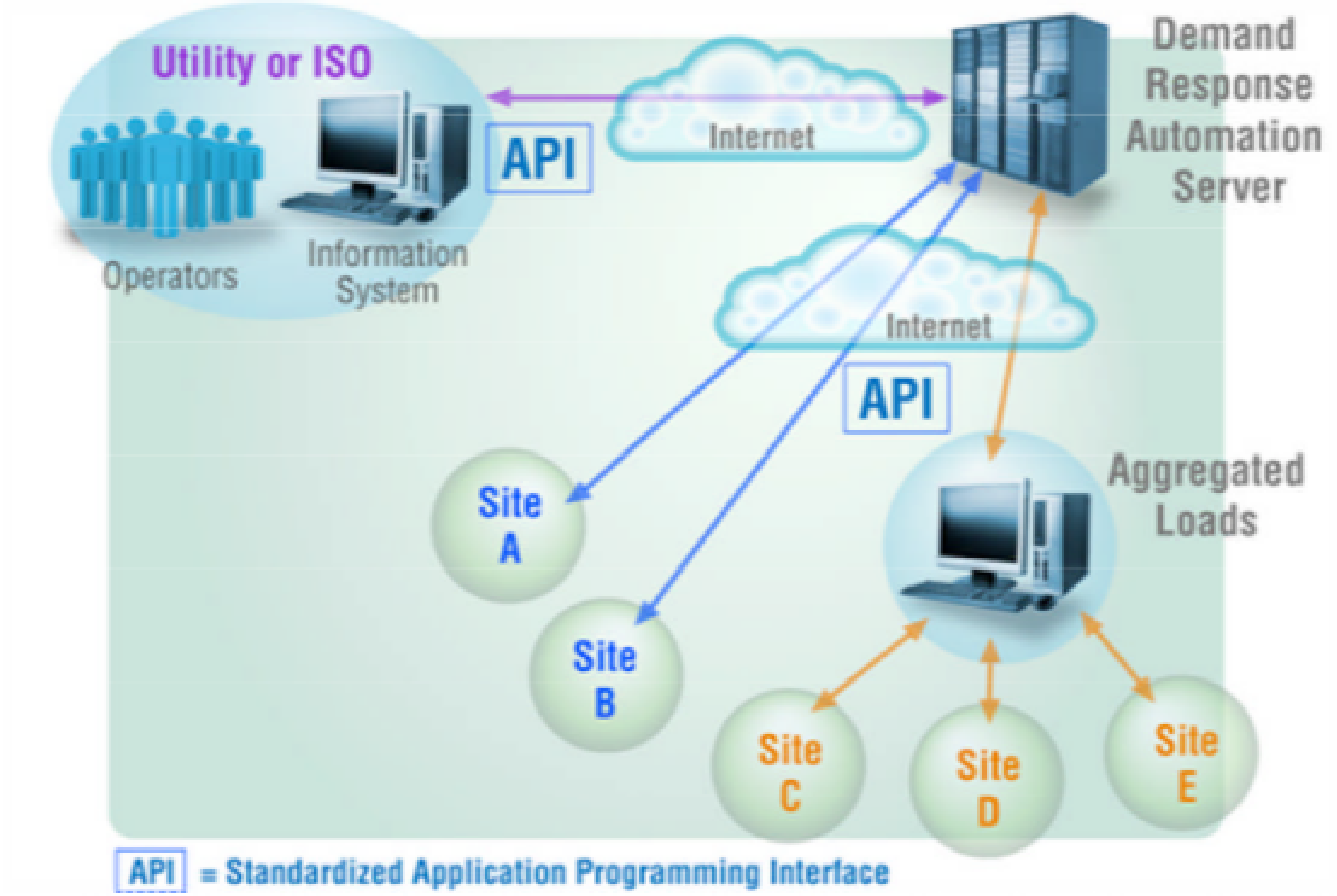
Consumers place DR bids

Manager notifies successful bidders

OpenADR 2.0

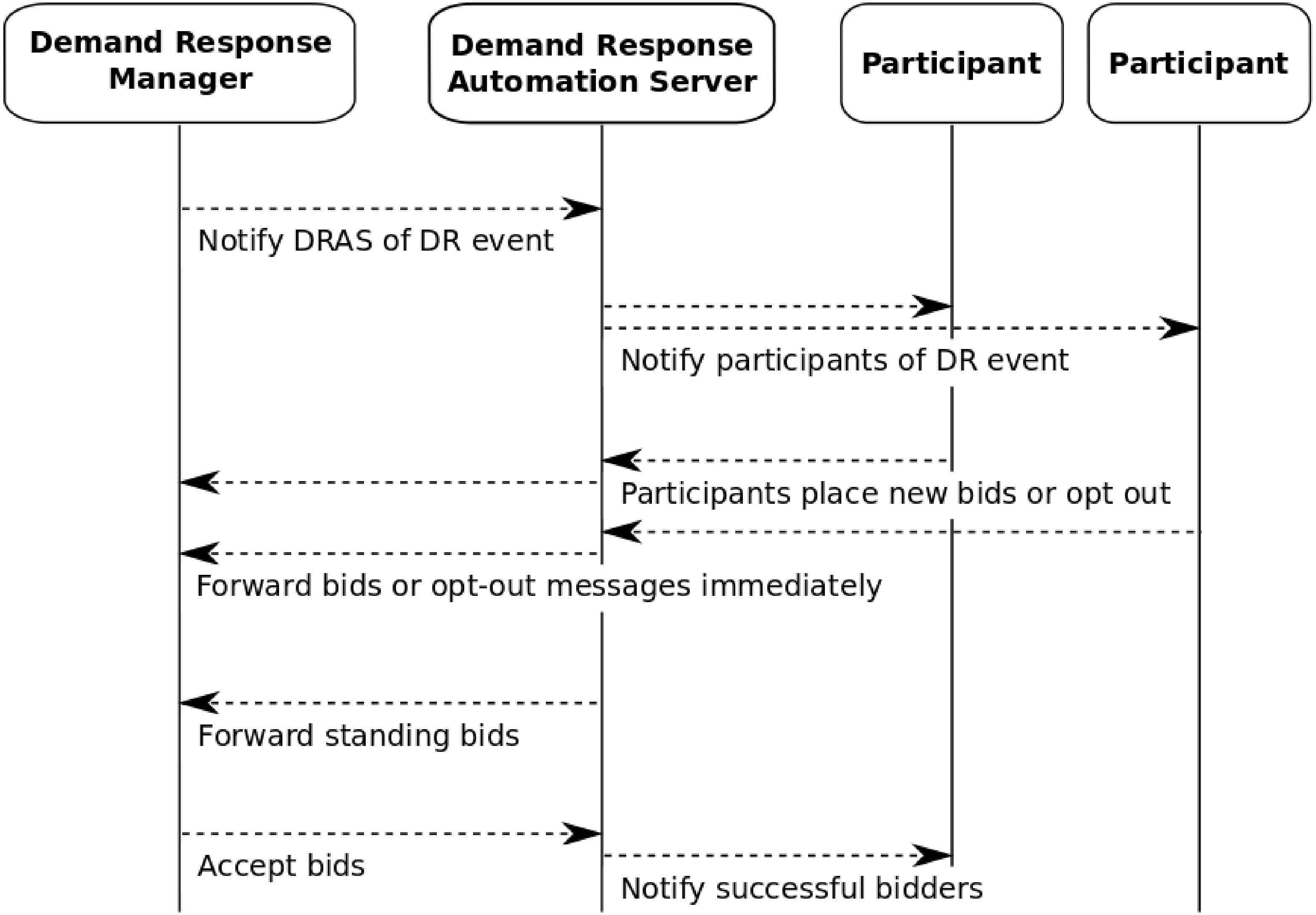
- Communication data model for DR systems
  - Enables price-based and/or incentive-based DR
- XML data over IP network
  - Medium independent (wireless, power line communication etc.)
  - HTTP, SOAP and XMPP
- Hierarchical structure
  - Virtual top node (VTN) and virtual end nodes (VEN)
- Demand Response Automation Server (DRAS)
  - Automate communication between entities

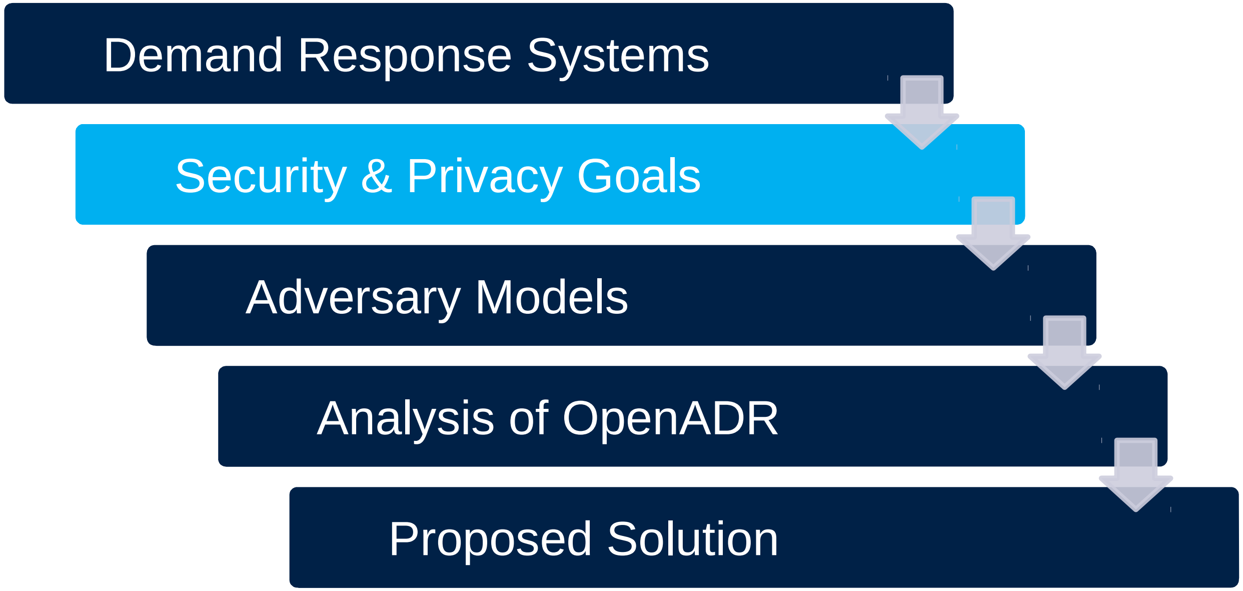
OpenADR 2.0



Source: OpenADR Alliance: The OpenADR Primer (2012)

OpenADR 2.0


Demand Response Manager
Demand Response Automation Server
Participant
Participant
Notify DRAS of DR event
Notify participants of DR event
Participants place new bids or opt out
Forward bids or opt-out messages immediately
Forward standing bids
Accept bids
Notify successful bidders



Demand Response Systems

Security & Privacy Goals

Adversary Models

Analysis of OpenADR

Proposed Solution

Security Goals

Primary security objective: Only legitimate entities participate in the DR protocol

Security Goal 1

Consumers must be able to verify the authenticity and integrity of all DR events.

Security Goal 2

The DR manager must be able to verify the authenticity and integrity of all DR bids.

Privacy Goals

** Based on work by M. Karwe and J. Strüker*

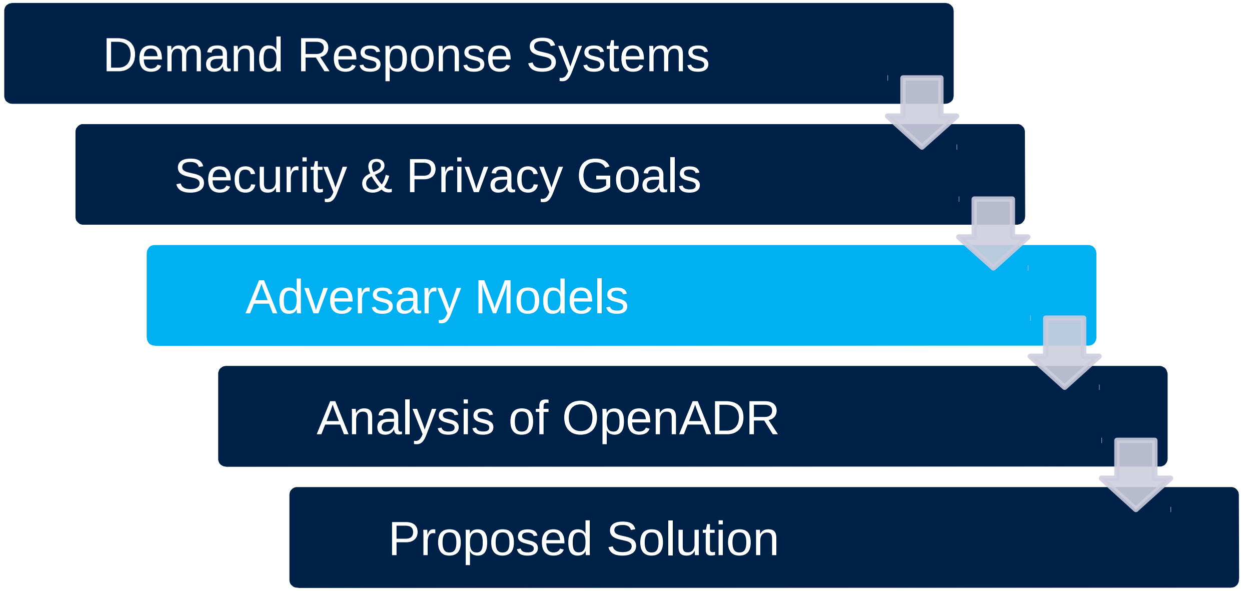
Primary privacy goal: Protect the privacy of individual consumers

Privacy Goal 1

Untrusted entities must not be able to link DR bids to individual consumers.

Privacy Goal 2

Untrusted entities must not be able to infer private information about individual consumers from the DR system.



Demand Response Systems

Security & Privacy Goals

Adversary Models

Analysis of OpenADR

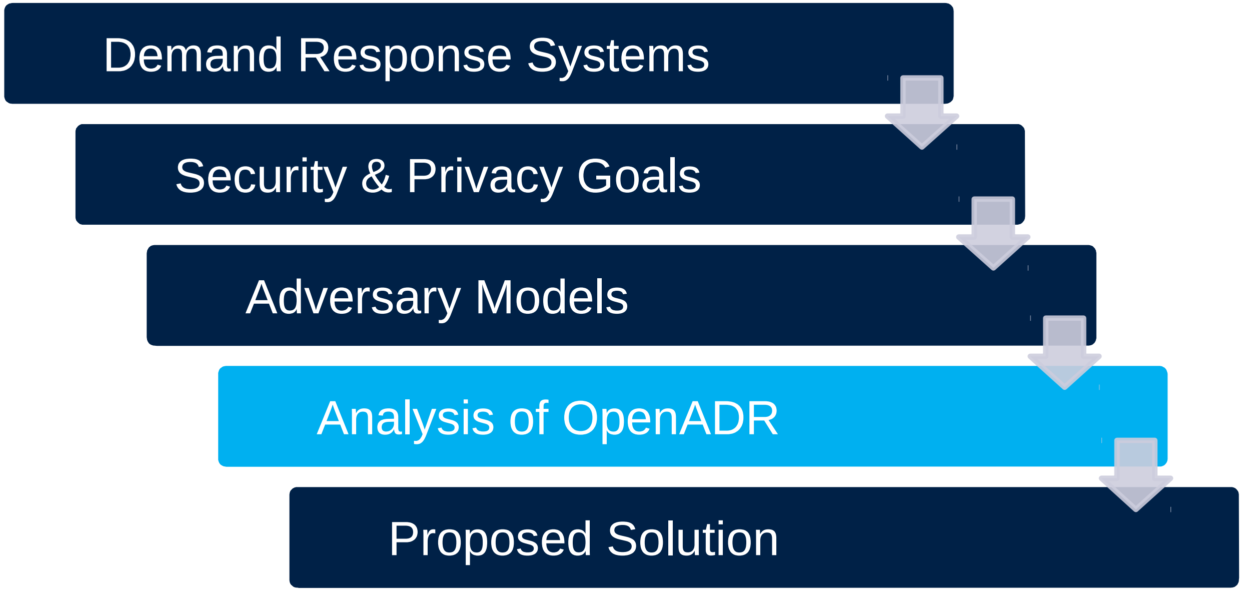
Proposed Solution

Adversary Models

** Based on AMI security & privacy research*

- Dolev-Yao (D-Y)
  - Strongest possible adversary
  - Passive: eavesdrop or intercept messages
  - Active: block, modify, replay or synthesize messages
  - Cannot break cryptographic primitives

- Honest-But-Curious (HBC)
  - More limited than D-Y adversary
  - Always follows protocol
  - Cannot break cryptographic primitives
  - Attempts to learn/infer/deduce sensitive information



Demand Response Systems

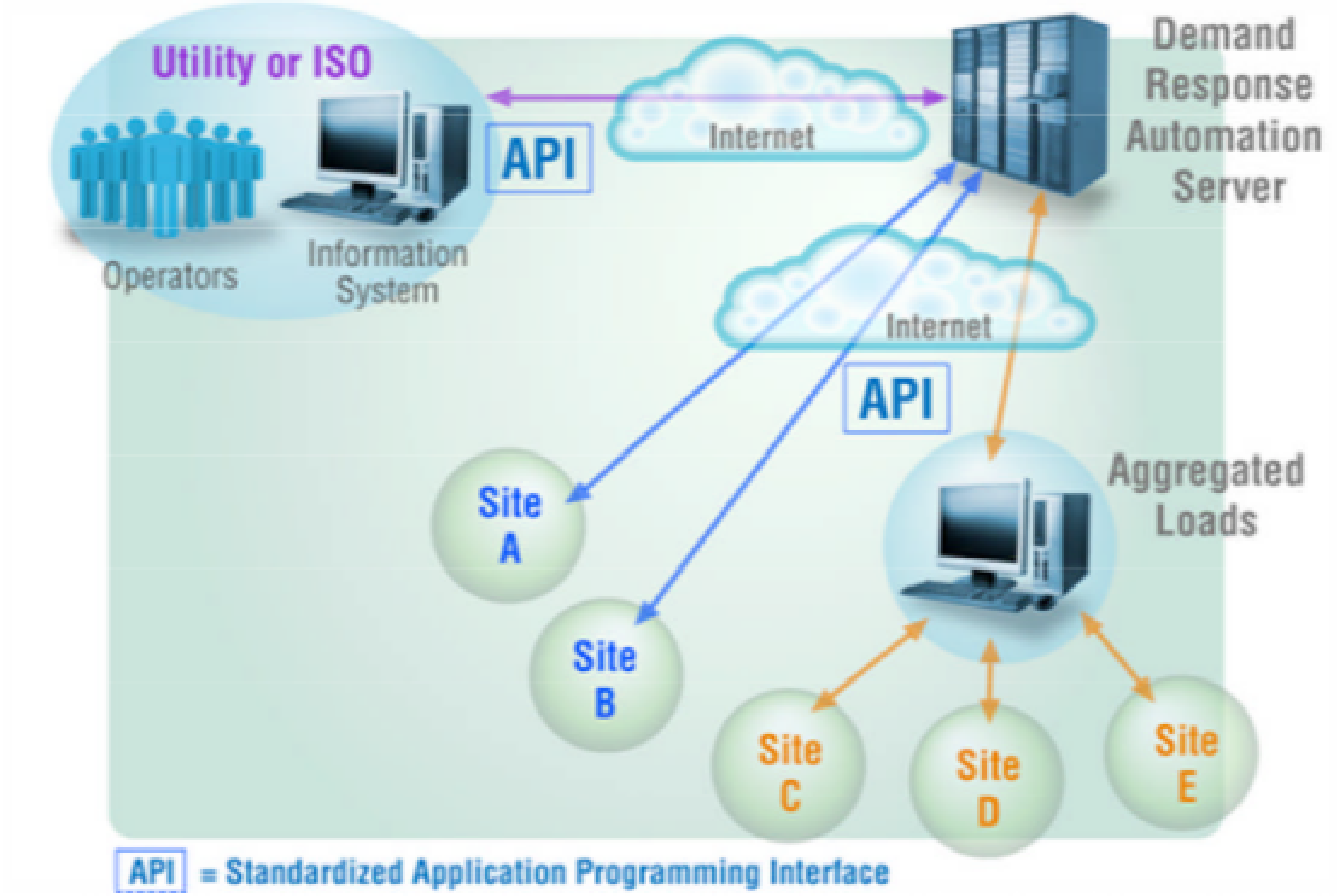
Security & Privacy Goals

Adversary Models

Analysis of OpenADR

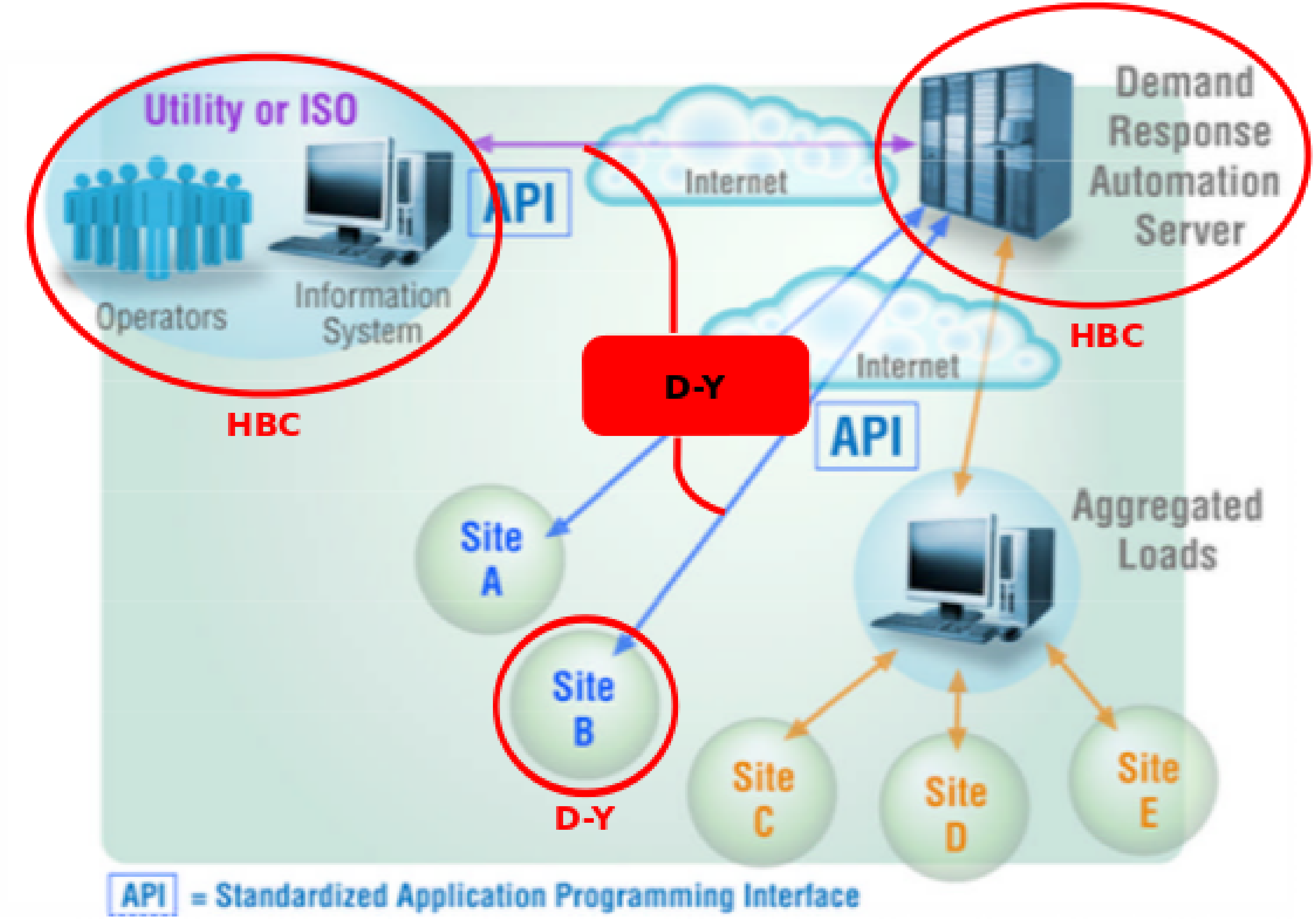
Proposed Solution

Adversary Model for OpenADR



Source: OpenADR Alliance: The OpenADR Primer (2012)

Adversary Model for OpenADR



Adapted from: OpenADR Alliance: The OpenADR Primer (2012)

External D-Y Adversary

Goal	Potential attack	Mitigation
S-1 S-2	Modify messages (e.g. change bid amount)	TLS (integrity)
S-1 S-2	Falsify messages (e.g. falsify bids)	TLS (mutual authentication)
P-1 P-2	Eavesdrop on messages to learn private information	TLS (confidentiality)
P-1 P-2	Traffic analysis (e.g. measure encrypted traffic)	Dummy traffic (permitted by specification)

- Specification satisfies all security and privacy goals
  - * Assuming no compromised keys

Consumer as a D-Y Adversary

Goal	Potential attack	Mitigation
S-2	Falsify messages (e.g. falsify bids)	Detected by service provider (TLS mutual authentication makes consumer uniquely identifiable)
S-2	Masquerade as other consumers	TLS mutual authentication makes consumer uniquely identifiable

- Specification satisfies all security goals
  - * Assuming no compromised keys
- Privacy goals as before

DRAS as an HBC Adversary

Goal	Potential attack	Mitigated using
P-1	Link bids to individual consumers	*End-to-end encryption between consumer and utility (Karwe & Strüker)*
P-2	Infer private information from the received bids	*End-to-end encryption between consumer and utility (Karwe & Strüker)*

- Security goals not applicable (HBC adversary)
- Privacy goals not satisfied by OpenADR specification
  - Require additional mechanisms

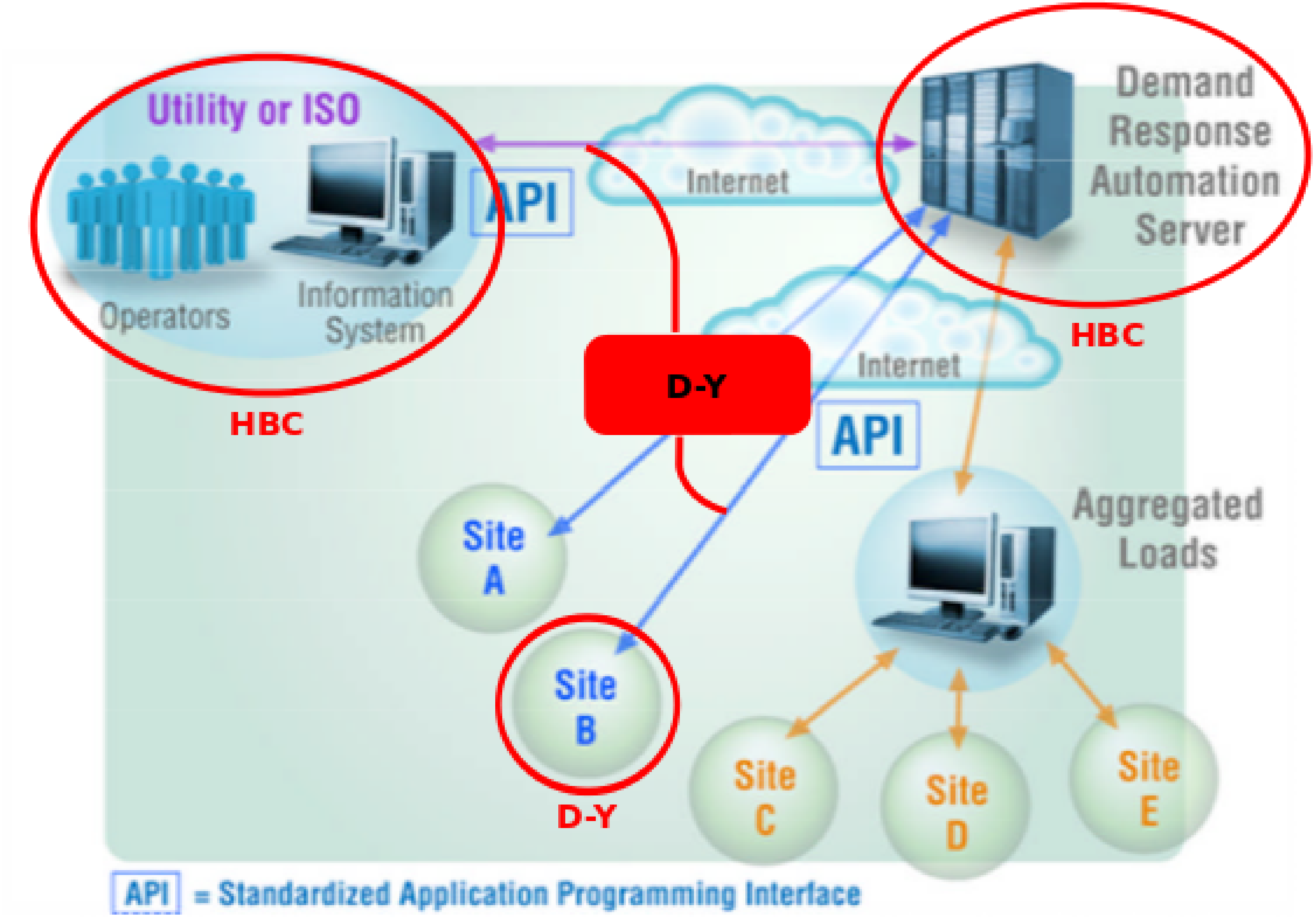
Utility/Supplier as an HBC Adversary

Goal	Potential attack	Mitigated using
P-1	Link bids to individual consumers	?
P-2	Infer private information from the received bids	?

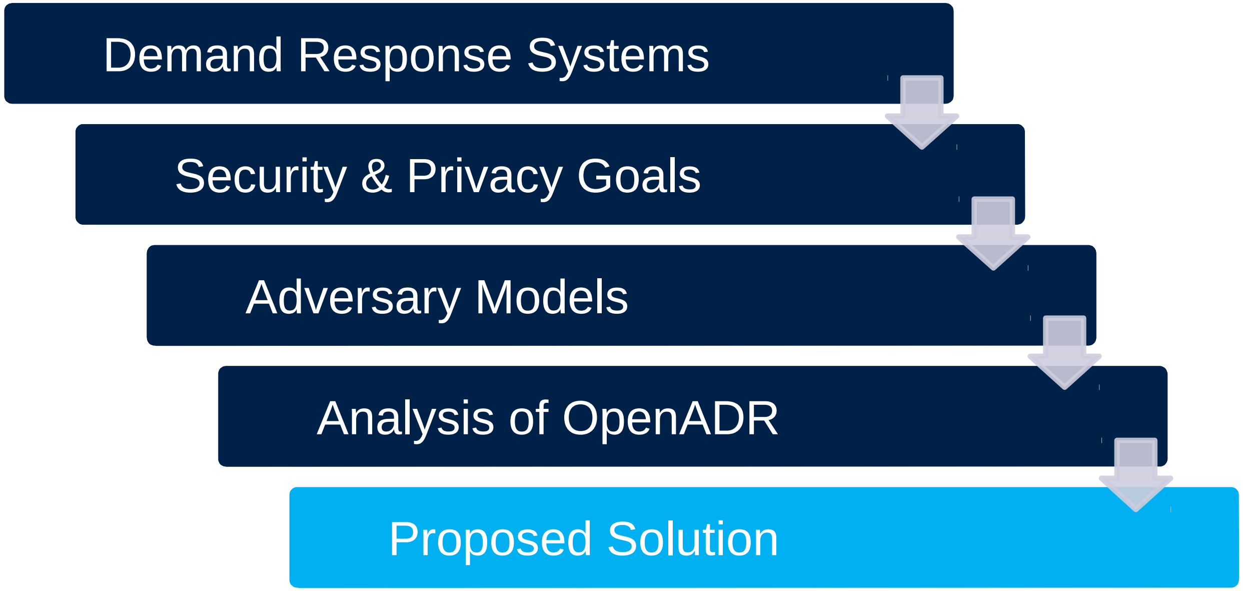
- Privacy goals not satisfied by OpenADR specification
  - Require further research

- Conflict between privacy and security goals
  - TLS mutual authentication allows utility to detect masquerading but ensures that utility will be able to link bids to consumers

Adversary Model for OpenADR



Adapted from: OpenADR Alliance: The OpenADR Primer (2012)



Demand Response Systems

Security & Privacy Goals

Adversary Models

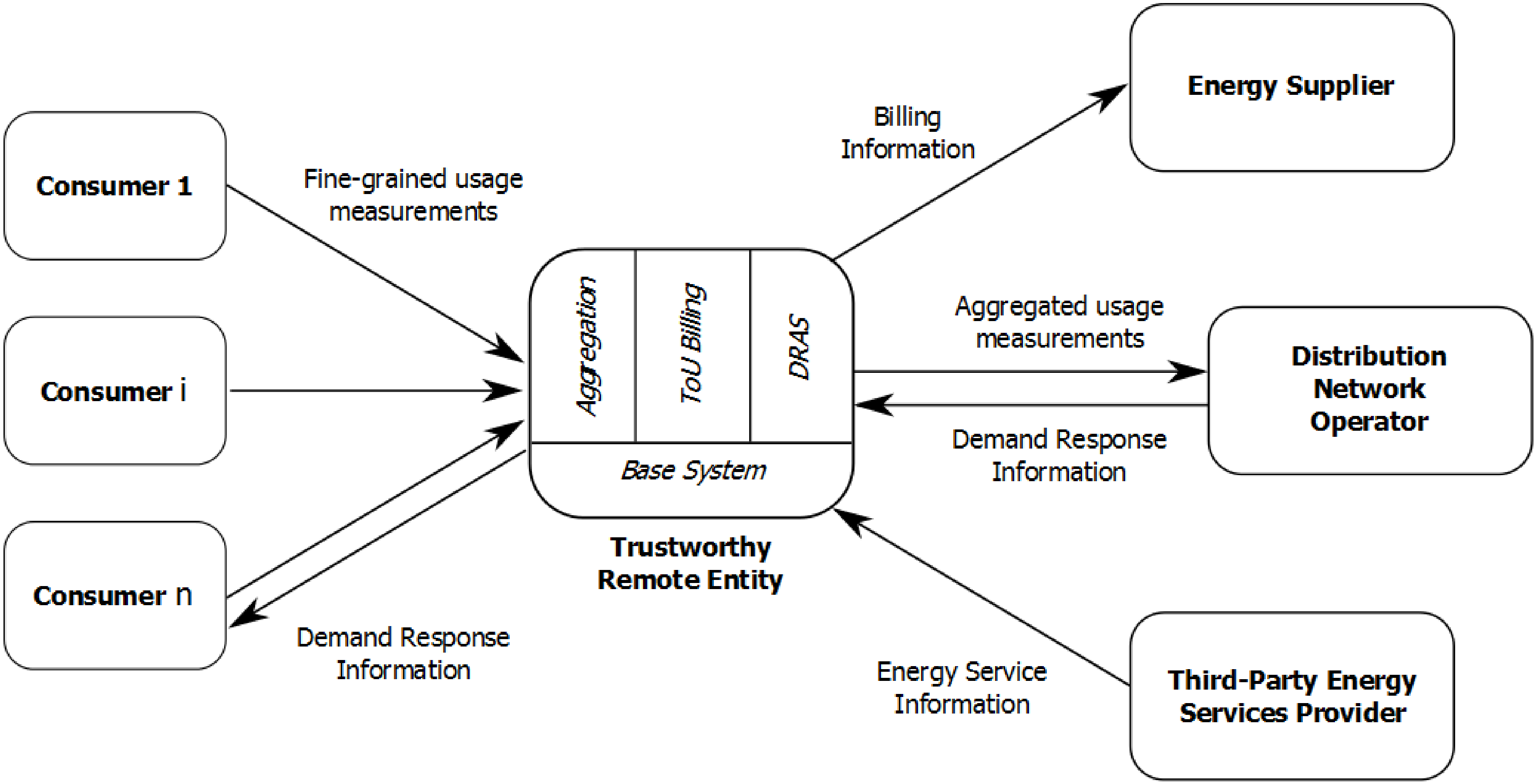
Analysis of OpenADR

Proposed Solution

Trustworthy Remote Entity (TRE)

- Trusted third-party
  - Intermediary between consumers and external entities
  - Information processing (aggregation, perturbation, etc.)
- Utilizing Trusted Computing
  - Secure/measured boot
  - Remote attestation of system state
  - Minimal trusted computing base
  - Isolated execution environment
- Multiple TREs in the grid
  - Multiple redundancy
  - Load balancing

Proposed Architecture


Consumer 1
Fine-grained usage measurements
Consumer i
Consumer n
Demand Response Information
Aggregation
ToU Billing
DRAS
Base System
Trustworthy Remote Entity
Billing Information
Energy Supplier
Aggregated usage measurements
Distribution Network Operator
Demand Response Information
Energy Service Information
Third-Party Energy Services Provider

Conclusions

- DR is an important aspect of the future smart grid
- Specific DR security and privacy goals
  - In addition to smart metering goals
- Various adversary models
- Multiple sources of threats
  - Must be addressed before wide-scale deployment
- Proposed solution
  - Opportunities for further research

Security & Privacy in Smart Grid Demand Response Systems

Andrew Paverd

Department of Computer Science
University of Oxford

Supervisors: Andrew Martin *(Department of Computer Science)*
Ian Brown *(Oxford Internet Institute)*