ISRCS 2012

A Case for Validating Remote Applications for Data Processing Systems

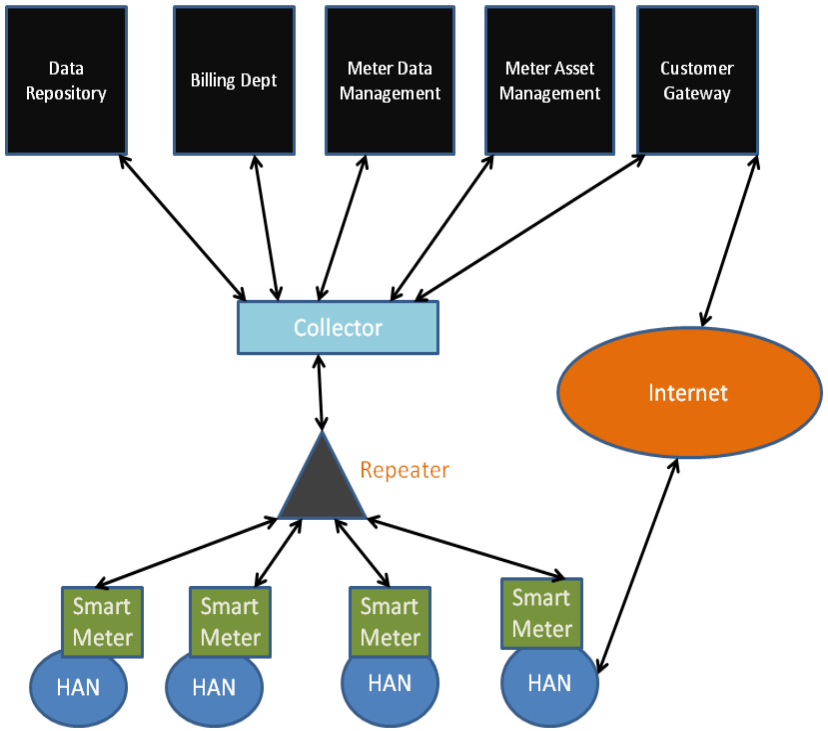
Jonathan M. Chu, Mirko Montanari, Roy H. Campbell

Smart Grid Security

- The smart grid is a growing infrastructure that presents its own set of unique security challenges
- It is composed of different parts such as the Advanced Metering Infrastructure(AMI) and Supervisory Control and Data Acquisition(SCADA)
- As the smart grid becomes more connected to the internet, there is an issue with how to secure the grid especially as it grows each year with the addition of more and more smart meters

Advanced Metering Infrastructure

- AMI is a system that provides 2 way communication with the smart meters
- It may perform such actions as measuring and analyzing energy usage as well as controlling the smart meter remotely
- In an AMI, data goes from the smart meter in people's homes to a Collector which connects the data to the internet



Advanced Metering Infrastructure

- Data from the smart meters may go to multiple places such as a Meter Data Management System(MDMS), a Meter Asset Management System(MAMS), Customer Gateway, Data Repository
- The MDMS may validate the meter data and cleanse it for errors or gaps, before sending it to the billing dept
- The MAMS may monitor the health of the meters and try to determine when a meter is not functioning properly
- The Customer Gateway may prepare the data to be accessed by consumers through the internet

AMI Security Principles

- The main danger from AMI is revealing confidential energy usage patterns of users
- Smart meters in AMI systems can measure what energy is being used and at what times. Some Home Area Networks(HAN) even have meters connected to specific devices allowing companies to know the energy usage of devices such as computers or washers.
- Users usually do not want others to know when they are using certain devices. Privacy is the main issue for AMI.
- AMI systems mainly do the measuring of power usage and do not typically control the distribution of power so availability is not a threat normally associated with AMI

Our Security Design Model

- We believe that security problems arise when systems become too complex and unwieldy to secure
- For every place where data must traverse, another spot must be secure.
- Instead we believe that raw meter data should ideally be stored in one place and if other units/departments want to access it, they can do so by sending remote programs that may be run by the server.

Database Processing Center

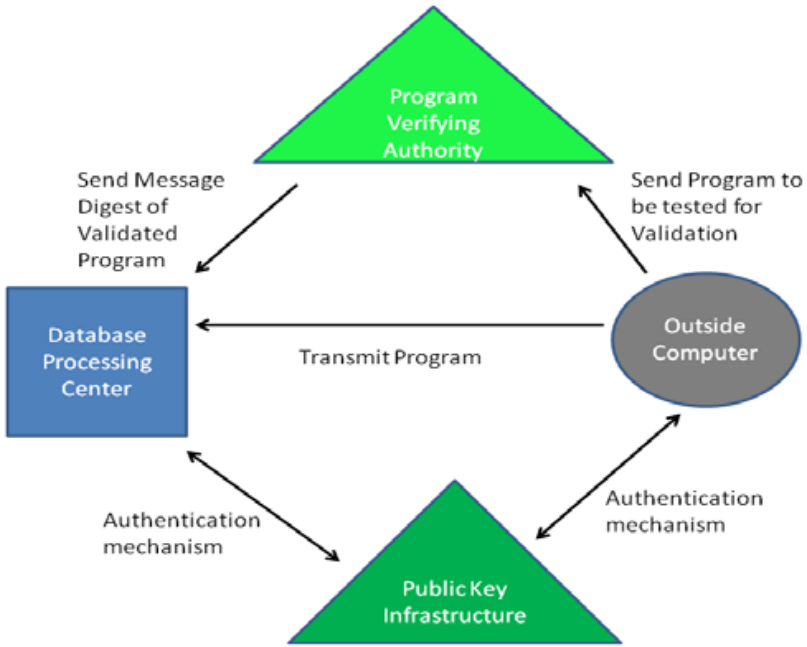
- We call the place where data may be collected and stored as the Database Processing Center(DBPC)
- The DBPC must be able to run other module's programs and should only allow modules to access what they need and nothing more as following the principle of least privilege
- In this way, data would only need to be secured at the DBPC and there would be less attack vectors for malicious hackers to take advantage of

The Importance of Program Validation

- Programs running on the DBPC may be malicious and perform actions that are not expected
- As such servers need to have mechanisms to ensure that programs which are downloaded to be run are safe
- We believe that there should be another component, that does verification of a program to determine that it does what it claims to do.
- We call this component the Program Verifying Authority.
- However, the task of a PVA would be difficult as there is not many tools to determine what a program does and manual code inspection takes too long and is extremely difficult

Setup of a Secure Data Model

- In our setup, the data would only go to the DBPC and be stored there.
- If a unit wanted to extract something from the data, they would need to write a program to be run remotely by the DBPC
- This program would first need to be validated by the PVA as ensuring that it does what the unit claims it does. Then the PVA could keep the DBPC updated on the list of qualified programs



A Need for Tools for Program Validation

- In order for our model to work, there would need to be a program validation mechanism
- However, good tools for program validation do not exist
- Most of the time, program validation is done after the fact as in people run programs and they report bad programs after they have already seen damage

Potential Avenues for Program Validation

- Information flow control looks at which information a program looks at or manipulates. This could be done through such methods as creating a new safe programming language or compiler

- There could also be more tools created to look at static analysis of existing programming languages

Conclusion

- We have analyzed the AMI and demonstrated a use case for how validating proper program execution through such techniques as information flow control could be applied to the Advanced Metering Infrastructure

- To secure smart meter data, there should be more development in these data security techniques. These techniques, if integrated, would help make the grid more secure

Questions