A User-centric Privacy Manager for Future Energy Systems

Authors: H. Simo Phom, Nicolai Kuntze, Carsten Rudolph, Marco Cupelli, Junqi Liu, Antonello Monti

2010 International Conference on Power System Technology

Presenter: Asim Sinan Yuksel

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Overview of Presentation

- Introduction
- Problems and Motivation
- Background (Trusted Computing and Virtualization)
- Proposed Solution
- Conclusion
- My Assessment
- References

Introduction

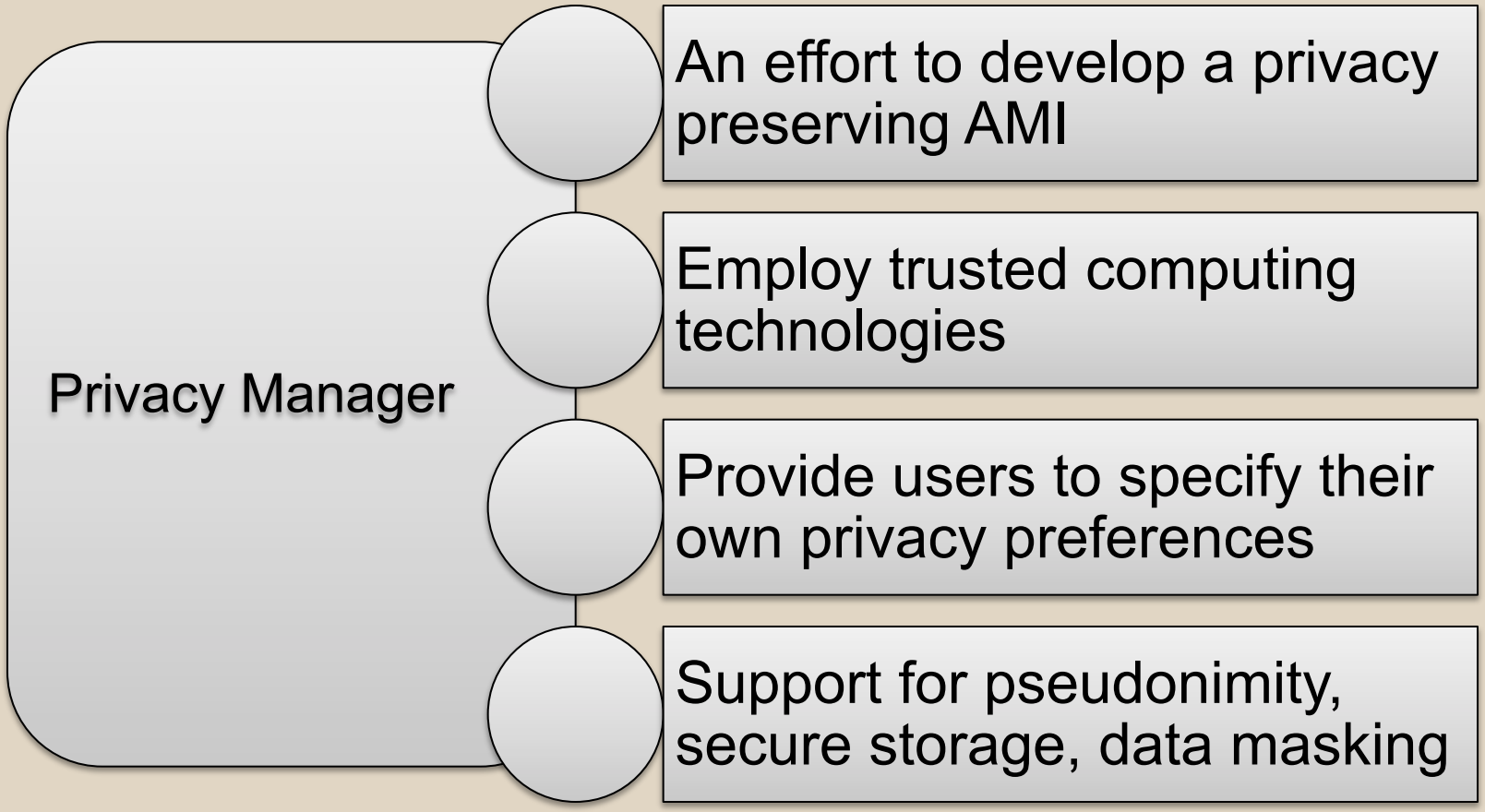
Information

(Ex.: energy usage)

Communication Technologies

Need for Strong User Centric Privacy Protection

Introduction (Continue)



Motivations And Background

- A) Two problem scenarios that motivate the authors:
  - 1) Dynamic metering and pricing schemes for Distributed Energy Resource
  - 2) Remote reinitialization for new customers
- Related privacy concerns.
- B) Key privacy requirements.
- C) Trusted computing.
- D) Platform Virtualization.

Scenario-1

Dynamic metering and pricing schemes for Distributed Energy Resource

- A gateway service provider (utility) provides its customers with SEG.
- Smart Energy Gateway:
  - Displays usage and pricing info
  - Monitors and controls distributed energy generation and consumption.
  - Log transactions.
  - Shared by several stakeholders (grid operator, energy supplier)

Scenario-1 (Continue)

With SEG:

- Customer can monitor its energy consumption and generation capacity.
- Customer can sell the overproduced electricity.
- Utility is able to detect load peaks, and can remotely disconnect a set of customers to reduce load level.
- Third party service providers (billing provider) can retrieve aggregated customer related energy information.

Related Privacy Concerns for Scenario-1

- Customers' usage habits, lifestyle might be deduced.
- Critical business data might be deduced.
- Misuse or uncontrolled disclosure of private data.
- Sharing with a third party without customers' consent and abusive advertisement.
- Combination of electric usage data, vehicle's current position, identity may be used to track the future electric vehicle and its driver.

Scenario-2

Remote reinitialization for new customers

- Smart control devices deployed to remotely capture customer's energy usage information.
- Old customer moves out, new customer moves in.
- As a default policy, energy usage information is needed to be reinitialized.

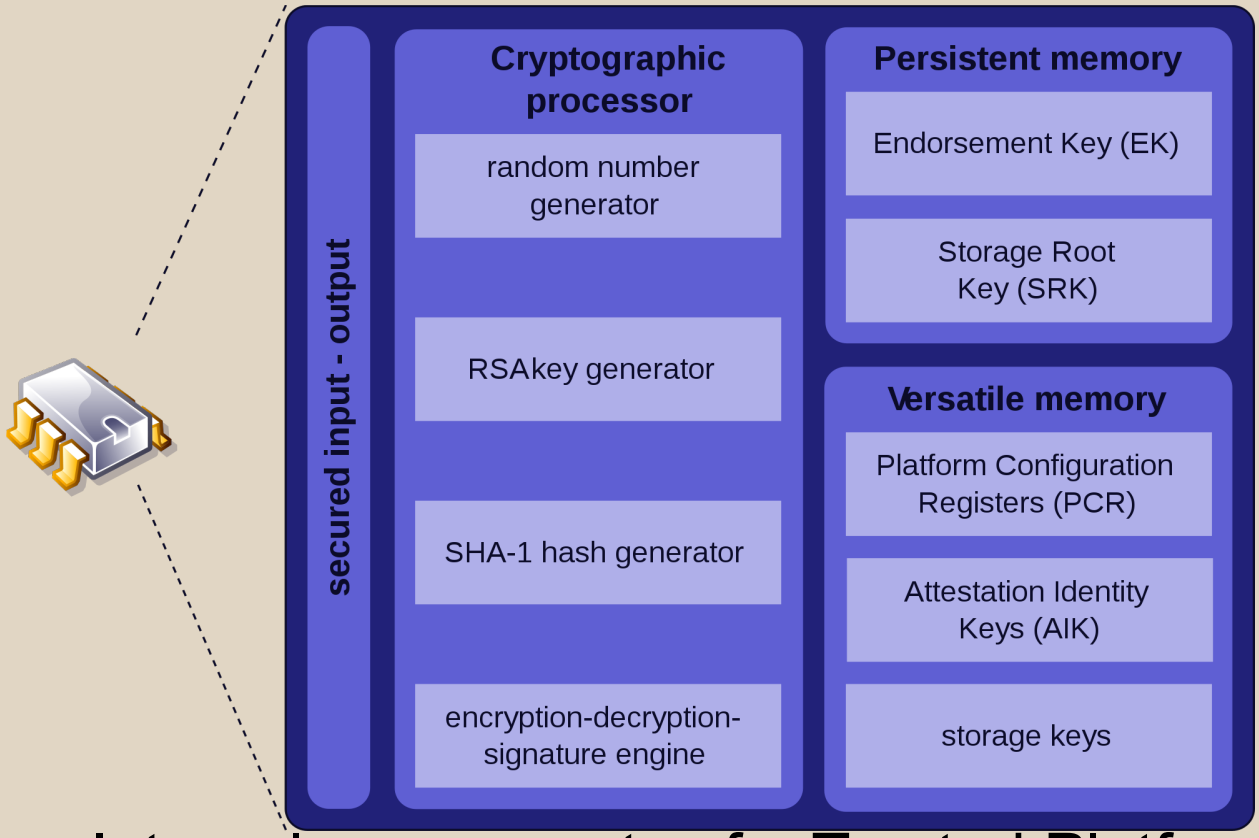
Related Privacy Concerns for Scenario-2

- If energy usage data, which were stored within the SEGs are not fully removed, following information can be deduced:
  - Energy usage patterns.
  - Details about daily routines of old customers.
  - Advanced analysis of metering data could lead to identity theft.

Key Privacy Requirements

- **Requirement-1 (Customer Empowerment):**
  - Notification of Customers.
  - Customer's consent.
  - Setting privacy preferences.
- **Requirement-2 (Data Protection):**
  - Ensure secure storage, transport, process of metered and other sensitive data.
  - Accordance with customer's privacy preferences.
  - Isolation.
  - Secure information flow.
- **Requirment-3 (Data Minimization):**
  - Collect and process when necessary.
  - Using pseudonyms
  - Identity must be hindered.

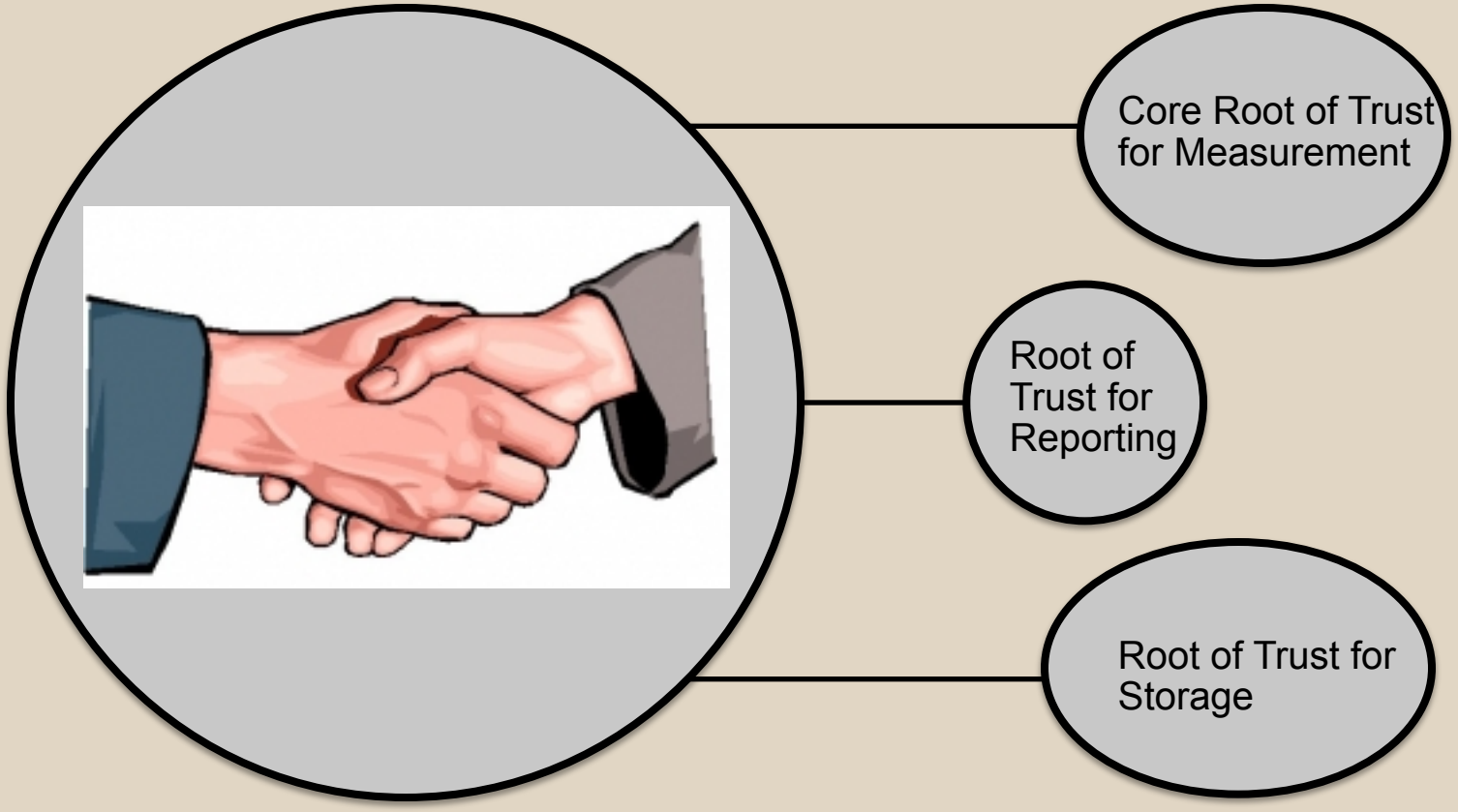
Background-Trusted Computing



Internal components of a Trusted Platform Module
(Figure from http://en.wikipedia.org/wiki/Trusted_Platform_Module)

Background-Trusted Computing

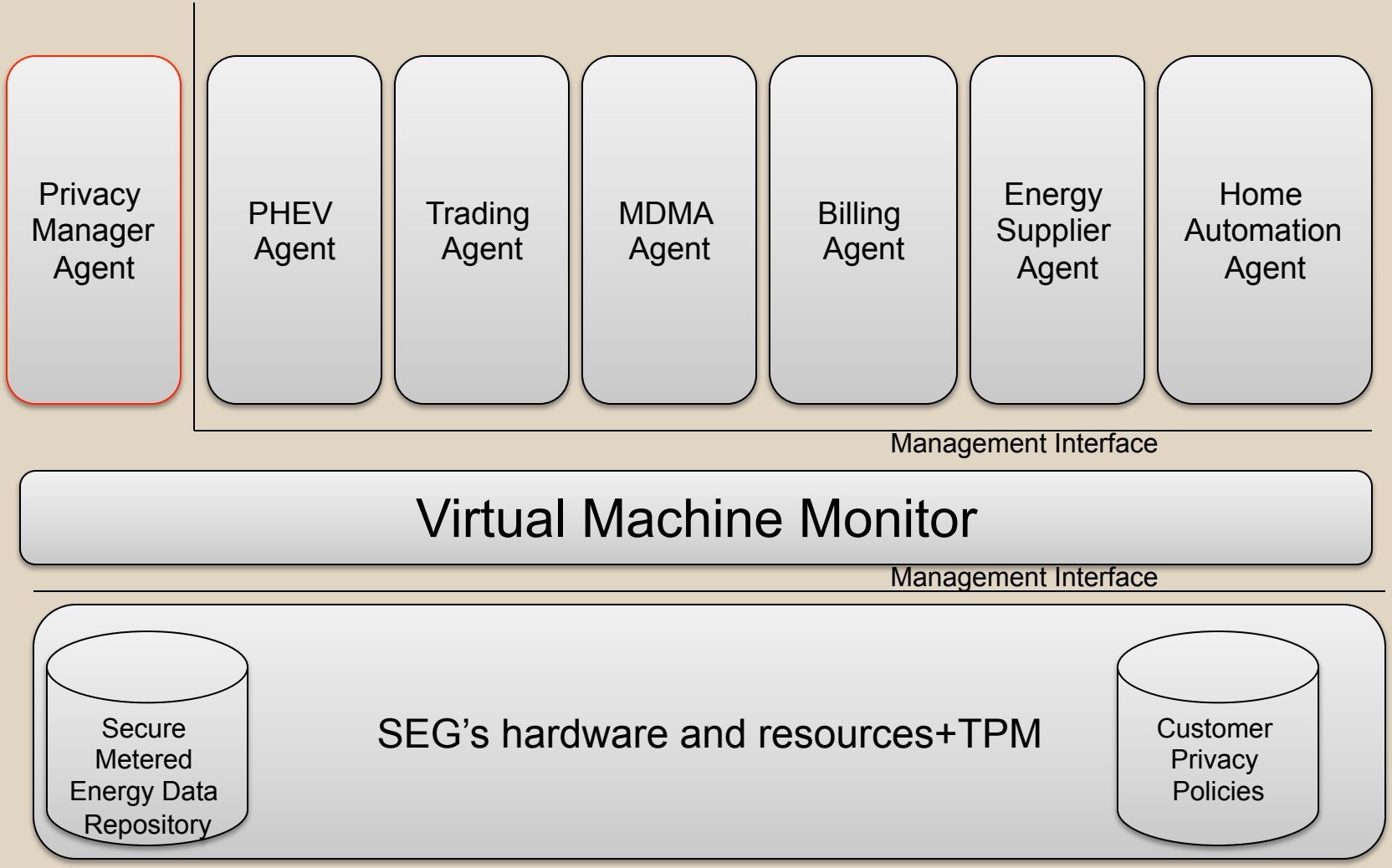
Roots of Trust



Background- Platform Virtualization

- Realizes several runtime environments in parallel but isolates computer platform resources (such as storage, memory, CPU)
- This isolated environment is called VM and provides an interface that is similar to physical shared resource.
- It extends the concepts of TC into virtual machines and provides the illusion of TPM on a VM.

Proposed Framework/Solution



A Trusted Virtualized Multi-Agent SEG Platform

Proposed Framework/Solution

Privacy Manager Agent - Features

1) Privacy Preferences Specification and Enforcement:

- How customer's information will be treated?.
- How revealed personal information should be handled?.
- Secure association between captured data and privacy policies.

2) Privacy Policies Enforcement:

- Validation against the SEG platform integrity policy during installation and runtime.
- Comply with the customer predefined policies whenever the energy usage data are handled.
- Flow of sensitive private.
- Ensure the integrity of VMM and PM.
- Support establishment of trust with the smart grid backend.

Example Policy

<PrivPol PolicyId='SamplePolicy'>

<Subjects> energy supplier; grid operator; utility distributor; end customer **</Subjects>**

<PersonalInformation> vehicle identifiers; serial numbers of in-house smart equipment; account number **</PersonalInformation>**

<AllowedOperations>read, write**</AllowedOperation>**

<Purpose>billing; accounting; pricing**</Purpose>**

<Condition> explicit customer consent; erase data after 12 months**</Condition>**

<Obligation> notify **</Obilgvation>**

</PrivPol>

Sample Energy Data Handling Policy

Proposed Framework/Solution

Privacy Manager Agent-Features

3) Secure Storage:

- Secure data repository.
- Allow only trusted and legitimate application to access metered data repository. (Meets R2)
- Sign energy data.

4) Pseudonymity:

Hide customer identity

5) Privacy Feedback:

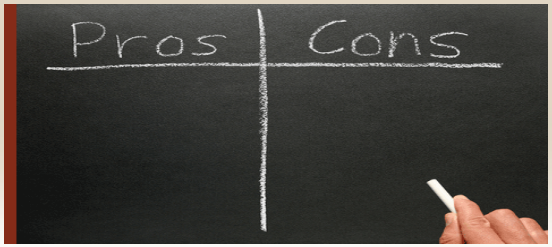
Notify the customer (Meets R1).

Conclusion

Authors proposed a user centric privacy manager which:

- Protects privacy of energy users.
- Helps customers to specify privacy conditions and obligation with respect to handling their private data.
- Provides application isolation, access control, pseudonymity, secure storage, encryption of data before transferring .
- Uses hardware based security (Trusted Computing) combined with virtualization techniques.

My Assessment



Pros:

- Strong privacy protection.
- Secure storage and transfer of energy data.
- Empowers customers
- Provides transparency

Cons:

- Cost of deploying TPM enabled SEGs?
- How to integrate the SEG with current smart meters other devices is not mentioned?
- Recent researches showed that TPM can be hacked. So TPMs are not really that much reliable.
- Very high level picture of their framework.

References

[1] Advanced Metering Infrastructure Security Task Force (AMI-SEC).

[2] Rakesh Bobba, Himanshu Khurana, Musab AlTurki, and Farhana Ashraf. Pbes: a policy based encryption system with application to data sharing in the power grid. In *ASIACCS '09: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pages 262–275, New York, NY, USA, 2009. ACM.

[3] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145. ACM New York, NY, USA, 2004.

[4] Christopher A Cassa, Shannon C Wieland, and Kenneth D Mandl. Re-identification of home addresses from spatial locations anonymized by gaussian skew.

[5] EU Directive. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the EC*, 23, 1995.

[6] EU Directive. 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). *Official Journal of the EC*, L201/37-L201/47, 2002.

[7] Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, and Dan Boneh. Terra: a virtual machine-based platform for trusted computing. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*, pages 193–206, New York, NY, USA, 2003. ACM.

[8] Electric Power Research Institute. Epri use case repository. www.smartgrid.epri.com/Repository/Repository.aspx, 2010.

[9] Michael Lemay, George Gross, Carl A. Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *in Hawaii International Conference on System Sciences. Big Island*. ACM, 2007.

[10] Michael LeMay and Carl A. Gunter. Cumulative attestation kernels for embedded systems. In Michael Backes and Peng Ning, editors, *ESORICS*, volume 5789 of *Lecture Notes in Computer Science*, pages 655–670. Springer, 2009.

References

[11] C. Mitchell et al. Trusted Computing. *Trusted computing*, page 1, 2005.

[12] Organisation for Economic Co-operation and Development. Oecd guidelines on the protection of privacy and transborder flows of personal data.

[13] S. Pearson. Trusted computing platforms, the next security solution. *HP Labs*, 2002.

[14] R. Sailer, E. Valdez, T. Jaeger, R. Perez, L. Van Doorn, J.L. Griffin, and S. Berger. sHype: Secure hypervisor approach to trusted virtualized systems. *IBM Research Report RC23511*, 2005.

[15] TCG Infrastructure Working Group. Architecture Part II - Integrity Management. Specification Version 1.0 Revision 1.0. Technical report, 2008.

[16] J. Tomić and W. Kempton. Using fleets of electric-drive vehicles for grid support. *Journal of Power Sources*, 168(2):459–468, 2007.

[17] H. Zhu, R. Lu, Shen, and X. Lin. Security in service-oriented vehicular networks - [service-oriented broadband wireless network architecture]. *Wireless Communications, IEEE*, 16(4):16–22, October 2009.

Questions?

Thank You!