Suggested documents / papers for review, presentation, and discussion at the seminar:

Cristina Rottondi, Giacomo Verticale, Christoph Krauß: Secure Distributed Data Aggregation in the Automatic Metering Infrastructure of Smart Grids. ICC 2013.

Abstract: “The widespread deployment of Automatic Metering Infrastructures in Smart Grid scenarios raises great concerns about privacy preservation of user-related data, from which detailed information about customer’s habits and behaviours can be deduced. Therefore, the users’ individual measurements should be aggregated before being provided to External Entities such as utilities, grid managers and third parties.

This paper proposes a security architecture for distributed aggregation of smart metering data relying on Gateways placed at the customers’ premises, which collect the data generated by local Meters and provide communication and cryptographic capabilities. We propose a secure communication protocol based on multiparty computation aimed at preventing Gateways and External Entities from inferring information about individual data. The routing of information flows can be centralized or it can be performed in a distributed fashion using a protocol similar to Chord.”


Abstract: “Smart Grid (SG) uses communication technology to gather information about the actual and planned power usage in order to enable efficient power provisioning and consumption. Wireless multi-hop communications are used for exchanging data and control messages between smart meters and the utility. With the advent of cybercrimes, there is a growing concern on privacy of the clients. We argue that any communication paradigm used in the SG should support privacy, anonymity, unlinkability, unobservability, and undetectability. Due to the broadcast nature of wireless transmissions, many cyber-attacks such as traffic analysis and flow tracing compromise privacy of the clients. We propose an innovative scheme for traffic routing that benefits from the enhanced network coding technology. Our analysis shows that our scheme maintains privacy of the users despite the possibility of detecting transmitted traffic by an adversary. Moreover, our scheme has extra favourable features such as less computation complexity and robustness of communication.”


Abstract: “A smart-meter (SM) measures and reports the energy consumption of a user at frequent time intervals, revealing critical private information about user’s energy consumption behavior. In this paper, privacy in a SM system is studied in the presence of an alternative energy source (AES). The privacy power function is introduced to study the trade-off between the achievable information
theoretic privacy and the average power that can be provided by the AES. A single-letter information theoretic expression is provided for the privacy-power function, and its correspondence with the rate-distortion function is established. It is shown that the output alphabet can be restricted to be equal to the input alphabet without loss of optimality, which simplifies the numerical analysis significantly. Some numerical results are provided for various input alphabets and distributions. “


Abstract: “Power utilities globally are increasingly upgrading to Smart Grids that use bi-directional communication with the consumer to enable an information-driven approach to distributed energy management. Clouds offer features well suited for Smart Grid software platforms and applications, such as elastic resources and shared services. However, the security and privacy concerns inherent in an information-rich Smart Grid environment are further exacerbated by their deployment on Clouds. Here, we present an analysis of security and privacy issues in a Smart Grids software architecture operating on different Cloud environments, in the form of a taxonomy. We use the Los Angeles Smart Grid Project that is underway in the largest U.S. municipal utility to drive this analysis that will benefit both Cloud practitioners targeting Smart Grid applications, and Cloud researchers investigating security and privacy.”


Abstract: “Smart electric meters pose a substantial threat to the privacy of individuals in their own homes. Combined with non-intrusive load monitors, smart meter data can reveal precise home appliance usage information. An emerging solution to behavior leakage in smart meter measurement data is the use of battery-based load hiding. In this approach, a battery is used to store and supply power to home devices at strategic times to hide appliance loads from smart meters. A few such battery control algorithms have already been studied in the literature, but none have been evaluated from an adversarial point of view. In this paper, we first consider two well known battery privacy algorithms, Best Effort (BE) and Non-Intrusive Load Leveling (NILL), and demonstrate attacks that recover precise load change information, which can be used to recover appliance behavior information, under both algorithms. We then introduce a stepping approach to battery privacy algorithms that fundamentally differs from previous approaches by maximizing the error between the load demanded by a home and the external load seen by a smart meter. By design, precise load change recovery attacks are impossible. We also propose mutual-information based measurements to evaluate the privacy of different algorithms. We implement and evaluate four novel algorithms using the stepping approach, and show that under the mutual-information metrics they outperform BE and NILL.”