Saal: Simulacron-3	20:00	01:00	Day: 2	Track: Science	nA

Title: **Singing Capacitors and Whining Inductors**

Subtitle: A Practical Introduction to Acoustic Cryptanalysis

Speaker: **Dan Hagon**

Short: *In this talk we provide a practical introduction to Acoustic Cryptanalysis using tools and techniques that are easily grasped and cheaply available. The intention is not to present any new results, but instead the emphasis is on gaining a foundation in the theory of such attacks, so that you will be able to apply them more effectively in more challenging scenarios. As we shall see, such attacks are an extension of other types of side-channel attack (timing and power analysis attacks in particular), with the added promise of bridging air gaps.*

Long: We open by introducing the subject of side-channel attacks with a short review of them in general, and focus on key examples of acoustic cryptanalysis in the literature, including analysis of keyboard emanations, a brief look at an historical account of an attack on the Hagelin cipher machine that played a critical role in the Suez Crisis of the 1950's and the more recent results of Genkin, Shamir and Tromer, which forms the primary basis and inspiration of the techniques we will discuss. We start the technical section of our talk by giving a background to power supplies for microcomputer systems, initially reviewing linear power supplies, so we have a basis on which we can compare them to the operating principles of switch-mode power supplies that form the key element of acoustic attacks. Along the way, we look at the important design principle of feedback and the relation this has to frequency response, which in turn gives us an estimate of the bandwidth of emanated signal available to us. Then, we explore the mechanisms by which key components of switch-mode power supplies can be caused to generate unwanted acoustics, show just how readily they will do so and how rich the spectral content of such signals can be. Our next task will be to look at signal acquisition techniques, where we scratch build an ultrasonic USB microphone with 125kHz of bandwidth, for a price at least two orders of magnitude cheaper than commercially available alternatives, yet still sensitive enough to capture the signals of interest. Specifically, we survey options for transducers, the design of the analog signal path and take a look at high data throughput techniques based on DMA to ensure that we can maintain the data rates required. We then discuss difficulties encountered in getting our signal from our data acquisition board into our data analysis system. Since a considerable amount of the literature on side-channel attacks, particularly simple and differential power analysis attacks, deals with attacks on block ciphers such the Advanced Encryption Standard, rather than public key cryptosystems such as RSA (as dealt with in the Genkin, Shamir and Tromer paper), the focus of our attack will be AES. We will quickly review the processing steps involved in AES and then develop a naive implementation of AES-128, paying particular attention to the construction of the S-boxes, since the data-dependent lookup times are the source of timing variations. Our attack is essentially an adaptation of the classic cache timing attack described by Daniel J. Bernstein, where the leaked timing information is obtained instead via the acoustic channel. Our target machine will be a netbook with an Intel Atom N270 (24kB L1 cache, 512KB L2 cache) together with a cheap and particularly noisy AC power supply (model PA-1700-02). We will discuss passive techniques to improve sound amplification in our test setup which will be familar to anyone who has played a stringed musical instrument. Finally, we move into the data processing and attack implementation section of the talk. In order to determine the run-time of our AES implementation for a given key, we will first need to be able to distinguish the difference in acoustic emanation of the system under load, compared to the idle-load condition. To do this, we will use the discrete-time Fourier transform of the acoustic signal, focusing on a suitable band of frequencies, where