Improved Video Eavesdropping using Pixel Clock Tracking and Complex-Domain Averaging

Christian O'Connell & Markus Kuhn

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

We demonstrate a video-eavesdropping attack on an air-gap protected Raspberry Pi target computer, using an Ettus USRP B200 software-defined radio receiver. Our experiment captures unintended electromagnetic emissions from an HDMI video cable using low-cost, off-the-shelf equipment. The USRP samples a 16 MHz wide part of the UHF radio spectrum, which it outputs as a sequence of complex numbers (IQ down-conversion). We convert that into a live video that approximates the target device's display. Traditionally, such demonstrations only performed amplitude demodulation. We show how phase information, normally discarded, can be used to improve signal quality by allowing periodic averaging in the complex IQ domain, increasing the range of the attack.

Every electrical communications cable, as an unintended side-effect, also acts as a transmission antenna, emitting the conducted information as a wide-band radio signal. This can enable nearby eavesdroppers to reconstruct the transmitted information content, at least partially.

Video signals are a particularly vulnerable source of *compromising emanations*. Due to their periodic nature and high redundancy, their information content can still be recognised in spite of interfering noise. We first estimate three characteristic frequencies: the pixel clock, the line rate, and the frame rate, enabling the reconstruction of an image raster.

We then tune the receiver to a centre frequency near one harmonic of the pixel-clock frequency, and

1. resample the data stream to the estimated pixel-clock frequency,
2. apply amplitude demodulation by taking the absolute value of the complex-valued IQ samples,
3. rasterise the demodulated signal into a grey-scale image, providing an empirically good representation of image content, and
4. average consecutive frames, which often display high levels of similarity, to attenuate noise.

Periodic averaging requires precise tracking of the pixel-clock frequency (around 1 ppb), otherwise image drift results in blurring. HDMI and DVI cables have a pixel-clock line we can track with a Phase-Locked Loop (PLL) as a two-stage process:

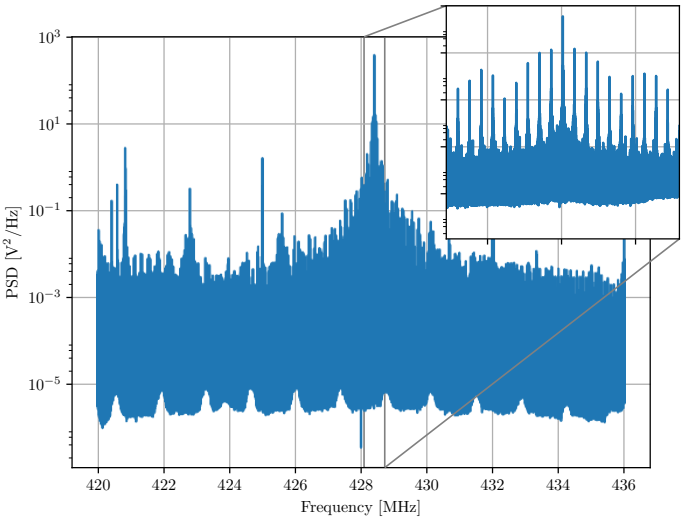

Figure 1: Power Spectral Density (PSD) showing pixel clock as most dominant peak

we first acquire the clock frequency by computing the PSD and searching candidate peaks (Figure 1). We further down-convert and low-pass filter the IQ samples, feeding the result into a Proportional-Integral-Derivative (PID) controller which compensates any remaining frequency and phase error, keeping it constant when averaged over an entire image frame. The output drives the resampling process, keeping the image aligned with sub-pixel accuracy for averaging (Figure 2).

We also use the PID output to unrotate the complex-valued samples, such that the video information presents a deterministic phase, allowing phase-coherent periodic averaging in the complex-domain (*before* demodulation). This better attenuates uncorrelated noise, as its expected value converges to zero, leaving the unrotated signal samples to produce a representative average (Figure 3). In the ideal case of Gaussian noise, we can expect the signal-to-noise ratio to improve in proportion to the root of the number of averaged frames.

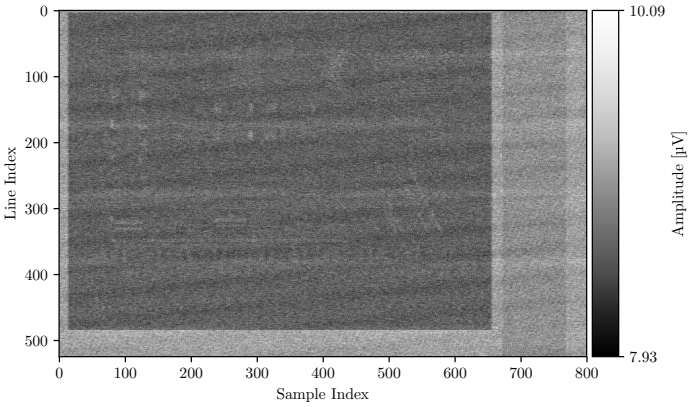

Figure 2: Real-Domain Averaging for 800 Frames

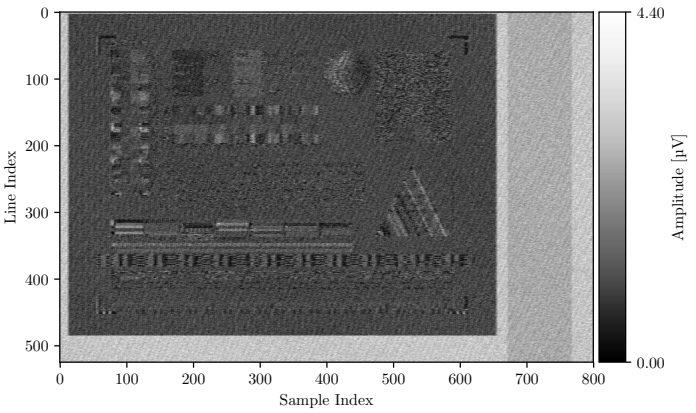

Figure 3: Complex-Domain Averaging for 800 Frames