

Analysing DisplayPort Eavesdropping Risks

Project proposal

Applicant: Stefany Nizamova

PI : Dr Markus Kuhn

Abstract

Electromagnetic emissions from digital circuits can unintentionally leak information; video interfaces including VGA, DVI, HDMI, and LVDS are known to be vulnerable to Tempest-style eavesdropping attacks that recover displayed images using radiated signals. DisplayPort, a newer interface, was considered more resistant due to its scrambled and non-linear 8b/10b encoding; however, recent work demonstrated the first practical attack by detecting scrambler reset times to synthesise a local copy of the scrambler – enabling a template-based attack. The applicant’s prior work extended this by resolving byte-level synchronisation challenges – known as “leap bytes” – to achieve full RGB colour reconstruction.

This project extends that work by addressing open challenges: multi-lane reconstruction and processing efficiency.

The programme is organised in two sequential stages: Phase 1 delivers the multi-lane DisplayPort feasibility study quoted here, and Phase 2 — to be approved subject to the successful completion of D1 — extends the validated methods to embedded DisplayPort (eDP) as used in laptop internal displays.

1 Introduction, approach and outcomes

Background

Tempest attacks are a well-known confidentiality risk and have been demonstrated on various video interfaces. DisplayPort [7] is a newer standard that is significantly more difficult to attack due to its complex encoding format involving a scrambler followed by a non-linear 8b/10b encoding step, resulting in random looking bit sequences. Recent work [1, 2] has demonstrated the feasibility of DisplayPort eavesdropping: by searching for predictable scrambled sequences, the attacker can synthesise a local synchronised scrambler. This can be used to construct template signals that may be correlated against the received signal to recover the transmitted data.

Since the link’s clock is chosen from a small number of fixed values whereas the pixel clock is dependent on the video mode, the average number of link bytes per line is not an integer, and therefore the length of a line varies by one byte. The pattern of these extra “leap bytes” is not well specified by the DisplayPort standard, creating challenges for the reconstruction process. Namely, the eavesdropper must know the position of leap bytes in order to maintain byte-level synchronisation with the source and achieve full RGB colour reconstruction.

This applicant’s work [4] found that the pattern of leap bytes follows the same fractional-accumulator pattern produced by Bresenham’s line drawing algorithm [3], and developed methods to automatically recover the accumulator’s parameters – its rate and phase – from the received signal. Predicting leap bytes from these recovered parameters enabled the first full-colour reconstruction of DisplayPort screen content.

Open problems

Several open issues remain.

Multi-lane — DisplayPort uses 1, 2, or 4 lanes depending on the video mode, and existing demonstrations target only the simplest single-lane modes. Since many common video modes are multi-lane, this extension is a key step towards characterising the practical threat of DisplayPort eavesdropping. From a signals perspective, the emissions of a multi-lane video mode are the superposition of the emissions from each individual lane; separating these may be possible by exploiting the fact that all lanes share the same scrambling sequence, offset by a fixed two-byte delay between adjacent lanes.

Alternative pixel formats — Some monitors automatically select alternative colour depths (e.g. 10-bit rather than 8-bit) which requires adaptations to the constructed templates. Attacks on such colour depths have been demonstrated, however more work is needed to understand the effect of colour depth on the attack and to potentially detect the colour depth from the signal dynamically.

Leap byte pattern detection — The leap byte pattern detection algorithm needs to be tested on a wider range of target images, video modes, device configurations and distances to characterise the attack's feasibility in practice. Different algorithms for leap byte parameter recovery should be tested, such as user-interactive search or integration with the existing scrambler-reset model. It is also possible that the *rate* parameter of the leap-pattern can be inferred directly from the video mode, but more testing is needed to understand whether this parameter is common across different GPU, monitor and driver combinations, or whether it is device-specific.

Processing efficiency — Additionally, there is scope for efficiency optimisations in the reconstruction process, particularly through GPU-parallelisation of key processing steps, which would enable a more realtime implementation. This may be a prerequisite for tackling problems that increase computational complexity, such as multi-lane reconstruction, and would also support interactive exploration of the leap-byte parameter search.

Embedded DisplayPort (eDP) — Finally, DisplayPort is also commonly used across USB-C (DisplayPort Alt Mode) or for internal displays such as laptop screens, where the interface is known as embedded DisplayPort (eDP). Both cases remain open problems due to limited access to their specifications. eDP's principal content-protection method, Alternate Scrambler Seed Reset (ASSR), has very limited publicly accessible documentation [6, 5]; however its name suggests the scrambler LFSR may be reseeded with an alternate value. In this case the attack might extend to eDP with only minor modification, provided the alternate seed can be determined, e.g. by brute-force search over the 16-bit LFSR state space.

Programme structure

The work is organised as two sequential phases with a decision gate between them.

Phase 1 (D1) is the multi-lane DisplayPort feasibility study, covering multi-lane reconstruction, processing efficiency and leap-byte detection. Its scope, objectives, deliverables and schedule are set out below.

Phase 2 (D2) transfers the methods validated in D1 to embedded DisplayPort (eDP) as used in selected internal laptop displays.

Stage gate. Progression to D2 is recommended if D1 demonstrates: (i) working multi-lane reconstruction, or a clear characterisation of the conditions under which it succeeds; (ii) a reconstruction pipeline efficient enough to make eDP experiments tractable; and (iii) no fundamental obstacle identified in the D1 eDP feasibility survey (below). The gate review uses D1’s written report as its evidence base.

Phase 1 (D1): scope of work

This project will investigate the feasibility of electromagnetic eavesdropping against DisplayPort on consumer GPU and monitor hardware. Work will focus on extending the existing attack to support multi-lane video modes and improving processing efficiency.

Phase 1 (D1): technical objectives

Multi-lane reconstruction. Attempt to extend the existing single-lane reconstruction pipeline to support multi-lane video modes, exploiting the fact that the same scrambling sequence is used across all lanes, with a fixed byte delay between adjacent lanes.

Processing efficiency. Develop a GPU-parallelised implementation of the reconstruction pipeline to approach a near-real-time reconstruction and support interactive parameter search.

Leap byte detection. Leap byte parameters (rate and phase) currently must be recovered per-recording. This work will test alternative recovery algorithms, such as user-interactive search.

(Extension) Survey. Time permitting, a wider survey of targets would help determine under what conditions the attack is feasible, and which features or implementations create challenges. This includes testing the full colour attack at distance and against realistic target images, testing against 10-bit colour depth, and investigating whether the leap rate can be inferred from the video mode, rather than recovered empirically, and whether any such relationship is device-specific.

(Extension) eDP feasibility survey. Time permitting, D1 will undertake an eDP feasibility probe — for example, investigating the emission characteristics of eDP links and whether the alternate scrambler seed can be recovered by brute-force search over the 16-bit LFSR state space. This will help guide the D1/D2 stage-gate decision and de-risks the Phase 2 scope. This is scoped as survey only; systematic eDP work is deferred to Phase 2 (D2).

Phase 1 (D1): expected deliverables

- A synchronisation and reconstruction pipeline extended to support decoding of multi-lane DisplayPort video modes.
- A GPU-accelerated implementation of the reconstruction pipeline.
- A written report summarising findings and their implications for DisplayPort’s real-world exposure to Tempest-style attacks.

Phase 2 (D2): embedded DisplayPort (eDP) — indicative scope

Phase 2 transfers the methods validated on external DisplayPort in D1 to eDP as used in selected internal laptop displays.

EM characterisation. Acquire a small set of representative targets and establish a recording setup for internal eDP links (which, unlike external DisplayPort, expose no accessible cable and radiate from the panel and its flat-flex connection). Characterise the emission spectra and identify usable bands. Compare the eDP emission profile against the external DisplayPort baseline.

Reconstruction feasibility. Adapt the Phase 1 reconstruction pipeline to eDP. Investigate ASSR to determine whether the scrambler is reseeded with an alternate value and, if so, attempt to recover that seed — for example by brute-force search over the 16-bit LFSR state space, informed by the scrambler-reset model. Attempt template-based reconstruction of screen content and assess the achievable image quality.

Technical limitations. Systematically characterise the limits of the eDP attack: which panels and configurations are susceptible, at what distances, and which features defeat or degrade it. Produce a threat characterisation for eDP and contrast it with the external DisplayPort threat surface.

Knowledge transfer. Transfer the validated methods and tooling to the funder’s team: documented and reproducible code handover, a setup and operating guide and representative recorded datasets.

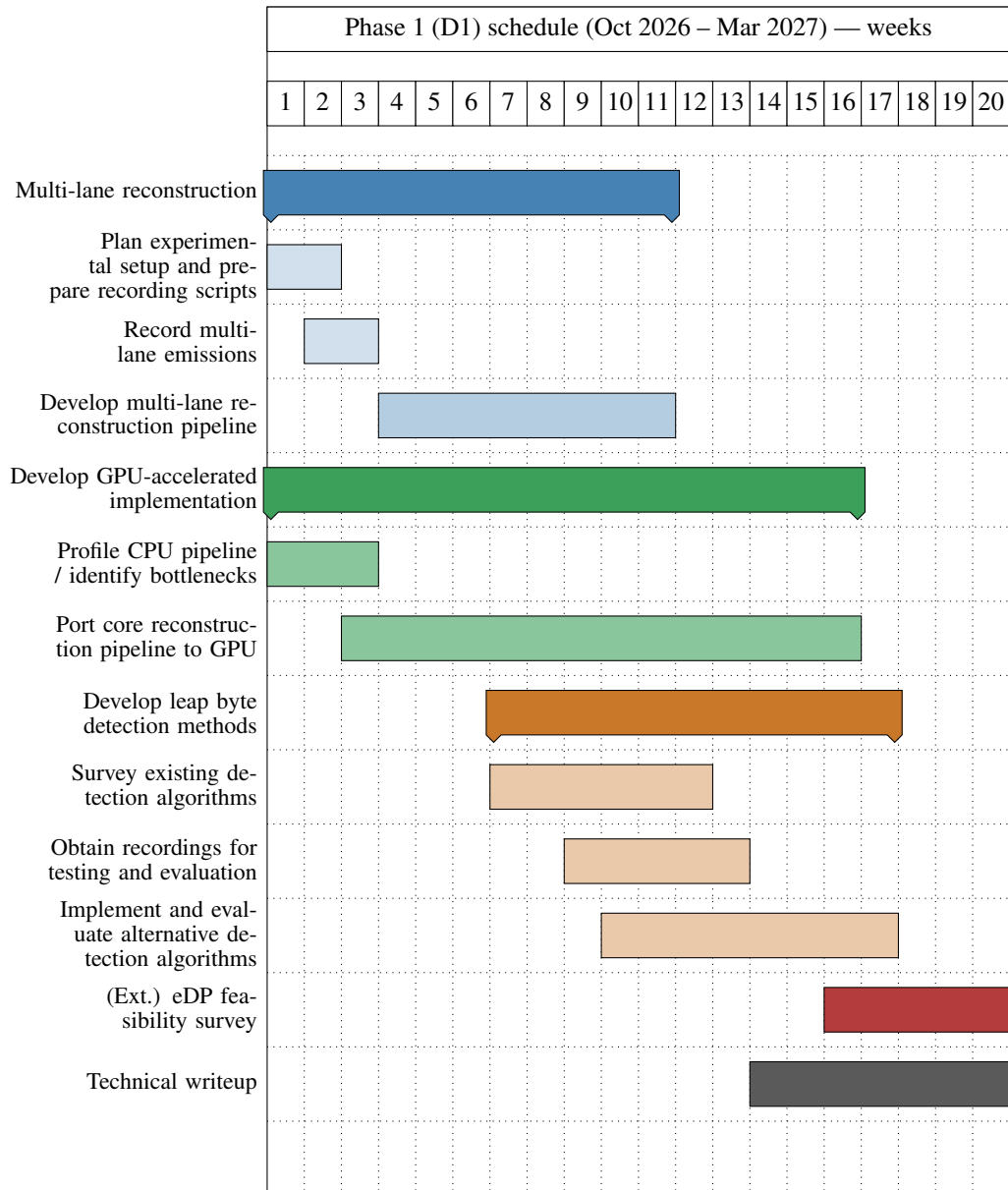
Phase 2 (D2): expected deliverables

- A reconstruction feasibility assessment for eDP, with reconstruction results or a documented negative result, including findings on ASSR seed recovery.
- A technical-limitations and threat-characterisation report for eDP.
- Knowledge transfer package: reproducible codebase, setup and operating documentation, recorded datasets and corresponding results.

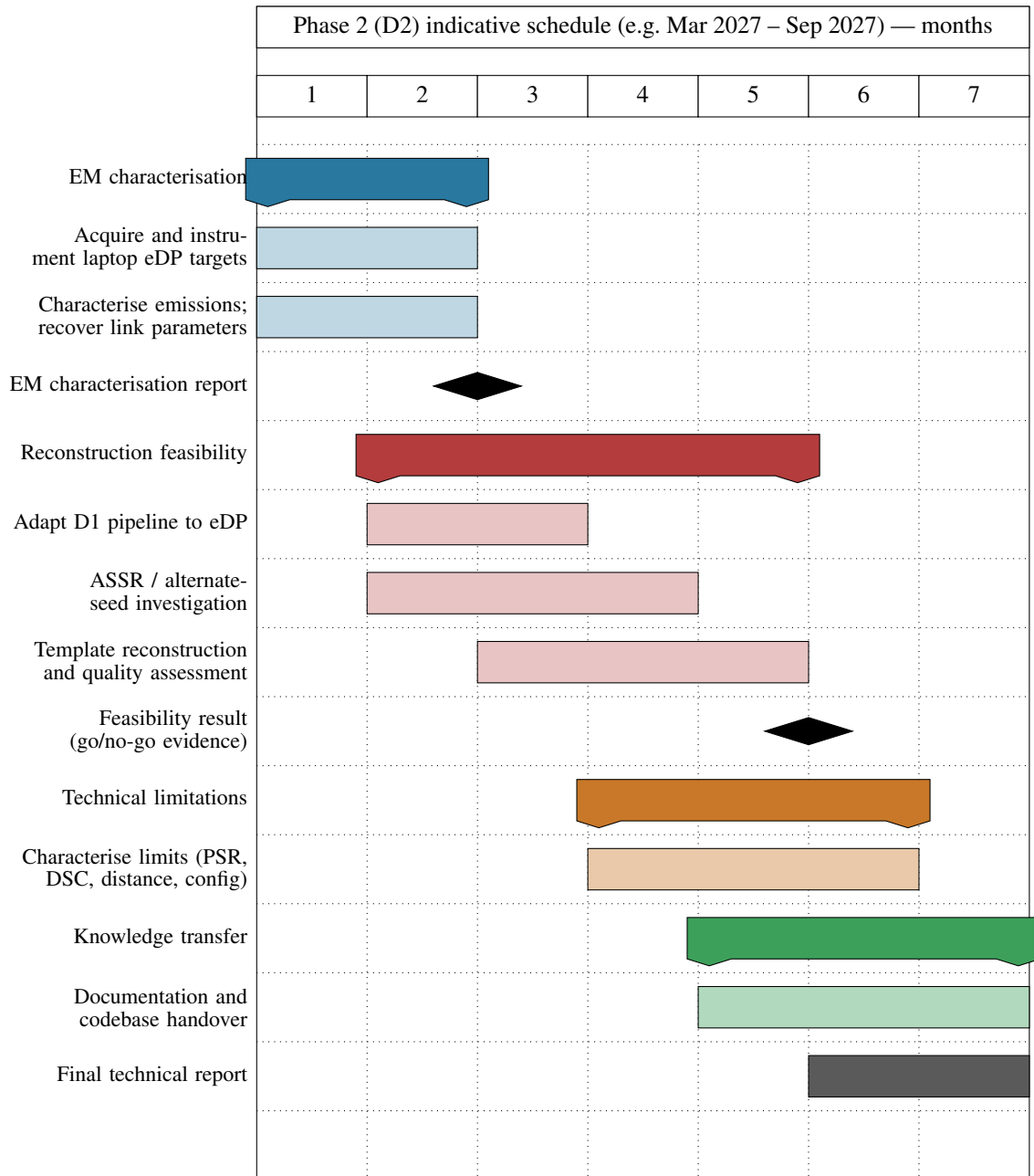
2 Timeline

The schedule below covers Phase 1 (D1), followed by the indicative schedule for the contingent Phase 2 (D2).

Phase 1 (D1): schedule



Phase 2 (D2): indicative schedule



References

- [1] Erdeljan, D.: Eavesdropping risks of the DisplayPort video interface (2023), <https://www.repository.cam.ac.uk/handle/1810/364583>
- [2] Erdeljan, D., Kuhn, M.G.: Electromagnetic eavesdropping on displayport. *IEEE Transactions on Dependable and Secure Computing* **23**(3), 5404–5421 (2026), 10.1109/TDSC.2026.3653840
- [3] Koopman, P.: Bresenham line-drawing algorithm. *Forth Dimensions* **8**(6), 12–16 (1987)
- [4] Nizamova, S.: RGB DisplayPort Eavesdropping, <https://www.cl.cam.ac.uk/~sn630/main.pdf>
- [5] NXP Semiconductors: PTN3460: eDP to LVDS Bridge (2015), <https://www.nxp.com/docs/en/data-sheet/PTN3460I.pdf>, datasheet; lists Copy Protection Method 3a (ASSR) and Method 3b (Enhanced Framing) per eDP 1.2
- [6] The Linux Kernel Development Community: Linux kernel: include/drm/display/drm_dp.h. https://raw.githubusercontent.com/torvalds/linux/master/include/drm/display/drm_dp.h (2024), DPCD 0x00D / 0x10A bit definitions for eDP configuration capability and set registers
- [7] Video Electronics Standards Association (VESA): Displayport™ standard version 1.2. Tech. Rep. Ver.1.2, Video Electronics Standards Association, Milpitas, CA (2010), <https://glenwing.github.io/docs/DP-1.2.pdf>