ProtectIOn: Root-of-Trust for IO in Compromised Platforms

Enis Ulqinaku

System Security Group, Department of Computer Science, Institute of Information Security, ETH Zurich, Zvicër
enis.ulqinaku@inf.ethz.ch

Security and safety-critical remote applications such as e-voting, online banking, industrial control systems and medical devices rely upon user interaction that is typically performed through web applications. Trusted path to such remote systems is critical in the presence of an attacker that controls the computer that the user operates. Such an attacker can observe and modify any IO data without being detected by the user or the server. We investigate the security of previous research proposals and observe several drawbacks that make them vulnerable to attacks. Based on these observations we identify novel requirements for secure IO operation in the presence of a compromised host.

As a solution, we propose ProtectIOn, a system that ensures IO integrity using a trusted low-TCB device that sits between the attacker-controlled host and the IO devices. ProtectIOn intercepts the display signal and user inputs from the keyboard and mouse, and overlays secure UI on top of the HDMI frames generated by the untrusted host. The guiding design principles of ProtectIOn are that (i) integrity of user input and output cannot be considered separately, (ii) all user input modalities need to be protected simultaneously, and (iii) integrity protection should not rely on error prone user tasks like checking the presence of security indicators. By following these guidelines, ProtectIOn achieves strong protection for IO integrity. We also propose an extension of ProtectIOn for IO confidentiality and implement a plug-and-play prototype and evaluate its performance.