



SECURITY VERIFICATION FOR FPGA BITSTREAMS

Automatically evaluate FPGA security settings and apply recommended security fixes

SOLUTION OVERVIEW

Bitwise is a point-and-click assurance tool that delivers rapid security analysis and hardening of FPGA bitstreams. Bitwise validates whether security settings in a generated bitstream are correctly implemented in a FPGA design and provides a security score, without access to project design files or vendor source code.

Bitwise delivers a variety of FPGA bitstream transformation and hardening techniques without requiring pre-requisite expertise or knowledge of vendor tools, as well as provides operators with recommendations for how to mitigate risks posed by identified threats.

CORE FEATURES	<ul style="list-style-type: none"> • Transformation: Perform AES-GCM encryption/decryption and RSA signature resigning/verification • Hardening: Remove/inject commands to prevent breaking of encryption • Security Analysis: Evaluate security configurations, identify risks/mitigations, generate reporting
BENEFITS	<ul style="list-style-type: none"> • Reduces evaluation time from weeks to days spent on security compliance • Reduces complexity in bitstream analysis and hardening • Expands accessibility to a broader set of end-users
QUICK ACTIONS	<ul style="list-style-type: none"> • Evaluate security settings and assess risk exposure according to DoD guidelines • Generate security reports and apply recommended risk mitigations
USER TYPE	<ul style="list-style-type: none"> • Novice, end-users (<i>primary</i>): point-and-click wizard • Expert, end-users (<i>secondary</i>): granular feature access
INTEGRATION & USE	<ul style="list-style-type: none"> • No access to source code or project design files required • Integrates seamlessly into design flow • No prerequisite knowledge required of the vendor tool flow or bitstream
COMPATIBILITY	<ul style="list-style-type: none"> • Current: Xilinx UltraScale/UltraScale+/7-Series • Future: Xilinx 6-Series; Intel Agilex/Stratix/Cyclone; Microchip PolarFire/IGL00

A LEADING SECURITY PROVIDER AND RESEARCH FIRM FOR EMBEDDED SYSTEMS ACROSS INDUSTRIES

Red Balloon Security defends commercial and U.S. Government embedded systems with a suite of host-based security solutions that provide firmware hardening, runtime monitoring and protection to secure embedded systems against exploitation. Our team has been funded by U.S. Government departments and agencies, including DARPA, AFRL, DHS S&T, and Navy.