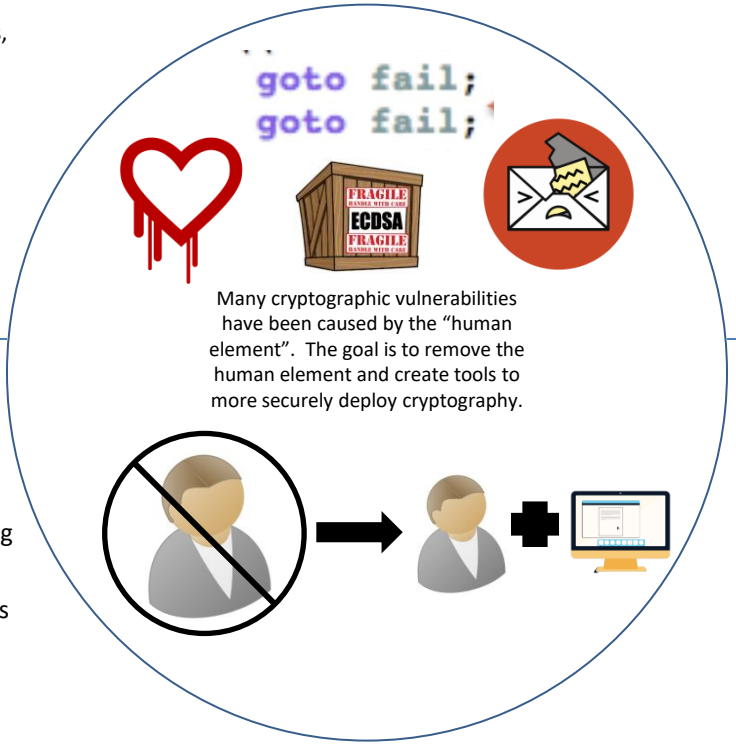
Removing the Human Element: Securing Deployed Cryptographic Systems through the use of Cryptographic Automation

PURDUE UNIVERSITY

Challenge:

- Cryptography is everywhere in our daily lives.
- We have seen a number of vulnerabilities in the cryptographic pieces of systems.
- These have been caused by various problems, including poor designs, difficulty of implementation, and use (or misuse) of (in)secure primitives.
- There is a common denominator: the human element.
- Many of these errors could have been prevented if both designers and software engineers had better tools to help them navigate the complex cryptographic space.



Many cryptographic vulnerabilities have been caused by the "human element". The goal is to remove the human element and create tools to more securely deploy cryptography.

Solution:

- This project is still in its early stages, but thus far we are working to:
- Leverage software security, machine learning, and natural language processing techniques, to discover and identify modern cryptographic algorithms and techniques in heavily obfuscated binaries to help aid in the analysis of closed-source programs.
- Leverage fuzzing, SAT solvers, model checking, and other techniques to help both programmers and end users detect inconsistencies and errors in zkSNARK circuits.

Scientific Impact:

- Make it both easier to discover the use of cryptography and potentially vulnerable algorithms in existing systems as well as design and securely deploy new and complex cryptographic systems while preventing insecurities from happening.
- Automating the discovery and identification of modern cryptography in binary applications.
- Automating the discovery of cryptographic vulnerabilities for advanced cryptography like zero-knowledge proofs.
- Building tools to aid in the secure deployment of complex cryptography.

Broader Impact and Broader Participation:

- Making (sophisticated) cryptography more accessible to non-experts.
- Developing and releasing new tools that help both expert and non-expert developers design and build both new and/or complex cryptography.
- Encouraging students to study cryptography and security who may not have considered it otherwise.

NSF SaTC Award ID: 2047991
Christina Garman, Purdue University
clg@purdue.edu