EFF CUP folks,

Galois has several ongoing projects relating to the intersection between cryptography and usability. Below are several abstracts on these topics.

Most of these abstracts relate to current system summaries in areas relating to usable cryptography, but not specifically for secure, private end-to-end encrypted communication tools. Rather, they focus upon complementary systems, or technologies on which such a tool must rest (e.g., crypto libraries or crypto protocols). Were a prize offered for such a tool, we may well consider building a demonstrator in this area via our non-profit Galois Foundation.

Consequently, we believe that our systems:

(a) provide additional case studies for evaluating usability and security,
(b) we believe that the security and usability of an end user product like a secure, private end-to-end encrypted communication tool is directly dependent upon the security and usability of the technologies on which that tool depends,
(c) we believe that the usability of developer security tools and APIs is as important as the usability of end-user products, and
(d) we have several tools in hand, and relevant world-class expertise available, to help further the goals of the EFF in this space.

We also have expertise in running and participating in contests, as summarized below.

We'd love to participate in a dialog about our thinking about usability of these kinds of systems and the EFF CUP contest.

Best,
Joe Kiniry, on behalf of several other Galwegians including Isaac Potoczny-Jones, Dylan McNamee, Joe Hendrix, Aaron Tomb, and others

---

* Usable and Secure Authentication *

Digital authentication - proving who we are - is a constant necessity on modern networks. Users are buried under the weight of too many passwords, and are faced with a conundrum: good passwords are impossible to remember, and bad passwords are easy to guess. Passwords are the biggest usability and security problem on the Internet today.

Tozny, a Galois spin-out, replaces passwords with a cryptographic app on your smart phone, making login both easier and more secure than passwords. Alternately, use Tozny to augment passwords with multi-factor authentication.

With modern user interfaces on our mobile devices, Tozny believes that easy to use, strong cryptography is at hand. Authentication is only the first step. Once a trust relationship is established, cryptographic authentication can be bootstrapped into an unlimited secure communications channel.

A key challenge with the adoption of Tozny in the marketplace is its usability, both from an end-user standpoint as well as an API usability one. As such, Tozny, or digital authentication in the general, is a topic area rich for analysis and a subsequent CUP competition.

---

* Usable, Verified Crypto Libraries *

Galois develops or uses three key technologies that facilitate usable, verified systems that rely upon cryptography: Cryptol, F*, and SAW.

** Cryptol. ** Cryptol is an Open Source domain-specific language for programming, executing, testing, and formally reasoning about algorithms that operate on structured streams of bits. Cryptol particularly excels at specifying and reasoning about cryptographic algorithms. Cryptol has been used by the U.S. intelligence community for over a decade to specify and reason about crypto systems.

Cryptol version 2 is the first Open Source release of the Cryptol system. Its purpose is to make rigorous applied cryptography available to all----whether in government, academia, or industry---thus we have adopted a BSD license. Moreover, we advocate that Cryptol should be used as the foundation for the specification and verification of past and future cryptographic algorithms standardized via NIST competitions and other similar activities.

The Cryptol system provides: (1) a REPL for experimentation, (2) a parser and typechecker for Cryptol programs, (3) an interpreter for executing Cryptol programs, (4) a validation tool for gaining confidence in the correctness of Cryptol programs via automatic randomized testing, and (5) a verification back-end for formally verifying properties of Cryptol programs through the use of SMT solvers.

** F*. **

F* is a ML-like programming language for the formal specification and reasoning system for secure multiparty systems. F* was developed by Microsoft Research with some academic partners and was recently open sourced under an Apache Foundation license.

F* permits one to reason about the correctness and security properties of protocols like those at the core of any secure, private end-to-end encrypted communication tool. As such, we believe that it use---and systems like it---is a critical component to evaluating the security of any system under consideration within the CUP contest.

Consequently, we believe that an important evaluation criteria for the security properties of any CUP tool is the formal verification of its protocols *as well as* the code that implements said protocols. Tools that have one or both of these artifacts should be evaluated in a significantly better light than those that argue for correctness based upon testing or peer review, both of which are necessary, but not sufficient, for guaranteeing the correctness and security of a high-assurance privacy-preserving communication tool.

** SAW. **

The Software Analysis Workbench, or SAW for short, is a formal verification tool suite developed at Galois. It is capable of mechanically, automatically formally proving the correctness of an implementation against a specification written in a high-level specification language. Cryptol is one of the specification languages supported by SAW.

Galois has used SAW and Cryptol to formally verify several cryptosystems, including pieces of OpenSSL. We contend that technologies like SAW should be used to guarantee that any CUP winner actually implements the (formally verified) security protocols it claims to conform to. Galois, and organizations that Galois can bring into the competition, have a multitude of tools that can be applied to this task as a kind of grand challenge for applied verification. We contend that this is a worthwhile mandatory requirement of any deployed, trusted, trustworthy privacy-preserving communication system and are happy to help fulfill this goal.

---

* Usable Secure Election Systems *

An active area of research that is slowly turning to an active area of development is end-to-end verifiable election systems, known as E2E election systems in the general. Some of these systems are kiosk-based and are used in supervised settings; others are internet-based where voters can vote from home; and still others support vote-by-mail voters.

A paramount---and as of yet unsolved---challenge in designing and developing E2E election systems is their usability. Most of these systems use novel, advanced cryptography to achieve their security requirements. A small number of these systems use novel-but-awkward ballot designs and voting procedures. As such, they are generally recognized as being unusable by virtually all voters, and are thus a failure in a non-academic sense. Usability researchers who have begun looking at these systems find that most voters cannot even submit their ballot successfully, let alone verify their ballot was recorded correctly, counted correctly, or that the election outcome is correct.

Consequently, E2E election systems provide a high-visibility, high-impact case study in cryptography-meets-usability, thus are ripe for gathering ideas about how evaluate such systems in these two dimensions, as well as represent a potential future CUP prize domain.

---

* Experience from Past Contests *

Galois has organized, participated in, or contributed to several past international contests. For example, we organized the most recent Verified Software Competition and we will be organizing the 2015 ICFP Programming Contest, we have participated in past ICFP and Verified Software competitions, and we have contributed benchmarks and thinking to the SAT and SMT competitions.

As such, we have concrete experience about what kinds of contests attract large numbers of interested participants, measurable criteria for objective evaluation of submissions, and the generation of demonstrators and benchmarks in the contest space.