

## Galois, Inc.

Galois specializes in the research and development of innovative new technologies that provide information assurance for challenging systems and software environments. We have extensive experience solving problems in the areas of cross-domain solutions, trusted collaboration, and communications security.

Galois is a technology transition company. We know it is not enough to simply generate innovative ideas — we are committed to transitioning our technology out of the lab and into the hands of users. We are strongly driven to realize the industrial potential of promising technologies; with creative and flexible licensing terms, we are continually building a path for commercialization through new and existing strategic partnerships.

Galois offers the opportunity to engage with us either through a services model — where we work directly on your R&D questions — or by licensing pre-existing technologies, or a blend of both. In brief, the kinds of things we offer include:

### CLIENT SERVICES

- Trusted software development
- Formal methods consulting
- Language and compiler development
- Customized code analysis tools
- Systems engineering
- Safety and security case analysis
- Technology transition support, including in-house training

### TECHNOLOGY SOLUTIONS

- Cross-domain components
- Trusted collaboration designs and components
- Cryptography in software or hardware
- Evaluation-support tools
- Code generation for embedded devices
- High-speed secure networking
- Secure virtualization

Many of our tools and techniques work across many different application areas, as they bring fundamental computer science principles to bear on the tough problems.

In the remainder of the document, we provide more detail our technology offerings in terms of three areas:

[1] *Assurable Components*,

[2] *Assurance Analysis Tools*,

[3] *Assurance Technologies*.

## [1] ASSURABLE COMPONENTS

### Trusted Services Engine (TSE)

The Trusted Services Engine (TSE) is network-enabled software appliance that enables secure file sharing across multiple security levels. The TSE allows users at higher security levels to gain an integrated view with read-only access to un-replicated files at lower levels and read/write access to files at their own level. It has been designed and built for high assurance, including a formal proof that the secure read-down policy will be enforced by the system. The TSE is designed to be hosted on a high assurance separation kernel, and is currently hosted on Security-Enhanced Linux (SELinux) and uses web standards for communication.

### Block Access Controller (BAC)

The Block Access Controller (BAC) is a high assurance cross-domain software component that mediates access between security levels, allowing read/write access to the current security level and read access to lower security levels. The BAC includes a formal proof of critical security and safety properties, in particular that only the intended information flows are possible and that error states are unreachable. The BAC code is generated directly from the formal model used to demonstrate these properties. This design simplicity enables cost-effective high assurance claims. A variant instantiation of the BAC is optimized for streaming data flows.

### Secure Federated Search Manager

Industry and government users need to aggregate and search data that is sensitive and secured as well as data that is freely available and open. Data with different levels of access are kept isolated, either with password protection, VPNs, firewalls, or even by "air-gaps" (where each security level has its own, isolated network). Searching over diverse data sets poses a problem: users cannot perform a single search that will return results from all the systems to which they have access. Indeed, virtually every user of the Internet experiences this problem to some degree. Galois is building a standards-based Secure Federated Search Manager (S-FSM) system that elegantly satisfies these dual requirements, enabling collaboration without compromising security. This solution is compatible with standard web mashup APIs as well as "discovery" systems like RSS and other Web 2.0 tools. A standards-based approach allows our system to aggregate content from search providers that are completely unanticipated by the S-FSM system, that store data in a variety of formats, and that utilize any kind of identity, authentication, and authorization system.

### Tearline Wiki

The Tearline Wiki is a cross-boundary wiki system based on the popular MediaWiki software that powers Wikipedia and Intellipedia. The Tearline Wiki can be used to collaborate across information boundaries, including those spanning multiple clearance levels. Separate knowledge repositories do not contain redundant or divergent information: data stays at its level of origin, but more privileged users can get a combined view of all of the data. The Tearline Wiki can also be used for aggregating multiple wikis. The Tearline Wiki is itself a single level component, designed for integration with a cross-domain component such as the Trusted Services Engine or Multi-Domain Dissemination System.

## Advanced Wiki Technologies (OAuth)

Galois has developed technologies for cross-wiki, cross-boundary collaboration. We have OAuth-based technology to allow wiki systems to share discretionary access control data on a per-page basis, as well as advanced merge capabilities that allow complex branching and other kinds of interaction between wiki instances. These technologies are designed to allow groups in different security domains to engage in rich collaboration without sacrificing the necessary security.

## Cross-Domain RSS

Really Simple Syndication (RSS) is an open standard publish-subscribe protocol for change notification of events or data, commonly used to allow users to maintain a kind of situational awareness across many web sites. The Cross-Domain RSS (CD-RSS) system provides a secure multi-level and cross-domain RSS routing, filtering, search and subscription service, ensuring timely access to news and events online. It is designed for groups collaborating on secure data, giving users the ability to aggregate across protected resources without relaying private security credentials to those endpoints. The CD-RSS is itself a single level component, designed for integration with a cross-domain component such as the Trusted Services Engine or Multi-Domain Dissemination System.

## Cryptol Generators

Cryptol "compilers" can generate software or hardware implementations of cryptography. The software implementations include C, C++, and Haskell, with Java tools currently under development. The hardware implementations include VHDL or Verilog, tuned to specific space and clock requirements. In effect, Cryptol allows engineers and mathematicians to program cryptographic algorithms on FPGAs as if they were writing software, and to explore multiple micro-architectures simply by changing high-level pragmas. These tools significantly reduce overall life-cycle costs by addressing the key cost drivers in the deployment of cryptographic solutions.

## Situational Awareness for Software Protection and Active Response (SASPAR)

Situational Awareness for Software Protection and Active Response (SASPAR) is an ongoing effort to develop an architecture and implementation infrastructure for a software protection mechanism capable of gathering information about ongoing cyber-attacks by highly skilled adversaries and adapting the behavior of running software to defend it against further attacks. The components that achieve this adaptive response are hidden from users and potential attackers using virtualization techniques. As an example use for the architecture, the early stages of this effort demonstrated the capability to detect exploits of software vulnerabilities to stack-based code injection attacks and modify the affected software in real time to block future exploits while keeping the system operational.

## Unavoidable Network Security

Galois has developed key technologies and insights in the utilization of virtualization to provide unavoidable network security. The primary goal of this work is to bridge the gap between today's off-the-shelf operating systems and the highly secure systems of the next ten years by creating a hidden security layer underneath a commodity OS. This security layer can perform any number of security transformations transparently, without the OS knowing; thus, OS-level viruses are incapable of avoiding them. Potential transformations include transparent VPN support for automatically routing through a trusted network, transparent steganographic tunneling of network traffic, or transparent disk encryption for local data.

## Embedded Systems Software

In both safety- and security-critical environments, it often makes sense to use lightweight Real-Time Operating Systems (RTOS) or Multiple Independent Levels of Separation (MILS) microkernels. Writing software for these systems is very different from writing software for a Unix or Windows environment. Galois has expertise in developing software components for RTOS or MILS environments, particularly components whose behavior or security properties need to be semi- or fully-formally described and proven.

## Nettle

Improperly configured computer networks can exhibit poor performance, are subject to attack by malicious agents, and are vulnerable to outages. The Nettle technology is a family of domain-specific languages (DSLs) for programming OpenFlow network switches as if the routing were being done in software.

## [2] ASSURANCE ANALYSIS TOOLS

### Cryptol Language

The Cryptol specification language was designed by Galois for the National Security Agency (NSA) as a public standard for specifying cryptographic algorithms. A Cryptol reference specification can serve as the formal documentation for a cryptographic module, eliminating the need for separate and voluminous English descriptions. Cryptol is fully executable, allowing designers to experiment with their programs incrementally as their designs evolve. The full Cryptol tool suite (which includes Cryptol Verifier and Cryptol Generators; see below) provides a rare combination: high productivity, high performance, and high assurance. Visit [www.cryptol.net](http://www.cryptol.net) for more information, including white papers, case studies, and software downloads.

### Cryptol Verifier

Cryptol tools can verify the faithfulness of an implementation to a reference specification, at multiple stages of the development process. Equivalence can be demonstrated between a reference Cryptol specification and a refinement of that specification, or between a Cryptol specification and a VHDL implementation. Equivalence with Java implementations is currently in development. These equivalence verifications enable the designer to incrementally refine an implementation to trade off space, time, and other performance metrics, while ensuring correctness of each refinement.

### Security Policy Configuration Language

Security-Enhanced Linux (SELinux) provides a very fine-grained, flexible base on which to create secure systems. But the fine-grained control comes at a price: every access right for every user, file, process, and kernel call has to be specified using a very detailed low-level configuration language. Galois' Security Policy Configuration Language is a high-level, hierarchical language for defining and validating SELinux policies and translating them to the low-level configuration language directly used by SELinux. It also allows the expression of legal interactions between components, and for expressing information flow properties over those connections. These same ideas apply to systems of systems and have the potential to be coupled with natural language translation to support natural language policies.

### Automated Security Analysis (ASA)

The aim of our Automated Security Analysis (ASA) is to automatically deduce the information flows in realistically sized C codebases and to communicate them in an understandable way to someone unfamiliar with the code. We have developed an information-flow static analysis and visualization technique, which is currently implemented as a research prototype tool. The static analysis discovers all information flows between program storage locations by decomposing the problem into two compositional properties, each of which can be computed using sound abstract interpretation techniques. For every deduced information flow, the static analysis keeps track of a set of source code locations that demonstrate the information flow, and this is used by the visualization component to communicate the information flow to a user browsing the source code.

## Embedded Software Verification and Validation

Galois has developed a domain-specific language called Copilot used for run-time monitoring of safety and security properties for hard real-time embedded systems, including SCADA systems and guidance, navigation, and control systems in UAVs. The development was in the context of a NASA-sponsored R&D project. Copilot monitors integrate with hard real-time systems, and they generate their own scheduler, obviating the need for an underlying RTOS. The language and compiler are open-source and include formal methods to ensure compiler correctness.

### ASN.1 Assured

ASN.1 is a data description language used extensively to specify the format of messages in almost every networking protocol in wide use today. It specifies how the data should be translated from internal representations to a binary, transmissible form and back again. ASN.1 encoder and decoder routines form the first line of defense for most network enclaves and are, therefore, also common targets of attack. We have developed tools to support high assurance development of applications of ASN.1 encoder/decoder routines, with a proof-of-concept compiler, an interpreter, and a tool supporting systematic, property-based testing of ASN.1 encode/decode routines (based on generating random values conforming to the given ASN.1 specification). The last of these, known as the ASN.1 Validator, has been used to find bugs in code generated by JSNAC (an ASN.1 to Java compiler) and is in use at an operational organization (as part of their build scripts).

### XML Assured

XML can be found at almost every layer of the standard software stack: network traffic, configuration, SOA, cloud computing, and application data storage, to name but a few. Based on our experience in building tools to support the development of high assurance ASN.1 encoder/decoder routines, we have designs for applying the same underlying technology to XML: tool support for property based testing of XML parser/serializers (modulo a given XML schema), a verified schema conformance checker, and a verified run-time library (providing generic parser/serializer routines). The latter has the potential to provide a software upgrade path to high assurance without needing to change application code at all: simply relink against the verified run-time library instead.

### [3] ASSURANCE TECHNOLOGIES

#### Formal Methods

Galois is a world leader in the use of applied formal methods in the development of high assurance software, with experts in the use of theorem proving and model checking for software verification. In house, we add formal methods capabilities to domain specific languages such as Cryptol and ASN.1, allowing users to produce security-critical components without the formal methods being “in your face.” We also use formal methods directly to prove significant properties of critical components.

#### Languages and Language Tools

Galois was founded as a company using insights and methods from functional programming to build trustworthy software. In particular, we rely on the Haskell programming language ([www.haskell.org](http://www.haskell.org)), infrastructure, community, and culture for much of what we do. Galois is the largest Haskell engineering house in the world. We also have a world-class reputation in the design and use of domain-specific languages and language tools for static and dynamic analysis of software to solve difficult problems in software security and safety.

#### Virtualization

Virtualization is an increasingly important technology that is being used to improve manageability and scalability of enterprise and cloud services. Sometimes it is assumed that using virtualization automatically improves security, because it creates a protected “sandbox” to isolate untrusted software, or to isolate trusted software from an untrusted environment. While this can be true, it requires careful design of the information assurance architecture. Galois is well versed in principles of virtualization design, including introducing policy-enforcing reference monitors, demonstrating their correctness, and developing an argument that they enable the broader security goals of the system. Galois also provides software for rapid building and configuring of lightweight virtual machines without the need for a full operating system on each machine.