Lillypond: A Platform for Independent Data Ownership

By Richard Hurley and Keith Guidry

Problem

"Many dedicated people join global non-profit organizations to help, but the market often fails to fund or incentivize building the necessary infrastructure. I have long expected more organizations and startups to build health and safety tools using technology, and I have been surprised by how little of what must be built has even been attempted. There is a real opportunity to build global safety infrastructure, and I have directed Facebook to invest more and more resources into serving this need."

Building Global Community - Mark Zuckerberg - Thursday, February 16, 2017
www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/

Abstract

Modern hospitals, Primary Care Providers, and Care Providers do not effectively or completely communicate important information among themselves, to the individual, or to those taking care of the individuals in a timely fashion. One study estimated that 80% of serious medical errors involve miscommunication during the hand off between medical providers. This error is compounded by continuous care scenarios stretching over decades of change and uncertainty. Such failures put special needs individuals at greater risk as interaction with internet services become more invasive, more complex and increasingly compromised.

Lillypond seeks to place within ownership of the individual a hyper-secure conduit for peer-to-peer agent automation intended to interdict improper and exploitive interaction on the internet. Designed to intercede between children with autism and increasingly nefarious exploits on vulnerable and unprotected communities, the Lillypond system uses hardware and software technologies to build an adaptable independent intelligent hedge between the child with autism and what blackhat technologists call 'the wild'. Lillypond intends to provide the individual with autism with an auditable record of smart-contract adaptable notations for interoperation with care services in any facet of modern life for a lifetime of care.

Stated Simply

Recent events demonstrate a lack of responsiveness to privacy demands by large companies dominating parts of the internet. The average internet user (User) faces many difficult challenges in securing personal data and maintaining documented proof of interaction with people and services on the internet. This difficulty is insurmountable for many people challenged by a disability such as autism.

A child with autism must have constant supervision to prevent improper or damaging interaction with internet sites as a child. But when a child with autism reaches adulthood, they are often expected to answer for their own internet usage and to reproduce documents to demonstrate their electronic interaction. When their parents or guardians pass on, the adult with autism is left in an unguarded world actively working to subvert their independence and prey upon their values and assets.

Lillypond is intended to form a historical basis detailing interaction and behavior during periods of internet use. This audit trail and captured data is designed to create a permanent electronic record for a child with autism, creating a pattern of interactions to build a trustworthy record of communications and documents with caregivers,

friends and useful resources. The accumulation of historic records and documents creating this trail serves to protect the child's interests by codifying communication behavior between the child and the internet world. Such a record secured throughout the years leading to adulthood can be used to present a record of independence for consideration in the young adult's effort to live a productive future. Securing this record with relevant documents and transactions throughout the individual's internet use can have added advantage in building an accurate metric for calibrating the level of care and concern a disability will require during adulthood. This must be a private, non-invasive method which can stand as an objective measure of computer/device use behavior as a supervising gateway for family, friends, pen-pals and caregivers while pro-actively interdicting evidence of improper interaction with strangers and websites used for nefarious purpose.

This ability to watch internet communications as they pass to and from the individual's computer will be carried out by a next-generation set of hardware methods which replace tasks currently done by vulnerable software. A hyper-secure communications 'sniffer' allows for the recording of behavior which may be analyzed by an automated artificial intelligence screening process. That process can be refined for the user's purposes with feedback to the interdicting capabilities of a planned overwatch device called 'Lillypad'.

As social media is the most obvious current means of interaction between children, young adults and older adults, we view 'internet use' as meaning user interaction with search engines, news and entertainment sites. Most communicative interactions are carried out using Facebook or other similar platforms such as Twitter. But there are many 'social media' software platforms in existence [1].

As each social media site has specific strengths and vulnerabilities, users have little control beyond broad privacy settings in each program to attempt to manage data use.

Recent news reports and testimony by the CEO of Facebook, Mr. Mark Zuckerberg, indicate that social media is not a safe place for the special needs community at large to use. This increasingly alarming fact admits even fully capable adults are unable to keep their own internet actions safe and auditable. As it is unlikely Facebook or any other large social media operations will focus their privacy and safety efforts toward a small business space such as the autism community, Lillypond intends to take up this task where social media is unable.

Description

Lillypond, as proposed by this white paper, is a first generation article use-case employing a novel hardware defense technology to allow creation of a user's independent historical basis for an auditable accumulation of pointers to documents encountered during the lifetime of a challenged individual. To accomplish this kind of immutable audit reference, the Lillypond System (System) will begin with the Lillypad Device [Device], a quantum resistant symmetric key engine with Merkle tree assurance across hardware agent technology. The single key nature of the circuitry means no key combinations are available beyond those created invisibly and used within the micro-circuitry, and are not distributed or accessible beyond peer-to-peer defense machines. Merkle Tree assurance [2] (the overarching basis for Blockchain type record keeping and robust automation processes) maintains a continuity of medical records needed in government interaction with parents and guardians (Wardship) for transfer of childhood behavior to adulthood independence metrics for this challenged individual (User). The intended first article Device seeks to equip each User with an indisputable independent record able to sustain a full audit pursuit while functioning as a living document reference system throughout the User's life.

The importance of this type of record keeping can be seen in Figure 1.

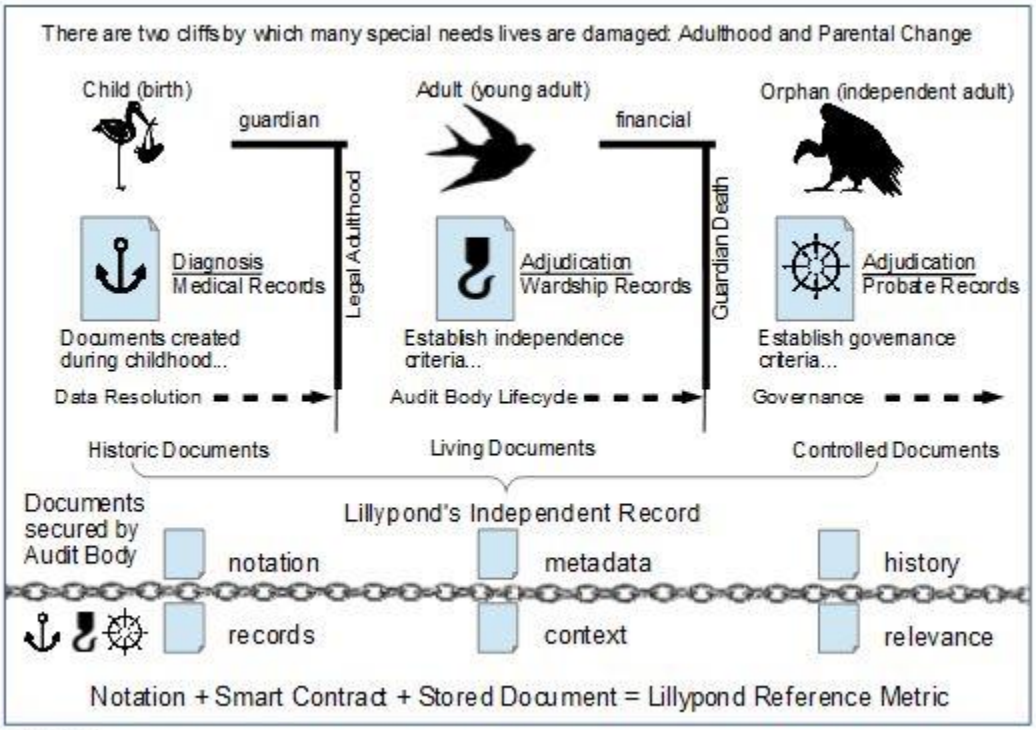

Figure 1

Healthcare management can only evolve if platforms are open to engage with many arbitrary service providers. It is difficult to gain entry to the healthcare marketplace as siloed players such as insurance companies and hospital networks lock in data and prevent new competitors from arriving in the space.

Lillypond intends to provide an open platform for competition while securing individual data using Merkle tree assurance and hyper-secure agent-based communications. We invite other innovators to create a distributed technology society built around artificial intelligence (AI) and open platform competition using Lillypond's notation engine smart outputs.

The Challenge

The central problem has to do with medical records. With a child with autism, every aspect of the child's behavior becomes a potential issue for review by caregivers and medical coverage. For that reason, parents of autistic children have few options beyond 'parental controls'. Such controls only offer a way to block large sections of internet content while providing nothing in the way of reliable, trustworthy and auditable records demonstrating the child's historical activity.

These observations from government study show the need for interoperable records is acute and long standing.

"The nation needs an interoperable health system that empowers individuals to use their electronic health information to the fullest extent; enables providers and communities to deliver smarter, safer, and more efficient care; and promotes innovation at all levels." [3]

"While many stakeholders are committed to achieving this vision, current economic and market conditions create business incentives to exercise control over electronic health information in ways that unreasonably limit its availability and use. Indeed, complaints and other evidence described in this referenced report suggest that some persons and entities are interfering with the exchange or use of electronic health information in ways that frustrate the goals of the HITECH Act (Health Information Technology for Economic and Clinical Health Act) [4] and undermine broader health care reforms. These concerns likely will become more pronounced as both expectations and the technological capabilities for electronic health information exchange continue to evolve and mature." [5]

“Most complaints of information blocking are directed at health IT developers. Many of these complaints allege that developers charge fees that make it cost-prohibitive for most customers to send, receive, or export electronic health information stored in EHRs (Electronic Health Records), or to establish interfaces that enable such information to be exchanged with other providers, persons, or entities. Some EHR developers allegedly charge a substantial per-transaction fee each time a user sends, receives, or searches for (or “queries”) a patient’s electronic health information. EHR developers may also charge comparatively high prices to establish certain common types of interfaces—such as connections to local labs and hospitals. Many providers also complain about the costs of extracting data from their EHR systems for their own use or to move to a different EHR technology.” [6]

Obviously, arbitrary interoperation is a difficult thing to achieve. How does Lillypond hope to create such a capability?

The Platform

The Lillypond platform is composed of a communications interdiction device (Lillypad), a first generation hardware obfuscated article designed as a defensive hardware sniffer installed within the data communication stream. Lillypad works in concert with a software obfuscated localized server/client agent (Defense Machine) applied to the User computer running agent based web automation code (Lillypod) capable of manipulating and translating arbitrary data. Obfuscation is the quality of hiding the operations of the host logic by injecting active masking.

Advanced generations of the Defense Machine will evolve into hardware obfuscated server/client defensible machines running within the Lillypond platform using undiscoverable symmetric key technology guaranteeing unbreakable encryption. This Defense Machine method is intended to evolve toward inclusion in major communication device chipsets to achieve maximum defensible hardware lock-down.

Lillypad’s Defense Machine employs automation tools available in standards based WAI-ARIA (Web Accessibility Initiative – Accessible Rich Internet Applications) [7] [8]. This specification allows greater automation control from within local web pages specified for the special needs community. Lillypond seeks to lock these automation capabilities to the local defense device hardware to achieve a hyper-secure independent data process to ensure User privacy with flexible deterministic data use.

This web application becomes a central means of communicating with and controlling existing social media applications. Ownership of that capability is achieved through a personality-privilege-property chain of data notations emanating from the User’s Token. Access to this data is achieved within the Defense Machine structure by smart contracts which have no access beyond the notation chain.

The Token

The basis for Lillypond monetization and automation is the Lili-Token (Hyperledger Fabric Token digest). The token represents a unit of ownership, meaning the User is the record owner being represented by one token which describes the independent history in a digest. Other parties seeking to interact with the User do so by ‘rented’ or ‘leased’ or ‘gifted’ Token components – fractional units created and destroyed per use-case.

This Token digest maintains the fiduciary link to the User historical records represented by the notation structure in the independent record.

The Token is a living document stored in defended storage as chosen by the User. These choices include local storage in the User defense machine or remote storage in cyclically audited peer-to-peer agent vaults between User devices and distributed defensible machines owned by third party financial governance entities.

Value for the monetization is represented by the Lili-Coin (Coin). The Coin represents units of value ascribed to the purposes derived by reference to the independent record data codified by time-frame notations. This time-frame system provides fractional valuation of the independent record usage by data brokers.

This Token-Coin structure is built and maintained by the Lillypond monetization engine representing that independent record's interests.

Security Issues

LillyPond is built on a complex blockchain-like technology (Merkle Tree) using a unique set of hardware-based security and defense measures. We assume the very possibility of any software-based security to be a lost cause. The National Security Agency (NSA) believes “A sufficiently large quantum computer, if built, would be capable of undermining all widely- deployed public key algorithms used for key establishment and digital signatures.” The NSA go on to say “It is generally accepted that quantum computing techniques are much less effective against symmetric algorithms than against current widely used public key algorithms. While public key cryptography requires changes in the fundamental design to protect against a potential future quantum computer, symmetric key algorithms are believed to be secure provided a sufficiently large key size is used.” [9]

“NSA published the advisory memorandum to move to quantum resistant symmetric key options and to allow additional continued use of older public key options as a way to reduce modernization costs in the near term. In the longer term, NSA is looking to all NSS vendors and operators to implement standards-based, quantum resistant cryptography to protect their data and communications.” [9]

Informed technology industry consensus is centering on a rework of internet architecture to achieve the kind of data security critical to the success of distributed automation in a wild world. Without such changes, the future for internet dreams is unachievable. [10]

The Future

The blockchain community intends to build autonomous automated systems which, along with AI, will allow an independent machine-to-machine economy based on interoperable smart contract notation to emerge. In short, we are at the dawn of a new AI community for our planet. Such frictionless autonomous automated capabilities will allow accelerated granular levels of economic activity to develop as the financial viability of human economic activity is no longer tied to population density. Automating interoperable connections between the individual and User-centric specified governance is the beginning of this vision for the future.

While modern efforts to secure electronic systems and data flows using a combination of cryptography and secure network software are critical, more must be done to prevent adversarial attacks and unauthorized use. This includes tailoring hardware to take on the bulk of security governance. Lillypond intends to use various patented hardware technologies to create electronic host circuits with untouchable parasitic automation.

Through tampering and behavioral engineering, attackers can learn enough about a system or system users to expose weaknesses. Exposed computing weaknesses may be found in hardware or software, or both. Lillypond solves this problem by allowing for a flexible on-the-fly defensibility designed to employ small monitors within the

electronics device interdicting communications to and from a User computer to detect and prevent tampering and adversarial engineering of data handling logic.

The biggest challenge facing any interdiction or interception system is anticipating the unknown. This problem is compounded by the potentially devastating cost of being wrong only once.

Detail

Such challenges may be confronted using a restructurable hedge between the internet and the User's host devices acting in concert with data chaining methods connecting document stores provisioned during the life of the computer use and AI derived data forms providing feedback and guidance to the interdiction processes.

From a system architecture perspective, this means using software and programmable hardware logic strategically and tactically to implement critical functionality. The benefit is that software and programmable logic can be updated on-the-fly to counteract new threats or resolve insufficiencies discovered in the system.

Lillypad is to be built using a novel, programmable-logic obfuscation hardware approach to significantly improve security coverage by adapting to behavior at the interdicting device level and extending it to the system level. Lillypond uses synthesizable programmable logic structures and powerful hardware insertion tools to embed programmable monitors within a Field Programmable Gate Array (FPGA) based integrated circuit within the Lillypad circuitry. The programmable monitors are created to overwatch the host process operations at the micro-circuit level. This overwatch/host fabric may be immediately loaded into an FPGA to take up an adapted interdiction based on feedback from the Lillypond system. Future versions of this reprogrammable/reconfigurable capability may be created in mass-produced micro-electronic products without the use of FPGA properties.

The programs to be loaded into the device monitors are designed and created during the circuit creation phase. New programs can be designed and installed at any point in the device lifecycle (silicon or FPGA), to enhance functionality, improve coverage, or guard against new threats with adaptable counter-measures.

The programs instruct the monitor to look for suspicious behaviors such as:

- Dark web sampled prohibited context
- Abnormal user machine behavior
- Abnormal power cycling and sequencing behavior
- Abnormal performance profiles
- Unauthorized memory accesses including BIOS changes
- Killed and interrupted processes

The application of these programmable monitors is nearly unlimited, restricted only by the programmable Finite State Machine (FSM) resources and reconfigurable engine assets provided within the host circuitry. The programmable monitors operate at-speed and can counteract suspected threats with immediate countermeasures when used in conjunction with Lillypond’s security wrappers.

These wrappers enable real-time responses to threats by the following:

- Forcing circuits into a reset state (e.g., communication peripherals, memory controllers)
- Blocking read and/or write access to select memories, memory regions, or peripherals
- Creating obfuscated bus activity or other masking functions
- Wiping out (erasing) sensitive data stored in select memories
- Creating alerts and pro-actively allowing the system to enter a “safe mode” gracefully

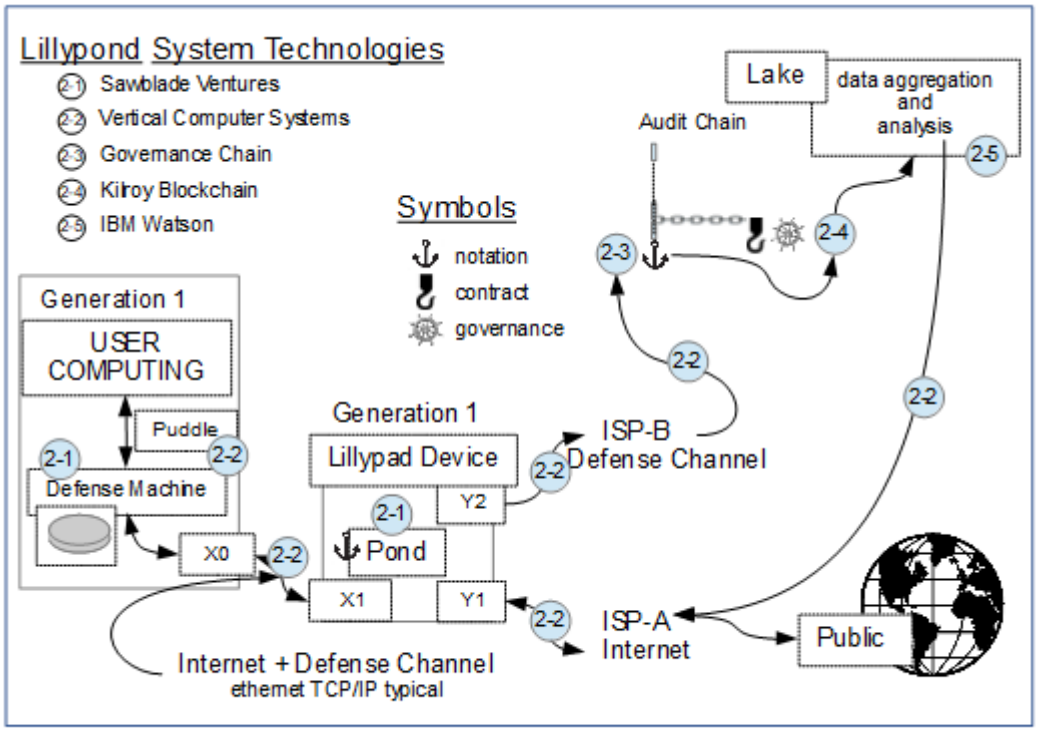

Figure 2

The Lillypond System referenced in Figure 2 is a reconfigurable, reprogrammable and obfuscated ethernet packet analyzer (2-1) coupled with controlled document storage (2-1) communicating over a secure peer-to-peer communications channel (2-2) to Audit Trail Custody Resources (2-3) and Objectification Facility (2-4) in conjunction with AI data lakes (2-5) holding resolved behavior.

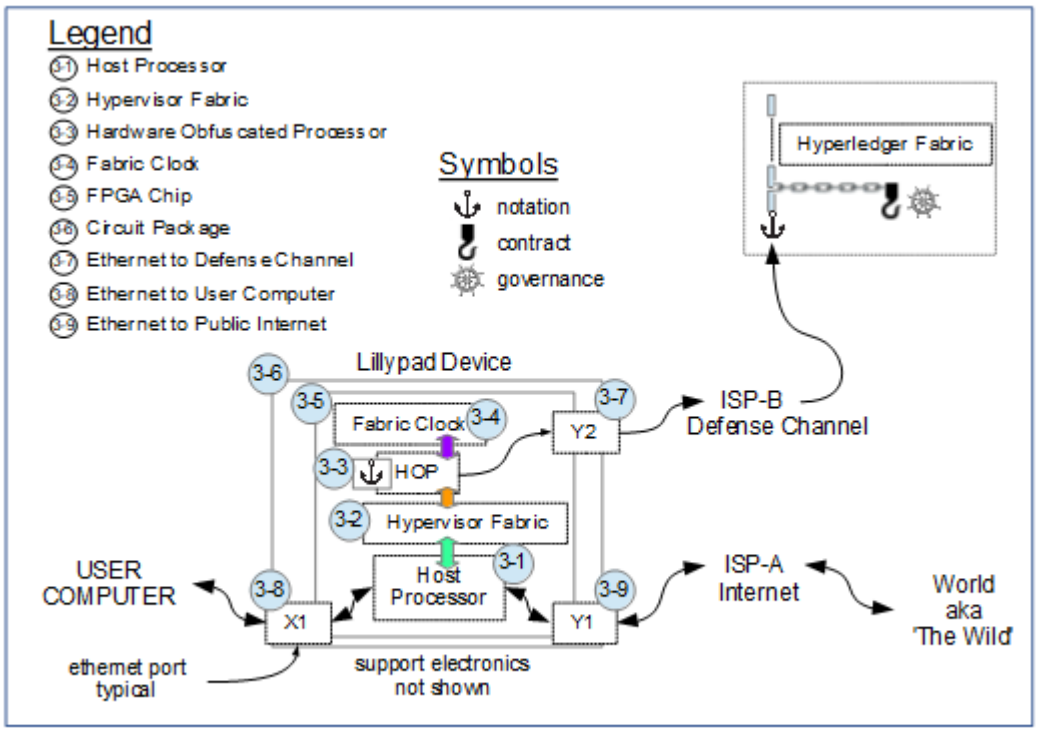

Figure 3

Lillypad referenced in Figure 3 consists of a Host Processor (Fig3-1) continuously sampling ethernet packets and assembling snapshot views of transactions between the User Computer and the Internet World. The Host Processor is controlled by an obfuscated Hypervisor Fabric (3-2) which provides execution patterns for resolving assertions placed against the snapshot.

A Hardware Obfuscated Processor (3-3) controls the Hypervisor Fabric and reports on assertions to the Fabric Clock (3-4) which resolves synchronization command control and emits anchored chain notations to the Defense Channel.

These facilities are installed on an FPGA (3-5) to create an integrated circuit “Chip” supported by electronic support circuits (3-6). The device package includes ethernet communication media access control address (MAC address) facilities from the Device to the outgoing Defense Channel (3-7), the User Computer (3-8) and the Internet World (3-9) which carries the incoming Defense Channel.

Lillypad is primarily protected against tampering and other adversarial behavior using unique patented reconfigurable and reprogrammable obfuscated hardware to achieve a reliable and trustworthy source for resolving, recording and executing interdiction protocols against behavior profiles encountered by naive or unskilled users communicating with adversarial or compromising resources on the internet at large. Obfuscation uses segregated tools to inject into a circuit, other circuits that hide the operations of the host circuitry.

There are many advantages to using multiple and distributed programmable monitors. With multiple programmable monitors instantiated within different clock domains, power domains, and functional domains, a full system view can be realized. Moreover, the monitors can be tied together with cross-triggering signals so that more elaborate intra-domain and inter-domain conditions can be analyzed. This provides similar benefits to the hardware/software interactions described above for system-wide obfuscation and protection. Sprinkling multiple programmable monitors throughout the design also provides operational redundancy. When an attacker attempts to manipulate the data streams or logic functionality in one subsystem, the monitors in the other subsystem will be alerted and create bastion actions against the behavior.

The fact that these programmable monitors can be repurposed at any point in time on-the-fly and at clock speeds is crucial. Monitors can be programmed in-system to perform different functions over time. By time-slicing functionality, a wider range of behaviors can be detected with the same resources. To the adversary, this creates the appearance of random countermeasures and ultimately makes efforts to tamper or reverse-engineer the system behavior increasingly difficult toward impossibility.

Obvious concerns are whether the programmable monitors are more vulnerable and whether they in fact provide additional portals of attack. The simple answer is no. There are multiple security features within the Lillypond system. The embedded communication channel is secure and the programming files are encrypted and chained, making it virtually impossible for an attacker to make undetected modifications to a programmable monitor. Cross-triggering between monitors and the handshakes with defense machines provide a reliable and redundant “neighborhood watch” and early warning system.

Additionally, the fact that the programmable fabric is inserted with automated tools on-the-fly ensures that the system is correct by design and construction, reducing the possibility that an implementation flaw will enable a breach. Automation tool segmentation ensures verification/validation compliance. Random repurposing of the structure by retracing the circuitry and rerouting signal paths means any attempt at penetration will be faced with a different circuit in the next moment. Ultimately, the inclusion of this programmable fabric will greatly increase the overall system security, allowing the protection of data property while at the same time protecting the end systems and the data storage.

The use of programmable logic extends beyond anti-tamper and countermeasure applications. Lillypond is developing new applications with programmable fabric to address anti-counterfeit and feature activation control – two key components required to secure supply chains and protect critical assets.

The anti-counterfeit and feature activation solutions are closely related. The anti-counterfeit solution uses a combination of programmable logic and one-time-programmable memory to store unique encrypted codes within

a device. Defended devices are programmed and subsequently authorized through a secure defense channel interface using Lillypond's software security application.

The combined use of distributed ID code storage and distributed programmable logic structures increases code security, as an adversary must compromise the encryption key, the programmable logic programming protocol, and the programmable bitfile(s) to be momentarily successful. Not only will each device store a unique encrypted ID, but each ID is written and retrieved using a different programming bitfile, meaning the bits of the code will be scrambled in different locations on each device.

The distributed programmable logic structures also provide a measure of obfuscation to thwart efforts to uncover program codes by physical examination of the Device. Lillypad defense machines will use encryption where most appropriate but will also use hardware signal braiding to provide random instantaneous intermittent scrambling of data buses without resorting to programmatic overhead.

Feature activation also uses a combination of non-volatile or one-time-programmable memory in conjunction with programmable logic wrappers. These wrappers are inserted on key control signals such as resets, mode controls, or power controls. The wrappers can be controlled by local software, through a secure distributed defense channel to change host circuit operation on-the-fly at-speed.

The wrappers are inserted using formal automated tools during the hardware build (FPGA configuration) phase. These may also be used for silicon manufacture. The choice of wrapper type is dependent on the security, configuration and authentication requirements of the Device or System.

The activation and deactivation of features can be volatile or non-volatile. If certain tampering or unauthorized activities are detected, features can be permanently disabled. Permanent deactivation uses one-time programmable storage designed into the signal wrappers. Control of power and clock operations may also be used to destroy the chip autonomously or remotely in ultra-sensitive use-cases.

Both the external and internal programming interfaces are secure, and all program bit files are stored in encrypted form.

Key Benefits of Lillypond Technology

• Protect your user history
Lillypond's use of novel programmable logic structures protect the system and provide assurance that any new and unexpected threats or security flaws can be mitigated through immediate on-the-fly firmware or software upgrade and reconfiguration.

• Protect your communications
Suppliers of consumer products and semiconductor manufacturers can reduce exposure to security threats by gaining assurance that their devices' critical data are transferred through or stored in the most secure methods.

• Low-cost / low-risk implementation
Patented silicon-proven IP and powerful automated hardware insertion tools along with partner technologies allow Lillypond's innovative and robust security schemes to be constructed with low cost reproducibility.

• Designed-in safety
Automated insertion and reuse of hardware creation capabilities in concert with software allow AI to leverage Lillypond's technology with the confidence that complexity does not increase design risk or device vulnerability.

Summary

Children with autism must have auditable access to internet services to help them cope with the complexities of medical care and interaction with the outside world as they grow into adulthood. Children and adults with special needs must have seamless healthcare during vulnerable and transitional periods to avoid setbacks and complications throughout life. This interaction must respect and preserve their privacy and appropriate use of personal data. Lillypond intends to provide a unique hardware/software platform to build a trusted independent record structure for individuals within the special needs communities, such as the autism community.

References:

[1] "List of social networking websites"
Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/List_of_social_networking_websites

[2] "Merkle tree"
Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Merkle_tree

[3] "Connecting Health and Care for the Nation: A shared nationwide interoperability roadmap."
Office of the National Coordinator for Health Information Technology. (2015) Version 1.0
www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability- roadmap-final-version-1.0.pdf

[4] "Health Information Technology for Economic and Clinical Health Act" (HITECH Act)
Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act

[5] [6] "Report on Health Information Blocking."
Office of the National Coordinator for Health Information Technology. (2015). Report to Congress.
www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

[7] "WAI-ARIA (Web Accessibility Initiative – Accessible Rich Internet Applications)"
Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/WAI-ARIA

[8] "WAI-ARIA: Method To Develop Disable Friendly Websites"
by Fazia Fatima, Shipra Rawal, Chinmay Garg3 and P N Barwal
International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 9 (2014), pp. 925-930
ripublication.com/irph/ijict_spl/ijictv4n9spl_09.pdf

[9] "Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator)"
Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Dual_EC_DRBG

[10] "Rearchitecting a defendable Internet"
by Halvar Flake / Thomas Dullien, July 2017, reference slide #12
www.sig-switzerland.ch/wp-content/uploads/2015/07/SIGS_Dec16_Thomas_Dullien_Re-architecting_a_defendable_Internet.pdf

Contact: keith@sawbladeventures.com