Securing the Digital Denizen™

A Redwall Technologies, LLC White Paper

January 2020

Digital citizens, connected devices, the Internet of Things (IoT), and Internet of all connected things speak to a worldscape defined by the myriad digital connections that exist within places, between people, and with devices. This worldscape is rapidly becoming irreversibly essential to 21st Century life.

Just as global positioning satellites have become irreplaceably essential; so is this new digital worldscape. From purely personal and social communications to just-in-time logistics and information retrieval, the pervasiveness is evident. What is also emerging is the prevalence of data "in-the-cloud." The digital cloud has become "home" to vast stores of data and hosts to information systems at an unprecedented scale. The digital worldscape is rapidly being assimilated into this digital cloud. In practical terms, this shift means that personal, enterprise, device, and interaction (transaction) data lives in this digital place and is no longer resident on premises, in paper form, or under personal control.

The Shift!

One could argue that the year 2020 will mark a *SHIFT*, an inflection-point, at which people, enterprises and things become digital identities having physical presences; rather than the converse – a physical reality with a digital presence. It is worthy of consideration that commerce, government, and communication of all types operate and transact predominantly in the digital worldscape. Consider the demise of *original* paper documents, signatures, and transaction records (receipts). Soon to follow are personal checks and postal mail. The phone number is rapidly supplanting the social security number as the primary link to an individual. At what point does habitation in the digital worldscape dominate personal, enterprise and connected device governance and survival? What are the security implications of identity ownership and protection in this emergent worldscape? Let's explore further…

infrastructure person control
plan internet CTO LTE protection
privilege citizen web cloud computer
patch risk technology BYOD wireless security update
encryption
identity theft cryptographic role accessible identity
persona patent society ID isolation liability ISP
digital denizen™
vehicle search
intelligence CISO server safety
surfing internet of things commerce systems SCADA conduct
4G theft
credit mobility information automation privacy global
digital connected market monitor ecosystem
vulnerability spoofing device data social network tablet
dark web
database online authentication community
operating system domain artificial intelligence presence

The term "digital citizen" is surprisingly prescient. The 21st century-only populous knows no-other reality. The oft repeated phrase "it's on my phone" might just as well be translated to mean "I am [on] my phone"- literally. To erase the digital presence of a digital citizen is to effectively erase the person. The digital citizen would cease to exist socially, at work, and financially. A sobering thought and reality!

The Emergence of the Digital Denizen™[1].

Digital citizens co-exist with a myriad of connected devices each with a unique identity and role. Redwall Technologies has coined a term for these digital identities – the "*Digital Denizen*™". To Redwall; **the Digital Denizen is the role-based digital identity and presence of any connected device.** It may represent an individual identity (citizen), as in the case of a smartphone user; or an end-point device such as a connected car or an industrial control system. The significance of the Digital Denizen is its unique role-based existence as an online entity that also has a physical presence expressed via a connected device. Like the digital citizen, the digital denizen exists in-part in electronic form, on the device, in the cloud, on other devices, and in-transit in between. Like the digital citizen, the digital denizen is moving to a state where a disruption or deletion of its digital presence would cause it to cease normal function or its practical existence.

[1] Digital Denizen is a Trademark of Redwall Technologies, LLC.

WHO WE ARE:

Redwall Technologies LLC is a cybersecurity technology leader delivering platform-agnostic trusted execution and role isolation to enable and protect the Digital Denizen. We provide our customers (and channel partners) an unmatched ability to deliver control, security and privacy across a wide spectrum of platforms, applications, and use cases. We enable one device to serve multiple roles via a unique, patented[2], cryptographic and temporal isolation capability. Our cybersecurity solutions are derived from our:

- National-level ethical hacker experience finding and exploiting systems,
- Unmatched security systems engineering capabilities in protecting systems, and
- Exceptional development team capable of addressing complex problems rapidly and with technical excellence.

THE PROBLEMS WE ADDRESS:

Compute systems and networks (Internet Protocol-based) were designed to rapidly store, retrieve and transmit data. In the beginning trust was assumed and security measures were minimal. Fast forward to the present and we now know how difficult it has become to achieve trust in our world of connected devices. The underpinnings of this trust are control, security, and privacy, which is the essence of cybersecurity. In spite of the $billions invested cybersecurity products, there remain two vexing challenges – securing the end point devices that connect to the Internet; and preventing (intentional or unintentional) compromise by humans. The time has come for a new paradigm.

Redwall uniquely addresses these challenges, and in so doing, resolves *control*, *security*, and *privacy* conflicts that exist between creators, maintainers, and users of connected and mobile devices. Let's explore one use case and our flagship Product – Redwall Mobile® (RwM) security.

RwM is the only mobile/end-point device security solution capable of withstanding extensive, intensive Federal Government testing and concerted attempts to "hack" RwM protected devices *for over five years*. **While other products patch, RwM protects.** It is the exclusive mobile device security solution for Motorola Solutions' rugged handheld LTE devices and body cameras. It has the only secure "multiple-mode" capability of any handheld device. RwM can create separate, secure and fully encrypted partitions (personas) that cannot be co-mingled or accessed simultaneously. We call this smartphone capability ***Secure Persona***®. It secures the digital citizen.

Secure Persona enables the digital citizen to operate in and between role-based personas; eliminating the inconvenience, cost, and risks of carrying multiple devices (work & personal). Secure Persona isolates and separates workplace sensitive information from personal information; and cannot be overcome by operator intent or error. Secure Persona creates an identity-specific profile for all applications, data, network & cloud connectivity, and storage. Secure Persona eliminates the need for, threats from, and risks of "Bring Your Own Device" (BYOD) in the workplace and in the field.

RwM and Secure Persona enable the digital citizen to securely and safely fulfill every life role; by providing role-dependent control, security and privacy. Apps and data available only at work cannot be accessed while in personal mode and vice versa. Smart device features, such as microphones and cameras can be controlled below the operating system to prevent eavesdropping and exfiltration of sensitive information. Location tracking services can be individually controlled and enabled only when appropriate and only for legitimate purposes. System access can be tailored for enterprise use while at work and personal use when away or off-duty. In each case there is no potential for co-mingling of data between modes (across roles) ensuring workplace data security and personal data privacy. Secure Persona can be employed to add levels of security within each role. In a military use case true "multi-level security" is possible on one device without the need to remove device media.

[2] US Patents 9514300 and 9990505

What about other markets?

The handheld mobile device (i.e., smartphone, tablet, wearable computers, etc.) markets are the first instantiation of Redwall's patented technologies. Other markets include connected vehicles, remotely operated and autonomous systems, the broader category of IoT, and a unique and patented[3] application in SCADA and operational technology (OT) systems. For each of these markets there remain the twin challenges of:

1) securing the device by preventing unauthorized exploitation, and
2) enabling authorized roles that have unique role-specific permissions.

Redwall's technology addresses these challenges and enables control, security and privilege for every device states, including: 1) as manufactured, 2) as maintained, and 3) as operated.

The Connected Vehicle

To illustrate, consider the connected car. The connected car has numerous physical and digital access points, a growing number of computers, and increasing software complexity. Securing these systems while enabling role-based access is a challenging prospect; given the:

- Extended lifetime of these systems,
- Need for frequent software patches, and
- Ready access by potential hackers equipped with the latest diagnostic tools.

Redwall's security solution can limit vulnerabilities and isolate access simply by deploying cryptographically and temporally isolated modes aligned with the roles of manufacturer, maintainer, and owner-operator. The "below the OS" security approach prevents the type of hacks that have been sensationalized in the press. For connected cars, the manufacturer can have deep access to device hardware and software via the Internet connection with the assurance (via signed digital keys) that only authorized employees and systems can make changes to the vehicle. Similarly, manufacturer authorized maintenance technicians can be granted specific privileges via their role without risk of compromise to manufacturer and owner-operator privileged information. Finally, owner-operators can establish their unique on-car digital presence, including connected devices (smartphones, media players, and online accounts, etc.) that may include personal and sensitive account information.

RwM security enables vehicle manufacturers to offer a secure mechanism for ensuring:

- Vehicle firmware and software is up-to-date, over the air, without a trip to the dealer,
- Maintenance technicians do their jobs without exposing proprietary systems to tampering, and
- Owners can create a rich personalized experience with their vehicle without concern for external surveillance, snooping or theft of personal data.

Remotely Operated and Autonomous Systems

RwM security enables manufacturers of remotely operated and autonomous systems (land and air vehicles in particular) to offer a secure mechanism for ensuring their systems operate as intended and cannot be exploited. Rogue vehicles, whether remotely operated or autonomous, would do great harm to these emergent industries. Role-based privilege will be vital to assuring safety when these systems are in use within proximity of human operated systems or over and among the population. Role-based access via RwM security will maintain the separation and accountability for the three critical devices states: 1) as manufactured, 2) as maintained, and 3) as operated.

On the Horizon

Redwall technologies will be introducing the ***Digital Bodyguard***™ in two releases (device and then cloud) during 2020. **Digital Bodyguard embraces the concept of *resilience* and the ability to fight-through a cyber-attack** that might otherwise render the target device unusable. Digital Bodyguard is sponsored by the US Marine Corps[4] for initial deployment on the Motorola Solutions LEX L11 rugged handheld LTE smartphone, and subsequently other smartphones and connected devices.

[3] US Patent 9,298,917

[4] Contracts M67854-18-C-6512 and M67854-19-C-6517

About Redwall

The beginning

Redwall's leadership team coalesced while developing a secure device technology, ProsettaCore™, for PCTEL Inc. (NASDAQ:PCTI). In 2013, seeing an opportunity to expand the core technology; the inventors and developers acquired (from PCTEL) the ProsettaCore™ server, device software, underlying IP, and complete development responsibility for the resultant security products. Redwall then successfully rolled ProsettaCore into Redwall Mobile® to take the original concept to the fully developed commercial product suite.

The products

The genesis of Redwall's technology suite is a direct result of offensive cyber-operations against mobile and embedded devices, and the inability of existing products and methods to defend against even the most basic threats. Redwall needed and created a new approach to solve the growing information assurance needs of both the public and private sectors for smartphones, tablets, and other connected devices such as those in SCADA/IoT networks. Redwall's products allow devices to operate with increased robustness and assurance, all controlled by mission, theatre, enterprise and user (role) specific policies that can easily adapt in the field in response to changing environments and threats.

Security is not an afterthought or add-on for Redwall - it's our business. We eschew the "promote and patch" approach to security so prevalent in the connected device ecosystem. Because of our expertise in offensive cyber, we know how attackers think, how to best stop and confound them, and where our client' resources will be most effective against them.

The hawk and eagle logo

Our logo of the hawk and the eagle represents our philosophy that sometimes we must defend our freedom and the freedoms of our allies through our great strength and vigilance as we work towards peace. In the cyber realm, however; we fight a more asymmetric battle against highly skilled foes, and Redwall stands ready to help protect our data, our systems, and the freedom and lives of those who depend on those systems.

Our mission

Redwall's mission is to provide high-quality and highly effective cyber-security expertise, software engineering, and leading-edge technology to assist public sector entities and private sector enterprises in preventing and responding to emerging threats against their mobile applications and connected infrastructure. Redwall delivers solutions to enable and secure all Digital Denizens!

Contact Redwall

Redwall Technologies, LLC
2365 Dayton Xenia Road Suite B
Beavercreek, OH 45434

John Rosenstengel
President & CEO
John.Rosenstengel@redwall.us
(937) 956-6156
Mobile: (937) 477-0424

Kevin Woods,
Chief Operating Officer
Kevin.woods@redwall.us
(937) 956-6156
Mobile: (937) 684-0529