



DASH7
Security and
Privacy, Part 1:
“Introduction”

August 23
2010

DASH7 Mode 2 is the most advanced sensor network platform on the market. As with all mainstream computing platforms (PCs, Smartphones), security and privacy are critical elements for mass adoption. The DASH7 Security Working Group has authored this first-in-a-series paper to energize the community on this topic with the ultimate goal of ensuring DASH7 technology is the most secure, private and efficient sensor network platform on the planet.

DASH7 Alliance
Security Working
Group (SWG)
www.dash7.org

Authored by:

Erik Wood- Revere Security
Daniel Engels- Revere Security

The following document describes:

- The context for security and privacy for the DASH7 Alliance community,
- Terms and use descriptions, and
- The approach recommendation

Introduction:

Moore's Law states that the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every two years. Integrated Circuit (IC) manufacturing technologies have followed Moore's Law since the late 1960s. This continual improvement in performance, or shrinking of the IC circuit, has directly enabled computing power and electronic functionality to move to the edge of computing networks and allowed those networks to pervade every corner of our lives.

For example, the 1970s computing experience was defined by terminals tethered to mainframe computers bound by application specific-software and physical location limitations. This was a purpose built environment generally limited to industrial offices and educational facilities to get a task done more efficiently. In the 1980s, operating systems allowed for home PCs to run software for personal use and to connect via modems to client server architectures in the office. Once personal and business software applications blossomed, the need for faster processing speed, more memory capacity and easy information exchange drove the development of today's computing and networking systems with laptops and the Internet being two significant components of our networked world.

Figure 1 illustrates this progression of computing power and extension of computing networks.

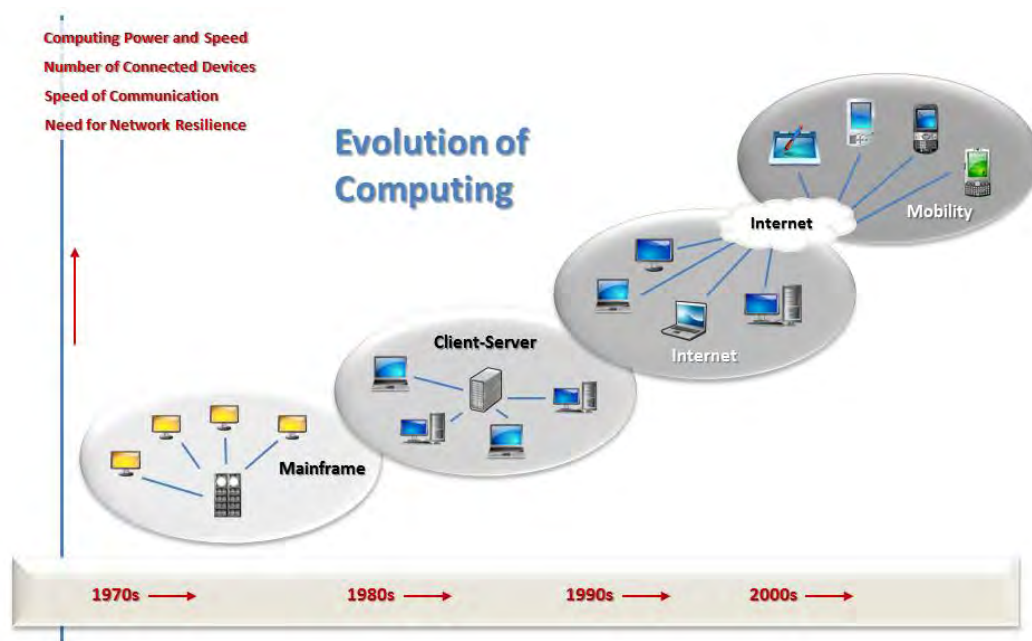


Figure 1

The extension of the computing network to laptops and other mobile devices with the computing power of a supercomputer has enabled a plethora of applications that have revolutionized the way we do business and the way we live. Unfortunately, the extension of the network from isolated mainframes acting as city-states to communicating city-states to communicating citizens with supercomputers has enabled a broad array of security breaches that were unthinkable with simple mainframes.

Just as Gordon Moore observed the rapid development of IC technologies and proclaimed what he saw as Moore's Law, the ever expanding computing network has shown us the following truth: as processing power and data move to the edge of the network, and as the transmission of data increases over the ever expanding networks, security inevitably emerges as a primary requirement for mass adoption. Antivirus software, firewalls, and Secure Sockets Layer (SSL) security

were all responses to the security issues that arose and were generally afterthoughts.

The paradigm of processing, memory and information exchange moving to the edge as a technology matures is also true as one reviews the history of mobile telephones.

As figure 2 illustrates, the evolution of the mobile phone has seen dramatic change from a simple voice platform to an ever expanding multimedia and computing platform. And, just as we witnessed in the evolution of the computer, the mass adoption of the smartphone now requires security.

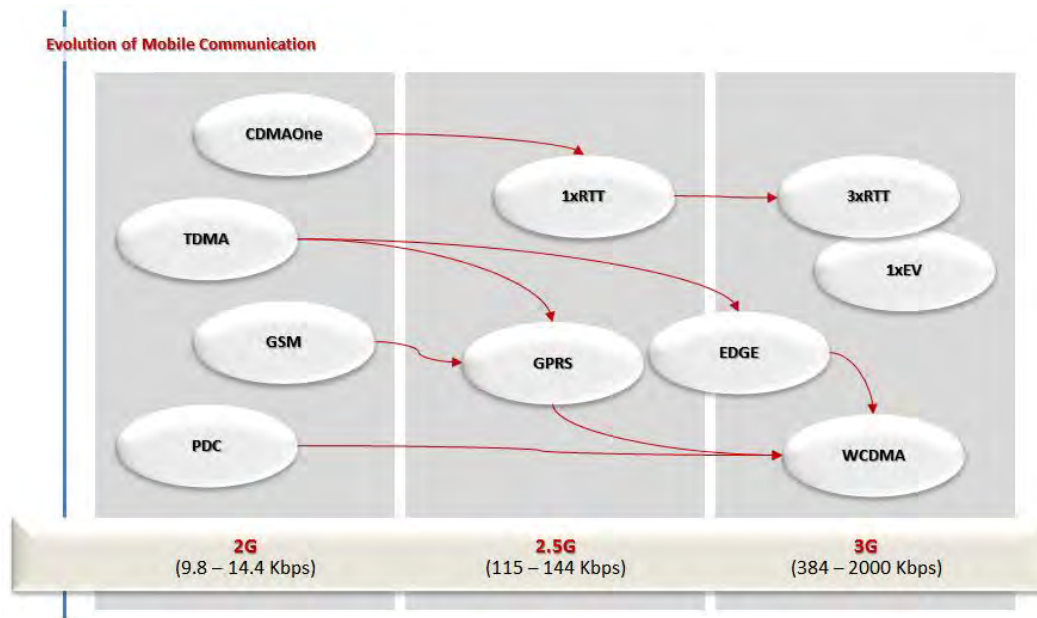


Figure 2

RFID

Since the late 1990s, another disruptive technology platform has emerged. Termed Radio Frequency Identification, or RFID, this platform enables the removal of humans from certain aspects of the object and machine environment allowing the edge of the computing network to

move to objects or things. Now, automated conveyances, global supply chain and transportation networks, and small to massive four wall enterprises can use machines to identify, track and monitor the condition of other machines and objects. Gathering and acting upon the huge amounts of data automatically collected has given rise to revolutionary new business models and cost savings.

Just as security, and the resulting trust it engendered, enabled the mass adoption of computing networks, security implemented within RFID devices and systems is required for the mass adoption and creation of the "Internet of Things." RFID technologies have been through their own evolutionary curve that virtually mirrors those of computing and smart phones. What once was a technology for identifying an object has grown to enable object location tracking, object condition monitoring, and object command and control. As preeminent RFID technology standards like ISO 18000-7 ("[DASH7](#)")¹ give rise to lower cost and increased functionality at the edge, security will be required to feed the engine for mass adoption as it did for RFID's disruptive predecessors, the computer and the smart phone.

DASH7 Security and Privacy

There is no better evidence to Moore's Law playing out in RFID than the advent of DASH7 Mode 2. Mode 2, the latest and by far greatest RFID platform, is designed for peak performance in terms of power, data rates and range as well as memory and sensor features allowing for "101" uses. While Mode 2 addresses encryption and key management in broad terms, the newly formed DASH7 Alliance Security Working Group (SWG) will take the actions needed to address the details of the RFID security and privacy challenge. In the near term, the SWG will put forth first a Charter and then a comprehensive draft proposal to ensure that DASH7

¹ DASH7 is the brand name given to devices which comply with the ISO 18000-7 standard for active RFID at 433.92 MHz, similar to the "Wi-Fi" brand given to devices which comply with IEEE 802.11 standard for wireless broadband.

Mode 2 is the most secure, private and efficient wireless sensor network platform on the planet.

Defining RFID Security & Privacy for DASH7 RFID

Terms:

- **Encryption:** The process of changing plaintext into cipher text for the purpose of security or privacy.
- **Tag Authentication:** Instant verification that a tag is trusted and safe to allow access to send data to the reader network.
- **Tag Cloaking (Reader Authentication):** Enables a tag to be invisible to interoperable readers that are not on the network.
- **Mutual Authentication:** The process of both entities involved in a transaction verifying each other.

Application Descriptions:

Security for resource-constrained wireless devices like RFID readers and tags must be viewed from a holistic standpoint. A wireless network's security is only as good as its weakest link; therefore each component of an RFID network plays a key part in true security. And equally important as true comprehensive security is the requirement that the features and functions that define the value of using RFID are not dramatically affected by the implementation of true and comprehensive security. Otherwise the proposition is moot.

First and foremost, **Data Encryption** is critical for DASH7 communications. Data exchanged via DASH7 bi-directional wireless transmissions to and from the tag(s) and reader(s) must be protected from those that may be listening. In the case of data rich tags, the information transmitted may be sensitive and/or a matter of privacy. In

the case of license plate ID tags, the risk comes from capturing the ID and cloning the tags for nefarious use as well as covertly tracking the tag based on its unique ID.

Information Assurance is a key element of security for DASH7 communications for many applications. Take sensor information related to an object or its environment that is captured from the DASH7 tag platform. When the sensor data is sent over the wireless link from tag to reader, it may not only be important to encrypt the data, but perhaps it is even more important to authenticate that no one has adulterated the sensor content, values and/or time stamp.

Tag Authentication is a modern response to the growing threat of network security. The days when firewall security was acceptable are truly over. Today, every point of computational data collection is an open window into the network of a commercial or government enterprise data system. In the case of DASH7 RFID, readers are open gateways to much larger and potentially much more vital networks. Therefore, tags must be commissioned with a secret key that is unique to the tag, is never transmitted in the clear and can never be statistically computed. This key, derived by a sophisticated yet minimal piece of code on the tag's processor, must be challenged by the reader network that manages the key database specific to the individual enterprise. Standardized legacy methods once made managing these keys prohibitive in terms of latency but new, and dramatically more efficient, approaches exist to make the performance impact negligible and maintain the timing requirement for the ISO 18000-7 air interface protocol.

Tag Cloaking is a novel approach to eliminating the awareness that a tag is present even if it is in the presence of a reader that is designed to

read it but not connected to the private network of keys required to make it respond to a query. Not only does this feature provide a truly valuable security function, but it also has operational benefits when one considers a world full of DASH7 tags and individual closed loop systems preferring only to see tags it cares about.

DASH7 Encryption Approach

When it comes to DASH7's approach to encryption, one size will not fit all. It is critical that a framework is designed so that multiple encryption algorithms can be used and referenced in the DASH7 standard.

Government encryption standards are an important consideration when it comes to methods for DASH7 products, but there is no standard in existence today designed for the new era of resource constrained devices such as RFID tags. In the U.S., the National Institute for Standards and Technology (NIST) defines cryptographic algorithm standards and validates implementations through its Federal Information Processing Standards (FIPS). NIST last put forth an encryption algorithm as a standard in 2002 called AES. AES was designed to secure 32bit computers and the Internet.

Certainly U.S. government customers prefer using standards for encryption since obtaining waivers to use non-standard encryption is time consuming. However, encryption standards have notoriously lacked innovation, and the current encryption advances specifically designed for the code space, speed and power constraints associated with RFID systems need to be referenced and available. Therefore, it is critical that the DASH7 approach to security (encryption and mutual authentication) needs to be that of a framework to allow, for example, NIST standards based security when required and more modern peak performance security when allowed.

Conclusion

The evolution of RFID, its features and uses, has reached a pinnacle with DASH7 Mode 2. One key to its mass adoption is defining an encryption framework to offer the strongest security and privacy, allowing options for government standards and ensuring options for peak performance. The DASH7 SWG will work with the DASH7 community to achieve that goal. Please look for future papers where we will dive deeper into encryption options, key management techniques and updates to the DASH7 SWG's progress.

For information on joining the DASH7 Alliance and participating in the Security Working Group, please contact Paul Ritchie, Executive Director, at paul@dash7.org.