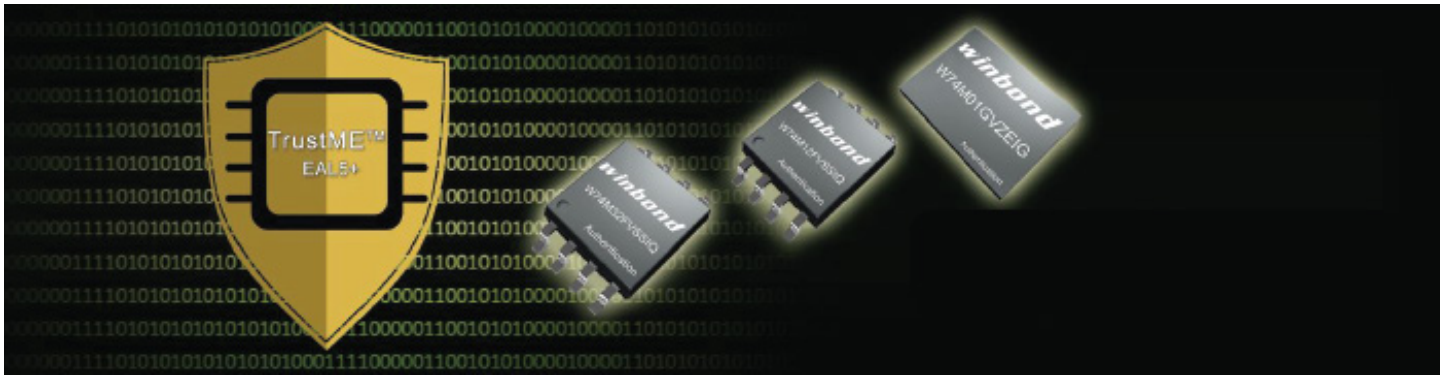
Security for IoT Devices

-By Fely Krewell



According to Gartner, there will be 50 billion (or more) connected IoT objects by 2020, all made possible using today's mobile and computing technologies. This presents an exciting opportunity for the electronics industry, however the biggest challenge and the number one concern is security. Lack of trust or weak security in the IoT objects will inhibit the adoption and slow down the IoT growth.

Strong security is accomplished with both software and hardware. The overall system security strength is a result of how much security services the system addresses and its ability to resist known security attacks or threats. Security technologies built deep into the hardware are less vulnerable to attacks.

Types of Security Services or Properties	Types of Security Attacks and Threats
Confidentiality, Integrity, Availability, Access Control (Authentication, Authorization), Attribution, Accountability, Audit, Attestation, Non-repudiation, Anonymity	Confidential Breach, Integrity Breach, Availability Breach, Authentication Breach, Privacy Breach, Anonymity Breach, Insider Threats, HW Attacks, SW Attacks, Side-channel Attacks

Using strong security design methods, like a military grade system that require all security services and counter measures against security treats, will add cost and tend to have a negative impact on system performance. Many IoT edge and gateway devices are cost sensitive and many of these devices does not need military grade security. IoT designers' challenge is deciding how much security services to add while remaining within budget.

For decades, standard flash memory has been playing a role in hardware security. Flash memory enable secure boot with its non-volatility and data retention capability. The use of the flash sector or block protection feature, adds insurance towards data integrity. Data confidentiality can be accomplished when the stored data is encrypted and the encryption process is managed by the host processor or microcontroller. Flash memory provide multiple sets of 256 bytes, in the flash registers, which are One Time Programmable (OTP) by the end user. The OTP sets are often used for storing manufacturers' unique private keys to enable authorized access. Most notably flash memory allows in-field code updates.

The latest security feature of Winbond W74M devices involves a multi-layer authentication process before accessing and executing code stored in the serial flash. Authentication is performed as needed and is initiated by the host. IoT devices using standard serial flash can easily upgrade their system security using the same footprint and with minimal cost increase.

Winbond's W74M product family comes with a standard key-hashed message authentication code (HMAC) SHA-256 crypto accelerator, four separate sets of 256-bit OTP root key storage, 256-bit volatile HMAC key storage and nonvolatile 32-bit storage area for the Monotonic Counter (MC) values. Multi-layer authentication is accomplished with a "Challenge and Response" routine that involves the secret root key, a session key and the updated MC value. Each W74M12F can provide the authentication security service for up to 4 different hosts or systems.

The W74M devices are available in densities ranging from 32 Mb to 1 Gb and use the same space efficient packages as conventional serial flash devices.

Density	Part Number	Package
1 Gb	W74M01GVZEIG	WSON 8×6
256 Mb	W74M25FVZEIQ	WSON 8×6
128 Mb	W74M12FVSSIQ	8-Pin SOIC, 208 mil
64 Mb	W74M64FVSSIQ	8-Pin SOIC, 208 mil
32 Mb	W74M32FVSSIQ	8-Pin SOIC, 208 mil

Winbond's Authentication flash memory product family is ideal for system designs requiring Authentication and Integrity security properties. The W74M devices can also prevent Replay Attacks, example of an Integrity Breach, and Counterfeiting of devices or systems in the field, with minimum cost impact.

About Winbond

Winbond Electronics Corporation is a memory IC company engaged in design, manufacturing and sales services to provide its global customers top quality memory solutions. Winbond's product lines include NOR Flash Memory, Serial and Parallel NAND, Specialty DRAM and Mobile DRAM.

Winbond products are widely used by companies in the IoT vertical markets such as computing, connected multimedia devices, automobile, networking systems, and industrial. Winbond offers automotive and Industrial-Plus Grade Flash and DRAM products with longevity support. Winbond has approximately 2,200 employees worldwide and is headquartered in Taichung, Taiwan.

Online
www.arrow.com/IoT

Five Years Out