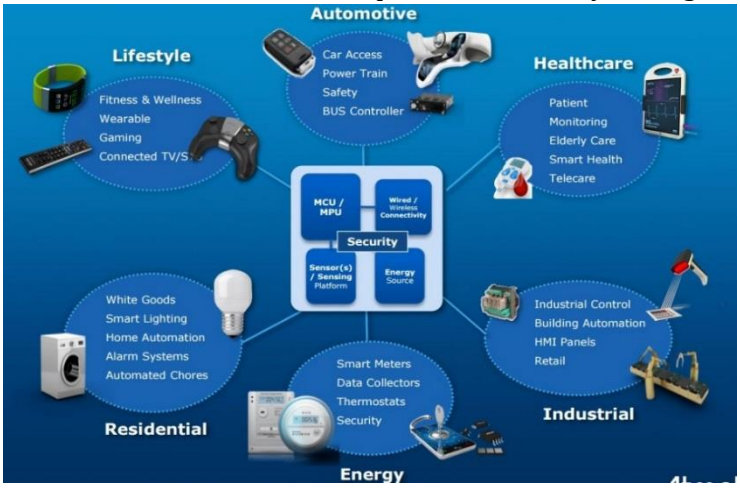
INTRODUCTION

In today's electronics market, the creative process has seen an explosion in innovation spurring the creation of the "Internet of Things" (IoT). The IoT can be defined as a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data. This has been seen in the development of consumer goods such as wireless light bulbs, smart refrigerators with touch screens and webcams, and smart locks for home security. These developments can also be apparent in safety-critical systems such as embedded medical devices, transportation, industrial control systems, power generation and smart grids, emergency response, aerospace and military applications. Society is creating a growing reliance on automated systems that are expected to communicate effectively and securely.

The increasing frequency of announcements of large scale security breaches into corporate and government systems, and the resulting damage caused, is a clear indicator that security is the latest challenge in the next generation of connected devices and systems. Former Secretary of Defense Chuck Hagel has said, "Our nation's reliance on cyberspace outpaces our cybersecurity" [1]. The U.S. State of Cybercrime published a survey that concluded online attackers are more technologically advanced than the cybersecurity technologies designed to thwart them. Ed Lowery of the U.S. Secret Service's criminal investigative division commented on that survey saying the government needs to take "a radically different approach to cybersecurity" [2]. Traditional software based encryption technology for network security combined with "on-device, burned in identifiers" for smart devices is vulnerable to malicious attacks from unwanted intruders.

SHORTFALLS AND FAILURES IN CYBER SECURITY

The meteoric rise in wirelessly connected devices and services also comes with an increase in examples of serious breaches in the security implemented to protect such systems. , In a recent article for WIRED Magazine two hackers from Illinois demonstrated their ability to wirelessly hack into a vehicle's internal computer network by taking advantage of their popular entertainment features. Vehicles are more commonly becoming internet-connected smart cars that feature a multitude of entertainment options that are wirelessly connected to a network. These features increase the luxury and leisure for a consumer but leave them available to attack. In the demonstration conducted for WIRED, the two hackers were able to disable the transmission of a vehicle driving 70 mph on a highway all without leaving the couch in their apartment. They had access to the transmission, brakes, electronics, climate control, and other critical components [3]. In



the industrial environment, highly desirable targets for malicious attacks include smart grid field controllers and utility flow monitors. In another recent experiment, reported by the BBC, security weaknesses in smart meters used in Spain were exposed [4]. Encryption keys were found to be easily accessible and a hacker knowing these keys can spoof transmissions from the meter to send false usage data. Additionally, one of the most recent high-profile examples of threats associated with user-accessible networked devices is when a hacker allegedly took control of a commercial airline flight [5]. According to court documents, the FBI is investigating whether a passenger gained access to the in-flight entertainment systems by plugging his laptop into the electronic box mounted under his seat, and then accessing other systems including the jet's thrust management computer.

In another WIRED publication, an article featured the hack of VW's key fob and door lock system. "The researchers found that with some "tedious reverse engineering" of one component inside a Volkswagen's internal network, they were able to extract a single cryptographic key value shared among millions of Volkswagen vehicles. By then using their radio hardware to intercept another value that's unique to the target vehicle and included in the signal sent every time a driver presses the key fob's buttons, they can combine the two supposedly secret numbers to clone the key fob and access to the car. "You only need to eavesdrop once," says Birmingham researcher David Oswald. "From that point on you can make a clone of the original remote control that locks and unlocks a vehicle as many times as you want." With 100's of sensors and controllers in modern automobiles similar vulnerabilities are presented regularly [6].

ENTHENTICA HELP KG

Enthentica introduces a new hardware-embedded delay PUF (Physically Unclonable Function) technology to address the vulnerabilities of existing security methods for generating and storing secret keys and bitstrings for encryption and authentication functions. The Enthentica Hardware Embedded Delay PUF (*HELP KG*) leverages the natural variations of the chip as a source of randomness (entropy) for the generation of a virtually unlimited number of unique bitstrings and Keys significantly increasing the difficulty for adversaries to attack and break a chip's security mechanism. This technology can be easily implemented into existing devices and will significantly improve the security and privacy of information and communications accessed from mobile platforms and in the cloud, as well as hardened safety-critical systems.

The current approach for storing secret bitstrings used in encryption based security functions is to store them in an on-board or on-chip non-volatile memory (NVM). Although NVM is highly reliable, it adds cost due to the additional masks required during chip fabrication, and is vulnerable to invasive attacks. The automatic, on-chip generation of keys and bitstrings by HELP KG simplifies and strengthens key management by eliminating the requirement of NVM storage of secret keys. Bitstrings and keys are generated on-the-fly as needed, and are also tamper-evident, whereby attempts by adversaries to invasively read-out PUF data in fact irreversibly changes and/or destroys that data.

DYNAMIC SECRET KEY GENERATION

The *HELP Key* Generation (KG) Engine provides reproducible bitstrings to serve as keys for encryption or authentication security functions. The strong PUF characteristic of HELP makes it possible to generate a virtually unlimited number of bitstrings and dramatically increases its resiliency to model-building attacks. The hardware interface is flexible and small, simplifying the integration of *HELP KG* into customer products. When a new key is needed (enrollment), challenges are delivered to the *HELP KG* engine from memory or a server. The input challenges are applied to the entropy source, and the responses are processed by the *HELP KG* engine into a key and corresponding helper data bitstring. The helper data bitstring is used by the *HELP KG* engine during regeneration, a process which reproduces the bitstring exactly with high reliability using the same challenges and helper data bitstring. The keys produced by the *HELP KG* engine are cryptographic quality and possess excellent statistical properties related to uniqueness and randomness.

EASE OF IMPLEMENTATION AND SMALL FOOTPRINT

A unique, distinguishing feature of *HELP KG* is its integration into existing functional units. This feature significantly reduces the overhead of incorporating HELP into small form-factor, low-cost resource-constrained devices while simultaneously taking advantage of the large source of entropy provided by the functional unit. The *HELP KG* in this case is truly 'embedded' and has a much smaller footprint and energy consumption profile. HELP can be fully and immediately integrated into any Xilinx-based FPGA system with no custom integrated circuit requirements. *HELP KG* provides hardware-derived bitstrings and keys for many types of application environments including:

- Keys for Encryption
- Unique bitstrings and nonces for Authentication of IoT devices
- Unique bitstrings for enabling data integrity
- Unique bitstrings for establishing providence and supply chain tracking
- Unique bitstrings for RFID applications
- Keys and unique bitstrings for Supervisory Control and Data Acquisition (SCADA) systems
- Tamper detection of cryptographic functional units

STRENGTHENING THE IOT

Enthentica's Strong *HELP KG*, is a hardware embedded cyber physical security solution for smart mobile or embedded devices in the Industrial and Consumer IOT. By starting at the silicon level the overall security of connected devices is fortified from the ground up.

HELP STATISTICAL PROPERTIES

HELP KG is evaluated using three statistical metrics, namely uniqueness (measured as Inter-chip Hamming Distance or HD_{inter}), reproducibility (measured using Intra-chip Hamming Distance or HD_{intra}) and randomness (measured using the NIST -- National Institute of Standards and Technology -- statistical tests).

Uniqueness

The overall HD_{inter} of the bitstrings generated using these 4096 timing values is between 49 and 50% (ideal is 50%).

Reproducibility

Overall HD_{intra} is less than 10^{-6}.

RANDOMNESS

The HELP KG generated bitstrings pass all of the NIST statistical tests.

These statistical results reflect the high quality of the generated bitsrings and demonstrate that they can be used in cryptographic applications.

APPLICATIONS AND BENEFITS

Enthentica's *HELP KG* can be easily implemented to run on any FPGA to increase on-chip security. This dynamic PUF keeps encryption keys unique and safe for the most critical of applications. The Defense, aerospace, and utilities industries can benefit from the improved silicon level security of Enthentica's HELP KG. Moreover, *HELP KG* can be used for supply chain authentication, preventing adversaries from substituting genuine parts with counterfeits or malicious clones. HELP KG has following characteristics

- Leverages existing on-chip functional unit as source of entropy for bitstring generation.
- Small footprint and low power consumption resulting in reduced overhead and cost savings
- Physical security improvement by eliminating storage or "burn-in" of the device's secret key in the Non Volatile Memory (NVM)
- Reduces susceptibility to machine learning or power probing by an adversary attempting to clone or steal secret identifiers (keys)
- Ability to change the secret identifiers (keys) frequently

- Traceable authentication and roots of trust during (chip) manufacturing (anti-counterfeiting)
- Easy to install and update remotely
- Impossible to copy or duplicate
- Can be implemented on any device with a Xilinx FPGA SoC

References

[1] http://www.usnews.com/news/politics/articles/2014/03/28/pentagon-to-triple-cyber-staff-to-thwart-attacks

[2] http://fortune.com/2014/05/28/cybercrime-is-outwitting-outpacing-security/

[3] https://www.wired.com/tag/car-hacking/

[4] http://www.bbc.co.uk/news/technology-29643276

[5] http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

[6] https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/