Plaintext
News and notes from SecureRF and the security industry

Sponsored by: SECURE RF
Embedded Security Solutions

SEPTEMBER/OCTOBER 2010

Announcing the LIME Tag™ Sensor 2.0

The first samples of SecureRF Corporation's new LIME Tag™ Sensor 2.0 are back from assembly and now in our hands undergoing final review. This battery-assisted passive (BAP) RFID tag with public-key Onboard Security™ contains a temperature sensor and has ports for 4 additional sensors.

The LIME Tag Sensor 2.0 provides a flexible platform to meet a wide range of industry needs for security and sensing while supporting the ISO18000-6 standard. Users can significantly reduce costs and risks associated with new projects with the LIME Tag's flexible configuration and implementation options. View the spec sheet at www.securerf.com/pdf/LIMETagSensor2.pdf.

As we prepare for production runs in Q1 of 2011, we welcome your project and pre-order inquiries. If you are interested in the LIME Tag 2.0, please contact us at Sales@SecureRF.com.

Recognition and Events

- SecureRF has been chosen as one of the 3 United States East Coast Finalists in the Best Security SME category of the Global Security Challenge Competition 2010. CEO, Louis Parks presents our innovation at the GSC East Coast Regional Final, at the British Embassy in Washington-DC on 23rd September 2010.
- SecureRF will be recognized as a "Company to Watch" at the CTC's Innovation & Entrepreneurship Summit - September 30, 2010 in New Haven, CT.
- Louis Parks will be part of panel discussion on DASH7 wireless data technology at the November 15th meeting of the **MIT Enterprise Forum of Cambridge RFID SIG (Auto-ID and Sensing Solutions)** - Register at http://www.meetup.com/MITRFID/calendar/14191442/.

IN THIS ISSUE

RFID SECURITY BLOG

Do you want to learn more and participate in the discussion on RFID Security? Visit the RFID Security blog. Recent topics have included:

- Smart Grid Security Warnings
- EU Prescription Drug Anti-counterfeiting Legislation
- Lack of Security in Smart-Meter Rollouts
- Data Protection Methods Only Work If You Use Them

And more…
Read these entries and add your comments at www.securerf.com/RFID-Security-blog/.

SecureRF Granted Patent - Cryptographic Solution Suitable For Embedded or Low Resource Computing Devices

SecureRF is excited to announce its latest patent!

The United States Patent and Trademark Office has granted SecureRF U.S. Patent 7,649,999 for the world's first cryptography method to run in linear time. The patented algorithm provides a key agreement protocol and a method for generating a secret key to facilitate secure communications. This patent broadly covers the foundation of our methods, known as the Algebraic Eraser™, and it is suitable for securing low resources computing devices such as sensors, Smart Grid microcontrollers, and of course, RFID tags. Our patent, titled "Method and apparatus for establishing a key agreement protocol," can be viewed at http://patft.uspto.gov/ by searching for patent number 7,649,999.

To learn more, read our press release: SecureRF Granted U.S. Patent for Secure Communications Method Targeting Sensors and Wireless Platforms - Cryptographic Solution Suitable for Embedded or Low Resource Computing Devices.

An Introduction to Cryptographic Security Methods

- What is the difference between private-key and public-key cryptography?
- What are the challenges in using asymmetric cryptography to protect low-resource devices?
- What is the difference between Diffie-Hellman and RSA asymmetric cryptography methods?

Since SecureRF's Algebraic Eraser™ technology offers both symmetric (i.e. private key or secret key) and asymmetric (i.e. public-key) cryptography of the Diffie-Hellman type, we found ourselves having to answer these questions a lot. We couldn't find a good overview describing these various cryptographic methods and decided to write one ourselves.

We invite you to read our new white paper:
An Introduction to Cryptographic Security Methods and Their Role in Securing Low Resource Computing Devices: An Overview of Public-key Cryptosystems based on RSA, Diffie-Hellman and the Next Generation of Public-key Cryptographic Security for Low-Resource Computing Devices - the Algebraic Eraser™.

This was written as an introduction to the topic for business people, engineers and logistics folks. Download it now (no registration required) at www.securerf.com/white.shtml.

VOTE FOR SECURERF

Vote for SecureRF's idea in the GE Ecomagination Challenge: Securing the "Social Network of Devices" - a safer Smart Grid. Deadline is September 30th.

ABOUT SECURERF

SecureRF Corporation provides security solutions for wireless sensor networks, radio frequency identification (RFID), embedded systems, machine-to-machine (M2) and other low resource devices. SecureRF's methods enable high value asset tracking, monitoring and anti-counterfeiting applications in the pharmaceutical, defense and homeland security sectors. The company's technology, based on a breakthrough in cryptography that is lightweight yet highly secure, provides Onboard Security™ features such as authentication and data protection for passive, semi-active and active RFID tags and other embedded systems. SecureRF supports EPCglobal, DASH7 and ISO standards and offers both standard and custom products with optional sensors.

CONTACT US

Headquarters:
175 Post Road West
Westport, CT 06880

Technology and Engineering Office:
5 Science Park at Yale
New Haven, CT, 06511

Phone: (203) 227-3151

www.SecureRF.com

Supported by National Science Foundation

SecureRF Corporation is halfway through a 2 year Small Business Innovation Research (SBIR) grant from the National Science Foundation. This SBIR Phase II funding allows us to continue our work developing a secure, passive RFID tag that meets EPCglobal protocols. The release of the LIME Tag 2.0 is one of the major milestones which shows that our Algebraic Eraser security protocol runs on a battery assisted UHF passive tag, and it will eventually run on a completely passive UHF tag.

This material is based upon work supported by the National Science Foundation under Grant No. IIP-0924363. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.