

09-17-01

AIPROV



PROVISIONAL APPLICATION under 37 C.F.R. §1.53
TRANSMITTAL FORM

Docket Number: **TI-3335**

Ass't Commissioner for Patents
 Washington, D.C. 20231

EXPRESS MAILING™ Mailing Label No **EL645452687**
 Date of Deposit **September 10, 2001.**

Dear Sir:

Enclosed application parts are:

☒	Spec w/Claims	Number of Pages	_____
☐	Spec w/o Claims	Number of Pages	<u>11</u>
☐	Formal drawings	Number of Sheets	_____
☐	Informal drawings	Number of Sheets	_____
☐	Other:	_____	

Inventor(s):

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY, STATE OR FOREIGN COUNTRY)
Bonnett	William	B.	Dallas, TX US
Dagani	Gabriel		Bluffton, OH US
Robinson	Alec	C.	Dallas, TX US

TITLE OF INVENTION.

System and Method for Firmware Upgrade

CORRESPONDENCE ADDRESS:

Robert D. Marshall, Jr.
 Customer Number 23494

PHONE: (972) 917-5290
 FAX: (972) 917-4418/4417
 E-Mail Address: r-marshall2@ti.com

Was this invention made under a Government contract? ☒ No ☐ Yes

Identify contract and the Government agency: _____

Please charge \$150 to Deposit Account No. 20-0668. An original and two copies are enclosed.

Respectfully submitted,

Robert D. Marshall, Jr.
 Registration No. 28,527

Date September 10, 2001**PROVISIONAL APPLICATION ONLY**

TI-33356

1379
EDM**TI INVENTION / INNOVATION DISCLOSURE**

SEND COMPLETED FORM TO: TI CORPORATE PATENTS
ATTN: Jackie McBride
E-Mail: j-mcbride@ti.com
FAX: (972) 917-4418
Mail Station M/S 3999
PC Drop PPC-B

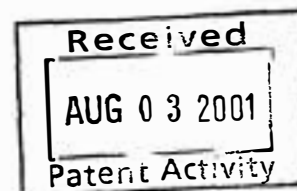
HELPLINE: William B. Kempler
E-Mail: w-kempler@ti.com
PHONE: (972) 917-5452
FAX: (972) 917-4418

If you are employed by a TI subsidiary company, send this form to your site coordinator.

To prepare your invention disclosure, follow the step-by-step directions on the form that follows. Type or print answers to the questions in the spaces provided.

**PLEASE PROVIDE ANSWERS TO ALL OF THE QUESTIONS
OTHERWISE THERE COULD BE DELAYS IN PROCESSING**

If you already have an engineering spec, please send it with your invention disclosure. Computer documentation and drawings, marketing foils, notebook entries, paper manuscripts, articles, and any other material that you already have can be copied or sent electronically.



PATENT DISCLOSURE FORM

33356

DOCKET NO. TI-(to be filled in by Patent Activity)

IF ELECTRONICALLY TRANSMITTED, PROCESSING OF YOUR
DISCLOSURE CANNOT BE COMPLETED WITHOUT A
FOLLOW-UP COPY SIGNED AND DATED BY ALL INVENTORS
AND AT LEAST ONE WITNESS.

1. Please suggest a descriptive title for your invention:

SYSTEM AND METHOD FOR FIRMWARE UPGRADE ACR

2. This invention supports strategy: (check 1 or more)

☐ DLP
☐ Materials
☐ Fab/Processes
☐ Assembly/Test/Packaging
☒ Other

DSPS
☒ Wireless
☐ Video
☐ Set Top
☒ Application Specific
☐ Remote/Access/Networking
☒ Emerging Markets
☐ Mixed Signal & Logic
☒ Mass Storage
☒ Other

Received

AUG 03 2001

Patent Activity

3. What is the problem solved by your invention?

Programmable portable electronic devices or appliances, such as digitized audio recorder/players can require field upgrade of their operating software. An easy and convenient method to perform this upgrade is to connect the appliance to a host computer such that the device appears as a disk drive or Mass Storage Class device to that host computer's operating system. The appliance operating system files are then copied to the appliance represented by the apparent disk drive using methods common to the host computer operating system and familiar to users. In this practice, the appliance's operating software is exposed to the user and appears as non-executable or non-useful files to the host computer's operating system. In this instance, there rises the potential for corruption or inadvertent deletion of the appliance's operating software by the user of the portable electronics device. If the

2

appliance's software is corrupted or deleted, then the appliance becomes useless.

4. What is your solution to the problem?

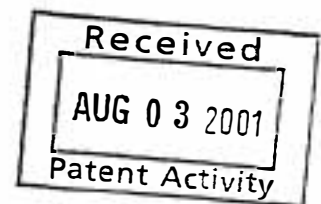
After the software upgrade transfer mentioned above is performed, the portable appliance identifies this software either automatically or by host computer command and hides it from the host computer's operating system. This is facilitated by partitioning the single storage media into at least two sections. All but one of these sections are hidden from the host computer's operating system. The portable device moves this software from the partitions exposed to the host computer to a partition hidden from the host computer. Additionally, this solution incorporated a method for decrypting an encrypted file while moving the file from the exposed partition to the hidden partition.

5. When was your solution first conceptually or mentally complete?

Date: May 1, 2001

6. What is the first tangible evidence of such completion?

Date: July 20, 2001



3

7. What is different about your solution, compared with other solutions to the same problem?

Other solutions do not allow the connection of the portable device to appear as a disk drive or Mass Storage Class device to the Host computer's operating system. These system require special utilities that are new and foreign to the user. There exist even other solutions that require the appliance to have storage media that can be removed from the appliance and then placed in an additional adapter.

8. What are the advantages of your solution?

This solution allows a single storage media that does not require removal from the appliance, thus reduces cost. Software upgrades effort is reduced and easily understood by the user. The cost of providing Host side utilities is eliminated. Additionally the cost additional adapters is eliminated.

9. What TI products, processes, projects or operations currently implement your invention?

Nokia's Maverick product whose Intellectual Property is bound to Texas Instruments by Texas Instrument's Internet Audio License Agreement

10. What is the date of the first implementation?

Date: July 20, 2001

11. What record exists to prove this date?

Archived Software Source Code

12. Is there any future implementation planned?

Yes ☒ No ☐

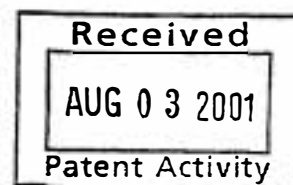
If so, please furnish the TI PART No. or project name

Secure Firmware Upgrade Utility

13. Has the invention been published or disclosed to anyone outside of TI?

Yes ☒ No ☐

When? June 14, 2001



4

If planned - when? none planned (Catalog, advertising, data book, application note, conference paper, magazine article, TI TJ, proposal document.)

Was there a nondisclosure agreement (NDA)?

Yes ☒ No ☐

14. Has a TI product incorporating the invention been publicly introduced, quoted, sampled or shipped?

Yes ☐ No ☒

When? If planned--when?

15. Was the invention conceived or first implemented in the performance of a government contract or subcontract?

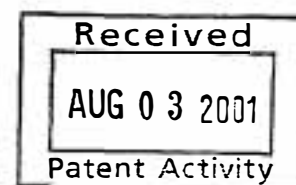
Yes ☐ No ☒

Contract #:

THE INVENTION DESCRIBED BY THIS DISCLOSURE IS SUBMITTED
PURSUANT TO MY EMPLOYMENT AGREEMENT WITH TEXAS INSTRUMENTS
INCORPORATED OR A TI SUBSIDIARY (SPECIFY):

Has this disclosure been previously sent to the Patent Department electronically (unsigned)?

Yes ☐ No ☒



PLEASE PRINT ALL INVENTOR INFORMATION.

Inventor 1's Name: William Bruce Bonnett
(First, Middle, Last)

Home Address: 9730 Kilarney Dallas, Texas 75218
(Street, City, State, Zip)

E-Mail Address: bruce_bonnett@ti.com

Employee #: a0157595

TI Division & Cost Center 003/02126

Phone #: (214) 480- 6036

Pager #:

Country of Citizenship: U.S.A

Inventor 1's Signature: 

Date: 01-AUG-01

Mail Station: 8634



Inventor 2's Name: Gabriel Dagani
(First, Middle, Last)

Home Address: 9064 Augsburg Rd, Bluffton OH 45817
(Street, City, State, Zip)

E-Mail Address: g-dagani1@ti.com

Employee #: a0323624

TI Division & Cost Center 003/00111

Phone #: (214) 480 2211

Pager #:

Country of Citizenship: U. S. A.

Inventor 2's Signature: 

Date: 8/1/01

Mail Station 8634



Inventor 3's Name: Alec Clement Robinson
(First, Middle, Last)

Home Address: 5427 Emerson Avenue, Dallas, TX 75209
(Street, City, State, Zip)

E-Mail Address: arobins@ti.com

Employee #: a0212638

TI Division & Cost Center 003/05117

Phone #: 214 480 3481

Pager #:

Country of Citizenship: U. S. A

Inventor 3's Signature: Alec C. Robinson

Date: 8-1-01

Mail Station: 8634



8

Inventor 4's Name:

(First, Middle, Last)

Home Address:

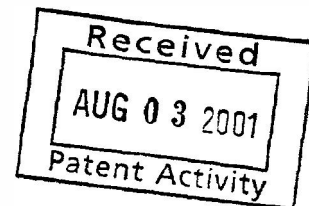
(Street, City, State, Zip)

E-Mail Address:**Employee #:****TI Division & Cost Center****Phone #:****Pager #:****Country of Citizenship:****Inventor 4's Signature:** _____**Date:****Mail Station:**
.....

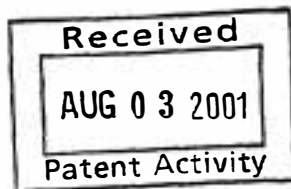
This invention disclosure with any attachments was read and understood by me on

Chah McInally
Witness 1:Aug 1, 2001
Date

This invention disclosure with any attachments was read and understood by me on

Charles D. Lueck
Witness 2:Aug 2, 2001
Date

(9)



Date 7/30/01

Alec Robinson
Bruce Bonnett
Gabe Dagani

Patent Disclosure for:

Secure Firmware Upgrade Utility**Introduction:**

In the world of digital devices, projects are completed in "Internet Time," which is to say that product development happens in a matter of weeks instead of months. With this decrease of time from design to manufacture, mistakes and bugs are found after software deliveries have been made. In order to update firmware in existing products during manufacture or even in the field, upgrade utilities are needed; these utilities are usually unique and reflect the needs of the appliance's peripherals.

The Internet Audio Applications team recently supported a DSP board design that incorporated a C54x based DSP, NAND flash memory, and USB capabilities. The NAND flash was initialized using a FAT system, and files were stored and accessed using a USB code image driven by Mass Storage Class Drivers.

The software architecture for this IA system supports dynamic loading of images into the DSP's RAM. These images consist of the Loader image, the MCU image, the USB image, and various decoder / encoder images. The main workhorse of this system is the load image, which is stored in the DSP's RAM. This is the code that is initially boot-loaded from the NAND; it searches and finds the other images to load into the remaining DSP RAM. For example, if the MCU detected that a user wanted to play an MP3 file, it would tell the Loader image to load the MP3 decoder image into the DSP's RAM and execute the file-decode.

Problem Encountered:

A user problem arises when Mass Storage Class Drivers are incorporated into a software system that requires image files to be loaded into the DSP. If the user deletes any image, then that functionality is lost for the appliance. If the USB or loader images are lost, then the appliance becomes useless. In any other flash based system, such as a compact flash based system, the card could be reloaded with images and everything would be fine. However, in the system mentioned, the NAND memory is only accessed through the DSP's interface. Therefore by eliminating the DSP's functionality, we eliminate all access to the NAND memory.

Firmware security is also a major concern for firmware developers and device manufacturers; these developers want to prevent the firmware images from being viewed or manipulated in any form. Furthermore, we want to protect copyrighted material from falling into the wrong hands.

Solution Overview:

In order to solve this problem, we needed to limit access to the images. The images should only be accessible to the developing companies, and they should be hidden to all customers. Once this decision was reached we decided to create an upgrade utility that took our current NAND setup and integrated a second hidden partition to store these image files.

10

Firmware Upgrade Security:

We created a wrapper for all the images using a tailored PC program. This program created a header that described how many images were images, the size of the images, and the image names. This utility allowed the individual upgrade files to be placed in one larger file.

In order to prevent pirated patches from entering our firmware, we licensed an encryption library to prepare an encrypted file from our image wrapper for easy encrypting, porting and authenticating purposes. An encrypted .lok file was created. The key for this encryption is proprietary to the library owners and specifically created for this line of products.

A PC utility was created to send a USB vendor specific command that tells the device to start upgrading. This utility is nothing more than a trigger for when the device is already plugged into the PC for Mass Storage Class purposes. If the device doesn't respond correctly, the user is notified. This could mean that the correct USB image file is not present on the device.

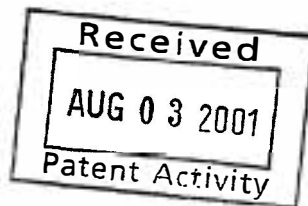
Secure Firmware Upgrade Details:

The following is a step-by-step description of how the upgrade process works:

- 1) The User puts the player in USB mode by connecting a USB cable from the host PC to the player.
- 2) A new USB firmware image is dragged and dropped onto the player using MSC drivers, along with the new upgrade .lok file (encrypted upgrade package).
- 3) The USB is unplugged and plugged back in, to reactivate the new USB firmware.
- 4) The user then launches the "Secure Firmware Upgrade.exe" utility by double clicking.
- 5) The SFU process then disconnects itself (software speaking) from the host PC, creates the second partition, formats it with FAT tables, and authenticates and decrypts the .lok file. Immediately after, it creates a new file from the decrypted info. and parses the specialized wrapper so it then places the new firmware on the hidden partition. It then reformats the first partition. The USB connection is reconnected. However, to access the new images, the new loader must be loaded, and this means that the player's power must be reset.

Conclusion

The whole upgrade process utilizes many processes that have been around for awhile. However, we hope to patent the whole process as a larger entity, such that it is a unique way to securely upgrade firmware on an embedded system with flash and USB as peripherals.



4