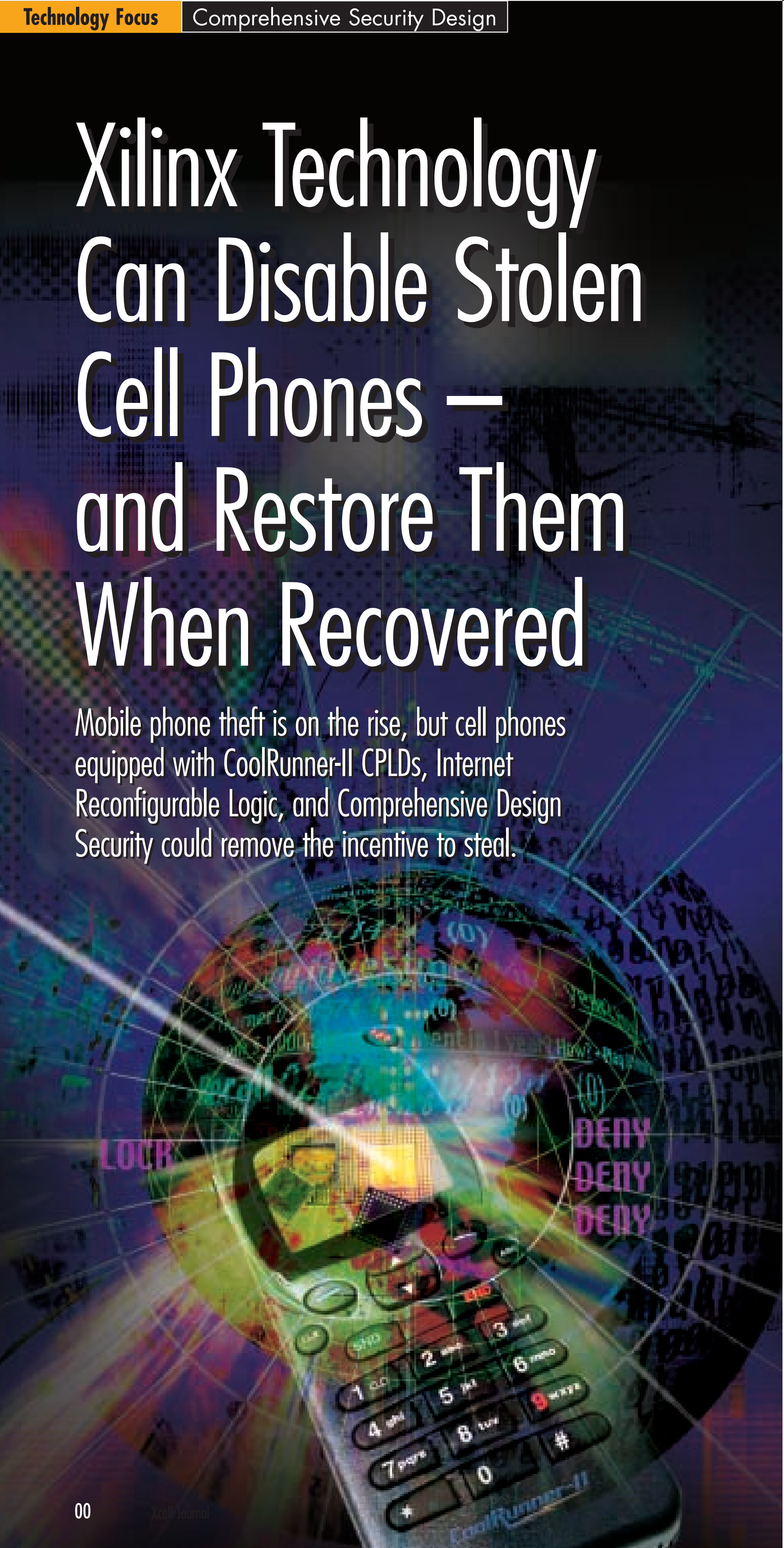
Xilinx Technology Can Disable Stolen Cell Phones – and Restore Them When Recovered

Mobile phone theft is on the rise, but cell phones equipped with CoolRunner-II CPLDs, Internet Reconfigurable Logic, and Comprehensive Design Security could remove the incentive to steal.



by Karen Parnell
Product Marketing Manager, Automotive
Xilinx Inc.
karen.parnell@xilinx.com

Researchers at the University of California at San Diego have found a way to "blow up" silicon chips with an electrical signal, according to a recent article, "Exploding Chips Could Foil Laptop Thieves," in *NewScientist.com.*

The practical application of self-destroying chips would be the ability to remotely disable stolen laptops, cell phones, PDAs, and other devices using wireless communication and containing confidential information.

According to the NewScientist.com article by Duncan Graham-Rowe, when a device is stolen, the victim or service provider could call the device and transmit a self-destruct order to "detonate" a small quantity of gadolinium nitrate. The resulting explosion would destroy the critical chips, rendering the stolen device useless – and irreparable. Unfortunately, information in the device memory might remain intact – and that data could sometimes be more useful than the device itself.

At Xilinx, we have a better idea. With IRL™ (Internet Reconfigurable Logic) technology, Comprehensive Design Security, and CoolRunner™-II CPLDs, we can remotely disable up to four different functions of a stolen device, rendering it inoperable, and with locked-down, tamperproof data. The beauty of the Xilinx solution is the unit is not damaged in any way – full functionality and data can be easily restored if the device is recovered.

Whose Problem Is It?

Every three minutes in the UK, a mobile phone is stolen, sometimes at knifepoint. This phenomenon is not just confined to the UK. It is a global issue and continuing to rise. For example, in New South Wales, in Australia, nearly 40,000 phones were stolen between October 1999 and September 2000, a 100% rise over the previous year.

But what if the phone hardware could be disabled and effectively rendered useless, then surely the need to steal this much-coveted possession would decline. Wouldn't it? Not necessarily ...

When a mobile phone is stolen, it is relatively easy for the phone operator to disable the Subscriber Identity Module (SIM) card inside the phone so that calls can not be made using that particular number. This is of great benefit to the bill player, but this is not usually why the phone has been stolen. Hackers can install a modified SIM card that fools the phone into believing it is a prepaid, "pay-as-you-go" phone with unlimited credits. This allows the phone to be used indefinitely, free of charge.

What Are Today's Solutions?

In March 2001, the then-UK Home Secretary Jack Straw said that he would meet with the world's mobile phone manufacturers and police to try to stop the growing threat of street robberies that target mobile phones. Among the measures considered were the need for general vigilance, discrete usage, knowledge of security codes to lock the phone, and the use of an International Mobile Equipment Identifier (IMEI) number.

In addition to the SIM card, digital mobile phones connected to the GSM (Global System for Mobile Communications) network possess an IMEI identifier that is associated with the handset itself. (GSM is the dominant cellular system used in Europe and Asia.)

Mobile phone owners are encouraged to note down this number so that if the handset is stolen, then the operator can bar that specific phone from working on their network.

But what about the other networks? The handset can theoretically still be used on other networks if a suitable SIM can be found on the black market.

The need, therefore, is to find a way to completely disable the handset hardware on any cellular system – without blowing up the phone itself. Thus, the phone is useless to the thief, but it can be reactivated and restored if the phone recovered and returned to its rightful owner.

This message was again reinforced in January this year with UK ministers considering whether to introduce legislation that will force networks to introduce the aforementioned anti-theft measures, but, they stipulated, this would be "a last resort."

What Is Tomorrow's Solution?

The average mobile phone thief is becoming more discerning, because in the black market, the newer "smart phones" are becoming the target of choice. To date, the growth of mobile communications has been fuelled by voice calls, but voice is becoming a saturated market, with increasing competition forcing a decline in average revenue per user.

To maintain growth and even sustain current income and profits, cellular providers must introduce new services that will be attractive and beneficial to users, who will then need new types of technically sophisticated handsets from the providers' manufacturers.

In order to capture the market for replacement cellular handsets, the next wave of mobile phone handsets must be smarter, lighter, and last longer on one charge. These new smart phones are reinvigorating the flagging mobile market by providing must-have functionality. The cell phone has now moved from being just a humble voice communications device to a combined PDA, Internet access device, MP3 player, and games console.

For instance, Nokia recently unveiled its latest "lifestyle" function phone, the 5510. The phone includes an integrated digital music player (with 64 MB memory) for ACC (Advanced Audio Coding) and MP3 files, a full keyboard to facilitate better messaging functionality, and a handful of embedded games.

Contrary to recent times, the full cost of smart phone will be borne by the customer – not subsidized as a free loss leader by a wireless service provider, who intends to recover the cost of the hardware with inflated air-time rates.

These smart phones are more costly for the owner and/or network operator to replace if stolen. This cost risk has made the mobile phone companies rethink how their products are designed. The hardware of handset must have the built-in capability to be remotely disabled if stolen – but still traceable via GPS (global positioning system) or similar geographic locator systems.

Once recovered, the phones must be able to be reactivated to full functionality when returned to their owners. A phone with blown-up chips isn't worth recovering. To be a viable consumer product, the disabling component of a stolen cellular phone must be small, lightweight, low cost, low power – and capable of fully restoring the functionality of the phone upon recovery.

The Xilinx Solution

With typical forward thinking, Xilinx has already developed the tools to combat phone theft – IRL technology, Comprehensive Security Design, and the CoolRunner-II CPLD.

If a CoolRunner-II CPLD were used to perform the keypad interfacing in a handset, then if it were stolen, the keypad could be disabled remotely by the mobile phone operator using Xilinx IRL technology (Figure 1). When returned to its owner, the handset could then be reprogrammed again via an IRL bitstream to enable the keypad again. (IRL technology enables the remote upgrading or programming process of CPLD or FPGA hardware over any kind of network, including wireless.)

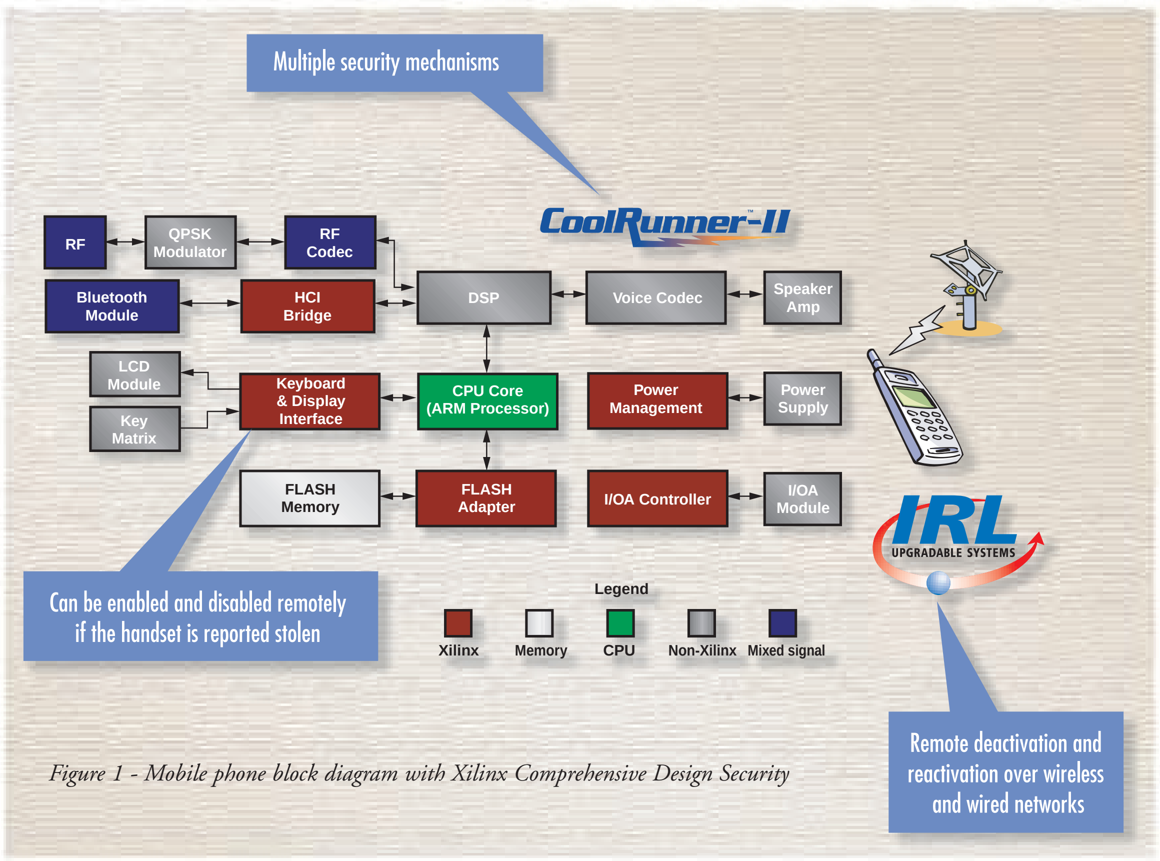


Figure 1 - Mobile phone block diagram with Xilinx Comprehensive Design Security

It is virtually impossible for the CoolRunner-II device (Figure 2) to be reactivated or for data to be retrieved from the handset by the thief or hacker. Xilinx Comprehensive Design Security provides an unprecedented four aspects of design security:

- Prevention of accidental/purposeful overwriting or read back of the configuration pattern
- Blocking visual or electrical detection of the configuration pattern
- Automatic device lockdown in response to electrical or laser tampering
- Physical implementation of the protection scheme that is virtually undetectable.

These design security aspects are not only buried within the layers of the device, but they are also scattered throughout the die to make their detection impossible. Designers can now design with the knowledge they are using the best design security available on any CPLD in the industry.

The enhanced features of CoolRunner-II also elevate the CPLD from an ASIC fix to that of an ASIC replacement. New features include clock doubling and clock division for lower power consumption, various I/O standards support for level translation, selectable Schmitt trigger inputs to solve signal integrity challenges, and bus hold.

Figure 2 - Multiple security functions embedded in CoolRunner-II CPLD

Conclusion

By utilizing a combination of IRL technology, Comprehensive Security Design, and ultra-low power CoolRunner-II CPLDs to remotely disable the hardware within a stolen mobile phone, phone operators and manufacturers can remove the incentive for theft – and improve the odds of recovery with geographic locator technology.

Furthermore, the triple-threat security technology of Xilinx-protected products can be extended to any consumer appliance, including laptops, set-top boxes for cable TV, PDAs, and other devices with wireless or wired network connectivity. As the word gets out, consumers will look for the Xilinx brand in the products they buy – and thieves will look the other way.