Set Top Box and Secure Video Player

Security Primer

Author: Bob Kulakowski
April 6, 2016

www.SecureTV.**TV** email: sales@secureTV.**TV**

Recent security advances in the silicon chips used to build Set Top Boxes (STBs) provide security advantages beyond smart-card based security for protecting broadcast television Pay TV and video services for Satellite, Cable, IPTV, Internet/Over The Top (OTT), and terrestrial networks. A major benefit to operators is that the newer security-enhanced STB chips provide better security than a smart card without smart card cost and smart card logistical issues. The enhanced STB security features are usually available without additional chip cost when compared to chips without enhanced security. This whitepaper describes the secure processing features of STB silicon chips and compares the benefits of security-enhanced STBs compared to smart card security. SecureTV will explain in more detail the enhanced security features of its security system after executing a Non-Disclosure Agreement.

Set Top Boxes are built using a single main processing chip often referred to as System-On-a-Chip (SOC) containing most or all of the processing required in a STB. A block diagram of a current day STB SOCs is shown in Figure 1, and the secure SOC contains a receiver/tuner front end, video stream processing, video decoders, audio decoders, stream decryption, USB, HDMI and other interface circuits.

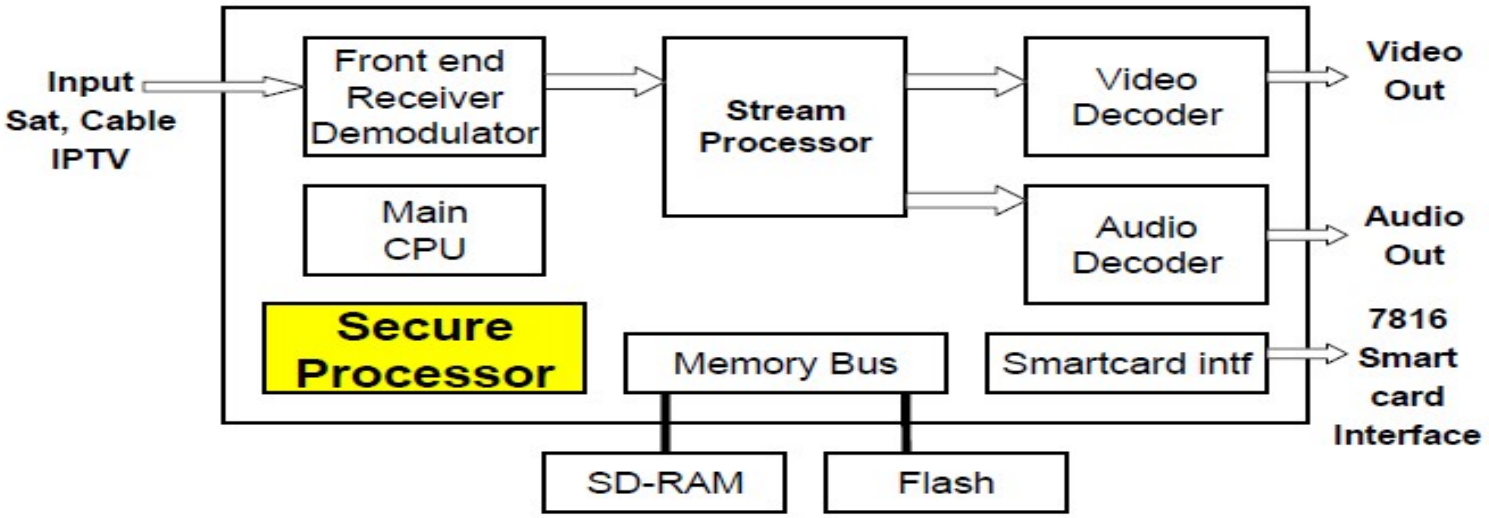

Figure 1. Secure STB System-On a Chip (SOC) containing Secure Processor

The secure processor section contained in a security enhanced STB SOC is shown in Figure 1 and typically includes the following security features:

- Secure Boot
- Device Specific Embedded Secret Keys
- Protected Control Word Stream Decryption
- Encrypted Memory Bus
- Anti-tamper circuitry
- Silicon circuitry camouflage
- Device clone protection
- JTAG Protection

A description of the security features contained in the Secure STB SOC is provided below.

Secure Boot – Secure SOCs include secure boot processing to verify that the security code running on the SOC has not been modified. Secure boot integrity checks the security software typically using RSA based digital code signature verification. Secure boot processing will detect when an adversary attempts to modify the security firmware and will prevent the code from running. Secure Boot protection is provided by processing inside the SOC and is extremely tamper resistant. The Secure Boot protection is designed in coordination with the STB manufacturer. Secure TV has works very closely with premier STB manufacturers to provide the most secure boot loader available.

Device Specific Embedded Secret Keys – Device specific cryptographic keys unique for each device are stored in protected memory in the Secure SOC. These keys prevent based device cloning because each Secure SOC has its own device specific keys stored in protected memory. The security system on headend servers uses these keys to send device specific encrypted data and messages that can only be decrypted on the device containing the appropriate device specific keys. As previously mentioned these keys are device specific and stored in silicon protected memory.

Secure Key Programming - Typically, device specific embedded Secret Keys are programmed in a secure facility, either during silicon chip manufacturing on the wafer fabrication line, or using a secure programming technique during STB manufacturing.

Black-box Programming - A device referred to as Black-Box is used to securely program keys from Conditional Access Security (CAS) vendors into the Secure SOC. Third party secure SOC programming companies provide secure black-box programming support for a number of Secure SOC manufacturers. The interesting benefit of these third-party services is that operators can prevent the CAS companies from controlling who owns the STB. Most CAS companies control ownership of the STB by preventing operators from having access to the secure boot key or the embedded secret key. In essence, when the CAS company owns the boot key or the embedded secret key the operator is prevented from replacing the CAS company at a later date. More information about the dirty tricks played by CAS vendors is described in the Key Escrow section below.

Protected Control Word – The keys used for encrypting and decrypting video are called Controlled Words (CWs) in DVB specifications. CWs are also referred to as the video scrambling keys. Control Words range in size from 56 bits to 128 bits and the CWs change frequently. In some systems CWs change every 300 milliseconds. Capturing and exporting CWs from a Set Top Box is one of the simplest ways to pirate a system. It is interesting to note that smart-card based systems provide no protection against control word piracy. The design of most Secure SOC chips includes hardware protection of Control Word thus preventing this simple form of piracy. The legacy CAS companies and smart-card vendors cannot prevent this form of piracy without secure SOCs. In the unlikely event that the Secure SOC hardware CW protection is hacked SecureTV has a

new patent-pending innovative software method that will protect hacked Secure SOCs. We know of no other vendor who can claim this.

Anti-tamper circuitry and Silicon circuitry camouflage - Silicon chip vendors selling Secure SOCs incorporate additional circuitry to prevent chip tampering. These vendors also use circuit camouflage techniques to increase the difficulty pirates face when reverse engineering STB and security chips. Secure SOC chip vendors have added similar anti-tamper and circuitry camouflage techniques commonly found in smart-cards.

Hacking a secure SOC at the silicon layer requires expensive hardware such as electron scanning microscopes, a lot of time, and is very expensive. Hacking a secure SOC is much more expensive than hacking a smart card because of the enormous complexity difference between the two. A smart card may have 2 million transistors while a secure SOC may have 50 million or more. The sheer physical silicon differences between the two dramatically increases the cost and complexity of hacking the secure SOC when compared to the smart card chip. While it is very difficult to hack a secure SOC chip, Secure TV is the only company that has designed software control word protection support as well as industry leading STB client renewability providing operators with the strongest arsenal against hacker threats.

Encrypted Memory Buses – Secure SOCs include memory bus encryption circuitry that encrypts data being written from the secure SOC and read into the secure SOC. Encrypted Memory buses make hacking a system using logic analyzer data capture more difficult when compared to a chip without memory bus encryption. Most secure SOCs change the memory bus encryption key each time the STB or device is powered on.

JTAG Protection – Larger silicon chips include JTAG support for chip and device debugging. The JTAG port also aids hackers in reverse engineering STB security code. Secure SOCs include JTAG password protection as well as the capability to disable the JTAG port. JTAG protection keeps the JTAG port disabled until a password is entered into the STB, thus enabling the JTAG port.

Smart-card support - Secure SOCs include an ISO 7816 smart card interface allowing for smart-cards to be used with the secure SOCs. Normally, an operator will not need to deploy smart-cards with secure SOCs. Smart-cards would only be deployed if the secure SOC is hacked in a way that innovative security systems such as that offered by SecureTV cannot repair. Most, or all current of the CAS vendors competitors to SecureTV do not have innovative security methods to secure hacked SOCs and will tell you that in the event of an SOC hack that you will need to buy smart cards. SecureTV does not need smart cards to re-secure a system wherein the secure SOC has been hacked. One might question whether legacy CAS vendors will support the hacking of secure SOCs to enable the sale of their antiquated smart card technology.

Key Escrow - A major problem facing Pay TV operators who use CAS systems from SecureTV's competitors is the way CAS vendors will lock themselves into the operators' system preventing the operator from switching to a different CAS supplier. We believe this is a dirty trick played on the unsuspecting customers of the CAS vendor. Many

operators who have purchased CAS systems from our competitors will gladly warn others of the dirty tricks plays be CAS vendors.

Key Escrow is a SecureTV solution that securely provides operators with key ownership and not the CAS company, giving the operator freedom to choose whichever CAS company they want. Additionally, DVB Simulcrypt allows operators to use a new CAS vendor for new STBs added to their network, while keeping the legacy STBs operating with the legacy CAS provider.

Secure SOC verses Smart Card Security – Secure SOCs offer significant security advantages when compared to smart cards. The Secure SOC benefits include the following two very important security features, namely Secure Boot, and Protected Control Words. These features make the total system security of a Secure SOC based CAS system much stronger than the security provided by smart-cards, without smart card costs and smart card deployment logistics.

Additionally, secure SOCs include the following security features often found in smart cards: embedded secret keys, anti-tamper circuitry, camouflage, device unique keys, black box programming, and other security circuitry.

One should question whether smart-card technology has been relegated obsolete or at best case one of the possible solutions to recover from the unlikely event of a secure SOC hack. Smart-card vendor claims in this area need to be carefully analyzed when compared to the innovative security offered by SecureTV.

CAS Vendor Technology Roadmap - The roadmap of the major CAS vendors includes updating their legacy and outdated systems by adding secure STB SOC support. However, now that the STB SOCs provide better security than their legacy systems, a company performing a security evaluation needs to question if their legacy approaches to security are simply outdated. The SecureTV system was designed from the ground up to support the new secure SOCs by security experts who understand secure SOCs, and have over 90 years of combined security design experience. In fact, the core of the SecureTV system in the year 2008 was one of the first deployed secure SOC based systems using security enhanced STB chips in the world.

Tivo-like devices and Video Players - Secure STB silicon can be used to build Tivo™ like devices that incorporate all of the security features discussed in this document. SecureTV's Hollywood approved security system incorporates patent-pending security technology that provides added layers of security in addition to the excellent security provided by the secure STB SOC for STBs, Tivo-like devices and Video Players.

The SecureTV system when used in Tivo like devices and Video Players store all of the content encrypted with device unique encryption keys, device hardware security bindings, and other device unique keys that provide the strongest level of protection in the industry.

Personal Video Recorder - The same security features described in the above section for Tivo-like Devices and Video Players is used to secure Personal Video Recorder content. Namely, the combination of recorded content using device unique keys, device hardware security bindings that result in industry leading security for PVR.

Security Comparison

The table below compares important security features and concepts of the SecureTV system with its competitors.

Security Feature	Legacy CASs (NDS,Nagra others)	SecureTV
Silicon protected device unique keys	✓	✓
Secure Boot	✓	✓
Independent Security audit	✓	✓
DVB, ATSC, MPEG, and other standards based system	✓	✓
Hollywood approved	✓	✓
Hardware control word (CW) protection	Yes in secure SOC	Yes in secure SOC
Software Control Word protection	No	✓
Technology to re-secure hacked SOCs	No	✓
Innovative breakthrough in software CAS client technology	No	✓
Key Escrow allowing operator to switch CAS vendors	No	✓
System designed from the ground up to support Secure SOCs	No	✓
Expensive smart card swaps	$$$	No
Excellent security	✓✓	✓✓✓

Conclusion

The addition of security processing into newer STB chips provides security features beyond that offered by smart-card vendors, without additional chip cost, and without the cost of smart-cards, or the expensive logistics of deploying smart-cards.

SecureTV's deployment of secure STB chips demonstrates the technology leadership offered by the company. The legacy systems offered by SecureTV competitors were designed years ago and do not enhance the security of secure SOCs, rather that they rely on it without enhancing security. SecureTV's innovative approach to security actually enhances the security of Secure SOCs and provides for software recovery methods in the unlikely event the chip is hacked. More details on the benefits of the enhanced security of the Secure TV system will be provided after an NDA is established.

SecureTV's next generation CAS system uses all the advanced security processing features of the secure STB chips, and enhances the secure SOC chip with innovative patent-pending enhanced security features unmatched by competitors.

Key Escrow technology provided by the SecureTV system protects operators from the dirty tricks CAS providers play to prevent operators from switching CAS vendors. This prevents a legacy CAS vendor from locking themselves into a system, something that has happened to many operators globally.

Finally, the SecureTV security philosophy can be summarized in the observation that "anything can be hacked", and SecureTV has leading edge patent-pending software technology to prevent piracy, and to re-secure hacked SOCs, hardware and networks in the unlikely event of a hack.

SecureTV is coupling leading edge security expertise with over 90 years of combined security experience, with advanced silicon security offered by newer STB chips, enhanced by patent-pending innovative security features resulting in the strongest level of security and piracy prevention available.

About Secure TV

Bob Kulakowski is the founder of Secure TV and is a recognized expert in video security. Bob co-founded Verimatrix in 2000 and was the CTO at Verimatrix through 2009. Bob assembled a world-class team of seasoned video and security programmers to develop the Secure TV product. Bob has 11 issued patents in security and technology. In 2016 Secure TV released *UltraCAS 4K* an ultra-secure, ultra-reliable, scalable, CAS system meeting or exceeding the MovieLabs recommendation for Ultra-High Definition 4K/8K content.

SecureTV – *Enhancing Silicon Security*™