

A "WHITE PAPER" ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION

Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system (OSDS™) which does not require the use of a "trusted authority". The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This "White Paper" is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about "information security," it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is "downloadable," security conditions can be changed repeatedly, depending on the use. In other words it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB "dongle") for instance, could securely access multiple video programmers via the Internet, each with it's own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

THE BASICS

The BBTSolution has two parts; a secure microchip in the receiving device, and an "HSM" (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information on the Internet, for instance. HSM's could also be integrated into

devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. While the cost of the HSM enabled equipment will vary depending on the use, the current design for cable television systems costs less than \$10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that basic HSM enabled equipment used on computer servers can be priced significantly lower than that.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a “thumb drive” or “dongle”) that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Micro, are inexpensive (they are currently priced at \$5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known “Dolby™” system is included in most consumer audio devices today.

BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBTSolution is that the receiving device, such as a television set, need not be a “two-way” device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBTSolution device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for “separable security” for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner, and descrambler) that had “integrated security”. That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or “conditional access” systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the “conditional access” components of the system. Unfortunately, CableCARDS are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers

today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, “backward compatible” with CableCARDS. One of the original objectives of BBT was to design a new “separable security” system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman's language used to describe these systems, which was subsequently adopted by the FCC, was “downloadable conditional access systems” or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption /decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A “TRUSTED AUTHORITY”

The traditional approach to establishing a secure communications path is to use a “public/private encryption key” dialog between devices. However this standard approach also requires that the “private key” be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a “trusted authority” holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a “trusted authority,” thus eliminating the two most significant drawbacks of the traditional approach.

With the BBTSolution, the “public/private” keys that enable devices to securely communicate are replaced by a “symmetrical key” approach. Keys are derived internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a “trusted authority” and the risk factor of “hacked” or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the “threat target” for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term “conditional access,” the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include “conditional access” protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus the BBTSolution has been designed in an “open” format where specifications will be made available so that anyone can design “conditional access” software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as rigorous as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB “stick”, which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized “conditional access”

protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be authorized only with thumb print verification as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a “virtual machine” or “tool box” that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12th power combination of encryption/decryption processes. However one can never assume that something simply can never be “broken,” so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a “software-only (DRM--”digital rights management”) approach to encryption or conditional access is subject to constant challenge. As the saying goes, “...there's a new crop of 18-year-old hackers every year!” The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional “DRM” chosen by the information provider, the ability to “download” protocols allows for other flexibility as well. For instance information stored in different formats may require that a “reader” be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a “trusted authority” and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet , in particular, can fundamentally change the way those platforms are used today.