Design of a Location-Based Authentication System for Satellite TV Systems (November 2008)

Christopher Pang, Kevin Uribe and Corry Yang

Abstract **- This document discusses a design of an authentication protocol for satellite television systems to overcome the unauthorized access of copyrighted material. The protocol includes an addition of a location aware module into the already existing security implementations of modern satellite systems. Two cases will be considered: The case when the communication is strictly one-way, receiving end point only receives, and the case when the communication is two-way and the receiving end point can also transmit.**

Index Terms **- Satellite Television, Piracy, Encryption, Location-Based Authentication, Satellite Dish, Artificial Satellites**

I. INTRODUCTION

SATELLITE television providers operate in a multi-billion industry plagued with widespread security issues and signal theft known as pirate decryption. For a long time providers of the satellite television service have come up with expensive anti-pirating operations to try and dissuade pirate businesses dealing in the black market that profit by selling duplicated and hacked smartcards as well as computer-aided emulators used to decrypt unauthorized satellite signals.

It is estimated that pirate decryption within the satellite TV industry costs the providers hundreds of millions of dollars annually. [1] Piracy has such an expensive impact on the industry that service providers have to come up with costly initiatives that work for a limited time only. A major problem is that service providers rely heavily on proprietary security mechanisms that are hidden to the public. A good example is the use of smartcards which now a days can be reprogrammed without any additional hardware apart from a PC, an internet connection and the knowledge of where to download the latest hack. The end user trying to access unauthorized content just needs to get a Satellite dish antenna and the receiver sold at any major electronics store. A smartcard can then be purchased from the black market and the user can either pay someone to reprogram it or do it itself by downloading the right hack.

When Smartcards were introduced, they became an unofficial standard of security for the receiver to decrypt only authorized channels and streams. Hackers at that time analyzed the Smartcard and duplicated the circuitry to create a working clone. The response from the industry was to spend a lot of money in redesigning the smart cards with more layers of hidden security. As expected, pirates became better equipped lured by better profits and continued to reverse engineer anything that the industry designed. Even though piracy through cloning Smartcards did diminish the arms race proved to be so costly for the satellite television industry that new attempts had to be introduced. [2]

Satellite television providers currently employ several countermeasures such as key changes and electronic countermeasure (ECM) attacks to destabilize Smartcards of unauthorized users. ECMs are embedded in the content streams sent from the geostationary artificial satellite in the sky that target non-registered users and erase their Smartcards. For the modern pirate, an ECM attack is an inconvenience that forces them to download the latest hack to reprogram the Smartcard.

Even though technological anti-piracy measures, coupled with the decline in satellite television prices, legal actions taken by the service providers and inconveniences to pirates through ECM attacks help diminish pirate decryption estimates in North America still claim that it costs the industry hundreds of millions of dollars a year. [3] This is why a new approach that does not fall prey to the anti-security principle of security through obscurity is necessary.

Due to the one way nature of an end-user's dish, there is no proper authentication giving weakness to Confidentiality in the CIA principal. In order to achieve mutual authentication, two way communications is necessary which can result with high upgrade costs. Since cost is a major factor in decision making, two designs are proposed:

a. A lower cost one way authentication protocol that only requires the Decryption module.

b. A higher cost two way authentication protocol that may require support from a third party.

There are five main objectives in both designs:

- Minimal Cost
- Simple Design
- Easy installation
- Security
- Reliability

The next section will outline related work in this field and it will be followed by an in depth description of our proposed solution.

II. RELATED WORK

A solution for locking content to a specific region is proposed on the report by Scott and Denning “Location Based Encryption & Its Role in Digital Cinema Distribution” [4]. In this report they argue that adding location layer to an encryption of a onetime media distribution like that of digital cinema can effectively safeguard it against anyone not in the same location. In their solution the encrypting side computes

where the authorized recipient needs to be and XORs the location with a session key to create a GeoLocked session key. The result is then encrypted and sent to the recipient. Only the recipient in the authorized location at a defined time slot can then decrypt the message using the GeoLocked session key.

The GeoLocked solution can be scaled to multiple authorized locations easily, but a limitation is that it is designed as a onetime distribution. On Satellite Television were streams have to be decoded in real time, such a design grants pirates an unbound timeslot to find a way to spoof the location, tamper the device, or brute force the algorithm.

An already existing location aware design is in use in some Direct Broadcast Satellite Systems. Some providers require the authorized user to have the receiver hooked up to a land line so the device can call-back every month the subscription is paid, and only then will the new keys will be released to that particular customer. The location of the originating call is tracked and it prevents the device from being moved.

The attacks on location by land line include: a long range wireless phone, changing address without changing phone number, or with an interference box and a forwarding box. The cost of the last scheme is just under a hundred dollars [5]. Another limitation on this approach is that users without a land line cannot receive the service, and in today's growing cell phone and Voice Over IP market, land lines are slowly disappearing. [6]

III. OUR SOLUTION

The main concept for both designs is to add an additional layer of encryption to the broadcasted signal which can only be decrypted using the Decryption module. The decryption key will also be frequently changed. The encryption method used is up to the TV provider since it is also related to the cost of the module's processor. A One-time pad can even be used due to the frequent changes and short message length which will be seen short.

The decryption module is easily installed by attaching it between the dish and receiver via the traditional RG6 coaxial connectors. In One way authentication, the module is simply a passive device while in Two way authentication, it also acts as a transceiver interfacing the third party.

To decrease the odds of corruption and load on the decryption key broadcasting medium, it is recommended that the message be transmitted within a single packet. The size will vary depending on the medium in which the message is transmitted which in turn can affect the type of encryption used.

{New Kd, Kd_Expiry, MAC}Ks
Where, Kd = Decryption Key
Kd_Expiry = Time of next Kd change
Ks = Symmetric/Session Key
MAC = Message Authentication Code

For flexibility, the length of the message is minimal and contains only necessary components as can be seen above. The use of an expiry to the decryption key is to reduce the processing overhead of the Decryption module.
In One way authentication, decryption of the new key is performed only when it is close to the expiry time; all other messages will be ignored. In Two way authentication, a request for the new key is sent when the expiry time is reached. If a session with the TV provider is not yet established, any messages received by the module will be ignored. The use of selective decryption reduces processing load which in turn increases the reliability of the module.
The main vulnerability of the message is Ks; should it ever be discovered, a hacker is able to acquire all decryption keys. To decreases this possibility, a new Ks is generated after a pre-specified number of Kd has been stored. At this time, all previous Kd will be hashed with the old Ks to form a new Ks allowing Forward Secrecy. Whenever a new Ks is created, all stored Kd are also deleted.

ONE WAY AUTHENTICATION
The basis of this protocol is to have a frequently changing decryption key embedded in the satellite signal. This protocol differs from existing smart card updates in that it is less disruptive and less time consuming. By using a simple encryption/decryption method, the extra layer of encryption can be transparent to the user and will not cause a negative impact on clients.

Discussion
Due to limited satellite bandwidth, single session implementation and one way nature of a dish, it is not possible to devise a true location based decryption scheme. A regional approach can be made by having a different Kd for each satellite the TV provider utilizes. The additional encryption layer can be applied at the transponder level however it may cause a significant change to the broadcasting system with minimal gain. Should multiple decryptions be used, the message will be prepended by a header indicating which satellite/transponder the decryption key is for.
A problem arises with One way authentication regarding Ks updating. If any previous Kd is missed, the new Ks cannot be created. Since messages are only acquired within the Kd expiry time window, an override message is required.

Exception Header, {New Exception Header, New Ks, New Kd, Kd_Expiry, MAC}Ks

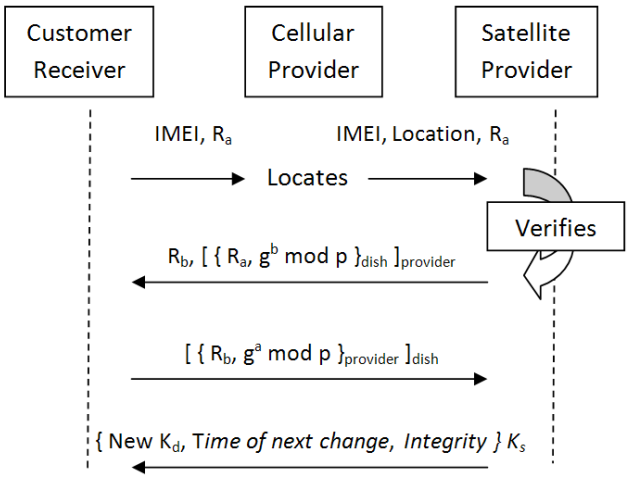
When the Exception Header is detected by the Decryption module, it will decrypt the appended message. This header is to be used once only for security purposes.

TWO WAY AUTHENTICATION
This protocol extends upon the One way authentication concept by adding mutual authentication. The pre-requisite of two way communications can be established via a third party such as a landline, internet or mobile provider. The decryption key is also acquired via this medium. In North America, most TV providers have an affiliation with such a

telecommunications provider which can greatly reduce costs compared to upgrading all clients to a two-way dish.

Discussion

Location authentication is added by sending only the Decryption module ID via the third party provider to the TV provider. Landline providers can acquire using the telephone number (or circuit ID for non-subscribers), internet providers by the IP address and the mobile provider by tower triangulation. Hence, the location of the source is appended to the message by the third party provider adding an additional layer of integrity. Once the TV cross references the ID with the location, mutual authentication and the session key is established via Diffie-Hellman and then the new decryption key is sent. A GPS receiver can also be added to the Decryption Module and coordinates sent along with the device ID to the TV provider for additional cross referencing.



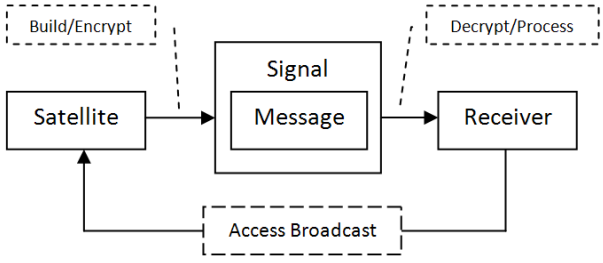
V. DESIGN EVALUATION

In order to help evaluate our design and verify its implementation, a C++ program was written to model message passing under our authentication protocol. The program was meant to provide a simple simulation of interactions between two components: a Satellite and a Receiver. The goal of the Satellite component was to ensure that invalid Receivers (representing satellite pirates) did not gain access to decrypted broadcast signals while the goal of valid Receivers was to be able to decrypt and watch the same broadcast signals. To verify that our solution was successful, we had to ensure that both components were able to achieve their goals at the end of message passing under our designed protocol.

The Satellite and Receiver components were each modelled using a C++ class. Variables such as stored decryption and symmetric keys were kept hidden from external entities through the strict use of private variables within these classes. Furthermore, certain variables such as symmetric keys could only be directly modified during initial instance declarations using the class constructor, and from then on, were only modifiable through randomized generation functions. This helped to ensure that external entities had no way to modify key variables directly. The Satellite class had methods for generating new keys and transmitting update messages using simplified encryption, while the Receiver class had methods for decrypting and processing messages and for attempts at accessing broadcast signals.

Encrypted Message objects were implemented and passed between objects while enclosed in a Signal object which contained information on the signal source. An example of information flow within the program is that the Satellite object would generate a Message, encase it within a Signal which would then be put into a FIFO Queue of Signal objects. Receivers would then pull and process the Signal at the front of the queue to simulate the transport flow of a signal from the satellite to the receiver.

The simulation executed using a loop that where one loop run-throughput represented one time slot of time. At the beginning of the loop, Satellite objects would first generate and issue all the messages they needed to send. The Receiver objects would then each process all messages held in the Queue, until the Queue was emptied. Finally to check whether all objects achieved their goals, Receivers would attempt to access the broadcast signal (encrypted channels). If the Receivers were valid, they should have been able to access the signal, while unauthorized Receivers should not have been able to. In order to check for the second case, fake Receivers instances were implemented without valid keys at the start of the simulation. A simplified diagram of information flow through objects and their methods is shown below.



Through the code implementation, we were able to successfully model for the one-way protocol: the generation and update process for new decryption keys, specified windows where key exchange could occur (for both the receiver and satellite) as well as the routine generation of new symmetric keys based on a hash of previously received decryption keys. The program demonstrated valid message passing between modelled objects, verifying that each object achieved their goals during and at the end of the simulation.

In evaluation our system we looked at various attacks on our design. There are several possible attacks on our proposed one way authentication protocol.

If the pirate decides to attempt a brute force attack on the symmetric key, he would have to do it within the time frame of the next key change making it more complicated. If the pirate wants to brute force to find the exception header then he could send commands to a dish, however he would still need to find the symmetric key to compromise the system.

As with Smartcards, a determined pirate can reverse engineer the IC to extract the symmetric key and compromise the whole system.

There are several possible attacks on our proposed two-way protocol. For instance cellular cloning can be employed which would allow users located close to valid customers to possibly gain authentication to the system. For instance, if an attacker was able to clone a valid receiver's IMEI, they would be able to if they were located close to their victim, authenticate themselves to the system. This type of attack however would only work within close proximities of other valid users, and would be dependent on the accuracy of tower triangulations. Typically, cellular cells have are approximately 26 square kilometres.

If GPS signals are used for additional accuracy over tower triangulation, reducing the location window of each receiver, there is also a threat of GPS spoofing. Because GPS receivers rely on the receipt of signals from GPS satellites to calculate their position, it is possible for attackers to block out actual GPS signals and simulate their own. For instance, attackers could directly feed fake GPS signals into the receiver in order to convince the receiver that it is currently at a different location. Additional attack on a GPS module could also be attempted if the GPS receiver module and the actual satellite receiver module were located in different locations. An attacker could then employ a man-in-the-middle attack through means of breaking the connecting data flow, and inserting their own fake location parameters to fool the satellite receiver into thinking that the location was that of a valid customer.

In evaluating our solution, we also compared the properties of our system's design to the common principles of secure systems design. [7]

Principle	System Properties
Least Privilege	N/A
Fail-Safe Default	If spoofed message is injected, signal cannot be decrypted
Economy of Mechanism	Requires only 'Location' and 'Decryption' mechanisms
Complete Mediation	N/A
Open Design	Open message structure
Separation of Privilege	Depends on provider's internal security
Least Common Mechanism	Distinct mechanism from smartcard security One compromised satellite does not affect entire system
Psychological Acceptability	Ease of installation, module controls all communications
Defense in Depth	Additional encryption layer provided on top of existing system Message encrypted in two-way regardless of communication medium.
Question Assumptions	Evaluated during protocol construction

VI. CONCLUSION

Piracy costs millions of dollars in the Satellite Television Industry and previous attempts to stop it violated the open design principle by trying to keep secret the security measures. There has been research in authentication mechanisms that incorporate "something you are" rather than simply "something you have" so our approach is to add this idea into the satellite television industry.

As long as there is one-way communication as a limitation the solution is at best partially secure because even though a new layer of security is added, the weaknesses can be exploited by a determined pirate without much trouble.

A completely Two-way authentication protocol is therefore recommended because it provides secure authentication. As long as the cost of breaching the protocol is higher than the profit to be made, it should be a powerful deterrence for pirates.

REFERENCES

[1] The New York Times, "In Satellite Piracy War, Battles on Many Fronts", [Online]. Available: http://query.nytimes.com/gst/fullpage.html?res=9A0DE4DF1330F93AA35756C0A9649C8B63#, [Accessed Nov. 30, 2008].

[2] R. Anderson, "Security Engineering A guide to building dependable distributed systems". New York, NY: Wiley, 2001, pp 304-320.

[3] Rocky Mountain News "Dish goes after signal pirates", [Online]. Available: http://www.rockymountainnews.com/news/2008/nov/15/dish-goes-after-signal-pirates/, [Accessed Nov. 30, 2008].

[4]L. Scott and D. E. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution", [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484503&Location=U2&doc=GetTRDoc.pdf, [Accessed Nov. 30, 2008].

[5] Eran Gabber and Avishai Wool, "On Location-Restricted Services", [Online]. Available:

http://www.eng.tau.ac.il/~yash/00806988.pdf, [Accessed Nov. 30, 2008].

[6] G. Cunningham, “Down to the wireless: telephone landlines going the way of the dinosaur”, [Online]. Available: http://www.fosters.com/apps/pbcs.dll/article?AID=/20081110/GJNEWS_01/711109951/0/FOSNEWS, [Accessed Dec. 1, 2008].

[7] M. Stamp, “Information Security - Principles and Practice”. Hoboken, NJ: John Wiley & Sons, 2006, p. 229