Innovative Systems Design and Engineering www.iiste.org
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol 2, No 4, 2011

Enhancement Security in Smart TV Web Application

Manimozhi Iyer
Asst. Prof, CMR Institute of Technology, VTU University
132 AECS Layout, IT Park Road, Bangalore - 560 037, India
Tel: +91-80- 28524477 E-mail: srimanisen@gmail.com

Senthilmurugan Sanmugam,
MVJ College of Engineering, VTU University
Near ITPB, Channasandra, Bangalore-560 067, India
Tel: +91 0 2845 2324 E-mail: ssenthilm@gmail.com

Jitendranath Mungara,
Dean & Prof, CMR Institute of Technology, VTU University
132 AECS Layout, IT Park Road, Bangalore - 560 037, India
Tel: +91-80- 28524477 E-mail: jmungara@yahoo.com

Janakiraman,
Asso.prof, Anna University of Technology
CPT Campus, Tharamani, Chennai 600 113.
Phone: 044 2254 1750 E-mail: drsj3376@gmail.com

Abstract

During the course of its research, the security firmware of the TV's Internet interface failed to confirm script integrity before scripts were run. The attacker could intercept transmissions from the television to the network using common DNS, DHCP server, and TCP session hijacking techniques. The code could then be injected into the normal DataStream, allowing attackers to obtain total control over the device's Internet functionality. This attack could render the product unusable at important times and extend or limit its functionality without the manufacturer's permission. More importantly, however, this same mechanism could be used to extract sensitive credentials from the TV's memory, or prompt the user to fill out fake online forms to capture credit card information.

Additionally, Hackers were able to recover the manufacturer's private "third-party developer keys" from the television, because in many cases, these keys were transmitted unencrypted and "in the clear." Many third-party searches, music, video and photo-sharing services delivered over the Internet require such keys, and a big TV Manufacturer often purchases high-volume "special" access privileges to these service provider's networks. A hacker could potentially employ these keys, for example, to access these high-volume services at no charge. This paper describes the new Authentication mechanism for online transaction payment for more secured service and, analyzing network managed challenge to avoid the vulnerabilities.

Keywords: Smart TV, online payment transaction, Security, and Authentications

1 Introduction

Most people are unaware of one of the more recent developments in interactive Internet connected TV [1]. This new technology brings all the benefits of the Internet and television connected together to create your

own personalized viewing experience. In simple terms Internet connected television means that you can get internet facility straight from your TV with limited features. Internets connected TV can give you access to content online. In most cases, these television sets will give you access to streaming video [2] from select free and paid services as well as providing widgets to give you access to information such as weather reports, stock information, traffic, Account details and so forth. Some also provide access to other sites such as Flickr [3]. They allow controlling all of this with your television remote. Access to YouTube, Amazon on Demand, and Netflix [3] are common, but there are many other providers as well. Providers are added periodically. While there is quite a bit of free content, some of it requires a subscription. Netflix and Amazon on Demand are examples of the paid services. Sony, Samsung, and LG are the leading providers of Internet connected TV models.

Internet connected TV sets don't offer at this time is web browsing capability or e-mail access. There is however one exception. Sony Internet TV now has the Google TV [3], which does indeed provide access to the entire web and provides search functions straight from the remote. But when you are analyzed the economical cost this TV is too much. The videos must always be streamed from the appropriate video server software. The applications are very expensive. Some Internet connected TV sets provide access to select online content, both free and for a fee. The vulnerability was found in the HDTV [3]'s Internet browser that was used to display Web pages on screen. Specifically, a maliciously crafted Script page was found to be able to exploit HDTVs [2] that don't verify script safety before executing the files. Hackers using this technique can intercept transmissions; modify data in transmissions and even trick users into providing credit card numbers or other sensitive information. So this paper proposed this new security mechanism [5] to avoided the vulnerability [8]

1.1 Challenging Managed Network Dynamics

Traditionally, TV operators jockey for position as the household's primary choice for Information and entertainment services. At stake is a significant monthly subscription fee plus the upside of transactional revenue from on-demand and e-commerce services. This marketplace is now being distorted, or some say undermined, by the increasing role of internet services. Static information feeds from the Web today are joined by an ever richer vein of mainstream programming delivered directly from its owners – often for free and with minimal advertising interruptions. While in the past this meant watching low-quality video on a PC monitor, today internet services can be watched on the big screen connected to game consoles, Internet-enabled TVs, and a variety of mobile devices. Online video seems to compete with other online activities and games as much as it does with traditional TV, but the statistics are also distorted by young people's tendency to multi-task, i.e. to watch TV and use an internet servicer simultaneously.

The trends of Internet video consumption in the home and beyond are such that no TV operator can afford to ignore them. Service convergence has become a market driven imperative representing an upside opportunity for service providers to expand revenues and differentiate service offerings. TV operators may still be in the power position since their claim to viewer's attention is as strong, if not stronger, than the new Internet-only players and there is a great incentive to preserve the current operator-subscriber relationship and extend it into the broadband delivery space. Since the technical innovation in broadband TV continues unabated, the prospects are excellent for this aspect of service delivery to meet the new expectations of the market. Whatever the physical delivery channel, the majority of TV technology used today relies on careful management of a shared bandwidth resource – one or more satellite transponders, cable plant bandwidth, terrestrial broadcast spectrum, or an ADSL link. To the extent the finite bandwidth available can be successfully allocated and controlled, the operator can offer a consistent digital service quality, which translates into a satisfying consumer experience. Carefully managing bandwidth has always been part and

parcel of the pay-TV broadcaster's expertise in using RF spectrum. The size of the "pipes" and the constituent linear channel content mix changes relatively slowly, but the same combined signal goes to all receivers. In the world of IPTV delivery, the last mile delivery pipe is typically much more limited in overall bandwidth (unless true fiber-to-the-home is deployed), and hence must be used in a more dynamic fashion. Typically, only the current linear channel or specifically requested video-on-demand (VOD) content stream is delivered over the network connection at any given moment. By using a predictable fixed bitrates for each content type, it is possible to manage the dynamics of this situation to offer a quality of experience comparable to competitive satellite and cable services. Exacting bandwidth management is really only feasible where the connection from head-end to receiver is fully controlled by the TV operator. For satellite services, the pipe up to the "bird" and down to the home, even through coaxial cable, feeds to each receiver, is dedicated to this task, and is quite effective. A similar dedicated network is employed for cable signal distribution, where even sharing the physical wire with high-speed Internet and voice over IP (VoIP) services does not impact the dedicated bandwidth for the television signals. When the consumer expects video to also be available on a home network – to either share recorded content between TVs, or extend services to PCs and other CE devices.TV services have a slightly different problem to solve because the TV service pipe to the home is essentially the same as that used for all other household broadband services. To assure that the Super Bowl picture is not disrupted by ill-timed iTunes downloads, the available bandwidth for TV services is typically reserved and kept completely distinct from that used for feeding PCs and other home broadband devices like TV.

The result is an odd situation: TV services, available in a natural IP format for in-home multi-device distribution and sharing, are essentially kept to preserve overall quality of service (QoS). It also presents conundrums for TV services provisioning in multi-TV households, Tuning to that additional channel on an extra STB may just hit the hard limit of the overall capacity of last mile connection. These are tough problems to solve for the otherwise highly flexible managed network technology behind today's leading TV deployments. Coming from a completely different direction, Internet video delivery has always suffered from unmanaged, multi-hop distribution that forms the backbone of the Web. Video is an exacting type of content, requiring relatively high data rates and very low rates of packet loss or delay. Unstable bandwidth availability results in long startup times, stuttering playback, degraded video quality and unpleasant audio effects.

Effective QoS management over a multi-hop Internet delivery system seems unrealistic. Yet consumers, unaware how these worlds have been independently constructed, demand that content flows freely whenever and wherever they want to consume it. We described to provide the more secured service for improve the QOS management.

1.2 Benefits of internet-enabled TV

Real time applications, such as the weather right before heading to a sporting event, stock exchange, Account balance, family video albums. Depending on the manufacturer, an Internet-enabled television may allow you to stream videos from YouTube, update your Twitter status, check the weather or stream high-definition movies from Netflix. In other words, Web-based TV functions are mostly related to news and entertainment and Social Networking.

2 Problem statements

2.1 Existing systems

Interface fails to confirm the script integrity.

Attacker could render the product unusable at important times and extend or limit its functionality without the manufacturer's permission.

Third party developer's keys transmitted over plaintext. So web applications developers key were leaked which would allow an attacker to perform action against 3rd party website such as you tube, Picasa.

Lack of cryptography could allow an attacker with read only access ability to obtain the sensitive information for example the parental lock on the television contain a bypass/master password to unlock the TV that is supplied by way of code in plain text. So Attackers who sniff the network would be able to retrieve this data and unlock the television.

3 Proposed systems

In this paper we described the following mechanism to avoid the vulnerability between the user and Interactive server. Encryption designed in TV platform through Remote Navigations Adaptive video streaming [6].Authentication mechanism to access services on servers distributed throughout the network [7]

3.1 Encryptions

Encryption protection is possible in network level or Device level. Networks level encryption is achieved by using common networks key. This prevents outsider attacker while adding very little in memory cost. Device level encryption achieved by using unique keys between pair of devices and this preventions insider and outsider attacks but has higher memory cost.

3.2 HTTP live streaming and Bandwidth for video delivery

Adaptive streaming is a process that adjusts the quality of a video delivered to a web page based on changing network conditions to ensure the best possible viewer experience. Internet connection speeds vary widely, and the speed of each type of connection also varies depending on a wide variety of conditions. For example, if a user connects to an ISP at 56 Kbps, that does not mean that 56 Kbps of bandwidth is available at all times. Bandwidth can vary, meaning that a 56-Kbps connection may decrease or increase based on current network conditions, causing video quality to fluctuate as well. Adaptive streaming adjusts the bit rate of the video to adapt to changing network conditions. Adaptive streaming simplifies content creation and management, making streaming video easy to deploy and does not require any coding.

The Technology behind the video delivery service is evolving to keep pace with the new market dynamics. The emerging substitute for managed network delivery of video is the technology of adaptive rate streaming. This technology existed in PC platform. But it's also an example of delivery formats that is particularly suited to STBs, TV, Mobile content delivery and increasing of interest to all connected devices. Adaptive rate streaming eliminates the concepts of network managed QOS in user managed consumer experience. The delivery technology makes use of what the web does the best efficient and massively scalable delivery of data using the HTTP protocol.

From the server point of view, HTTP live streaming media is offered though a single URL reference, in

simultaneous parallel streams that are configured to offer the choice of several different bitrates and aspect ratios. The stream also each segmented into logical time segment or "chunks "where the chunks are synchronized start and end times across the set of components streams. Each user device receiving the service dynamically detects its capability and current network conditions. The HTTP live streaming server can host several different bit rates encoding of the same video content. Each bit rate encoding has a separate playlist, which is defined by master playlist. These playlist should be in M3U formats and contain the list of chunks in order. When the user detects either insufficient bandwidth or more available bandwidth it can switch to the either lower or higher bitrates playlist and download the chunks in the list each chunk is synchronized with each other bit streams, there is a seamless transition between bit rate .so that the video player is not interrupted. This mechanism maintains a high quality user experience even in the face of dynamically adjusting network condition.

Video must always be deployed using video server software. ISP must have the correct video server software or you'll need to pay extra for hosting elsewhere. Network congestion described by the video server software monitors each connection and will automatically switch to a lower bandwidth speed to prevent the video from pausing to re-buffer. The file storage requirements are greater than for individually encoded streams. Web page integration by only a single play button or link is required on the web page. The physical dimensions of the video must remain constant throughout the entire video. Individual speed versions cannot be optimized and made larger to take advantage of higher bandwidth stream versions. The same audio settings must be used for each version to avoid noticeable and unwelcome changes in audio quality as the video server changes which bandwidth version the viewer is watching.

3.3 Authentication mechanism

We described fruitful approaches that have been capable of controlling attack traffic to a major extent. Source authentication is insufficient, given the widespread attack strategies employed by attackers. It is helpful but not a complete solution towards powerful attacks such as DDoS. Any complete solution attacker must give control over resource usage to the owner of the resource. This is because only the destination knows which users are legitimate. Similarly only the network can shed load before it is excessive. There are two necessities to give a good solution to Attackers. Firstly, a destination controlled network filtering is a must. Secondly, authorization needs to be explicit so that it can be checked throughout the network. 'From anyone to anyone paradigm' of the Internet can be overcome with a capability or token based approach towards restricting service that are directed to a particular user. Instead of sending anything to anyone at any time, user must send UID specified by TV manufacturer. The combination of UID and IP encrypted by when it's travelled in the network and Proxy of the GUI server decrypt for authentication. A token is a secret that is generated only for legitimate users maintained by the database of Proxy of the GUI server for temporary one time use. The receiver gives tokens or capabilities to user from which it agrees to accept traffic. The Proxy of the GUI server designed to generate the token with authentication mechanism for more security. This token sends to the user with privilege port number. The recommended proposed system is further supported by the router forwarding packets to the user and target web server. The

intended solution in the router classifies traffic into privileged and unprivileged flows to the user. The router takes the responsibility of forwarding only the packets to the privileged port and hence controls unwanted flow to the server.

This ensures that the service have been certified as legitimate by both endpoints as well as the path in between. This clearly discards unauthorized traffic. When an attacker is underway, routers check to see if the received service has the secret token embedded as part of its IP address. If the verification turns out successful, these services are allowed access to the target internet facility. Thus the service with embedded tokens are given priority over other unprivileged attacker service (user which do not clear the verification of token).These unprivileged service are dropped; the target Internet facility upholds service for the authentic user. Timestamps are issued by the server to avoid stale tokens. Capabilities authorize a legitimate user to establish a privileged communication channel with the server. We proposed the system can be considered as an intelligent system that tries not to completely stop or eliminate service attack but continue providing service to its valid users even in the presence of an attack. The solution strongly supports the idea that a service can be extended to only those users who already establish a trust relationship with the provider of service.

4 Conceptual framework

This generation of authenticated token can be used as a defending mechanism against attackers. A user hosting a service can allow its trusted legitimate users to its privileged service through a privileged port number maintained by the Proxy of the GUI server. A trusted user needs to only give its UID to obtain a privilege internet service for the target web server, and which certifies the user's service privilege by the Proxy of the GUI server. When the target is undergoing an attack and not accessible directly, router in its local network will drop unprivileged packets to protect privileged users' flows. The frame work designed by following steps.

4.1 Privilege Internet service:

A user greater privilege to access its service by assigning to it a secret fictitious called Privilege Internet service with a capability token embedded in part of the IP and port number fields. Through that service, the user can establish a privileged channel with that Proxy of the GUI server even in the presence of flooding attacks. A user may obtain a privilege internet service access directly from the target Proxy of the GUI server. A Proxy of the GUI server offers a privilege Internet service if the user is trusted. A qualified user will get authenticated token which contains the key with IP.

4.2 Protection Mechanism

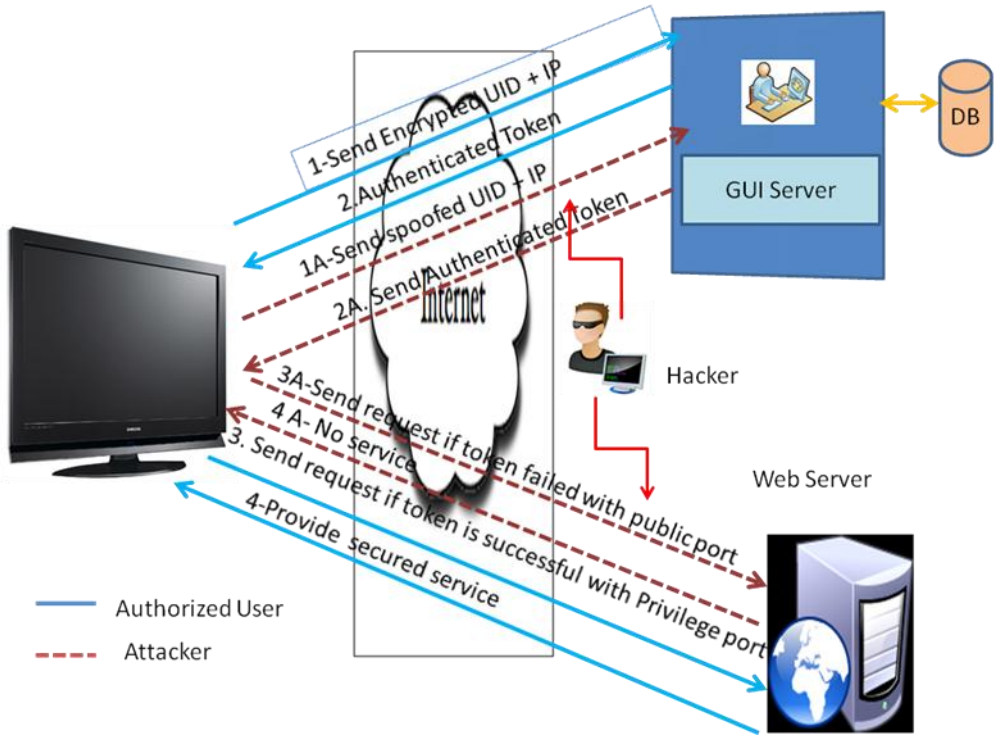
A privilege internet service leads its holder to the target website through a protection mechanism which protects the web server from unauthorized flows. The border of this mechanism is the router, which classify traffic into privileged and unprivileged flows. Within the protection perimeter, router protects privileged traffic by dropping unprivileged packets during congestion. The Proxy of the GUI server generates the authenticated token send to trust user with the target website's privileged service. The http server of the website listens to two ports, one privileged and one not. A local validation system controls access to these ports. Only the port corresponding to the unprivileged traffic, typically port 80, is publicly accessible. The

other specified port as a key [5] can be accessed only by source IP addresses explicitly permitted by the web server. This port is called the privilege port. The user design is based on an architecture that consists of a collection of components which work together to achieve the objective of the protection mechanism in the system.

The Service received on the incoming link is processed by extracting the IP address. The packet processing consists of token extraction and subsequent comparison to validate it. The service is forwarded or rejected depending upon the result of token comparison. A valid service is forwarded to the router with privilege port and an invalid packet is blocked. The management module takes care of the generation of key that is to be secretly exchanged between the proxy GUI server and user. The key generation at regular intervals is also done by management module. The token is the most important component of the system responsible for responsible for building the protection mechanism. The primary functions of the token are receive from proxy of GUI server, check them and forward the privilege port to the web server. The last two octets of a received packet are extracted since it specifies the token of the user. The user computes MAC over the received IP address, compares it with the extracted string. If they are found to be equal, the port is set to the privileged one of the server and then forwarded. In case the token does not match, the service is forwarded to the public port. The user module supports packet processing and packet forwarding by setting appropriate filtering rules to the packets received. The filtering enables router to decide to which port packet should be forwarded. The MAC is computed using the hashing algorithm SHA-1.The authentication key generated is passed by the proxy GUI server to the user.. The time stamp is set for a time period that is feasible for the user to browse the site. If the key expires, the MAC verification fails and the user has to apply for the privileged service again. This communication of the user with the proxy of GUI server is entirely independent of the web server.

4.3 Referral port

The router collects its privilege port from user and sends to the Web Server for which type of service they need. The web server designed by any request from the privilege port must give access of specified Internet applications.



5 Proposed Model Algorithms

ITV_ALGO ()

Initialize the connection (TV_UID, K1, IP)

TV_UID←TV unique no provided by manufacturer
K1← key shared between user &GUI server
IP ←user network address

ENCRYPTIONS (TV_UID, K1, IP) //user

DECRYPTION (TV_UID, K1, IP) // GUI server

M_TV_UID ←Manufacturer M_TV_UID
Do **if** M_TV_UID = TV_UID
then generate authenticated token T (t)
else Reject request service
end

T← COMPUTE TOKEN (T (t)) // GUI server

S← bt || p ||MAC (k (t), IP) //User

do **if** T = S // compute matcher (t, s) in user
then service redirect to privilege port to access the service
else service direct to normal public port
end

COMPUTE TOKEN1 (T (t))

T(t) = bt || p ||MAC (k (t), IP)

T(t) ← valid time of token
P ←priority(optional)
K(t) ←key shared between user ,GUI server, web server
bt ← authentications (optional)
IP ← user network address
end

We proposed token generation for more secured service when we are using the online payment transaction using the internet enabled TV. This second token can use in the high-end configurations model TV.

COMPUTE TOKEN2 (T (t))

T(t) = bt || p ||MAC (k1 || MAC (k_2 (t) || IP)

T(t) ← valid time of token
P ←priority(optional)
K1(t) ←key shared between user ,GUI server, web server
K2(t) ←key shared between user ,GUI server, web server

bt ← authentications (optional)
IP ← user network address
end

6 Privilege Internet service acquisitions

Step 1: user applies for Internet service with UID to the Target Proxy of the GUI server. This application process is as per the manufactures policies.

Step 2: The target Proxy of the GUI server verified with its decrypted UID with IP, and valid referrer's in the database of the server's privilege port.

Step 3: The Proxy of the GUI server generates a capability token for the user T1 (t) = bt || p || MAC (k (t), IP) and T2(t) = bt || p ||MAC (key1 || MAC (k2 (t) || IP)

Where k1 (t) - the key shared between user and target web server.

K2 (t) - the key shared between user and target web server for high end model TV

t - the time period for which the privilege URL remains valid.

bt - one bit key field for authentication (optional)

p - Priority class (optional)

Step 4: The Proxy of the GUI server send the privilege port for communication to the user

Protection Mechanism: A privileged channel is established by the Proxy of the GUI server with newly configured privilege port to protect all privileged user flows during attack.

Step 5: the user receive token from the Proxy of the GUI server

Step 6: the user extracts a string S of length equal to the capability token from every serviced.

Step 7: If S= bt || p ||MAC (k (t), IP) or S =bt || p ||MAC (key1 || MAC (k2 (t) || IP) then - Translate the fictitious destination IP address to the target web server IP address. Set the destination port number of the packet to the privilege port then forward the packet. Else - Reject or forward the packet as an unprivileged packet.

Step 8: Web server provides service based on the privilege port from the user.

7 Conclusions & Future Scope

we proposed an idea of how to protect the internet enabled TV with Adaptive streaming, adjusts the bit rate of the video to adapt to changing network condition and using Authentication mechanism to get permission from the GUI server then authorized can access the internet enabled TV with security. The attacker couldn't intercept transmissions from the television to the network using common DNS, DHCP server, TCP session hijacking techniques using these mechanisms and avoid the vulnerability. The flood attacks are a continuing threat to Internet websites. Such threats could be mitigated through exploring the enormous interlink age relationships among the websites of the Internet. The referral privileged port architecture is constructed upon the existing web site graph. The existing hyperlinks are transformed to privilege port links. The trusted user can get preferential access to a website under a flooding attack. The performance factors of such a referral port have many points in favor. The referral port architecture enables port to evade very intensive flooding attacks, connecting to a website smoothly even when any normal connection becomes infeasible and different token generation for high end model TV. The overheads of this architecture are affordable to routers to find out the privileged port. The privileged port architecture can be used as a simple approach to encourage many small websites to help protect an important website and facilitate the search for referrers during DoS attacks. The privileged port architecture supports only user that use fixed IP addresses. It can be further extended to support dynamic IP addresses, by generating token from the IP prefix rather than the whole IP address. The discovery of referrer websites is not transparent to user in the

built architecture. This can be alleviated if the user ISP itself can act as a referrer in a large scale deployment. This will help the user in not being necessitated to become an authenticated user of the referrer. Studying the performance of the system under the attack with respect to the number of referrals and the time required to receive service can be further researched upon.

8 References

Damien Stolarz(2004), "Mastering Internet Video: A Guide to Streaming and On-Demand Video" Addison-Wesley

J. Chakareski (May 2009.)," Rate- Distortion Optimized Packet Scheduling for Video Streaming: Optimizing Video Delivery in Packet Networks. Saarbr&uumlcken" , Germany: VDM Verlag, 144 pages

Philip j.cianc (2007)," HDTV and Transitions to digital Broadcast" Elsevier

William Stallings (2010)," Network security Essentials Applications and standards" Pearson Editions

XiaoFeng Wang, and Michael .K. Reiter (June 2010)," "Using Web Referral Architecture to mitigate Denial of Service threats" Proc. IEEE transactions on Dependable and Secure Computing.

Jason Garman (2009)," Kerberos: the definitive guide –Network Security.

A. Yaar, A. Perrig, and Song (2004),"An End host Capability Mechanism to Mitigate DDoFlooding Attacks" Proc. IEEE Symp. Security and Privacy(S&P'04).

"Vulnerability Assessment of Internet connected HDTV "(2010), publisher Mocana