DEVELOPING EFFECTIVE CAS FOR MSOs

Digital Addressable Systems (DAS) provide subscribers with a degree of choice and has multiple advantages over the analogue system. DAS environment consists of the Conditional Access System (CAS), which is the cornerstone of transmission system as it is responsible for the encryption of content.

ISSUES RELATED TO SUB-STANDARD CAS & SMS

The Cable Television Networks (Regulation) Act, 1995, the permission/ license to DPOs and the extant regulatory framework lay down requirements to be met by the Addressable Systems. However, broadcasters and distributors regularly raise issues arising out of deployment of sub-standard systems. The issues reported are described herein under three broad heads viz. Security related issues, Operational issues and Support related issues.

SECURITY-RELATED ISSUES:

Transmission of unencrypted signals, unauthorized transmission of signals

This is by far the most recurring issue reported by various broadcasters from various territories. It is also probably the most critical issue as it amounts to theft of content and thereby results in direct loss of revenue to the concerned broadcaster and also to the government. The transmission of unencrypted signals is a clear violation of section 4A of the Cable Television Networks (Regulation) Act, 1995. It enables unauthorized reception of the content and thereby amounts to infringement of provisions of the Indian Copyrights Act, 1957 and constitutes a criminal

एमएसओ के लिए प्रभावी सीएएस विकसित करना

डिजिटल एड्रेसेबल सिस्टम (सीएएस) ग्राहकों को पसंद का विकल्प प्रदान करता है और एनालॉग सिस्टम की तुलना में इसके कई फायदे हैं। डीएएस वातावरण में कंडीशनल एक्सेस सिस्टम (सीएएस) शामिल है जो ट्रांसमिशन सिस्टम की आधारशिला है क्योंकि यह सामग्री के एन्क्रिप्शन के लिए जिम्मेदार है।

सब-स्टैंडर्ड सीएएस और एसएमएस से संबंधित मुद्दे

केबल टेलीविजन नेटवर्क (विनियमन) अधिनियम, 1995, डीपीओ को अनुमति/लाइसेंस और मौजूदा नियामक ढ़ांचा एड्रेसेबल सिस्टम द्वारा पूरी की जाने वाली आवश्यकताओं को निर्धारित करता है। हालांकि, प्रसारक और वितरक नियमित रूप से घटिया प्रणालियों की तैनाती से उत्पन्न होने वाले मुद्दों को उठाते रहे हैं। रिपोर्ट किये गये मुद्दों को यहां तीन व्यापक शीर्षकों के तहत वर्णित किया गया है। सुरक्षा संबंधी मुद्दे, परिचालन संबंधी मुद्दे और समर्थन संबंधी मुद्दे।

सुरक्षा संबंधी मुद्देः

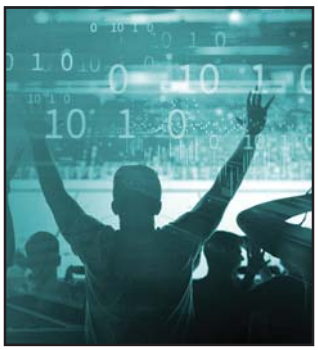
अनएन्क्रिप्टेड सिगनलों का प्रसारण, सिगनलों का अनाधिकृत प्रसारण

यह विभिन्न क्षेत्रों के विभिन्न प्रसारकों द्वारा रिपोर्ट किया गया अब तक का सबसे अधिक सामने आने वाला मुद्दा है। यह शायद सबसे गंभीर मुद्दा भी है क्योंकि यह सामग्री के चोरी के समान है और इसके परिणामस्वरूप संबंधित प्रसारक और सरकार को राजस्व का सीधा नुकसान होता है। अनएन्क्रिप्टेड सिगनलों का प्रसारण केबल टेलीविजन नेटवर्क (विनियमन) अधिनियम 1995 की धारा 4ए का उल्लंघन है। यह सामाग्री के अनधिकृत रिसेप्शन को सक्षम बनाता है और इस तरह भारतीय कॉपीराइट अधिनियम 1957 के प्रावधानों का उल्लंघन है और एक आपराधिक अपराध बनता है। जिसके परिणामस्वरूप अपराधी को गैर-कानूनी लाभ और प्रभावित हितधारकों को हानि होती है।

offence resulting in unlawful gain to the offender and loss to the affected stakeholders.

Finger printing/watermarking not supported by the system

Schedule III of the Interconnection Regulation (Annexure I) has specific provisions for fingerprinting (both visible and covert) and watermarking to be complied by the distribution equipment. This is a critical tool to identify the source of a breach of security if it happens and thereby taking corrective measures such as barring content access by the compromised STBs and blacklisting them, apart from other actions. A timely action is important in minimizing the extent of loss due to piracy, especially in case of time-critical content, such as sports events. Non-compliance of fingerprinting/ watermarking deprives the affected parties of this damage control mechanism.



Cloning of STB:

Even though Schedule III categorically mandates that each STB should be individually addressable, there are reported cases of cloning of STBs, wherein by hacking of secure key of a STB, it was cloned into several STBs while only the hacked STB was reflected in the system. This is another instance of piracy resulting in leakage of revenue.

OPERATIONAL ISSUES:

Integration issues between CAS and SMS

Interconnection Regulations mandate that activation and deactivation of STBs should be done with commands of the SMS and that CAS should not have the facility to activate/deactivate STBs. As such, the SMS and CAS should be in absolute synchronization at all times. However, issues are raised from time to time from field in this regard. It is alleged that in few cases, there may be mirror SMS which, while able to configure subscribers, does not reflect subscribers' information in main subscriber database. This issue has multiple implications. Firstly, it results in improper reporting of subscription figures. As revenue sharing under the regulatory framework is subscription based, this has serious implications. On the other hand, synchronization issue also has implications on service provisioning to

फिंगर प्रिंटिंग/वॉटरमार्किंग, सिस्टम द्वारा समर्थित नहीं है

इंटरकनेक्शन विनियमन (अनुलग्नक 1) की अनुसूची 3 में वितरण उपकरण द्वारा अनुपालन किये जाने वाले फिंगरप्रिंटिंग (दिखने वाले और गुप्त दोनों) और वॉटरमार्किंग के लिए विशिष्ट प्रावधान है। यदि ऐसा होता है तो सुरक्षा के उल्लंघन के स्रोत की पहचान करने के लिए यह एक महत्वपूर्ण उपकरण है और इस तरह अन्य कार्रवाईयों के अलावा, समझौता किये गये एसटीवी द्वारा सामग्री की पहुंच को रोकना और उन्हें ब्लैकलिस्ट करना जैसे सुधारात्मक उपाय किये जाते हैं। पायरेसी के कारण होने वाले नुकसान को कम करने के लिए समय पर कार्रवाई महत्वपूर्ण है, खासकर खेल आयोजनों जैसे समय महत्वपूर्ण सामग्री के मामले में। फिंगर प्रिंटिंग/वॉटरमार्किंग का अनुपालन न करने से प्रभावित पक्ष इस क्षति नियंत्रण तंत्र से वंचित रह जाते हैं।

एसटीवी की क्लोनिंगः

भले ही अनुसूची 3 स्पष्ट रूप से आदेश देती है कि प्रत्येक एसटीवी को व्यक्तिगत रूप से संबोधित किया जाना चाहिए, एसटीवी के क्लोनिंग के मामले सामने आये हैं, एक एसटीवी की 'सिक्योर की' को हैक करके, इसे कई एसटीवी में क्लोन किया गया था, जबकि सिस्टम में केवल हैक किया गया एसअटीवी ही परिलक्षित होता था। यह चोरी का एक और उदाहरण है जिसके परिणामस्वरूप राजस्व का नुकसान हुआ है।

परिचालन के मुद्देः

सीएएस और एसएमएस के बीच एकीकरण मुद्दे

इंटरकनेक्शन विनियमों में कहा गया है कि एसटीवी का सक्रियण और निष्क्रियकरण एसएमएस के आदेशों के साथ किया जाना चाहिए और सीएएस के पास एसटीवी का सक्रिय/निष्क्रिय करने की सुविधा नहीं होनी चाहिए। इस प्रकार एसएमएस व सीएएस हर समय पूर्ण सिंक्रनाइजेशन में होना चाहिए। हालांकि इस संबंध में समय-समय पर क्षेत्र में मुद्दे उठते रहते हैं। यह आरोप लगाया गया कि कुछ मामलों में, मिरर एसएमएस हो सकते हैं जो ग्राहकों को कॉनफिगुर करने में सक्षम हैं, लेकिन मुख्य ग्राहक डेटाबेस में ग्राहकों की जानकारी को प्रतिबिंबित नहीं करते हैं। इस मुद्दे के कई निहितार्थ हैं। सबसे पहले इसके परिणामस्वरूप सब्सक्रीप्शन आंकड़ों की अनुचित रिर्पोटिंग होती है। चूंकि नियामक ढ़ांचे के तहत राजस्व साझाकरण स्ब्सक्रीप्शन पर आधारित है, इसलिए इसके गंभीर निहितार्थ हैं। दूसरी ओर, सिंक्रोनाइजेशन मुद्दे का उपभोक्ता को सेवा प्रावधान पर भी प्रभाव पड़ता है। उदाहरण के लिए इसका परिणाम ऐसी स्थिति में हो

consumer. For example, this may result in a situation where a program has been subscribed to a particular customer/STB but due to integration problem it may not reflect in CAS and the consumer may remain deprived of the service. The converse is also possible wherein a customer may be availing subscription to certain program(s) while the same are not reflected in SMS. This issue can lead to serious discrepancies during bulk activation/deactivation.

Absence of creation / modification logs in the system

Absence of proper, tamper-proof log in the CAS/SMS has serious consequences. The presence of temper proof logs gives the confidence to technical audit team that nothing is being hidden and helps in complete investigations. Absence of temper proof logs raises suspicion of wrong-doing. It provides opportunity to an unscrupulous operator to manipulate subscription data and thereby distort the revenue reports. Another way in which it provides a window for manipulation is through the Access Criteria defined in the CAS. Access criteria controls all the service ids of the channels and decides whether an STB will have access to certain channels or not based upon its entitlement. If the access criteria is disabled then the STB will have complete access to all the channels and this will not reflect in the CAS and SMS reports. In the absence of proper log, there would be no mechanism to check whether the access criteria is manipulated anytime to under report the active subscriber count.

Absence of blacklisting feature in SMS

As described earlier, fingerprinting and watermarking are important tools in identifying the source of piracy and the compromised STBs and taking corrective action by restricting access and blacklisting them. However, there are instances where the SMS does not have the facility to blacklist such compromised STBs, thereby causing irreparable harm.

SUPPORT RELATED ISSUES:

In addition to the security related and operational threats as summarized above, there are instances of complaints raised by MSOs regarding support-related issues from CAS/SMS vendors. Specifically, such complaints either pertain to delay or lack of support in relation to needed software modification in the system in compliance to a

सकता है जहां किसी प्रोग्राम को किसी विशेष ग्राहक/एसटीबी के लिए सब्सक्राइब किया गया है, लेकिन एकीकरण समस्या के कारण यह सीएएस में प्रतिबिंबित नहीं हो सकता है और उपभोक्ता सेवा से वंचित रह सकता है। इसका विपरित भी संभव है जिसमें एक ग्राहक कुछ कार्यक्रमों की सदस्यता का लाभ उठा राह हो, लेकिन यह एसएमएस में प्रतिबिंबित नहीं होता है। यह समस्या थोक सक्रियण/निष्क्रियण के दौरान गंभीर विसंगतियों का कारण बन सकती है।

सिस्टम में निर्माण/संशोधन लॉग का अभाव

सीएएस/एसएमएस में उचित, छेड़छाड़-रोधी लॉग के अभाव के गंभीर परिणाम होते हैं। तापमान प्रुफ लॉग की उपस्थिति तकनीकी ऑडिट टीम को यह विश्वास दिलाती है कि कुछ भी छिपाया नहीं जा रहा है और पूरी जांच में मदद मिलती है। तापमान प्रुफ लॉग की अनुपस्थिति गलत काम करने का संदेह पैदा करती है। यह एक बेईमान ऑपरेटर को सब्सक्रीप्शन डेटा में हेरफेर करने और इस तरह राजस्व रिपोर्ट को विकृत करने का अवसर प्रदान करता है। एक अन्य तरीका जिसमें यह हेरफेर करने के लिए विंडो प्रदान करता है वह सीएएस में परिभाषित एक्सेस मानदंड के माध्यम से है। एक्सेस मानदंड चैनलों की सभी सेवा आईडी को नियंत्रित करता है और यह तय करता है कि एसटीबी को उसकी पात्रता के आधार पर कुछ चैनलों तक पहुंच प्राप्त होगी या नहीं। यदि पहुंच मानदंड अक्षम है तो एसटीबी के पास सभी चैनलों तक पूर्ण पहुंच होगी और यह सीएएस व एसएमएस रिपोर्ट में प्रतिबिंबित नहीं होगा। उचित लॉग के अभाव में यह जांचने के लिए कोई तंत्र नहीं होगा कि सक्रिय ग्राहक संख्या को कम रिपोर्ट करने के लिए एक्सेस मानदंड में कभी भी हेरफेर किया गया है या नहीं।

एसएमएस में ब्लैकलिस्टिंग सुविधा का अभाव

जैसाकि पहले बताया गया है कि फींगरप्रिंटिंग और वॉटरमार्किंग चोरी के स्रोत और समझौता किये गये एसटीबी की पहचान करने और पहुंच को प्रतिबंधित करके और उन्हें ब्लैकलिस्ट करके सुधारात्मक कार्रवाई करने में महत्वपूर्ण उपकरण हैं। हालांकि, ऐसे उदाहरण हैं जहां एसएमएस के पास ऐसे समझौते किये गये एसटीबी को ब्लैकलिस्ट करने की सुविधा नहीं है जिससे अपूरणीय क्षति होती है।

सपोर्ट संबंधी मुद्देः

जैसाकि ऊपर संक्षेप में बताया गया है कि सुरक्षा संबंधी और परिचालन संबंधी खतरों के अलावा सीएएस/एसएमएस विक्रेताओं से समर्थन संबंधी मुद्दों के संबंध में एमएसओ द्वारा की गयी शिकायतों के उदाहरण हैं। विशेष रूप से ऐसी शिकायतें या तो लाइसेंस या नियामक आवश्यकता के अनुपालन में सिस्टम में आवश्यक

license or regulatory requirement. Pursuant to coming into effect of the new regulatory framework, there have been cases, where a DPO could not implement the new billing regime timely. Not only the DPO faced regulatory actions, it also incurred losses in terms of higher pay-out to broadcasters as well-as the consumers, as it failed to activate channels as per consumer choice(s). There have been reports where the vendor sought exorbitant charges for a modification or an upgrade as the DPO became a captive customer.

CHALLENGES ASSOCIATED WITH SUB-STANDARD SYSTEMS:

Analysis of the reported issues as summarized above reveals there are primarily two ways in which these issues can be manifested. One is due to deployment of sub-standard systems (CAS/SMS) in the field and the other is due to fraudulent operation of the systems. As far as fraudulent operation of the systems with a malicious intent is concerned, inspections and operational oversight mechanism can probably be the only effective way to curb the menace with relevant technical support and audit trail. However, creating a framework that prevents deployment of sub-standard systems in the network can be expected to bring a preventive control as far as potential threats arising due to vulnerability of such systems to hacking is concerned. Further, it may also be argued that support related issues can perhaps be addressed more effectively through suitable policy framework. Few of the ways in which sub-standard systems put the eco-system to risk are described below:

No protection against Control Word (CW) Sharing

CW is not sent in an encrypted format in the Entitlement Control Message (ECM) in substandard CASs. It is possible to get the CW by snooping methods. If CW is not protected, then it would allow the Local Cable Operator (LCO)/ Hacker/to redistribute the signals without the knowledge of the Operator/Broadcaster and get profited from it.

Weak encryption of Entitlement Control Message (ECM) and Entitlement Management Message (EMM)

ECM and EMM are not encrypted in sub-standard CAS. It does not have mechanism for Custom EMM generation and handling. If ECM/EMM are not protected, then it would allow the hackers to redistribute the signals unlawfully.

सॉफ्टवेयर संशोधन के संबंध में देरी या समर्थन की कमी से संबंधित है। नये नियामक ढ़ांचे के प्रभाव में आने के बाद ऐसे मामले सामने आये हैं जहां एक डीपीओ नयी बिलिंग व्यवस्था को समय पर लागू नहीं कर सका। न केवल डीपीओ को नियामक कार्रवाई का सामना करना पड़ा, बल्कि प्रसारकों के साथ-साथ उपभोक्ताओं को भी उच्च भुगतान के मामले में नुकसान उठाना पड़ा, क्योंकि यह उपभोक्ता की पसंद के अनुसार चैनल सक्रिय करने में विफल रहा। ऐसी रिपोर्ट आयी हैं जहां डीपीओ के कैप्टिव ग्राहक बन जाने पर विक्रेता ने संशोधन या अपग्रेड के लिए अत्यधिक शुल्क की मांग की।

उप-मानक प्रणालियों से जुड़ी चुनौतियां

जैसाकि ऊपर संक्षेप में बताया गया है कि रिपोर्ट किये गये मुद्दों के विश्लेषण से पता चलता है कि मुख्य रूप से दो तरीके हैं जिनमें ये मुद्दे प्रकट हो सकते हैं। एक क्षेत्र में घटिया सिस्टम (सीएएस/एसएमएस) की तैनाती के कारण हैं और दूसरा सिस्टम के फर्जी संचालन के कारण है। जहांतक दुर्भावनापूर्ण इरादे से सिस्टम के धोखाधड़ीपूर्ण संचालन का सवाल है, प्रासंगिक तकनीकी सहायता और ऑडिट ट्रेल के साथ इस खतरे को रोकने के लिए निरीक्षण और परिचालन निरीक्षण तंत्र संभवतः एकमात्र प्रभावी तरीका हो सकता है। हालांकि नेटवर्क में उप-मानक प्रणालियों की तैनाती को रोकने वाला एक ढ़ांचा बनाने से हैकिंग के प्रति ऐसी प्रणालियों की भेद्यता के कारण उत्पन्न होने वाले संभावित खतरों के संबंध में निवारक नियंत्रण लाने की उम्मीद की जा सकती है। इसके अलावा यह भी तर्क दिया जा सकता है कि समर्थन संबंधी मुद्दों को शायद उपयुक्त नीति ढ़ांचे के माध्यम से अधिक प्रभावी ढ़ंग से संबोधित किया जा सकता है। कुछ तरीके जिनमें उप-प्रणालियां पारिस्थितिकी तंत्र को खतरे में डालती हैं, उनका वर्णन नीचे किया जा रहा हैः

कंट्रोल वर्ड (सीडब्लू) शेयरिंग के खिलाफ कोई सुरक्षा नहीं

घटिया सीएएस में एंटाइटेलमेंट कंट्रोल मैसेज (ईसीएम) में सीडब्लू को एन्क्रिप्टेड प्रारूप में नहीं भेजा जाता है। जासूसी विधियों द्वारा सीडब्लू प्राप्त करना संभव है। यदि सीडब्लू संरक्षित नहीं है तो यह स्थानीय केबल ऑपरेटर (एलसीओ)/हैकर/सह-ऑपरेटर/प्रसारक की जानकारी के बिना सिगनल को फिर से वितरित करने और इसका लाभ उठाने की अनुमति देगा।

एंटाइटेलमेंट कंट्रोल मैसेज (ईसीएम) और एंटाइटेलमेंट मैनेजमेंट मैसेज (ईएमएम) का कमजोर एन्क्रिप्शन

ईसीएम और ईएमएम घटिया सीएएस में एन्क्रिप्टेड नहीं है। इसमें कस्टम ईएमएम जेनरेशन और हैंडलिंग के लिए तंत्र नहीं है। यदि ईसीएम/ईएमएम संरक्षित नहीं है तो यह हैकर्स को गैरकानूनी तरीके से सिगनल को फिर से वितरित करने की अनुमति देगा।

Unsecure Boot Loader

Sub-standard CAS does not have secure boot loader and hence it allows non-authenticated software to boot up the STB. Further it allows malicious software to be downloaded in an STB. Non-Secure Boot Loader can put investment of the operator on the STB at risk because if a malicious software is running on the STB it can make the boxes to behave abnormally and can even make STBs in operation to stop working completely, making the operator to re-invest in buying all the boxes once again. Several complaints have been received from operators alleging malpractices by such substandard CASs, owing to which support issues are faced by the concerned MSOs.

Non-secure Boot Loader can also result in releasing the control word which would allow the end user to redistribute the signals without the knowledge of the Operator/Broadcaster.

Poor Support for Detection of Security Breach

It has been mentioned in Chapter 1 that CASs deployed have varying level of security robustness against piracy, varying from Advanced embedded type to non-advanced. CASs with non-advanced security are obviously more vulnerable to piracy. Fingerprinting/watermarking mechanisms do provide a mechanism to block access of content to compromised devices/ network in case of a security breach. However, sub-standard CASs may not even have fingerprinting mechanisms. Owing to these factors content can be pirated and redistributed on various online as well as offline modes mechanisms without the knowledge of the operator or the broadcaster.

Blacklisting of STBs

Sub-standard CASs allow compromised STBs to continue to run in the network, as they do not have a provision for blacklisting of smart cards or ID's of the STBs, thereby allowing content piracy to continue without the knowledge of the operator or the broadcaster.

Issues with CAS Server Hardware

Sub-standard CAS are not deployed on head-end server hardware specifically supplied by CAS provider and it is possible to deploy sub-standard CAS in just any

असुरक्षित बूट लोडर

उप–मानक सीएएस में सुरक्षित बूट लोडर नहीं है और इसलिए यह गैर–प्रमाणित सॉफ्टवेयर को एसटीबी को बूट करने की अनुमति देता है। इसके अलावा यह दुर्भावनापूर्ण सॉफ्टवेयर को एसटीबी में डाउनलोड करने की अनुमति देता है। गैर–सुरक्षित बूट लोडर एसटीबी पर ऑपरेटर के निवेश को खतरे में डाल सकता है क्योंकि यदि एसटीबी पर कोई दुर्भावनापूर्ण सॉफ्टवेयर चल रहा है तो यह बॉक्स को आसामान्य रूप से व्यवहार करने के लिए मजबूर कर सकता है और यहां तक कि एसटीबी पूरी तरह से काम करना बंद कर सकता है, जिससे ऑपरेटर को एक बार फिर से सभी बॉक्स खरीदने में निवेश करने के लिए मजबूर होना पड़ सकता है। ऐसे घटिया सीएएस द्वारा कदाचार का आरोप लगाने वाले ऑपरेटरों से कई शिकायत प्राप्त हुई हैं जिसके कारण संबंधित एमएसओ को समर्थन संबंधी समस्याओं का सामना करना पड़ता है।

गैर सुरक्षित बूट लोडर के परिणामस्वरूप नियंत्रण शब्द भी जारी हो सकता है जो अंतिम उपयोगकर्ताओं को ऑपरेटर/प्रसारकों की जानकारी के बिना सिग्नल को फिर से वितरित करने की अनुमति देगा।

सुरक्षा उल्लंघन का पता लगाने के लिए खराब सपोर्ट

अध्याय 1 में उल्लेख किया गया है कि लगे सीएएस में चोरी के खिलाफ सुरक्षा मजबूती का स्तर अलग–अलग है, जो आधुनिक एंबेडेड प्रकार से लेकर गैर आधुनिक तक भिन्न है। गैर–आधुनिक सुरक्षा वाले सीएएस स्पष्ट रूप से चोरी के प्रति अधिक संवेदनशील होते हैं। फिंगरप्रिंटिंग/वाटरमार्किंग तंत्र सुरक्षा उल्लंघन के मामले में समझौते किये गये उपकरण/नेटवर्क तक सामग्री की पहुंच को अवरूद्ध करने के लिए एक तंत्र प्रदान करते हैं। हालांकि उप मानक सीएएस में फींगरप्रिंटिंग तंत्र भी नहीं हो सकता है। इन कारकों के कारण सामग्री को ऑपरेटर या प्रसारकों की जानकारी के बिना विभिन्न ऑनलाइन और ऑफलाइन मॉड तंत्रों पर पायरेटेड और पुनर्वितरित किया जा सकता है।

एसटीबी को ब्लैकलिस्ट में डालना

उप–मानक सीएएस, समझौता किये गये एटीबी को नेटवर्क में चलते रहने की अनुमति देते हैं, क्योंकि उनके पास स्मार्ट कार्ड या एसटीबी की आईडी को ब्लैकलिस्ट करने का प्रावधान नहीं है, जिससे ऑपरेटर या प्रसारक की जानकारी के बिना सामाग्री चोरी जारी रखने की अनुमति मिलती है।

सीएएस सर्वर हार्डवेयर से संबंधित समस्यायें

उप–मानक सीएएस को सीएएस प्रदाता द्वारा विशेष रूप से आपूर्ति किये गये हेडएंड सर्वर हार्डवेयर पर तैनात नहीं किया जाता है और किसी भी व्यावसायिक रूप से

commercially available generic servers thereby removing any extra layer of data/cyber security and increasing the probability of any backdoors and malicious software deployments.

Integration Issues with the SMS

Sub-standard CAS normally has integration issues with the SMS. Such CAS does not have consistency in term of integration and is not able to accept/recognize commands from SMS on regular basis or during bulk activation/deactivation. Any activation/deactivation command or any other command sent from SMS can be rejected or not accepted by CAS. This will result into reconciliation issues between CAS and SMS because the same STB can be found in active state in CAS whereas in SMS it will be showing inactive or vice versa.

Auto Expiry and Disentitlement of Services

In sub-standard CAS the Set Top Box (STB) does not get disentitled to the services automatically on the expiry date set at the beginning of the subscription period and needs a command from the Subscriber Management System (SMS) to get disentitled. Therefore, substandard CASs increases the traffic of the SMS commands to send entitlement and de-entitlement commands every month for every customer. It results in significant bandwidth consumption if the network has few thousand customers and few hundred services and packages to subscribe.

Issues with Addressability

In sub-standard CAS the EMM addressability in individuals/groups/ region/global/LCO is not achievable. The definition of the groups may not be based on rules definitions such as geographic locations based on pin code, city, etc. Consequently, the operator and broadcaster lose the control on the field network and its STBs.

Generation of CAS Reports & data bases in editable formats

Sub-standard CAS/SMS deployment results into increasing the probability of misreporting the usage and subscription numbers, as it also generates CAS reports in editable Formats such as csv, excel. It generates logs which are accessible by any user or operator for manipulation and/or modification. This may result into revenue loss to the operator, broadcaster as well as to the government in form of taxes. Further, the Sub-standard CASs do not have an option to back up all the critical data as per the configuration.

उपलब्ध जेनेरिक सर्वर में उप–मानक सीएएस को तैनात करना संभव है, जिससे डेटा/साइबर सुरक्षा की कोई भी अतिरिक्त परत हट जायेगी और किसी भी पिछले दरवाजे और दुर्भावनापूर्ण सॉफ्टवेयर परिनियोजन की संभावना बढ़ रही है।

एसएमएस के साथ एकीकरण मुद्दे

उप–मानक सीएएस में आमतौर एसएमएस के साथ एकीकरण संबंधी समस्यायें होती हैं। ऐसे सीएएस में एकीकरण की अवधि में स्थिरता नहीं होती है और यह नियमित आधार पर या थोक सक्रियण/निष्क्रियण के दौरान एसएमएस के आदेशों को स्वीकार/पहचानने में सक्षम नहीं होता है। किसी भी सक्रियण/निष्क्रिय आदेश या एसएमएस से भेजे गये किसी अन्य आदेश को सीएएस द्वारा अस्वीकार या स्वीकार नहीं किया जा सकता है। इसके परिणामस्वरूप सीएएस और एसएमएस के बीच सामंजस्य संबंधी समस्यायें उत्पन्न होगी क्योंकि सीएएस में वही एसटीबी सक्रिय अवस्था में पाया जा सकता है जबकि एसएमएस में यह निष्क्रिय या इसके विपरीत दिखायी देगा।

सेवाओं की स्वतः समाप्ति और अपात्रता

उप–मानक सीएएस में सेट टॉप बॉक्स (एसटीबी) सदस्यता अवधि की शुरूआत में निर्धारित समाप्ति तिथि पर स्वतः रूप से सेवाओं से वंचित नहीं होता है और हकदारी से वंचित होने के लिए सब्सक्राइबर मैनेजमेंट सिस्टम (एसएमएस) से एक कमांड की आवश्यकता होती है। इसलिए घटिया सीएएस प्रत्येक ग्राहक के लिए हर महीने एंटाइटेलमेंट और डी–एंटाइटेलमेंट कमांड भेजने के लिए एसएमएस कमांड का ट्रैफिक बढ़ाता है। यदि नेटवर्क में कुछ हजार ग्राहक और सब्सक्राइबर के लिए कुछ सौ सेवायें और पैकेज हैं तो इसके परिणामस्वरूप महत्वपूर्ण बैंडविड्थ खपत होती है।

एड्रेसेबिलिटी से संबंधित मुद्दे

उप–मानक सीएएस में व्यक्तियों/समूहों/क्षेत्र/वैश्विक/एलसीओ में ईएमएम एड्रेसेबिलिटी उपलब्ध नहीं है। समूहों की परिभाषा नियमों की परिभाषा पर आधारित नहीं हो सकती है, जैसे कि पिन कोड, शहर आदि पर आधारित भौगोलिक स्थान। नतीजतन ऑपरेटर और प्रसारक फील्ड नेटवर्क और उसके एसटीबी पर नियंत्रण खो देते हैं।

संपादनयोग्य प्रारूपों में सीएएस रिपोर्ट और डेटा बेस तैयार करना

उप–मानक सीएएस/एसएमएस परिनियोजन के परिणामस्वरूप उपयोग और सदस्यता संख्याओं की गलत रिर्पोटिंग की संभावना बढ़ जाती है, क्योंकि यह सीएसवी, एक्सेल जैसे संपादन योग्य प्रारूपों में सीएएस रिपोर्ट भी उत्पन्न करता है। यह लॉग उत्पन्न करता है जो किसी भी उपयोगकर्ता या ऑपरेटर द्वारा हेरफेर और/या संशोधन के लिए पहुंच योग्य है। इससे ऑपरेटर, प्रसारकों के साथ–साथ सरकार को करों के रूप में राजस्व हानि हो सकती है। इसके अलावा, उप–मानक सीएएस में कॉनफिगुरेशन के अनुसार सभी महत्वपूर्ण डेटा का बैकअप लेने का विकल्प नहीं होता है।

By Mails / Alerts

Sub-standard CAS makes it difficult to send message to end user which may be critical to continue the service or inform the end user of some life-threatening disaster/calamity etc.

A comparison of the standard and sub-standard CASs on the lines of major areas of concern is provided at Annexure II, indicating associated risk factors and their threat level.

IMPLICATIONS AND POSSIBLE THREATS FROM DEPLOYMENT OF SUB-STANDARD CAS / SMS

The issues reported from time to time indicate that a lot of proprietary solutions have made way into the Indian market offering cheap security. Because of this, different stakeholders in the ecosystem suffer, not just the end consumer, but also the service providers and the Government.

Impact on the Consumer

Sub-standard CAS increases the workload of the operator and creates a confusion among the end consumers who may get non-uniform services from the same operator. It may result in frequent disruptions and hence poor Quality of Service (QoS) for the end consumer.

The consumers get locked in with STBs with limited functionality because of sub-standard proprietary software, which in turn results into the wastage of money for the end consumer as they may have to replace the STB many times during the subscription period.

Impact on the Broadcaster

Broadcasters and content developers are impacted directly by deployment of sub-standard CAS/SMS, as security of their content is compromised. It leads to content piracy and redistribution without the knowledge and permission of the broadcaster and the operator.

Further, certain features such as LCN etc. can't be implemented seamlessly across all STBs in a network owing to sub-standard proprietary software. Sub-Standard CAS/ SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the broadcaster and disputes with the operators in cases of under/excess billing.

Frequent disruption of services results into creating a lot of issues on the ground as the revenue collection is disrupted. It may attract lawsuits against the operators which may have the potential to disrupt their entire business operations

मेल/अलर्ट

उप–मानक सीएएस अंतिम उपयोगकर्ताओं को संदेश भेजना कठिन बना देता है जो सेवा जारी रखने या अंतिम उपयोगकर्ताओं को किसी जीवन घातक आपदा/घटनाओं आदि के बारे में सूचित करने के लिए महत्वपूर्ण हो सकता है।

चिंता के प्रमुख क्षेत्रों के तर्ज पर मानक और उप–मानक सीएएस की तुलना अनुबंध **2** में प्रदान की गयी है जो संबंधित जोखिम कारकों और उनके खतरे के स्तर को दर्शाती है।

घटिया सीएएस/एसएमएस की तैनाती से निहितार्थ और संभावित खतरे

समय–समय पर रिपोर्ट किये गये मुद्दों से संकेत मिलता है कि सस्ती सुरक्षा की पेशकश करने वाले कई मालिकाना समाधान भारतीय बाजार में आ गये हैं। इसके कारण पारिस्थितिकी तंत्र में विभिन्न हितधारकों को नुकसान होता है, न केवल अंतिम उपभोक्ता बल्कि सेवा प्रदाता और सरकार भी।

उपभोक्ता पर प्रभाव

उप–मानक सीएएस ऑपरेटरों के कार्यभार को बढ़ाता है और अंतिम उपभोक्ताओं के बीच भ्रम पैदा करता है जिन्हें एक ही ऑपरेटर से गैर–समान सेवायें मिल सकती हैं। इसके परिणामस्वरूप बार–बार व्यवधान हो सकता है और अंतिम उपभोक्ता के लिए सेवा की गुणवत्ता (क्यूओएस) खराब हो सकती है।

उप–मानक मालिकाना सॉफ्टवेयर के कारण उपभोक्ता सीमित कार्यक्षमता वाले एसटीबी में फंस जाते हैं जिसके परिणामस्वरूप अंतिम उपभोक्ता के लिए पैसे की बर्बादी होती है क्योंकि उन्हें सदस्यता अवधि के दौरान कई बार एसटीबी को बदलना पड़ सकता है।

प्रसारक पर प्रभाव

घटिया सीएएस/एसएमएस की तैनाती से प्रसारकों और कंटेंट बनाने वाले सीधे प्रभावित होते हैं, क्योंकि उनकी सामग्री की सुरक्षा से समझौता किया जाता है। यह प्रसारक और ऑपरेटर की जानकारी और अनुमति के बिना सामग्री की चोरी और पुनर्वितरण की ओर ले जाता है। इसके अलावा कुछ सुविधायें जैसे एलसीएन आदि को घटिया मालिकाना सॉफ्टवेयर के कारण नेटवर्क के सभी एसटीबी में निर्बाध रूप से लागू नहीं किया जा सकता है।

उप–मानक सीएएस/एसएमएस परिनियोजन के परिणामस्वरूप उपयोग और सदस्यता संख्याओं की गलत रिपोर्टिंग की संभावना बढ़ जाती है जिसके परिणामस्वरूप प्रसारक को राजस्व हानि हो सकती है और कम/अतिरिक्त बिलिंग के मामलों में ऑपरेटरों के साथ विवाद हो सकता है।

सेवाओं में बार–बार व्यवधान के परिणामस्वरूप राजस्व संग्रह बाधित होने से जमीनी स्तर पर कई समयायें पैदा होती हैं। इससे ऑपरेटरों के खिलाफ मुकदमें दायर हो सकते हैं जिससे उनके संपूर्ण व्यवसाय संचालन को बाधित करने की संभावना हो सकती है।

Impact on MSO / DPO / Pay TV Distributor

Since majority of the CAS companies do not have their own SMS, Middleware (MW) and User Interface (UI), it increases the dependency of the MSOs on several Third party (TP) software solution providers. Since most of the MSOs lack in technical expertise as they have migrated from Analog Cable TV regime, they fall prey to sub-standard solutions and face support issues subsequently.

MSOs get locked down to only one kind of boxes/ STB original equipment manufacturer (OEM) with non-standard implementation of middleware features and incur high maintenance overhead to maintain and execute such proprietary software. It increases their operational cost as technical issues arise. Their flexibility to extend features is reduced.

Additionally, it creates tension with broadcasters, as there is a potential to manipulate the readings and log numbers which may result into misrepresentation of the data and may affect the revenue for all parties concerned due to excess/under billing.

Since deployment of a substandard proprietary software can result into content leakage and piracy, it may lead to various legal and commercial actions by the content owner and hence disrupt the complete operations of the MSOs.

Further, in absence of Hardware Specifications and Performance Parameter standards, MSO may keep on investing into poor/cheap quality hardware which results into wastage of time, the generation of a lot of e-waste, resource wastages in terms of financial resources, human resources as well as management resources.

Impact on the Government

Sub-standard CASs defeat the very purpose of the Government of India's DAS (Digital Addressable System) initiative. Sub-standard CAS/ SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the operator, broadcaster as well as to the government in form of taxes.

Further, CASs which follow accepted global standards can be useful when changes from middleware perspective, such as STB Interoperability are implemented by the government. ■

सत्यमेव जयते

Ministry of Information & Broadcasting
Government of India

एमएसओ/डीपीओ/पे टीवी वितरक पर प्रभाव

चूंकि अधिकांश सीएएस कंपनियों के पास अपना स्वयं का एसएमएस, मिडलवेयर (एमडब्लू) और यूजर इंटरफेस (यूआई) नहीं है इससे कई तीसरे पक्ष (टीपी) सॉफ्टवेयर समाधान प्रदाताओं पर एमएसओ की निर्भरता बढ़ जाती है। चूंकि अधिकांश एमएसओ में तकनीकी विशेषज्ञता की कमी है क्योंकि वे एनालॉग टीवी व्यवस्था से चले गये हैं, वे घटिया समाधानों के शिकार हो जाते हैं और बाद में समर्थन समस्याओं का सामना करते हैं।

मिडलवेयर सुविधाओं के गैर-मानक कार्यान्वयन के साथ एमएसओ केवल एक प्रकार के बक्से/एसटीबी मूल उपकरण निर्माता (ओईएम) तक सीमित हो जाते हैं और ऐसे मालिकाना सॉफ्टवेयर को बनाये रखने और निष्पादित करने के लिए उच्च रखरखाव ओवरहेड खर्च करते हैं। तकनीकी समस्यायें उत्पन्न होने पर इससे उनकी परिचालन लागत बढ़ जाती है। सुविधाओं का विस्तार करने का उनका लचीलापन कम हो गया है।

इसके अतिरिक्त, यह प्रसारकों के साथ तनाव पैदा करता है, क्योंकि रीडिंग और लॉग नंबरों में हेरफेर करने की संभावना है जिसके परिणामस्वरूप डेटा की गलत प्रस्तुति हो सकती है और अधिक/कम बिलिंग के कारण संबंधित सभी पक्षों के राजस्व पर असर पड़ सकता है।

चूंकि घटिया स्वामित्व वाले सॉफ्टवेयर की तैनाती के परिणामस्वरूप सामग्री रिसाव और चोरी हो सकती है, इससे सामग्री स्वामी द्वारा विभिन्न कानूनी और वाणिज्यिक कार्रवाइयां हो सकती हैं और इस प्रकार एमएसओ के संपूर्ण संचालन में बाधा उत्पन्न हो सकती है।

इसके अलावा हार्डवेयर विशिष्टताओं और प्रदर्शन पैरामीटर मानकों के अभाव में, एमएसओ खराब/सस्ते गुणवत्ता वाले हार्डवेयर में निवेश करना जारी रख सकता है जिसके परिणामस्वरूप समय की बर्बादी होती है, बहुत सारे ई-कचरे का उत्पादन होता है, वित्तीय संसाधनों, मानव संसाधनों के साथ-साथ प्रबंधन संसाधनों की बर्बादी होती है।

सरकार पर प्रभाव

घटिया सीएएस भारत सरकार की डीएएस (डिजिटल एड्रेसेबल सिस्टम) पहल के उद्देश्य को ही विफल कर देते हैं। उप-मानक सीएएस/एसएमएस परिनियोजन के परिणामस्वरूप उपयोग और सदस्यता संख्याओं की गलत रिपोर्टिंग की संभावना बढ़ जाती है जिसके परिणामस्वरूप ऑपरेटर, प्रसारक के साथ-साथ सरकार को करों के रूप में राजस्व की हानि हो सकती है।

इसके अलावा, स्वीकृत वैश्विक मानकों का पालन करने वाले सीएएस तब उपयोगी हो सकते हैं जब सरकार द्वारा एसटीबी इंटरऑपरेबिलिटी जैसे मिडलवेयर परिप्रेक्ष्य से परिवर्तन लागू किये जाते हैं। ■