SOFTWARE vs SMART CARD

SOFTWARE BASED VS SMART CARD BASED CAS

In the early days of the Satellite TV era the question of Content rights and Content protection appeared. With the growing awareness of free to air satellite based channels like Sky, broadcasted from London with footprint over Europe the question of Content rights and protection became crucial. The first IRD and STB devices appeared with some sort of protection built into the IRD/STB. Not long after, the broadcasters started to complain about piracy and the race against content piracy started.

Mr. TRYGGVE ARVESCHOUG
CEO,
Conax Access Systems Pvt Ltd.

The first battle was between onboard HW security modules versus detachable HW security modules. As the pirates continued to succeed to break into the early days protection systems, it became expensive to change all the IRD's and STB's whenever the security was compromised. Soon the onboard security chip was outclassed by the relatively inexpensive detachable chip.

Research was soon shifted towards developing a small tamperproof security device called a Smart Card and had the size and shape of a credit card and a standard Smart Card communication protocol (ISO 7816) was developed and became the leading standard.

In today's modern high security systems we continue to use Smart Cards. Why?

The answer is both complex and simple. First of all; changing the STB's and IRD's if the security is compromised is expensive. The security technology of STB's is known to be 10 years behind state of the art Smart Card technology. Then, why not simply put a state of the art Smart Card onboard the STB? The answer can be yes, but for how long time will that particular Smart Card chip remain secure before you need to replace it? How do you replace it?

Many SW CAS vendors today rely on what is known as security by obscurity. Hiding the Key in SW

सॉफ्टवेयर बनाम स्मार्ट कार्ड आधारित सीएएस

प्रसारण परीक्षेत्र में सिक्यूरिटी मॉड्यूल्स पर आधारित सीएएस वनाम डीटैचवल स्मार्ट कार्ड पर आधारित एसडब्लू का विस्तार सैटेलाइट टीवी युग के प्रारंभिक दिनों में विषयवस्तु अधिकार और विषयवस्तु संरक्षण का प्रश्न उपस्थित हुआ। फ्री टू एयर सैटेलाइट आधारित चैनलों की वढ़ती जागरूकता के साथ लंदन से प्रसारण और यूरोप में फुटप्रिंट रखने वाले स्काई के साथ विषयवस्तु अधिकार और संरक्षण महत्वपूर्ण प्रश्न वन गयी।

प्रारंभिक आईआरडी व एसटीवी उकरणों में ऐसा लगता है कि कुछ हद तक संरक्षण के उपाय किये गये थे। कुछ समय के वाद प्रसारकों ने पाइरेसी के विषय में शिकायत करनी शुरू की और विषयवस्तु पाइरेसी के खिलाफ अभियान की शुरूआत हुई।

पहला संघर्ष ऑनवोर्ड एचडब्लू सिक्यूरिटी मॉडयूल्स वनाम डीटेचवलएचडब्लू सिक्यूरिटी मॉड्यूल्स के वीच थी। जैसे जैसे पाइरेसी प्रारंभिक दिनों के संरक्षण प्रणाली को तोड़ने में सफलता प्राप्त करता गया, उस हाल में जवकी सुरक्षा के साथ समझौता करने की नौवत आयी तो सभी आईआरडी व एसटीवी को वदलना वेहद महंगा सावित हुआ। शीघ्र ही ऑनवोर्ड सिक्यूरिटी चिप को अपेक्षाकृत सस्ते डीटैचवल चिप ने वहिष्कृत कर दिया था।

शोधकर्ताओं ने शीघ्र ही स्मार्ट कार्ड कहलाने वाले छोटे छेड़छाड़ विहिन सुरक्षा उपकरण के विकास की ओर ध्यान दिया और केडिट कॉर्ड के आकार व प्रकार और स्टैंडर्ड स्मार्ट कार्ड कम्युनिकेशन्स प्रोटोकॉल (ISO 7816) का विकास किया गया है और यह प्रमुख मानक वन गया।

आज के आधुनिक सिक्यूरिटी सिस्टम के युग में हम अभी भी स्मार्ट कार्ड का इस्तेमाल कर रहे हैं। क्यों?

इसका उत्तर जटिल व सरल दोनों है। सवसे पहले सुरक्षा के साथ समझौता करने की हालत में सभी एसटीवी व आईआरडी को वदलना काफी महंगा होता था। एसटीवी से जुड़ी सुरक्षा तकनीकी स्मार्ट कार्ड तकनीकी के मुकावले दस साल पुराना है। तव क्यों नहीं सरलता के साथ स्मार्ट कार्ड को ही एसटीवी के साथ लगाया जाए? इसका उत्तर हां में भी हो सकता है, लेकिन इस विशेष स्मार्ट कार्ड को कितने समय तक सुरक्षित रहने के वाद हमें वदलने की जरुरत होगी? आप इसे हटा कर कैसे दूसरे को लगायेंगे?

SOFTWARE vs SMART CARD

or HW of various levels of security will only delay the inevitable. Hackers today is typically an employee working in a high tech laboratory fitted out with logic analyzers, Scanning Tunneling Microscopes, access to advanced Differential Power Analysis HW and so on. These people do not necessary have a commercial drive, but works for fame and reputation. They very often share knowledge with each other via the Internet in large secret communities where there are no borders.

"If you can make it you can break it" is a well known term among security specialists. What matters is your track record and how much time and money are required to restore security should a breach occur. Changing a relatively inexpensive Smart Card is far less costly than changing the whole STB. Not to mention the difference in size of the logistic operation. STB's comes in containers and Smart Cards come in boxes.

Once a Key is located by hackers in any CAS system, the most common response by the CAS vendor is to replace that particular Key using a higher level Key. However, once the security device is hacked whether being a Smart Card or not, the higher level Keys will also be found by the hackers until it is no longer possible to restore any kind of security. This happens often within 3-6 months for most low level security systems following the initial security hack. The only way out is to replace the security device being an STB or a Smart Card.

The most expensive commodities for any broadcast operator are content and to roll out STB's often by heavily subsidizing them. The business model is pulled between cost of STB and content and how to recover these costs. It is tempting for an operator to buy cheap low security grade STB's and often a cheap SW based Conditional Access System. However, in the end many operators in other parts of the world have been forced by content owners to replace both the CAS and the STB to re establish security, often resulting in near bankruptcy or at the best a hefty financial setback for the operator.

Today in India, where the ARPU level is significantly lower than in other parts of the world it is extremely difficult to recover from a security breach requiring full STB replacement. Buying cheap is often an expensive exercise. Remember that hackers very often work for fame and reputation not for money. For hackers the ARPU level means nothing only fame and reputation and free access to content. ■

कई एसडब्लू सीएएस प्रदायक अस्पष्टता द्वारा सुरक्षा पर भरोसा करते हैं। सुरक्षा के विभिन्न स्तरों के एसडब्लू या एचडब्लू में की (Key) को छुपाना सिर्फ अनिवार्य रूप से देरी करेगी। आज हैकर विशिष्ट तौर पर हाई टेक लैबरोटरी के कर्मचारी होते हैं जिनके पास लॉजिक एनालाइजर, स्कैनिंग ट्यूनिलिंग माइक्रोस्कोप, एक्सेस टू एडवांस डिफिरेंसियल पॉवर एनॉलिसिस एचडब्लू और कई अन्य उपकरण होते हैं। इन लोगों के पास जरूरी नहीं की कमर्शियल ड्राइव हो, वे प्रसिद्धि व ख्याति के लिए काम करते हैं। वे प्राय: विशाल गुप्त समुदाय में इंटरनेट की सहायता से एकदूसरे के साथ जानकारी का आदान प्रदान करते हैं जहां कि कोई सीमा नहीं होती है। 'यदि आप बना सकते हैं तो ब्रेक भी कर सकते हैं', यह सुरक्षा विशेषज्ञों के बीच जानी मानी उक्ति है। सबसे महत्वपूर्ण है कि आपका ट्रैक रिकॉर्ड क्या है और आप नियमभंग करने वाली सुरक्षा को स्थापित करने में कितना समय और पैसा लेते हैं। पूरे एसटीवी को बदलने के मुकाबले अपेक्षाकृत सस्ते स्मार्ट कार्ड को बदलने का खर्च कहीं कम आयेगा। यहां लॉजिस्टीक संचालन के आकार में भिन्नता का उल्लेख न हो। एसटीवी जहां कंटेनर में आता है, वहीं स्मार्ट कार्ड बॉक्स में।

किसी सीएएस सिस्टम में हैकर द्वारा की (Key) की पहचान के बाद सीएएस प्रदायकों द्वारा उस उच्चस्तरीय की (Key) का इस्तेमाल करके उस खास की (Key) को हटा कर दूसरा लगाना। हालांकि एकबार जैसे ही सुरक्षा उपकरण को हैक कर लिया जाता है तो वह स्मार्ट कार्ड हो या न हो, उच्चस्तरीय की (Key) भी हैकर द्वारा प्राप्त कर लिया जाता है, तब तक किसी तरह की सुरक्षा की वापसी संभव नहीं है। प्रारंभिक सिक्यूरिटी हैक के बाद अधिकतर निम्नस्तरीय सिक्यूरिटी, सिस्टम के लिए **3** से **6** महीने के भीतर प्रायः घटती है। इसका एक मात्र उपाय सिक्यूरिटी उपकरण के स्थान पर एसटीवी या स्मार्ट कार्ड को लगाना। किसी भी प्रसारक ऑपरेटर के लिए सबसे मूल्यवान संपत्ति विषयवस्तु होती है और एसटीवी लगाने के लिए प्राय: उन्हें भारी अनुदान देना पड़ता है। बिजनेस मॉडल को एसटीवी व विषयसूची के खर्च के बीच व इन खर्च को कैसे वापस प्राप्त किया जाए उस पर खींचतानी होती है। एक ऑपरेटर को यह प्रलोभित करता है कि वे सस्ते निम्न सुरक्षा वाले सिक्यूरिटी ग्रेड वाले एसटीवी और प्रायः सस्ते एसडब्लू आधारित कंडिशनल एक्सेस सिस्टम खरीदें। हालांकि अंत में विश्व के कई हिस्सों में ऑपरेटरों को कार्यक्रम प्रदायकों की ओर से बाध्य होकर सुरक्षा की पुर्नस्थापना के लिए सीएएस और एसटीवी दोनों को बदलना पड़ा, जिसका परिणाम प्राय: लगभग आर्थिक बर्बादी या ऑपरेटरों के लिए भारी आर्थिक क्षति के रूप में देखने को मिला है। आज भारत में, जहां एआरपीयू स्तर विश्व के अन्य हिस्सों के मुकाबले काफी नीचे है, सुरक्षा उल्लंघन से निबटने के लिए आवश्यक पूर्णतया एसटीवी की पुर्न स्थापना करना बेहद कठिन है। सस्ता खरीदना प्राय: महंगा साबित होता है। याद रखें कि हैकर प्राय: प्रसिद्धि व ख्याति के लिए काम करते हैं, न कि पैसे के लिए। हैकर के लिए एआरपीयू स्तर का मतलब सिर्फ ख्याति व प्रसिद्धि और कार्यक्रमों के मुफ्त एक्सेस से अधिक नहीं है। ■