

## Forum-Gewerberecht | Spielrecht | Bringt die Prüfung der Checksumme Sicherheit?

Autor	Beitrag
<p><a href="#">Meike</a> 10.05.2008 13:42</p>	<p>Gruß an alle,</p> <p>einige propagieren die Checksummenprüfung als Höchstmaß an Sicherheit. Sie glauben durch äußerliche Überprüfung der Checksumme am GGSG leicht nachsehen zu können, ob das was im GGSG "drin ist" auch so geprüft wurde.</p> <p>Wie ich hörte sind die Prüfmethode der §7 SpielV Prüfungen ähnlich, aber von interner Seite her aufgebaut.</p> <p>Nachdem ich den PTB-Prüfbericht gelesen hatte, wurde ich äußerst kritisch und fand auch einige Schriftsätze, die sich schon seit Jahren mit dem CRC-Verfahren auseinander setzen.</p> <p>Kann mir jemand erklären warum dieses Verfahren gewählt wird, wenn schon im Juli 2002 nachfolgend erscheint:</p> <p>Universität der Bundeswehr München, "Internet Economics I", Hrsg. Burkhard Stiller und Oliver Braun, Bericht Nr. 2002 - 04</p> <p>Seite 89</p> <p>"Die CRC-32 Funktion ist aber linear, was es ermöglicht, die Änderungen im Inhalt des Datenpaketes zu errechnen und den CRC-Wert entsprechend zu ändern. Somit ist es einem Angreifer möglich, beliebige Bits innerhalb einer Nachricht zu verändern und die Checksumme so zu ändern, dass das Paket als gültig anerkannt wird."</p> <p>oder</p> <p>so heißt es auch 2005 zu "WLAN-Einführung an der Fachhochschule Regensburg, Grundlagen und Pilotierung", von Thomas Cornelesen</p> <p>Seite 59</p> <p>Dort werden die Lücken bei der Integritätskontrolle dargestellt.</p> <p>"Zur Erkennung mutwilliger Manipulationen ist das CRC-Verfahren ungeeignet, da der CRC-Algorithmus bekannt ist und somit für manipulierte Nutzdaten problemlos neu berechnet werden kann."</p> <p>Gruß Meike</p> <p>P.S.: Wollte diesen Beitrag eigentlich erst unter Jaspers Beitrag zum Wahlcomputer "packen", - passt so schön-, aber wäre dann etwas off topic geworden.</p>
<p><a href="#">dieter116</a> 11.05.2008 06:27</p>	<p>Dann erscheint aber eine andere Checksumme im Display.</p> <p>Neuberechnung = neue Checksumme</p>

Autor	Beitrag
<p><a href="#">Meike</a> 11.05.2008 07:16</p>	<p>Hallo Dieter,</p> <p>wenn man den Arbeiten der Informatiker glaubt, dann soll das eben nicht der Fall sein.</p> <p>So auch "Empirische Untersuchung zur WLAN-Sicherheit mittels Wardriving", von Stefan Dörhöfer, RWTH Aachen, vom 14.09.2006</p> <p>Seite 32</p> <p>"Das CRC-Verfahren wurde jedoch ursprünglich für die Erkennung zufälliger Fehler bei der Datenübertragung entwickelt. Für den Schutz gegen gezielte Manipulationen ist das Verfahren hingegen nicht geeignet, da es linear ist. Veränderungen bestimmter Bits der Nachricht wirken sich immer nur auf bestimmte Bits der CRC Checksumme aus. Nimmt ein Angreifer eine Änderung an der Nachricht vor, kann er genau bestimmen, auf welche Weise die Checksumme verändert werden muss, damit die Manipulation nicht erkannt werden kann."</p> <p>Gruß Meike</p>
<p><a href="#">eric</a> 11.05.2008 09:42</p>	<p>CRC-Checksummen sind ziemlich sicher, denn die Checksumme wird errechnet aus den vorliegenden Programmdateien, wenn man die Programmdateien ändert, ändert sich die Checksumme ! Was für mich aber heisst, jede neue Programmversion (Update) hat eine neue Checksumme, welche den Prüfern bekannt gemacht werden müsste. Dazu passt auch die Situation vor Wochen, dass die meisten Programme von adp oder auch Novo erneuert werden mussten MIT PTB Segen.</p> <p>Das Verfahren wird seit Jahren bei Softwarekomprimierung eingesetzt. Bekanntestes Beispiel ist der Packer ZIP !</p> <p>Nur am Rande.</p>
<p><a href="#">TM</a> 11.05.2008 23:35</p>	<p>hallo Meike,</p> <p>hier geht es nicht um verschlüsselte nachrichten um angreifer abzuwehren, sondern um software in verbindung mit spezieller hardware die nicht im electronic-versandhaus geführt wird.</p> <p>gruss TM</p>

Autor	Beitrag
<p><a href="#">Meike</a> 12.05.2008 06:52</p>	<p>Hallo TM,</p> <p>der "Angriff auf verschlüsselte Nachrichten" kann vielfältig sein. Bitte nicht nur im militärischen Bereich sehen. Denk an online-banking und ähnliches.</p> <p>Das könnte nach meinem laienhaften Verständnis hier z.B. bedeuten, dass in das GGSG Programmbestandteile hinzukommen oder verändert worden seien und damit dies nicht auffällt, müsste die Checksumme, die durch die neuen "Nachrichten" erstmal verändert wurde, neu berechnet werden, damit diese sich wieder im "alten Bild" darstellt.</p> <p>Um welche veränderten "Nachrichten" es sich z.B. handelt könnte und wie diese übertragen werden könnten, ergibt sich z.B. auch aus dem Prüfbericht.</p> <p>Seite 20</p> <p>"Ein der PTB bisher nicht bekannt gegebene Funktion dieses Auslesegerätes besteht in der Abspeicherung eines ggf. neuen Steuerungsprogrammes von einem eingesteckten Datenspeicher in die Datenbank des Sicherheitsmoduls eines Geldspielgerätes. Sofern auf der eingesteckten RAM-CARD ein X-File mit dem (verschlüsselten) Steuerungsprogramm gespeichert ist, erfolgt dessen Abspeicherung im Geldspielgerät automatisch, sobald..... Solche Einlesefunktion eines Auslesegerätes ist im Zulassungsschein eines Geldspielgerätes nicht genehmigt worden."</p> <p>Gruß Meike</p>
<p><a href="#">dieter116</a> 12.05.2008 08:26</p>	<p>" ...auf welche Weise die Checksumme verändert werden muss..." Du schreibst selbst, dass die Checksumme verändert wird, es also erkennbar ist.</p> <p>Etwas Anderes wäre es, wenn das Betätigen der Tasten zum Abruf etwas Anderes macht als die Checksumme anzuzeigen, also immer, auch bei Programmänderungen eine fest vorgegebene Zahl anzeigt. Das ist aber Sache der PTB , dies bei der Zulassungsvergabe zu überprüfen.</p> <p>Die Ram Card dient zum Programmupdate, ähnlich wie der Epromwechsel bei anderen Herstellern. Das hat nichts mit Manipulation zu tun.</p> <p>Da kann ein normaler Aufsteller herute nichts mehr manipulieren. Was die Hersteller mit den von Ihnen betriebenen Geräte machen , ist eine andere Sache.</p> <p>Meike, Du hast gute Rechtskenntnisse, aber was die Technik der Geräte betrifft, da haben andere doch bessere Kenntnisse.</p>

Autor	Beitrag
<p data-bbox="92 145 327 212"> <a href="#">TM</a>            12.05.2008 13:49         </p>	<p data-bbox="352 145 427 174">@alle</p> <p data-bbox="352 215 422 244">hallo,</p> <p data-bbox="352 284 1485 412">           der hier oft zitierte PTB-Prüfbericht aus dem Jahr 2005 bezieht sich auf Geräte aus dem Jahr 2004 und älter. bei diesen Geräten oder ähnlicher Bauart ist die Laufzeit schon längst überschritten und sind somit nicht mehr in Betrieb.         </p> <p data-bbox="352 452 1401 517">           aktueller ist doch die Feststellung der PTB in chronologisch richtiger Reihenfolge zu lesen in Jaspers Beitrag: "Eine PTB und zwei Meinungen!"         </p> <p data-bbox="352 557 416 586">Zitat:</p> <p data-bbox="352 624 1485 752">           " PTB am 09.01.2007:            „Ohne auf technische Einzelheiten einzugehen, stellt die PTB klar, dass die in Augsburg festgestellten Veränderungen grundsätzlich nicht den Spielerschutz gemäß § 33e GewO betreffen“         </p> <p data-bbox="352 792 831 822">und auch aktuell nachzulesen ist die:</p> <p data-bbox="352 862 1054 1055">           Technische Richtlinie            Geldspielgeräte im Sinne von § 33c Gewerbeordnung            Mit Anhang            Entwurf der Version 4.0 vom 8. November 2007            Hervorgegangen aus der            Version 3.3 vom 4. Mai 2007         </p> <p data-bbox="352 1095 400 1124">z.B.</p> <p data-bbox="352 1128 1433 1290">           1.4 Schutz vor Veränderungen und Eingriffen            Das Geldspielgerät ist so konstruiert, dass es mit einfachen Mitteln nicht verändert, ergänzt oder abweichend gegenüber den beschriebenen Möglichkeiten benutzt werden kann. Wichtige Komponenten unterliegen einem besonderen Schutz .....         </p> <p data-bbox="352 1330 400 1359">z.B.</p> <p data-bbox="352 1400 1390 1592">           Für die Spielsteuerung werden die zurzeit angewendeten Sicherungsverfahren (z.B. Checksummenvergleich, Dongle-Funktionen) als ausreichend angesehen. Diese Sicherungsmaßnahmen gelten auch für die Kontrolleinrichtung und für die Aufbereitungseinheit der steuerlichen Daten als ausreichend, wenn die ProTechnische Richtlinie für Geldspielgeräte, Entwurf Version 4.0 8. November 2007         </p> <p data-bbox="352 1597 422 1626">- 17 -</p> <p data-bbox="352 1630 1433 1928">           gramme integraler Teil der Software für die Spielsteuerung sind. Das gilt auch für die Kommunikation zwischen den Komponenten. Wenn die Kontrolleinrichtung auf separater Hardware realisiert ist, sind zusätzliche Sicherungsmaßnahmen zur Wahrung der Authentizität und Integrität der Kontrolleinrichtung sowie der Kommunikation zwischen Kontrolleinrichtung und Spielsteuerung erforderlich. Die zwischen der Kontrolleinrichtung und der Spielsteuerung übertragenen Daten müssen mit einem Hash-Verfahren signiert und die Signatur muss geeignet gesichert werden. Dabei werden folgende Mindeststandards         </p> <p data-bbox="352 1933 576 1962">vorausgesetzt<sup>10</sup>:</p> <p data-bbox="352 1966 1433 2136">           • Signaturerzeugung durch MD5, SHA1 oder ein vergleichbares Verfahren,            • asymmetrische Verschlüsselung der Signatur nach RSA mit einer Schlüssellänge von 1024 Bit oder            • asymmetrische Verschlüsselung der Signatur mit elliptischen Kurven mit         </p>

Autor	Beitrag
	<p>einer Schlüssellänge von 128 Bit oder        &amp;#8722; symmetrische Verschlüsselung der Signatur auf der Basis von 3-DES oder AES und Wechsel des Sessionschlüssels.        Wenn die Aufbereitungseinheit der steuerlichen Daten auf separater Hardware realisiert ist, ist die Kommunikation zwischen Kontrolleinrichtung und Aufbereitungseinheit bzw. zwischen Spielsteuerung und Aufbereitungseinheit zu signieren und die Signatur in angemessener Stärke zu verschlüsseln. Bis auf weiteres wird eine Signaturerzeugung durch MD5, SHA1 oder ein vergleichbares Verfahren und 3-DES oder AES und Wechsel des Sessionschlüssels für die Verschlüsselung als ausreichend angesehen.</p> <p>Zitat ende</p> <p>meine Frage nun was versteht ein einfacher aufsteller unter :</p> <p>"&amp;#8722; asymmetrische Verschlüsselung der Signatur mit elliptischen Kurven mit einer Schlüssellänge von 128 Bit oder        &amp;#8722; symmetrische Verschlüsselung der Signatur auf der Basis von 3-DES oder AES und Wechsel des Sessionschlüssels."</p> <p>Gruss TM</p> <p>PS : er kennt bestenfalls seine automaten Schlüssel und wird kaum die Spielsteuerung verändern können.</p>
<p><a href="#">hansi</a>        12.05.2008 19:22</p>	<p>Hallo TM,</p> <p>und was versteht ein Gerätehersteller darunter, der gleichzeitig eine bundesweite Spielhallenkette mit vernetzten Glücksspielgeräten betreibt? Es geht hier doch nicht um den Automatenaufsteller der nur seinen Automaten Schlüssel kennt. Es geht nicht darum, dass ich als Automatenaufsteller daran gehindert werde die Software im Nachhinein zu manipulieren.</p> <p>Es geht darum, dass es Gerätehersteller gibt, die gleichzeitig auch Automatenaufsteller sind und daher bereits ab Werk entsprechende Vorbereitungen treffen könnten.        SIEHE PTB-BERICHT. Der daran geschilderte Sachverhalt bezog sich NICHT auf einen einfachen Automatenaufsteller!!</p> <p>Schläferprogramme welche bereits im Testgerät zur PTB Bauartprüfung „versteckt“ waren, können unbemerkt in die Nachbaugeräte gelangen und jederzeit aktiviert werden, ohne das sie über einen Checksummenvergleich zu lokalisieren sind. – Für einen findigen Programmierer eines Geräteherstellers ist es ein leichtes ein Schläferprogramm innerhalb einer Checksumme zu verstecken.</p> <p>Ein Großteil der im PTB-Bericht aufgeführten Geräte sind noch heute zugelassen. Was bereits 2005 möglich war, dürfte heute für jeden Softwareprogrammierer eines Geräteherstellers ein Kinderspiel sein.</p> <p>Ich für mein Teil bin mir nicht sicher, dass die Gerätehersteller ihre Glücksspielgeräte wirklich nur in derselben Art nutzen können wie wir Aufsteller.</p> <p>Und wie sicher bzw. unsicher Software sein kann, musste die PTB jetzt mit dem Wahlcomputer erfahren. Leider hat es bis zur deren Einsicht sehr viel unnötige Zeit gebraucht.</p>

Autor	Beitrag
<p><a href="#">magnum</a> 13.05.2008 14:20</p>	<p>:gruessgott:</p> <p>Security by Obscurity</p> <p>Sicherheit durch Undurchsichtigkeit - die naive, aber immer noch weit verbreitete Annahme, dass ein System dann sicher ist, wenn man seine Funktionsweise geheim hält.</p> <p>Der gegenteilige Ansatz verwendet Algorithmen, die auch dann sicher sind, wenn potenzielle Angreifer sie kennen. Dabei heißt es bereits im Lehrbuch: "Zum Ersten soll der Entwurf eines Systems öffentlich zugänglich sein. Die Annahme, dass ein Eindringling nicht weiß, wie ein System funktioniert, dient lediglich der Täuschung der Entwickler." (Tanenbaun, 1995, S. 231)</p> <p>Schläferprogramme die z.B. zur beleglosen Zwischenkassierung aktiviert werden können, können in jedem Lampentreiber „versteckt“ sein. Wenn solch eine „Schadsoftware“ die Bauartzulassung der PTB überstanden hat, dann befindet sie sich in jedem Nachbaugerät und ist über einen Checksummenvergleich nicht auffindbar. Kann aber jederzeit beliebig aktiviert und deaktiviert werden.</p> <p>Die Lösung kann nur im „Open Source System“ liegen. Der PTB, die das nationale Metrologie-Institut mit wissenschaftlich-technischen Dienstleistungsaufgaben darstellt und mit höchster Genauigkeit und Zuverlässigkeit – Metrologie als Kernkompetenz mißt, (siehe: <a href="http://www.ptb.de/de/zieleaufgaben/dieptb.html">http://www.ptb.de/de/zieleaufgaben/dieptb.html</a>) dürfte das sicherlich bekannt sein, oder etwa nicht?</p> <p>:danke:</p>
<p><a href="#">TM</a> 13.05.2008 20:16</p>	<p>@hansi</p> <p>Ein Großteil der im PTB-Bericht aufgeführten Geräte sind noch heute zugelassen. Was bereits 2005 möglich war, dürfte heute für jeden Softwareprogrammierer eines Geräteherstellers ein Kinderspiel sein.</p> <p>Hallo hansi ,</p> <p>du hast recht damit das es noch geräte dieser bauserien mit zulassung gibt aber nicht zum grossteil sie sterben jetzt langsam aus , und sollten eigentlich ein update ohne schläferprogramm haben.</p> <p>ich habe mich verschätzt weil ich von diesen baureihen selbst keine mehr aufstelle und so wie ich weis bei den grossfilalisten auch keine stehen.</p> <p>somit brauch man über diese geräte auch nicht mehr sprechen.</p> <p>sonst bin ich schon deiner meinung.</p> <p>nur das gesetz wird nicht kommen das hersteller nicht aufstellen dürfen.</p> <p>sollten aber hersteller u.aufsteller wiederholt mit illegalen mitteln arbeiten dann müsste die herstellung sowie aufstellung verboten werden und mit saftigen geldstrafen belegt werden.</p> <p>und der wettbewerb wäre etwas gerechter.</p> <p>gruss TM</p>

Autor	Beitrag
<p><a href="#">hansi</a> 14.05.2008 08:29</p>	<p>Hallo TM, was hat sich seid dem PTB-Prüfbericht an der Technik der Geräte geändert, wodurch wir Aufsteller abgesichert werden, dass die von den Geräteherstellern betrieben Geräte genauso laufen wie unsere?</p> <p>Die Ergebnisse des PTB-Berichts sind heute genauso aktuell wie die darin aufgeführten Gerätehersteller. Die heutigen Geräte tragen zwar andere Namen und evtl. ein anderes Design, die Technik bzw. deren Überprüfungsmöglichkeiten sind jedoch weiterhin die gleichen. Daher sollte auch weiterhin vom PTB-Bericht gesprochen werden. Die Hersteller wollten und mussten, bei solch einer lächerlichen Strafe, nichts daraus lernen und der PTB war es scheinbar zu peinlich!</p> <p>Hallo Magnum, bis du ein Informatiker? Wenn es solch eine "beleglose Zwischenkassierung" gibt, warum kann ich das nicht? Das mit der im Lampentreiber versteckten Software zur beleglosen Zwischenkassierung ist ein guter Denkansatz. Wenn es den Verantwortlichen wirklich ernst ist, dann sollten sie sich über das „Open Source System“ mal ganz schnell ernsthafte Gedanken machen.</p>
<p><a href="#">gmg</a> 15.05.2008 21:05</p>	<p>@ alle</p> <p>1) Wer hat eigentlich seinerzeit den CRC-Checksummentest als Testmittel für jeden halbwegs mit einem Geldspielgerät vertrauten Nutzer ( egal ob Automatenaufsteller oder Behördenbediensteten ) ins Gespräch gebracht ? Der CRC-Checksummentest sollte ja ein einfaches Testmittel sein.</p> <p>2) Wenn ich den Inhalt der Wortbeiträge zu diesem Threat richtig gelesen habe, dann wird hier also von verschiedenen Usern die Meinung vertreten, dass der CRC-Checksummentest nicht als Allheilmittel angesehen werden kann, um die Software sicher gegen Veränderungen von dritter Seite zu schützen.</p> <p>Darüber hinaus taugt der CRC-Checksummentest nichts, wenn die Software des Geldspielgerätes mit einem sog. Schläferprogramm vor der Prüfung der Software im Rahmen des Zulassungsverfahrens durch die PTB belegt worden ist.</p> <p>Da ich technisch nicht entsprechend vorgebildet bin, bleibt mir eigentlich nur eine einzige Frage an die anderen User:</p> <p>Gibt es eine andere und bessere einfache Überprüfungsmöglichkeit, um feststellen zu können, dass die gerade überprüfte Software des entsprechenden Geldspielgerätes nicht verändert worden ist bzw. der zugelassenen Software entspricht ??</p> <p>Grüße</p>
<p><a href="#">dieter116</a> 16.05.2008 05:39</p>	<p>Bitvergleich mit der bei der PTB hinterlegten Software oder Prüfung durch Prüfer.</p>

Autor	Beitrag
<a href="#">magnum</a> 17.05.2008 13:29	<p>:gruessgott:</p> <p>Hallo Hansi,  man muss kein Informatiker sein, um solche Schwachstellen erkennen zu können.</p> <p>Eine "beleglose Zwischenkassierung" ist nur mit einem „Schlüssel“ zum aktivieren der Schläferprogramme möglich. Wenn Du solch einen Schlüssel nicht hast und Deine Geräte nicht vernetzt sind, dann musst Du weiterhin die Gerätetür aufschließen.</p> <p>Hallo dieter,</p> <p>wenn das Schläferprogramm bereits im PTB-Testgerät hinterlegt wurde, bring ein Bitvergleich keine Sicherheit. Denn die Grundlage des Vergleichs ist die bei der PTB hinterlegte Software.</p> <p>Noch einfacher ist es, wenn das Schläferprogramm zwar innerhalb des Gerätes versteckt wird, jedoch außerhalb der Software, die von der PTB überprüft wird. Eine Aktivierung über die Geräteschnittstelle der Hersteller ist somit ohne Einfluss auf die Checksumme möglich.</p> <p>:danke:</p>
<a href="#">TM</a> 17.05.2008 16:34	<p>org.magnum  [COLOR=teal</p> <p>hallo magnum,</p> <p>was verstehst du unter einem programm ausserhalb der software.  und erkläre uns bitte mal die ""beleglose zwischenkassierung"" am geldspielgerät.</p> <p>gruss TM</p>
<a href="#">jasper</a> 18.05.2008 12:12	<p>Hallo magnum,  als Geräteschnittstelle der Hersteller meinst du bestimmt die so genannte VDAI Schnittstelle. Deine Bezeichnung gefällt mir besser! Sollte wir nicht mal alle gemeinsam recherchieren, wer eigentlich für die Belegung und die Kontrolle dieser Schnittstelle der Industriespielhallenbetreiber (Schnittstelle unserer Mitbewerber) :D zuständig ist?</p> <p>Bitte beachte meine pn.</p>

Autor	Beitrag
<a href="#">magnum</a> 19.05.2008 09:20	:moin:  Hallo TM,  unter einem Programm außerhalb der geprüften Software, verstehe ich, dass die PTB lediglich die Software überprüft, die für das Spiel um Geldgewinn bzw. Geldverlust zuständig ist. Da sich das eigentliche Spiel jedoch um Punktegewinn und Punkteverlust dreht, ist bereits dadurch reichlich ungeprüfter Platz für Schadsoftware vorhanden.  Beleglos heißt: Ohne Beleg. Also ohne einen tatsächlichen Nachweis.  Zwischenkassierung bezeichnet man eine unreguläre Kassierung die zwischen zwei regulären Kassierungen stattfindet.  Und was ferngesteuert heißt dürfte klar sein.  Für Eric: Ferngesteuert hat nichts mit "auslesen" zu tun!  :danke:
<a href="#">TM</a> 19.05.2008 17:26	Hallo magnum,  schau dir mal eine bauartzulassung geldspielgerät an, da wird jede schraube berücksichtigt. und belege von gsg sind fortlaufend gekennzeichnet und lückenlos für eine mögliche nachprüfung aufzubewahren.  TM
<a href="#">gmg</a> 19.05.2008 18:33	@ alle  Dann gibt es also NICHTS, was besser wäre für die Überprüfung der Software an Geldspielgeräten als den CRC-Checksummentest ?  Keine andere und bessere einfache Überprüfungsmöglichkeit ?  Grüße

Autor	Beitrag
<p><a href="#">dieter116</a> 20.05.2008 05:40</p>	<p>Wie oben bereits geschrieben nur der Bitvergleich mit der bei der PTB hinterlegten Software, bzw. externer Checksummentest, wie es auch die Prüfer machen.</p> <p>Hiermit kann die Übereinstimmung der Software des GSG mit der hinterlegten Software überprüft werden.</p> <p>Wenn die PTB aber nicht den vollständigen Quelltext hat und diesen auch genau analysiert hat, weiss natürlich nur der Hersteller, was die Software beinhaltet.</p> <p>Das Ganze wäre interessant in Hinblick auf die Ferneinwirkung für das Spielverhalten des Gerätes.</p> <p>Die 'beleglose Zwischenkassierungen' der Hersteller an ihren Geräten halte ich für ein Hirngespinnst, allein aus organisatorischen Gründen.</p> <p>Wie kam dieses Gerücht doch eigentlich auf ?</p> <p>Der normale Aufsteller kann es jedenfalls nicht. Eine externe Änderung der Gerätesoftware wäre sehr aufwendig und würde bei den obengenannten Testmethoden zum Vorschein kommen, hierzu gibt es auch ein Mustergutachten</p> <p>.</p>
<p><a href="#">hansi</a> 20.05.2008 21:02</p>	<p>Hallo dieter123, wie kam dieses Gerücht doch eigentlich auf, dass es sich hierbei um ein Gerücht handeln soll?</p> <p>Warum Hirngespinnst? Was für organisatorische Gründe?</p>
<p><a href="#">dieter116</a> 21.05.2008 08:22</p>	<p>Welche konkreten Hinweise gibt es denn, dass jemand beleglose Zwischenkassierungen durchführt oder durchgeführt hat ? Unter beleglosen Zwischenkassierungen verstehe ich Geldentnahmen aus den Geräten ohne dass dieses irgendeiner Form dokumentiert wird, also auch nicht auf dem Geräteausdruck. Und es sich somit um die Erzielung von Schwarzgeld handelt.</p> <p>Aus organisatorisch Gründen meine ich Folgendes:</p> <p>Soweit ich mich erinnern kann, war hier die Rede davon, dass dies ein Hersteller macht, der gleichzeitig Spielhallen betreibt. Wie bitte soll dieser das durchführen ohne das Dritte es mitbekommen ? Er wäre existenzbedrohend erpressbar. Kann er so dämlich sein ?</p>

Autor	Beitrag
<p><a href="#">tfis</a> 21.05.2008 14:17</p>	<p>Natürlich funktioniert die beleglose Zwischenkassierung und das seit Jahren!</p> <p>Tür auf, Kohle raus, Tür zu!*</p> <p>Kein Beleg!</p> <p>(natürlich differiert dann bei Belegerstellung die buchhalterische mit der physischen Kasse).</p> <p>Das tolle an Verschwörungstheorien: Sobald man Argumente dagegen aufbringt, wird die Meinung der Befürworter automatisch verstärkt, dann man ja beweist, das man selbst Teil der Verschwörung ist.</p> <p>Kurzum: Wenn ich sage es gibt keine Ufo, dann bin ich ein Ausserirdischer!</p> <p>Wenn ich sage "Elvis ist tot", dann...ähm.... oh Gott... ich geh mal meine Koteletten stutzen....</p> <p>*Achtung ironisch zu verstehen!!!</p>
<p><a href="#">magnum</a> 22.05.2008 11:07</p>	<p>:moin:</p> <p>@tfis</p> <p>Dann bring doch bitte mal ein Argument dagegen auf!</p> <p>@alle</p> <p>Hier nur eine Möglichkeit:</p> <p>Beleglose Geldentnahme = ferngesteuerte Spielergewinnabschöpfung</p> <p>Zitat:</p> <p>4.2. Transparenter Geldfluss</p> <p>In zweiter Linie geht es aber auch um einen transparenten und somit nachvollziehbaren Geldfluss. Denn wodurch wird beim Einsatz solcher Systeme technisch sichergestellt, dass es nicht die System-Betreiber selbst sind, die den eigentlichen „Spielergewinn“ durch den Einsatz ihrer speziellen Chipkarten (z.B. einer Jugendschutzkarten) abschöpfen?</p> <p>Weil „Ferneinstellungen via Netzanbindung“ und jeglicher Einsatz von „Chipkarten“ zum „Player-Tracking“ führen kann und in keiner Weise zu kontrollieren ist.</p> <p>Zitat Ende!</p> <p>Gefunden: <a href="http://www.player-tracking.de">www.player-tracking.de</a></p> <p>:danke:</p>
<p><a href="#">jasper</a> 25.05.2008 15:32</p>	<p>Warum die Checksumme für teures Geld und viel Aufwand prüfen lassen, wenn man die beim Hersteller einfach die Zulassung austauschen kann? :D</p>

Autor	Beitrag
<p data-bbox="92 143 325 210"><a href="#">RudiCartell</a> 26.05.2008 09:09</p>	<p data-bbox="352 143 1528 340">Ich war einige Zeit außer Gefecht, habe aber ein Telefonat mit Dr. Möck von der PTB geführt, um mein erstes Thema aus dem Februar (Eigentümer, Aufsteller, Hersteller, Geräteinhaber) vor der Geräteprüfung geklärt zu bekommen. Ich komme aber auch gleich zu den Checksummen und wer da was mit prüfen kann. PTB Auskunft Aufsteller und Geräteinhaber aus §7 SpielV sind als gleichbedeutend anzusehen. Nun zu den Prüfsummen:</p> <p data-bbox="352 344 1465 412">Ich habe einer Prüfung in echt beigewohnt und auch den Prüfer befragt. Roland kann uns da sicher auch noch mit Wissen bereichern.</p> <p data-bbox="352 416 1522 515">Nun, die CRC-32 Checksumme wurde erfunden und vorwiegend genutzt, um einen Datenübertragungsweg mit zusätzlicher Prüfinformation zu versehen, um Verfälschungen an einem Datenpaket erkennen zu können (Folge: Wiederholung).</p> <p data-bbox="352 519 1490 815">Das Verfahren ist nicht geeignet, um eindeutig Verfälschungen an einer Softwaredatei (Dateninhalt &gt; 0,5 MB) nachweisen zu können. Es gibt Programme, die es erlauben Dateiinhalte unterschiedlichem Inhaltes zu erzeugen ohne die Länge der Daten (Größe des Programms) zu verändern und mit exakt gleicher CRC-32 Nummer. Diese Kenntnis herrscht nach meiner Einschätzung auch bei der PTB vor. Neuere Modelle (Bauarten) werden, wenn ich das richtig verstanden habe, bereits mit der MD5 Checksumme hinterlegt und überprüft. Hiermit kann das Vergleichsproblem zwischen Hinterlegung des Binärcodes bei der PTB und ausgelesener Software im zu prüfenden Spielautomaten technisch sauber abgehandelt werden.</p> <p data-bbox="352 819 1422 887">Das ist aber technisch und rechtlich für das Ziel des Gesetzes nur die halbe Miete (wenn überhaupt).</p> <p data-bbox="352 891 1469 1120">Es wurde ja bereits zuvor erläutert, was los ist, wenn risikobereite Hersteller bzw. deren Softwareschmieden, es wagen den "ungewollten" Programmcode mit zu hinterlegen oder was sicher viel cleverer ist, den relevanten Programmcode extern in einem Bereich zu halten, der nur indirekt durch den hinterlegten Code nutzbar ist und der bei der Auslesung seitens des Gerätes in der Prüfung auch nicht mitgeliefert wird. Der Prüfer sagte mir, die Auslesesoftware, die er benutze, sei vom Hersteller. Was darf man da erwarten?</p> <p data-bbox="352 1124 1458 1290">Da kann man sich das Gewissen zwar ruhig prüfen, aber eine gewisse Unruhe bleibt dann doch, zumal die Hersteller sicher auch Wege probieren (oder Fehler machen und Programmmodule "vergessen", die nur zum Test gedacht waren - gleich eine plausible Begründung, falls so etwas gefunden würde). Wie komme ich darauf, dass man mal was probieren könne?</p> <p data-bbox="352 1294 1469 1393">Probiert wird momentan schon etwas in herstellernahen/eigenen Spielhallen, wo man bei geputzter Brille "Magie III" lesen kann. Wir Aufsteller bekommen Magie II als brandneu und ich glaube, das ist derzeit auch nur zugelassen.</p> <p data-bbox="352 1397 1533 1496">Also vielleicht kann man ja die Gutwilligen mal dazu bekommen, wirklich einen schlüssigen, unabhängigen Prüfungsvorgang zu installieren, damit man weiß was hat und nicht nur ahnt was man nicht haben sollte.</p> <p data-bbox="352 1500 1474 1729">Bei einem Kollegen aus Oldenburg habe ich jetzt zusätzlich einen Tipp erhalten, dass es wohl auch schon Prüfer geben soll, die selbst Spielhallenbetreiber waren oder sind oder enge Familienverflechtungen in dieser Hinsicht haben. Sollte das zutreffen, scheint mir die Technik-Diskussion um Prüfsummen dann schon fast zweitrangig. Auch wird wohl das Thema vom Jasper mit den Anschlusszulassungen zukünftig den Herstellern mehr in die Karten spielen, weil man damit scheinbar den ganzen Prüfzirkus umgehen kann.</p> <p data-bbox="352 1733 603 1765">Schauen wir mal ...</p> <p data-bbox="352 1800 571 1832">Grüße vom Rudi</p>

Autor	Beitrag
<p><a href="#">hansi</a> 26.05.2008 18:10</p>	<p>Hallo Rudi, na das nenne ich offene Worte. DANKE für die Aufklärung der Allgemeinheit. :respekt: Jetzt dürfte keiner mehr daran zweifeln, dass einer ferngesteuerte Spielergewinnabschöpfung per Vernetzung zwar möglich, aber von außer nicht zu erkennen ist.</p> <p>Das mit den "Magie III" in herstellernahen/eigenen Spielhallen, wäre doch ein ganz klarer Fall für den .....</p> <p><a href="#">ROTEN BRIEF</a></p> <p>vom BA, wenn da nicht diese finanzielle Abhängigkeit vom Verbandsfinanzierer wäre! :schimpf: :heul: :schimpf:</p>
<p><a href="#">jasper</a> 27.05.2008 07:12</p>	<p>@Hansi, dann kannst Du den Roten Brief auch gleich direkt zum Gerätehersteller senden :D</p> <p>@Rudi KLASSE!</p> <p>@alle Ein unsicherer Checksummenvergleich ist schon schlimm genug, noch schlimmer ist, dass die Nachbaugeräte 2 Jahre lange ungeprüft von den Herstellern selbst betrieben werden dürften und eine Überprüfung der Vernetzung überhaupt nicht stattfindet. Am schlimmsten ist jedoch, dass es überhaupt keinen gibt, der für eine Überprüfung zuständig ist! :wand:</p>
<p><a href="#">gmg</a> 29.05.2008 20:28</p>	<p>Hallo RudiCartell</p> <p>Zitat on Rudi Neuere Modelle (Bauarten) werden, wenn ich das richtig verstanden habe, bereits mit der MD5 Checksumme hinterlegt und überprüft. Hiermit kann das Vergleichsproblem zwischen Hinterlegung des Binärcodes bei der PTB und ausgelesener Software im zu prüfenden Spielautomaten technisch sauber abgehandelt werden. Zitat off Rudi</p> <p>Kannst Du mitteilen, um welche neueren Modelle ( Bauarten ) von welchen Herstellern es sich handelt ? Wenden diese Technik alle Hersteller bei den neueren Geräten an ?</p> <p>Grüße</p>
<p><a href="#">jasper</a> 30.05.2008 11:45</p>	<p>Damit das rechtliche Ziel einer „PTB – Zulassung“ auch wirklich erreicht wird, bedarf es aus meiner Sicht zunächst einer genauen Definition für den Begriff „PTB – Zulassung“ und zwar eine Definition welche allen Anforderungen an Manipulationsschutz, Spielerschutz und sauberem Wettbewerb gerecht wird!</p> <p>Solange wie es ungeprüfte Nachbaugeräte, keine Überprüfungsmöglichkeiten, Gerätehersteller gibt die auch Automatenaufsteller sind und sich die PTB nur mit einem einzigen Geräte (Prototype) einer ganzen Baureihe auseinandersetzt, hat die heutige „PTB – Zulassung“ nicht mal den Wert des Papiers der so genannten „Zulassungsurkunde“. :wut:</p>

Autor	Beitrag
<p><a href="#">RudiCartell</a> 31.05.2008 20:25</p>	<p>Ich habe nochmals in den Zulassungen der PTB nachgesehen und in Stichproben mindestens drei Kandidaten von Bally gefunden die mit einer MD5 Prüfsumme zugelassen worden sind: Bauart 2091, 2092, und 2141 (die neuen Multigamer). Dann gibt es auch noch Kurioses, wenn man sich die 2097 Fruit-Runner anguckt SHA1 Checksumme in der Anzeige. Und ganz toll wird es wenn man eine 80 GB Festplatte über CRC-32 absichern möchte, wie beim Golden Island Fire. Auch die 2 GB CF-Card oder 1GB USB-Sticks oder 2GB HDs (2090) sind nicht wirklich Dateigrößen, die sich bei CRC-32 eindeutig mit der Hinterlegung vergleichen lassen. Das Zauberwort heißt "Kollisionsfreiheit", dass eine Prüfsumme aufweisen muß, damit sie geeignet ist, zwei Versionen auf Identität zu prüfen. Unter einem unverdächtigen Link kann man sich da noch etwas aufschlauern:</p> <p><a href="http://de.wikipedia.org/wiki/Hash#Pr.C3.BCfsummen">http://de.wikipedia.org/wiki/Hash#Pr.C3.BCfsummen</a></p> <p>Super sind auch Anzeigen von sehr langen Zeichenketten, die eine "unbekannte" Checksumme widerspiegeln, wie bei der Bauart 2128. Es ist aufgrund der Länge sicher besser als CRC-32 aber für den Inhalt der Festplatte (80GB) wird dann doch wieder auf etwas zurückgegriffen, was wesentlich schlechter ist.</p> <p>So recht verstehen kann man es nicht, warum man sich nicht auf was Einheitliches (Stand der Technik Angepasstes) verständigt. Man könnte eigentlich eine allseits anerkannte kollisionsfreie Checksumme zum Identitätsnachweis auch ohne das Zutun der Hersteller verwenden, weil das Berechnungsverfahren bei der Hinterlegung und bei der Überprüfung von Softwareständen durch den Prüfer vollkommen unabhängig die Berechnung durchführen kann. Letztlich nur, wenn der Hersteller die Zahlenreihe am Gerät im Display anzeigen muss oder möchte, dann muss auch er den Berechnungsalgorithmus in der Gerätesoftware eingebaut sein. Aber selbst das ist kein unlösbares Problem und die jetzigen Anzeigen am Gerät zeigen die CRC-32 Nummern auch nicht an, sondern andere Zeichenketten.</p> <p>Aber nochmals mein Hinweis an gmg, dies ist nur die halbe Miete, weil man auch fehlerhafte Software auf Identität prüfen kann und im Sinne der gewollten Funktion nichts gewonnen hat.</p> <p>Gruss vom Rudi.</p>
<p><a href="#">gmg</a> 01.06.2008 17:35</p>	<p>Hallo RudiCartell</p> <p>zunächst erst mal ein ganz grosses :danke: für die Hinweise.</p> <p>Ich werde versuchen, die Informationen jetzt für mich umzusetzen.</p> <p>Ich werde mich bestimmt noch mit Fragen melden....</p> <p>Grüße</p>

Autor	Beitrag
<p data-bbox="92 145 325 210"><a href="#">Meike</a> 17.08.2008 11:10</p>	<p data-bbox="352 145 523 248">Gruß an alle, bzgl.</p> <p data-bbox="352 315 1318 347"><a href="http://www.justiz.nrw.de/Presse/dpa_ticker/DPA_15086/index.php?print=1">http://www.justiz.nrw.de/Presse/dpa_ticker/DPA_15086/index.php?print=1</a></p> <p data-bbox="352 416 1436 481">"Allein die technische Möglichkeit der Manipulation habe nicht ausgereicht, betonte Pollmann."</p> <p data-bbox="352 517 1485 582">Ist davon auszugehen, dass wenn ein Pressesprecher einer Staatsanwaltschaft so etwas mitteilt und dies auch über justiz.nrw veröffentlicht wurde, dieser Satz korrekt ist.</p> <p data-bbox="352 618 437 649">Frage:</p> <p data-bbox="352 685 1485 750">Sind die §7 Prüfer schon darüber informiert worden, wie die technische Möglichkeit der Manipulation "aussieht" und worauf sich diese Möglichkeit erstrecken kann ?</p> <p data-bbox="352 786 1414 851">- Da hier einige §7 Prüfer Mitglieder im Forum sind, wäre eine Rückmeldung sehr hilfreich.-</p> <p data-bbox="352 887 1445 990">Besteht diese technische Möglichkeit der Manipulation, von der der Pressesprecher der Staatsanwaltschaft Bielefeld spricht, nur bei GGSG nach alter SpielV oder auch bei GGSG nach neuer SpielV?</p> <p data-bbox="352 1025 1342 1090">- Wurden die Aufsteller/Spielhallenbetreiber über die technische Möglichkeit unterrichtet, bzw. wie diese "ausgeschaltet" werden kann?</p> <p data-bbox="352 1126 1536 1229">Wurden die zuständigen Überwachungsbehörden (Ordnungsämter) von dieser Möglichkeit unterrichtet, bzw. wie man erkennen kann, ob die technische Möglichkeit der Manipulation genutzt wurde oder nicht?</p> <p data-bbox="352 1332 432 1397">Gruß Meike</p>

Autor	Beitrag
<p><a href="#">Meike</a> 28.08.2008 06:50</p>	<p>Schade, aufgrund der Reaktionen hier, ist davon auszugehen, dass bis heute keine Informationen erfolgt sind !!</p> <p>Vielleicht sollte sich der ein oder andere nochmal an die EUGH-Rechtsprechung erinnern.</p> <p>Vereinfacht formuliert, hatte das EUGH nämlich keine Probleme mit dem Monopol, wenn zwei Punkte erfüllt werden sollen</p> <ul style="list-style-type: none"> <li>- Kriminalitätsprävention</li> <li>- Suchtprävention</li> </ul> <p>Darf man bei der Einhaltung von kriminalpräventiven Gesichtspunkten dann "die technische Möglichkeit der Manipulation" zulassen oder muss man diese strikt abschaffen?</p> <p>Gruß Meike</p>
<p><a href="#">dieter116</a> 28.08.2008 08:46</p>	<p>Die Fragen haben wohl weniger mit Prüfern zu tun, als mit dem Zulassungsverfahren der PTB.</p> <p>Inwieweit wird hier die Software auf Konformität mit der SpVO geprüft ?</p> <p>Liegen der PTB Quelltext und eine komplette Dokumentation detr Software vor ?</p> <p>Die Hersteller werden sicherlich an Aufsteller keine Informationen über nur von ihnen eventuell zu nutzende 'Zusatzfunktionen' ihrer Gerätesoftware geben. Und von aussen erkennbar ( für OÄ z.B. ) dürften die wohl auch nicht sein.</p>

In diesem Thema befinden sich folgende Anhänge: