HbbTV – I Know What You Are Watching

Marco Ghiglieri, Florian Oswald, Erik Tews[1]

Kurzfassung:
Die Vernetzung von Geräten nimmt stetig zu; so ist dieser Trend auch in der Unterhaltungsbranche zu beobachten. Im Handel können bereits TV-Geräte und Zubehörprodukte wie Blu-ray Player oder Set-Top-Boxen mit Netzwerkanschluss erworben werden.
Mit dieser Schnittstelle besteht die Möglichkeit, eine Verbindung zum Internet aufzubauen. Spezielle für diese Geräte geschaffene Dienste im Internet bieten mittlerweile eine Reihe von Vorteilen für vernetzte Unterhaltungselektronik.
Ein Beispiel dafür ist HbbTV, welches Internet und DVB-Empfang auf dem Fernseher kombiniert und damit den Kunden einen Mehrwert für das laufende TV-Programm bietet. Sendeanstalten können so zusätzliche Inhalte zum laufenden Programm oder auch zu vergangenen Sendungen direkt auf dem Fernseher zur Verfügung stellen.
Wir beschreiben in dieser Arbeit, wie Sendeanstalten das Nutzungsverhalten ihrer Zuschauer mit HbbTV noch genauer messen und welche Techniken dazu eingesetzt werden können. Die dabei gewonnenen Informationen sind aus Datenschutzaspekten durchaus als bedenklich einzustufen. Weiterhin zeigen wir, dass auch ein Dritter das Nutzungsverhalten ohne Kooperation des Zuschauers oder der TV-Sender aufzeichnen kann, falls der Zuschauer einen HbbTV tauglichen Fernseher mit WLAN verwendet. Das ist selbst dann möglich, wenn das WLAN mit Hilfe von WPA2 abgesichert wurde.

Stichworte: Aufklärung und Sensibilisierung, Datenschutz, Smart-TV, HbbTV

1. Einleitung

Mit der Einführung von Smart-TV oder auch Connected TV-Geräten setzt sich der allgemeine Trend zur Vernetzung von elektronischen Geräten auch in der Unterhaltungselektronik durch. Dieser Trend ist somit auch bei TV-Geräten, die Smart-TV oder auch Connected TV-Geräte (im folgenden Smart-TV) von den Herstellern genannt werden, zu erkennen. Diese Geräte finden immer mehr Verbreitung bei den Nutzern; so ist eine umlaufende Anzahl von 20,1 Millionen Geräten für 2016 in Deutschland prognostiziert [1].
Smart TVs verbinden zwei Medien miteinander, DVB (Digital Video Broadcast) und das Internet, und stellen somit ganz neue Funktionen auf TV-Geräten bereit. Eine dieser Funktionen ist bekannt unter dem Namen HbbTV (Hybrid Broadcast Broadband TV), die es ermöglicht, interaktive (übertragungsabhängige sowie auch unabhängige) Inhalte auf ein Smart-TV auszuliefern. Die neueste Spezifikation von HbbTV ist von der ETSI im November 2012 freigegeben worden [2]. Sie spezifiziert, wie eine HbbTV-Anwendung grafisch sowie technisch aufgebaut werden sollte. Die Verbreitung von HbbTV-fähigen TV-Geräten wird bis zum Jahr 2016 auf wahrscheinlich 13,4 Millionen Geräte (35% aller Haushalte [3]) in Deutschland steigen [4].

[1] Technische Universität Darmstadt/CASED & ECSPRIDE, Fachbereich Informatik, Darmstadt

Die bei HbbTV übertragenen Inhalte bieten vielfältige interaktive Möglichkeiten sowohl für den Nutzer als auch für Werbetreibende. Für den Nutzer bestehen die Vorteile beispielsweise im Abrufen von Inhalten aus Mediatheken, Wetterberichten aus dem Internet oder Zusatzinformationen zu laufenden Programmen. Eine Umfrage der GfK bestätigt die steigende Akzeptanz dieses neuen Mediums [5]. Ein Vorteil auf der Seite der Werbetreibenden ist, dass das Anbieten von lokaler Werbung möglich ist und direkt gemessen werden kann, wie viele Werbemittelkontakte es gab. Mehreinnahmen von 350 Tsd. Euro bis 930 Tsd. Euro können so von beispielswiese den bayerischen regionalen TV-Sendern erwirtschaftet werden [3]. Weiterhin kann HbbTV in Zukunft den heutigen Teletext (Videotext) ersetzen, so ARTE in einer Mitteilung auf der Unternehmenswebseite [6].
Wir zeigen in dieser Arbeit, dass die Verwendung von HbbTV nicht nur Vorteile für den Nutzer bietet, sondern auch weitreichende Datenschutzprobleme mit sich bringt. Bei den im Broadcast-Verfahren ausgestrahlten Sendern, welche über DVB-S/-T/-C[2] empfangen werden können, und keinen Rückkanal zur Sendeanstalt oder zu anderen Dritten bieten, wird das Nutzungsverhalten des Nutzers nicht direkt offen gelegt, so dass dort keine zusätzlichen Datenschutzprobleme entstehen. Wird hingegen HbbTV eingesetzt, kann das Nutzungsverhalten von Sendeanstalten und potentiell auch gegenüber Dritten ausgewertet werden.

1.1. Unser Beitrag

In dieser Arbeit zeigen wir, dass

- in Deutschland und in Österreich bereits verschiedene Mechanismen zum Einsatz kommen, die es sowohl der Sendeanstalt selbst als auch anderen Dritten ermöglichen, das Nutzungsverhalten des Nutzers zu erfassen,
- der HbbTV-Standard keine Hinweise zur Implementierung einer datenschutzfreundlichen HbbTV-Anwendung enthält,
- die HbbTV-Anwendungen in der Praxis teilweise mehr Daten erhebt als für die korrekte Funktion der Anwendung notwendig wären,
- es auch mit aktueller Verschlüsselung in drahtlosen Netzwerken möglich ist, Nutzungsverhalten durch Dritte ohne Kooperation der Sender oder des Nutzers zu erheben.

Wir gehen in dieser Arbeit nicht auf rechtliche Aspekte der Übertragungen ein und bleiben bei einem rein technischen Standpunkt.

1.2. Verwandte Arbeiten

Nach unserem Kenntnisstand ist dieses Papier das erste, das sich mit Datenschutz in Smart-TVs, im Speziellen HbbTV beschäftigt.
Es gibt einige Arbeiten, die das Thema HbbTV diskutieren. Eine technische Beschreibung einer Implementierung sowie der Evaluierung ist in [7] zu finden. Es wird eine Middleware vorgestellt, die HbbTV Funktionalität implementiert.

[2] Satellit (DVB-S), Terrestrisch (DVB-T), Kabel (DVB-C)

Eine weitere Arbeit [8] beschreibt die Probleme beim Aufzeichnen von Übertragungen mit HbbTV-Anwendungen und das Wiedergeben der Inhalte. Der Nutzer soll das gleiche Erlebnis haben als würde er die Sendung bei Erstausstrahlung ansehen.
Entfernter erschienen Arbeiten, die Sicherheitslücken in Smart-TVs aufdeckten um vor allem Angriffe auf das darunterliegende Betriebssystem darzustellen [9,10]. Parallel zu dieser Arbeit ist eine studentische Arbeit entstanden, die auch weitere Sicherheitslücken aufdeckt [11].

1.3. Aufbau des Papiers

Im ersten Kapitel führten wir kurz in das Thema und den Trend in der Unterhaltungselektronik ein. Im zweiten Kapitel erläutern wir den zugrundeliegenden HbbTV-Standard und gehen in Kapitel drei auf die angewandte Praxis ein. In Kapitel vier geben wir unsere Analysen an und geben in Kapitel fünf einen Ausblick auf die möglichen Gegenmaßnahmen. Im letzten Kapitel schließen wir dieses Papier mit einem Fazit und dem Ausblick ab.

2. HbbTV-Standard

In diesem Kapitel stellen wir kurz die im Abschnitt 5.3 des HbbTV-Standards [2] beschriebenen Möglichkeiten vor, wie sich ein HbbTV-Sender einem Nutzer präsentieren sollte. Die Zusatzfunktionalitäten werden im Folgenden HbbTV-Anwendung (oder Anwendung) genannt. Technisch gesehen, ist eine HbbTV-Anwendung eine Webseite, die üblicherweise zu einem großen Teil transparent ist und über das Fernsehbild gelegt wird. Die URL dieser Seite wird von den Sendeanstalten im DVB-Datenstrom übertragen und vom Fernseher ausgewertet. Eine Übertragung der eigentlichen Inhalte selbst findet über DVB nicht statt. Die Webseiten werden aus dem Internet geladen und können über JavaScript oder andere Web-Techniken im Aussehen und Verhalten verändert werden. Im Rahmen dieser Arbeit gehen wir auf die Grundfunktionalitäten ein, die für das Verständnis des Sachverhaltes notwendig sind.

2.1. Aktivierung einer HbbTV-Anwendung auf dem Smart-TV

Es sind fünf verschiedene Varianten in [2] beschrieben, wie eine HbbTV-Anwendung gestartet werden kann:

1. Zugriff auf eine übertragungsabhängige Autostart-Anwendung beim Drücken des „Red Button“ auf der Fernbedienung des Smart-TVs.
2. Starten einer digitalen Textanwendung beim Drücken des „TEXT“ Button auf der Fernbedienung des Smart-TVs.
3. Starten einer übertragungsunabhängigen Anwendung über das Internet TV-Portal des Fernsehers (falls eines existiert).
4. Starten einer weiteren Anwendung in einer bereits laufenden Anwendung.
5. Auswahl eines Kanals, welcher einen Autostart für Anwendungen sendet. Diese startet dann im Vollbild (normalerweise nur bei Radio- oder reinen Datenkanälen).

In dieser Arbeit betrachten wir nur übertragungsabhängige Anwendungen, die beim Drücken auf den „Red Button“ aktiviert werden (siehe Variante 1).

2.2. Status der übertragungsabhängigen HbbTV-Anwendungen

Eine HbbTV-Anwendung kann sich laut Standard in einer der drei folgenden Sichtbarkeitszustände befinden:

1. Anzeigen des „Red Button“ auf dem Bildschirm zur Benachrichtigung, dass eine Anwendung verfügbar ist.
2. Es wird keine Benutzeroberfläche angezeigt.
3. Anzeigen der Benutzeroberfläche im Vollbild

Weiterhin ist spezifiziert, dass eine Anwendung nicht direkt im Vollbild starten sollte, sondern der Benutzer nur informiert werden soll, dass eine Anwendung verfügbar ist. Weitere Anwendungsteile sollen erst bei Drücken des Red Button aktiviert werden.
Die HbbTV Spezifikation in der aktuellen Version [2] hat keinen Hinweis auf Benutzerdatenschutz oder Schutz der Privatsphäre.

3. HbbTV in der Praxis

HbbTV ist von vielen TV-Sendern in Deutschland bereits im Einsatz. Darunter sind die ARD-Gruppe mit vielen regionalen Sendern, die ZDF Gruppe, Arte, RTL, Vox, Kabel eins, Pro7, Sat.1, Anixe, QVC und noch einige mehr (vgl. Tabelle 1).
Wir haben das HbbTV-Verhalten aller oben aufgeführten Sender über einen Zeitraum von sechs Monaten untersucht. Sender ohne HbbTV wurden nicht untersucht, da diese kein erhöhtes Datenschutzrisiko durch HbbTV haben. Bei HbbTV-Sendern konnten einmalige und periodische Internetanfragen festgestellt werden:

Einmalige Anfrage: Nach Einschalten des Senders wurden einmalig HTTP-Anfragen an den Server des Senders gesendet, der daraufhin einen „Red Button“ ausliefert oder, wenn keine Applikation zur Verfügung steht, keinen weiteren Inhalt ausliefert. Jeder HbbTV Sender, der ein „Red Button“ ausliefert, führt eine einmalige Anfrage durchführen.
Periodische Anfragen: Zusätzlich zur einmaligen Anfrage wurden periodische Internetanfragen in einem Zeitabstand von einer Sekunde bis 15 Minuten festgestellt. Der „Red Button“ wurde zu diesem Zeitpunkt noch nicht vom Benutzer gedrückt.

Gleich ist bei allen Anfragen, dass sie an einen Server der jeweiligen Sendeanstalt/-gruppe gesendet werden und daraufhin verschiedene Inhalte ausgeliefert werden. Die darüber übertragenen Daten sind senderspezifisch und werden durch die Sendeanstalt bestimmt. Wir haben keine Zugriffe auf Server des Fernsehherstellers feststellen können und somit keinen Zusammenhang zwischen HbbTV und dem jeweiligen Herstellern.

Die Funktionalität der HbbTV-Anwendung nach Drücken des „Red Button“ ist sehr unterschiedlich und reicht von einem Ersatz des bekannten Teletextes (Videotext) bis hin zu umfangreichen Mediatheken mit der Möglichkeit vergangene Sendungen abzurufen. Ab dem Zeitpunkt, nachdem der „Red Button“ gedrückt wurde, ist für den Nutzer klar erkennbar, dass er einen Zusatzdienst aus dem Internet außerhalb des herkömmlich übertragenen Fernsehprogramms nutzt.

4. Analyse

In diesem Kapitel diskutieren wir im Detail, welche Daten versendet und empfangen werden, dabei werden wir die Sender in verschiedene Gruppen einteilen. Wir beginnen mit dem Testaufbau und folgen dann mit den Ergebnissen im Detail.

4.1. Testumgebung

Als Testgeräte standen uns zwei Geräte von Samsung[3] zur Verfügung: UE40D6200, UE40ES6300. Beide Geräte verfügen über Triple-DVB Receiver und können somit ein TV-Signal auf allen Sendewegen empfangen und verarbeiten. Das erst genannte Smart-TV diente zur Verifizierung der Ergebnisse auf unserem Referenzgerät UE40ES6300. Beide Geräte verfügen über die Funktion „Datendienste“, die nicht eindeutig als HbbTV erkennbar ist.

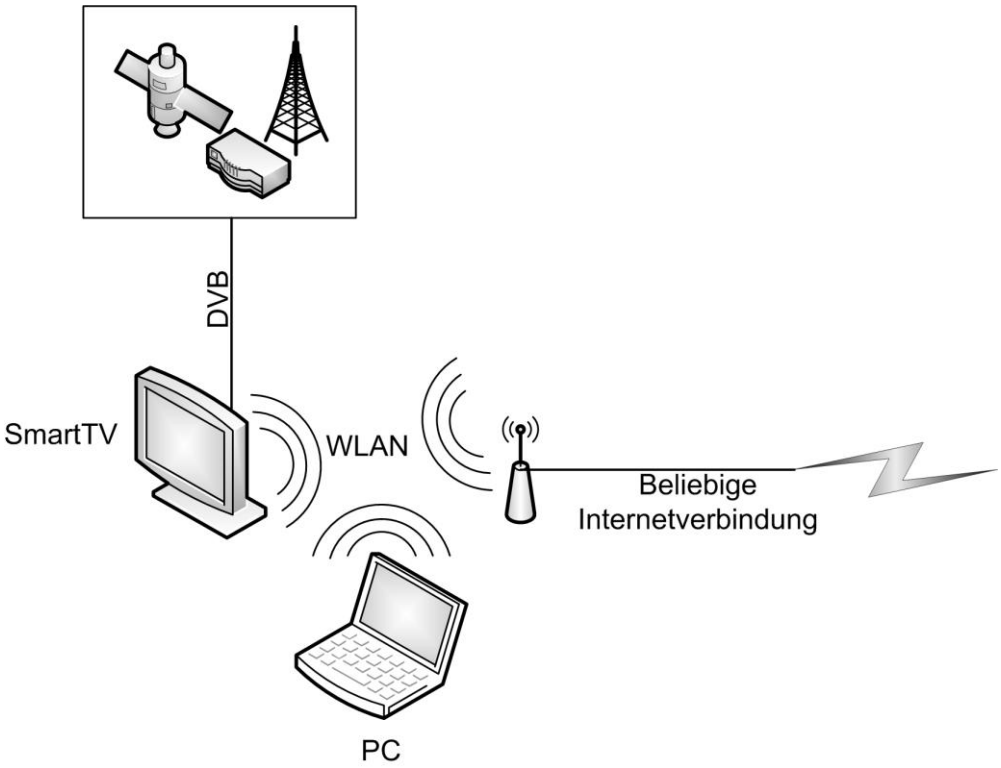

Abbildung 1: Aufbau Testumgebung

[3] Wir möchten an dieser Stelle hervorheben, dass das Verhalten nicht Samsung-spezifisch ist, sondern alle HbbTV-kompatiblen Endgeräte betreffen, die den Standard umsetzen.

In Abbildung 1 ist der technische Aufbau skizziert und beschreibt die einzelnen Wege zum Empfang und Analyse des Datenstroms. Das Smart-TV ist mit DVB verbunden und über WLAN baut es eine Verbindung zum Internet auf. Ein beliebiger PC, der nicht im heimischen Netz ist und das WLAN Signal empfängt, ist in der Lage, die Datenpakete von und zum Smart-TV auf dem WLAN Kanal (verschlüsselt oder unverschlüsselt) mitzulesen.
Für die Analyse in Kapitel 4.2 wurde die Verschlüsselung komplett deaktiviert, damit übertragende Pakete direkt lesbar sind. Im Gegensatz dazu wurde in Kapitel 4.3 WPA2 als Verschlüsselung eingesetzt. WPA2 ist derzeit die Standardmethode, um eine abhörgeschützte Verbindung über ein WLAN zu realisieren.

4.2. Analyse

Das Verhalten der HbbTV-Sender wurde auf allen Sendearten DVB-C/-S/-T analysiert und keine signifikanten Unterschiede festgestellt; deshalb sind alle Messungen für alle Empfangswege gültig. Systematisch wurden die gesichteten Netzwerkpakete in folgende Zeitphasen eingeteilt:

- Einschalten des Senders bis Einblenden des „Red Button“ (Phase 1),
- Einblenden des „Red Button“ bis Drücken des „Red Button“ (Phase 2) und,
- Drücken des „Red Button“ und Ausführen der HbbTV Anwendung (Phase 3).

Phase 3 ist in unserer Analyse nicht betrachtet worden, da dies das Starten der HbbTV-Anwendung darstellt und der Nutzer eine Interaktion mit dem Internet erwartet. Der Schwerpunkt unserer Analyse lag auf den Phasen 1 und 2, bei denen der Nutzer keine Interaktion des Smart-TVs mit dem Internet erwartet. In den Phasen 1 und 2 konnten wir einmalige und periodische Anfragen feststellen, die wir nach Häufigkeit der Anfrage einteilen. Wird eine Anfrage nur dafür benötigt, um den „Red Button“ einzublenden, und in Phase 2 ist keine gleichartige Anfrage, reden wir von einmaliger Anfrage (siehe Abbildung 2).

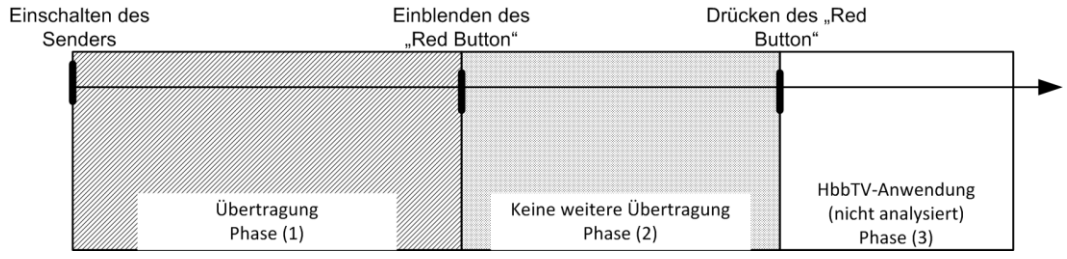

Abbildung 2: Einmalige Anfragen

Wiederholt sich die Anfrage von Phase 1 auch in Phase 2 oder beginnt in Phase 2 und wiederholt sich laufend, reden wir von periodischer Anfrage (siehe Abbildung 3).

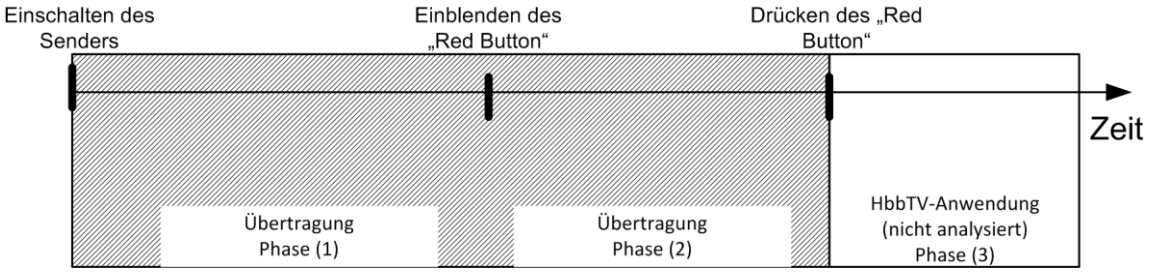

Abbildung 3: Periodische Anfragen

Eine Anfrage erfolgt dabei immer vom Smart-TV zu einem Server im Internet, eine Antwort durchläuft die Gegenrichtung. Die Anfrage beim Smart-TV wird initial beim Einschalten des Senders über ein Signal, welches im DVB-Signal empfangen wird, übertragen und kann dann durch die Antwort vom Server beeinflusst werden.
Unsere Messungen haben gezeigt, dass periodische Anfragen in einem Abstand von einer Sekunde bis hin zu 15 Minuten bei einigen Sendern getätigt werden.
Die Analyse der Datenpakete, die bei den periodischen Anfragen übertragen wurden, konnten wir in folgende Kategorien einteilen:

- Vorladen des Inhalts für die HbbTV-Anwendung,
- Tracking-Skript (auch von Drittanbietern) und
- (personalisierte) Werbeeinblendungen.

Daraus haben wir die Sendergruppen wie folgt gebildet (siehe auch Tabelle):

- Sendergruppe A: Einmalige Anfragen für Einblenden des „Red Button“ auf dem Bildschirm des Nutzers
- Sendergruppe B: Eigenschaften von Sendergruppe B erweitert durch die periodische Anfrage, um den Inhalt der HbbTV-Anwendung im Voraus aktuell zu halten.
- Sendergruppe C: Eigenschaft von B erweitert um Trackingskripte von dritten Dienstleistern (z.B. Google Analytics)
- Sendergruppe D: Eigenschaften von Sendergruppe A erweitert mit personalisierter Werbung, die in Zeitabständen von 15 Minuten eingeblendet wird.

Im Folgenden zeigen wir den Verlauf jeder Sendergruppe im Zusammenhang.
Die initiale Anfrage des „Red Button“ wird mit dem DVB-Signal übertragen und veranlasst ein Smart-TV, eine bestimmte URL im Internet aufzurufen. Als Antwort werden Senderlogo-Bilder und verschiedene JavaScripte, die das Starten der Anwendung erlauben, übertragen. Der „Red Button“ wird nach erfolgreichem Laden dem Nutzer im unteren Bildbereich angezeigt. Dieser signalisiert, dass eine HbbTV-Anwendung verfügbar ist und durch Drücken des „Red Button“ im Vollbild erscheint. (Sendergruppe A-D)

Gruppe	Sender	Eigenschaften						
		HbbTV	Einmalige Anfrage	Periodische Anfrage	Tracking	Datenüber-mittlung an Dritte	personalisierte Werbung	WPA2 – Tracking möglich
A	ZDF (HD), ZDF Infokanal, ZDFneo, 3Sat (HD)	x	x	-	-	-	-	x
A	Bibel TV	x	x	-	-	-	-	x
A	QVC (HD)	x	x	-	-	-	-	x
B	ARD-Gruppe (Erste (HD), hr-fernsehen, SWR, SR, rbb, EinsPlus, EinsExtra, EinsFestival, WDR, NDR, MDR, SWR, MDR, br alpha, Phoenix (HD), br	x	x	x	-	-	-	x
C	ProSiebenSat1-Gruppe(Pro Sieben, Kabel 1, Sat 1)	x	x	x	x	x[4]	-	x
C	ARTE (HD)	x	x	-	x	x	-	x
C	Puls 4 Austria	x	x	x	x	x	-	x
C/D	Sonnenklar TV	x	x	x	x	-	-	x
D	Anixe (HD), Anixe iTV	x	x	x	x	-	x	x
-	RTL, VOX	x	HbbTV der RTL-Gruppe ist auf unseren Testgeräten nicht verfügbar[5].					x
-	n-tv	x	x[6]	-	-	-	-	x

Tabelle 1: Übersicht der Sender

Bei den Sendergruppen B-D sind periodische Anfragen, bevor der Benutzer den „Red Button“ drückte und damit die Anwendung wissentlich aufruft, aufgefallen.
Diese Anfragen an den Server der Sendergruppe geschehen im Abstand von einer Sekunde bis mehreren Minuten. Der Abstand der Anfragen ist je nach Sendergruppe unterschiedlich. Diese periodischen Anfragen werden im

[4] Chartbeat.com, Google Analytics und Webtrekk
[5] Nur von der RTL-Gruppe zertifizierte Geräte können HbbTV verwenden.
[6] „Red Button“ wurde nicht angezeigt.

Allgemeinen in Web-Anwendungen (wie oben beschrieben, wird die Technik auch bei HbbTV genutzt) für das Aktualisieren von Inhalten oder das Verfolgen von Nutzern eingesetzt.
Eine Aktualisierung der Inhalte in hoher Frequenz ist bei noch nicht aktivierter Anwendung aus unserer Sicht technisch nicht notwendig. Das Verfolgen von Nutzern ist bei Sendergruppe C und D dadurch bestätigt worden, dass Fremdanbieter wie Google Analytics, Chartbeat.com und Webtrekk zum Einsatz kommen. Diese sind eindeutig einem Tracking zuzuordnen und verstoßen so gegen das mentale Modell des Benutzers, der nur eine Interaktion mit dem Internet erwartet, wenn er auch den „Red Button“ drückt.
In der Zeit, in der ein Smart-TV (versteckte) HbbTV-Inhalte über das Internet abruft, muss der jeweilige Sender eingeschaltet sein, da die Architektur von HbbTV dies so vorsieht. Uns ist nicht bekannt, wie diese Daten durch die Sender ausgewertet werden, jedoch alleine die Möglichkeit deutet auf ein erhöhtes Datenschutzproblem hin.
Genutzt werden können diese Daten, um die Einschaltquoten in einem noch genaueren Maße festzustellen und so sogar in Echtzeit Inhalte des Programms zu verändern.
In Sendergruppe D konnten wir Vollbildwerbung mit einem Abstand von 15 Minuten beobachten. Diese Werbung enthält auch Geo-Daten unseres Einwahlstandorts in der URL. Wir stufen dies nicht als weiteres Risiko ein, da dieser Standort durch die IP-Adresse immer (auch versteckt) ermittelt werden kann. Als Nutzer erwartet man dies jedoch nicht.
Die meisten Internet-Provider teilen eine IP-Adresse 24 Stunden einem Nutzer zu, somit ist der Nutzer mindestens über diesen Zeitraum eindeutig identifizierbar. Als Unterstützung nutzt man im Internet gewöhnlich Cookies, die eine Identifizierung auch über die 24 Stunden hinaus zulassen, allerdings haben unsere Testgeräte zwar Cookies empfangen, aber diese nicht wieder an den Server zurückgesendet. Hier ist nicht abschließend geklärt, ob es sich um einen Implementierungsfehler oder um eine datenschutzfreundliche Implementierung des Herstellers handelt. Falls die Cookies angenommen werden würden, gäbe es keine einfache Möglichkeit für den Nutzer, diese zu löschen oder gar zu verhindern.

4.3. Analyse mit verschlüsseltem WLAN

Wir haben ebenfalls eine Analyse mit verschlüsseltem WLAN durchgeführt, und das Ergebnis zeigte, dass neben den Sendeanstalten und ihren Dienstleistern auch Dritte die Möglichkeit (im weiteren Angreifer genannt) haben, das Nutzungsverhalten mit aufzuzeichnen.
Der Angreifer muss sich lediglich in der Reichweite des WLANs des Nutzers befinden. Ein erfolgreiches Abhören ist selbst dann möglich, wenn das WLAN nach dem aktuellen Stand der Technik mit WPA2 gesichert ist, und der Netzwerkschlüssel nicht einfach durch Raten bestimmt werden kann.

Bei WPA2 wird AES-CCMP oder TKIP zur Verschlüsselung der Netzwerkpakete eingesetzt. Bei beiden Verfahren (wie auch bei WEP) wird der Klartext des Paketes mit einer Stromchiffre (RC4 bei WEP und TKIP, AES im Counter-Mode bei AES-CCMP) verschlüsselt, und es wird anschließend noch ein Block fester Länge zur Integritätssicherung angehängt. Ein Padding, wie bei Blockchiffren üblich, welches die Länge des Klartextes verschleiern würde, ist nicht vorgesehen. Ebenso wird die MAC-Adresse des Senders bzw. Empfängers des Paketes im Klartext übertragen. Ein Angreifer kann so immer die Hersteller aller Geräte in einem WLAN bestimmen, so wie die Länge aller Klartexte der verschlüsselt übertragenen Datenpakete [12].

Alle von uns untersuchen HbbTV-Anwendungen bestehen im Wesentlichen aus einer Benutzeroberfläche, die sich selten ändert, sowie einer Art von Konfigurationsdatei, die sich auf das aktuelle Programm bezieht und oft geändert wird. Alle dafür benötigten Daten werden beim Einschalten des HbbTV-Senders per HTTP geladen. Die vom Client gesetzten HTTP-Header können je nach User-Agent in ihrer Länge variieren, die vom Server gesetzten HTTP-Header waren aber in unserem Test immer von gleicher Länge. Die Menge der abgerufenen Daten sowie die Größe der einzelnen Datenpakete variiert von Sender zu Sender. Zwischen den einzelnen Sendergruppen gab es allerdings in unseren Tests immer Unterschiede in der Paketgröße.

Um HbbTV-Sender alleine über die verschlüsselte Datenübertragung über ein WPA2 gesichertes WLAN identifizieren zu können, haben wir folgende Technik benutzt: Ein Angreifer probiert auf seinem eigenen Smart-TV alle HbbTV-Sender und erstellt zuerst für jeden Sender bzw. Sendergruppe eine Liste von charakteristischen Paketgrößen. Paketgrößen, die bei mehr als nur einer Sendergruppe zu finden sind, werden nicht berücksichtigt. Paketgrößen, die zu Inhalten gehören, die ggf. vom Browser zwischengespeichert werden, müssen anschließend aus der Liste entfernt werden.

Danach schneidet der Angreifer den gesamten verschlüsselten WLAN-Datenverkehr mit. Mit Hilfe der MAC-Adresse werden nur die Datenpakete für das Smart-TV ausgewählt. Da nur die Antworten auf HTTP Anfragen interessant sind, werden Pakete ausgewählt, die vom Access Point zum Smart-TV übertragen werden. Ein weiterer Filter entfernt alle Datenpakete, die volle MTU Größe haben. Mit einer Sliding-Window Methode werden dann alle Paketgrößen, die innerhalb eines Intervalls von 10 Sekunden zu sehen waren, mit der Liste verglichen. Sind alle Paketgrößen, die zu einem Sender gehören, in diesem Zeitfenster vorhanden, kann man davon ausgehen, dass dieser Sender auf dem Smart-TV eingeschaltet wurde.

Bei unseren Experimenten ist es uns nicht gelungenen, mit dieser Methode falsche Treffer zu erzeugen (sog. false positives). Schaltet man allerdings einen HbbTV-Sender für wenige Sekunden ein, und wechselt sehr schnell danach auf einen anderen Sender, so wird die HbbTV-Applikation in dieser Zeit nicht vollständig geladen, und von unserem Angreifer der Sender so auch nicht erkannt.

Erfolgt der Internetzugang über DSL mit PPPoE oder über ein VPN, so dass das Smart-TV nicht die volle Paketgröße von 1500 Bytes verwenden kann, muss die Liste von charakteristischen Paketgrößen an diese Umgebung angepasst werden. Eine mögliche Erweiterung dieser Angriffstechnik wäre es, zusätzliche Timing-Informationen und die Datenmenge mit zu verwenden, da unser Angriff aber bereits sehr zuverlässig funktionierte, haben wir ihn nicht weiter entwickelt.

5. Mögliche Gegenmaßnahmen

Da es sich im Feld der Unterhaltungselektronik um noch eine neue Technik handelt, sind die umsetzbaren Sofortmaßnahmen beschränkt. Einige Lösungen lassen sich nur mit langer Umsetzungszeit implementieren.
Die möglichen Gegenmaßnahmen lassen sich grob anhand der Quelle der Änderungen in die Kategorien: HbbTV-Standard, HbbTV-Anwendungen und HbbTV-Endgeräte einteilen.

5.1. HbbTV-Standard

Die Spezifikation des HbbTV-Standards zeigt kein Indiz dafür, dass es sinnvoll ist, bei der Entwicklung Privacy by Design als Entwicklungsprinzip von HbbTV-Anwendungen zu berücksichtigen. Die Spezifikation sollte so erweitert werden, dass auch einige konkrete Richtlinien zum Datenschutz enthalten sind. Zum Beispiel wäre das Festlegen einer Liste der Funktionen vor Drücken des „Red Button“ erstrebenswert. Der HbbTV-Standard sollte die Übertragung des „Red Button“ standardisieren, so dass es nicht möglich ist, anhand des ersten Pakets Rückschlüsse auf den Sender zu ziehen. Dies bedeutet, dass bestimmte Techniken wie das Auffüllen mit Füllzeichen angedeutet werden können, um die Paketgrößen ununterscheidbar zu machen.
Des Weiteren sollte ausdrücklich im Standard verboten werden, Tracking-Skripte zu nutzen, bevor die Anwendung wissentlich durch den „Red Button“ aktiviert wurde.

5.2. Technische Änderungen der Empfangsgeräte

Die Empfangsgeräte stellen, wie bei anderen Endgeräten, den Browser zur Verfügung, um die HbbTV-Inhalte anzeigen zu lassen. Leider sind die HbbTV-Browser so minimal, dass auch übliche Funktionalitäten in aktuellen Webbrowsern, wie die Cookie-Verwaltung nicht vorhanden sind oder die Erweiterung mit datenschutzfördernden Erweiterungen nicht vorgesehen ist. In heutigen Browsern auf Desktop PCs lassen sich eine ganze Reihe Gegenmaßnahmen (AdBlock, NoScript, Cookies verbieten) umsetzen, die so leider architekturbedingt nicht auf Smart-TVs funktionieren.
Wir konnten feststellen, dass in den Einstellungen unserer Testgeräte Datendienste aktiviert werden können, aber die möglichen Risiken nicht dem Nutzer auf dem Smart-TV dargestellt werden. Eine Einstellung pro Sender wäre

sehr wünschenswert. So kann jeder Benutzer entscheiden, ob er wirklich HbbTV auf bestimmten Sendern benötigt, und so das Risiko minimiert, unbemerkt getrackt zu werden.
Ein restriktiverer Ansatz wäre, dass der „Red Button“ nicht mehr aus dem Internet abgerufen wird, sondern direkt vom TV-Gerät eingeblendet wird, sobald das Signal im DVB Stream erkannt worden ist. Dadurch würde keine Verbindung mit dem Server des Senders beim Einschalten des Senders aufgebaut werden, allerdings geht die Individualisierung jeweiliger Senderlogos verloren. Dieser Ansatz könnte optimiert werden, indem man Caching-Mechanismen verwendet, die Logos speichern.

5.3. Änderungen an den HbbTV-Anwendungen

HbbTV-Anwendungen sollten nach dem Ansatz Privacy by Design konzipiert werden und möglichst wenige Daten an den Server schicken. Der Benutzer sollte die Möglichkeit haben, zu kontrollieren, ob Trackingskripte verwendet werden. Dies könnte durch ein einmaliges Setzen einer Option auf dem Fernseher geschehen. Die Anwendung müsste dies dann umsetzen.

Eine weitere Gegenmaßnahme, die aber auch Verlust einiger Vorteile mit sich bringen würde, wäre das komplette Deaktivieren der Datendienste. Doch Smart-TVs werden gerade mit diesen neuen Funktionen vermarket. Damit die Nutzer von der Vielfalt der Informationen und Inhalten profitieren können, ist eine datenschutzfreundlichere Implementierung wünschenswert.

6. Fazit & Ausblick

In diesem Papier zeigten wir, dass ein Datenschutzrisiko bei der Nutzung von HbbTV besteht. Wir haben anfangs nicht erwartet, dass bereits solche Möglichkeiten mit HbbTV bestehen. Nach unseren Untersuchungen stufen wir allerdings das Problem aktuell als akut ein. Die gesendeten Inhalte können nicht durch den Nutzer kontrolliert werden, und die einzige derzeitige Möglichkeit mit dem Problem umzugehen, ist das Abschalten der Datendienste, was ein Smart-TV überflüssig machen würde. Der Grund für die Datenschutzprobleme ist nicht auf der Seite des TV-Herstellers zu suchen, sondern bei den HbbTV-Anwendungen, die nicht in der Verantwortung des TV-Herstellers liegen.
Im Internet ist es üblich, dass verschiedene Tracking Methoden verwendet werden. Dies muss gesondert in den Datenschutzbestimmungen einer Webseite aufgenommen werden. Im Gegensatz zu HbbTV geht der Nutzer wissentlich auf bestimmte Webseiten eines bestimmten Anbieters. Bei HbbTV jedoch wird der Inhalt automatisch ohne Wissen des Nutzers – sobald er Datendienste aktiviert hat – abgerufen und auch in einigen Fällen Tracking-Mechanismen verwendet.
Die Sendeanstalt hat die Möglichkeit durch gezieltes Tracking genauere Einschaltzahlen zu ermitteln, und dies sogar in Echtzeit, und personalisierte Werbung zu buchen.

Wir haben die hier gefunden Resultate sowohl gegenüber dem Gerätehersteller als auch den betroffenen Sendeanstalten kommuniziert. Samsung hat in dieser Angelegenheit signalisiert, dass keine HbbTV-Änderungen von Ihrer Seite durchgeführt werden, da die technische Implementierung standardkonform ist und die HbbTV-Anwendungen ganz in der Hand der Sendeanstalten liegt. Leider konnten wir feststellen, dass das Problem nur von wenigen Sendern ernst genommen wird. So konnten wir die Problematik lediglich mit einer Sendergruppe, die Bereitschaft zur Verbesserung gezeigt hat, diskutieren.

Ein Nebeneffekt, den wir als äußerst problematisch einstufen, ist, dass sogar das Abhören des Nachbars mit der von uns genannten Technik genaue Informationen darüber gibt, wie das Nutzungsverhalten seines Smart-TVs ist. Hier sollte dringend eine Anpassung gemacht werden, so dass Datenpakete nicht unterscheidbar sind.
Der Markt rund um smarte Unterhaltungselektronik ist noch recht neu, deswegen werden dort in nächster Zeit weitere Innovationen erwartet. Im Falle von Smart-TVs wäre es wünschenswert, wenn die Hardware mit bestimmten (bereits bekannten) Hardening Techniken gesichert werden würde. Anwendungen für Smart-TVs jeglicher Art sollten nach aktuellem Wissenstand entwickelt werden, um hier keine Neuarbeit leisten zu müssen.

7. Danksagung

Diese Arbeit wurde von ECSPRIDE (BMBF) und CASED (LOEWE) unterstützt.
Wir wollen an dieser Stelle Marit Hansen und Michael Waidner danken, die beide sehr wertvolles Feedback zu diesem Papier gegeben haben.
Wir danken auch für die informativen Gespräche mit dem ARD Play-Out-Center Potsdam (POC) und der Hauptstelle von Samsung.

Literatur

[1] Statista, Anzahl der Smart TV-Haushalte in Deutschland im Jahr 2010 und Prognose bis 2016 (in Millionen) (Quelle Goldmedia). URL: http://de.statista.com/statistik/daten/studie/208236/umfrage/ prognose-zur-entwicklung-der-smart-tv-haushalte-in-deutschland/ Oktober 2011.

[2] IRT GmbH, HbbTV Specification (approved by ETSI as ETSI TS 102 796 v1.2.1 in November 2012). http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf

[3] Bayerische Landeszentrale für neue Medien BLM, HbbTV beinhaltet Chancen für Lokalfernsehen - Smart-TV-Anwendungen können Reichweiten und Umsätze lokaler TV-Anbieter erhöhen. URL: http://www.blm.de/de/pub/aktuelles/pressemitteilungen.cfm?eventPress=press.DisplayDetail&pressrelease_ID=1741 April 2012.

[4] Statista. Anzahl der Haushalte (in Mio.) mit mind. einem an das Internet angeschlossenen TV-Gerät von 2011 bis 2016 (Quelle: BLM, Goldmedia).

http://de.statista.com/statistik/daten/studie/223468/umfrage/ prognose-der-smart-tv-entwicklung-nach-anteil-der-tv-geraete-in-deutschland/ Oktober 2011.

[5] Statista. Welche der folgenden Funktionen nutzen Sie mindestens 1x täglich bzw. mehrmals pro Woche auf ihrem Smart-TV ? URL: http://de.statista.com/statistik/daten/studie/223465/umfrage/nutzung-von-internetfaehigen-tv-geraeten/ November 2011.

[6] ARTE G.E.I.E. HbbTV - Der Standard für hybrides Fernsehen. URL: http://www.arte.tv/de/2153564,CmC=3977990.html Juni 2011.

[7] Z. Lukac, M. Radonjic, B. Veris, T. Maruna, and N. Kuzmanovic. The experience of implementing a hybrid broadcast broadband television on network enabled tv set. In MIPRO, 2011 Proceedings of the 34th International Convention, pages 840-844, may 2011.

[8] J. Dufourd, S. Thomas, and C. Concolato. Recording and delivery of hbbtv applications. In Proceedings of the 9th international interactive conference on Interactive television (EuroITV'11), pages 51-54, 2011.

[9] Heise, Sendepause durch Firmware-Lücken vom 24.04.2012, URL: http://www.heise.de/security/meldung/Sendepause-durch-Firmware-Luecken-1557589.html 11.01.2013

[10] Heise, Samsung-TVs: Smart, aber unsicher vom 21.12.2012, URL:http://www.heise.de/security/artikel/Samsung-TVs-Smart-aber-unsicher-1773710.html, 11.01.2013

[11] TU-Darmstadt, Sicherheit in der Informationstechnik, URL: http://www.sit.informatik.tu-darmstadt.de/de/security-in-information-technology/student-projects-theses/, 11.01.2013

[12] IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) pp.1-2793, March 29 2012 doi: 10.1109/IEEESTD.2012.6178212