RUHR-UNIVERSITÄT BOCHUM

50 Jahre

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

50 JAHRE FAKULTÄT FÜR ELEKTROTECHNIK UND INFORMATIONSTECHNIK

IT-SICHERHEIT

Smartphones, Browser, Ladesäulen schützen

PLASMAFORSCHUNG

Kunststoffe dichter machen und Keime töten

#25 Jahrgang
Sonderheft | 2015
4,00 Euro

DIE INTERNETPOLIZEI

Die Liste der Datendiebstähle im Internet wird immer länger. Auch das Team am Lehrstuhl für Netz- und Datensicherheit hat Know-how, das man für solche Angriffe braucht. Doch sie setzen es ein, um Sicherheitslücken zu finden und zu schließen.

Wenn man Prof. Dr. Jörg Schwenk vom Lehrstuhl für Netz- und Datensicherheit bei seinen Erzählungen über die Risiken des Internets zuhört, kann einem Angst und Bange werden, und man fragt sich, ob nicht just in diesem Moment das eigene Bankkonto durch skrupellose Internetbanditen leer geräumt wird. Dabei, so Jörg Schwenk, könnte das Internet durchaus sicherer sein, als es aktuell ist. Doch noch immer geht Funktionalität vor Sicherheit. „Den Nutzern ist es wichtig, dass Anwendungen wie zum Beispiel Browserspiele schnell laufen, und dass ständig neue Anwendungen über neue Browserfeatures ermöglicht werden. Diese Komplexität geht immer zulasten der Sicherheit“, sagt der IT-Experte.

Am Lehrstuhl von Jörg Schwenk hat man sich auf die Sicherheit von Webanwendungen spezialisiert. „Auf der Ebene der Betriebssysteme gibt es bereits viele Produkte zum Schutz vor Angriffen, zum Beispiel Antivirenscanner“, so Schwenk. Seine Forschung findet jedoch auf der Ebene der Webbrowser statt, und die bieten von sich aus nur geringen Schutz. Ursprung dieser Misere sind die sogenannten Browserkriege. Als Microsoft in den 90er-Jahren die Firma Netscape vom Markt drängte und später Google mit dem Browser Chrome vorpreschte, hatte dieser Kampf um Marktanteile Folgen für die Sicherheit im Internet. Die Anbieter bauten möglichst viele Features in die Browser ein, denn das sicherte ihnen die Gunst der Anwender. Allerdings achteten die Entwickler der Browserfirmen nicht allzu sehr auf Sicherheit, und so wiesen die Programme damals wie heute Schwachstellen auf. Angreifer können die Programmiersprache JavaScript nutzen, um eigenen bösartigen Programmcode einzuschleusen (Cross-Site Scripting, XSS). Den Hackern stehen so in vielen Webanwendungen Tür und Tor offen, um zum Beispiel vertrauliche Daten wie Passwörter oder Kreditkartennummern abzufangen. Dieses Risiko ist bekannt, und trotzdem bieten viele Webanwendungen nur unzureichenden Schutz. „Privatanwender gehen oft sehr sorglos mit dem Medium Internet um“, weiß Prof. Schwenk. „So werden sogar nach dem NSA-Skandal die allermeisten E-Mails noch unverschlüsselt verschickt. Und selbst Politiker und Wirtschaftsbosse machen einen Bogen um abhörsichere Handys und nutzen lieber das gewohnte Smartphone. Eben weil dies mehr Komfort und Services bietet.“ Angriffe auf den Webbrowser sind schwer zu erkennen, da die Angreifer verschiedene Verschleierungstechniken nutzen können. Deswegen hat man sich am Lehrstuhl für Netz- und Datensicherheit dem Kampf gegen Browserangriffe verschrieben und im BMBF-Projekt „JSAgents“ eine Lösung konzipiert, mit der die Webanwendung, beispielsweise ein Onlinebuchungsformular für Flüge, im Browser geschützt werden kann. Dazu haben die Forscher ein JavaScript-Framework entwickelt, das im Hintergrund während der normalen Internetnutzung läuft (Abb. 1). Es ist in der Lage, Angriffe gegen Browser im Moment des tatsächlichen Angriffs zu erkennen, zu protokollieren und anschließend zu verhindern. Grundlage dieser Funktionalität sind moderne JavaScript-Features, die genutzt werden, um vor der HTML-Darstellung im Browser gefährliche Elemente aus der Webseite zu entfernen. Indem die Forscher JavaScript verwenden, erreichen sie, dass die Software in jedem Webbrowser – Firefox, Google Chrome, Internet Explorer, Safari – sofort genutzt werden kann. Die Schutzsoftware ermöglicht es zum Beispiel, den Schreib- und Lesezugriff auf bestimmte Elemente einer Webseite für andere Skripte zu blockieren. So lässt sich verhindern, dass die Tastaturanschläge, die ein Nutzer macht, auf den Server des Angreifers übertragen werden oder dass von außen jemand auf den Rechner zugreift und Eingabefelder ausfüllt, ohne dass der Nutzer es bemerkt. Damit

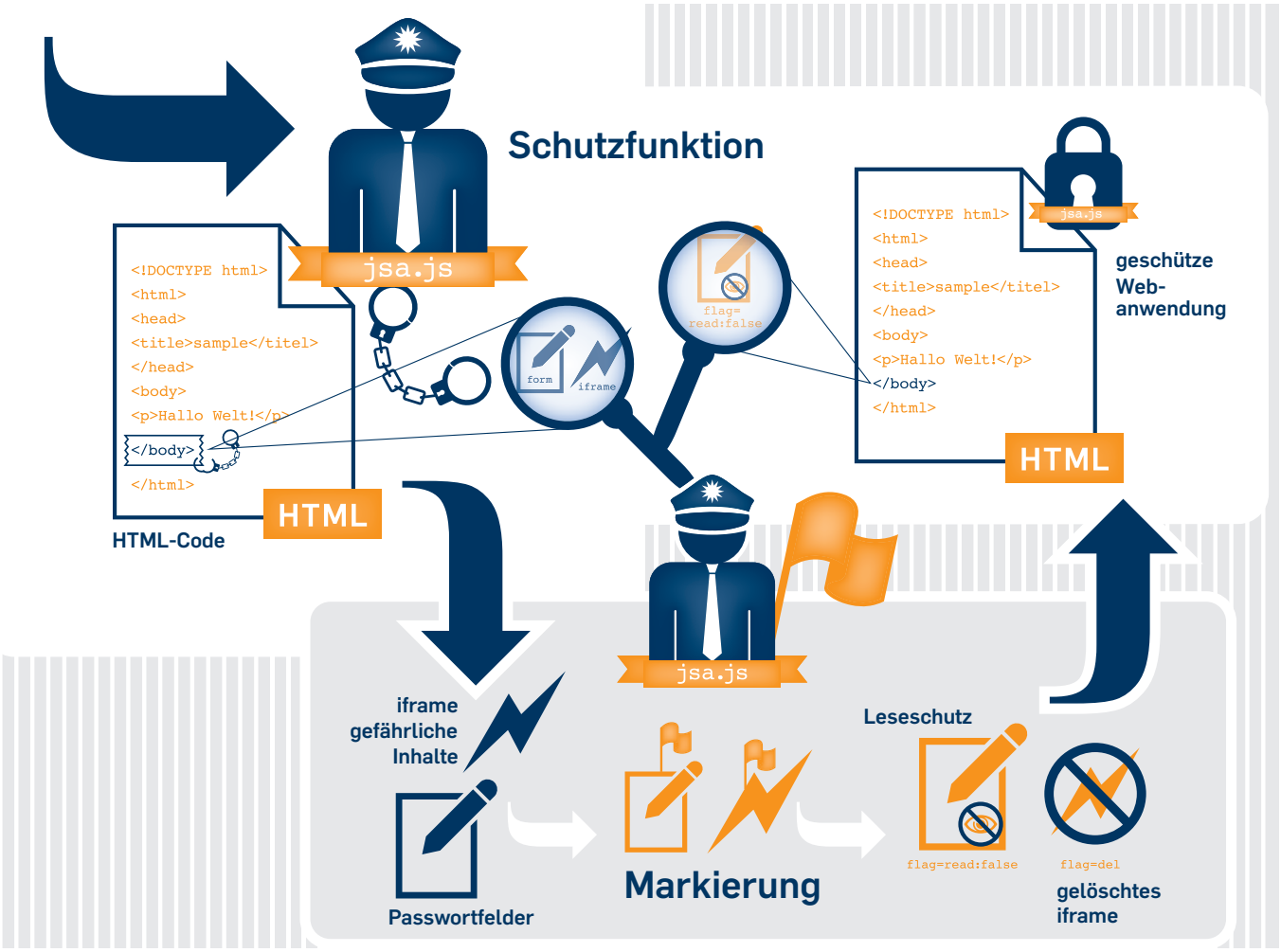

Abb. 1: Der HTML-Code einer Internetseite kann gefährliche Inhalte, *iframes*, enthalten. Die am Lehrstuhl für Netz- und Datensicherheit entwickelte Schutzfunktion „jsa.js“ kapselt diesen Teil des Programms kurzzeitig ab und versieht ihn mit einer Markierung. Diese verbietet Dritten einerseits den Lesezugriff auf Passwortfelder und sorgt gleichzeitig dafür, dass das *iframe* gelöscht wird. Anschließend wird der nun geschützte und bereinigte *body* dem Programmcode wieder zugeführt.

die Schutzsoftware greifen kann, muss sie allerdings beim Öffnen einer Internetseite als erstes ausgeführt werden, im HTML-Text also möglichst weit oben stehen.

„Auf den ersten Blick scheint die Programmiersprache JavaScript eine Schwachstelle zu sein, die leicht missbraucht werden kann. Eine Zeit lang gab es daher die Empfehlung vom Bundesamt für Sicherheit in der Informationstechnik, JavaScript im Browser zu deaktivieren“, erzählt Prof. Schwenk (Abb. 2). Sein Lehrstuhl zeigte jedoch, dass das keine Lösung ist. Nicht nur, weil ohne JavaScript praktisch keine moderne Internetseite läuft. Sondern auch, weil nicht nur JavaScript ein Problem darstellt, sondern weil HTML5 selbst viele skriptähnliche Features enthält. Ein möglicher Angriffspunkt ist das neu eingeführte Grafikformat SVG, denn hier kann ein Bild selbst (Schad-)Code enthalten. Das bedeutet, Angreifer können ein Bild einschleusen, das einen Programmcode enthält. Das Tückische daran: Bilder und Fotos gelten bei Anwendern in der Regel als harmlos und können leicht in Webanwendungen eingeschleust werden, zum Beispiel als Bild in einem Wikipedia-Artikel. Über Features wie Grafikfilter für SVG können dann sogar *Scriptless Attacks* ausgeführt werden, mit denen Passwörter trotz deaktiviertem JavaScript gestohlen werden können. Die Mitarbeiter am Lehrstuhl für Netz- und Datensicherheit haben in der Vergangenheit schon zahlreiche solcher Sicherheitslücken entdeckt. Auf der Suche nach Schwachstellen in Browsern gehen sie ähnlich vor wie ihre kriminellen Gegenspieler. Mit ihrem Know-how würden die IT-Spezialisten es als Hacker wahrscheinlich weit bringen. Doch die Sicherheitsexperten haben sich der guten Sache verschrieben und machen die betroffenen Webseitenbetreiber auf die Risiken ihrer Seite aufmerksam. *Responsible Disclosure* nennt sich dieses Verfahren, bei dem den Webseitenverantwortlichen eine gewisse Zeit gegeben wird, um die Schwachstelle zu beheben. Erst danach geben die Entdecker ihre Information an die Öffentlichkeit. Erstaunlicherweise kümmern sich einige Firmen jedoch gar nicht um die Behebung der Sicherheitslücken. „Manchmal ist es schwierig, kleinere Firmen zu erreichen. Dort gibt es einfach niemanden, der für die Sicherheit der Webseite verantwortlich ist“, sagt Jörg Schwenk. Rechtlich gesehen bewegen sich die Anbieter damit in einer Grauzone, denn es ist nicht klar definiert, welche Softwarelücken eine Firma schließen muss.

Große Firmen haben hingegen sogenannte *Bug Bounty*-Programme initiiert. Google zum Beispiel setzt viel daran, nicht durch Sicherheitslücken negative Schlagzeilen zu machen. Dem Suchmaschinenbetreiber ist das Auffinden und Melden

Abb. 2: Prof. Jörg Schwenk hat seit 2003 den Lehrstuhl für Netz- und Datensicherheit an der RUB inne. Sein Team und er forschen und entwickeln in den Bereichen kryptografische Protokolle, Internet- und XML-Sicherheit.

> *„ÜBER BROWSER KANN MAN SICH EINE MENGE ÄRGER EINFANGEN.“*

von Schwachstellen Pi Millionen Dollar, also 3,141 Millionen Dollar, wert. Mit dieser Belohnung spricht der Internetgigant gezielt die „White Hat“-Hackercommunity an, also die „guten Hacker“, deren Ziel es ist, Sicherheitslücken aufzudecken und zu melden, ohne sie auszunutzen. Die White Hats haben ein enormes Know-how, das Google auf diese Weise nutzt. Ähnliche wirtschaftliche Anreize gibt es in Deutschland kaum, weiß Jörg Schwenk: „Die Deutsche Post ist meines Wissens die einzige deutsche Firma, die in der Vergangenheit zwei öffentliche Sicherheitswettbewerbe veranstaltet hat. Beim ersten Durchgang hat die RUB dabei neun von zehn Preisen gewonnen.“

Ein Erfolg, der alle am Lehrstuhl motiviert und für sich spricht. Geht es bei „JSAgents“ vor allem darum, Passwörter zu schützen, beschäftigt sich Prof. Schwenk in dem vom Bundesministerium für Wirtschaft und Energie initiierten Projekt „SkIDentity“ (Abb. 3) damit, Passwörter im Internet ganz zu vermeiden (siehe „So funktioniert SkIDentity“). Dabei nutzt „SkIDentity“ bereits existierende sichere Chipkarten wie den elektronischen Personalausweis und die elektronische Gesundheitskarte (Abb. 4). „Die bisher realisierten öffentlichen Chipkartenprojekte werden kaum genutzt“, sagt Schwenk und kennt auch den Grund dafür: „Die Karten sind sicher.

SO FUNKTIONIERT SKIDENTITY

1. Ein Nutzer möchte auf eine Webanwendung zugreifen. Statt ein Passwort einzugeben, klickt er auf den Login-Button von SkIDentity, der in die Startseite integriert ist. Dadurch wird sein Browser zum SkIDentity-Server umgeleitet.
2. Ist er an diesem Server noch nicht angemeldet, wird er aufgefordert, seinen elektronischen Ausweis auf das Kartenlesegerät zu legen. Die Nutzerdaten wie Name und Adresse werden ausgelesen und nach Bestätigung durch den Nutzer an den SkIDentity-Server gemeldet. Das Ganze wird durch ein kryptografisches Protokoll abgesichert. (Ist der Nutzer beim SkIDentity-Server bereits angemeldet, so kann dieser Schritt entfallen.)
3. Anschließend werden diese Daten in eine *SAML Assertion* geschrieben, die vom SkIDentity-Server digital signiert wird. SAML steht für *Security Assertion Markup Language*; dies ist ein Framework zum Austausch von Identitäts- und Autorisierungsinformationen.
4. Über den Browser wird die *SAML Assertion* an die Webanwendung gesandt.
5. Die Webanwendung prüft die *SAML Assertion*. Ist die Signatur gültig und die Identität der Anwendung bekannt, so erhält der Nutzer Zugriff.

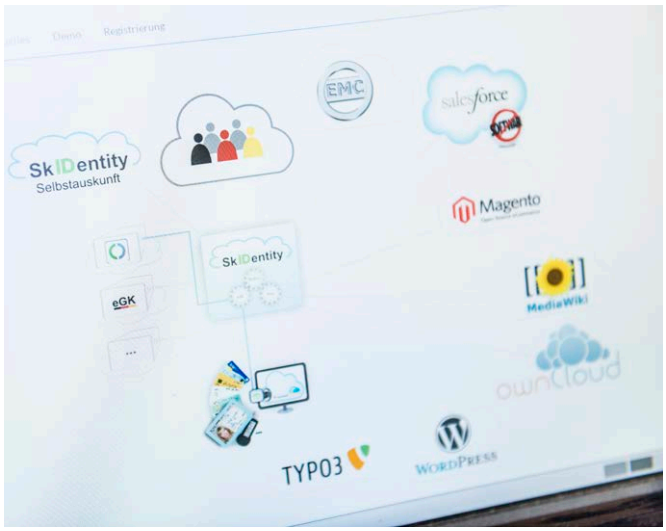

Abb. 3: „SkIDentity“ unterstützt vor allem Cloud-basierte Dienste. Obwohl klar ist, dass eine zuverlässige Identitätsverwaltung unabdingbar für vertrauenswürdiges Cloud Computing ist, erfolgt die Benutzerauthentifizierung in vielen Fällen noch durch Benutzername und Passwort – höchst unsicher.

Abb. 4: Für die Anmeldung bei einem Internetdienst über „SkIDentity“ benötigt man ein Kartenlesegerät.

Aber sie werden vor allem von internationalen Firmen nicht akzeptiert. Dafür sind sie zu sehr auf den deutschen Markt zugeschnitten, und die Anwendung ist zu kompliziert und zu teuer.“ Mit „SkIDentity“ schlagen die am Projekt Beteiligten eine Brücke zwischen der sicheren Lösung Chipkarte und der Welt des Internets. Schwenk und sein Team haben die Aufgabe übernommen, eine Funktion in das System einzubauen, die die deutschen Standards in internationale Industriestandards übersetzt.

Nun stellt sich zum Schluss noch die Frage, ob denn ein ausgewiesener IT-Sicherheitsexperte vor Angriffen im World Wide Web gefeit ist. „Nein. Auch mich hat es schon erwischt“, gibt Jörg Schwenk zu. „Ich habe mir auch schon einen Virus im Netz eingefangen, als ich einen Blog gelesen habe. Plötzlich schaltete sich die Antivirensoftware aus und ein Teil meiner auf dem Rechner gespeicherten Daten wurde versteckt.“ Zum Glück war der Schaden reparabel. Doch eins weiß Jörg Schwenk seitdem ganz sicher: „Über Browser kann man sich eine Menge Ärger einfangen.“

Text: rr, Fotos: dg, Grafik: Melanie Arps

REDAKTIONSSCHLUSS

99,9 %

DES UNIVERSUMS BESTEHEN AUS PLASMA.

Die Erde ist hingegen beinahe plasmafrei – bis auf Blitze, Feuer und Polarlichter. Da Plasmen aber den energiereichsten Zustand der Materie darstellen, sorgt der Mensch dafür, dass sie ein klein wenig häufiger auf der Erde werden. In Forschung und Industrie werden Plasmen technisch hergestellt und für eine Vielzahl von Anwendungen genutzt. Wofür? Ein paar Beispiele finden sich in diesem Heft auf den Seiten 12 bis 27.

Bild: NASA, ESA, and M. Livio and the Hubble 20th Anniversary Team (STScI)

IMPRESSUM

HERAUSGEBER: Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25528, Fax: 0234/32-14136, rubin@rub.de, rubin.rub.de

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Raffaela Römer (rr)

Die Redaktion hat sich um die Einholung der nötigen Bildrechte mit allen Mitteln bemüht; wo das nicht möglich war, bitten wir eventuelle Rechteinhaber, sich mit der Redaktion in Verbindung zu setzen.

FOTOGRAFIE: Damian Gorczany (dg), Hofsteder Str. 45a, 44791 Bochum, Tel.: 0176/29706008, www.damiangorczany.de; Roberto Schirdewahn (rs), RUB Agentur

COVERFOTO: Damian Gorczany

WEBAUFTRITT: Andreas Rohden, Abteilung Markenbildung, RUB

GRAFIK, LAYOUT UND SATZ: VISUELL MARKETING GMBH, Springorumallee 2, 44795 Bochum, Tel.: 0234/459803, www.visuell-marketing.com

DRUCK: VMK Druckerei GmbH, Faberstrasse 17, 67590 Monsheim, Tel.: 06243/909-110, www.vmk-druckerei.de

AUFLAGE: 4.000

ANZEIGENVERWALTUNG UND -HERSTELLUNG: VMK GmbH & Co. KG, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-0, www.vmk-verlag.de

BEZUG: Die Sonderausgabe 2015 des Wissenschaftsmagazins RUBIN ist erhältlich in der Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität, Gebäude ID, Etage 1, Raum 643. Das Wissenschaftsmagazin RUBIN erscheint zweimal im Jahr. ISSN 0942-6639