Darmstädter Cybersecurity-Forschung

CRISP
Center for Research in Security and Privacy

Sichere Internet-Infrastrukturen

Das Internet ist das größte und komplexeste Kommunikationsnetz und als solches die weltweit größte IT-Infrastruktur. Zentral für das einwandfreie Funktionieren des Internets ist das Domain Name System (DNS) und entsprechende IT-Protokolle wie z. B. das Border Gateway Protocol (BGP).

DNS- und BGP-Server bilden das Rückgrat des Internets und sorgen zum Beispiel dafür, dass E-Mails sicher ihr Ziel erreichen, indem Daten den Weg entsprechend eigenständig wählen. Die Wegewahlfunktionen im Internet helfen dabei, auf unvorhergesehene Ereignisse wie etwa den Ausfall von Internet-Knoten zu reagieren und sichern so die Verfügbarkeit des Internets. Doch die Wegewahl kann auch missbraucht werden, indem Datenpakete bewusst über bestimmte Internetknoten gelenkt werden, um somit auf Inhalte zugreifen zu können und diese auszulesen oder zu verändern.

Durch besondere Analysekompetenz des Fraunhofer-Instituts für Sichere Informationstechnologie SIT gelang es, besonders gravierende Schwachpunkte in den Internet-Infrastrukturen zu identifizieren und das Ausmaß der Bedrohung zu bestimmen. Basierend auf diesen Analyse-Ergebnissen werden im CRISP-Leuchtturmprojekt „Sichere Internet-Infrastrukturen" Handlungsempfehlungen sowie neue Protokolle und Cybersicherheitslösungen entwickelt, um den globalen Herausforderungen in diesem Bereich zu begegnen.

Weitere Informationen:
www.crisp-da.de/forschung/leuchtturmprojekte/sichere-internet-infrastruktur

CRISP ist ein gemeinsames Vorhaben von

TECHNISCHE UNIVERSITÄT DARMSTADT
CYSEC
Fraunhofer SIT
Fraunhofer IGD
h da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

TRACING – Cyber Incident Monitor

Die Bedrohung durch Cyber-Angriffe nimmt stetig zu. Um diesen Angriffen gezielt begegnen zu können, sind mehrere Schritte notwendig:

1. Ein allgemeines Bewusstsein der Bedrohungslage muss etabliert werden
2. Angriffe müssen zeitnah erkannt werden und
3. detaillierte Informationen über Angriffe müssen Forschern zugänglich sein, um neue Schutzmechanismen entwickeln zu können.

Das Fachgebiet Telekooperation unter der Leitung von Prof. Dr. Max Mühlhäuser an der TU Darmstadt stellt sich diesen Herausforderungen unter anderem mit dem „TU Darmstadt Cyber Incident Monitor". Das großflächige Projekt sammelt durch gezielt platzierte Sensoren, zum Beispiel Honeypots, Informationen über Angriffe und Angriffsvorbereitungen.

Diese Informationen können von Wissenschaftlern für weitere Forschung genutzt werden. Durch die Aggregation der Informationen, vor allem durch den einfachen Web-Zugang, wird der breiten Öffentlichkeit die aktuelle Lage vermittelt.

Weitere Informationen:
www.tracingmonitor.org

Dieser Demonstrator wurde entwickelt von

Telecooperation Lab

CRISP – Center for Research in Security and Privacy
Mornewegstraße 32
64293 Darmstadt
info@crisp-da.de
www.crisp-da.de

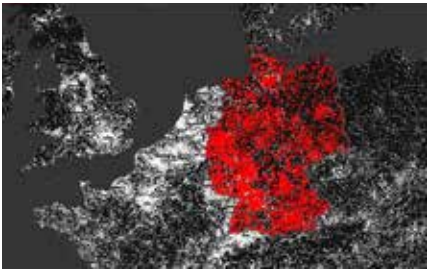
CRISP
Center for Research
in Security and Privacy

Visuelle Analyse des Internet Routing

Im Rahmen des Center for Research in Security and Privacy (CRISP) wird in diesem Teilprojekt die visuelle Analyse der gesamten Internet-Infrastruktur ermöglicht. Das weltweite Internet besteht dabei aus so genannten Routern, die autonom miteinander kommunizieren und den Internet-Verkehr leiten. Bei der damaligen Entwicklung dieser Infrastruktur wurden Sicherheitsaspekte leider nicht ausreichend betrachtet.

Wissenschaftler des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD haben einen Prototyp entwickelt, der sich auf die Analyse vergangener Ereignisse fokussiert. Auf einer Weltkarte werden dazu alle vergebenen Internetadressen dargestellt, die von Providern verwaltet werden. Cyber-Kriminelle nutzen häufig kurzlebige Netzwerke, die nur wenige Stunden oder Tage existieren, um Angriffe auf andere Netzwerke zu fahren. Ein Ziel des Prototyps ist es daher, solche Veränderungen und ungewöhnliche Umleitungen des Datenflusses über die Zeit sichtbar zu machen.

Abschließend wird auf Basis der Ergebnisse der forensischen Analyse eine automatisierte Erkennung von ungewöhnlichen Ereignissen im globalen Routing erstellt.

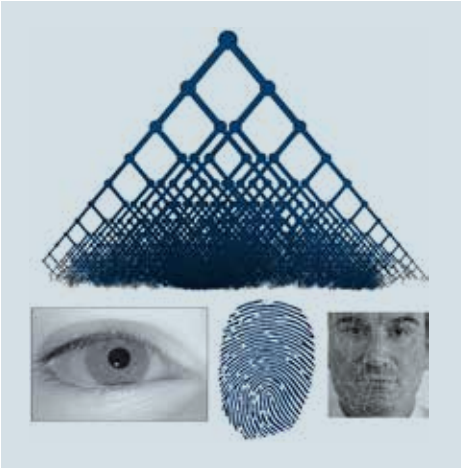


Weitere Informationen:
crisp.igd.fraunhofer.de

Gefördert von
Bundesamt
für Sicherheit in der
Informationstechnik
HESSEN
Hessisches
Ministerium für
Wissenschaft
und Kunst

BIO-INDEX

Biometrie ist die Wissenschaft der Körpermessung am Lebewesen. Automatische Erkennungssysteme nutzen messbare, individuelle Merkmale (Charakteristika) – physiologische (Fingerabdruck, Gesichtsbild, Muster der Iris) oder verhaltensbedingte (Schreibverhalten, Lippenbewegung, Stimme) – zum Zweck der Identifikation/Verifikation einer Person. In den vergangenen Jahren hat sich die Biometrie-Forschung an der Hochschule Darmstadt international etabliert.



Ziel des Teilprojektes BIO-INDEX ist es, die Zugriffszeiten in einem biometrischen Identifikations-System zu reduzieren, ohne dabei an biometrischer Genauigkeit des Gesamt-Systems einzubüßen. Das Arbeitsziel ist, durch geeigente Methoden eine Unterteilung einer biometrischen Datenbank vorzunehmen, so dass eine robuste Suche auf einen Unterraum begrenzt werden kann.

Zusätzlich werden multi-biometrische Anwendungen sowie ein Design von datenschutzfreundlichen Identifikationssystemen untersucht.

Weitere Informationen:
www.dasec.h-da.de/projects/current-projects/bioindex

Darmstädter Cybersecurity-Forschung

CRISP
Center for Research in Security and Privacy

NFCGate: Sicherheitstests mit dem Smartphone

Drahtlose Near Field Communication (NFC) wird in vielen sicherheitskritischen Anwendungen, wie Schließ- und Bezahlsystemen sowie elektronischen Ausweisdokumenten, verwendet.

Die geringe physikalische Entfernung von wenigen Zentimetern zwischen Sender und Empfänger erschwert die Sicherheitsforschung an NFC-Systemen, da bisher spezialisierte Hardware verwendet werden musste. Viele moderne Smartphones verfügen allerdings über eine eingebaute NFC-Funktionalität und stellen damit günstige Analysegeräte dar.

Die Forscher haben eine App entwickelt, die sowohl das Weiterleiten von NFC-Daten zwischen zwei Geräten, als auch das Kopieren und Verändern der Seriennummer ermöglicht. Diese Seriennummer wird von vielen Systemen als Sicherheitsmerkmal verwendet, da sie als schwer zu fälschen gilt.

Mit zwei herkömmlichen Smartphones können nun Sicherheitstests von NFC-Systemen einfach und schnell durchgeführt werden.

So können Sie sich schützen:
Benutzer können Ihre NFC-Karten in auslesesicheren Kartenhüllen aufbewahren, die im Internet oder im Fachhandel erhältlich sind.

Das sollten Hersteller tun:
Hersteller von NFC-Systemen sollten ihre Geräte mit dem sogenannten „Distance Bounding“ ausstatten, einer zusätzlichen Sicherheitstechnologie.

Für weitere Informationen und zum Herunterladen der App besuchen Sie seemoo.de/nfcgate

Dieser Demonstrator wurde entwickelt von

SEEMOO
SECURE MOBILE NETWORKING

CRISP ist ein gemeinsames Vorhaben von

TECHNISCHE UNIVERSITÄT DARMSTADT
CYSEC
Fraunhofer SIT
Fraunhofer IGD
h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

CRISP

Center for Research
in Security and Privacy

Gefördert von

Bundesamt
für Sicherheit in der
Informationstechnik

HESSEN
Hessisches
Ministerium für
Wissenschaft
und Kunst

CRISP – Center for Research
in Security and Privacy

Mornewegstraße 32
64293 Darmstadt

info@crisp-da.de
www.crisp-da.de