

► TNC / T-NAC

Trusted Computing schließt außerdem die präventive Absicherung von Netzwerken mit ein, indem nur vertrauenswürdige Komponenten einen Netzwerkzugang erhalten – bezeichnet als Trusted Network Connect (TNC). Die Hauptidee ist es, die Sicherheitseigenschaften der Sicherheitskomponenten (Firewall, Virens Scanner, ...) eines zugreifenden Rechnersystems auf deren Integrität zu messen. Neben der Einbindung dieser Sicherheitsmechanismen in Turaya werden darauf aufbauend, Policy Management Funktionen und ein vertrauenswürdiges Sicherheits-Gateway entwickelt. Erarbeitet werden diese Ziele im Projekt tNAC.



► Identity Management

Im engeren Sinne beschreibt der Begriff Identity Management (IM) jeglichen Einsatz von digitalen Identitäten und deren Berechtigungen sowie deren Pflege, Erzeugung, Nutzung und Löschung. Das von IM verfolgte Ziel ist es, vertrauenswürdige, identitätsbezogene Prozesse plattformübergreifend und standardisiert nutzbar zu machen.

► elektronischer Personalausweis (ePA)

Der Ausweis verfügt über einen Chip mit SmartCard-Funktionalitäten und enthält personenbezogene Daten in elektronischer Form. Um das Prinzip des neuen Identifikationsnachweises zu veranschaulichen, hat das Institut für Internet-Sicherheit eine Demo für die Online-Authentisierung entwickelt.

► Weitere Projekte

Web-Services Sicherheit, XKMS, Sicherheit von mobilen Geräten, Next Generation Network (NGN), Internet-Recht, Voice over IP, Branchenbuch IT-Sicherheit.

**Branchenbuch
IT-Sicherheit**

www.branchenbuch-it-sicherheit.de

► Dienstleistungen

Neben den Forschungs- und Lehrtätigkeiten bietet das Institut verschiedene Dienstleistungen an. Die günstige Lage der Fachhochschule Gelsenkirchen gibt uns die Möglichkeit zur interdisziplinären Zusammenarbeit mit anderen Aufgabenfeldern der Informatik und Fachbereichen. Damit können wir auch größere Dienstleistungsangebote in wirtschaftlich attraktivem Rahmen für Sie durchführen und bleiben trotzdem flexibel.

Unser Lehrpersonal sorgt für ein hohes Niveau in der Lehre und Weiterbildung an unserem Institut. Dadurch besitzen unsere Mitarbeiter eine exzellente Fachkompetenz, wenn sie Ihre Arbeit auf dem IT-Markt fortsetzen.

Wir bieten Ihnen ein breites Spektrum an Dienstleistungen:

- IT-Sicherheitsschulungen / Awareness-Performance Workshops (Live-Hacking)
- Forschungs- und Entwicklungsleistungen für Ihr Unternehmen
- Entwicklung von Studien (Fachthemen, Machbarkeitsstudien)
- Erarbeiten von Konzepten und Spezifikationen für Ihre Projekte
- Prototypenentwicklung
- Benchmarking

Kontakt

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Fachbereich Informatik
Neidenburgerstr. 43
45877 Gelsenkirchen

Institutsleitung

Prof. Dr. Norbert Pohlmann
Tel.: +49 / 209 - 9596 515
Fax: +49 / 209 - 9596 490
E-Mail: information@internet-sicherheit.de



www.internet-sicherheit.de



www.fh-gelsenkirchen.de

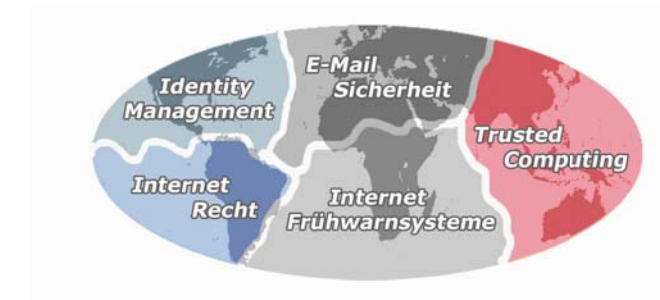
Zuviel Vertrauen
ist häufig eine Dummheit,

zuviel Misstrauen
ist immer ein Unglück

[Johann Nestroy]

In diesem Spannungsfeld forschen, beraten und entwickeln wir im Institut für Internet-Sicherheit um eine passende Vertrauenswürdigkeit und Sicherheit im Internet herzustellen.

stay aware,
stay secure!



Wir, das Institut für Internet-Sicherheit, sind eine innovative, unabhängige, wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Neben der Forschung und Entwicklung sind wir Dienstleister auf dem Gebiet der Internet-Sicherheit. Seit der offiziellen Eröffnung im Mai 2005 hat das junge, kreative Forscherteam das Institut schnell zu einer der bedeutendsten Kompetenzen für Internet-Sicherheit gemacht. Unser Ziel ist es, einen Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herzustellen.

www.internet-sicherheit.de

► Internet: Erforschung / Frühwarnsysteme / Lagebild

Bei der Internet-Erforschung geht es darum, eine solide Wissensbasis über das Internet zu erlangen. Ein wichtiger Schritt in diese Richtung ist die detaillierte Analyse von Kommunikationsprotokollen. Im Projekt „Strukturelle Analyse des Internets“ visualisieren wir die Konnektivität von Autonomen Systemen (Peering, Transit) und erstellen eine Karte der Internet-Infrastruktur, z.B. in Deutschland. Der praktische Teil unserer Forschung umfasst den Aufbau eines internationalen Lagezentrums für den Zustand des Internets. Das Ziel dabei ist, Autonome Systeme und das Internet in definierten Teilen aktiv zu schützen, indem wir Angriffe



so früh wie möglich erkennen und Warnungen und ggf. Gegenmaßnahmen einleiten. Dazu hat das Institut für Internet-Sicherheit verschiedene Komponenten entwickelt, die eine permanente Sicht auf den aktuellen Zustand des Internets ermöglichen, eine detaillierte Kommunikationsanalyse zulassen und Kennzahlen zur Verfügung stellen. Das Motto, das uns und unsere Partner leitet, ist: If you can measure it, you can manage it!

► Internet-Frühwarnsysteme / Internet-Lagebild

Das Internet-Frühwarnsystem oder Internet-Lagebild vereint alle Analysekomponenten wie IAS, LVS, LAS und weitere if(is) Projekte sowie Partnerprojekte.

► Internet-Analyse-System (IAS)

Das IAS bindet sich mittels Sonden passiv in die Kommunikationsleitung ein und analysiert datenschutzkonform Kommunikationsparameter, welche umfangreich ausgewertet und visualisiert werden können. Zusätzlich werden Angriffe erkannt und Zukunftsprognosen generiert.

► Verfügbarkeit der Dienste im Internet (IVS)

Das IVS überprüft die Verfügbarkeit und Funktionalität von verschiedenen Servern und Diensten durch den Einsatz von Drohnen. Diese führen Messungen von Güteparametern wie Bandbreite, Verzögerung, Schwankung und Paketverlusten, etc. durch.

► Log-Daten-Analyse-System (LAS)

In diesem Projekt analysieren wir die gesammelten Log-Daten einer lokalen Infrastruktur. Bei Angriffen wird ein Alarm erzeugt und analysiert, wie auf die Angriffe optimal reagiert werden kann.

► E-Mail-Sicherheit

Im Schwerpunkt E-Mail-Sicherheit forschen wir an IT-sicherheitsrelevanten Themen rund um den E-Mail-Dienst. Dabei werden unter anderem verschiedene Antispam-Maßnahmen angewendet und evaluiert. Untersuchungen zu DNS-basierten IP-Blacklists sowie Analysen zum E-Mail-Adress-Harvesting runden das Forschungsthema E-Mail-Sicherheit ab.

► Antispam

Wichtiger Bestandteil unserer Antispam-Forschung ist die Entwicklung von verteilten Reputationsdiensten zur Spamabwehr, z.B. das „Distributed IP Reputation System“. Hinzu kommen empirische Untersuchungen von Antispam-Mechanismen auf Netzwerkebene, wie beispielsweise unsere Untersuchungen von DNS-basierten IP-Blacklists sowie Korrelationsanalysen von IP-Listen mit Routing-Informationen.

► Applied Antispam

Neben der Entwicklung von Spam-Abwehrmechanismen versuchen wir diese Techniken auch in Mail-Transfer Systeme zu integrieren und zu evaluieren. Ziel hierbei ist es, einen Mail Transfer Agent zu erstellen, der optimale Voraussetzungen für Forschungsaufgaben rund um E-Mail bietet.

► Harvesting

Wir untersuchen das sog. Harvesting mit der Absicht, das Verhalten von Harvesting-Bots zu analysieren. Darüber hinaus könnte eine Analyse des Harvesting-Verhaltens Rückschlüsse auf Spamming-Strukturen liefern.

► Trusted Computing

Das Ziel von Trusted Computing ist es, IT-Systeme vertrauenswürdiger und sicherer zu machen. Vertrauenswürdig bedeutet in diesem Zusammenhang, dass die Hard- oder Software sich exakt gemäß definierten Vorgaben verhält. Die Hauptidee besteht darin, manipulationsgeschützte Sicherheitskomponenten in die Hardware zu integrieren, die als vertrauenswürdige „Anker“ mit der Unterstützung einer Sicherheitsplattform sowohl die Integrität als auch die Authentizität des Rechnersystems garantieren.

Aktuellen softwarebasierten Angriffen (Trojaner, Viren, Würmer) kann durch diese hardware- und softwareunabhängigen Konzepte effektiv entgegengewirkt werden. Das Institut für Internet-Sicherheit verfolgt das Ziel, quelloffene Anwendungen und technische Lösungen auf Basis der Trusted Computing Idee zu entwickeln.

► Turaya

Turaya ist eine vertrauenswürdige, faire und offene Sicherheitsplattform, die Trusted Computing Funktionalitäten verwendet und als Basis für vertrauenswürdige IT-Systeme dient. Durch die Bereitstellung der Sicherheitsplattform für PCs, mobile Geräte und embedded Systeme werden neue, innovative Geschäftsmodelle ermöglicht. Turaya wurde innerhalb des European Multilaterally Secure Computing Base Projektes (EMSCB) initiiert, in dessen Rahmen bereits interessante Piloten fertig gestellt wurden: Turaya.Crypt, Turaya.VPN, Turaya.ERM (mit der SAP AG), Turaya.Embedded (mit Bosch/Blaupunkt). Die wichtigsten Kerntechnologien sind: Virtualisierung, starke Isolation, Minimalisierung der kritischen Technologien und die intelligente Nutzung der Trusted Computing Technologie.

