

Sichere und integrale IT-Systeme

**Seminar im HT 2008
an der Universität der Bundeswehr**

**Dr. Udo Helmbrecht
udo.helmbrecht@unibw.de**

Neubiberg, 21. 10. 2008

Inhalt

- Bedrohungen: BotNetze
- Sichere Plattformen / Trusted Computing
- SINA Sichere Inter-Netzwerk Architektur
- Sicherheit durch Verschlüsselung
- Sicherheit durch Self-Protection oder Self-Healing

Bot-Netze

- Ein Bot (Kurzform von Robot) ist ein Programm, das ferngesteuert arbeitet. Im Kontext von Computer-Schadprogrammen ist mit Bot ein Programm gemeint, welches einem Angreifer die Fernsteuerung von infizierten Rechnern ermöglicht.
- Von Bot-Netzen spricht man, wenn viele infizierte PCs per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden.
- Bot-Netze werden zum Beispiel zur Durchführung von DDoS-Angriffen oder zur Versendung von Spam verwendet.



- Themen
 - Funktionsweise von Bot-Netzen
 - Zugriffe, Administration, ...
 - Beispiele
 - u.a. Spam, DDoS, ...
 - aktuelle Situation
 - Gegenmaßnahmen
 - Provider
 - Hersteller

- Quellen

http://www.bsi-fuer-buerger.de/abzocker/bot_netze.htm

<http://www.bsi.de/literat/lagebericht/lagebericht2007.pdf>

<http://www.bsi.bund.de/literat/lagebericht/>

C.Eckert, IT-Sicherheit: Konzepte - Verfahren - Protokolle



Trusted Computing

- Im April 2003 wurde von führenden Konzernen der Informationstechnik eine nicht profitorientierte Organisation gegründet, die offene Standards für eine neue Generation von sicheren Hardware- und Softwareprodukten in nahezu allen Anwendungsbereichen erarbeiten soll.
- Unter dem Namen "Trusted Computing Group" (TCG) versuchen die beteiligten Unternehmen, ihre unterschiedlichen eigenen Sicherheitsinitiativen zu koordinieren.
- Den zentralen Punkt der TCG bildet die Spezifikation eines neuen Bausteins, auf dem das gesamte Sicherheitskonzept aufbaut: das "Trusted Platform Module" (TPM). Die ersten Spezifikationen der TCG haben bereits zur Entwicklung von Hardware geführt, die in verschiedenen Produkten vermarktet wird

- Themen:
 - Trusted Computing, Trusted Mobile Computing
 - Windows Drive Encryption (BitLocker) in Windows Vista
 - "Identity Management"
 - Chancen, Risiken, Aufwände
 - Anwendungen des ePA
 - Übersicht und Diskussion wichtiger Normen und Standards betreffend den Schutz von sicheren Systemen

Herkömmlicher Ausweis	Elektronische Funktionen
 <p>Ab 01.11.2010: Ausweis in Scheckkartengröße</p>	Immer (verpflichtend): ■ digitales Lichtbild (nur für Polizei und Grenzkontrolle)
	Auf Wunsch (im Preis enthalten): ■ Internetausweis (Name, Anschrift, Geburtstag, Geburtsort, Ablaufdatum) ■ 2 Fingerabdrücke (nur für Polizei und Grenzkontrolle)
	Auf Wunsch (mit Zusatzkosten): ■ Qualifizierte elektronische Signatur

- Quellen

TCG/TPM:

http://www.bsi.de/sichere_plattformen/trustcomp/infos/tcgi.htm

<https://www.trustedcomputinggroup.org/home>

http://www.bsi.de/sichere_plattformen/trustcomp/infos/tpm_report/quellen.htm

BitLocker Drive Encryption Technical Overview:

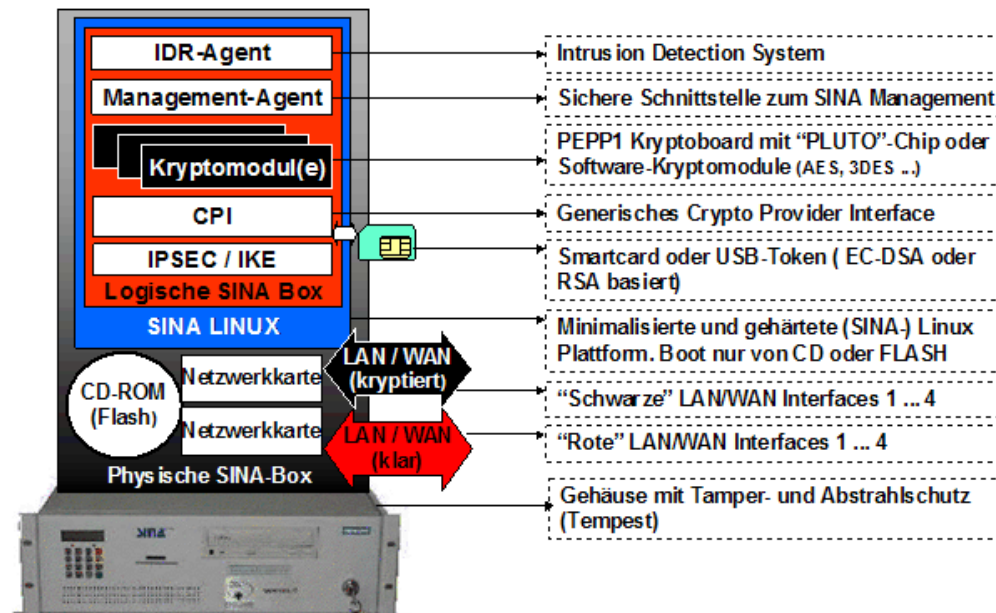
<http://technet.microsoft.com/en-us/library/cc732774.aspx>

ePA:

http://www.bmi.bund.de/cln_028/nn_1082274/Internet/Content/Themen/PaesseUndAusweise/Listentexte/ePersonalausweis.html

- Im Jahr 1999 startete das BSI ein Projekt zur Absicherung von IP-basierten IT-Netzen unter Verwendung kryptographischer Sicherungsmechanismen. Getrieben wurde das Projekt von dem bevorstehenden Umzug der Bundesregierung von Bonn nach Berlin und den Anforderungen an moderne, vernetzte Bürokommunikation unter der besonderen Herausforderung des Geheimschutzes der zu verarbeitenden Daten.
- Inzwischen sind SINA-Produkte für Desktop-PCs und Notebooks verfügbar, die unter Verwendung BSI-eigener Kryptoalgorithmen höchste Sicherheit bei der Verarbeitung, der Speicherung und der Übertragung vertraulicher Daten garantieren.

- Thema
 Beschreibung der SINA Systemarchitektur in verschiedenen Einsatzszenarien



- Quellen
<http://www.bsi.bund.de/literat/faltbl/Sina.pdf>
<http://www.bsi.bund.de/fachthem/sina/sysbesch/sysbesch.htm>

Verschlüsselung

- Sicherheit durch Verschlüsselung
Sichere und vertrauenswürdige Kommunikation ist im Internet nur durch den Einsatz kryptographischer Verfahren möglich.
- SSL-Verschlüsselung, digitale Signaturen, Sprach- und Datenverschlüsselung.
- Hinreichende Sicherheit (Integrität und Vertraulichkeit der Daten) und eine aussagekräftige Authentizität (Identifikation und Unabstreitbarkeit) können auf der Grundlage einer Public Key Infrastruktur (PKI) erreicht werden.
- Themen
 - Elliptic Curve Cryptographie
 - PKI der eGK

- Elliptic Curve Cryptography

elliptische Kurve sind Lösungen der folgenden Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

für kryptographische Anwendungen haben sich folgende Kurven bewährt:

$$y^2 = (x^3 + ax + b) \pmod{p} \quad \text{mit } 4a^3 + 27b^2 \text{ ungleich } 0$$

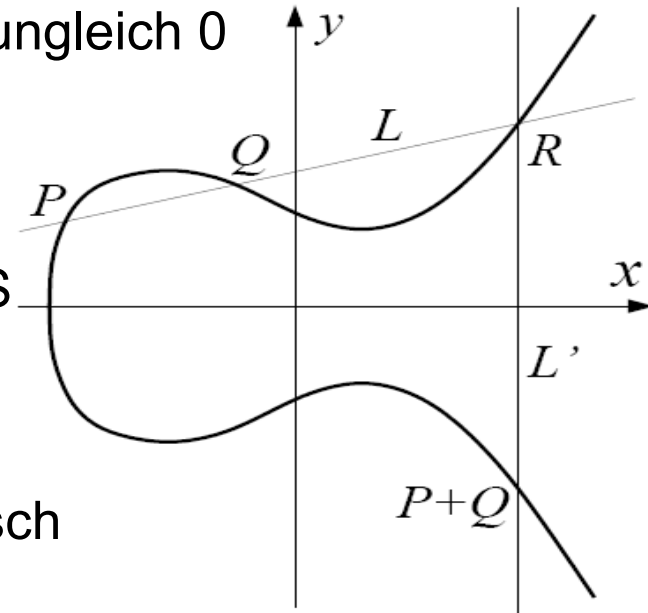
$$y^2 + xy = x^3 + ax^2 + b \quad \text{mit } b \text{ ungleich } 0$$

- Anwendungen

ePass, ePA, SINA, Elcrodat, BOS

- Aufgabe: Theorie und Praxis

Diffie Hellmann Schlüsselaustausch



- PKI der eGK

Gesamtarchitektur

8 Logische Architektur – Public-Key-Infrastruktur

8.1 Abgrenzung und Einordnung des Kapitels

Das aktuelle Kapitel bildet die in den beiden vorangegangenen Kapiteln eingeführten Sicherheitsobjekte auf eine verteilte Public-Key-Infrastruktur und diese auf PKI-Basisservices ab.

Abbildung 29: Einordnung Kapitel 8

Funktionale Grundlage ist der Anforderungsrahmen aus Kapitel 3, der durch bestehende Systeme und durch die durch §291a neu geschaffenen Systeme gebildet wird.

Technische Grundlage sind das Sicherheitskonzept [gemSiKo] und die Sicherheitsarchi-

http://www.bmg.bund.de/cln_110/nn_1168248/SharedDocs/Downloads/DE/GV/GT/Gesundheitskarte/Architektur_20und_20uebergreifende_20Dokumente/Gesamtarchitektur,templateId=raw,property=publicationFile.pdf/Gesamtarchitektur.pdf

Self -Protection /-Healing

- Um die Komplexität des Managements verteilter und vernetzter Systeme beherrschen zu können, stoßen konventionelle Ansätze an ihre Grenzen.
- Als Alternative werden Ansätze aus dem Autonomic Computing wie z.B.
 - Self-Protection oder
 - Self-Healingals mögliche Lösungsansätze im Bereich IT-Security betrachtet. Obwohl erste Überlegungen bereits existieren, steht hier die Forschung erst am Anfang.

- Themen
 - Verwendung eines Hypervisors zur Anomalieerkennung auf einem Hostsystem
 - Analyse des "Bluepill"-Hypervisor Prinzips hinsichtlich Penetration und Abwehrmöglichkeiten sowie als Methode zur "freundlichen,, Systemüberwachung
 - Stand der Technik bei Anomalieerkennung als Mittel hostbasierter Überwachung
- Quellen zu Virtualisierung, Hypervisor
 - <http://www.invisiblethingslab.com/>
 - <http://www.microsoft.com>
 - <http://www.ghs.com/> (Green Hills Inc.)
 - <http://www.bluepillproject.org>