Sicherheit für IBEs

Lutz Donnerhacke

```
2048/39F37F5D  1996-04-25
 A4 C1 50 8F 00 D9 28 60
 70 BB 0B 5D D9 3A 0B B6

1127/DB089309  1997-03-17
 1C 1C 63 11 EF 09 D8 19
 E0 29 65 BE BF B6 C9 CB
```

Überblick

- Begrifflichkeiten zur Sicherheit
- Grundschutz – Ein Inhaltsverzeichnis
- Fallbeispiele: Software

Begriff Sicherheit

Sicherheit ist *binär* für ein bestimmtes Szenario. Jedes Szenario muß in allen Randbedingungen exakt und konkret sein.

Ein System ist sicher gegenüber einem bestimmten Szenario, wenn die Kosten eines Angriffs die des möglichen Gewinns übersteigen.

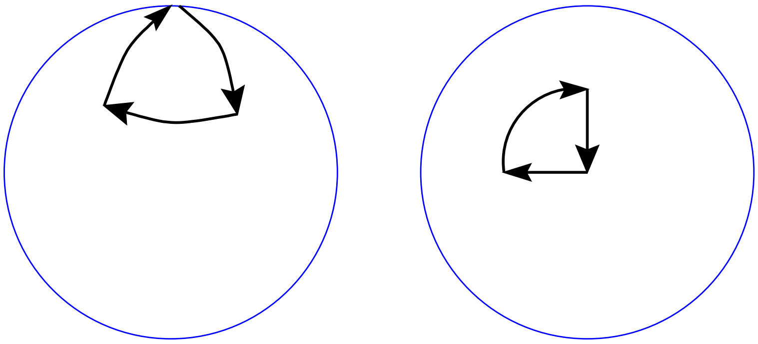
Bspw. verjagt der Hofhund Bello die Nachbarskatze Minka, die er nicht mag, nur dann, wenn er jetzt wach und satt ist und den Eingangsbereich im Blickfeld hat.

≫Unmögliche≪ Ereignisse

Ein Forscher verläßt sein Zelt und geht 2 km nach Süden. Dann geht er 2 km westwärts, dreht nochmals und geht 2 km nach Norden. Als er so sein Zelt erreicht, frißt gerade ein Tier seine Vorräte. Welches Tier ist das ?

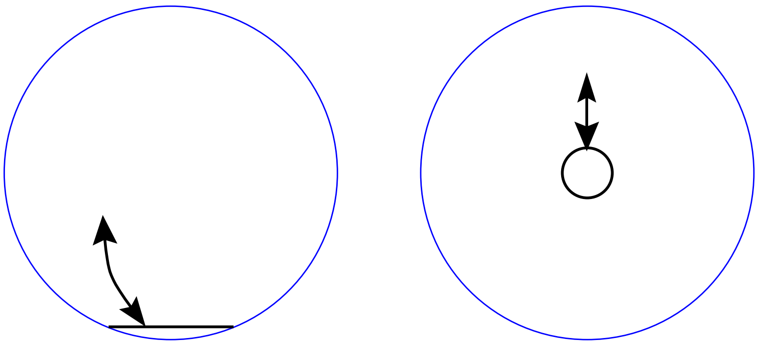
Kanonische Lösung

Ein Eisbär, denn der Forscher hat sein Zelt am Nordpol aufgeschlagen.



Überraschende Lösung

Ein Pinguin, denn der Forscher hat sein Zelt in der Nähe des Südpols aufgeschlagen.



Wo genau muß das Zelt stehen? Gibt es weitere Lösungen? Was passiert bei leichten Meßfehlern?

Denkfremde Kreativität

Angreifer, Naturereignisse und der Zufall halten sich nicht an die Konventionen. Hacking ist *kreative* Auslegung von Vorgaben.

⇒ Etzel McMurphy hatte doch Recht.

⇒ Planungen, Richtlinien und Programme müssen durch »Denkfremde« auditiert werden.

Welcher magnetische Pol liegt in der Nähe des geographischen Nordpols?

Prozentuale Sicherheit

Kann man Sicherheit verbessern?
Was heißt 80 % sicher?

Z := Menge aller möglichen Szenarien

Sicherheitsfunktion $S : Z \to \{0, 1\}$

$$\text{Sicherheit} := \int_{z \in Z} S(z)$$

Doppelbedeutung des Wortes Sicherheit!

Ausflug in die Analysis

$$f(x) := \begin{cases} 0 & : x \text{ irrational} \\ 1 & : x \text{ rational} \end{cases}$$

Welchen Wert hat $\int_0^1 f(x)$?

Nichts ist sicher!

Man kann Schutz nur vor konkreten Bedrohungsszenarien haben, also endlich oder zumindest abzählbar endlich vielen Szenarien.

$\Rightarrow$ Es gibt keine Sicherheit!

$\Rightarrow$ Man kann Sicherheit nicht verbessern!

Szenarienklassen

Man kann die Sicherheit von ganzen Mengen von Szenarien (mit beschränkt variablen Parametern) beurteilen und so *meßbare* Fortschritte für die Sicherheit erzielen.

Sicherheit ist möglich. $\Rightarrow$ Welt gerettet.

Welche Bedrohungsklasse deckt Bello ab?

Was leistet Kryptographie?

Authentisierung Von wem kommt das?

Autorisierung Was darf er?

Identifizierung Wer ist es?

Integrität Wer darf's mitbekommen?

Vertrauen Wem glaube ich was?

Protokolle, Web of Trust, X.509 & IBM.

Was leistet Steganographie?

Kommunikation Wird kommuniziert?

Partner Mit wem wird kommuniziert?

Wächter, Mixe, Wasserzeichen & RIAA.

Grundschutz

Organisation Verantwortlichkeit, Datenträgerverwaltung

Personal Vertretungen, Schulungen, Ausscheiden

Notfallvorsorge Konzept, Testplan

Datensicherungskonzept Refresh, Tests

Datenschutz Logfiles, Zugriffsregeln

Virenschutz Erkennen, Alarmieren

Krypto Heterogenität, Remote Zugriffe, Speicherung

Sicherheitsvorfälle Konzept, Training

Hard-/Softwaremanagement Einkauf, Update, Doku, Austausch

Gebäude Stromversorgung, Brand-, Gebäudeschutz, Schlüsselverwaltung

Verkabelung Brandabschottung, Kabeltypen, Trassenwege, Dokumentation

Büroraum Fenster, Türen, Fremdpersonen

Serverraum Wasserleitungen, Klima, USV, Rauchmelder, Zutritt

Datenträgerarchiv Handfeuerlöscher, Zutritt, Sicherheitstüren

Technikräume externe Kommunikation, Niederspannung, Verteilerraum

Schutzschränke Ersatz für extra Räume

Heimarbeit VPN, Zutritt, Laptop

Rechenzentrum mehr als Serverraum

DOS-PC Biospasswort, Viren, Backup

Unix Netz, Terminals, Auslastung

Laptop Diebstahl, Verschlüsselung, VPN vs. Terminaldienst

öffentlicher PC Keine lokale Datenablage, Passwortschutz

WinNT-PC Nutzertrennung

Win95-PC wie DOS-PC

W2K-PC Policies

Internet-PC Keine Datenablage, Imagekopie, Linux

andere Systeme spezifische Regelungen

Netz mit Server Zentrale Software, Daten, Backup

Unix Server Terminals, AFS, NIS+, ssh

Peer2Peer Administration, Beschränkung

WinNT Netz Kerberos, Administration

W2K Server Policies, Active Directory

andere spezifische Regelungen

heterogene Netze sichere Protokolle, Management

Management Alarmierung, Audit, Revision, Redundanz

Datenträgeraustausch Verschlüsselung, Versandarten

Modem Callback, Verschlüsselung, Fernwartung

Firewall Konzept, Installation, Auswertung, Alarmierung

E-Mail Konfiguration, Filter, Sicherheitsbestimmungen

WWW Clientkonfiguration, HTTPS, Pflegezugriff Server

Einwahl Authentisierung, Autorisierung

Notes Trennung Groupware und Kommunikation, Planung, Konfiguration

TK-Anlage Konfiguration, Steuerung, Zugriffe

Fax Zugriff, Protokoll, Entsorgung, Absprachen für Empfang

Anrufbeantworter Fernabfrage, Raumüberwachung, Abwesenheitstest

ISDN-Filialkopplung Callback, Verschlüsselung, Authentisierung

Handy Sperrungen, Abrechnungen, SuperPIN-Verwaltung

Standardsoftware Anforderungen, Auswahl, Test, Freigabe, Installation, Sicherheitsinfo, Update, Deinstallation

Datenbanken Auswahl, Installation, Konfiguration, Einrichtungsreglungen, Zugriff, Replikation, Backup, Protokolle

Telearbeit Terminalserver, Autorisierung, Verschlüsselung

Directory Zugriff, Sichtbarkeiten, Pflegehierarchie

Fallbeispiele

- Fehlerbehandlung
- Fehlertest
- Böse Fallen

Fehlerbehandlung

Never test for an error condition unless you known how to handle it.

Spiele und neue/alte Hardware. (Installorgie)

Netzwerkfehler, was nun? (SNA, eMule)

Do not trust anybody.

Daten von extern führen immer zur Katastrophe. (Webformulare vor Datenbanken)

Fehlertest

Fehlerverhalten gehört zum Pflichtenheft, zu den Regessionstests und zur Abnahme.

Entwickler werden mit Fehlersituationen allein gelassen. Absturz ist zulässiges Verhalten.

```
($currdom, $currmx) = ($newdom, $newmx)
  if $newmx = DNS::query("MX", $newdom);
```

```
$newmx = DNS::query("MX", $newdom)
  or die("no mx found.")
($currdom, $currmx) = ($newdom, $newmx);
```

Böse Fallen

Viel Programmierwerkzeuge sind ungeeignet. Vornehmlich: Perl, Basic, C, C++, Java.

Beispiel: Berechne die Größe des Buffers für eine base64 Kodierung.

```
size_t base64len(size_t binarylen) {
  return 3*binarylen/4;
}
```

- Brain V1.0
- Spaß mit Mathe
- Grundschutzhandbuch
  `http://www.bsi.de/gshb/`
- The Art of Computer Programming;
  Donald Emerald Knuth
- The Codebreakers; David Kahn
- Angewandte Kryptographie;
  Bruce Schneier
- Intelligent Fragen mit
  `http://www.google.com/...&safe=off`
  `http://groups.google.com/...&safe=off`