Sicherheit und Zuverlässigkeit Zusammenfassung Kein Gewähr auf Richtigkeit und Vollständigkeit Stand:09.02.18

**VERLÄSSLICHES SYSTEM**: ein System, dem man vertraut, dass es spezifizierte Dienste bzw. eine spezifizierte Funktionalität auch beim Auftreten von Störungen oder Fehlern korrekt und verlässlich erbringt. **URSACHE FÜR STÖRUNGEN**:(1) Security-Probleme,z.B. gez.Störversuche (2)Verläslk.-> z.B.fehlerhafte, unzuv. Abläufe||

**VERTRAUT HEISST** das das System nachweisbar sicher,verlässlich und korrekt arbeitet.

**WECHSELWIRKUNG(VERLÄSLK+SICH.)** 🡪Bsp. Durch unerlaubten Zugriff von außen(Sichverletz)arbeitet System nicht mehr verlässlich.etc.pp.||

**HAUPTZIELE DER VERLÄSSLICHKEIT UND SECURITY: 1:***Verfügbarkeit(V+S)*Schutz vor unbefugter Beeinträchtig. der Funktionalität*,****Maßn.:***Festlegen und Kontrollieren von Regeln zur Aufzeichnung und Überwachung **Schutzmech.:**Schreiben von Logdateien, Sichern der Logdateien,Backups und Mirroring**2:***Zuverlässigkeit(V)Schutz vor Fehlern in einem Zeitintervall* ***Maßn.:*** Festlegen undKontrollieren von Regeln zur Zuverlässigkeitsbewertung und Erkennung kritischer Komponenten und ständige Systemverbesserung über den Lebenszyklus **Schutzmech.:** Einsatz betriebsbewährter und qualifizierter Komponenten, Maßnahmen der Fehlerselbsterkennung, Anwendung des Prinzips „Fail-Safe“**3:***Safety(V)*Schutz der Umgebung / des Menschen (vor katastrophalen Auswirkungen eines Systemversagens) ***Maßn.:*** Festlegen und Kontrollieren von Regeln zur Vermeidung, Erkennung, Beseitigung und Einschränkung katastrophaler Auswirkungen **Schutzmech.:** Verwendung betriebsbewährter und qualifizierter Komponenten, Maßnahmen der Fehlerselbsterkennung, Stress Testing,Anwendung des Prinzips„FailSafe“**4:***Vertraulichkeit(S)*Schutz vor unautorisierter Informations-gewinnung ***Maßn.:*** Festlegen und Kontrollieren von Regeln für zulässige/unzulässige Informationsflüsse **Schutzmech.:** Verschlüsselung: symmetrisch oder asymmetrisch || Kontrollierte Informationsweitergabe **5:***Integrität(V+S)*Schutz vor unautorisierter und unbemerkter Modifikation ***Maßn.:*** Festlegen und Kontrollieren von Regeln für zulässige/unzulässige Datenänderungen **Schutzmech.:** Verschlüsselung, Hashfunktionen und MACs,Zugriffsrechten,Firewall **6:**Instandhaltbarkeit(V) Fähigkeit eines Systems, unter gegebenen Anwendungsbedingungen in einem Zustand erhalten bzw. in ihn zurückversetzt werden zu können, in dem es eine geforderte Funktion erfüllen kann, wobei vorausgesetzt wird, dass die Instandhaltung unter den gegebenen Bedingungen mit den vorgeschriebenen Verfahren und Hilfsmitteln durchgeführt wird (DIN IEC 60300-3-10). ***Maßn.:***Verwendung von standardisierten Bauteilen,Sicherstellung einer leichten Zugänglichkeit der Komp. Und einer einfachen Prüfbarkeit

**CIA/HAUPTZIELE DER SEC** (**C**onfidentiality(VERTRAULICHKEIT)Integrity(INTEGRITÄT)Availability(VERFÜGBARK.)

**weitereZiele**: **7:***Verbindlichkeit,*Schutz vor unzulässigem Abstreiten durchgeführter Handlungen ***Maßn.:***Festlegen, was verbindliche Aktionen sind **Schutzmech.:**qualifizierte digitale Signaturen und Zertifikate, Logbücher **8:***Authentizität*:Nachweis der Echtheit und Glaubwürdigkeit der Identität eines Objekts/Subjekts ***Maßn.:*** Festlegen und Kontrollieren von Regeln zu Vergabe von eindeutigen Identifikationen von Subjekten und Objekten und Verfahren zum Nachweis der Korrektheit der Identität **Schutzmech.:**Passwörter, PINS,Smartcards signierter Code**9:***Privatheit:*Schutz der personenbezogenen Daten, Schutz der Privatsphäre, Gewährleistung des informationellen Selbstbestimmungsrechts ***Maßn.:***Datensparsamkeit,Festlegen von “Verfallsdaten” **Schutzmech.:**Pseudonyme anstelle von realen Identitäten, Verschlüss. der Identitäten**SCHUTZBEDARFSERMITTLUNG**(1)niedr./mittel🡪Schadenauswirkung begr. und überschaubar (2)hoch🡪 Schadenauswirkung können beträchtlich sein(3) Sehr hoch 🡪 Schadenausw. Können existentiell bedrohliches, katastrophales Ausmaß annehmen|| RISIKOANALYSE **VORGEHEN:QUALITATIV(1)**Strukturierte Analyse mittels *Bedrohungsbäumen*/pro Angriffsziel ein Baum|| Methode ist primär für die Analyse von aktiven Angriffen ausgelegt, Methode hilft Systeme zu analysieren, für die es noch keine publizierten Analysen möglicher Angriffe bzw. Tabellen mit Risiken / Gefährdungslagen gibt(2)*Stride-methode* Schwachstellen-Analyse der Software-Komponenten in Bezug auf die sechs Angriffsklassen (S,T,R,I,D und E), Modellierung der Syst. Und Komp. mittels UML|| Single Points of Failure werden durch *Failure ImpactAnalysis(SPOF)* rasch entdeckt

**Vort.:**Anschaulichkeit, Gute Möglichkeit der Diskussion

**Nacht.:** Reproduzierbarkeit, Einschätzung hängt stark von der Erfahrung der Beteiligten ab

**VORGEHEN:QUANTITATIV:** Sicherheitsrisiko R = S \* P mit Schadenshöhe/.Potenzial S ; Eintrittswahrscheinlichkeit P

S=1.000.000E ;P=0,01 🡪 R=10.000 E || Bestimmung von P durch: (1) Eig Erf (2) Öff. Stat. (3) Einschätz. Des Nuztens für den Angreif.

**Vort.:** Vergleichbarkeit der Ergebnisse, Methode in der Finanzwirtschaft weit verbreitet, Gute Möglichk. der Diskussion

**Nacht.:** Unschärfe bei Schadenshöhen, Eintrittswahrscheinlichkeit oft nicht bekannt, Wechselwirk. Nicht berücksichtigt

**VORGEHEN:GRUNDSCHUTZMETHODE** Kataloge aus Standards(ISO 27001),Inspiration aus Grundschutzkatalogen des BSI*These:* Es gibt ein Sicherheitsniveau, das für durchschnittliche Verfahren ausreichend ist.Dieses ist durch ein Set an Risiken und korrespondierenden Maßnahmen (in den Grundschutzkatalogen) beschrieben

***RISIKOBEHANDLUNG:*** Umgang mit Risiken 🡪**(1)** ***Reduzierung***1.1. Zusammenstellen der zu reduzierenden Risiken1.2.Ermitteln geeigneter Maßnahmen1.3.Analyse der Wirkung von Maßnahmen **(2)** ***Vermeidung*** durch Änderung in den Verfahren der Infrastruktur **(3)** **Verlagerung** versichern (**4)** **Tragen** Restrisiko

**MASSNAHMEN UND SCHUTZMECHANISMENAUS DER KRYPTOGRAPHIE**

Klassen von Authentifikationstechniken: Authentifikation durch**: I: Wissen**(PW,PIN**) II: Besitz**(Smartcard,SIM) **III:biometrische Merkmale** **IV: Mehrfach-Auth.** / Kombination vorheriger || **I.1.** Challenge-response-Verfahren(CR) Subjekt 🡨🡪Instanz; **I.2.** Symetrisches CR-Verfahren , Subjekt A 🡨🡪Instanz B !!Vorab geheimer Schlüssel!! **I.3.** EinmalPassworte(OTP)**I.4.S/key Verfahren 🡪** Setup: Benutzer(besitzt geheimes PW s(ist preshared Secret) mit lokalem PC, entf. Server(kennt s nicht) !|| 2 Phasen: **(1)** OTP-Berechnung Initiierung und **(2)** Nutzung

**(1)**PC berechnet aus s einmal benutzte Passworte pi,Wahl Zahl N, Wahl Seed-Wertes k 🡪 Übertragen der Werte an Login-Server**(2)** Ablauf:i-te Auth. des Benutzers **I.5. Hardware-basierte OTP-Verfahren:ID-Token** Benutzer erhält Hardware-Token mit eindeutiger Nummer, die der Server kennt.|| Alle 60 sek gen. Token und Server neues Passwort. AES-Hashwert: Tokencode = AES(TokenD | s | Zeit) **I.6. Zero-Knowledge Verfahren** Angreifer darf beliebig viele Nachrichten belauschen 🡪 **Fiat-Shamir-Verfahren;** beruht auf der Schwierigkeit, Quadr.wurzeln in Zn\* zu berechnen;geg: n=p\*q, x=r2 mod n, ges:r|| einfach wenn p und q bekannt, sonst schwierig I:Schlüsselerzeugung: A erzeugt 2 große Primzahlen(p und q geheim); berechnet n=p\*q (nöffentlich);wählt s und berechnet v=s2mod n (v öff.) ; s Geheimnis von A II:Anwendungsphase(Protokoll) [A will B davon überzeugen dass Sie *s* kennt.]

**I.6.Biometrie:** Anforderungen: (1) Universität: Jede Person besitzt das Merkmal(2) Eindeutigkeit: Merkmal ist für jede Pers. verschieden(3) Beständigkeit: Merkmal ist unveränderlich (4)quantitave Erfassbarkeit mittels Sensoren (5)Performance:Genauigkeit und Geschw. (6)Akzeptanz: des Merkmals beim Benutzer (7)Fälschungssicherheit

**A** wählt zufälliges raus Zn\* und berechnet: x=r2 mod n

**A** sendet Wert x an B

**B**: B wählt zufälligesBit b und sendet b anA

**A** antwortet auf diese Challenge mit

*y*=*r*, falls *b*= 0 und mit *y*=*r*·*s*mod *n*, falls *b* = 1

**B** prüft dieseAntwort von a wiefolgt:

Falls *b* = 0, prüft B,ob gilt: *x* =*y*2 mod *n*

Falls *b* = 1, prüftB,ob gilt: *x*·*v* mod*n* =*y*2 mod *n*

*k*-malige Challenge durch B mit neuem *b* und *r*

Klassen biometrischer Merkmale: I: physiologische Merkmale(STATISCH)🡪Fingerabruck,Gesichtsbild,Iris II:Verhaltensmerkmale(DYNAMISCH)🡪Unterschrift,Sprache,Tippverhalten|| Vorgehen: 1.Daten erfassen;2.Benutzer registrieren 3.Erfass. der Verifikationsdaten 4.VD digit.;5.Mit gesp. Referwert vergl.***Problembereiche:*** Abweichungen zwischen Ref. und Verifikationsdaten🡪 2 Fehlertypen(1)Berecht. User wird abgewiesen (2)Unberechtiger wird akzept. 🡪🡪 Leistungsmaß zur Bewertung eines Systems ist die **False-Acceptance-Rate(FAR);False Rejection Rate(FRR);Equal Error Rate(EER) *Sicherheitsprobleme biometrische Techniken🡪***Angriffsstrategien (Direkt. Täuschung des biom. Sensors; einspielen von Daten)*Probleme:* enge Kopplung zwischen Merkmal und Person (1)Bedrohung der informationellen Selbstbestimmung (2)Gefahren durchgewaltsame Angriffe gegen Personen (3)Problem der öffentlichen Daten und rechtliche Aspekte

**KRYPTOGRAPHISCHE VERFAHREN**Ein kryptographisches Verfahren ist ein Tupel(M,C,EK,DK,E,D) M🡪Menge von KlartextnachrichtenC🡪Menge von KryptonachrichtenEK🡪Menge von Verschl.schlüsseln DK🡪Menge von Entschl.schlüsseln E🡪eine Familie von VerschlüsselungsverfahrenD🡪 eine Familie von Entschl.verfahren **Grundsatz**:Sicherheit darf nicht von der Geheimhaltung der Ver und Entschl.funktionen abhängen! **Kerckhoffs-Prinzip:**Stärke (Sicherheit) des Verfahren sollte nur von der Güte desgeheimen Schlüssels abhängen!**Konsequenz**🡪Schlüsselraum EK muss sehr groß sein. Ausprobieren aller Schlüssel (brute-force) soll nicht mitpraktikablem Aufwand möglich sein (exhaustive searchsoll nichtmöglich sein). **Anforderung:** symmetrische Verfahren:Schlüssel >= 128 Bit; asym. VF: Schlüssel >= 2048 Bit; Schlüssel >=224 Bit bei ECC-Varianten ***SYMMETRISCHEVERFAHREN:*** Charakteristika🡪 Ver und Entschl.schl. sind gleich oder leicht ableitbar. VSer und Eser nutzen gleichen,gemeinsamen und geheimen Schlüssel.[DES,AES,RC4, A5/3]Achtung: Starke Chiffre: notwendig, aber nicht hinreichend zurGewährleistung des Schutzziels Vertraulichkeit!Starke Verfahren und gutes Key-Management sind erforderlich!1.Schlüsselgenerierung, hohe Entropie, starke Schlüssel2.Sicherer Austausch des gemeinsamen Schlüssels 3.Sichere Schlüsselspeicherung

**BLOCKCHIFFRE:** Aufteilung des Klartextes in fester Länge(z.B.64Bit)Verschlüssel. Mit gleichem Schlüssel K

Verschlüsselungs-Modi: (1)ECB(Electronic Code Block) Verschlüsselung kann parallesiert werden🡪sehr effizient || gleiche Klartextblöcke ergeben gleiche Chiffretextblöcke(2)CBC(Cipher Block Chaining) Klartextblock wird mit vorh. Chiffretextbl. Verknüpft (XOR) || Gl. Klartextbl. Ergeben ungleiche Chiffretextbl.

**DES(DataEncryptionStandard)🡪**erfolgreichstes Verschlüss.verf.**Eig.:** BC mit BL 64 Bit und SL 64 Bit|| sym.

**🡪**Produktchiffre(komb. Diffusion und Konfusion)sogennante Feistel-Chiffre|| ***Entschlüsselung:*** Umkehrung der Verschlüsselung Runde für Runde|| ***Sicherheit:*** S-Boxen(kern nicht linear);Avalanche-Effect(Nach der5-ten Runde jedes Bit von jedem Bit des Eingabeblocks und jedem Bit des Schlüssels abhängig)***Fazit:*** SL 64 Bit zu schwach für heutige Syst.||Wird immernoch eingesetzt, Austausch aufwendig. **AES(AdvancedEncryptionStandard)🡪 Eig.:** BC mit BL 128 Bit und drei SLgen 128,192 oder 256 Bit|| arbeitet in Runden|| Alg. in Schichten aufgeteilt|| Pro Runde 4 Transformationsschritte (1):Bytesub; (2)ShyftRows; (3)MixColumns;(4)AddRoundKey|| Mathematische Basis: GaloisFeld/Körper ***Entschlüsselung:*** AES ist keine Feistel-Chiffre: alle Schichten müssen invertiert und die Rundenschlüssel in umgekehrter Folge angewandt werden. ***Sicherheit:***AES besitzt starke Diffusions und Konfussions-Eig.|| Verbesserung durch Erhöhung der Rundenanzahl**STROMCHIFFRE:**bitweise Verschlüsselung einer Nachricht M mittels zuf. Schlüsselstrom K || K gleiche Länge wie M ***ASYMMETRISCHEVERFAHREN:***Basis: Zahlentheoretisch schwierig zu lösende Probleme|| 🡪**Public Key Kryptographie** zentrale Idee(Schlüsselpaar mit privatem und öff. Schlüssel)

**Anf.:** Schlüsselpaare müssen effiz. erzeugbar sein und mit vertretbarem Aufwand berechenbar**Basis:**Einwegfunktionen

**(1)RSA**(“Quasi-Standard”) Falltür zur Entschlüsselung ist der private Schlüssel| Ver-und Entschlüsselung basiert auf Ganzzahl-Ring**Sicherheit:**Wettlauf mit Rechengeschwindigkeit(Modul muss groß sein 🡪 2048 Bit bis 4096 Bit)**(2)ECC**Elliptische Kurvenkryptographie|| gut für embedded systems;Gruppe von Punkten anstatt Integern🡪Reduktion von Rechenaufwand **Sicherheit:** Parameter können kleiner sein als bei RSA 🡪 ECC kann zum Verschlüsseln, Signieren und zum Schlüsselaustausch eingesetzt werden. **Hashfunktionen:** notwendig, die Kollisionen auflösen/erkennen mind. 160 Bit || Klassen: Hfkt basierend auf Block-Chiffren ; dedizierten Hfkt (z.B. SHA [Secure Hash-Algorithm] **Sicherheit:** Keccak guter Standard;MD4 und MD5 gut ***Zuverlässigkeit*** Echt-Fail-Safe-Verfahren 🡪 Keine Ausfall oder Fehlererkennung; Sichere Ausfallrichtung durch Zusammenschaltung von Komponenten; ||Maßnahmen gegen Softwarefehler: (1): fehlerabwehr(2)Fehler-Offenbarung und Korrektur(3)Fehlerauswirkungsausschluss || Einsatzmöglichkeiten zur Realisierung von Redudant: (1)Untersch. Algor; Programmiersprachen;Teams|| Kombination der Zuverlässigk.: Bestimmung der Hardware und Softwarezulässigkeit! PENIS