

1 Grundbegriffe

Angriffsarten: Lauschangriff, Maskerade, Integrieren, Replay, DOS, Eindringen

Safety: Funktionssicherheit **Security:** Angriffssicherheit

Risiko: Schadenshöhe * Eintrittswahrscheinlichkeit

Schutzziele: Authentizität, Integrität, Vertraulichkeit, Verbindlichkeit, Verfügbarkeit, Privatsphäre

Hashfunktionen: *preimage resistance*: schwierig ein input für bekannten output zu finden; *second preimage resistance*: schwierig zweiten möglichen Input zu finden; *collision resistance*: nicht mehrere gültige Passwörter für Hash

2 Identity Management

Authentisierung: Überprüfung **Autorisierung:** Zuweisung

Verifikation: 1:1 **Identifikation:** 1:n

Authentifikation durch: Wissen(Passwort, PIN), Besitz(SIM, Smartcard), Merkmal(biometrische)

Passwortsicherheit: "for Schleife": $2^{\log_2(N)}$, N sizeof(Passwortraum)

Passwortangriffe: Dictionary, BruteForce, Vorberechnung **Gegenmaßnahmen:** Salt, Pepper

3 Mathematische Grundlagen

LFSR: $r_n = r_x \oplus r_x \mod x$; Frobeniusbegleitmatrix: umgedrehte r_x

RSA: wähle Primzahlen p und q $N = p * q$; $\Phi(N) = (p - 1) * (q - 1)$; suche e mit $1 < e < \Phi(N)$, muss teilerfremd sein; $d =$ multiplikatives Inverses von $\Phi(N)$; public key: (e, N) ; private key (d, N) ; encrypt: $m^e \mod N$; decrypt: $(m^e)^d \mod N$

4 Gesetze

Datenschutzgesetze: Datensparsamkeit, Einwilligung, Zugriffs-/Änderungsschutz; **Hacker-paragraph:** Vorbereitung ist illegal; **Malware:** Virus, Trojaner, Würmer, Spyware, Adware, Dialer, Zombie;

Wardriving: Wlan Autofahrt