Vorlesung Kryptographie

Teil 1

Dr. Jan Vorbrüggen

Übersicht

- Teil 1
  - (Nicht-) Ziele
  - Steganographie vs. Kryptographie
  - Historie
  - Annahmen
  - Diffie-Hellman
  - Angriffe
- Teil 2
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hashverfahren
  - Alles zusammen: elektronische Signatur
  - Rechtliche Aspekte
  - Standards
  - Komplexe Anwendungen
  - So bitte nicht!

Ziele

- Überblick über die Breite des Gebietes – „…das schwächste Glied der Kette.“
- Annahmen und Voraussetzungen
- Mathematische Grundlagen und –ideen
- Motivation für technische Festlegungen
- Startpunkt für‘s Selbststudium
- Erfahrungen aus der Praxis - wie man‘s richtig und wie man‘s falsch macht: „lernen, wie man ein Verfahren einsetzt“

Nicht-Ziele

- „lernen, wie man ein Verfahren implementiert“
- Mathematik im Detail
- Details von Standards, Software, …

Steganographie

- Griechisch:
  - „steganos“ – verdeckt
  - „graphein“ – schreiben
- ein Dritter merkt nicht, dass kommuniziert wird
- Erste Beispiele bei Herodot, 440 v. Chr.
- Klassische „James Bond“-Techniken
- …aber auch modern:
  digitale Wasserzeichen

Kryptographie

- Griechisch:
  - „kryptos“ – verborgen
- ein Dritter bemerkt Kommunikation, kann aber nichts verstehen
- Schon bei den Ägyptern im 3. Jahrtausend v. Chr. dokumentiert
- Kontinuierliche Entwicklung von verbesserten Verfahren
  - Wettstreit mit der Krypt(o)analyse

Ziele von Kryptographie

- Vertraulichkeit / confidentiality
- Änderungsschutz / integrity
- Fälschungsschutz / authenticity

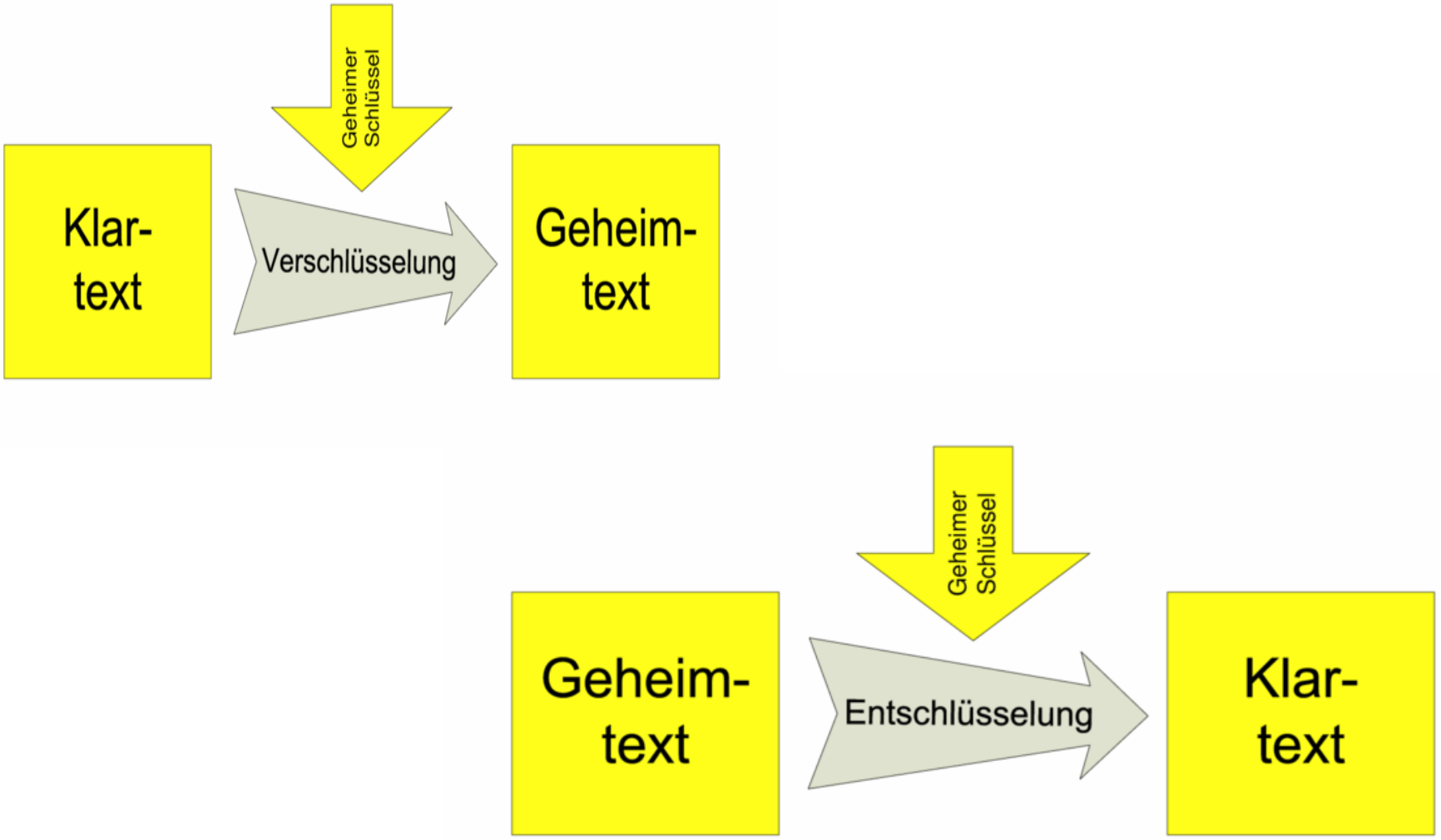
- Nicht-Abstreitbarkeit / non-repudiation
- Erneuerbarkeit / renewability

- Nicht alle Verfahren realisieren alle Ziele

Begriffe

- Chiffre / cipher
  - Verfahren zur Ver-/Entschlüsselung
- Schlüssel / key
  - Parameter des Verfahrens, geheim zu halten
  - Maßeinheit: Bit
- Klartext / clear text
  - Information, die ausgetauscht wird
- Geheimtext / cipher text
  - verschlüsselter Klartext

Begriffe im Bild



Fragen

- Verschlüsselung = Entschlüsslung?
- V-Schlüssel = E-Schlüssel?
- Kodierung von Klar- und Geheimtext?
- Welche Betriebsmittel sind erforderlich?

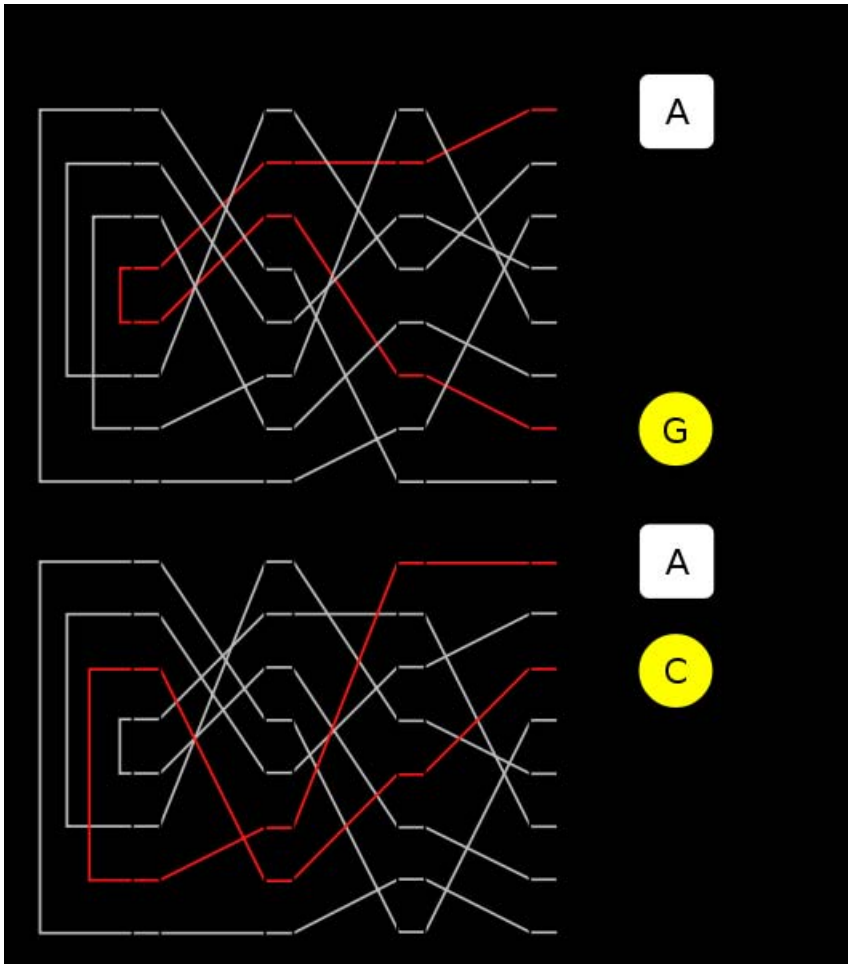
Historische Beispiele

- Transposition – Skytale, Gartenzaun
- Substitution
  - Monoalphabetisch – Julius Caesar
  - Polyalphabetisch – Vignière
  - Bigraphisch – Playfair-Chiffre v. Wheatstone
  - Sherlock Holmes, Lord Peter Wimsey, …
- Enigma im 2. Weltkrieg

Wie knackt man diese Verfahren?

- Sprache ist nicht zufällig
  - hohe Redundanz (ca. 70%)
  - starke kurzreichweitige Korrelationen
  - schwache bis keine langreichweitigen Korr.
  - Vermutungen über Klartext
- Starke Bezüge zur Informationstheorie und angewandter Statistik
  - Shannon
  - entweder ganz zufällig oder ganz regelmäßig
  - ultimativ und unpraktikabel: „one-time pad“

Enigma – „Rätsel“



Annahmen

- Kommunikationspartner sind vertrauens-würdig
- Ihre Betriebsmittel sind vertrauenswürdig und nicht kompromittierbar
- Kommunikation ist *nicht* vertrauenswürdig
- Der Gegner ist „allwissend“

Kerckhoffs‘ Prinzip

- Auguste Kerckhoffs von Nieuwenhoff, 1835-1903, Linguist
- …schrieb 1883 „La cryptographie militaire“
- Heutige Folgerungen
  - Sicherheit beruht auf (Un)kenntnis d. Schlüssels
  - Ein Schlüssel ist leichter erneuerbar als ein Verfahren
  - Veröffentlichte Verfahren sind sicherer
  - Fürchte Dich vor Hintertür(ch)en!

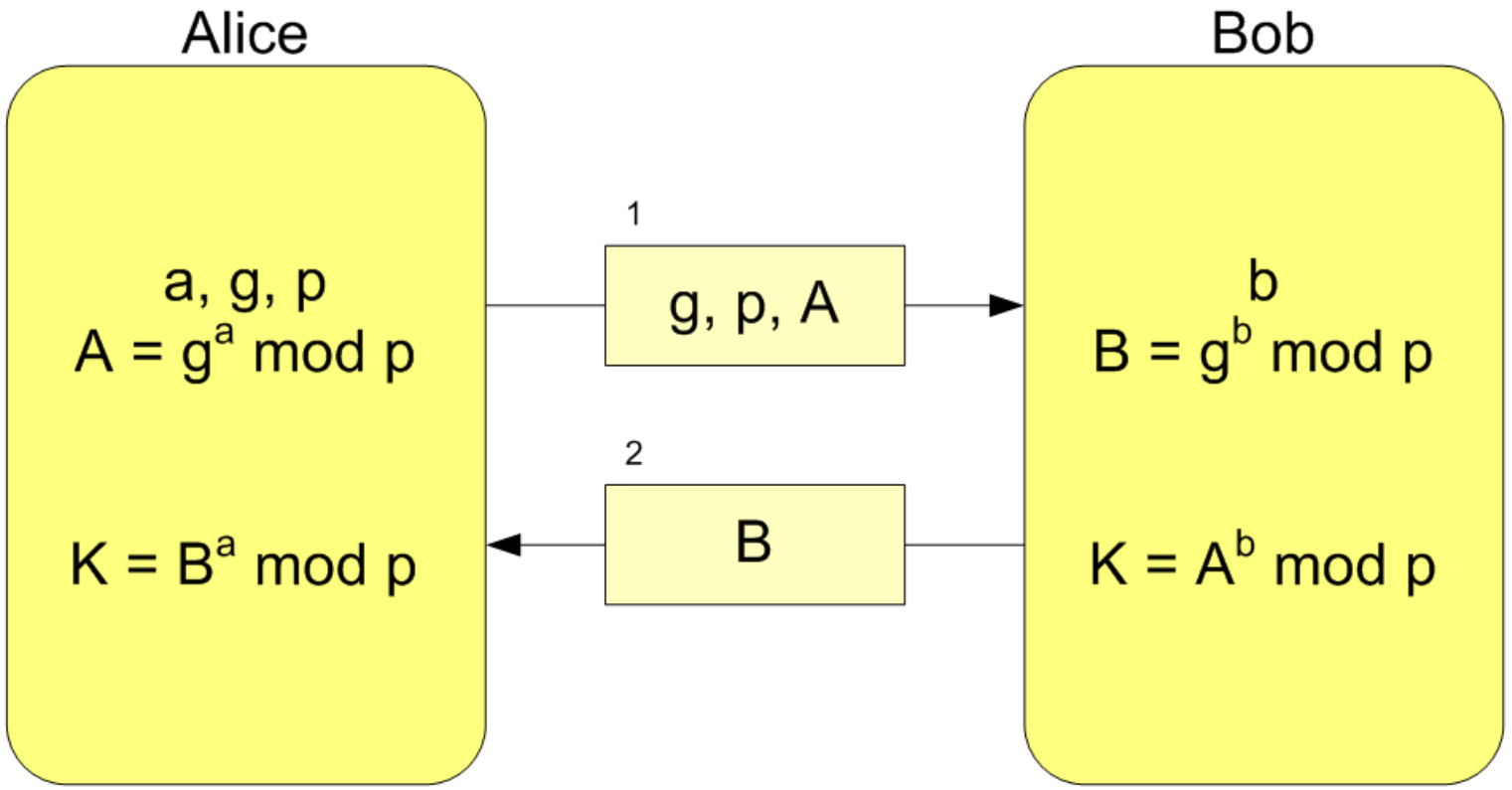
Folgerungen aus Informationstheorie

- Zufallszahlen - „Rauschen“ - sind gut
  - aber schwierig zu produzieren
  - Menschen können‘s schon gar nicht
    - …aber wie helfe ich ihnen, sich „Rauschen“ zu merken?
- Daher:
  - Der Geheimtext sollte „rauschähnlich“ sein
    - z.B. gleich viele 0- und 1-Bits
  - Es hilft, wenn der Klartext auch so ist
    - z.B. durch Kompression
- Das Gegenteil ist auch gut

Diffie-Hellman-Merkle Key Exchange

- Aufgabe: Vereinbare mit der Gegenseite einen Schlüssel,
  - ohne vorher ein gemeinsames Geheimnis zu vereinbaren und
  - ohne dass ein Lauscher („eavesdropper“) den Schlüssel erhalten kann

Wie geht das?



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Bedingungen

- p ist prim
- g ist Primitivwurzel in Z_p
- a, b sind Zufallszahlen

- $a, b < p \Rightarrow p$ muss ausreichend groß sein
- g kann klein sein, typisch 2 oder 5

Warum funktioniert das?

- In Z oder R sind die Umkehroperationen
  - Exponenzieren und
  - Logarithmieren

  gleich aufwändig.
- In Z_p ist das nicht der Fall!

- Analog sind
  - Primzahltesten (Lucas-Lehmer, ECPP) und
  - Faktorisierung einer Zahl

  verschieden aufwändig.

Was leistet das Verfahren nicht?

- Authentisierung
- Verschlüsselung an sich

- Komponente mehrerer Protokolle (IKE, …)
- Kompromittierbar, falls
  - *p* bestimmte Eigenschaften nicht erfüllt
  - *a, b* nicht ausreichend zufällig

Angriffe

- …gefährden ein kryptographisches Verfahren oder eine konkrete Umsetzung

- Wer? – Eve und ihre Schlange
- Wo?
- Mit welchen Mitteln?
- Unter welchen Voraussetzungen?
- Welches Schadenspotential?

Grobe Klassifikation

- Angriffe auf das Verfahren an sich
- Angriffe auf die Implementierung
- Angriffe auf die Kommunikation
- Angriffe auf die Beteiligten / Betriebsmittel

Angriffe auf das Verfahren

- Schlüsselraum ist zu klein
  - „brute force search“ erfolgreich
  - Maßstab für die Qualität eines Verfahrens
- Math. Analyse offenbart Schwachstellen
  - „weak keys“ in DES
  - Enigma: Reduktion des Schlüsselraums
- Klartextanalyse
  - Enigma: Feste Texte in Funksprüchen
- Geheimtextanalyse

Angriffe auf die Implementierung

- Fehlerhafte Implementierung reduziert Komplexität
  - WEP
  - fehlerbehaftete Multiplikation
- (differential) power analysis
  - z.B. bei smartcards oder USB-Tokens
  - s. kürzliche Angriffe auf RFID-Karten
- Seitenkanal-Angriffe
  - Rechenzeiten, Laufzeiten, …

Angriffe auf die Kommunikation

- „man in the middle“
  - auch bei Zusendung von Karte und PIN
- „impersonation“
- Eingabe einer PIN
- Speichern der Kommunikation und spätere Analyse

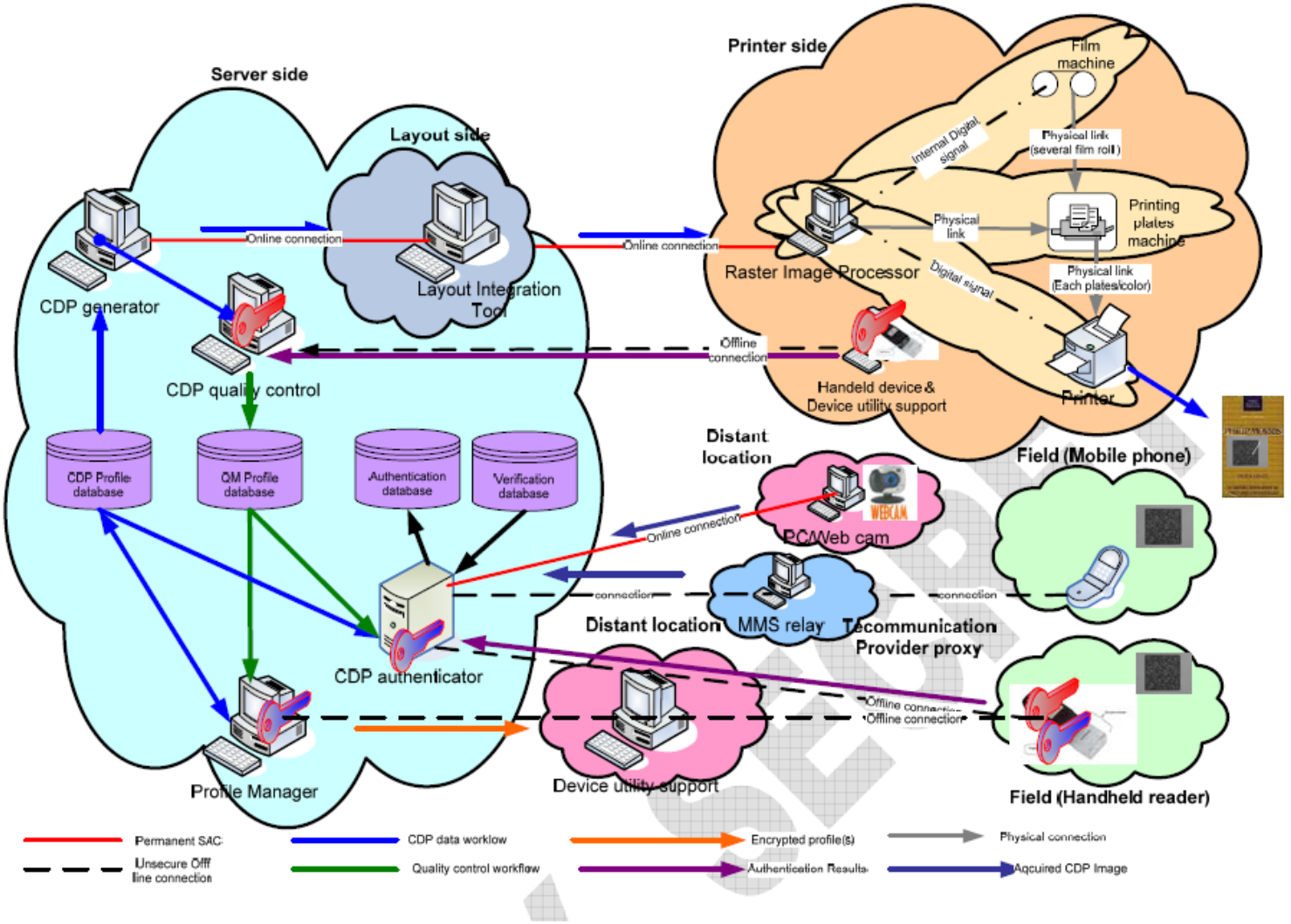
Angriffe auf die Beteiligten

- Bestechung, Erpressung von Mitarbeitern
- „social engineering“
- Diebstahl von Betriebsmitteln
- Manipulation von Betriebsmitteln
  - „key logger“ – FBI vs Mafia-Pate

„Threat Analysis“

- Methodisches Vorgehen zur Analyse von potentiellen Bedrohungen
- Festlegung von möglichen Gegenmaßnahmen
- Kriterien (Beispiele)
  - Auswirkung
  - Wahrscheinlichkeit des Auftretens
  - Risikoaversion
  - Fähigkeiten des Angreifers

Überblick Arbeitsablauf, Betriebsmittel



Kriterien

I0	**Negligible** impact: Impact is negligible or null
I1	**Low** impact: Small impact which is not a human perceptible. Security incident may be bypassed by workaround.
I2	**Medium** impact: Human perceptible impact that cause limited financial loss or that does not cause durable service loss.
I3	**High** impact: Impact that cause durable service interruption, great financial or brand image losses.
I4	**Very high** impact: Impact that cause irreversible damage. In one word, underlying technology could be considered as too weak for secure usage. It may also involve service that can not be recovered for long time.

P0	**negligible** potentiality : << 1 time upon Δ,
P1	**low** potentiality ; < 1 time upon Δ,
P2	**certain** potentiality ; = 1 time upon Δ,
P3	**high** potentiality ; > 1 time Δ , ~ 3 occurrences per Δ
P4	**very high** potentiality ; very >> 1 time Δ , 1 occurrence during each event

A0	**Negligible** risk or residual risk : no countermeasure is provided
A1	**identified** risk, supportable or tolerate : countermeasures may be applied according cost
A2	**serious** risk : Countermeasures must be applied and consigned in a project plan
A3	**critical** risk : countermeasures shall be immediately planned
A4	**insupportable** risk: immediate countermeasure or action shall be taken into account

Analyse einer Bedrohung

T[1.4] Eavesdrop a CDP element together with the theft of an identification

Asset: The communication link that conveys a CDP in different form factors. It can refer to a communication link such as the Link between the CDP generator and the Layout IT Link between the Layout IT and the RIP machine, Device support utility link. This also requires the disclosure of identification such as VPN/SSL identification between the CDP generator and the Layout IT, VPN/SSL identification between the layout IT and the RIP machine, or the Handheld communication secret key.

Description: The attack consists in first spoofing and then storing a network communication where CDP elements are conveyed. This also requires the theft of the identification element of the communication link. Therefore, an attacker may decrypt and access the digital CDP content. External IT or network-based attacks that exploit vulnerabilities on the given communication link must be considered. As an example, if an IPSEC VPN is used, it has the potential vulnerability of allowing site-to-site connected users access to entire network resources.

Risk probability: P0 (Hacker), P3 (Insider), P1 (Industrial), P2 (Mafia)

Countermeasures: See also Separation of duties (CM[16])

CM[11] IT security: *Assessment of the IT security of the various links concerned.*

Ergebnis einer Analyse

Threat Nb	Identified Threat	content impact	max risk aversion	amateur /hacker	Insider	Industrial	Mafia
T[1.1]	Reproduce a CDP from an analog CDP image acquisition	confidentiality	A4	P0	P0	P2	P2
T[1.2]	Scan and re-print a CDP with powerful equipment	confidentiality	A4	P0	P0	P1	P1
T[1.3]	Theft of a CDP element and reproduce a copy	confidentiality	A4	P1	P4	P2	P3
T[1.4]	Eavesdrop a CDP element together with the theft of an identification	confidentiality	A4	P0	P3	P1	P2
T[1.5]	Reproduce a CDP with the original elements at the server side	confidentiality	A4	P1	P4	P2	P3
T[1.6]	Reproduce a CDP with the original elements with handheld device	confidentiality	A4	P1	P2	P2	P3
T[1.7]	Get a generated CDP image from internal memory	confidentiality	A4	P2	P2	P4	P4
T[1.8]	Eavesdrop a CDP printing signal and re-apply it later	confidentiality	A4	P0	P2	P1	P1
T[2.1]	Reverse CDP data from the MSBP SDK implementation	confidentiality	A4	P1	P2	P2	P3
T[2.2]	Reverse CDP from tampering the handheld reader	integrity	A4	P2	P2	P4	P4
T[3.1]	Alter the integrity of checked elements on server side	integrity	A3	P0	P3	P0	P0
T[3.2]	Alter the integrity of the verification process for the mobile phone	integrity	A3	P1	P2	P0	P0
T[3.3]	Alter the integrity of the verification process for handheld device	integrity	A2	P1	P1	P0	P1
T[3.4]	Alter the integrity of the generation process	integrity	A2	P1	P1	P0	P0
T[3.5]	Alter the integrity of the records	integrity	A2	P1	P1	P0	P0
T[4.1]	Hamper the generation process through a denial of service	availaibility	A2	P1	P1	P0	P0
T[4.2]	Hamper the verification process through a denial of service	availaibility	A2	P2	P1	P0	P2
T[5.1]	Loss of traceability and control of the handheld device	traceability	A3	P1	P0	P1	P3
T[5.2]	Loss of traceability and control of the CDP	traceability	A3	P1	P2	P1	P3
T[5.3]	Loss of traceability and control of the MSBP SDK	traceability	A2	P1	P2	P1	P2
T[5.4]	Loss of control of confidential elements of documentation	traceability	A2	P0	P2	P1	P2