Die Praxis der IT-Sicherheit:
Ziele, Prioritäten, status quo

Hannes Federrath

http://www.inf.fu-berlin.de/~feder/

Was sind die Ziele?

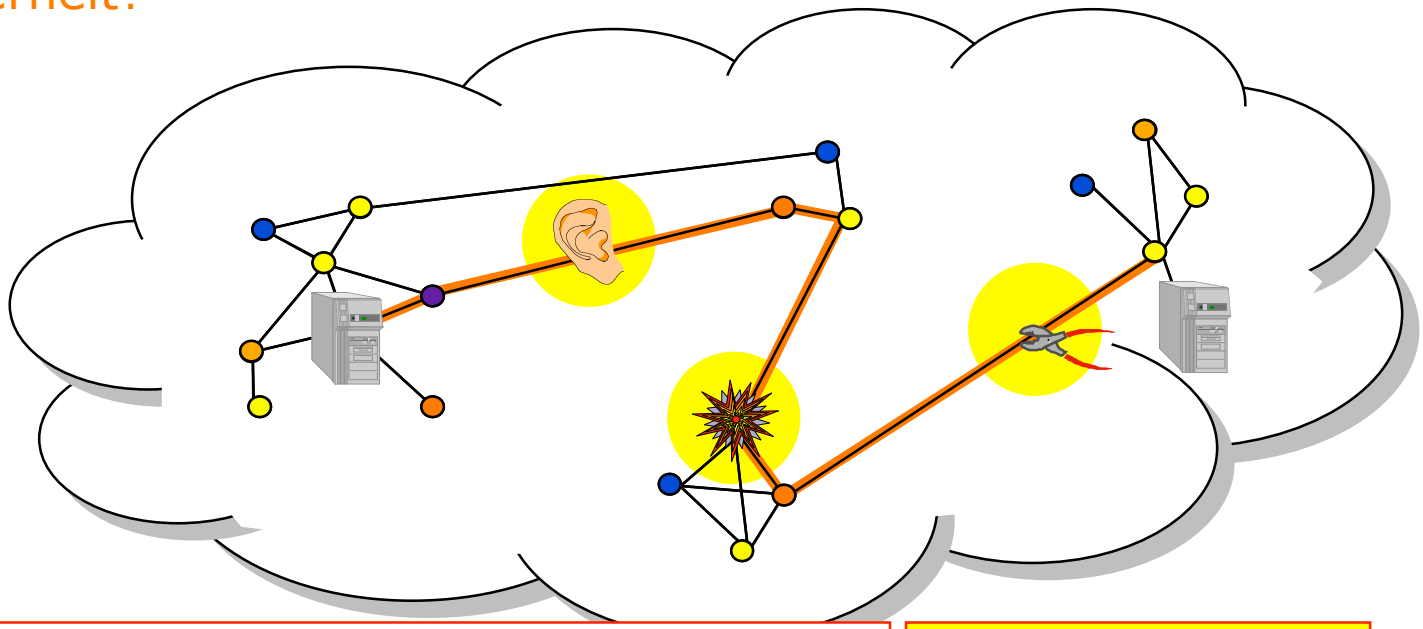
Was brauchen wir?

Wo stehen wir heute?

Was sind die Prioritäten?

Problemstellung

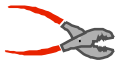
⌘ Was ist Sicherheit?



Bedrohungen

 unbefugter Informationsgewinn

 unbefugte Modifikation

 unbefugte Beeinträchtigung der Funktionalität

Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Sicherheit: Abgrenzung von Security & Safety

SECURITY
Schutz gegen beabsichtigte Angriffe

Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit
- Ermöglichen von Kommunikation

SAFETY
Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

Schutzziele: Einordnung

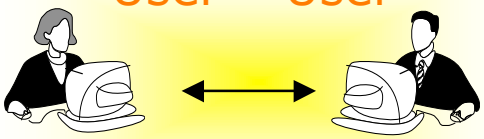
	WAS?	WANN?, WO?, WER?
	Kommunikations-gegenstand	**Kommunikations-umstände**
Un-erwünschtes verhindern	**Vertraulichkeit** **Verdecktheit** **Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Empfänger** **Ort**
Erwünschtes leisten	**Integrität** **Inhalte**	**Zurechenbarkeit** **Senden** **Empfangen**
	Verfügbarkeit **Inhalte**	**Erreichbarkeit** **Rechtsverbindlichkeit** **Bezahlung**

Schutzziele und deren Durchsetzung

- Schutz gegen Bedrohungen erstreckt sich auf viele existentielle Bereiche
  - Schutz des Bürgers
  - Schutz von Firmen
  - Schutz des Staates
- Gegensätzliche Interessen
  - Aushandlungsprozess zwischen den Interessen

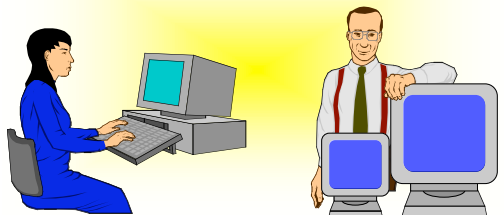
- Konzept Mehrseitige Sicherheit
  - besitzt das Potential, die Probleme zu lösen
  - ursprünglich entwickelt, um Kräfteausgleich zwischen den Akteuren zu erzielen

User – User



User – Netzbetreiber

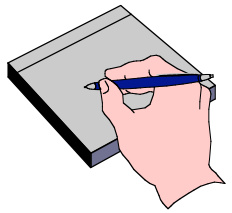
Kunde – Händler



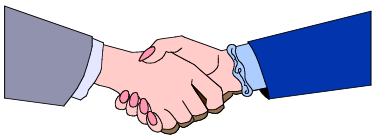
Mehrseitige Sicherheit

- Jeder Beteiligte hat **Sicherheitsinteressen**.

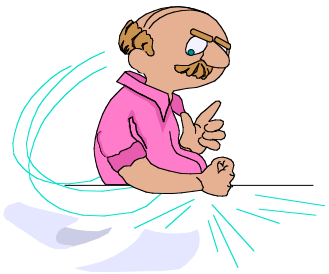
- Jeder Beteiligte kann seine Interessen **formulieren**.



- Konflikte werden erkannt und Lösungen **ausgehandelt**.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.

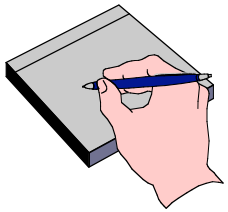


Sicherheit mit minimalen Annahmen über andere.
So wenig wie möglich Vertrauen in andere setzen müssen.

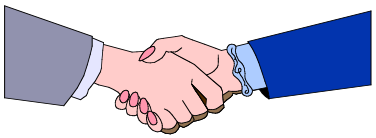
Mehrseitige Sicherheit: Wie?

- Jeder Beteiligte hat **Sicherheitsinteressen**.
  - Schutzziele

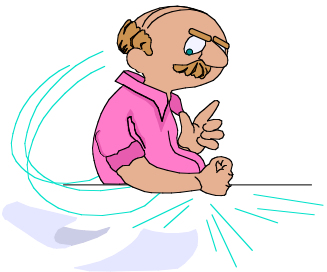
- Jeder Beteiligte kann seine Interessen **formulieren**.
  - Setzt Verständnis des Benutzers voraus
  - Gute Bedienoberflächen sind nötig



- Konflikte werden erkannt und Lösungen **ausgehandelt**.
  - Setzt entsprechende Tools und
  - Technische Protokolle voraus



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.
  - Anwender brauchen Werkzeuge zum Selbstschutz



Die Praxis der IT-Sicherheit:
Ziele, Prioritäten, status quo

Was sind die Ziele?

Was brauchen wir?

Wo stehen wir heute?

Was sind die Prioritäten?

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verschlüsselungsverfahren

- **Symmetrische Verschlüsselung, z.B. DES, AES**
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits
- **Asymmetrische Verschlüsselung, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Verschlüsselungsschlüssel
    - *Privaten* Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit
- **Bekannte Verschlüsselungssoftware**
  - Pretty Good Privacy
  - http://www.pgp.com

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

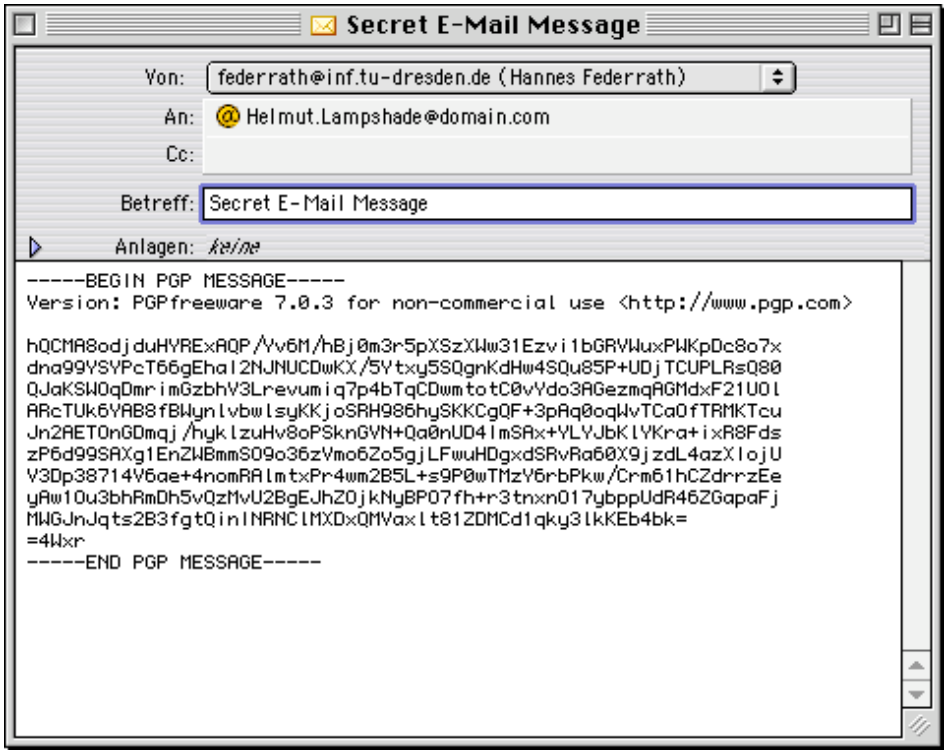
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verschlüsselungssoftware

- Pretty Good Privacy
  - http://www.pgp.com
- Gnu Privacy Guard
  - http://www.gnupg.org



Verdecktheit: Steganographie

Vertraulichkeit

Verdecktheit

Integrität
Zurechenbarkeit

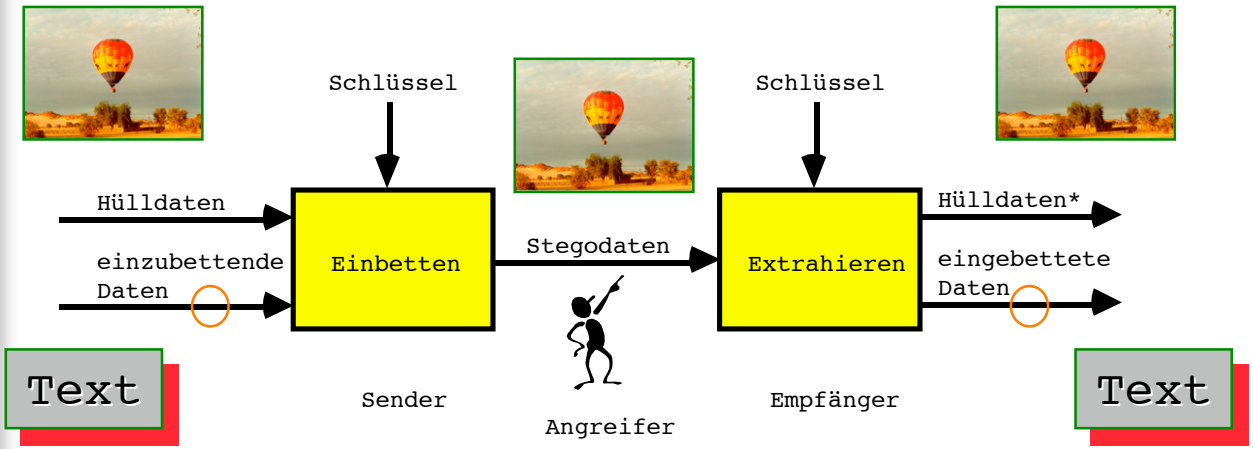
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**
  - geheimzuhaltende Nachricht wird in eine Hülle eingebettet
  - minimale Veränderungen kaum bzw. nicht erkennbar
  - Veränderungen nicht mit Messmethoden nachweisbar



Integrität und Zurechenbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Message Authentication Codes

- **Symmetrisches Verfahren**
  - Kommunikationspartner teilen ein gemeinsame Geheimnis (symmetrischer Schlüssel)
- **Gehört heute zum Grundschutz**
  - Verfälschungen von Nachrichten (böswillige und zufällige) sind erkennbar
- **Keine Nachweisbarkeit gegenüber Dritten**

Digitale Signatur

- **Asymmetrisches Verfahren, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Testschlüssel
    - *Privaten* Sigierschlüssel
- **Nachweisbarkeit gegenüber Dritten**
- **Ebenfalls einsetzbar:**
  - Pretty Good Privacy
  - http://www.pgp.com

Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Adressierungsinformationen können nicht verschlüsselt werden**
  - Problem Verkehrsdaten:
    - Wer mit wem, wann, wie lange, wo, wieviel Information?
  - Problem Interessensdaten:
    - Wer interessiert sich für was?

- **Spezielle Verfahren:**
  - Proxies
  - Mix-Netz
  - DC-Netz
  - Dummy traffic
  - ...

Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

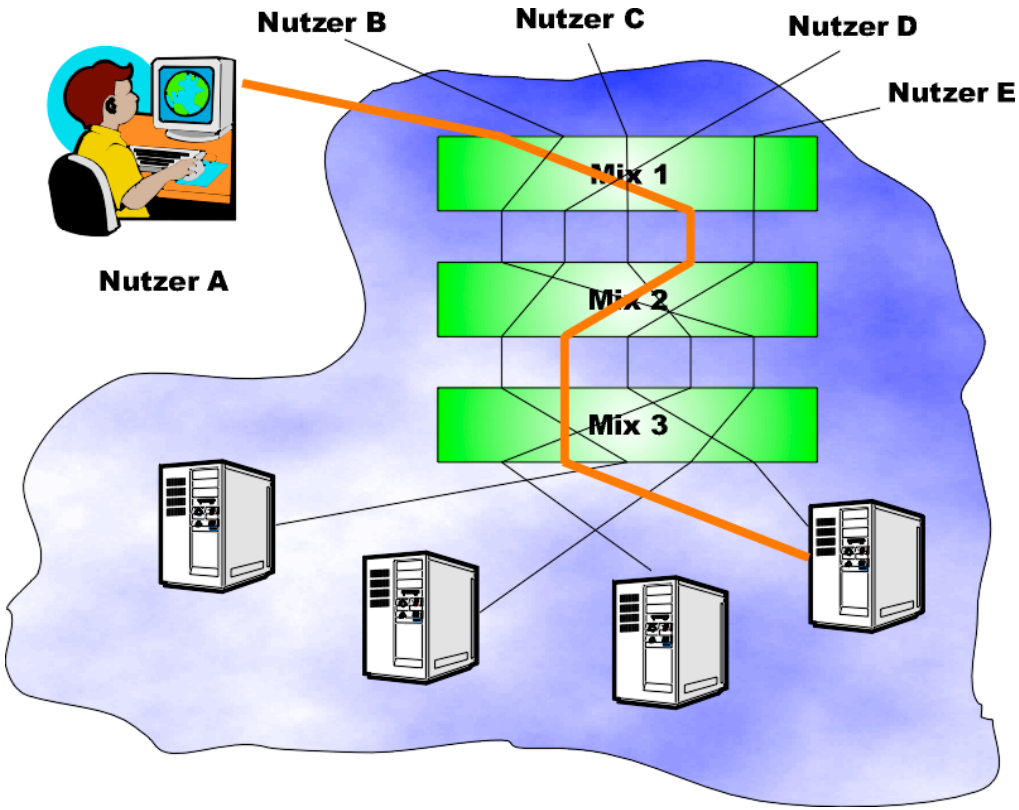
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://jap.inf.tu-dresden.de



Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

- **Verfügbarkeit**
  - Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.
- **Erreichbarkeit**
  - Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.
- **»Mechanismen«**
  - Mehrfach redundante Leitungsführung
  - Diversitärer Entwurf der Komponenten
  - Starke Vermaschung der Kommunikationsverbindungen
- **Techniken zur Verteilung von Kontrolle**
  - Offenlegung von Designkriterien und Algorithmen
  - Open Source Software
  - Sichere Betriebssysteme

Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

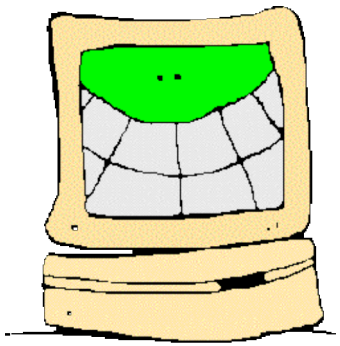
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

Denial-of-Service-Angriffe

- **DoS-Angriffe auf Schwachstellen im System**
  - Mail-Bombing – Spamming
  - Broadcast-Storm
  - SYN-Flooding
  - Angriffe auf einen Switch
- **DoS-Angriffe auf Implementationsfehler**
  - Ping of Death
  - WinNuke
  - Teardrop und Nachfahren



Vorher

Nachher

Rechtsverbindlichkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

- **Rechtsverbindlichkeit**
  - Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.
  - Kann nicht technisch geschaffen werden
- **Rechtsverbindlichkeit der Digitalen Signatur**
  - Klare Regeln bzgl. Beweiswert
  - Zertifizierung von Schlüsseln (Public Key Infrastructure PKI)
- **Sicherheit der Netzkomponenten**
  - Zertifizierung von Netzkomponenten
  - Physische Sicherheit, immer dann, wenn Vertrauen in fremde Netzkomponente aufgebracht werden muss.

Die Praxis der IT-Sicherheit:
Ziele, Prioritäten, status quo

Was sind die Ziele?

Was brauchen wir?

Wo stehen wir heute?

Was sind die Prioritäten?

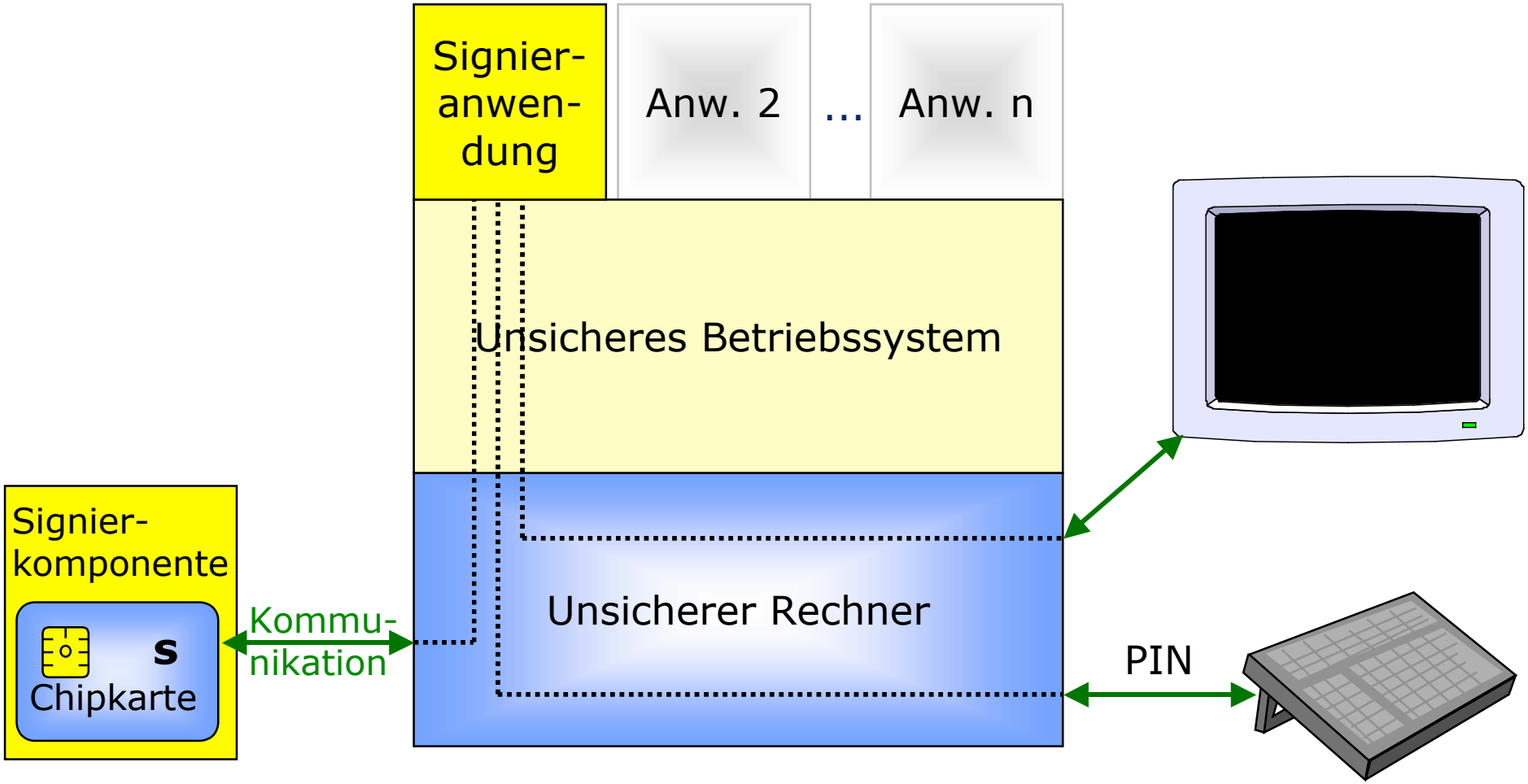
Was sind die Prioritäten?

- Mehr Transparenz erreichen
  - Offenlegung des Quellcodes
  - Förderung von Open Source
- Mehr Diversität erreichen
  - Sichere Betriebssoftware
  - Sichere Hardware *für* denjenigen, der sie betreibt
- Investions- und Urheberschutz erhalten
  - Digital Rights Management Systeme
  - Sichere Hardware *gegen* denjenigen, der sie betreibt
- Möglichkeiten zum Selbstschutz stärken und fördern
  - leicht bedienbare Tools

Standard-PC mit Chipkarte

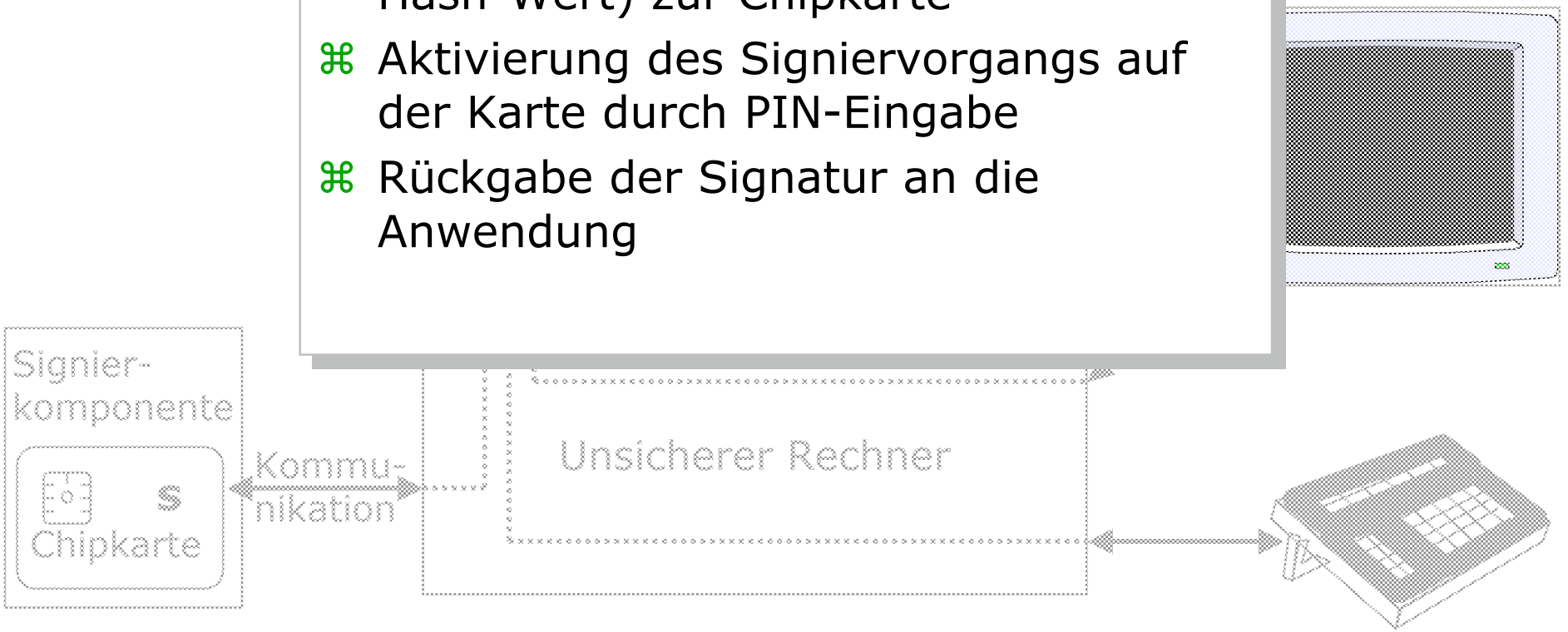
⌘ Sichere Geräte sind eine Voraussetzung für sichere Signaturen

UNSICHER



Ablauf auf Standard-PC mit Chipkarte

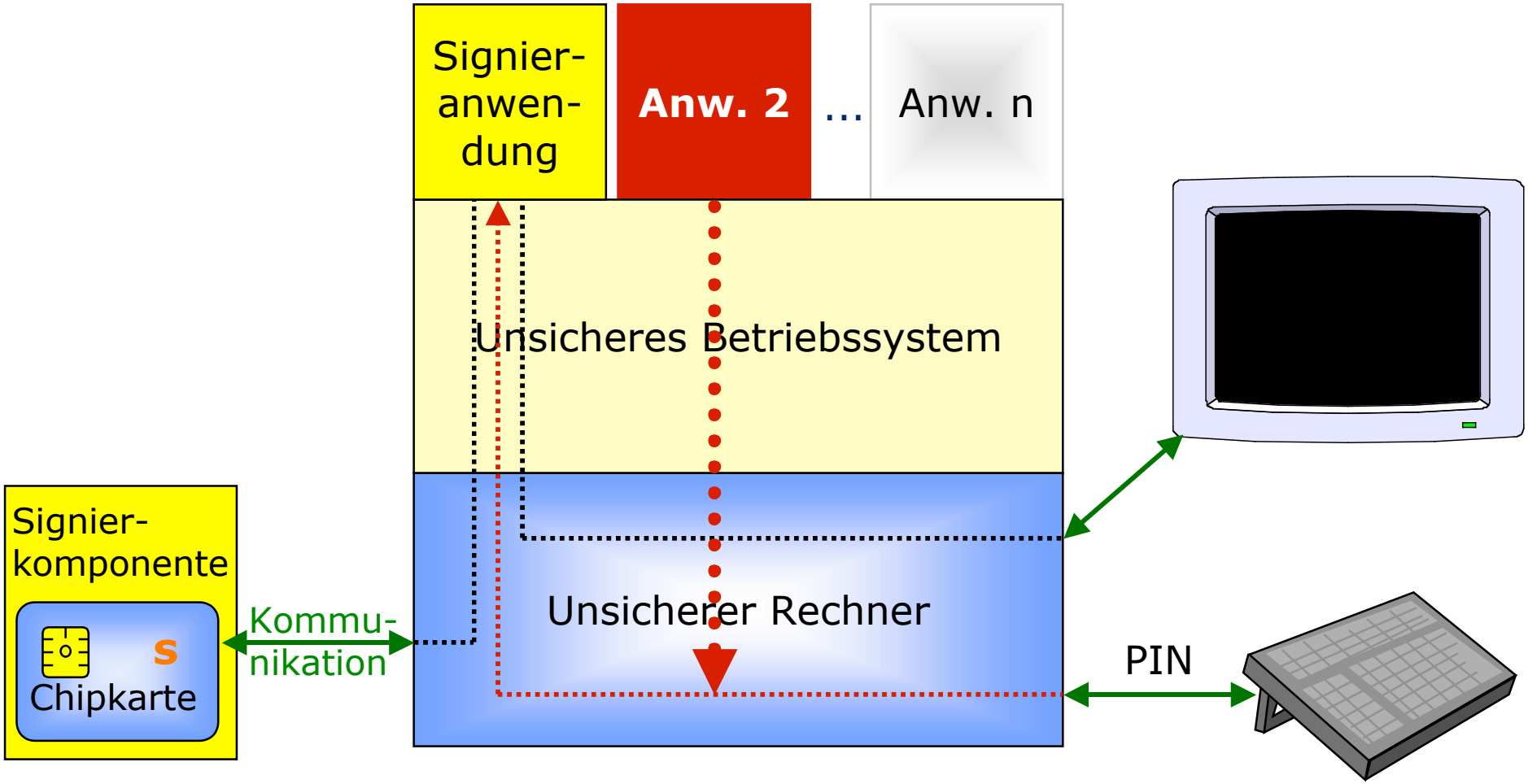
- Anzeige des Dokuments auf dem externem Monitor
- Senden des Dokuments (bzw. dessen Hash-Wert) zur Chipkarte
- Aktivierung des Signiervorgangs auf der Karte durch PIN-Eingabe
- Rückgabe der Signatur an die Anwendung



Standard-PC mit Chipkarte

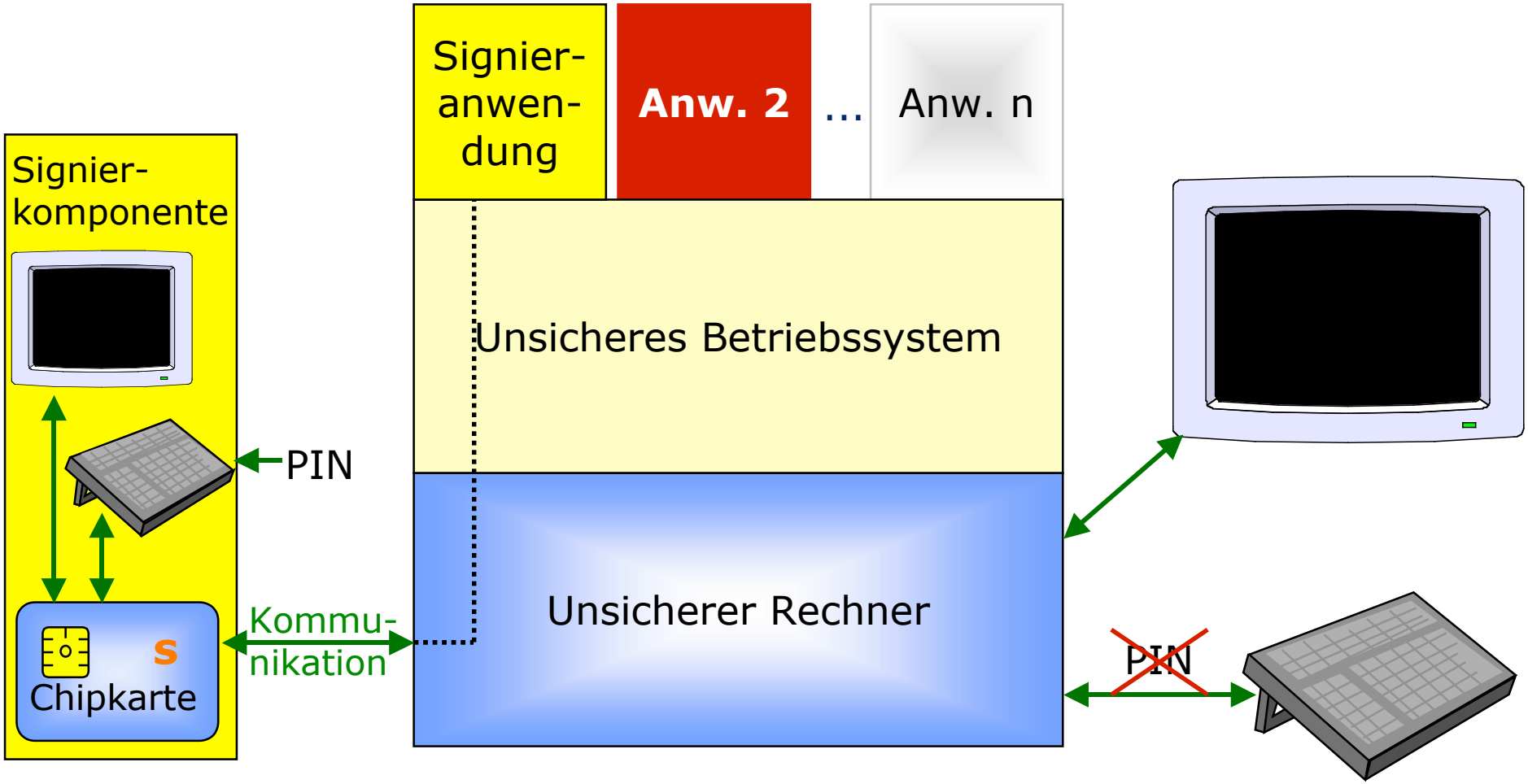
UNSICHER

Bösartige Anwendung könnte z.B. PIN abfangen oder Text nach Anschauen und vor Senden an Signierkomponente heimlich ersetzen



Sichere Signierkomponente mit Standard-PC

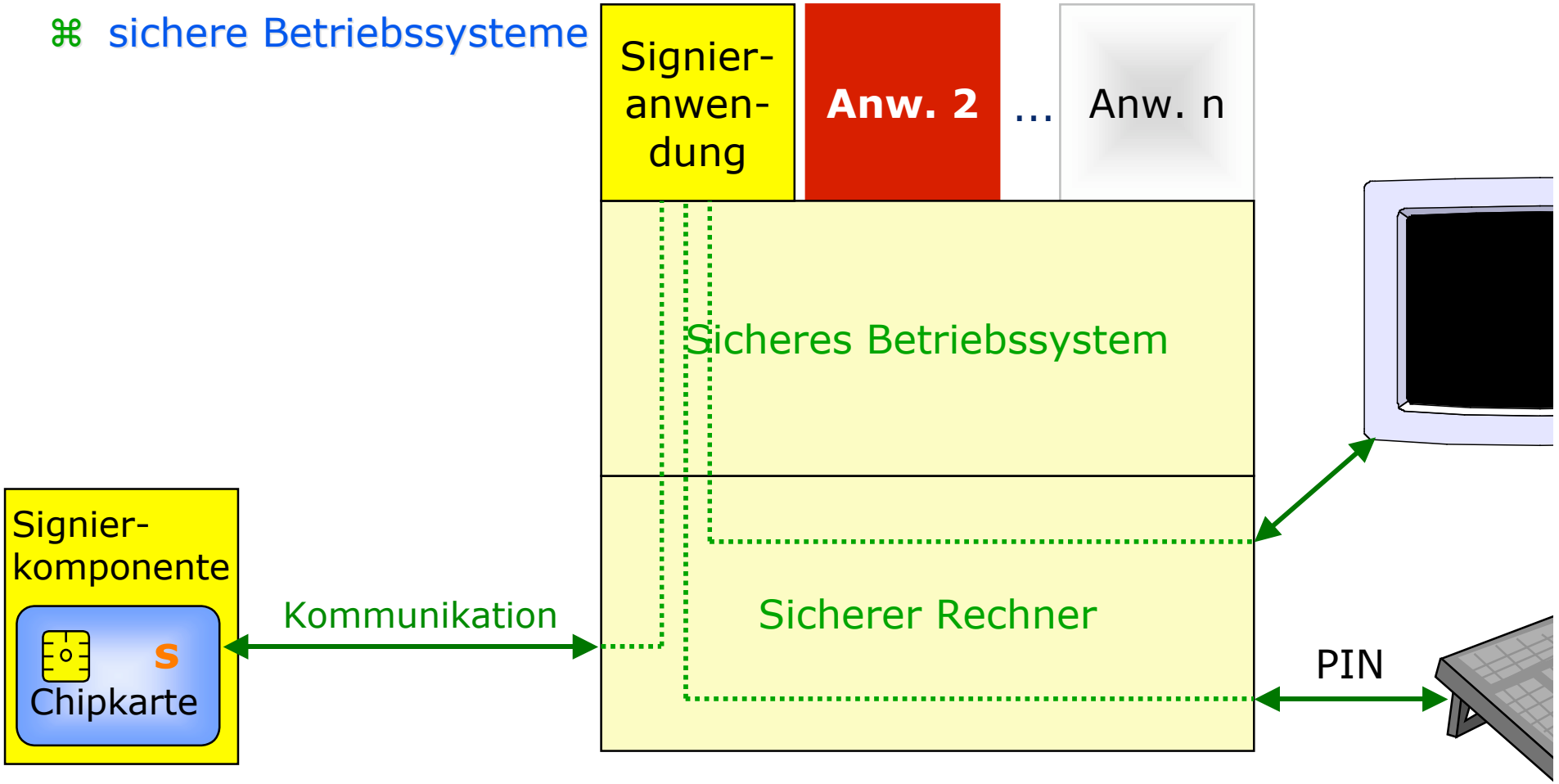
SICHER



Physisch sichere Geräte und sichere Betriebssysteme

SICHER, wenn

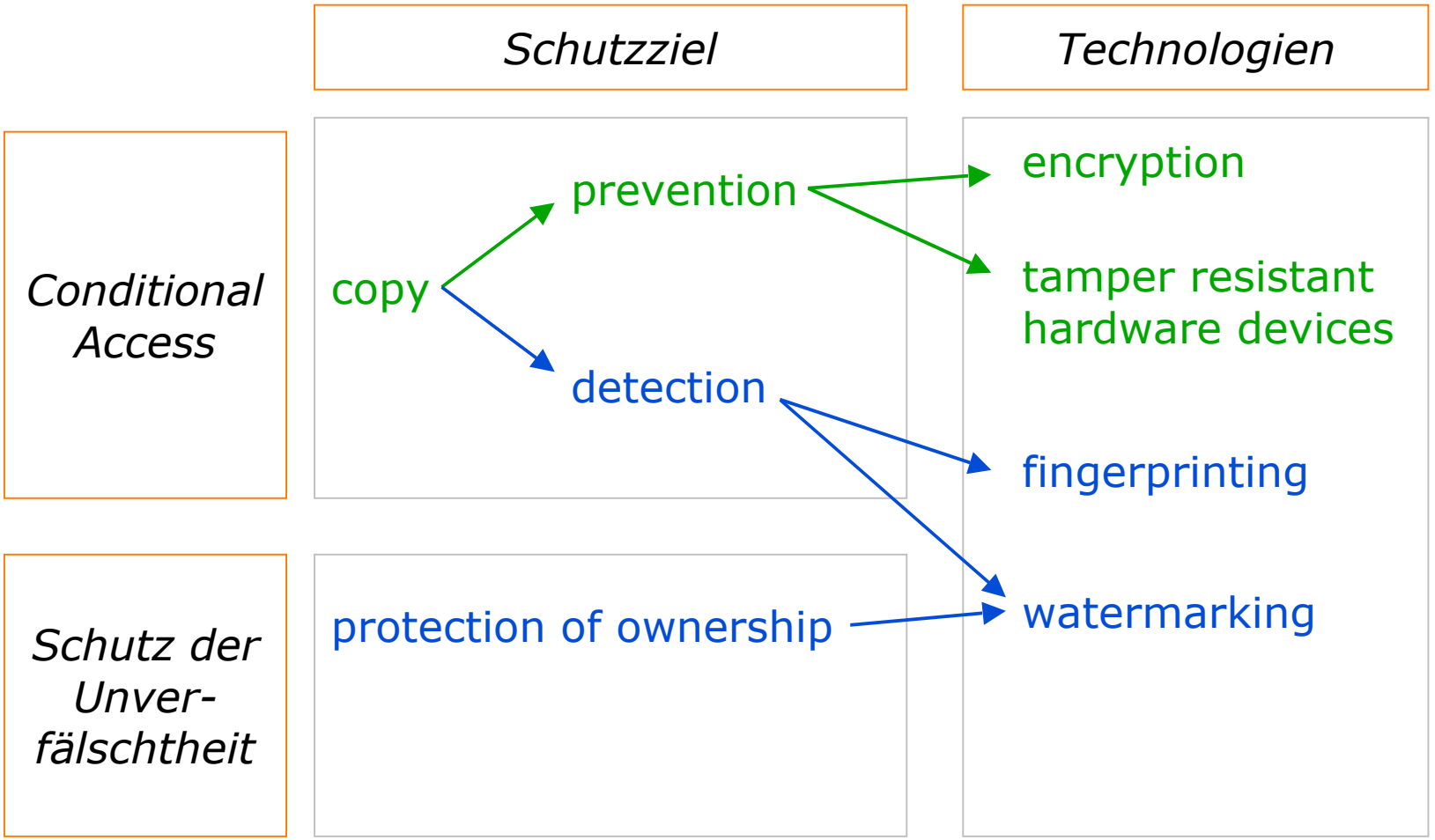
- Physisch sichere Geräte
- sichere Betriebssysteme



Was sind die Prioritäten?

- Mehr Transparenz erreichen
  - Offenlegung des Quellcodes
  - Förderung von Open Source
- Mehr Diversität erreichen
  - Sichere Betriebssoftware
  - Sichere Hardware *für* denjenigen, der sie betreibt
- Investions- und Urheberschutz erhalten
  - Digital Rights Management Systeme
  - Sichere Hardware *gegen* denjenigen, der sie betreibt
- Möglichkeiten zum Selbstschutz stärken und fördern
  - leicht bedienbare Tools

Schutzziele und Techniken in DRM-Systemen



Tendenzen

- "Reverse engineering" von DRM Systemen
  - Nutzbarmachen von Inhalten auf alternativen Betriebssystemen
  - Unabhängigmachen von einem bestimmten Software- und Hardwareproduzenten
- Piraten könnten zukünftig legal erworbene Inhalte direkt vom Computer unbedarfter Nutzer abgreifen
  - Trojanische Pferde
- Viele Angriffe sind inzwischen automatisiert
  - Angriffswerkzeuge sind kostenlos im Internet herunterladbar
  - Aus Laien werden Piraten

Sichere DRM-Systeme

- Sichere DRM-Systeme verknüpfen ein DRM-Signal so eng mit dem Inhalt, dass der Inhalt ohne das DRM-Signal nutzlos ist.

- Gestaltungsspielraum
  - DRM-Signal ist Teil des Inhalts (z.B. wie bei Watermarking-Systemen)
  - DRM-Signal ist nötig, um den Inhalt zu entschlüsseln bzw. zuzugreifen
- Wichtig:
  - Detektor für das DRM-Signal darf nicht umgangen werden können
  - Hardware- oder Software-Kapselung

- Software
  - nicht empfehlenswert
- Hardware
  - hilft nur begrenzte Zeit je nach (finanziellem) Aufwand

DRM-Systeme: Künftige Forschungsfelder

- Klassifikation und Evaluation
  - Wie kann die Stärke eines DRM-Systems gemessen werden?
  - Evaluationskriterien
  - Kategorisierung von Angriffen
- Schnittstellen
  - Application Programming Interfaces (APIs)
  - Enforcement Interfaces (Erkennen von unberechtigter Nutzung)
  - Updating Interfaces (Aktualisierung, nachdem Verfahren gebrochen wurde)
- DRM-Architekturen
  - Software: Multimedia Home Platform (MHP)
  - Hardware: Trusted Computing Platform Alliance (TCPA)

Was sind die Prioritäten?

- Mehr Transparenz erreichen
  - Offenlegung des Quellcodes
  - Förderung von Open Source
- Mehr Diversität erreichen
  - Sichere Betriebssoftware
  - Sichere Hardware *für* denjenigen, der sie betreibt
- Investions- und Urheberschutz erhalten
  - Digital Rights Management Systeme
  - Sichere Hardware *gegen* denjenigen, der sie betreibt
- Möglichkeiten zum Selbstschutz stärken und fördern
  - leicht bedienbare Tools

Selbstschutz-Tools: Beispiele

- Verschlüsselung, Signatur
  - PGP, GnuPG
- Filter
  - Webwasher, JunkBuster, CookieCooker
- Personal Firewall
  - Norton Personal Firewall, Zone Alarm
- Anonymisierer
  - Anonymizer, JAP
- Sichere Dienste anstelle ihrer unsicheren Vorläufer verwenden
  - telnet ssh, ftp scp, http https
- Betriebssysteme mit Zugriffskontrolle/Rechtevergabe/OpenSource
  - Linux, BSD

Was sind die Prioritäten?

- Mehr Transparenz erreichen
  - Offenlegung des Quellcodes
  - Förderung von Open Source
- Mehr Diversität erreichen
  - Sichere Betriebssoftware
  - Sichere Hardware *für* denjenigen, der sie betreibt
- Investions- und Urheberschutz erhalten
  - Digital Rights Management Systeme
  - Sichere Hardware *gegen* denjenigen, der sie betreibt
- Möglichkeiten zum Selbstschutz stärken und fördern
  - leicht bedienbare Tools