Autopsie einer Anwendung im Gesundheitswesen

oder

Wie funktioniert eigentlich: Sicherheits- + Kryptoanalyse?

Ein Beispiel aus der Praxis

Thomas.Maus@alumni.uni-karlsruhe.de

Fahrplan

- Einleitung
- Auswahl und Beschreibung des Beispiels
- **Die Analyse**
- Einige Anmerkungen
- Fragen und Diskussion

Einleitung

Interessant für Wen?

- Nachwuchs
  Wie läuft eine Sicherheitsanalyse ab?
- Sicherheitsverantwortliche + Systemnutzer
  Was kann eine Sicherheitsanalyse leisten?
- Systemarchitekten + -entwickler
  Was sind die leicht vermeidbaren Fehler?
  Warum gehört ein Sicherheitsarchitekt ins Team?
- Öffentlichkeit
  Warum sind „Hacker“ unverzichtbar?

Einleitung ...

Warum ich?

- die freundliche Einladung des Veranstalters ;-)
- ein Vierteljahrhundert Erfahrung in IT + IT-Sicherheit
- ein gutes Dutzend Jahre Beratungspraxis als freier Sicherheits-Analytiker + -Architekt
- ein interessantes Beispiel parat

Auswahl des Beispiels

- **explizite Erlaubnis** des Auftraggebers!
  teilweise Entbindung von Geheimhaltungspflicht
- Parteigutachten in Rechtsstreit → strittig, aber prinzipiell öffentlich
- wurde mit öffentlichen Gelder gefördert
- Gesundheitswesen → betrifft praktisch jeden
- Gesundheitswesen → sehr schutzbedürftige Daten
- besonders reiche Fundgrube → sehr lehrreich

Beschreibung des Beispiels

Problemstellung aus dem Gesundheitswesen:

- Vermeidung von Doppeluntersuchungen
- Bereitstellung der Patientenakte an alle behandelnden Ärzte (unbekannte Adressaten!)
- Verfügungsgewalt über Akte beim Patienten
- ärztliche Schweigepflicht (juristisch bedeutsam!)

Erhofft:

- Kostenersparnis
- Effizienz+Qualitätssteigerungen

Beschreibung des Beispiels ...

Lösungsansatz des Beispielsystems:

- Daten lagern beim Arzt
- werden zum Austausch auf zentralen Server verschlüsselt zwischengelagert
- Abruf vom Überweisungsziel mittels „Einmal-Schlüssel“ des Patienten
- Schutz vor Betreiber und Teilnehmern: Verschlüsselung und Zugriffsklassen

(Laut Befund – Problem: Abweichung Ist/Soll!)

Die Analyse

- Ziele + Grenzen
- Strukturanalyse
- Verdachtsmomente
- Schutzziele + Schutzobjekte
- Bedrohungsannahmen
- Schwachstellenanalyse
- Dokumentation + Berichterstattung

Ziele + Grenzen

Ziele:

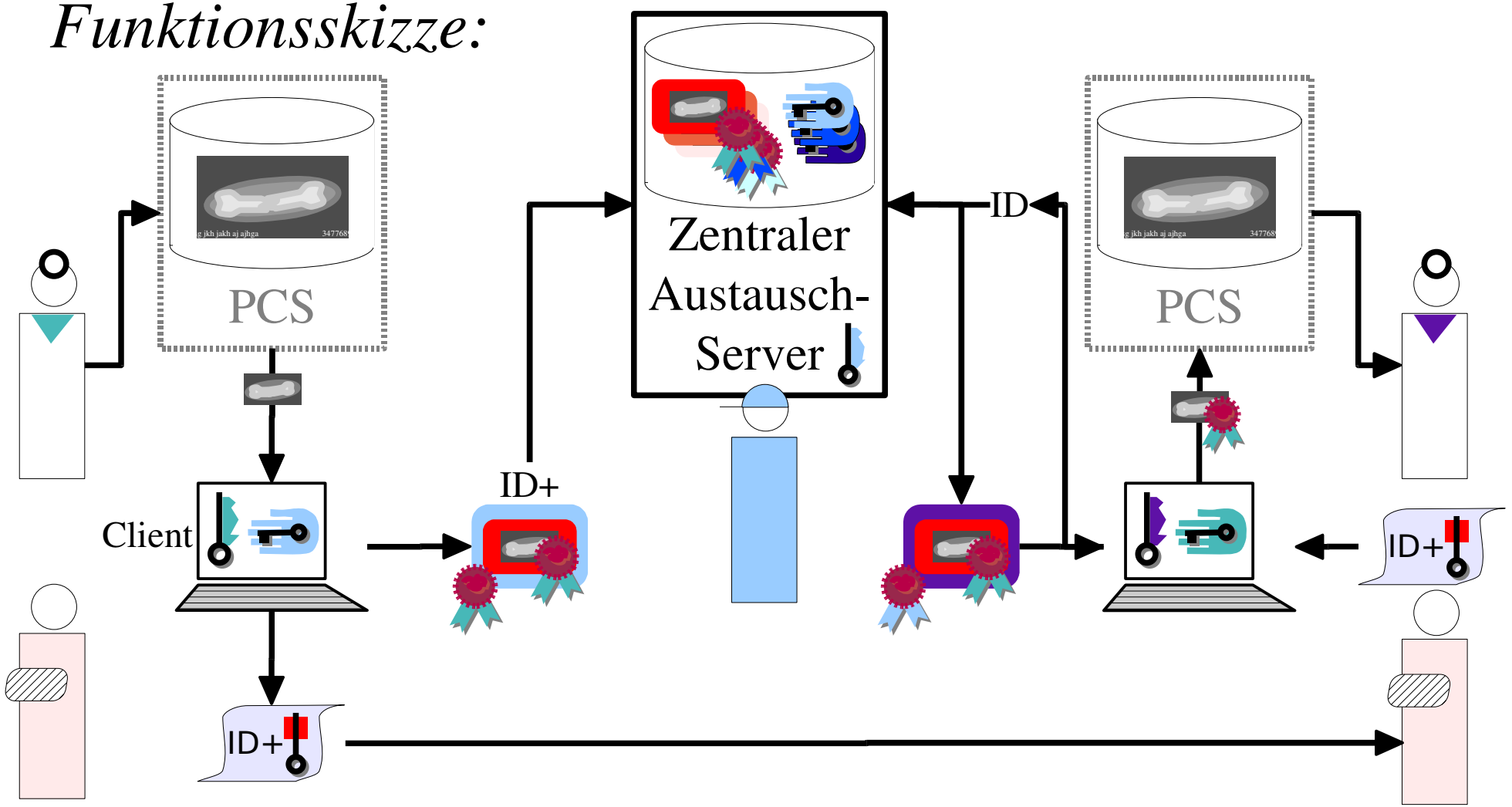
- primär: Entziffern Patientendaten aus Betreiberposition (Widerlegung Systemanspruch)
- sekundär: allgemeine Schwachstellensuche

Grenzen:

- sehr knappes Zeitkontigent (4 Tage!)
- Zuarbeit des Auftraggebers (≠Hersteller!)
- Systemversion Stand etwa Mitte 2003

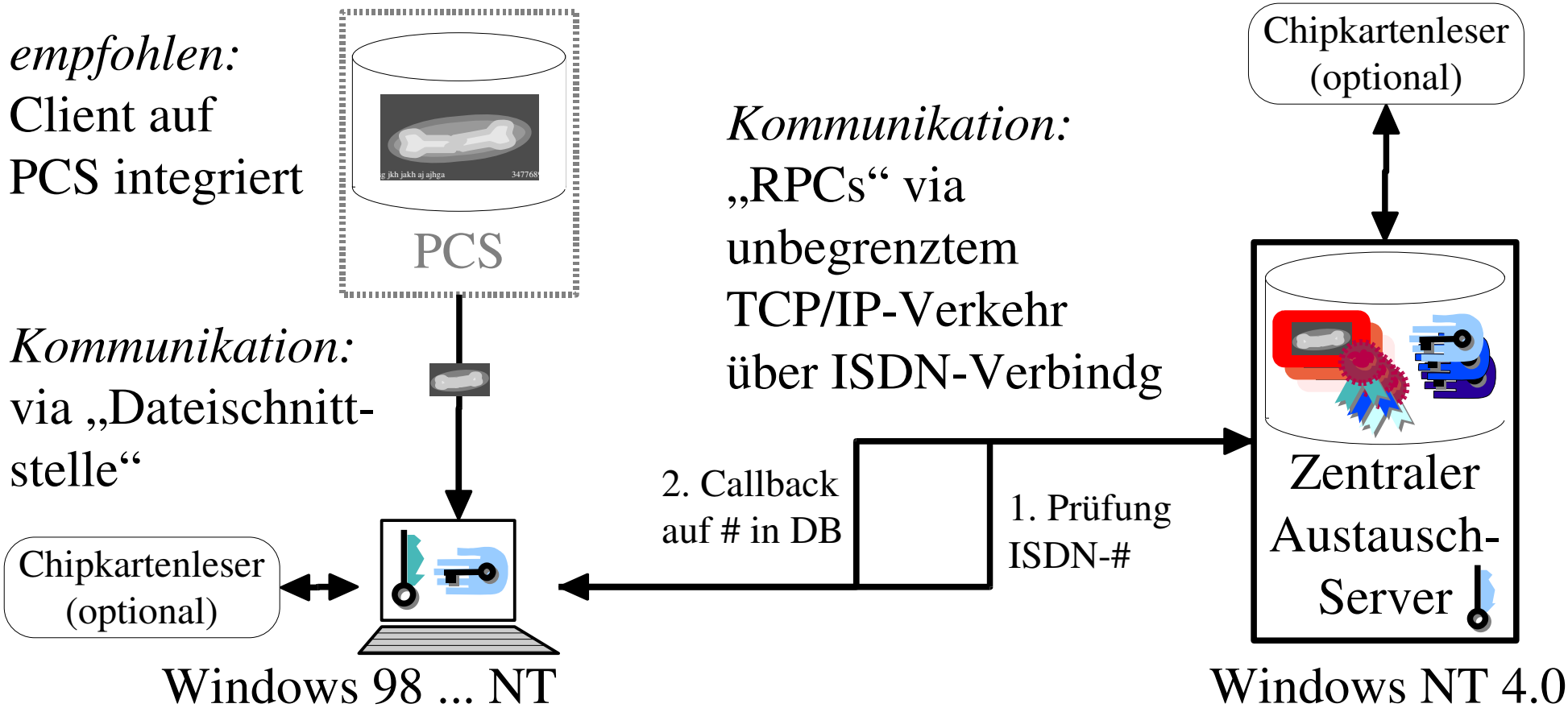
Strukturanalyse
„Hohe Mauern, stolze Zinnen, ...“

Funktionsskizze:



Strukturanalyse ...

Technikskizze:



Strukturanalyse ... Schutzziele + Schutzobjekte

- Systemanspruch:
  - Vertraulichkeit, Integrität, Authentizität und Rechtsverbindlichkeit der Patientenakten
  - Kontrolle des Zugriffs durch den Patienten
  - insbesondere Schutz vor dem Betreiber
- außerdem sinnvollerweise:
  - Vertraulichkeit der Datenbestände im PCS
  - Integrität und Verfügbarkeit von Daten+Funktions-beständen im PCS

Untersuchungsbedürftige Risiken und Nebenwirkungen

Unbefugter Zugriff auf Patientendaten

- massive Verletzung der Intimsphäre und der Persönlichkeitsrechte
- Krankheitsdispostionen über Generationen ableitbar → gefährdet Versicherbarkeit des Patienten und seiner Nachkommen
- Interpretation als Schweigepflichtverletzung

→ *Vertraulichkeit der Patientendaten hochsensibel, hochattraktives Angriffsziel für viele*

Untersuchungsbedürftige Risiken und Nebenwirkungen …

Manipulation von Patientendaten

- Verlust von Krankengeschichte
- bei sachkundiger Manipulation Gefahr für Leib und Leben
- Interpretation als Kunstfehler
- Haftung

→ *Integrität der Patientendaten hochsensibel, hochattraktives Angriffsziel für Schwerkriminelle*

Untersuchungsbedürftige Risiken und Nebenwirkungen …

Fälschung elektronischer Arztunterschriften

- erlaubt Zugriff auf Krankenakten
- erlaubt Manipulation von Krankenakten
- im Kontext erweiterter eHealth-Konzepte: erlaubt z.B. Rezeptfälschungen
- alles rechtsverbindlich dem Arzt zugerechnet!

→ *elektronische Identität des Arztes hochsensibel, hochattraktives Angriffsziel für viele*

Untersuchungsbedürftige Risiken und Nebenwirkungen …

Unbefugter Zugriff auf Praxis-Computersysteme

- kann – je nach PCS-Sicherheit – alle vorigen Risiken auch im PCS auslösen
- Sabotage + Lähmung Praxisbetrieb
- Beweislage? Haftung?

→ *Sicherheit des Praxis-Computersystems hochsensibel, hochattraktives Angriffsziel*

Allgemeine Verdachtsmomente

Wie denken die Konstrukteure?

- Neuerfindung des Rades (NetNews, MIME, ...)
- Geheimniskrämerei (Geheimhaltung RPCs)
- IPC via „Dateischnittstelle“ – lahm + heikel
- ISDN als Kommunikationskanal – Radiologe, Onkologe: Röntgenbilder, Sonogramme, CTs, ...?
- Nutzlast-Bandbreite/Medien-Bandbreite < 10% !

→*unerfahrene Bastler ohne Praxis und Detailliebe?*

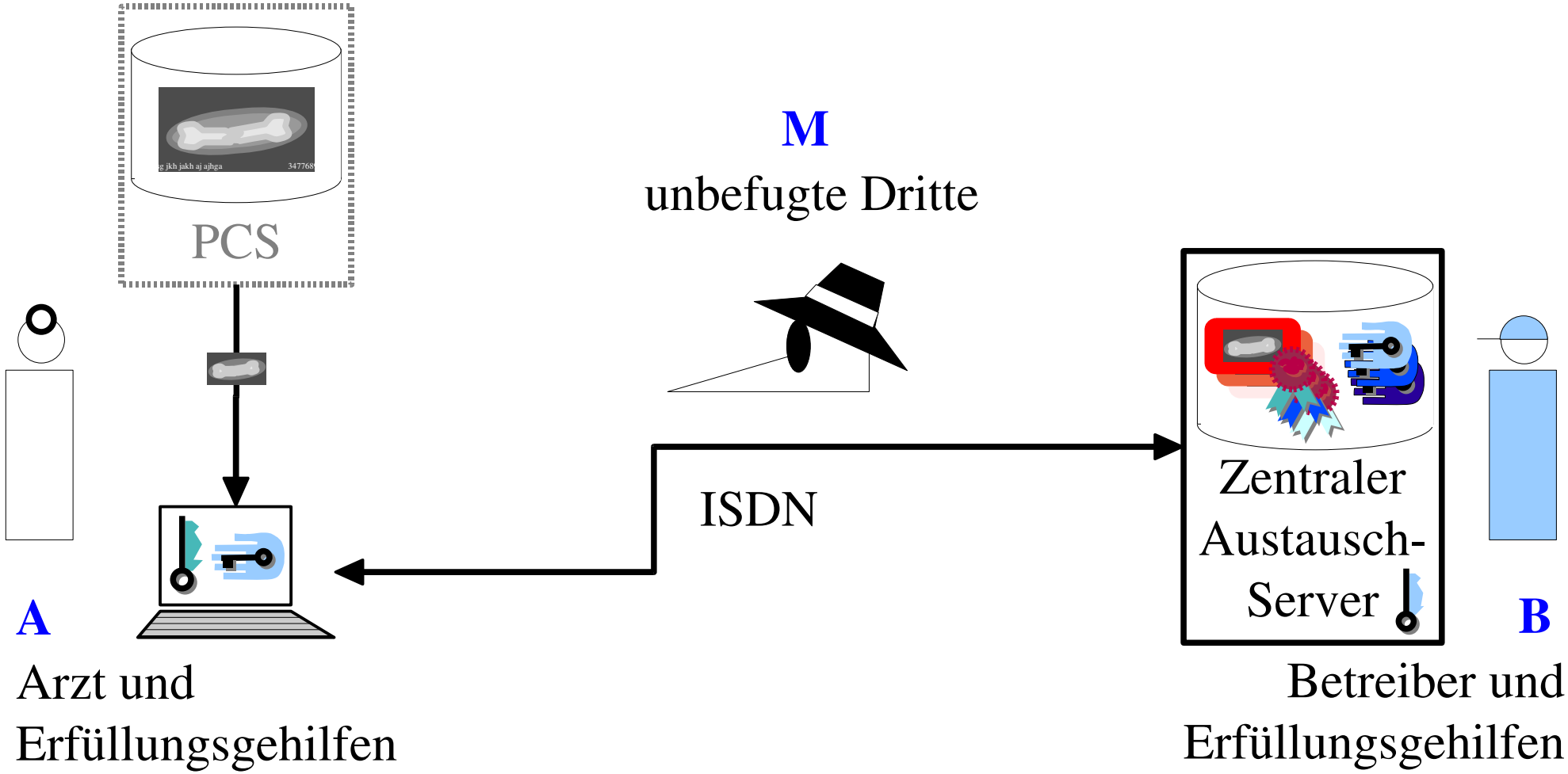
Sicherheitsspezifische Verdachtsmomente

Sicherheitskonzept: „ISDN=kein Internet=sicher“ *?*

- unbeschränktes TCP/IP via ISDN ohne VPN
- keine Firewalls (explizit „unnötig“)
- ISDN-Rufnummern-Prüfung + Call-Back
- Austausch beliebiger Dokumente (und Viren)
- unsichere „Betriebssysteme“ und keine Härtung
- eine riesige „Vertrauensblase“ ...

→*Sicherheit lästiges Detail, Buzz-Word-Weaseling?*

Bedrohungsannahmen
Angriffspositionen



Bedrohungsannahmen ... Angriffspositionen ...

- Position **B** – Betreiber und Erfüllungsgehilfen
  (Systemanspruch: außer DoS keine Angriffe)
  Betreiber des zentralen Servers, Admins, Wartungstechniker (Fernwartung?), Reinigungspersonal
  → Systemvollmacht auf Server (legal oder illegal)
- Position **A** – Arzt und Erfüllungsgehilfen
  Ärzte, Personal, Admins, Wartungstechniker, Kinder, Reinigungspersonal → Systemvollmacht auf Client
- Position **M** – unbefugte Dritte
  direkter Zugang weder zu Clients noch zum Server

Bedrohungsannahmen ... Eskalationsmöglichkeiten

- aus Position **B** – B→A_i
  - Sterntopologie, kommuniziert mit allen Clients direkt : keine Firewalls, unbeschränkte TCP/IP-Kommunikation → kann höchstwahrscheinlich beliebige Clienten kapern
- aus Position **A** – A→B+A_i
  - direkte Kommunikation nur mit Server: keine Firewalls, unbeschränkte TCP/IP-Kommunikation → kann Server höchstwahrscheinlich kapern
  - indirekt Kommunikation mit anderen Ärzten: Versand von Viren/Würmern, Aufbau eines Bot-Nets → kann Clients höchstwahrscheinlich fernsteuern

Bedrohungsannahmen ... Eskalationsmöglichkeiten ...

- aus Position **M** – M→B+A_i
  - Frage der kriminellen Energie, Möglichkeiten: Wartung TK-Anlage, Mitarbeiter TK-Provider, Anzapfen Telefonleitung (z.B. im Keller), Anrufweiter-leitung (z.B. Social Engineering), Einbruch, ...
  - nach Einklinken in ISDN-Verbindung: keine Firewalls, unbeschränkte TCP/IP-Kommunikation → kann Server+Client höchstwahrscheinlich kapern
  - reine Lausch- oder Man-in-the-Middle-Attacke erlaubt zwar Einblicke/griffe in RPC, aber wohl keine direkte Ausspähung der Patientendaten-Nutzlast

Bedrohungsannahmen ... Eskalationsmöglichkeiten ...

→aus jeder Angriffsposition kann jede andere wahrscheinlich relativ leicht erreicht werden:

- Unterscheidung kann aufgegeben werden
- potentieller Täterkreis sehr groß
- anonyme Angriffe möglich
- erhebliche Beweisschwierigkeiten im Ernstfall
- wohlfeile Schutzbehauptungen für Innentäter

Schwachstellenanalyse

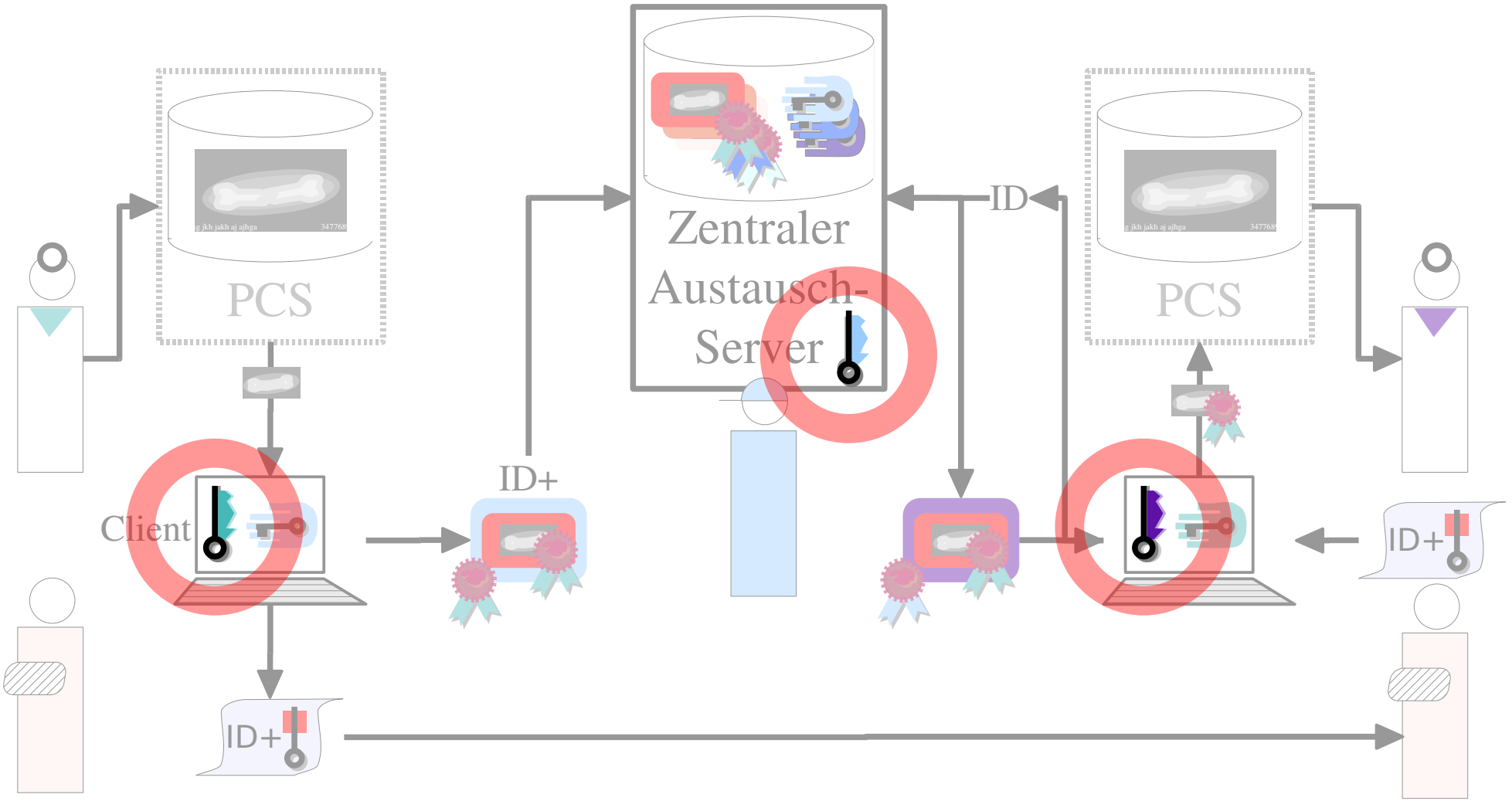
„Die Tür macht hoch, die Tor macht weit“

- kleine Zwischenbilanz:
  - Viren- und Wurmbefall möglich (Vektor Patient ;-)
  - unbeschränkte TCP/IP-Kommunikationsprofile
  - ungehärtete, bekannt schwache Betriebssysteme
  - PCS + Client ein System oder freie Kommunikation
- Wahrscheinliche Konsequenzen:
  - Angreifer agiert in allen Rollen mit Systemvollmacht
  - auf Client: Klartext-Patientenakte und PCS-Zugriff
  - eigentlich sind wir fertig ;-)

Schwachstellenanalyse ... Blick in Executables + Doku

- Netter Beifang – aber Kleinkram:
  - „ninali“ – Paßwort der Datenbank im Klartext, danke! (fest codiert, also überall gleich und unverändert!)
  - Login der Ärzte auf dem Server + Änderung der Paßworte über Klartext-Verbindung
  - verschlüsselte Dateien mit Originalsuffix (z.B. `.doc`)
- Kryptosystem:
  - NetKey 2.10 laut Doku und verschlüsselten Dateien
  - „SSLeay 0.9.0b 29-Jun-1998“ ??? Schwachstellen in Schlüsselaufbereitung
  - ältere, evtl. modifizierte PGP-Version, ungenutzt?

Schwachstellenanalyse ...
Angriff auf die Private-Keys



Untersuchung ...
Angriff auf die Private-Keys …

Chipkartenleser an seriellem Anschluß:

- Überwachung des Ports per SW (remote möglich)
- nur bei Initialisierung (Client+Server) genutzt
  → Verschlüsselung im Betrieb via Softkey!
- rein: verschlüsselter Private-Key aus Datei + PIN
- raus: **entschlüsselter Private-Key – Danke!**

→identitätsstiftende Private-Keys leicht zugänglich

→Authentizität und Rechtsverbindlichkeit futsch!

→elektronische Unterschriften fälschbar

→Patientendaten manipulierbar

Schwachstellenanalyse ... Angriff auf das Kryptosystem ...

Public-Keys:

- wahrscheinlich ungesicherter Keyring
- Betreiber+Ärzte-Public-Keys in einem Ring
- Verteilung + Pflege des Keyrings?

→Server-Betreiber kann Ärzte in allen Fachgruppen „spoofen“ und direkt eigene Clients nutzen (und damit auch Angriffstrategie $A \rightarrow A_i$)

→wahrscheinlich Public-Keys lösch- und einfügbar

Schwachstellenanalyse ...
Angriff auf das Kryptosystem ...

„Lager“verschlüsselung mit Patienten-„Token“:

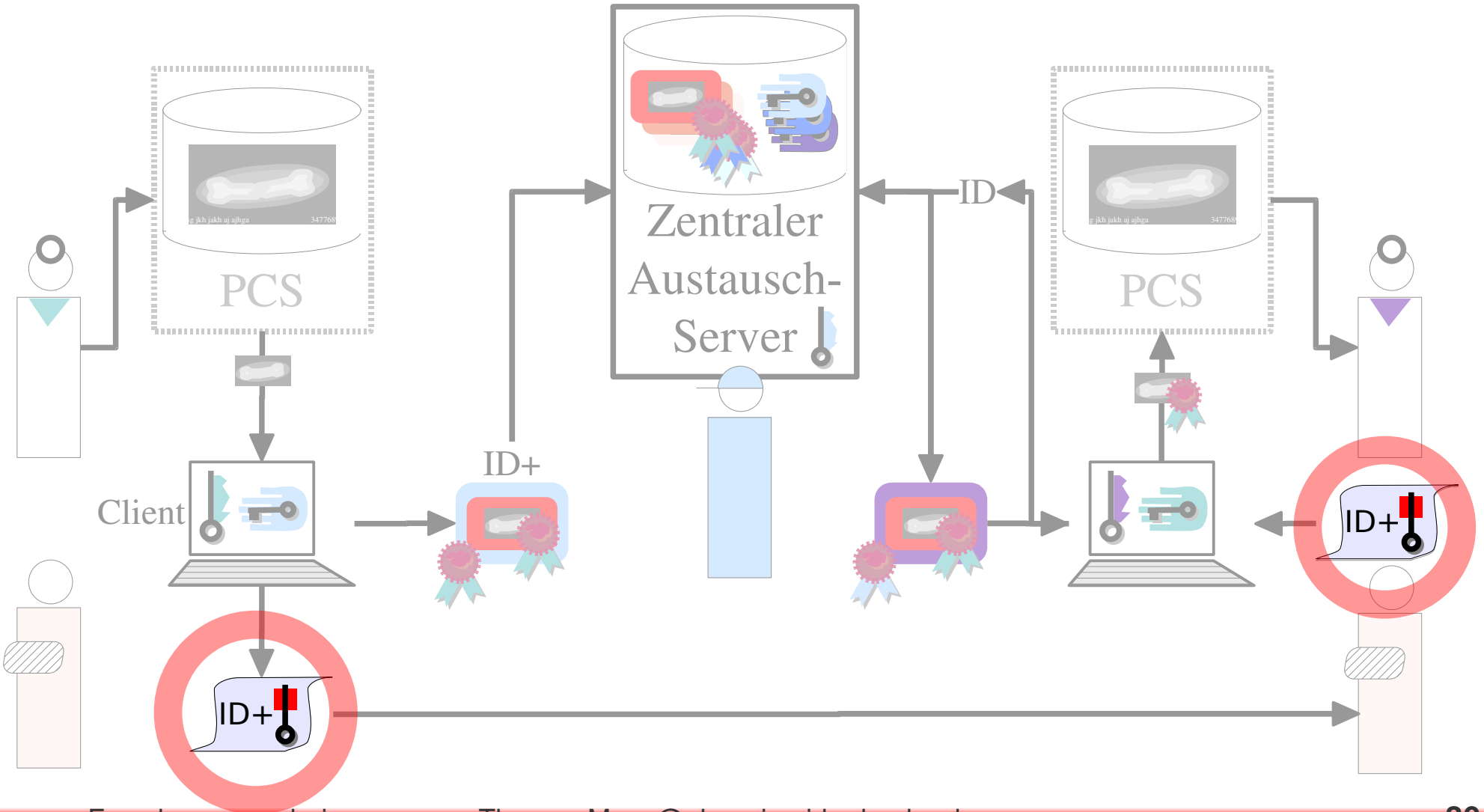
- Testdateien aus 1, 2, ..., 2048, ... „@“
- in Testumgebung zum Server übermittelt
  - „Lager“version auf Client via Temp-Datei erhalten
  - inkompressibel, also Chiffre nicht ganz schlecht

→Stromchiffre: kein Padding, „Netkey 2.10“ ???

→Patientenakte auf Server nur „Lager“verschlüsselt (entgegen Systemdokumentation!), Dateinamen!

→Patienten-„Token“ nur mit Sekundenauflösung!!!

Schwachstellenanalyse ...
Angriff auf das Patienten-Token



Schwachstellenanalyse ... Angriff auf das Patienten-Token ...

Generierung der Patienten-„Token“:

- Erzeugung einiger Millionen Patienten-„Token“
- strukturelle und statistische Analyse
- Beispiel von einem Client:

```
aa1zfugs0jzxcx905yu7h
aa1zfugs0jzxcxa0ecLh3
aa1zfugs0jzxcxb0eco8j
aa1zfugs0jzxcxc05yu7r
aa1zfugs0jzxcxd0ecsz0
aa1zfugs0jzxcxe0ecvqg
aa1zfugs0jzxcxf05yu81
aa1zfugs0jzxcxg0ed0gx
aa1zfugs0jzxcxh0ed40u
aa1zfugs0jzxcxi05yu8b
```

```
aa1zfugs0jzxcxj0ed8ra
aa1zfugs0jzxcxk0edaqb
aa1zfugs0jzxcxL05yu8L
aa1zfugs0jzxcxm0edg98
aa1zfugs0jzxcxn0edj0o
aa1zfugs0jzxcxo05yu8u
aa1zfugs0jzxcxp0edojL
aa1zfugs0jzxcxq0edqiL
aa1zfugs0jzxcxr05yu94
aa1zfugs0jzxcxs0edv92
```

Schwachstellenanalyse ...
Angriff auf das Patienten-Token ...

- 128 Bit Schlüsselbreite empfehlenswert
  ≙ 38,5 Dezimalen
- 21 Stellen Basis 36 ≙ 108,6 Bit
  ≙ 32,7 Dezimalen
- Token = ID + Vorgangsschlüssel

`aa1zfugs0jzxcx90` `5yu7h`

VorgangsID:
ArztID, Datum, Tageszähler

Vorgangssclüssel
(nur 5 Stellen!)

- 5 Stellen Schlüssel ≙ 25,9 Bit ≙ 7,8 Dezimalen
  (etwa 65 Millionen ≙ 18h bei 1000 Versuche/s)

Milchstraße
ø ~100.000 LJ

Suchen darin eine
Bakterie (75 µm)

ø ~57 Lichttage

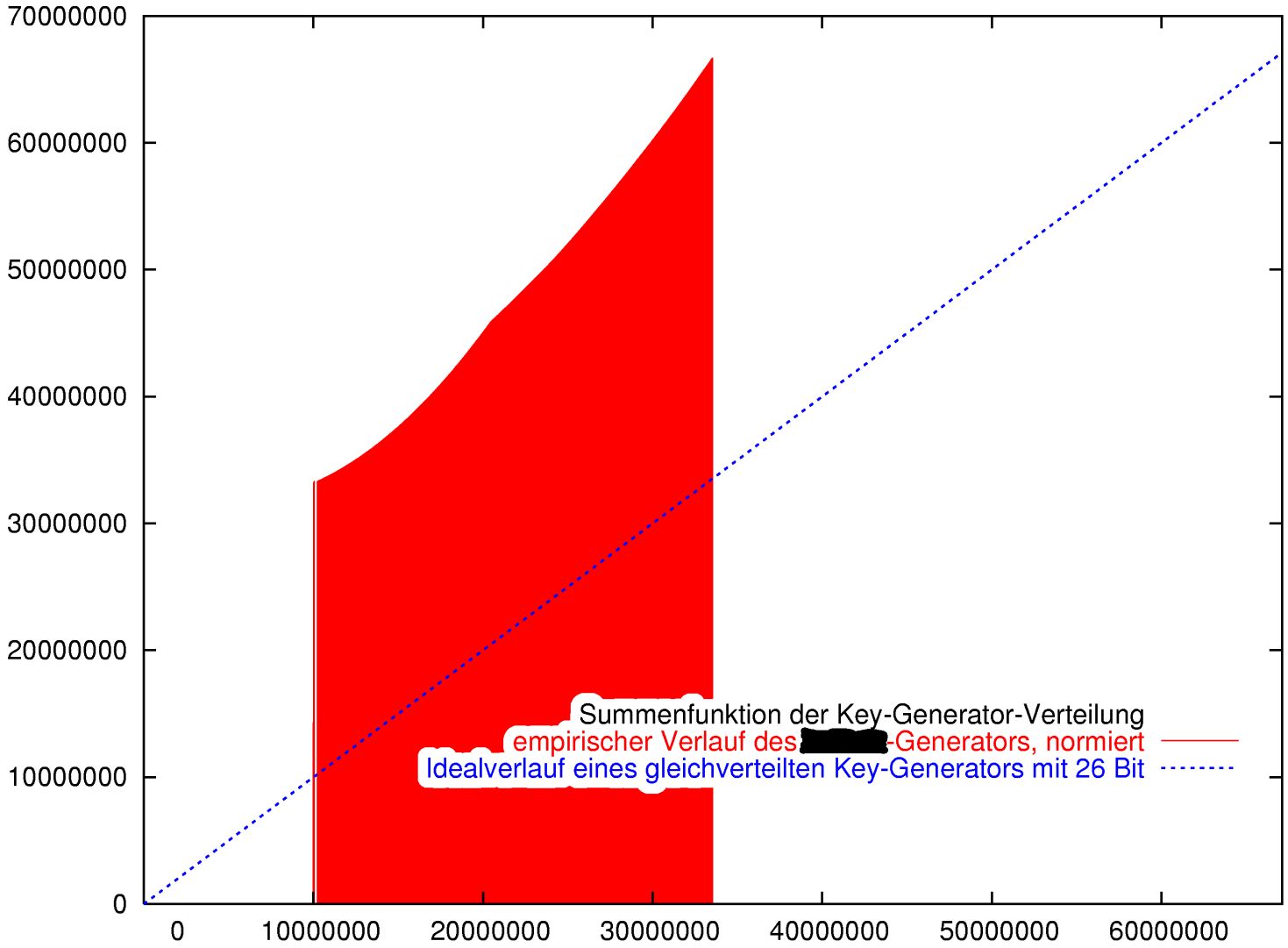
ø knapp 5 km

Schwachstellenanalyse ...
Angriff auf das Patienten-Token ...

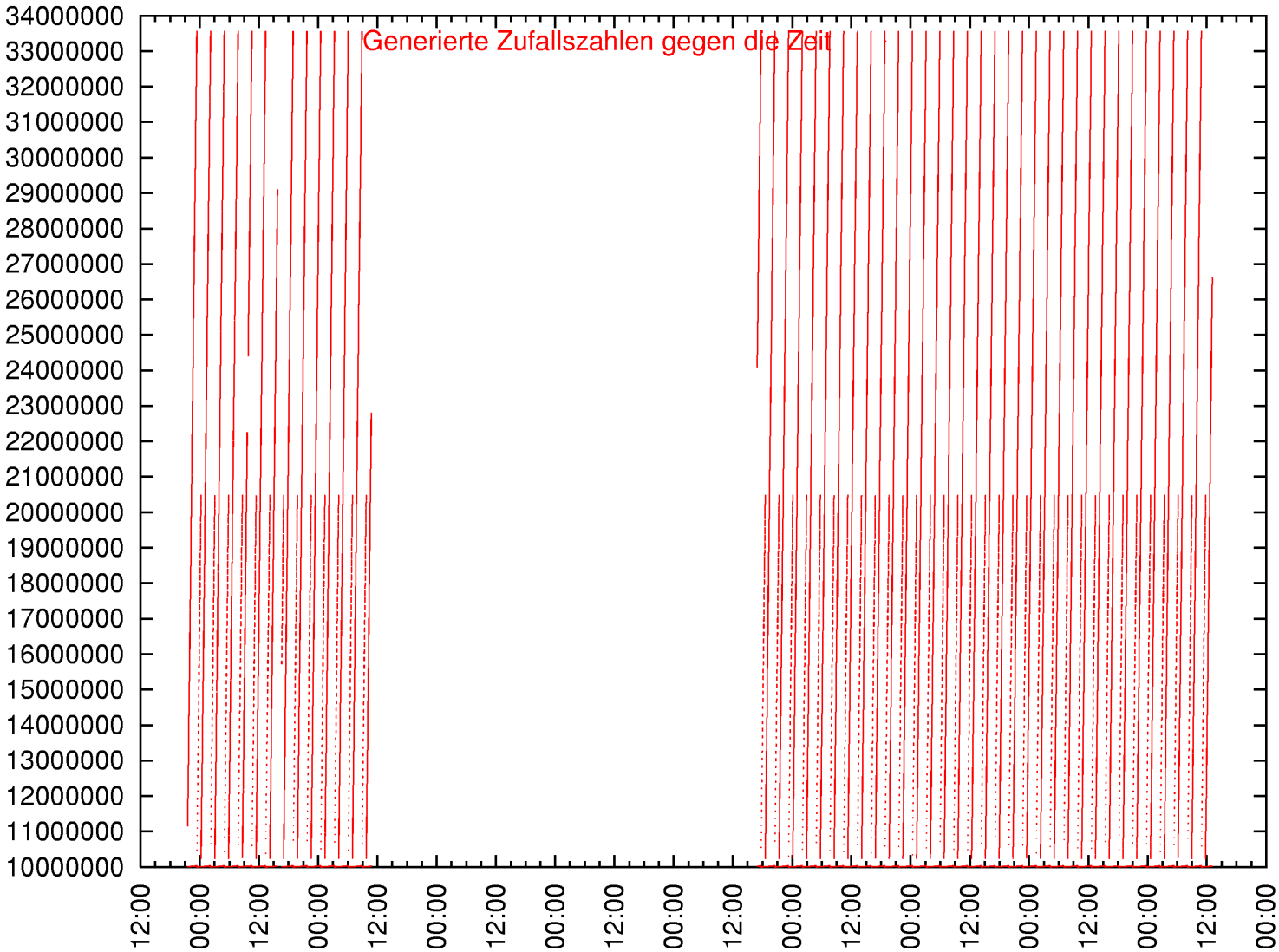
statistische Analyse:

- zur gleichen Systemzeit liefern alle Clients identische Schlüssel
- Oops – der Schlüsselraum ist nur dünn besetzt ...
- Oooops – nicht gleichverteilt ...
- Entropie nur etwa 17,3 Bit ≙ 5,2 Dezimalen
  ø etwa 12 Meter große Petrischale …
  etwa 160.000 Versuche ≙ < 3 min bei 1000 V./s
- Korrelationsanalysen ...

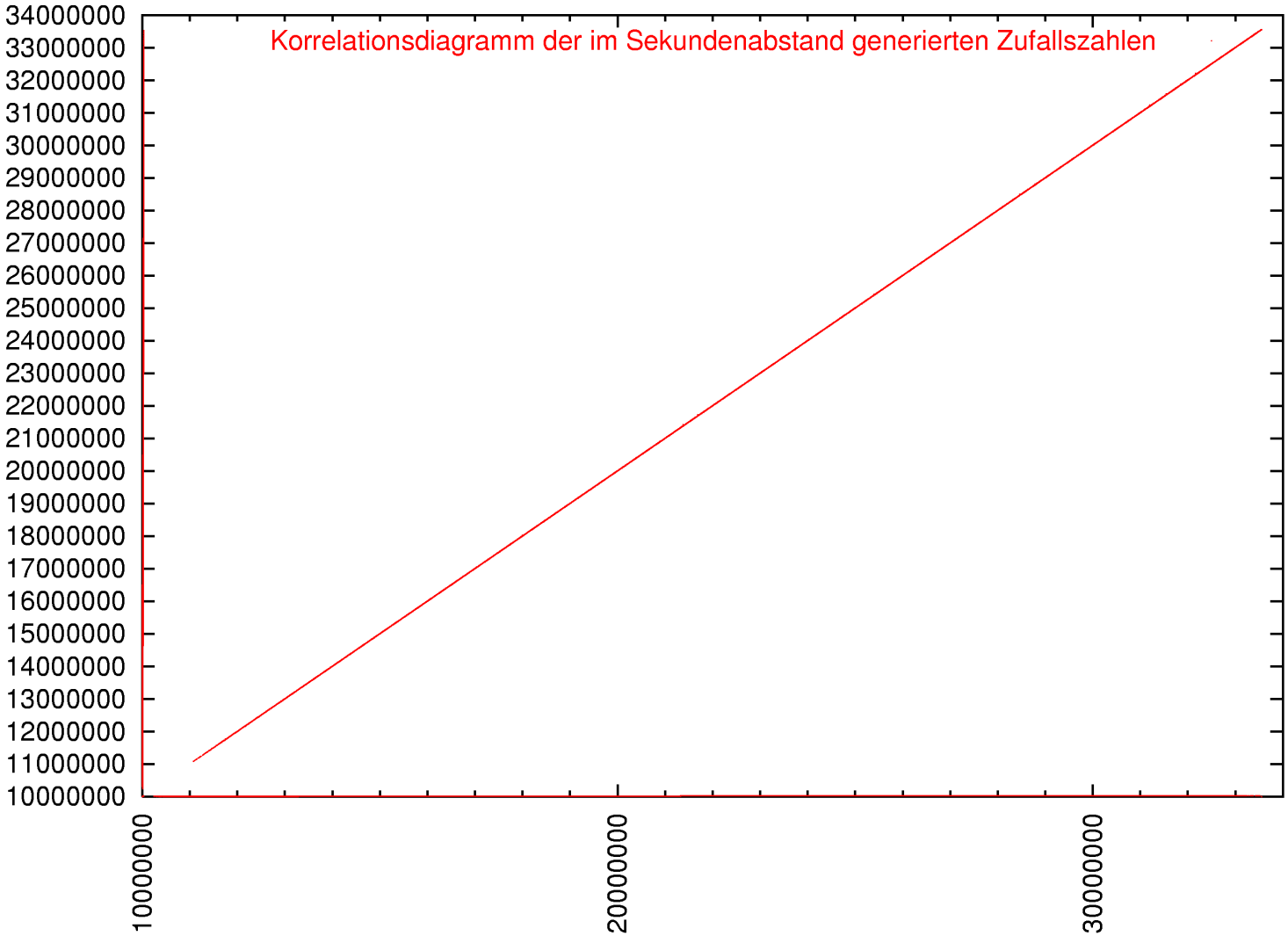
Schwachstellenanalyse ...
Angriff auf das Patienten-Token ...



Schwachstellenanalyse ...
Angriff auf das Patienten-Token ...



Schwachstellenanalyse ...
Angriff auf das Patienten-Token ...



Schwachstellenanalyse ... Angriff auf das Patienten-Token ...

- der Schlüsselgenerator (rekonstruiert):

```
// 1. Zufallsfunktion mit der Client-Systemzeit
// initialisieren, zwei Zufallszahlen erzeugen.
srand(SystemZeit);
mZufall1 = rand();
mZufall2 = rand();
// 2. über die 10-Mio-Grenze springen
if ( mZufall2 >= mZufall1 ) // Verfahren A
   { return mZufall1 + 10000000; }
// 3. Zufallszahl 1 in den Bereich von 33 Mio.
// verschieben und dann die zweite Zufallszahl
// aufaddieren, maskiert 0x3FF.
mZufall1 <<= 10;
mZufall1 |= (mZufall2 & 0x3ff);
if( mZufall1 < 10000000 ) // Verfahren B
   { mZufall1 += 10240000; }
return mZufall1;
```

Schwachstellenanalyse ... Angriff auf Patienten-Token ...

- Schlüssel berechenbar aus Systemzeit des Clients
- Ablage der Patientenakten auf Server:
  - Vorgangsverzeichnis: ArztID + Datum „TTMMJJJJ“
  - Dateien: Client-Zeitstempel „TTMMJJJJhhmmssµµµ“
- älteste Datei ~ Zeitpunkt Schlüsselgenerierung, liegt maximal 1-2 Sekunden früher ...
- liegt Betreiber direkt vor, Client kann abgefragen
- wir müssen nur 1-3 Schlüssel probieren!!!
- manueller Angriff ohne Systemeingriff möglich!

→Patientendaten ohne Patientenzutun einsehbar!

Angriff auf das Patienten-Token ... Ein Einwand

- Laut Hersteller:
  - angeblich 128 Bit für Verschlüsselung Patientenakte
  - „Token“ erzeugt echten Schlüssel
  - Details? Nein: Geheim, laufendes Patentverfahren ...
- durchaus möglich, aber völlig irrelevant, denn
- „Token“ gewährt Zugang – entweder als „Seed“ oder durch Entschlüsselung des eigentlichen Aktenschlüssel
- dramatische kryptographische Ahnungslosigkeit?
- bewußte Irreführung?

Dokumentation + Berichterstattung

- Abstract
- Ziele, Grenzen + Untersuchungsgegenstand
- Strukturanalyse
- Bedrohungsannahmen
- Schwachstellen
- Ausblick
- Begriffe + Definitionen

Gefundene Risiken und Nebenwirkungen

Unbefugter Zugriff auf Patientendaten

- auf Gesamtheit der Patientendaten für jeden mit Kontrolle über den zentralen Server trivial möglich – insbesondere Server-Betreiber
- für jeden mit befugtem oder unbefugtem Zugang zu Arzt-Client ohne Patientenhilfe mindestens innerhalb der Fachgruppe trivial möglich

→ *Vertraulichkeit der Patientendaten war (und ist) m. E. extrem gefährdet!*

Gefundene Risiken und Nebenwirkungen …

Manipulation von Patientendaten

- Voraussetzung: Möglichkeit zur Fälschung elektronischer Arztunterschriften – mit krimineller Energie wohl leicht erreichbar …
- im Modellversuch mindestens unnötige, stark belastende Eingriffe als Schadensszenario

→ *Integrität der Patientendaten war sehr wahrscheinlich gefährdet, weitere Nutzung daher mindestens fragwürdig*

Gefundene Risiken und Nebenwirkungen …

Fälschung elektronischer Arztunterschriften

- Voraussetzung: Administrationsrechte auf System, Zugang physisch oder über Datennetze
- keine Vorkehrungen gegen klassische Angriffs-strategien für unbefugte Remote-Kontrolle
- falscher Chipkarteneinsatz exponiert PrivateKeys
- Zugriff je nach Angriffsposition und krimineller Energie leicht erreichbar

→ *Identitätsstiftende Wirkung war nicht gegeben*

→ *Keine Nachvollziehbarkeit und Rechtssicherheit*

Gefundene Risiken und Nebenwirkungen …

Unbefugter Zugriff auf Praxis-Computersysteme

- Voraussetzung: Administrationsrechte auf System, Zugang physisch oder über Datennetze
- keine Vorkehrungen gegen klassische Angriffs-strategien für unbefugte Remote-Kontrolle
- Zugriff je nach Angriffsposition und krimineller Energie leicht erreichbar

→ *Beteiligte PCS können bleibend kompromittiert, Patientendaten außerhalb des Modellversuchs ausgespäht oder modifiziert worden sein*

Fazit

- Zeitkontingent äußerst knapp + Zulieferungen
  → Fehler möglich, Unvollständigkeit sicher
  → viele Fragen ungeklärt
- Ergebnis vom System-Hersteller bestritten (aber nicht widerlegt …)
- Beschwichtigungsversuche: „altes System“, „nicht mehr im Einsatz“, „nur Modellversuch“, „so kompetente Leute wie Hr. Maus gibt es nur ganz selten“, ...
- vor diesem Hintergrund meine Einschätzung:

Fazit …

Meine Einschätzung:

- Einsatz im Modellversuch ohne ausführliche vorherige Sicherheitsprüfung sehr leichtfertig
- vom Einsatz hätte ich *dringend* abgeraten!
- System mangelhaft unter Sicherheitsaspekten
  → Sicherheitskompetenz des Herstellers???
- dramatische Risiken für Modellprojektteilnehmer, Ärzte+Patienten, Schadensbegrenzung aufwändig
  → Sicherheitswahrnehmung des Herstellers???
- Vertrauensvorschuß endgültig verspielt …

Einige *emotionale* Anmerkungen

- viel zitiert, viel reklamiert:
  Gesellschaftliche Verantwortung von Wissenschaft und Technik
  nun denn – es ist natürlich nicht recht und wird mit juristischen Drohungen belohnt:
- das untersuchte System – ein Einzelfall?
- etliche Milliarden € Staatsbudget verloren in IT-Ruinen – pardon, „Zukunftsprojekten“ – wie „InPol Neu“, Tollhaus LKW-Maut, Herkules, Virtueller Arbeitsmarkt, ...

Einige *emotionale* Anmerkungen ...

- etwa 1 Million Kinder unter der Armutsgrenze *in Deutschland* (und es werden mehr werden!)
  - → verschlechterte Bildungschancen
  - → vergeudete Talente
- Deutschland ist so „arm“, dass *Kindersparbücher geplündert* werden müssen
  - → weiter verschlechterte Bildungschancen
  - → Lernziele für die nächste Generation: Gemeinsinn? Leistung? Sparen? Planen?
- Kinder die Zukunft unserer Gesellschaft???

Fragen und Diskussion

Vielen Dank für Ihre Aufmerksamkeit!

für Rückfragen

Thomas.Maus@alumni.uni-karlsruhe.de