



Vorlesung
***Methodische Grundlagen des
Software-Engineering***
im Sommersemester 2014

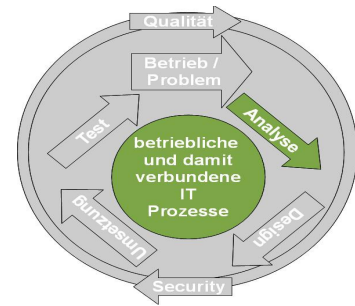
Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Teil 3.5: Kryptographische Protokolle

v. 08.07.2014

- Geschäftsprozessmodellierung
- Process-Mining
- **Modellbasierte Entwicklung sicherer Software**
 - Einführung: Software Security
 - Hintergrund IT-Sicherheit
 - Wiederholung: Modellbasierte Software Entwicklung
 - Modellbasierte Sicherheit mit UML
 - Sichere Architekturen
 - **Kryptographische Protokolle**
 - Protokollanalyse
 - Biometrische Authentisierung
 - Biometrische Authentisierung: Analyse
 - Elektronische Geldbörsen
 - Clouds
 - Elektronische Signatur
 - Bankarchitektur



Literatur:

[Jür05] Jan Jürjens: **Secure systems development with UML**, Springer-Verlag 2005.

Unibibliothek (e-Book):

<http://www.ub.tu-dortmund.de/katalog/titel/1361890>

Papier-Version:

<http://www.ub.tu-dortmund.de/katalog/titel/1091324>

Kap. 5



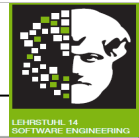
- **Letzter Abschnitt:** sichere Architekturen
 - Guarded Objects
 - no down-flow, data security
- **Dieser Abschnitt:** Kryptographische Protokolle
 - Probleme von Sicherheitsprotokollen
 - ISO OSI Schichten-Modell
 - Sicherheitsanalyse
 - Kryptographische Ausdrücke



- System über **nicht vertrauenswürdiges** Netzwerk verteilt.
- Angreifer kann Nachrichten abfangen, modifizieren, löschen und einfügen.
- **Kryptographie** ermöglicht Sicherheit.
- **Kryptographisches Protokoll:**
 - Austausch von **Nachrichten**
 - für verteilte Sitzungsschlüssel, authentisierenden Auftragsgebern...
 - durch Benutzung von **kryptographischen** Algorithmen.
- Korrekter Entwurf sehr schwierig.

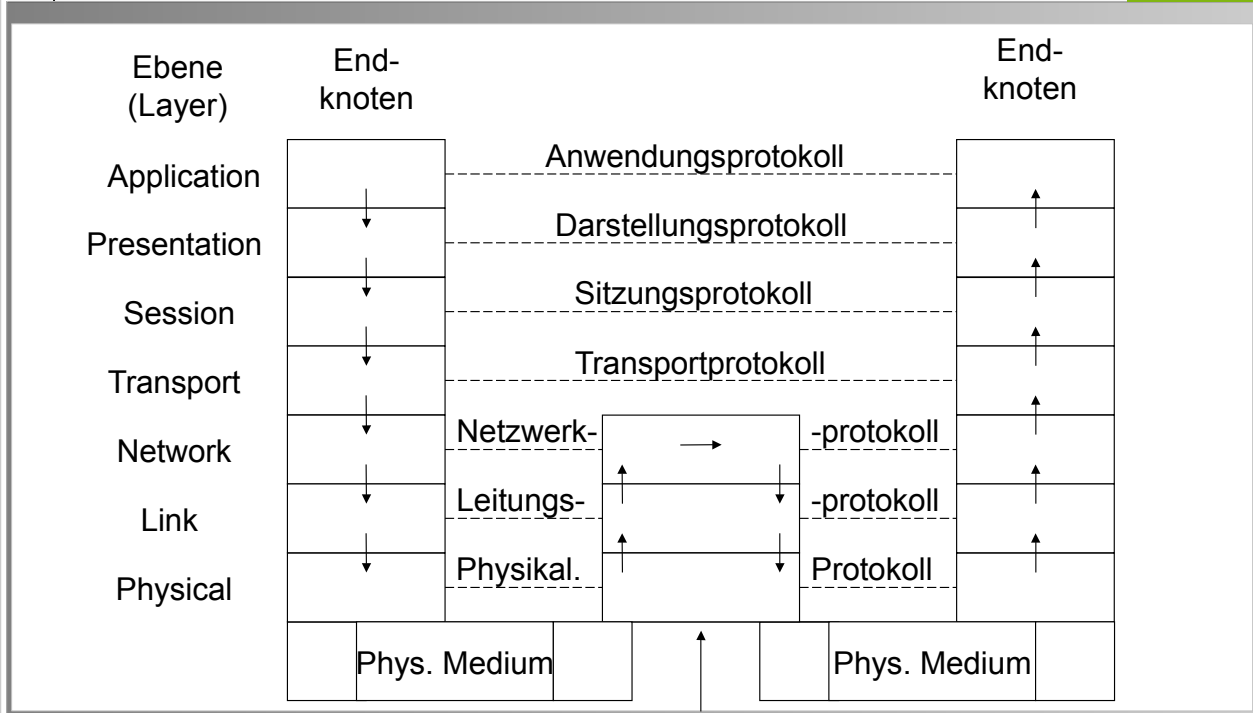


- Ziel: Sichere **Authentisierung** von Kommunikationspartnern.
- Bedrohungen:
 - **Fälschung** von Identitäten.
 - **Unautorisierte Verwendung** von Identitäten.
- Weitere Ziele von Sicherheitsprotokollen:
 - **Schlüsselmanagement**,
 - Elektronische **Transaktionen**, ...



Schwachstellen vieler Protokolle aus verschiedenen Gründen:

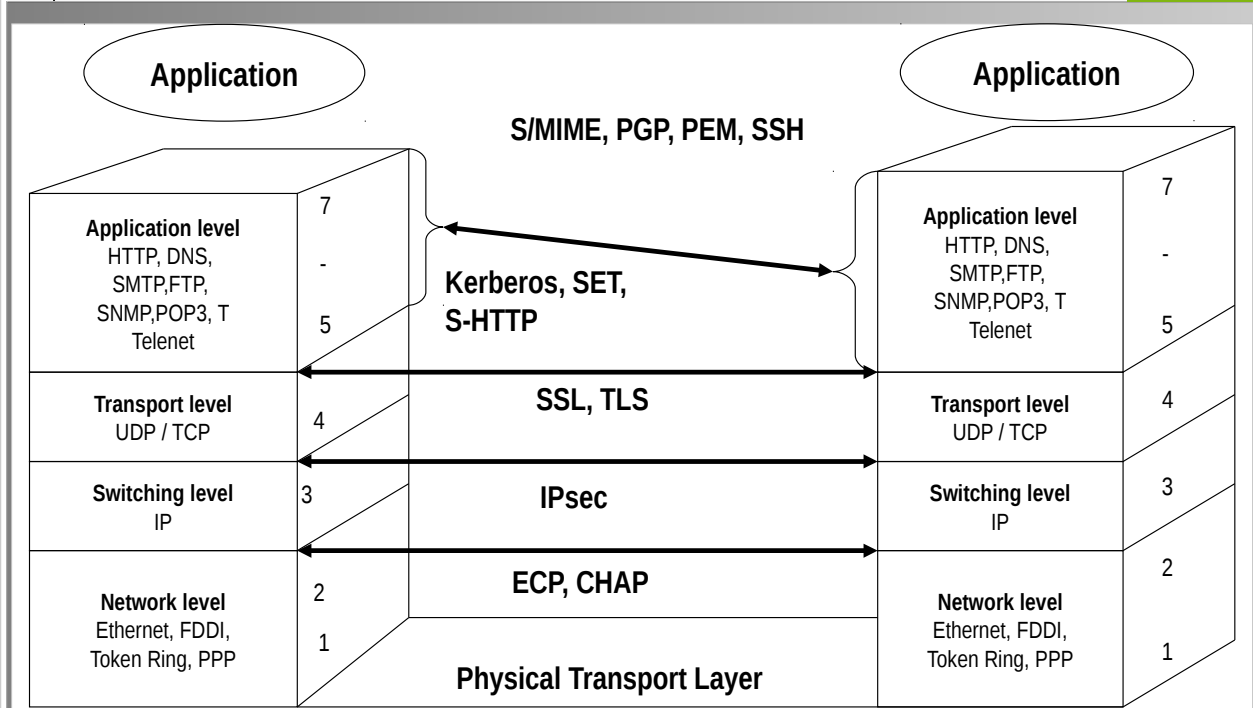
- Schwache Kryptographie.
- **Zentraler Nachrichten-Austausch.**
- **Schnittstellen, Prologe, Epiloge.**
- Verwendung.
- Implementierungsfehler.



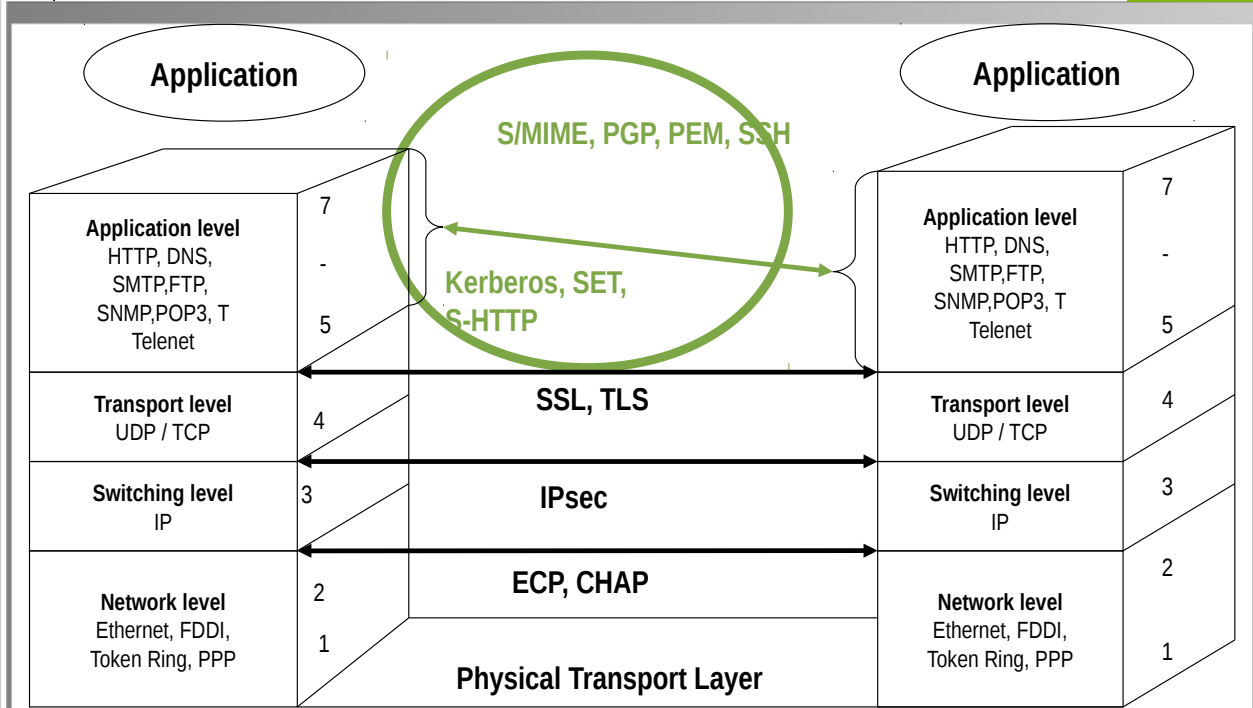
Zwischenknoten

7

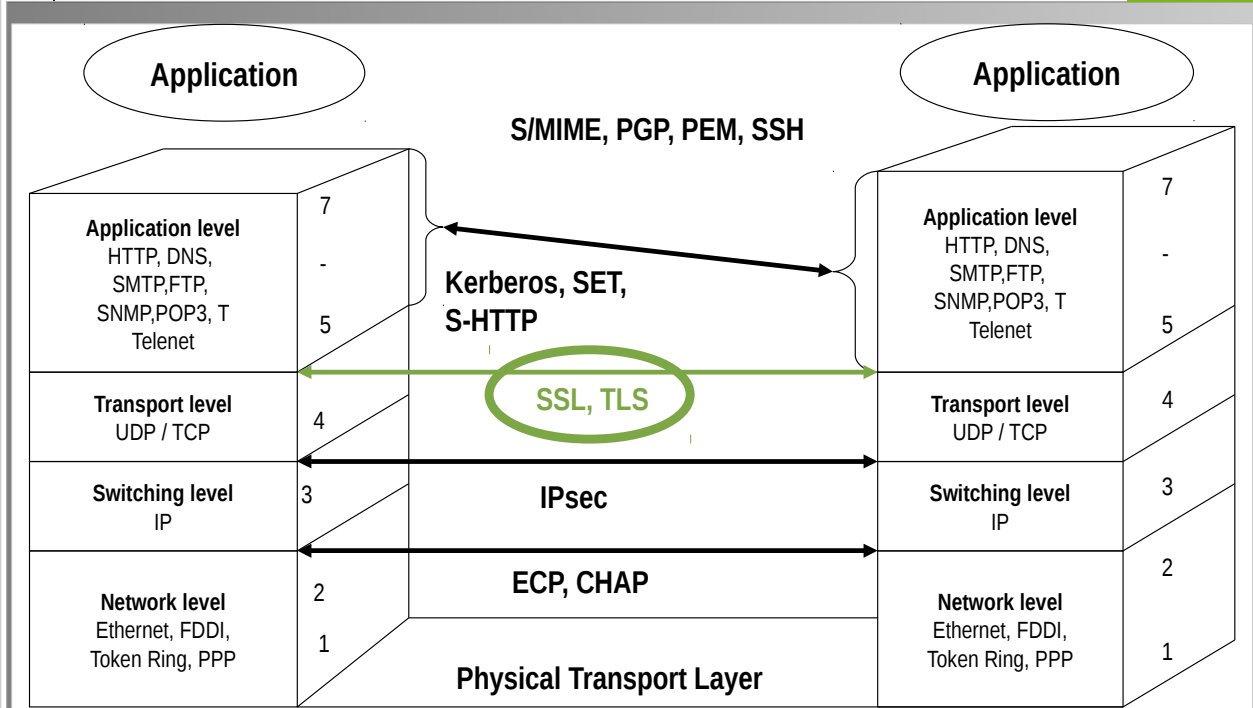
Verschlüsselung und Protokollebenen



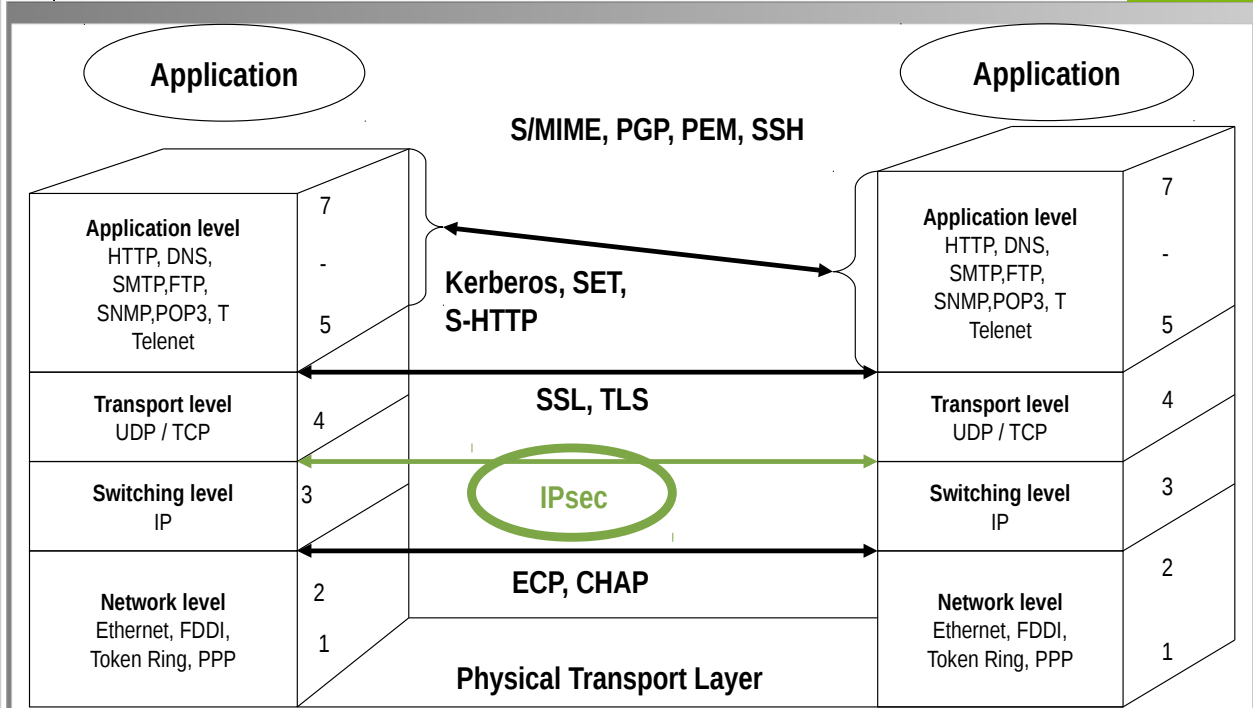
Verschlüsselung und Protokollebenen



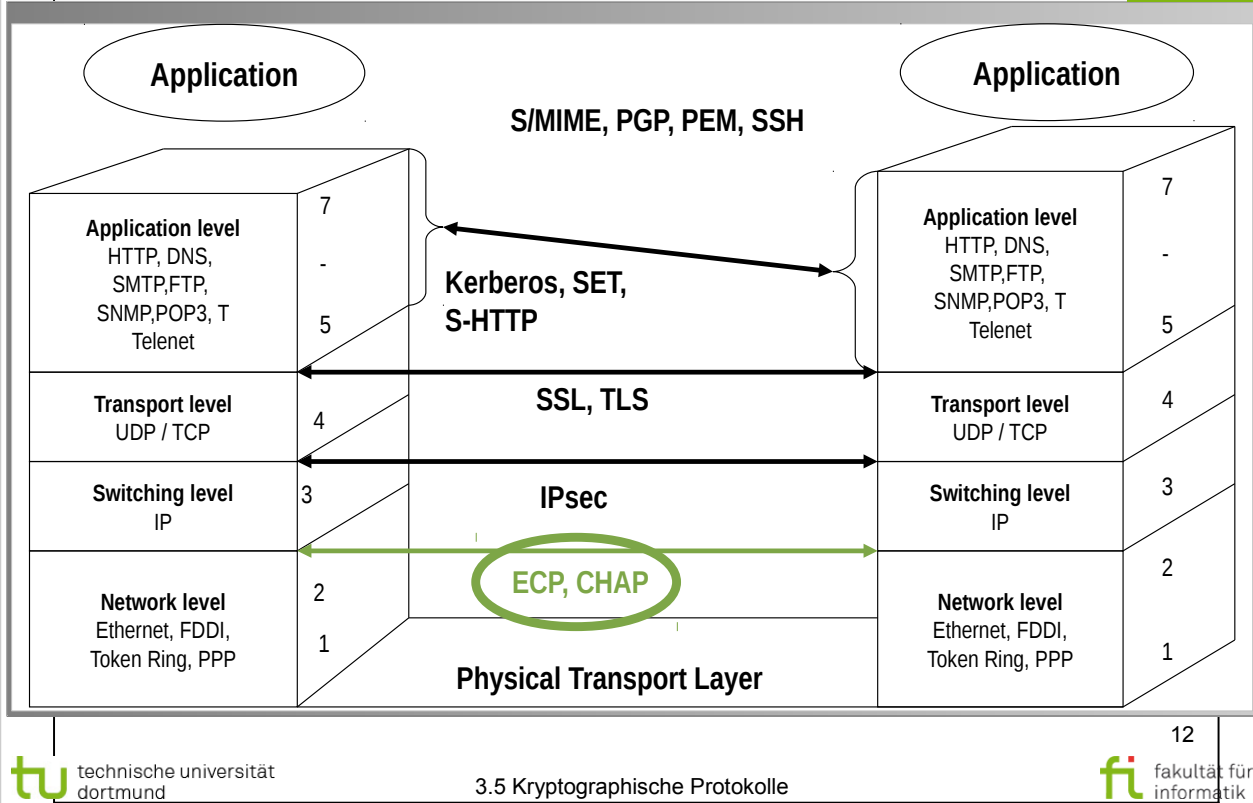
Verschlüsselung und Protokollebenen

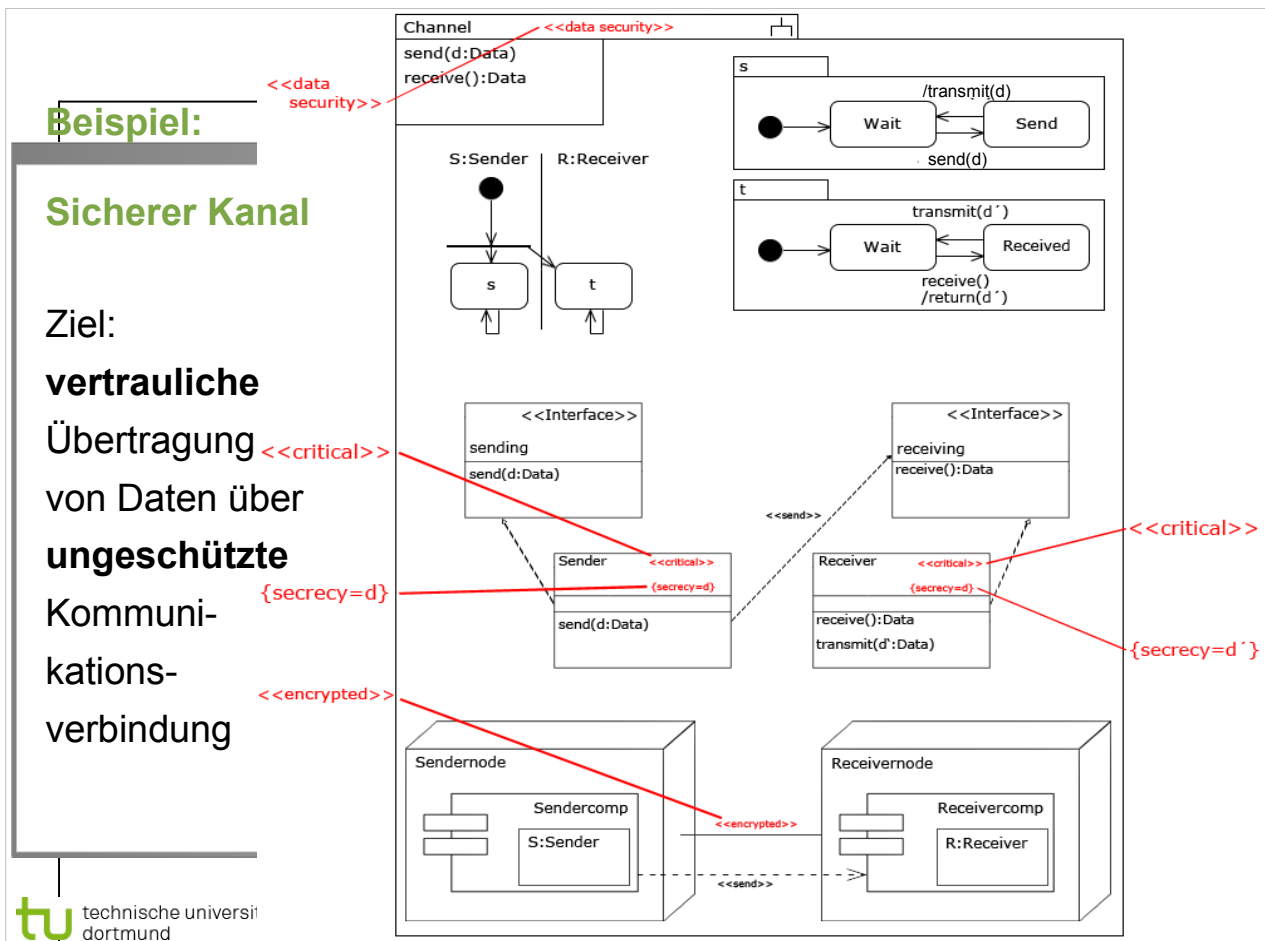


Verschlüsselung und Protokollebenen



Verschlüsselung und Protokollebenen

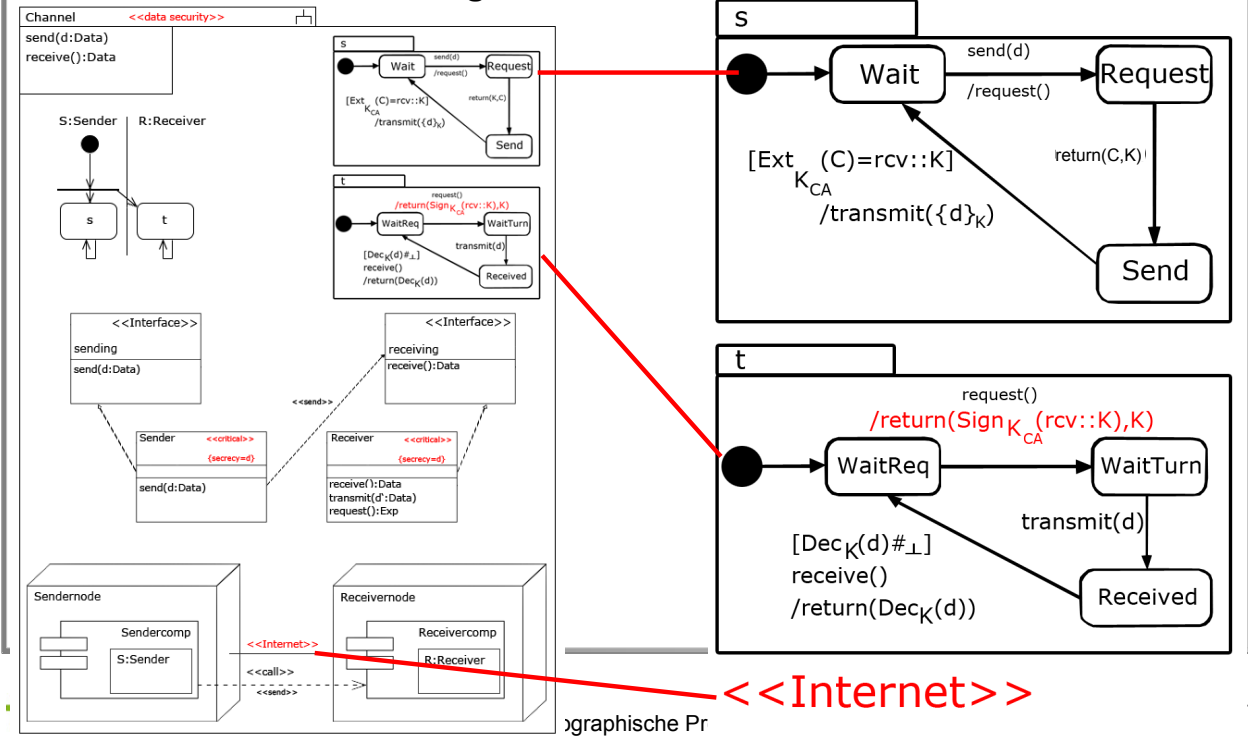




Literatur:

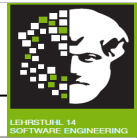
- Jan Jürjens: Secure systems development with UML
- Kap. 5.1: S. 76 Abb. 5.1

Verschlüsseln unter Sitzungsschlüssel nach Austausch eines Zertifikates.



Literatur:

- Jan Jürjens: Secure systems development with UML
- Kap. 5.1: S. 78 Abb. 5.2

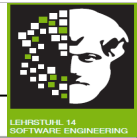


Nach Dolev, Yao (1982):

- Sicherheitsanalyse: **Verifiziere Systemmodell** gegen Angreifermodell.
- Auf Basis Bedrohungsszenarien in Verteilungsdiagrammen.
- Eigenschaften von Systemmodell:
 - Teilnahme an Protokollläufen.
 - Daten im Voraus **kennen**.
 - Nachrichten von Kommunikationsverbindungen **abfangen**.
 - Nachrichten in Kommunikationsverbindungen einfügen.
 - Zugriff auf System-Knoten.



- Verschiedene **Angreifer-Klassen greifen** unterschiedliche Stellen des Systems **an**.
 - Entsprechend der Gefährdungsszenarien.
- Beispiel: **Insider**-Angreifer kontrolliert Kommunikationsverbindungen im LAN.
- Für Sicherheitsanalyse der Spezifikation: Simulation zusammen mit gegebenem Angreifermodell.



Im Kontext der Sicherheitsanalyse:

- Schlüssel = **Symbole**.
- Kryptoalgorithmen = **abstrakte** Operationen:
 - Nur mit **richtigen** Schlüsseln entschlüsselbar.
 - Keine **statistischen** Angriffe ausführbar.



- **Keys:** Folge mit partieller injektiver Abbildung:
 $()^{-1} : Keys \rightarrow Keys$
- Schlüssel: **unabhängig** (Keine Gleichungen wie $K = K' + 1$ für zwei verschiedene Schlüssel $K, K' \in Keys$).
- **Öffentlicher** Schlüssel für **Verschlüsselung** und **Überprüfung der Signatur** benutzbar.
- Schlüssel, die für **sicher** gehalten werden, für **Entschlüsselung** und **Unterzeichnung** benutzbar.
- Schlüssel: entweder Verschlüsselungs- oder Entschlüsselungsschlüssel (**asymmetric**), oder beides falls $k \ k^{-1} = k0$ zufriedenstellt (**symmetric**).
- Zahlen von symmetrischen & asymmetrischen Schlüssel: **unendlich**.



- *Var*: eine unendliche Folge von Variablen.
- *Data*: eine unendliche Folge von Datenwert.
- *Keys*, *Var* und *Data*: wechselseitig disjunkt.
- *Data* beinhaltet die Namen *UMNames* \cup *MsgNm*.
- *Data* kann auch nonces und andere secrets beinhalten.



Wdh.: **Termalgebra** durch Folge von Elementen & Operationen erzeugt.
→ Folge von Termen, gebildet durch Anwendung der Operationen auf Elementen.

Quotient der Termalgebra unter gegebenem Satz von Gleichungen abgeleitet durch:

- **Einführung** dieser **Gleichungen** und
- den von ihnen unter den Bedingungen abgeleiteten.

Algebra **kryptographischer Ausdrücke** *Exp*: Quotient der Termalgebra erzeugt durch die Folge:

Var \cup *Keys* \cup *Data*

**Exp:** Menge der **Krypto-Terme**

- Bildung aus Symbolen in Mengen *Data*, *Keys*, *Var*
- Unter Verwendung der Operationen:
 - $_::_$ (Konkatenation), *head*($_$), *tail*($_$),
 - $(_)^{-1}$ (K^{-1} : zum Verschlüsselungsschlüssel K gehöriger Entschlüsselungsschlüssel).
 - $\{_\}_K$ ($\{M\}_K$: Verschlüsselung der Nachricht M mit Schlüssel K).
 - *Dec*($_$) ($Dec_K(C)$: Entschlüsselung der Daten C mit Schlüssel K).
 - *Sign*($_$) ($Sign_K(M)$: Signatur der Nachricht M mit Schlüssel K).
 - *Ext*($_$) ($Ext_K(S)$: Extrahieren der Signatur S mit Schlüssel K).

Literatur:

Jan Jürjens: Secure systems development with UML

- Kap. 3.3: S. 37



- Unter Berücksichtigung folgender Gleichungen:
 - $\forall E, K. Dec_K^{-1}(\{E\}_K) = E$
 - $\forall E, K. Ext_K(Sign_K^{-1}(E)) = E$
 - $\forall E_1, E_2. head(E_1 :: E_2) = E_1$
 - $\forall E_1, E_2. tail(E_1 :: E_2) = E_2$
 - Assoziativität für $::$.
 - Bessere Lesbarkeit: schreibe $E_1 :: E_2 :: E_3$ für $E_1 :: (E_2 :: E_3)$ und $fst(E_1 :: E_2)$ für $head(E_1 :: E_2)$ etc.
- [NB: Bei Bedarf o.g. Gleichungen um weitere krypto-spezifische Eigenschaften erweiterbar (z.B. bei XOR).]

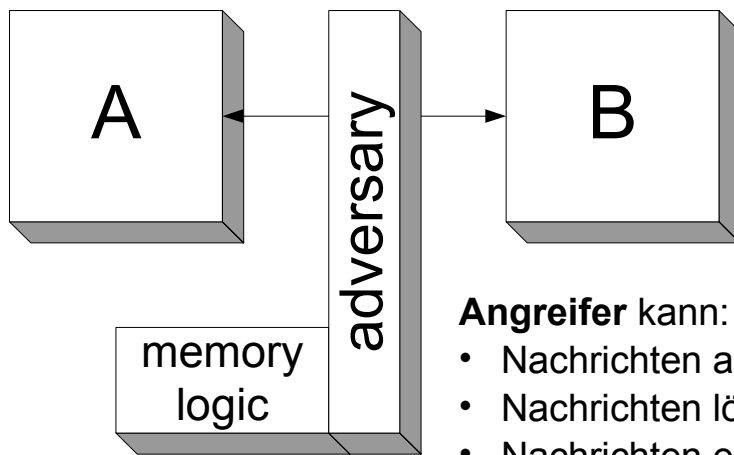
Literatur:

Jan Jürjens: Secure systems development with UML

- Kap. 3.3: S. 37

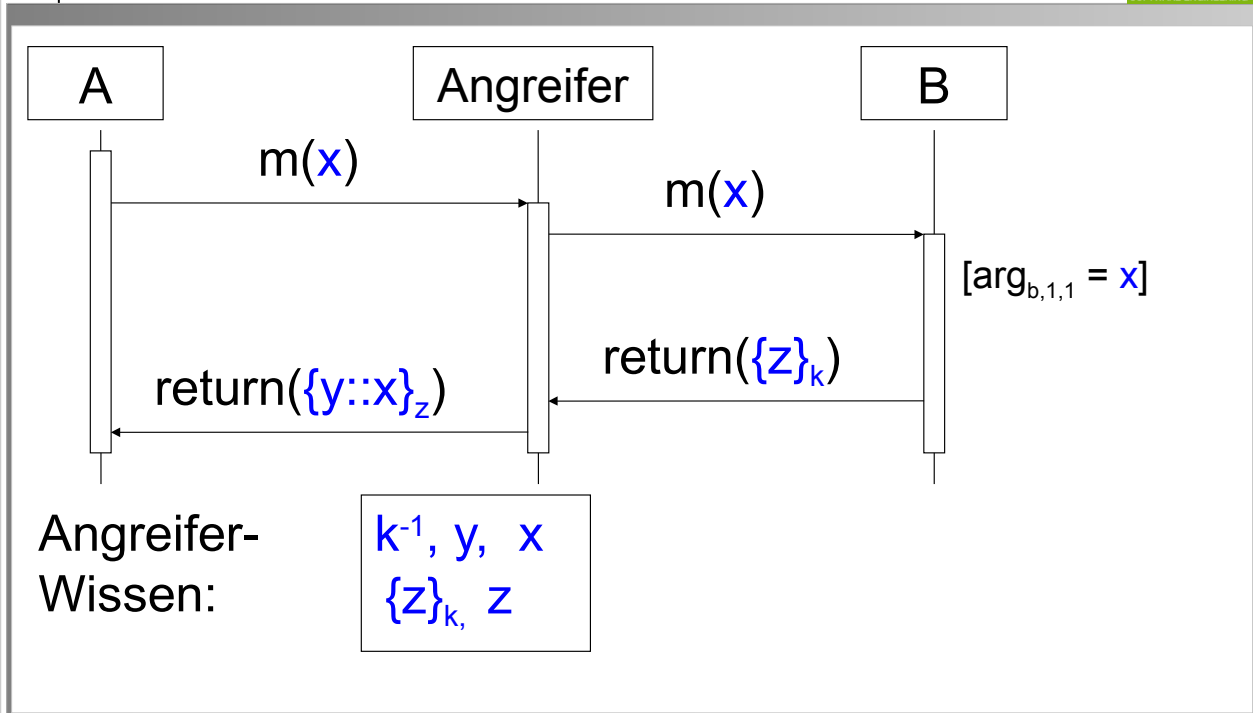


- Für jede $E \in Exp$, folgende Abkürzungen benutzen:
 - $fst(E) =^{def} head(E)$
 - $snd(E) =^{def} head(tail(E))$
 - $thd(E) =^{def} head(tail(tail(E)))$
- Weitere **kryptospezifische** Grundelemente und Gesetze (**XOR**, ...) einbeziehen.
- Abstraktes Model von kryptographischen Algorithmen: **abstrahiert Details auf Ebene der Bitfolge weg**. → Mechanische Analyse möglich.
- Anhand Formalisierung kryptographischer Operationen (**freshness, secrecy, integrity, authenticity**)
 - wichtige Voraussetzungen für sicherheitskritische Daten auf Ebene der UML Diagrammen in mathematischer präziser Art formulierbar.



Angreifer kann:

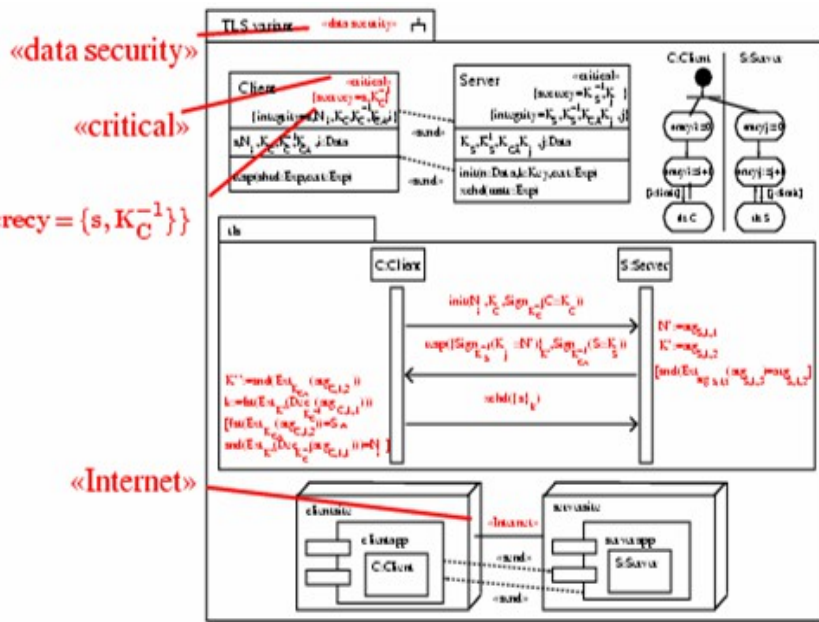
- Nachrichten abspeichern.
- Nachrichten löschen.
- Nachrichten einfügen.
- Nachrichten erstellen.
- **Kryptographische Funktionen** benutzen.
- Bestimmte Systemknoten kontrollieren.
- Bestimmte Daten vorab kennen.



IEEE Infocom 1999.

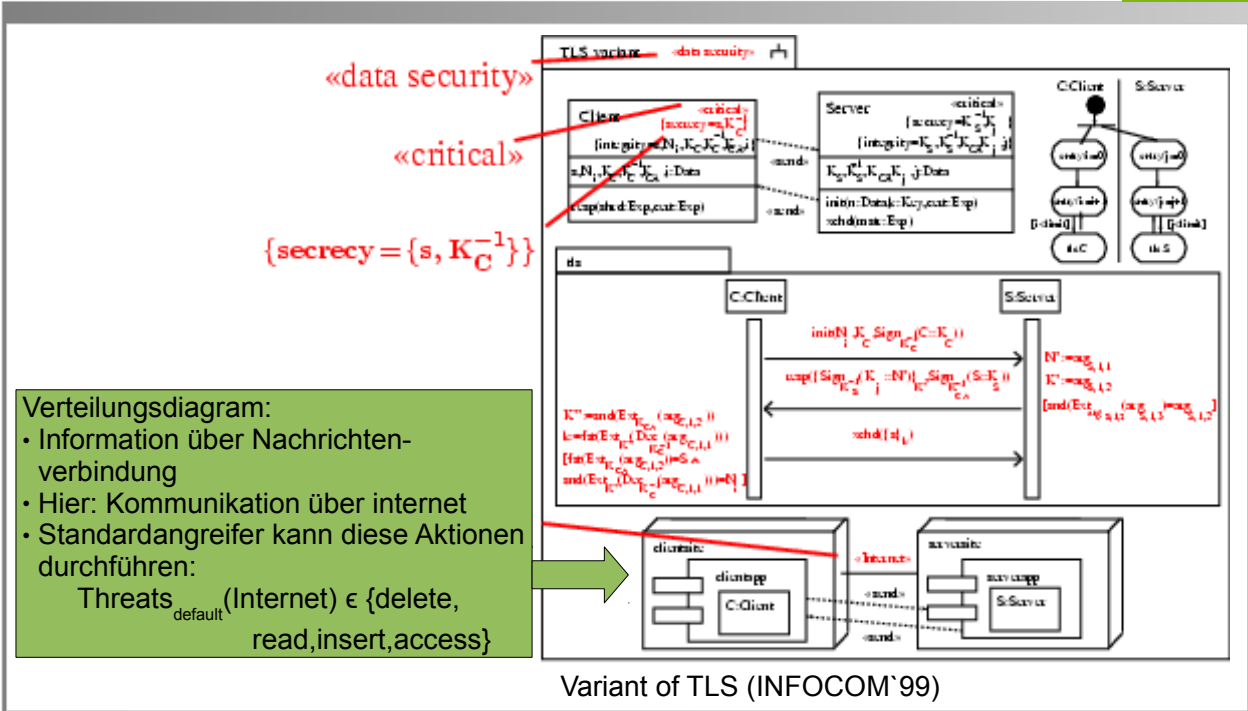
Ziel:

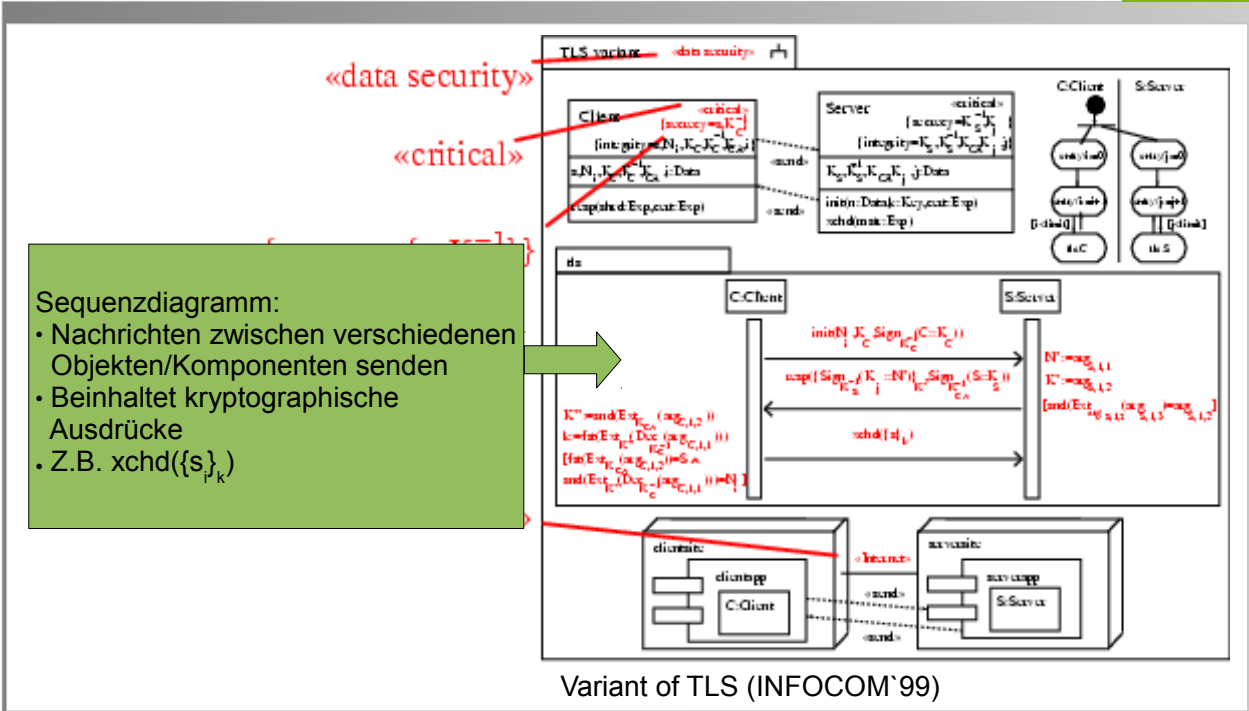
- Vertrauliche Daten verschlüsselt unter Sitzungsschlüssel.
- Weniger Serverbelastung als bei TLS.



Literatur:

- Jan Jürjens: Secure systems development with UML
- Kap. 5.2: S. 85 Abb. 5.4



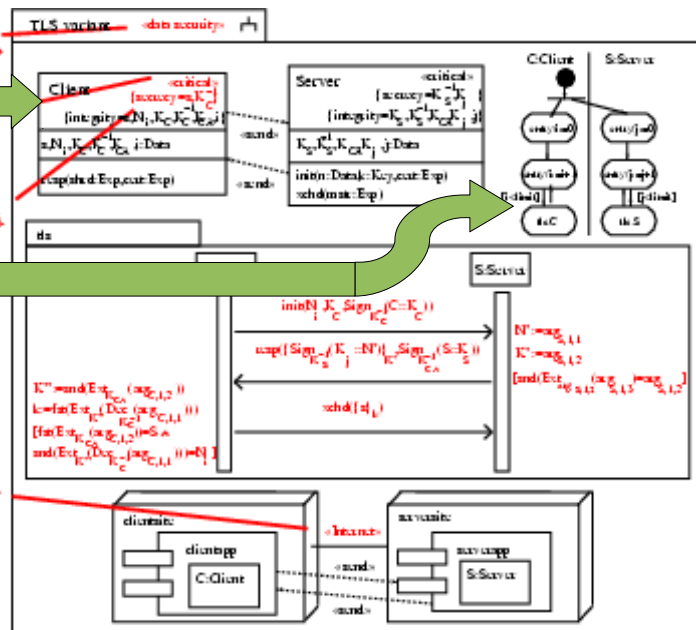


Klassendiagramm:
• Information über Variablen der Daten und Operationen

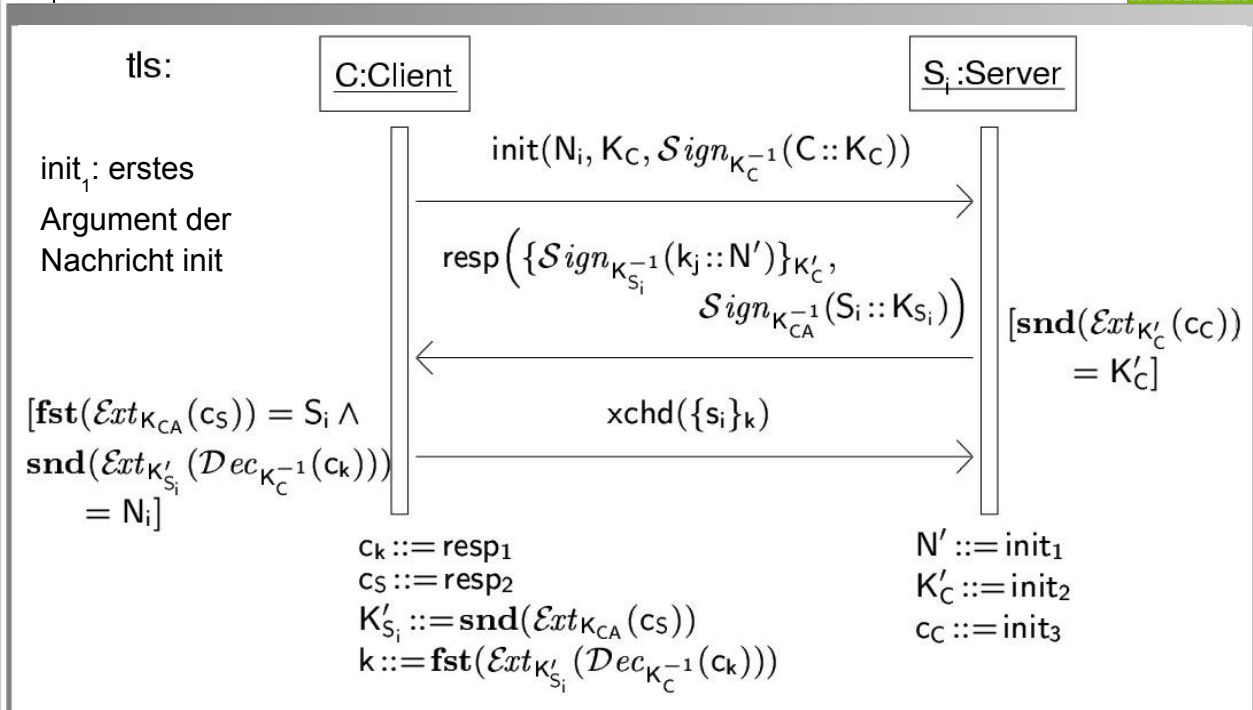
Aktivitätsdiagramm:
• Koordiniert Aktivitäten verschiedener Objekte/Komponente

$$\{secrecy = \{s, K_C^{-1}\}\}$$

«Internet»



Variant of TLS (INFOCOM'99)



Literatur:

- Jan Jürjens: Secure systems development with UML
- Kap. 5.2: S. 85 Abb. 5.4



- Annahme: Angreifer besitzt zum Schlüssel K_{CA} gehörenden vertraulichen Signaturschlüssel der Certification Authority (CA).
- Wie kommt er damit an zu übertragendes Geheimnis s_i ?

Literatur:

Jan Jürjens: Secure systems development with UML

- Kap. 5.2: S. 86-87



- ISO Schichtenmodell und Sicherheit
- Angreifer-Modell
- Kryptographische Ausdrücke
- Kryptographische Protokolle