Voice over IP – Sicherheitsaspekte

Dipl.-Wirtsch.-Inf. Florian Scheuer
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

Dresden, 30.09.2008

Agenda

1. IT-Sicherheit und Voice over IP

2. Gefahren für VoIP-Nutzer und Gegenmaßnahmen
   - Vertraulichkeit
   - Integrität
   - Verfügbarkeit

3. Skype – erfolgreich und proprietär

IP-Telefonie - Überblick

- SIP-basierte Systeme
- H.323-basierte Systeme
- Skype
- sonstige Systeme (z.B. Jingle/GoogleTalk, IAX, ...)

Festnetztelefonie vs. Voice over IP

- Exklusivität der Leitung bei VoIP nicht mehr gegeben.
- Kosten für VoIP wesentlich geringer.
- Verfügbarkeit von Hard- und Software für Angriffe bei VoIP wesentlich größer.
- Verfügbarkeit des Anschlusses bei VoIP nicht so sicher wie bei Festnetztelefonie.

IT-Sicherheit bei VoIP?

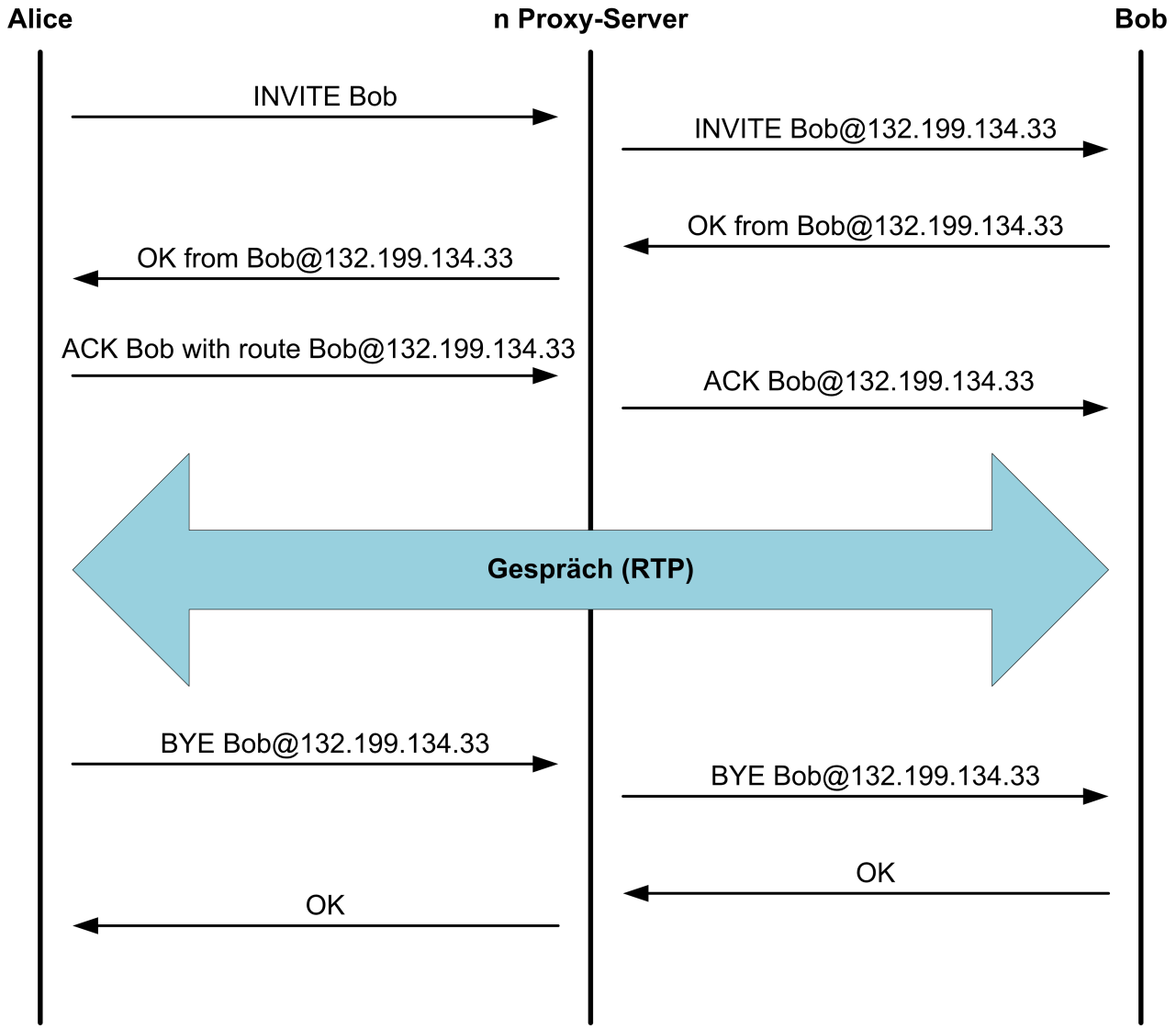
- VoIP ist ein IT-System wie andere Internetdienste auch.

- Gefahren sind vielfältig:
  - Abhören von Gesprächen ((Industrie-)Spionage, Datenschutzproblematik, …)
  - Manipulation von Daten (Telefonieren auf Kosten anderer, Verfälschen von Telefonaten, …)
  - Lahmlegen von Telefonsystemen (Konkurrenz ausschalten, Notrufe unterbinden, …)

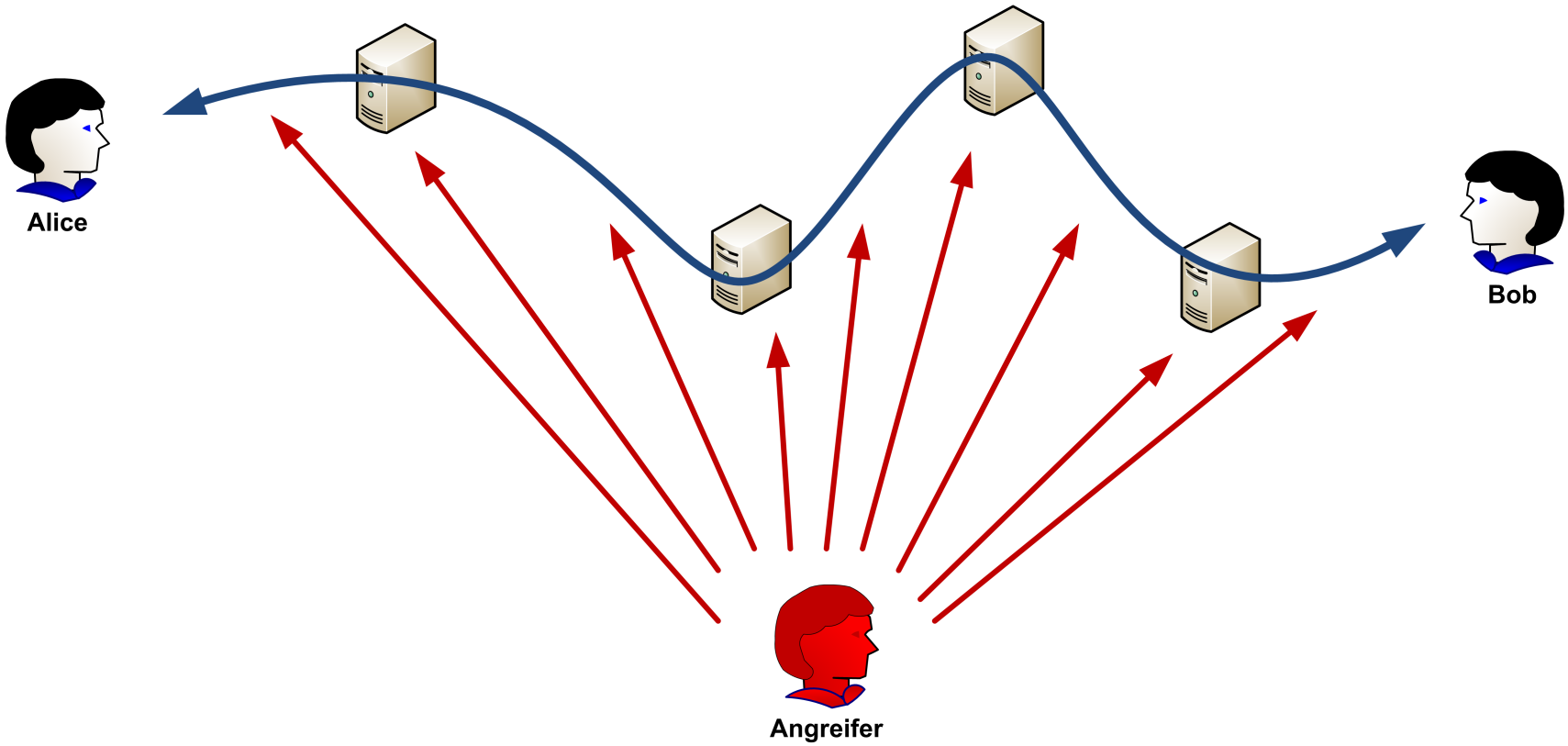
Schutzziele der IT-Sicherheit

- Vertraulichkeit
  - geheime Kommunikation, Anonymität, Unbeobachtbarkeit, ...
- Integrität
  - Unverfälschtheit, Zurechenbarkeit, Rechtsverbindlichkeit, ...
- Verfügbarkeit
  - Möglichkeit der Dienstnutzung zu jedem Zeitpunkt gegeben

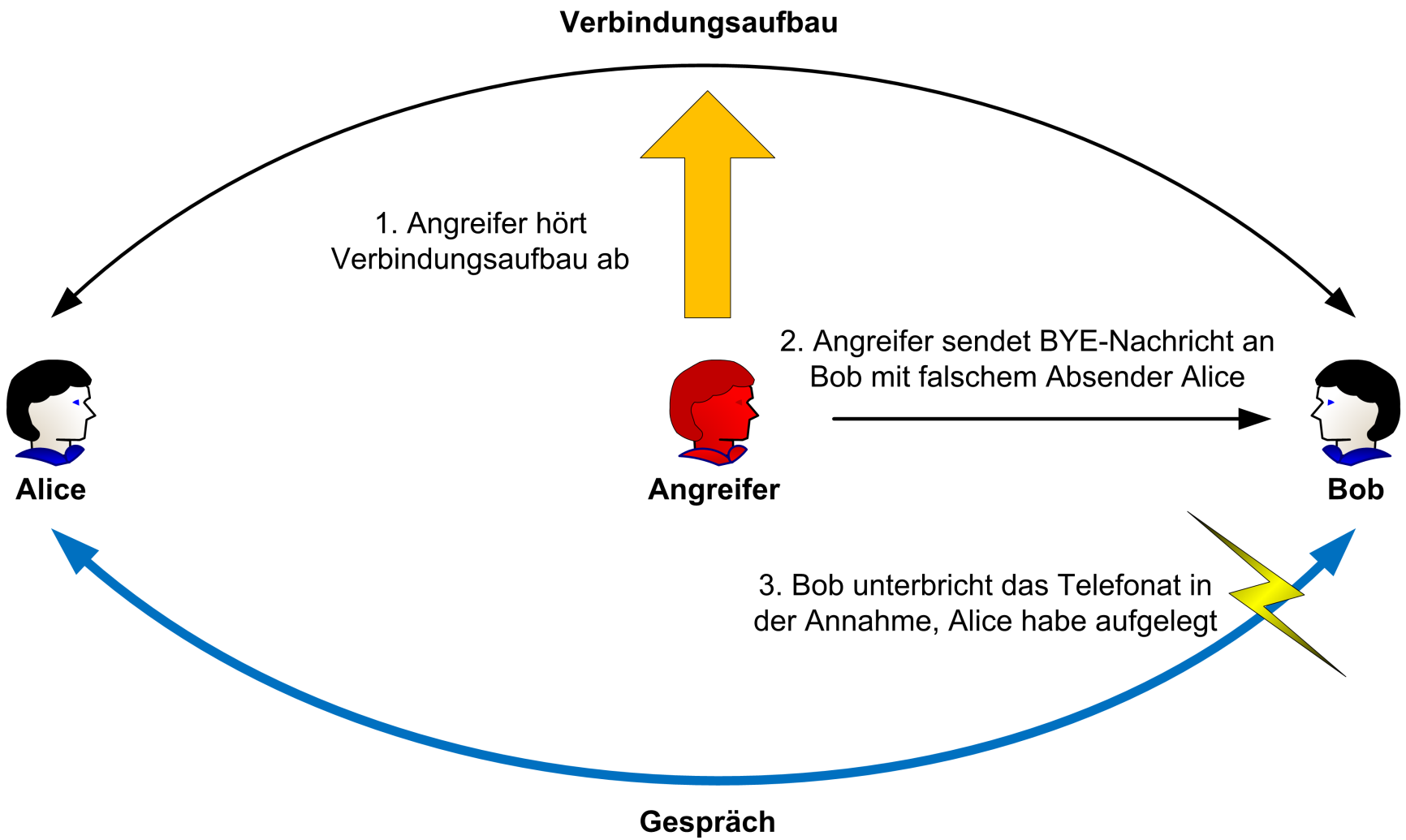
SIP - Protokollablauf



Unverschlüsselte Verbindungen



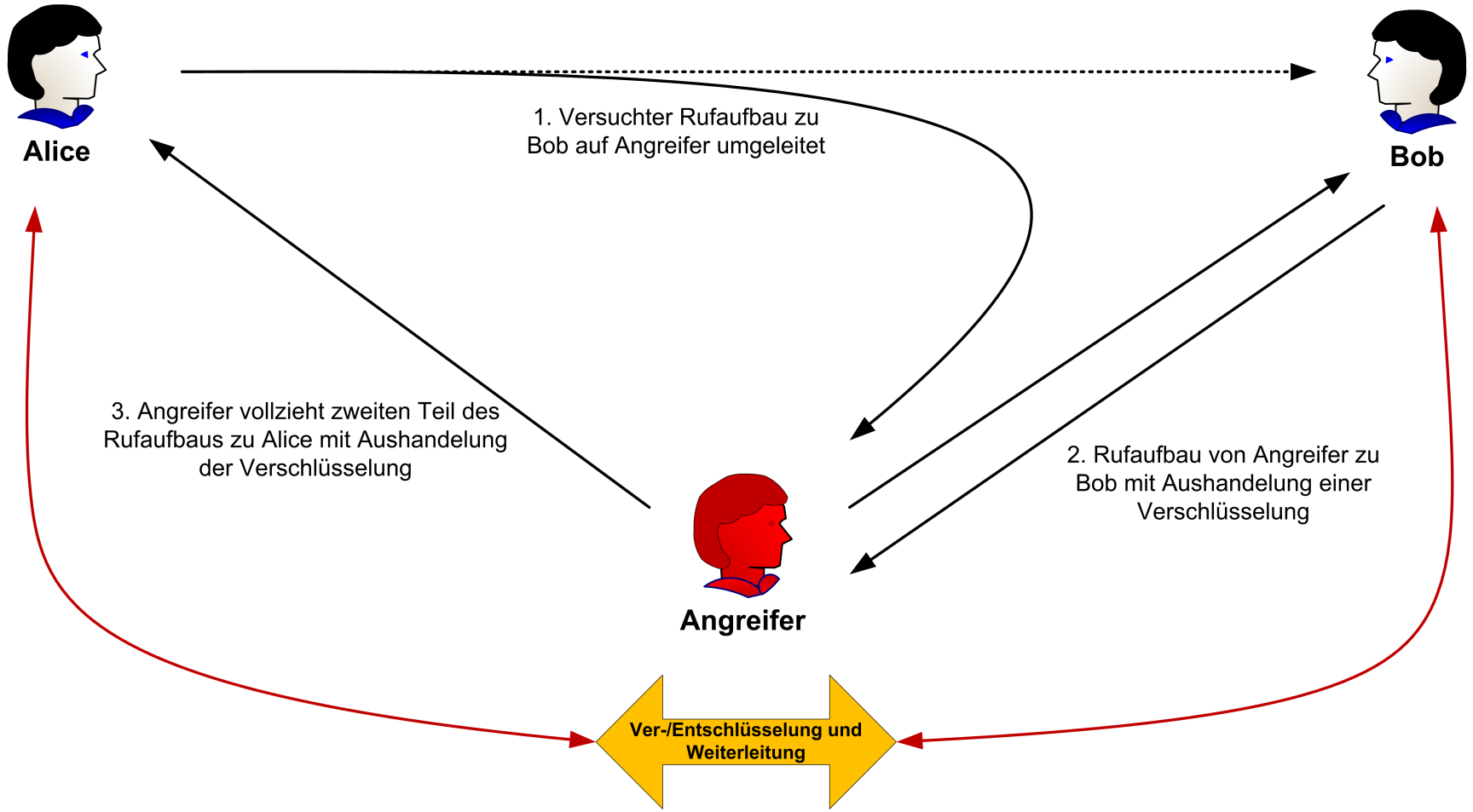
Unautorisierte Trennung der Verbindung



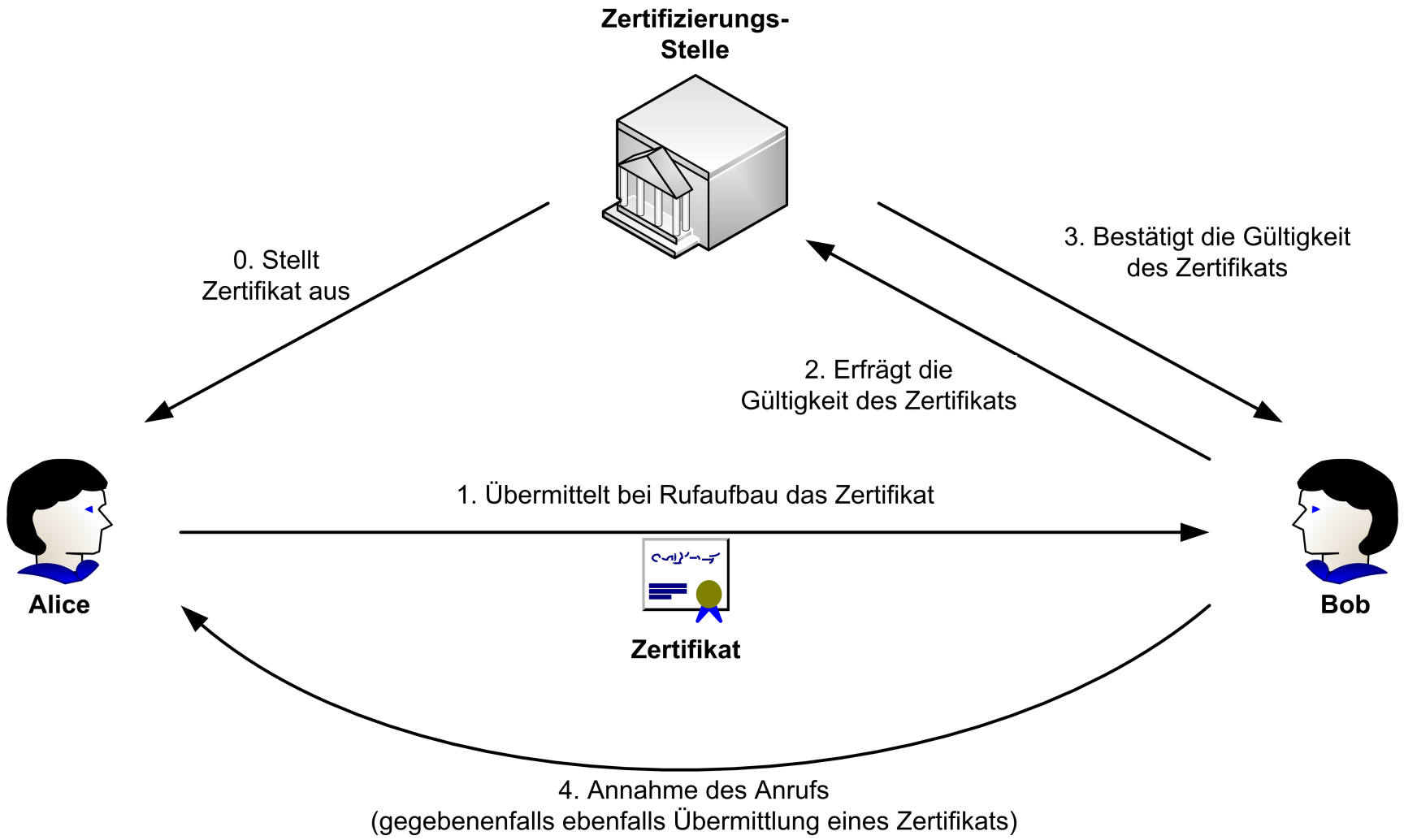
Angriffe auf die Vertraulichkeit

- Probleme:
  - Unverschlüsselte Übertragung ist einfach abzuhören.
  - Unverschlüsselter Verbindungsaufbau gibt Informationen über die Gesprächspartner preis.
- Lösungsmöglichkeiten:
  - RTP kann relativ einfach verschlüsselt werden (SRTP).
  - Verschlüsselung von SIP schwierig – Zwischenstationen müssen Daten lesen und ändern können.
- Fazit:
  - Gesprächdaten lassen sich gut verschlüsseln, der Rufaufbau dagegen nur mit sehr aufwändigen Mechanismen.

Man-in-the-Middle – Angriff



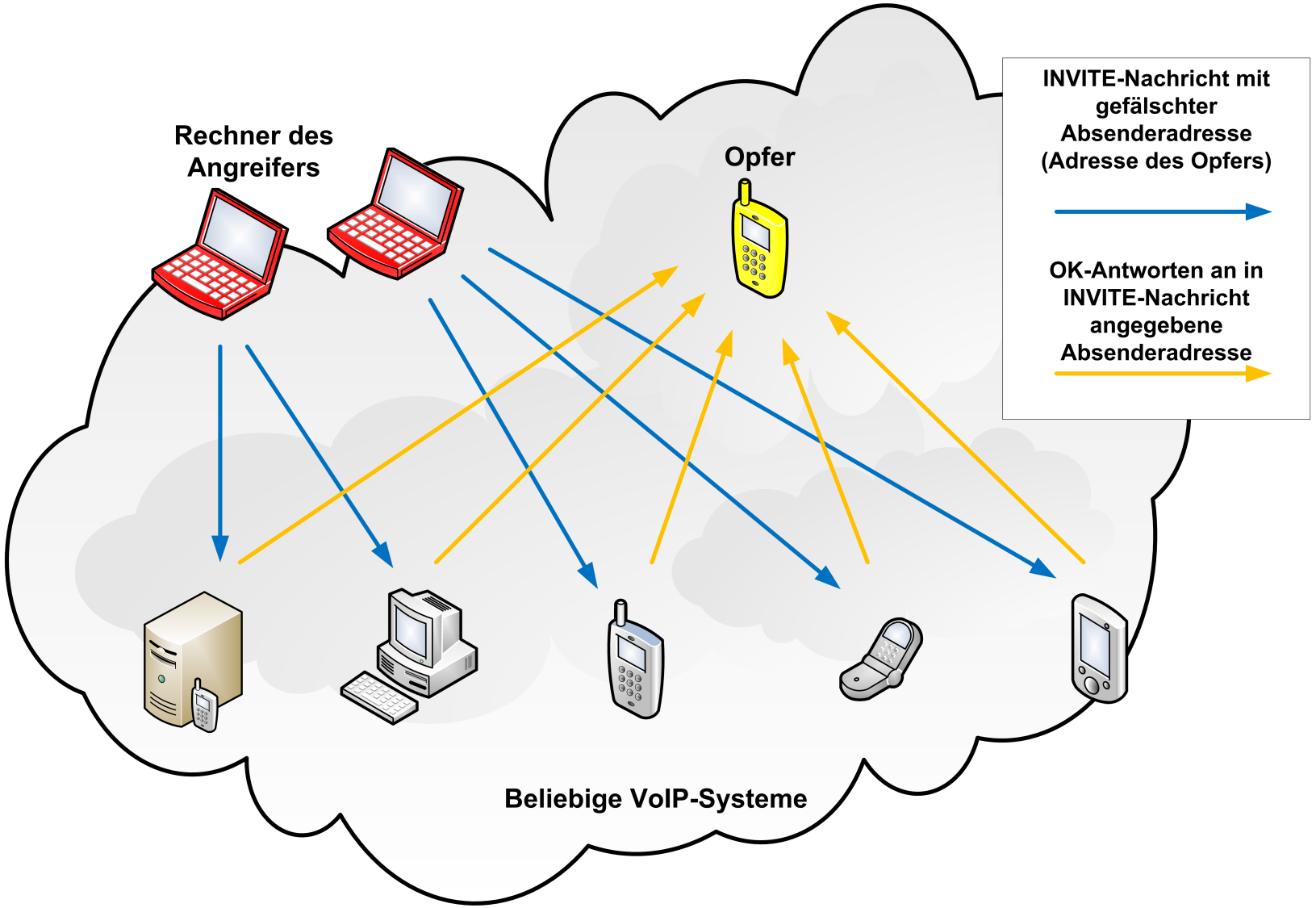
Sicherer Rufaufbau mit Zertifikaten



Angriffe auf die Integrität

- Probleme:
  - Manipulation von SIP- oder SDP-Paketen kann viele unerwünschte Nebeneffekte haben.
  - Teilnehmer sollten authentifiziert werden.
- Lösungsmöglichkeiten:
  - Integritätssichernde Kryptographie muss zum Einsatz kommen (Message Authentication Codes); bei SIP wiederum teilweise schwierig.
  - Es wird eine Zertifikatsstruktur (z.B. PKI) benötigt.
- Fazit:
  - Integritätssichernde Maßnahmen aufwändig aber realisierbar.

Distributed Denial of Service (DDoS)



Blacklisting vs. Whitelisting

- Damit ein Anruf entgegengenommen wird, ...

... darf der Anrufer nicht auf einer Liste stehen (Blacklist/Sperrliste).

VS.

... muss der Anrufer auf einer Liste stehen (Whitelist).

Angriffe auf die Verfügbarkeit

- Probleme:
  - Telefonsysteme können mit verschiedenen Angriffen lahmgelegt werden.
- Lösungsmöglichkeiten:
  - Schutz vor Denial-of-Service–Angriffen schwierig, da sie häufig „echte“ Nachrichten verwenden. Filterung teilweise über aufwändige Firewalls auf Applikationsebene möglich.
  - Blacklisting bietet akzeptablen Schutz, führt jedoch ebenfalls zu Problemen.
- Fazit:
  - Die Verfügbarkeit von VoIP-Systemen ist sehr schwierig zu schützen. Hier müssen noch effektive Mechanismen gefunden werden.

SPIT

- Spam over Internet Telephony
- Automatisierte Werbeanrufe über das Internet äußerst einfach und kostengünstig realisierbar.
- Möglicherweise unter Verwendung fremder Computer (Stichwort: Botnetz).
- Filterung sogar noch problematischer als bei SPAM, da Vorab-Filterung praktisch unmöglich (Inhalt wird erst bei Verbindung übermittelt).
- Blacklisting sehr schwierig.

- Viel diskutierter Lösungsansatz: Geringe Preise auch für VoIP-Gespräche.

Skype – Überblick

- Proprietäres, nicht offengelegtes System
- Peer-to-peer – Ansatz ermöglicht gute Skalierung und vermeidet zudem Probleme mit Firewalls
- Setzt *vermutlich* auf sichere Basistechnologien in Hinblick auf Kryptographie und implementiert sie *vermutlich* korrekt
- unterstützt Videotelefonie
- Whitelist-Ansatz mit Hilfe einer „Kontaktliste“
- Inzwischen auch Hardware-Clients (Telefone) verfügbar

Skype – Kritik

- Nicht kompatibel zu anderen Systemen (SIP, …).
- Unter Verschluss gehaltener Code verhindert Aufdeckung wahrscheinlich vorhandener Abhörmechanismen.
- Nicht analysierbare Software mit möglichen Hintertüren ist im Unternehmensumfeld als kritisch zu bewerten.
- Peer-to-peer–Ansatz hebelt teilweise Firewalls aus.

Vielen Dank für Ihr Interesse!

Sind Fragen offen geblieben?

Sie können mich auch gerne kontaktieren:

florian.scheuer@wiwi.uni-regensburg.de