VoIP Fraud

Klaus Darilion
klaus.darilion@ipcom.at
www.ipcom.at

Klaus Darilion

- Elektrotechnik Studium TU-Wien
- Dissertation TU-Wien: „Voice over IP for safety-critical applications“
- Voice over IP seit 2001
- seit 2004 bei nic.at/IPCom GmbH
- aktiv in der Open Source VoIP Community
  - Asterisk, Openser

IPCom GmbH

- Tochter der nic.at (.at Registry, cert.at)
- Beratung,
- Softwareentwicklung,
- Schulungen und
- Systemausstatter für
  - VoIP
  - DNS (Registry Systeme, Anycast)

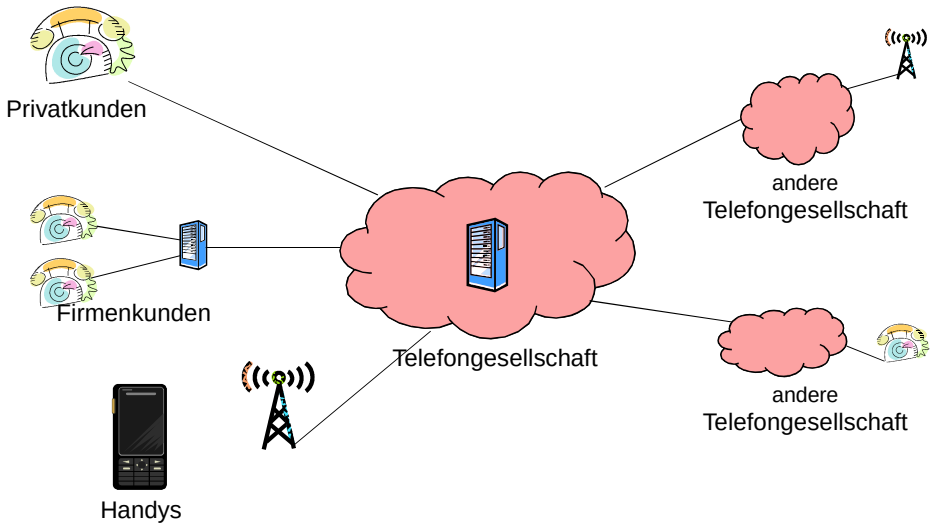
IPCom - VoIP

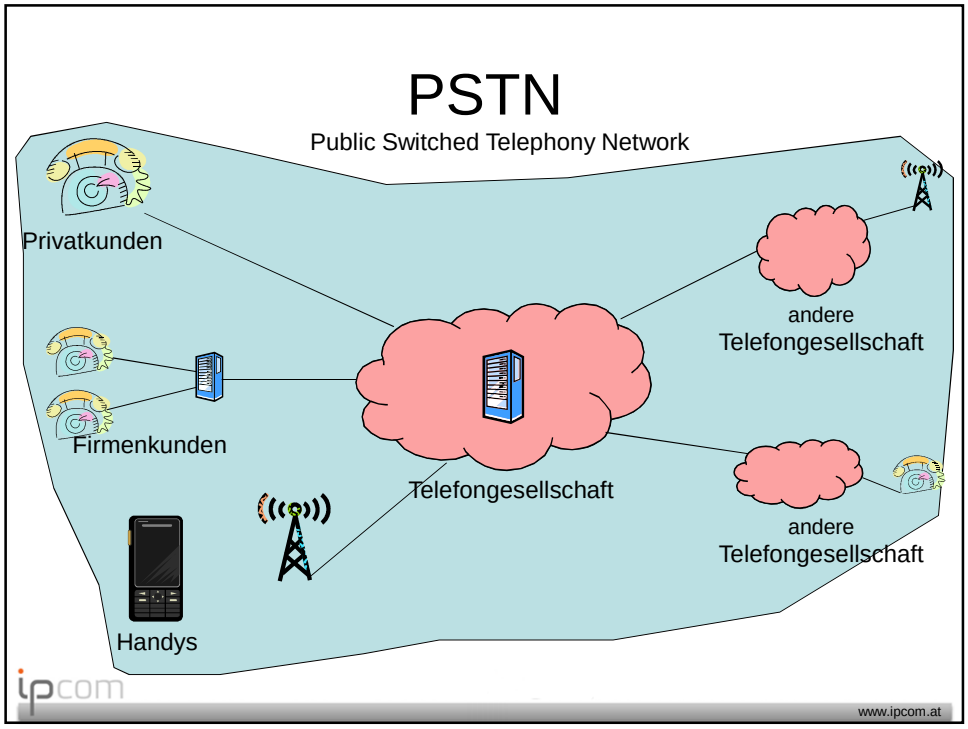
- VoIP-Systeme
  - Beratung, Systemdesign
  - Netzwerkausstatter
  - Carrier (VoIP-Switches, Hosted PBX)
  - Enterprise (VoIP-PBX)
- Security (cert.at)
  - Forschung
  - Beratung
  - Security Audits

Inhalt

- Überblick: klassische Telefonie (analog, ISDN, PBX)
- Fraudmöglichkeiten: Kunde vs. Betreiber
- Fraud bei klassischer Telefonie
- Überblick: Voice over IP (Technik, Einsatzmöglichkeiten)
- Fraud bei Voice over IP
- Fraud Beispiele
- Lösungsansätze (Security, Fraud-Detection)
- Rückverfolgbarkeit (forensic)

Klassische Telefonie





Begriffe

- Telefongesellschaft, Synonyme:
  - Telefonieanbieter
  - Telefoniebetreiber
  - Betreiber
  - Kommunikationsdienstebetreiber (KDB)
  - Kommunikationsnetzbetreiber (KNB)
  - Telephone Provider
  - Telephone Company (Telco)
  - Carrier

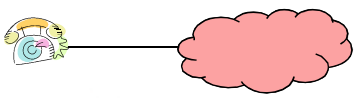
ipcom
www.ipcom.at

Begriffe

- Interconnect
  - Zusammenschaltung der Netze zweier Betreiber
- Telefonanlage, Synonyme:
  - Nebenstellenanlage
  - PBX (Private Branch Exchange)
  - PABX (Private Automatic Branch Exchange)

Technologien

- Analoge Telefonie
  - klassisches “Festnetz”
  - 2-Draht Kupferleitung
  - max 1 Telefonat gleichzeitig
  - typisch für Privatkunden
  - POTS (Plain Old Telephone Service)
  - üblicherweise „post-paid“



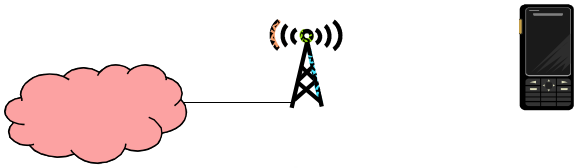
Technologien

- Digitale Telefonie
  - ISDN (Integrated Services Digital Network)
  - auch “Festznetz”
  - 2-Draht Kupferleitung
  - digitale Übertragung
    - Basis-Anschluss: max 2 Telefonate gleichzeitig
    - Multi-Anschluss: max 30 Telefonate gleichzeitig
  - üblicherweise in Verbindung mit einer Telefonanlage
  - typisch für Firmenkunden
  - üblicherweise „post-paid“

ipcom

Technologien

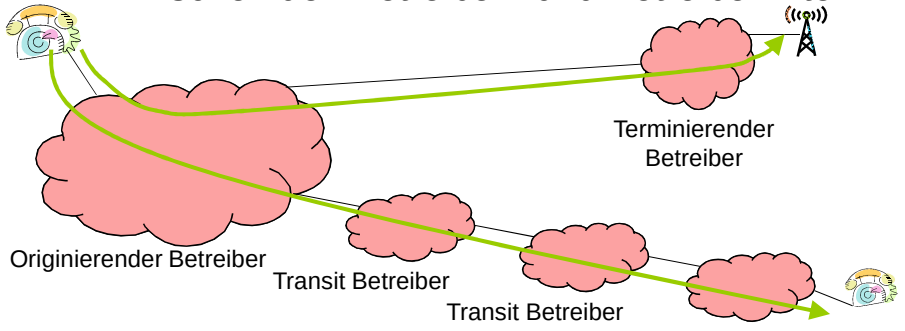
- Mobiltelefonie
  - GSM und UMTS
  - digitale Übertragung
  - sowohl Privatkunden als auch Firmenkunden
  - „post-paid“ und „pre-paid“



ipcom

Technologien

- Interconnect
  - SS7 (Signaling System Number 7)
  - zwischen den Betreibern und Betreiber-intern



ipcom www.ipcom.at

Schnittstellen

- zwischen Endkunden und Betreiber
  - UNI: User-Network-Interface
- zwischen Betreibern (Interconnect)
  - NNI: Network-Network-Interface

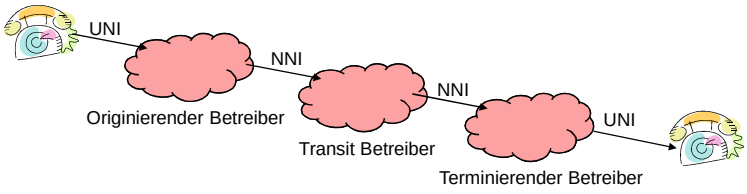
ipcom www.ipcom.at

Abrechnung

- erfolgt anhand von CDRs (Call Detail Records), auch „Tickets“ genannt
  - Wer?
  - Wann?
  - Wohin?
  - Wie lange?

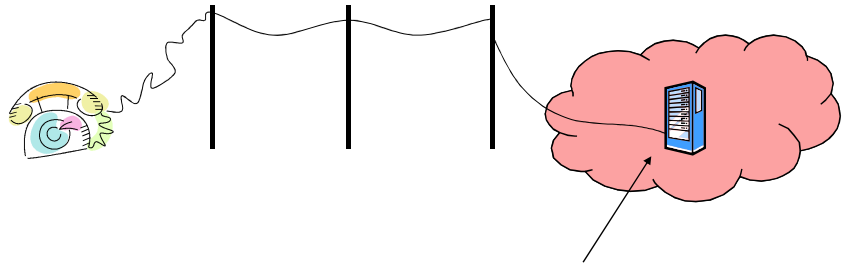
Wer? → Identifizierung des Anrufers

- UNI: Identifizierung des Anrufers (Endkunden)
- NNI: Identifizierung des anderen Betreibers



Identifizierung

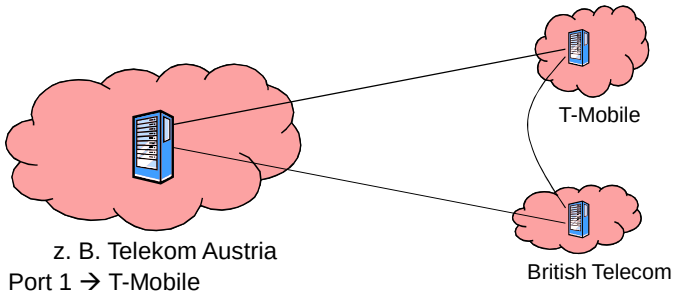
- Klassische Telefonie
  - Authentifizierung durch Kupferleitung „Trust by Wire“



Port 1 → Kundennummer 1538596
Port 2 → Kundennummer 4256536

Identifizierung

- Interconnect
  - Authentifizierung durch Kupferleitung



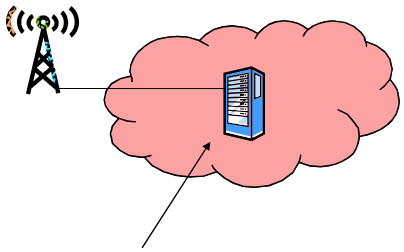
z. B. Telekom Austria
Port 1 → T-Mobile
Port 2 → British Telecom

Identifizierung

- Mobiltelefonie
  - Authentifizierung durch SIM-Karte
  - Kunde bzw. anonymes Pre-Paid-Konto

SIM IMSI: 232018386363

SIM IMSI: 232018386111



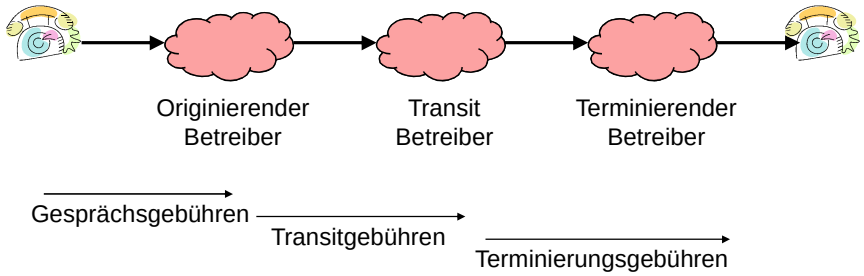
IMSI: 232018386363 → Kunde 1538596
IMSI: 232018386111 → Kunde 4256536

Identifizierung

- in der klassischen Telefonie sehr verlässlich
  - Kupferleitung
    - Identität kann nicht getäuscht werden
    - „anzapfen“ erfordert physikalische Präsenz
  - SIM-Karte
    - geheimer Schlüssel (kennt nur SIM Karte und Betreiber)
    - optional Schlüsselfreigabe durch PIN-Code geschützt
    - nicht kopierbar
    - Diebstahl fällt auf

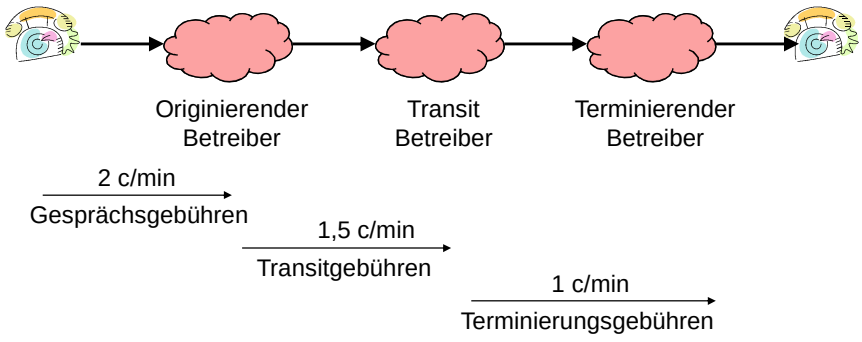
Fraud

- gibt's dort wo Geld fließt
- Geschäftsbeziehungen



Festnetz→Festnetz

01 5056416



Festnetz→Ausland

Kuba
+53 12345678

Originierender Betreiber | Transit Betreiber | Terminierender Betreiber

90 c/min
Gesprächsgebühren

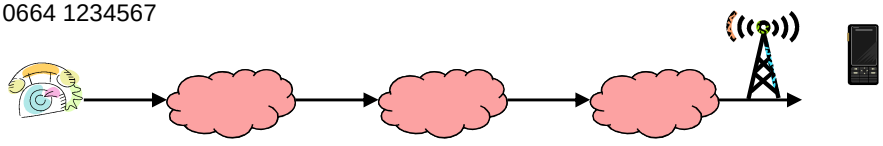
70 c/min
Transitgebühren

60 c/min
Terminierungsgebühren

ipcom
www.ipcom.at

Festnetz→Mobil

0664 1234567



Originierender Betreiber | Transit Betreiber | Terminierender Betreiber

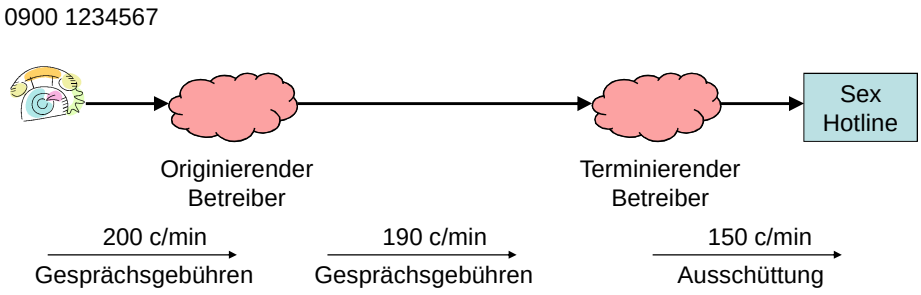
20 c/min
Gesprächsgebühren

5 c/min
Transitgebühren

3,5 c/min
Terminierungsgebühren

ipcom
www.ipcom.at

Festnetz→Mehrwert



Fraud Ziele und Täter

- Ziel
  - gratis/billig telefonieren
  - durch Telefonate verdienen
- Opfer
  - Endkunde: auf Kosten eines Kunden telefonieren
  - Betreiber: auf Kosten des Betreiber telefonieren
- Täter kann sein
  - Endkunden
  - Betreiber
  - oder Dritter

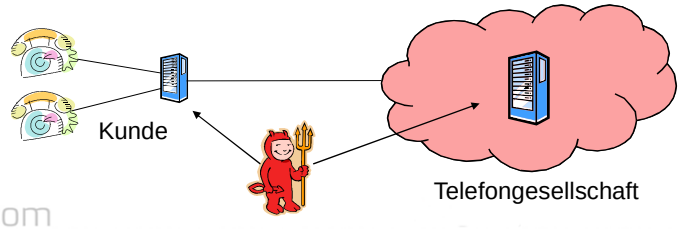
Fraud Arten

- Technologie-Fraud: „hacken“ der verwendeten Protokolle
  - z. B. Umgehung von Authentifizierung, SIM Cloning
- Fraud auf Bezahl-Ebene
  - klassischer Betrug wie er auch außerhalb des Telefoniesektors vorkommt

Technologie-Fraud

- Protokolle relativ sicher
- Starke Authentifizierung durch Hardware-Token: SIM-Karte, Kupferleitung

→ keine direkten Angriffe auf den Telco, aber Angriffe auf dessen Kunden



Fraud auf Bezahl-Ebene

- Kunden mit falscher Identität: Subscription Fraud
  - Identitätsdiebstahl, …
- zahlungsunfähiger Kunde
- hohes Gesprächsaufkommen
- hoch tarifierte Ziele (Mehrwertnummern)

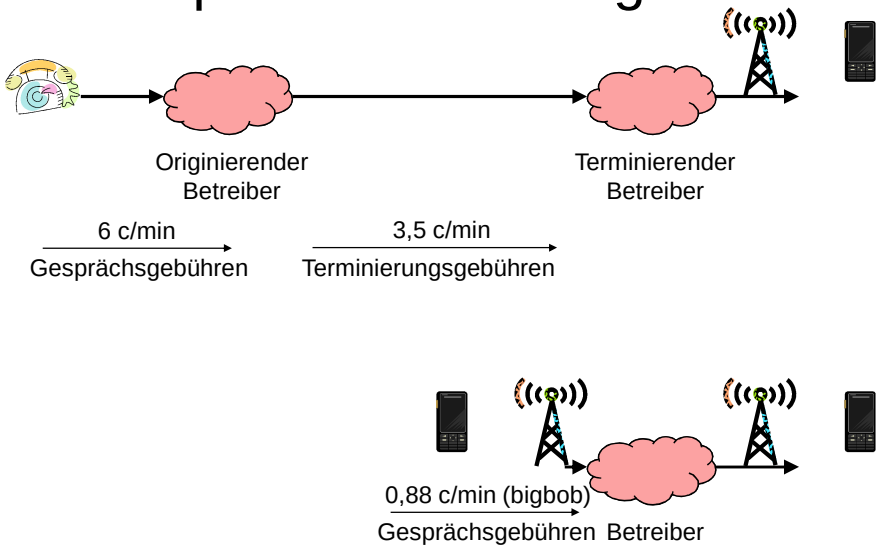
→ Geld nicht eintreibbar (oft hohe Summen)

- Umgehung von hohen Terminierungsgebühren

Beispiel Mehrwert-Fraud

- Kunde wird bereits gepfändet
- Kunde ruft 0900 Nummer an
- 10 000€ Telefonrechnung an Kunde
- 7 000€ Ausschüttung an Mehrwertanbieter
- Betreiber kann vom Kunden kein Geld mehr eintreiben
- Mehrwertanbieter gibt die Hälfte des Gewinns an Kunden (nicht nachweisbar)

Beispiel Terminierungsfraud

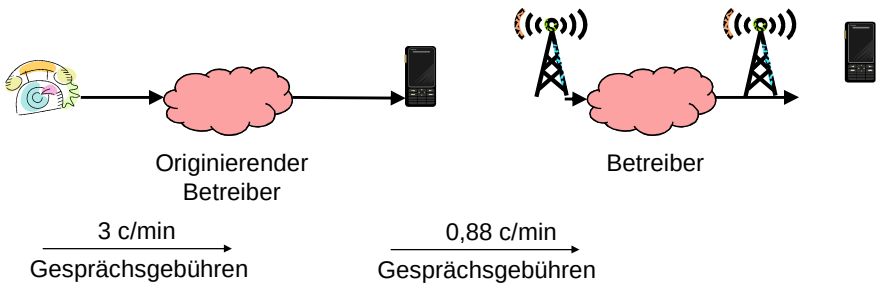


ipcom

www.ipcom.at

Beispiel Terminierungsfraud 2

- Originierender Betreiber kauft SIM Karten
- Gespräche werden über GSM-Gateways terminiert (laut AGBs oft nicht erlaubt)



ipcom

www.ipcom.at

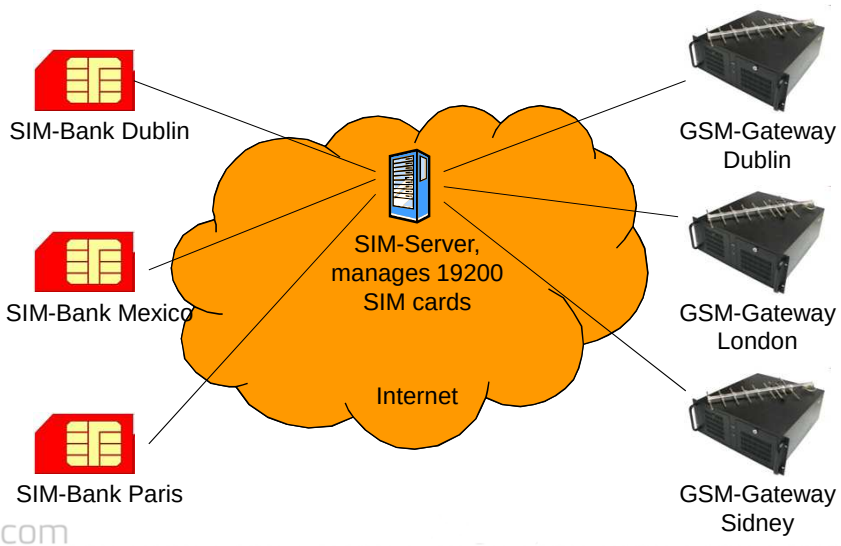
Beispiel Terminierungsfraud 3

- SIM-Gateway Detection
  - Vendor ID
    - wird gefakt
  - verwendet immer gleiche Basisstation
    - viele GSM-Gateways mit shared-SIM
    - Einbuchung in anderen Netzen
  - a-typisches Telefonieverhalten (viele verschiedene Ziele)
    - gegenseitige Anrufe um das Profil zu verändern

Beispiel Terminierungsfraud 4

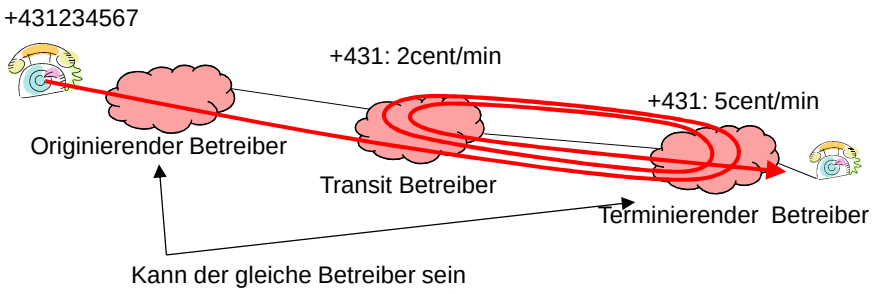
- GSM-Gateways mit vielen SIM-Karten → „SIM Boxing“
- z. B. Elgato SIM-Server, SIM-Bank and GSM-Gateway
  - http://www.elgato.com.ua/

Beispiel Terminierungsfraud 5



Beispiel Interconnect Fraud

- Terminierender Betreiber erhöht Terminierungsgebühren
- Transit Betreiber vergisst die Gebühren anzupassen
- Gespräche werden absichtlich mehrmals über Transit Betreiber geroutet



Beispiel 0800 Fraud

- Kunde (Calling-Card Anbieter) kauft 0800 Nummer mit Weiterleitung zu Nummer in Italien
  - Kunde „verkauft ital. Spezialitäten und will am österreichischem Markt Fuß fassen“
- Kunde zahlt brav seine Rechnung (0800 kostet dem Angerufenen)
- Nach 2-3 Monaten gibt der Kunde Calling-Cards aus mit der 0800 Nummer als Zugangsnummer

→ immenses Gesprächsaufkommen → hohe Rechnung an Kunde in Italien → Briefkastenfirma → Geld nicht eintreibbar

Beispiel 0900 Fraud

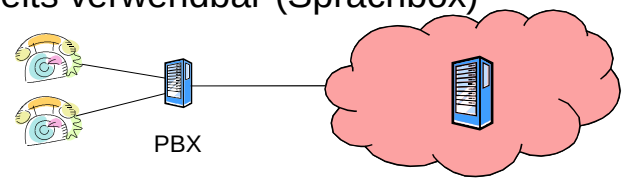
- 0900 Nummer wird meistens auf Festnetz- oder Mobilrufnummer weitergeleitet
- dahinterliegende Rufnummer rausfinden (Altpapier des Dienstanbieters) und direkt anrufen
  - Premiumdienst zum Ortstarif
  - Geld verdienen wenn hinter der 0900 Nummer z.B. ein Bezahldienst angeboten wird

Angriffe auf andere Kunden

- Angreifer gibt sich als anderer Kunde aus → telefoniert auf dessen Kosten
  - Angreifer telefoniert über das Equipment des anderen Kunden
  - Angreifer konfiguriert Equipment um
  - Angreifer hackt das Webinterface (Kunden-Login) und konfiguriert Rufweiterleitung

PBX Fraud

- PBX hat viele nützliche und ausnützbare Features
  - Rufweiterleitung
  - 2-stage Dialing
  - Sprachboxen
- PBX wird „gehackt“ um diese Features zu konfigurieren, oder
- PBX ist schlecht konfiguriert → Features sind bereits verwendbar (Sprachbox)



2-stage Dialing

- Anrufer wählt bestimmte Durchwahl
- PBX “hebt ab”
- Authentifizierung
  - Absenderrufnummer
  - PIN
  - keine („geheime“ Durchwahl)
- PBX wartet auf neue Telefonnummer
  - “Bitte geben Sie die Rufnummer ein. Beenden Sie die Eingabe mit #”
  - DTMF/IVR
- PBX ruft Rufnummer an und verbindet die beiden Telefonate
- Sprachboxen bieten oft 2-stage dialing an
  - wenn die Sprachbox den Default-PIN 0000 hat, sehr einfach auszunutzen

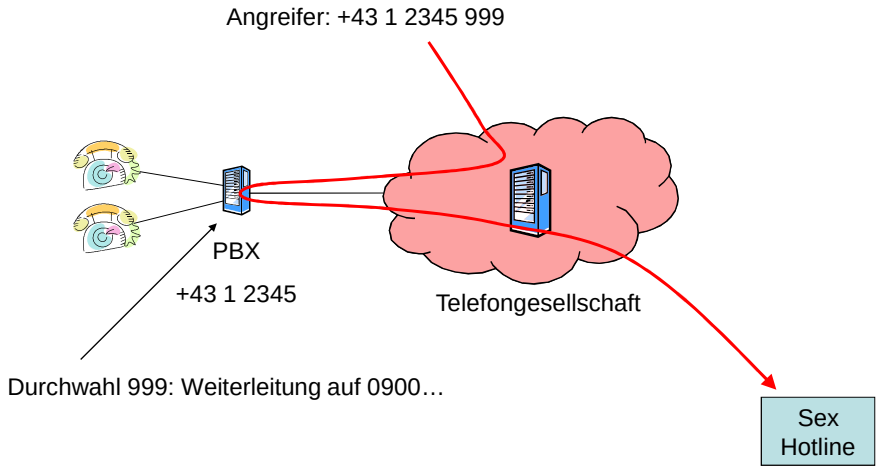
PBX Konfiguration

- über Telefon
- lokal über Software am PC
- entfernt über Software am PC
  - PC hat Modem und ruft eine bestimmte Nebenstelle der PBX
  - Nebenstelle selbst ist auch Modem
  - Datenverbindung zwischen PC und PBX
  - Authentifizierung über Absenderrufnummer oder Username/Passwort

PBX Hacking

- Durchwahl des Fernwartungszugang und 2-stage Dialing
  - Standarddurchwahlen
  - War-Dialing (alle Durchwahlen ausprobieren und warten ob ein Modem abhebt)
- Authentifizierung
  - Standard-Passwörter, Insider-Wissen
  - falsche Absender Rufnummer verwenden

PBX Hacking, Beispiel



PBX Fraud

- Oft ISDN Multi: 30 Leitungen
  - hoher Schaden in kurzer Zeit:
    30/2 x60x24 x 1€/min → 21 600 €/Tag
- Schaden oft auch für Betreiber
  - Kunde sieht nicht ein, dass er 100 000€ Telefonrechnung zahlen soll oder geht in Konkurs

  → oft Vergleich und Betreiber hat auch Verlust

PBX Fraud

- Motivation
  - Anruf auf Mehrwertnummern → Gewinnausschüttung
  - Anruf auf teure Auslandsdestinationen → Gewinnausschüttung
  - Terminierung von Auslandgesprächen für Calling-Card Provider
- PBX Fraud für Betreiber technisch nicht erkennbar

  → Fraud Detection Systeme

Roaming Fraud

- Roaming Grundlagen
  - GSM / UMTS
  - Handy bucht sich in ausländischen Netz ein
  - ausländischen Netz überprüft beim Heimnetz ob die SIM Karte gültig ist
  - Kunde telefoniert
  - ausländischen Netz übertragt CDRs an Heimnetz
  - ausländischen Netz stellt Rechnung an Heimnetz
  - Heimnetz stellt Rechnung an Kunden

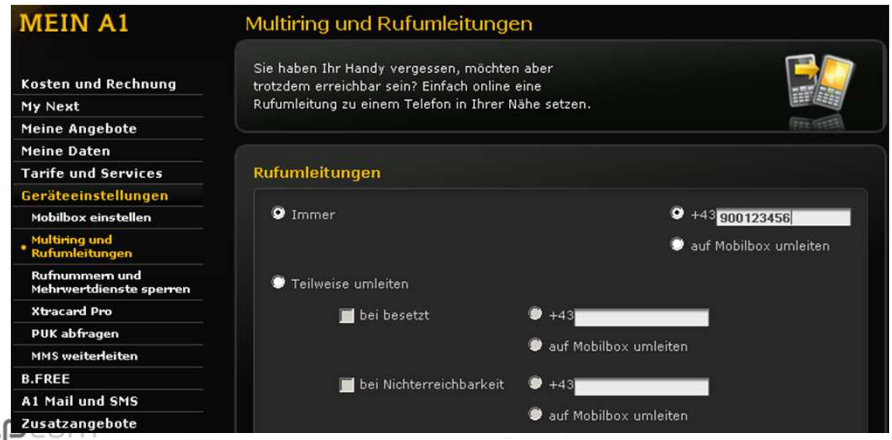
Roaming Fraud

- SIM Karte wird im Ausland verwendet, z. B. in einem GSM-Gateway
- Viele Gespräche zu teuren Destinationen
- Visiting-Provider macht keine Fraud Detection weil es kein Kunde von ihm ist
- CDRs werden zeitverzögert zum Home-Provider übertragen (bis zu mehrere Tage)
- Fraud Detection des Home-Providers schlägt viel zu spät an
- Telefonrechnung nicht eintreibbar (Subscription Fraud)

→ Echtzeitübertragung von CDRs

Rufumleitungs-Fraud

- Betreiber erlaubt Konfiguration von Rufumleitung über Webinterface



Rufumleitungs-Fraud

- Hacker erlangt Zugriff:
  - Webapplikation unsicher
  - Username/Passwort durch Trojaner
  - unsichere Passwörter
- richtet Weiterleitung auf 0900 oder teure Auslandsdestination an

Calling Line Identity (CLI) Fraud

- Network provided number, ANI (automatic number identifaction), calling party number, …
  - "set up" by the provider
  - number that correlates with the physical line or SIM card
  - more or less trustworthy
- User provided number, user number, additional calling party number, …
  - "set up" by the user
  - not trustworthy

CLI Issues

- CLI authenticated services
  - 2stage dialing (call through)
  - voicebox
  - premium rate services (voice and SMS)
  - mobile payment (voice and SMS)
- Implicates trust to the originating provider
  - chain of trust → trust in every operator
- CLI less trustworthy
  - easier becoming a telco
  - SS7 equipment gets cheaper
  - untrained administrators
  - bad telcos
  - only local generated CLIs are 100% trusthworthy

Zusammenfassung

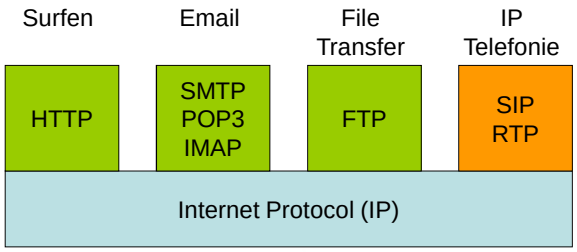
- Fraud auf Bezahl-Ebene (Opfer=Betreiber)
  - Geld nicht eintreibbar
    - falsche Identität (Subscription Fraud)
    - Kunde hat kein Geld
  - AGBs brechen (Terminierung über GSM-Gateway)
- Hacking von Kundenequipment (Opfer=anderer Kunde)
  - PBX Hacking
  - Rufumleitungen

Voice over IP

und Fraud

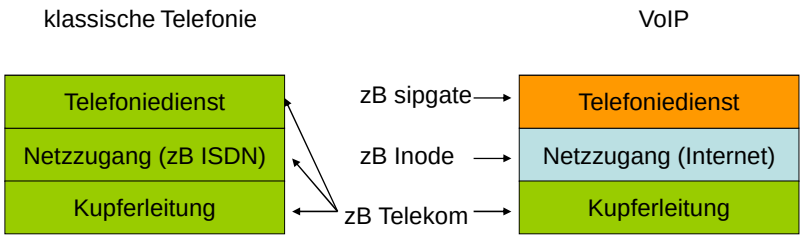
Voice over IP (VoIP)

- Signalisierung und Mediendaten werden über ein IP-Netzwerk übertragen
- VoIP ist einer der möglichen „Dienste“ über IP
  - Signalisierung: Session Initiation Protocol
  - Medien: Real-time Transport Protocol



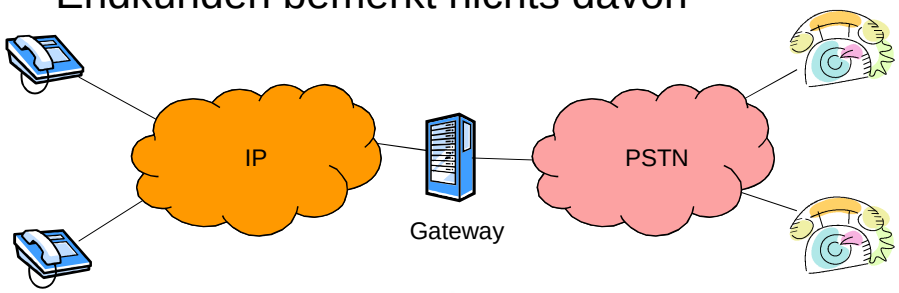
VoIP

- Telefoniedienst ist unabhängig vom Internetzugangsdienst und physikalischem Anschluss



Anbindung von IP-Netzen an das PSTN

- Gateways übersetzten zwischen VoIP (SIP, Skype, …) und PSTN (analog, ISDN, SS7)
- Endkunden bemerkt nichts davon



ipcom

www.ipcom.at

VoIP Anwendungen

- IP ≠ Internet
- VoIP ≠ Internet-Telefonie

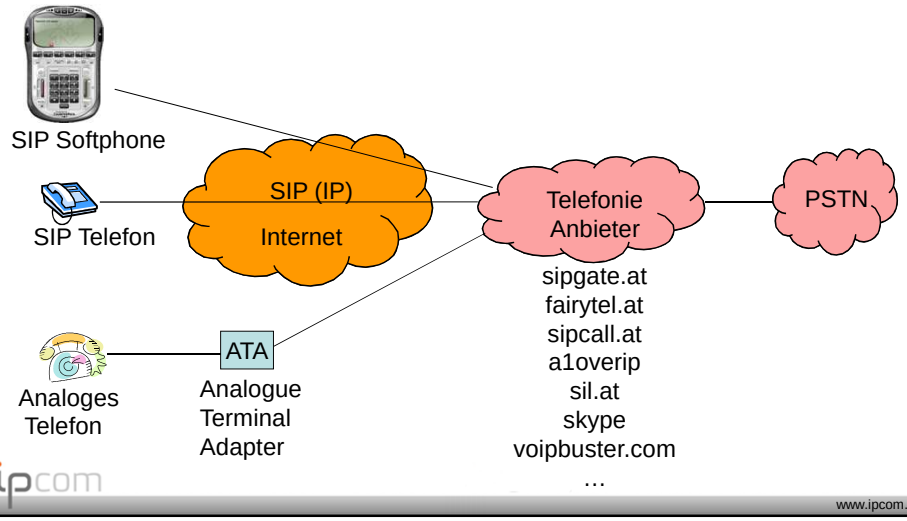
- VoIP wird verwendet in:
  - privaten IP Netzen
  - VPNs (privates Netz über das Internet)
  - öffentlichen IP Netzen (Internettelefonie)

ipcom

www.ipcom.at

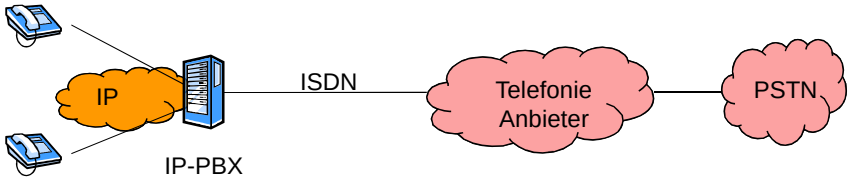
Festnetzersatz

- auch „ POTS Replacement“ genannt



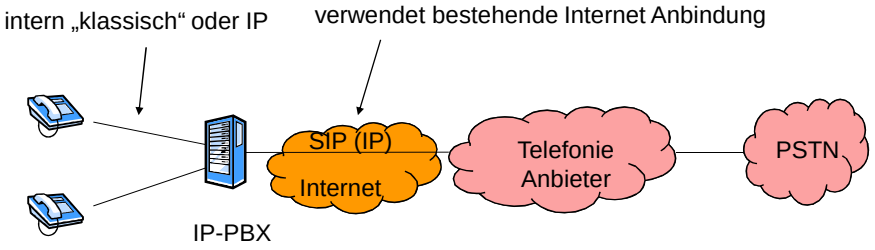
Interne Vernetzung

- Voice over IP Nebenstellenanlage



Anbindung zum Telefonie Anbieter

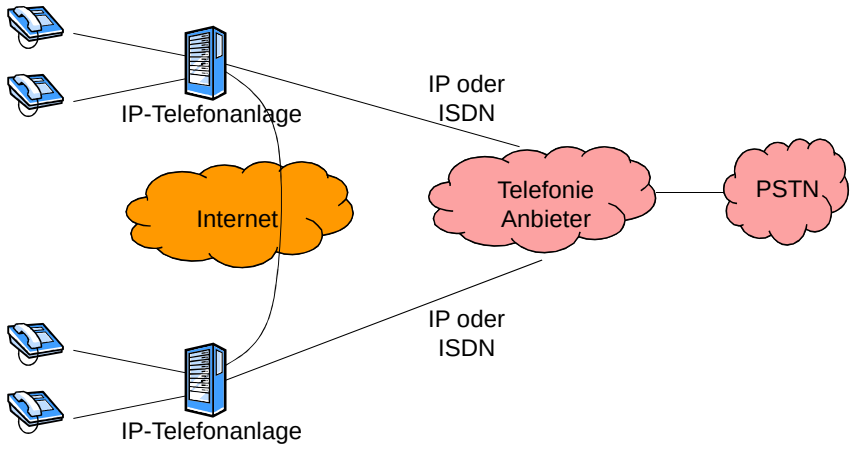
- „SIP Trunking“



ipcom

www.ipcom.at

Standorte vernetzen

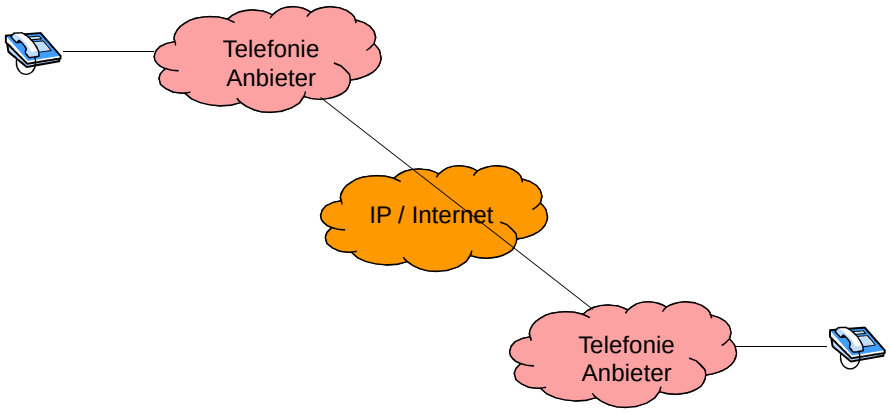


ipcom

www.ipcom.at

Interconnect

- zwischen Betreibern



VoIP Fraud

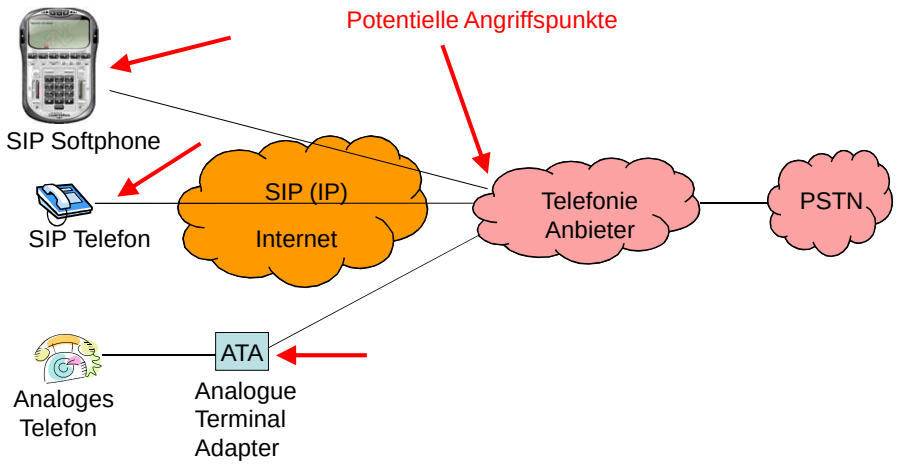
- Fraud auf Bezahl-Ebene
  - genau wie bisher
- Hacking des User-Equipment
  - wie bisher, und neue Methoden über IP
- Attacken auf Protokoll und Applikationsebene
  - gestohlene Zugangsdaten
  - verwundbare Beitreiber-Infrastruktur

VoIP Gefahren

- private Netze sind einigermaßen sicher
  - außer Insider und Hintertüren ins Internet
- Gefahr besteht bei Internetanbindung
  - ist aber notwendig, denn Kommunikation läuft über das Internet
  - Angriff auf den Betreiber
  - Angriff auf/über den Kunden
- Wo sind die Eingangstore für Angreifer?

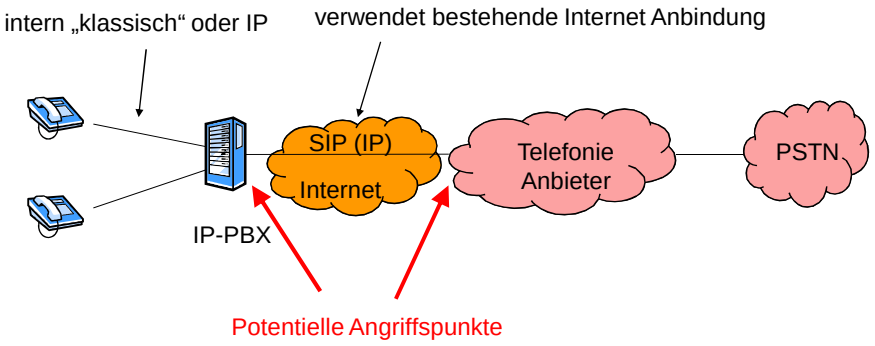
POTS Replacement

- Festnetzersatz



Anbindung zum Telefonie Anbieter

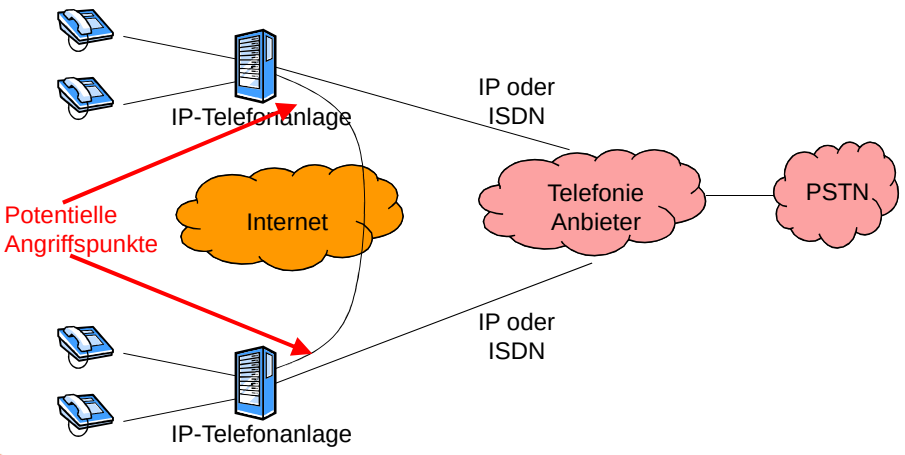
- „SIP Trunking“



ipcom

www.ipcom.at

Standorte verbinden



ipcom

www.ipcom.at

Authentifikation

- traditionelle Telefonie
  - Hardware Token (Telefonleitung, SIM-Karte)
- VoIP
  - Privatkunden
    - Username und Passwort (wie bei E-Mail und Co)
      - Mobilität (Nomadische Nutzung)
  - Firmenkunden
    - Username und Passwort, oder
    - IP Adresse der IP-PBX

Beispiel: Gestohlene Zugangsdaten

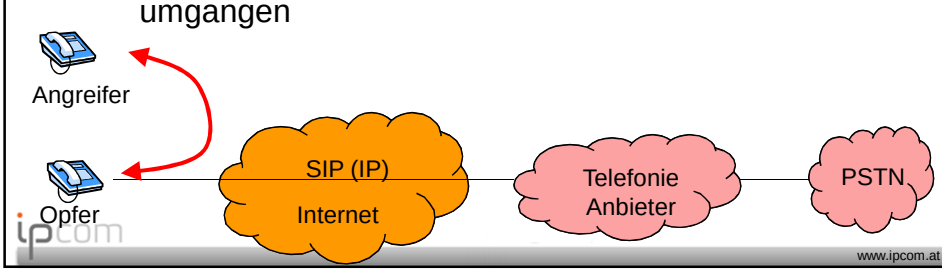
- VoIP:Diebstahl der Zugangsdaten möglich
  - werden im PC/Telefon gespeichert → durch Trojaner auslesbar
  - Übertragung abhören und Brute-Force Attacke gegen unsichere Passwörter
    - unsichere Übertragung (z. B. offenes WLAN)
    - User-Equipment direkt angreifen (über Internet)
  - Kein Sorgsamer Umgang beim Benutzer
- Streitfrage Haftung: Wer ist Schuld? Kunde oder Betreiber?
  - Schwer nachweisbar

Beispiel: Kunde direkt angreifbar

- IP-PBX und SIP Telefone
  - üblich: gesamte Kommunikation läuft über den Betreiber, aber
  - SIP wurde entsprechend den Internet-Ideen entwickelt: Clients können direkt end-2-end kommunizieren

  →Clients erlauben meistens auch direkte Kommunikation

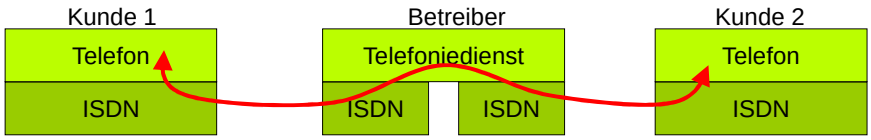
  →Sicherheitsmechanismen des Betreibers werden umgangen



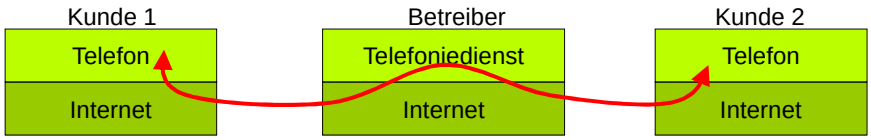
www.ipcom.at

Beispiel: Kunde direkt angreifbar

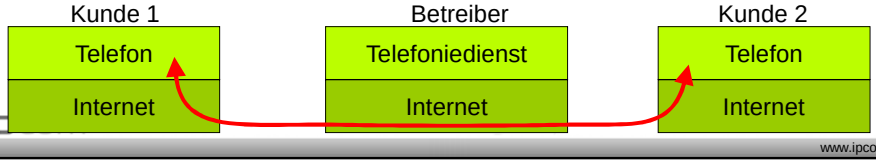
klassische Telefonie:



VoIP – üblich:



VoIP – Hacking:



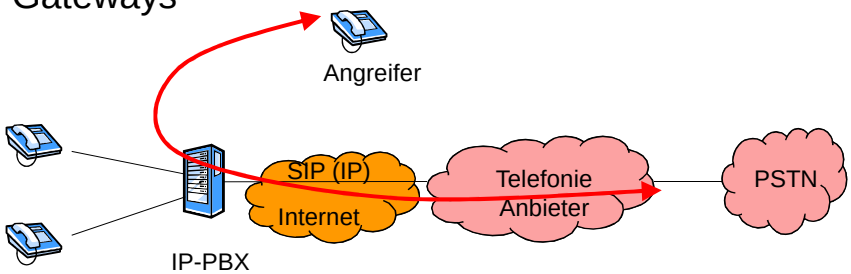
www.ipcom.at

Beispiel: Kunde direkt angreifbar

- durch Umgehung des Betreibers
  - beliebige CLI → Phishing
  - Signalisierung von verbotenen CLIs (0900…)
  - Authentisierungs-Request vortäuschen um einen Passwort-Hash zu bekommen → offline brute-force Attacke
  - manipulierte Pakete schicken → Crash der Software/Hardware (Denial of Service Attacke)

IP-PBX Hacking

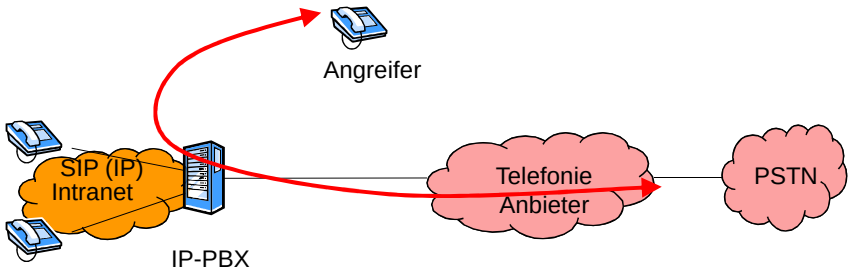
- Suche nach offenen Telefonie-Relays und Gateways



- Indirekt: Hacking eines Linux/Windows Servers und Umkonfiguration der PBX
- Direkt: per SIP eine unsichere Konfiguration ausnutzen

IP-PBX Hacking

- Lokale Nebenstelle unsicher (schwaches/kein Passwort)



- → Angreifer kann sich als lokale Nebenstelle ausgeben

IP-PBX Hacking

1. Auffinden von SIP Clients: Portscanning
   – diverse Tools/Portscanner: sipvicious

```
# ./svmap.py --randomscan
| SIP Device           | User Agent                  |
-------------------------------------------------------
| 194.186.57.234:5060 | Cisco-SIPGateway/IOS-12.x    |
| 121.45.59.124:5060  | unknown                      |
| 218.147.129.28:5060 | unknown                      |
| 222.226.39.117:5060 | unknown                      |
| 84.188.144.141:5060 | AVM FRITZ!Box Fon WLAN 7240  |
| 188.194.10.144:5060 | AVM FRITZ!Box Fon WLAN 7270  |
```

IP-PBX Hacking

2. Überprüfen ob der Client als Relay verwendet werden kann
   - SIP Requests mit verschiedensten Rufnummern in unterschiedlichen Rufnummernformaten
   - SIP Honeypots melden PBX-Hacking Aktivitäten
     - http://www.ipcom.at/fileadmin/public/2008-10-22_Analysis_of_a_VoIP_Attack.pdf
     - http://blog.sipvicious.org/2010/02/rtp-traffic-to-1111.html

IP-PBX Hacking

3. gehackte PBX wird an Telefonie-Anbieter (wissend und nichtwissend) verkauft
   - VoIP Betreiber
   - Calling-Card Anbieter
   - Call-Shops

→Traffic wird über die gehackte PBX abgeführt

IP-PBX Probleme

- unsichere Konfiguration
  - IP-PBX Konfiguration muss „abgehärtet“ werden für Betrieb im Internet
- IP-PBX wird von ahnungslosen Administratoren konfiguriert
  - anhand fehlerhafter, unvollständige HOWTOs
  - oft wird nur getestet ob die gewünschten Feature funktionieren, nicht ob diese auch sicher sind
  - Easy to install, easy to pwn! (own)

IP-PBX Probleme

- IP-PBX wird für Benutzung im LAN konfiguriert, später aber auch im Internet verwendet
  - Standardpasswörter, einfache Passwörter
  - Routing erlaubt Telefonate ins PSTN ohne Authentifizierung
- manche IP-PBXen sind einfach nicht für einen Einsatz im Internet konzipiert!

Betreiber Hacking

- Infrastruktur unzureichend abgesichert, z. B.
  - Application Layer Attacks
    - komplexe Rufumleitungsszenarien werden in den CDRs of falsch abgebildet.
  - Protocol Attacks
    - Routing Manipulation, Source IP Address Spoofing, CLI Spoofing, Unsichere Passwörter
  - Bidirektionales Early Media
    - VoIP-Gateways sind oft schlecht konfiguriert

Security Audits

- VoIP Telefonie Anbieter in AT und SK überprüft
- typische gefundene Schwachstellen
  - falsche Absendernummer (CLI Spoofing)
  - gratis Telefonieren
  - auf Kosten anderer Kunden telefonieren

Unsichere Passwörter

- Testaccounts
  - user/pass: test/test
- leere Passwörter
- einfache Passwörter
  - 1234567, abcdefg, passwort=username
- SIP: Passwort nie im Klarttext übers Internet, aber
  - 5-stelliges Passwort ist in 3h gecrackt!
  - Wörterbuch-Attacken noch schneller

Konsequenzen für Betreiber

- SIP verschlüsseln (TLS), keine vom Benutzer frei wählbare Passwörter
- Fraud-Detection: Monitoring von Gesprächsumsatz, Destinationen (Userprofile)
- Pre-Paid (auch für Kunden empfehlenswert)
- Intrusion Detection Systeme (auch IP-PBX Kunden)
  - fehlgeschlagene Logins
  - ungültige Rufnummern (viele fehlgeschlagene Anrufe)
- Die stärkste Verschlüsselung zwischen Kunde und Betreiber hilft nicht gegen eine gehackte PBX!

Konsequenzen für Kunden

- Standard IT-Sicherheit für alle VoIP Komponenten
- „sicherer“ Wählplan
  - eingehende Anrufe dürfen niemals rauswählen können
  - fertige Konfiguration von Experten überprüfen lassen
  - deaktivieren von PBX-Features auf eingehenden „Trunks“
- IP-Kommunikation nur mit Anbieter erlauben, Credentials nur zum bekannten SIP Proxy
- mit Betreiber ein Limit vereinbaren
- Mehrwertnummern beim Betreiber sperren lassen

Forensische Analysen

- Logins für Konfiguration, Fernwartung, Webinterface mitloggen
  - Absender bei Login über PSTN kaum feststellbar/verlässlich
  - IP Adressen können gehackte PCs sein
- Verwendung von 2-stage Dialing mitloggen

Forensische Analysen VoIP

- typische IT-Forensic: Logfiles
  - Logins: SSH, SIP
  - Absender-IP Adressen bei Telefonaten mitloggen
    - muss man konfigurieren oder wird nicht unterstützt
    - IP-Adressen oft nicht aussagekräftig (relays, dyn.IPs)
  - Traces erstellen
    - SIP: in großen System riesige Datenmengen
    - Netflow: Nadel im Heuhaufen bzw. Brute-Force erkennen

Noch Fragen?

Klaus Darilion, IPCom GmbH
klaus.darilion@ipcom.at
www.ipcom.at

ipcom
IPCom Gesellschaft für internetbasierte Kommunikationsdienste mbH