SPAM over Internet Telephony

and how to deal with it

Diplomarbeit von Rachid El Khayari
Supervisor: Prof. Dr. Claudia Eckert, Nicolai Kuntze, Dr. Andreas U. Schmidt

Einleitung Vogelpersepktive

- Schätzungen zu folge ist Email Spam 80-90 % des Email Traffics
- Bedrohung kann sich auch auf VoIP Umfeld ausbreiten
- SPAM over Internet Telephony (SPIT) ist sogar noch kritischer (höherer Störfaktor)
  - E-Mail um 4 Uhr nachts vs. Anruf um 4 Uhr nachts!

Einleitung
Agenda

- Was ist SPIT?
- Was gibt es für SPIT Abwehrmechanismen?
- Haben diese Abwehrmechanismen Schwächen?
- Wie kann ein Angreifer diese Schwächen ausnutzen?

Anmerkung:
Diskussion basiert auf dem Session Initiation Protocol (SIP)

Was ist SPIT?

Erste Herangehensweise

Was ist SPIT?

- SPIT vs. SPAM
- Gemeinsamkeiten:
  - beides unerwünschte Nachrichten
  - Angreifer benutzen Infrastruktur des Internets
- Unterschiede:
  - Email ist ein asynchroner Dienst
  - VoIP ist ein synchroner Dienst
  - Email enthält zu übertragende Daten bereits in sich
  - VoIP Inhalt wird erst nach! Sessionaufbau übertragen

Was ist SPIT?
SPIT vs. SPAM

- Konsequenz des Unterschiedes:
  - Email Spam Empfänger kann entscheiden wann und ob Nachricht gelesen wird
  - SPIT Empfänger hat diese Freiheit nicht, wenn das Telefon klingelt
  - Email Inhalt kann analysiert werden bevor Nachricht eintrifft
  - SPIT Inhalt kann nicht überprüft werden bevor Telefon klingelt

Wenn das Telefon klingelt ist es bereits zu spät und das Telefon klingelt sofort!

Jetzt wissen wir was SPIT nicht ist

und nicht was SPIT ist!

Was ist SPIT?
Intuitive SPIT Definition

- Einige Definitionen aus der Literatur:
  - Unerwünschte, nicht angeforderte Anrufe
  - Unerwünschte Werbeanrufe
  - Massenweise Übertragung unerwünschter Anrufe
  - Massenweise unerwünschte Verbindungsaufbauversuche, mit dem Ziel eine Voice, Video oder IM Session aufzubauen
- Problem mit diesen Definitionen:
  - entweder zu spezifisch oder zu allgemein
  - decken nicht alle Facetten von SPIT ab

Was ist SPIT?
SPIT Analyse

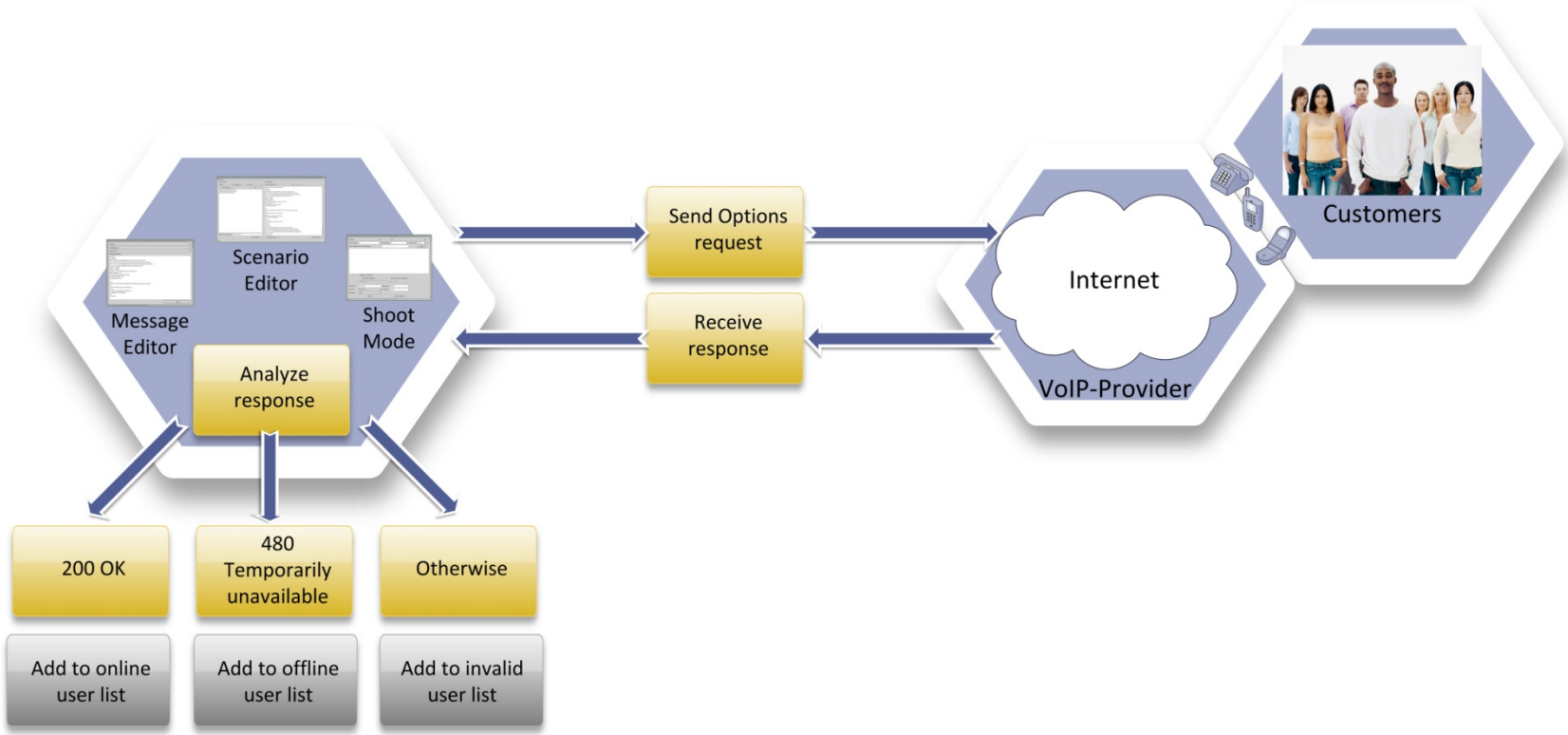
- Wie kann man eine bessere Definition finden?
  - Was ist das Ziel eines Angreifers?
    - Eine Kommunikationssession mit so vielen Opfern wie möglich aufbauen, um so eine Nachricht an alle möglichen erreichbaren Endpunkte zu übertragen
  - Wie kann dieses Ziel erreicht werden?
    1. Systematisches Sammeln von Kontaktadressen potentieller Ziele
    2. Kommunikationssession mit den Zielen aufbauen
    3. Nachricht übertragen

Fundamentalen 3 SPIT Schritte

Was ist SPIT?
Schritt 1 – Informationen sammeln

- Wir können 2 Arten von Kontaktadressen unterscheiden:
  1. Temporäre SIP URIs
     (z.B. <sip:someone@192.0.2.5>)
  2. Permanente SIP URIs
     (.g. <sip:someone@example.com>)
- Scan Attacke:
  - Angreifer scant Netzwerk um folgendes herauszubekommen:
    - Temporäre URIs
    - Permanente URIs
    - Oder beides (im besten Fall)

Was ist SPIT?
Schritt 1 – Informationen sammeln



Was ist SPIT?
Schritt 1 – Informationen sammeln

- Scan Attacke (permanente URIs):
  - Angreifer kennt das Nummernschema eines Providers (z.B. 555XXXX)
  - Angreifer sendet INVITE Request zu allen möglichen Zielen (z.B. 5550000-5559999)
  - Antwort ist '404 Not found'
    - folglich: Nummer nicht vergeben
  - Antwort ist '480 Temporarily unavailable'
    - folglich: Nummer ist vergeben, User aber offline
  - Antwort ist '200 OK'
    - Nummer ist vergeben, User erreichbar
  - Attacke kann auch „im Stillen" durchgeführt werden:
    - Sende 'OPTIONS' Request oder einen anderen SIP Request statt INVITE

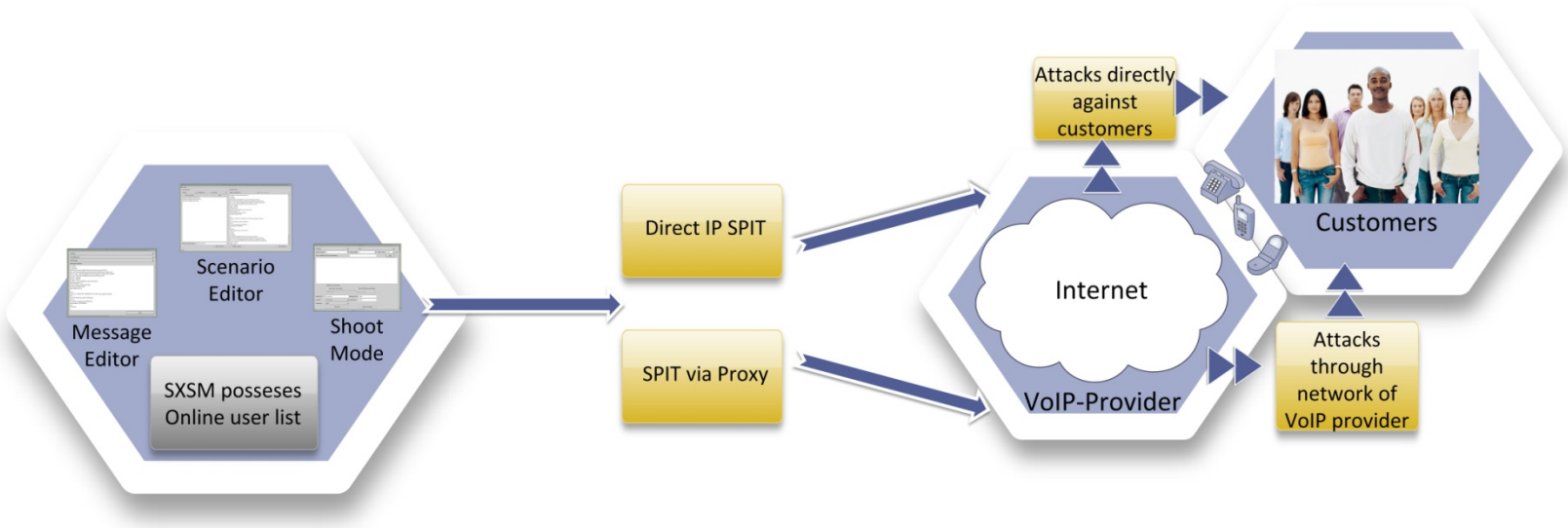
Was ist SPIT?
Schritt 1 – Informationen sammeln

- Scan Attacke (temporäre URIs):
  - Selbe Vorgehensweise wie bei permanenten URIs
    - Zusätzlich IP Adresse aus 'Contact' Header der SIP Response extrahieren
  - Wenn IP Adresse nicht mitgeteilt wird?
    - Brute force (einzig verbleibende Möglichkeit)
  - Angreifer weiß, dass Provider IP Adressen aus Adressraum 192.0.2.5-192.0.2.155 vergibt
    - Sende 'INVITE' Requests zu UDP Port 5060 zu jeder IP Adresse aus Zielbereich
    - Probiere alle möglichen Nummern durch (e.g. 5550000-5559999)
  - Letztere Variante ist erschöpfend:
    - Vorteil SIP Proxy ist nicht involviert

Was ist SPIT?
Schritt 2 – Sessionaufbau

- Zwei Möglichkeiten des Sessionaufbaus:
  - SPIT via Proxy
    - Angreifer benutzt permanente URIs als Ziel
    - Vorteil: Permanente URIs sind einfach aufzufinden
    - Nachteil: Angreifer brauchte gültige Accounts, weil SIP Proxy/Registrar involviert ist
  - Direct IP SPIT
    - Angreifer benutzt temporäre URIs als Ziel
    - Vorteil: Angreifer braucht keine gültigen Accounts
    - Nachteil: Temporäre URIs sind schwerer aufzufinden

Was ist SPIT?
Schritt 2 – Sessionaufbau



Was ist SPIT?
Schritt 3 – Nachrichtenübertragung

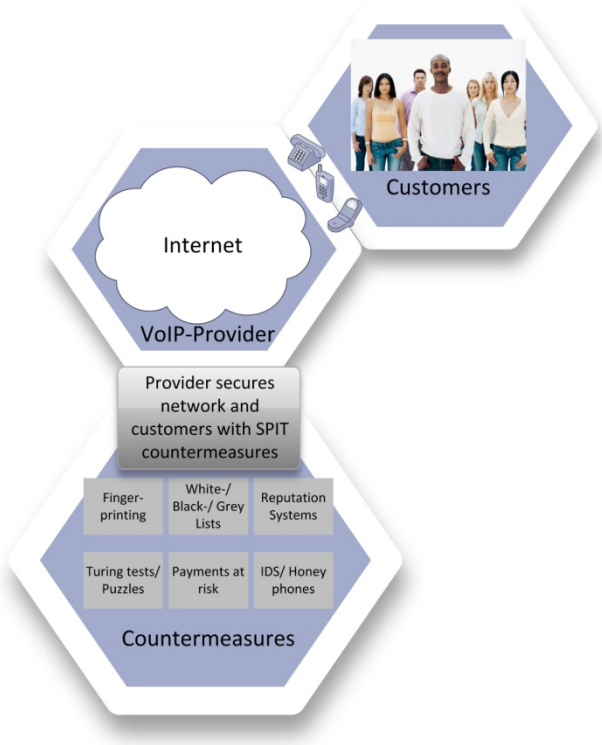
- Welche Art Nachricht übertragen wir, hängt von SPIT Scenario ab:
  - Call center:
    - Computer stellt Verbindung her
    - Übergibt Anruf an Call Center Agent
    - Agent spricht mit Angerufenem
  - Calling bots:
    - Im Voraus aufgezeichnete Nachricht
  - Ring tone SPIT:
    - Der Klingelton ist bereits SPIT Nachricht
    - oder nur das Ziel Angerufenen zu stören

Jetzt wissen wir genau was SPIT ist.

Was wurde aber bisher dagegen getan?

SPIT Abwehrmechanismen Überblick

- Device Fingerprinting
- White-, Black-, Grey Lists
- Reputation Systems
- Turing Tests/Computational Puzzles
- Payments at Risk
- Intrusion Detection/Honey phones



SPIT Abwehrmechanismen Device Fingerprinting

- Annahme:
  - Angreifer kann von „normalen“ Anrufer unterschieden werden, da er Spezial Tools verwendet
- Passives Fingerprinting:
  - Reihenfolge und Auftreten von SIP Header felder wird geprüft z.B. „INVITE“
  - Wenn der Fingerabdruck nicht Standard entspricht -> als SPIT klassifizieren
- Aktives Fingerprinting:
  - Anrufer mit unerwarteten SIP Nachrichten fordern (z.B. ‘OPTIONS’)
  - Reaktion entspricht nicht der eines Standardclients -> als SPIT klassifizieren

SPIT Abwehrmechanismen
Device Fingerprinting - Schwächen

- Passives Fingerprinting:
  - Angreifer sortiert SIP Header Felder wie ein Standard Client
- Aktives Fingerprinting:
  - Angreifer muss sich wie Standard Client verhalten
- Angriff kann „Device Spoofing“ genannt werden

- Anwendungsschwächen:
  - Es gibt viele SIP User Agents (soft phones, hard phones)
  - Administrator muss Fingerprint Liste aktuell halten
    - Ansonsten werden „normale“ Anrufe als SPIT klassifiziert

SPIT Abwehrmechanismen Black-, White-, Grey Lists

- Black Lists:
  - Anrufe von Identitäten, die als Spitter bekannt sind werden geblockt
- White Lists:
  - Nur Anrufe von bekannten Identiäten (Buddies) werden akzeptiert
- Grey Lists:
  - Anrufer wird bei erstem Anruf blockiert, wenn nicht in White List
  - Bei zweiten Anrufversuch wird er erst akzeptiert (zeitliche Nähe)
  - Oder Angerufener kann Grey List durchgehen und für die Zukunft entscheiden (Black oder White)

SPIT Abwehrmechanismen
Black-, White-, Grey Lists - Schwächen

- Black Lists:
  - When Identität auf Black List braucht Angreifer lediglich eine neue
    - SPIT via Proxy: Neuer Account wird benötigt
    - Direct IP SPIT: SIP Identität kann gespooft werden (SIP Identity Spoofing)
- White Lists/Grey Lists:
  - Angreifer braucht eine Identität die bereits auf White List steht
  - Woher weiß der Angreifer welche Identität er annehmen muss?
    - Direct IP SPIT: Brute force -> Alle möglichen ausprobieren (Erschöpfend)
    - Distributed White Lists: White List importieren mit gültigem Account
- Anwendungsschwächen:
  - Black Lists kann nur genutzt werden um zukünftige Angriffe abzuweheren
  - Anrufe kommen oft von Identitäten die nicht auf White List stehen
    - z.B. Anruf von Bankangestellten (Introduction problem)
  - Grey List: Entscheidungsbasis für zukünftige Anrufe ist lediglich Rufnummer
    - Angerufener muss entscheide ob zukünftige Anrufe geblockt werden!

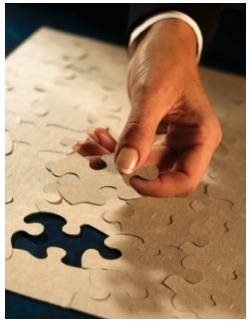
SPIT Abwehrmechanismen Reputation Systems

- Nach einem Anruf kann ein Reputationswert (Ruf) gesetzt werden
  - Spitter werden z.B. mit negativem Wert markiert
  - Oder „normale“ Anrufer werden mit positivem Wert markiert
- User Feedback kann in eigene SIP Nachricht oder in Header integriert werden
- Reputationswert des Anrufers wird bei Anruf signalisiert
- kann mit Grey Listing kombiniert werden:
  - Bessere Entscheidungsbasis

SPIT Abwehrmechnanismen Reputation Systems - Schwächen

- User mit negativen Ruf kann als global Black Listed betrachtet werden
  - Um wieder Anrufen zu können wird neuer Account benötigt
- Reputationswert als SIP Header kann gespooft werden (Direct IP SPIT)
- Ballot stuffing, Reputation Pushing:
  - Angreifer erstellt mehrere Accounts
  - Ruft sich gegenseitig an mit den Accounts
  - Gibt dabei positives Feedback

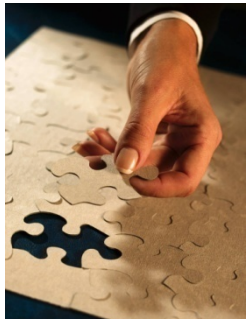
- Anwendungsschwächen:
  - Nur zukünftige Anrufe von Identitäten mit schlechtem Ruf werden geblockt
  - Identität muss erst oft genug markiert worden sein um geblockt werden zu können



SPIT Abwehrmechanismen
Turing Tests/Computational Puzzles

- Turing Tests: Anrufer bekommt eine Aufgabe, die
  - von einem Menschen leicht gelöst werden kann
  - von einer Maschine (Computer) schwer gelöst werden kann
- z.B. Audio CAPTCHA
  - IVR (Interactive voice response) System nimmt Anruf entegen
  - Fordert mit einer Aufgabe Anrufer heraus (z.B. Wählen Sie „123“)

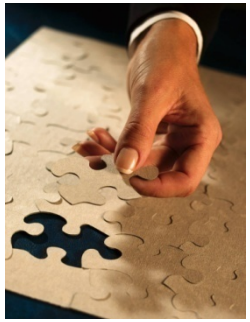
- Computational Puzzles:
  - User Agent (z.B. Telefon) des Anrufers muss eine Aufgabe lösen
  - z.B. das pre-image eines mit SHA1 gehashten Wertes finden
  - Ziel: CPU Kosten erhöhen



SPIT Abwehrmechanismen Turing Tests - Schwächen

- Audio CAPTCHA kann an einen Menschen weitergeleitet werden
- CAPTCHA Relay Attacke:
  - Wenn CAPTCHA erkannt wird, Anruf weiterleiten
  - Hilfsarbeiter lösen CAPTCHAs (Länder mit niedrigen Lohnkosten)
  - oder eine high traffic Seite aufsetzen (z.B. kostenfreie adult hotline) und leite CAPTCHA an Kunden weiter

- Anwendungsschwächen:
  - Sehr eingreifend, störend für „normale“ User
  - User Interaktion wird erzwungen (z.B. Jedes mal wenn Anrufer nicht in White List ist)



SPIT Abwehrmechanismen
Computational Puzzles - Schwächen

- Angreifer haben in der Regel starke Ressourcen (CPU Power)
- Es wird nichts weiter als CPU Rechenpower benötigt um Computational Puzzles zu umgehen

- Anwendungsschwächen:
  - „Normale“ Anrufer haben Telefone mit geringer Rechenleistung
  - Anrufverzögerungen zu Lasten „normaler“ Anrufer

SPIT Abwehrmechanismen Payments at risk

- Verlange Geld von unbekannten Anrufern
- Wenn User A User B anrufen möchte:
  - A zahlt geringen Betrag an B
  - Wenn B A als „normalen“ Anrufer klassifiziert wird der Betrag erstattet
  - ansonsten wir der Betrag nicht erstattet
- Ziel: Anrufkosten für SPIT Anrufer erhöhen
- Kombinierbar mit White List
  - Nur wenn User nicht in White List Payments at risk verlangen
- Kombinierbar mit Reputation System
  - Wenn Reputationswert sehr hoch erlaube anrufe
  - Wenn Reputationswert sehr niedrig blockiere Anrufe
  - Wenn wert im Mittelbereich verlange Payments at Risk

SPIT Abwehrmechanismen
Payments at risk - Schwächen

- Wenn kombiniert mit White List:
  - Auf selbe Weise wie White List umgehen
- Wenn kombiniert mit Reputation System:
  - Auf selbe Weise wie Reputation System umgehen
- Wenn Bezahlung bei jedem Anruf verlangt wird
  - SIP Identity Hijacking Attacke:
  - Angreifer gibt sich als jemand anderes aus
  - Kosten werden auf „normale“ User abgewälzt

- Anwendungsschwächen:
  - Relativ hohe Kosten für Micropayment Infrastruktur
  - Währungs Ungleichmäßigkeiten wenn Anrufteilnehmer aus verschiedenen Ländern

SPIT Abwehrmechanismen
Intrusion Detection Mechanisms

- Entdecke intrusives Verhalten innerhalb eines Systems:
  - Unterscheide „normale“ Anrufe und SPIT Anrufe anhand von Charakteristiken, wie z.B.:
    - Request Intensität
    - Fehler Response Intensität
    - Anzahl verscheidener Ziele
    - Anzahl Dialoge im Wartezustand
  - Annahme:
    - Intrusives Verhalten wird erkannt da es in diesen Variablen Unterschiede gibt

SPIT Abwehrmechanismen
Intrusion Detection Mechanisms - Schwächen

- Angreifer kann sich an Verhalten normaler User anpassen
- Call Rate Adaption Attacke:
  - Während der Attacke wird die Anrufrate variiert
  - z.B. zu Beginn 5 Anrufe pro Stunde dann hoch und runter variieren
- Account Switching Attacke:
  - Verschiedene Accounts benutzen und während des Angriffs wechseln
  - Statistische Werte können nicht über Accounts hinweg korreliert werden

- Anwendungsschwächen:
  - Grenzlinie zwischen normalem und intrusiven Verhalten muss präzise gesetzt werden
    - Andernfalls enstehen False Positive und False Negative Abweichungen
  - Statistische Werte sind bisher auf Vermutungen basiert und nicht verifziert

SPIT Abwehrmechanismen Honey Phones

- Können als Teil von Intrusion Detection Systems betrachtet werden
- Teil eines VoIP Netzwerks, dass nicht von „normalen“ Usern erreicht werden kann
  - z.B. Wenn Anrufer nicht vergebene Rufnummern wählt
  - this can be viewed as an attack
- Stark gegen Scan Attacken

SPIT Abwehrmechanismen
Honey Phones - Schwächen

- SIP Identity Hijacking ist effektiv gegen Honey Phones
- Angreifer nimmt Identität „normaler“ User an
- Annahme, dass Honey Phone nur von Angreifern erreicht wird ist somit verworfen

- Anwendungsschwächen:
  - Ein Angreifer, der bereits über Liste gültiger, vergebener Accounts verfügt greift nicht auf Honey Pot Teil des Netzwerkes zu

SPIT Abwehrmechanismen Zusammenfassung - Weaknesses

- Jeder Angreifer, der folgende Angriffe durchführen kann:
  - Device Spoofing
  - SIP Identity Spoofing
  - SIP Header Spoofing
  - Reputation Pushing oder Pulling, Ballot Stuffing
  - CAPTCHA Relay Attack
  - SIP Identity Hijacking
  - Call Rate Adaption
  - Account Switching
- kann präsentierte Abwehrmechanismen umgehen

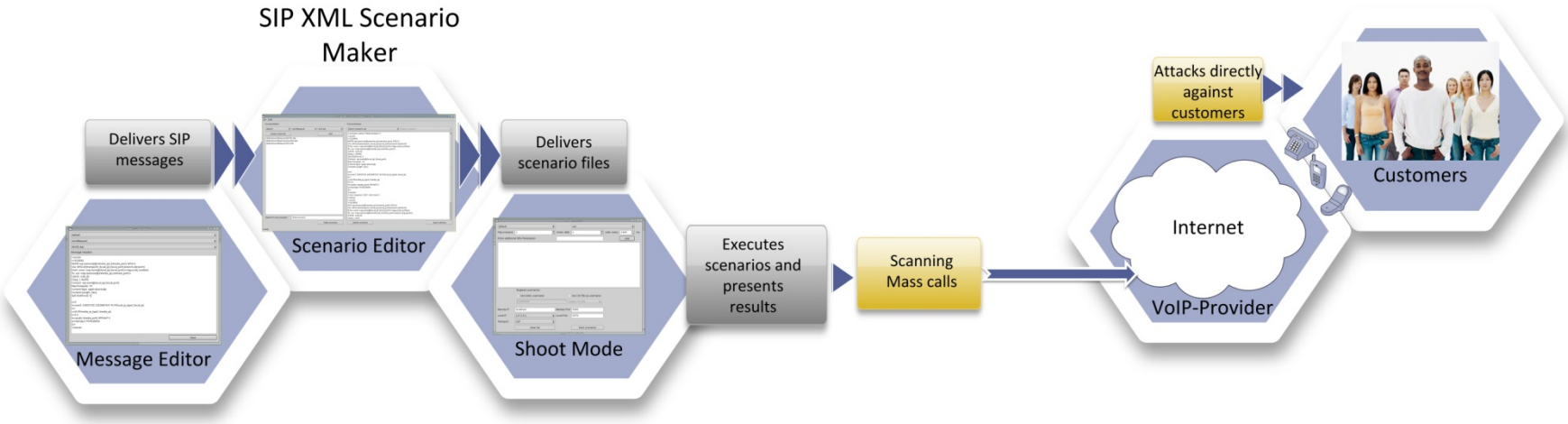
Abwehrmechanismen haben Schwächen!

Wie kann man sie in der Praxis ausnutzen?

SIP XML Scenario Maker

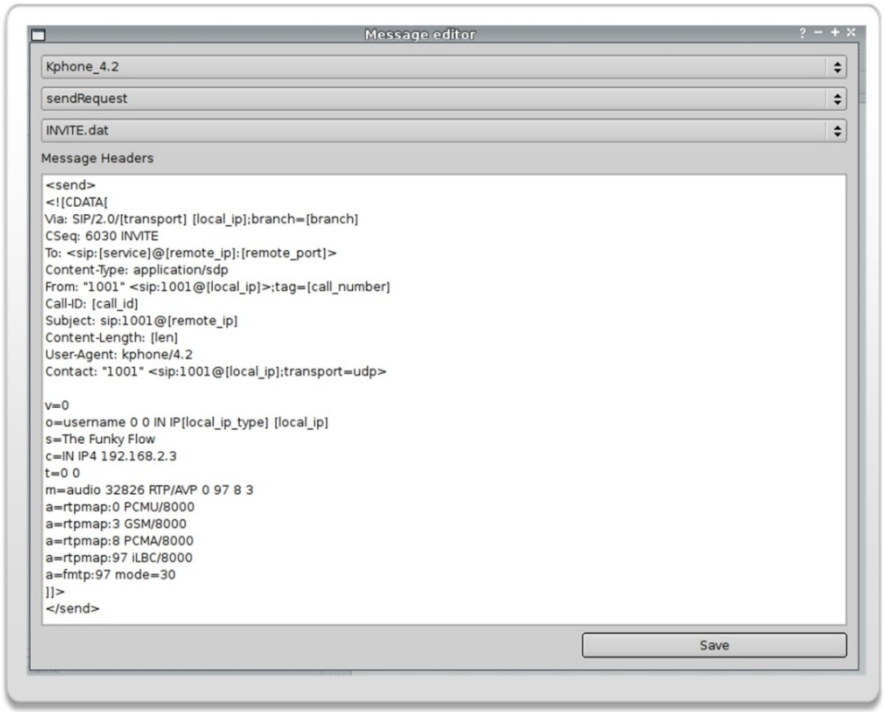
- Zunächst wird ein Werkzeug benötigt, dass Angriffe implementiert:
  - SIP XML Scenario Maker erweitert SIPp mit der Möglichkeit schnell
  - individulle SIP Szenarien mit einer GUI zu erstellen
  - Erstellte Szenarien auszuführen und Ergebnis auszuwerten mit Hilfe von
  - Zwei Editiermodi (Scenario Editor, Message Editor)
  - Einem Ausführungsmodus (Shoot Mode)

SIP XML Scenario Maker Workflow



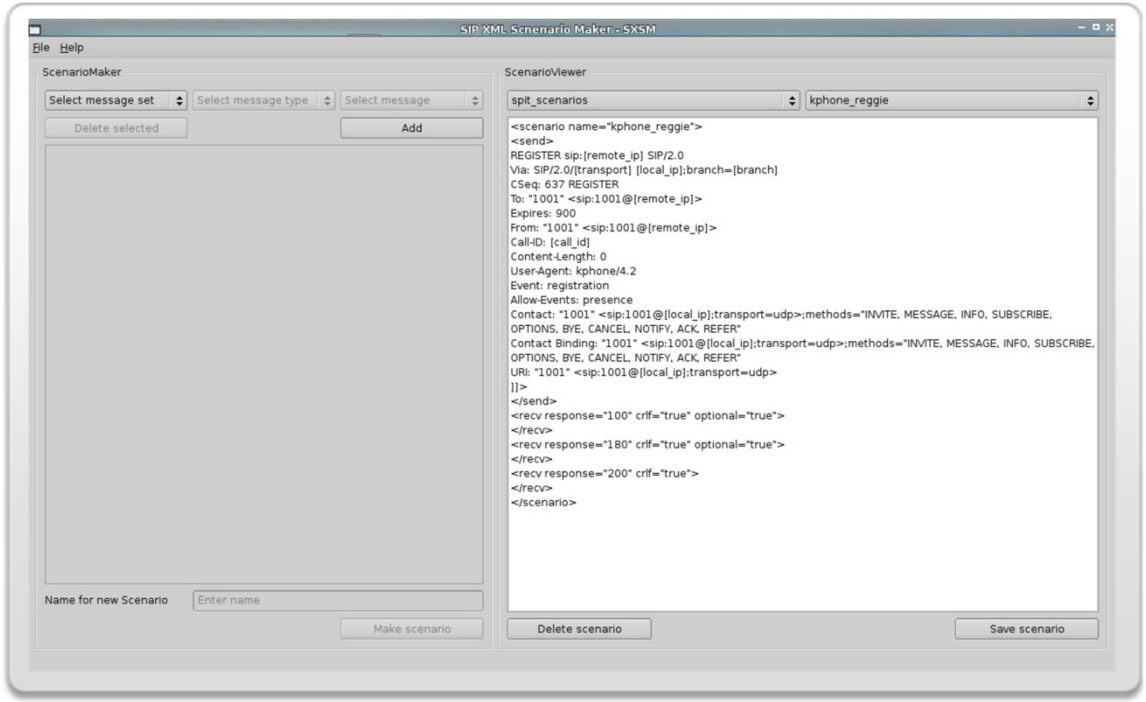
SXSM – Message Editor

- Individulle SIP Nachrichten erstellen
- Nachrichten in Sets und nach Typ verwalten



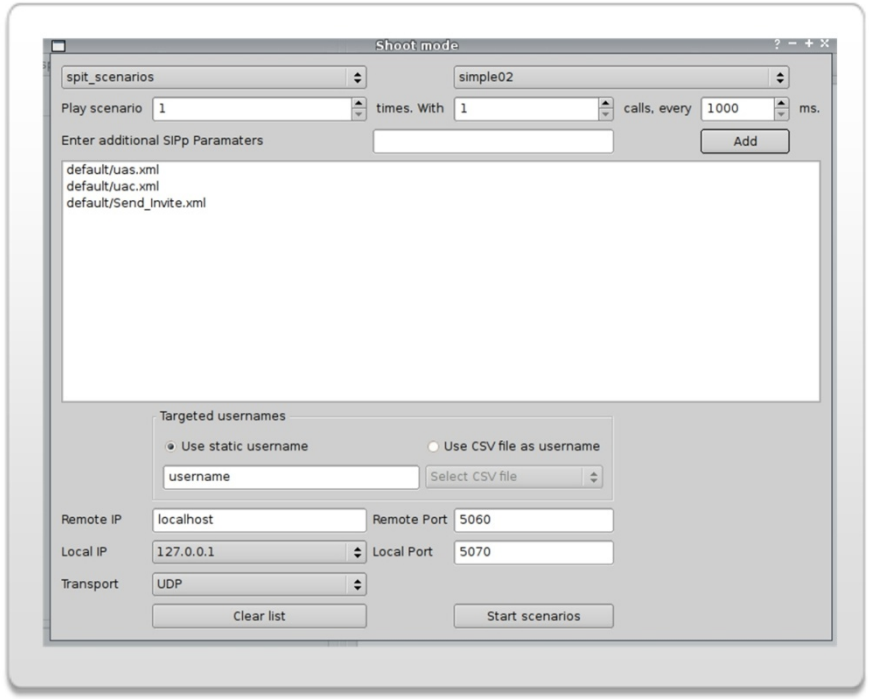
SXSM – Scenario Editor

- Sequenz von SIP Nachrichten als Szenario erstellen
- Komplexe SIP Szenarien mit wenigen Klicks erstellen



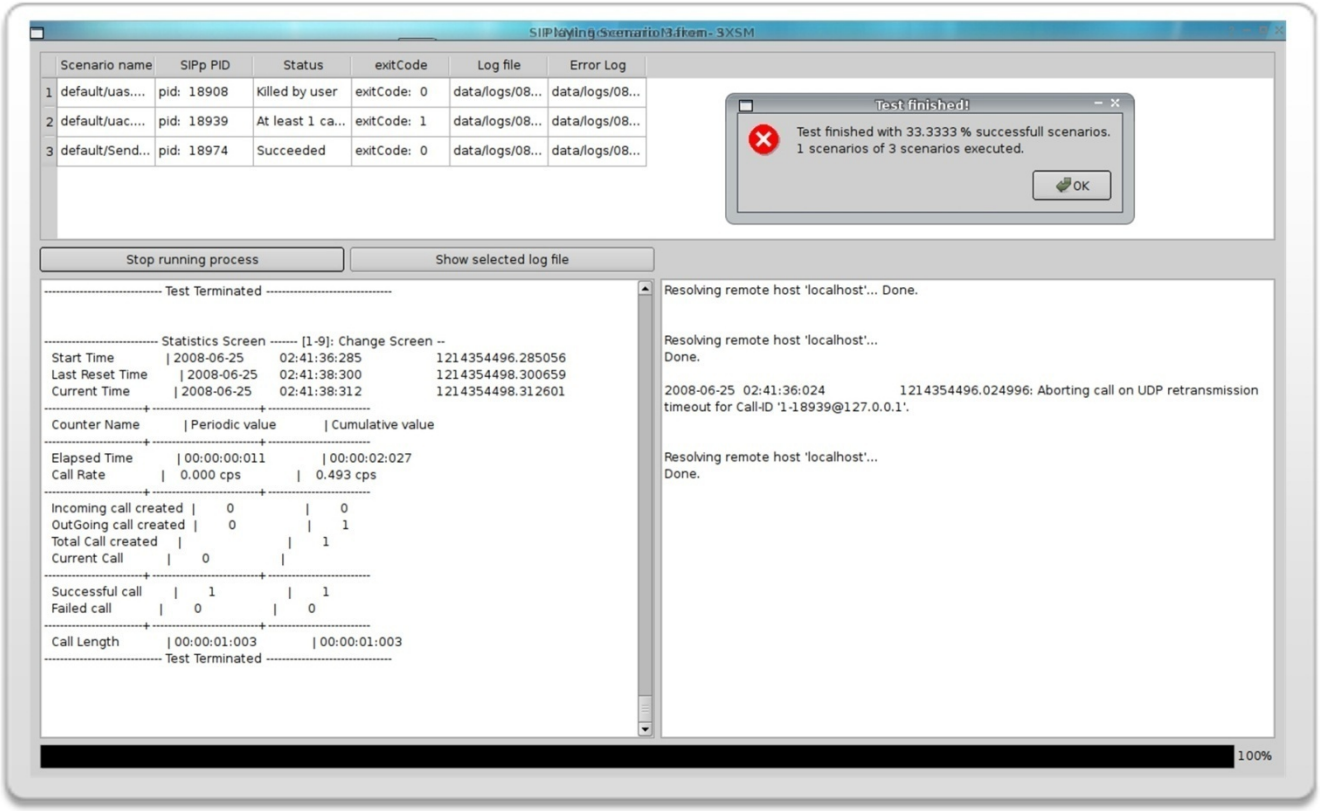
SXSM – Shoot Mode

- Erstellte Szenarien als Stapel ausführen
- Ausführungsparameter festlegen (Anrufrate, Ziele, …)

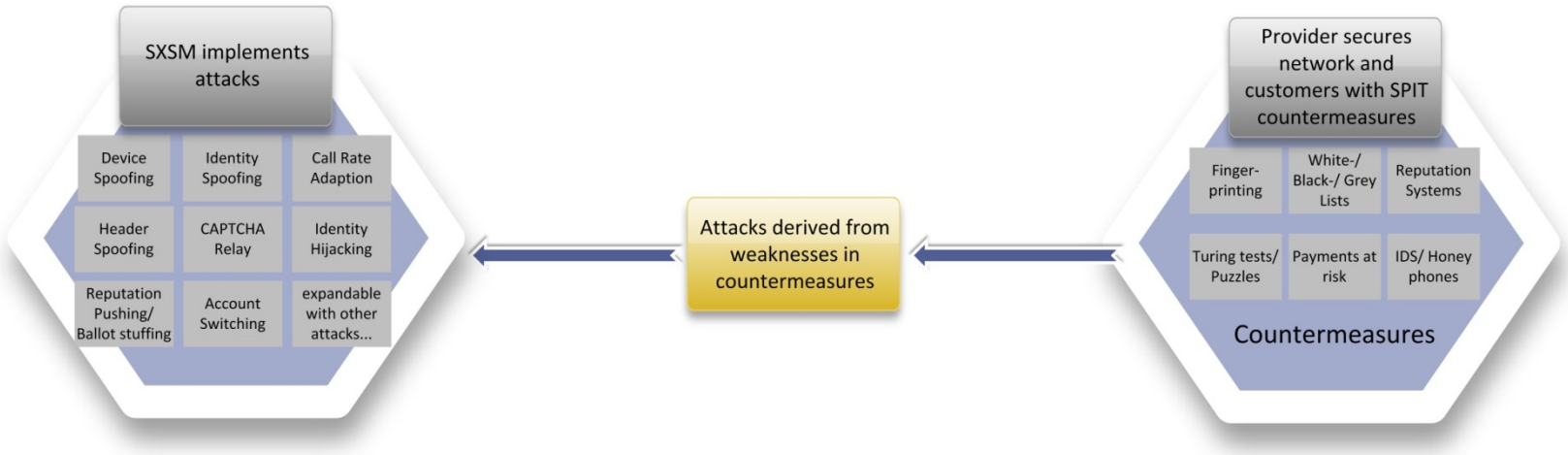


SXSM – Shoot Mode

- Ausgabe der Ausführung evaluieren
- Anzeige: Erfolgsrate (Anzahl erfolgreicher Anrufe) und Error Logs



SXSM – Angriffsimplementierung



SIP XML Scenario Maker
Device Spoofing

- Passives Device Spoofing
  - Analysiere Layout von SIP Nachrichten eines Standard Clients (z.B. KPhone)
  - Erstelle einen neuen Nachrichten Set im Message Editor für diesen Client
  - Erstelle eine SIP Nachricht mit genau dem gleichen Layout im Message Editor

- Aktives Device Spoofing
  - Analysiere Verhalten eines Standard Clients bei Challenges
  - Erstelle ein Szenario, dass alle unerwarteten Nachrichten abfängt
  - Schema: Wenn Nachricht X empfangen gehe zu Untersektion Y (Szenario mit Sprungmarken)

SIP XML Scenario Maker
SIP Identity Spoofing

- SIP Message Header im Message Editor ändern
  - Gewünschte Werte im „From“ und „Contact“ Header eintragen
- SIP Message Headers im detail view des Scenario Editors ändern
- Werte aus CSV Datei einspeisen
  - From: [field0 file=“caller.csv”] <sip:[field1 file=“caller.csv”]@[local ip]:[local port]>;
  - CSV Datei kann mehrere Accounts beinhalten

SIP XML Scenario Maker
SIP Header Spoofing

- Header Felder und ihre Werte können manipuliert werden
  - Im Message Editor
  - Im Scenario Editor

- Direct IP SPIT Scenario -> Header Felder und Werte beliebig
- SPIT via Proxy -> nur reguläre Werte

SIP XML Scenario Maker
Reputation Pushing/Ballot Stuffing

- Erstelle zwei Szenarien
  - Szenario 1 ruft mit der Identität an die manipuliert werden soll
  - Scenario 2 nimmt Anruf an, terminiert Anruf und sendet positives Feedback
  - Wiederhole Prozedur mit genug Identitäten für Szenario 2

SIP XML Scenario Maker CAPTCHA Relay Attack

- Third Party Call Control Feature von SXSM
- Erstelle ein Szenario, dass folgendes macht:
  - Rufe Opfer an
  - Rufe Human Solver an
  - Leite Opfer an Human Solver weiter
- Human Solver löst das CAPTCHA

SIP XML Scenario Maker
SIP Identity Hijacking

- Erstelle ein Szenario, das folgendes macht:

- Lege die Registrierung des Opfers lahm durch:
  - eine DoS Attacke gegen das Endgerät des Opfers oder
  - Deregistrierung des Opfers
  - Eine Registrierung Race-condition herbeirufen
    Angreifer sendet wiederholt 'REGISTER' Requests innerhalb kurzer Zeit (z.B. 15 Sekunden)

- Sende ein REGISTER Request mit der IP Adresse des Angreifers anstatt der legitimen

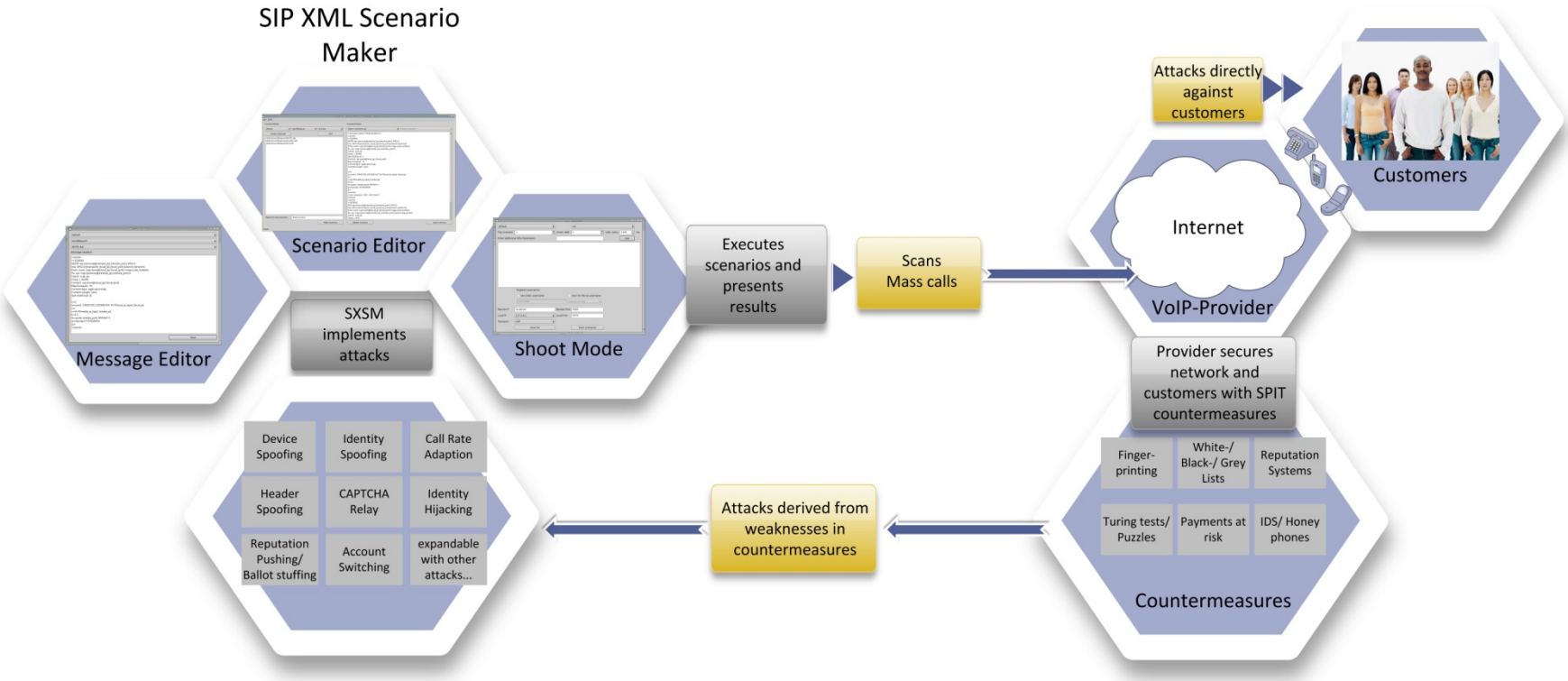
SIP XML Scenario Maker
Call Rate Adaption

- Anrufrate kann innerhalb des Shoot Modes gesetzt werden
- z.B. 100 Anrufe mit einer Rate von 10 Anrufen pro Minute
- Füge Szenario mehrere Male in die Shoot Liste
  - z.B. einmal mit 100 Anrufen pro Minute
  - Dann mit 50 Anrufen pro Minute
- Anrufrate kann wie gewünscht angepasst werden

SIP XML Scenario Maker Account Switching

- Benutze CSV Datei sowhl für Anrufer als auch für Ziel
- Anrufer kann im Message Editor gesetzt werden
- Ziel kann innerhalb des Shoot Modes gesetzt werden
- z.B. 10 Identitäten in caller.csv und 100 in callee.csv
- Während des Angriffs werden die Identitäten automatisch gewechselt

SIP XML Scenario Maker Überblick



Fazit

- SPIT Problem wurde genau klassifiziert
- Vorhandene Abwehrmechanismen wurden vorgestellt
- Schwachpunkte wurden erfasst
- Auf Protokollebene wurden Schwachpunkte für systematische Angriffe ausgenutzt

Vielen Dank für die Aufmerksamkeit!

Fragen?