

Netzicherheit – Architekturen und Protokolle SPAM & SPIT



Einführung

- "The SMTP design is based on the following model of communication: as the result of a user mail request, the sender-SMTP establishes a two-way transmission channel to a receiver-SMTP. The receiver-SMTP may be either the ultimate destination or an intermediate." [RFC 821]
 - Keine Identifizierung des Absenders
 - Keine Kosten
- **SPAM**
 - Unsolicited Bulk E-Mail, Unsolicited Commercial E-Mail
 - Collateral spam
 - Usenet-Spam, Index-, Link-, Blog- und Wikispam
- Problem: Mail-Provider darf keine (SPAM-)Mails ausfiltern

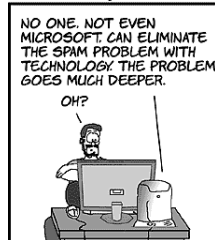
1



Was ist das Problem?

- Gewünscht, dass von unbekannten Personen Nachrichten versandt werden
- Diskussion: Ende-zu-Ende Authentifizierung
- Geschäftsmodell
 - Versenden einer E-Mail billig
 - Geringe Erfolgsrate genügt

USER FRIENDLY by J.D. "Illiad" Frazer



THE PROBLEM LIES IN THE FACT THAT SPAMMING REMAINS PROFITABLE, AND THAT'S BECAUSE PEOPLE STILL CLICK ON SPAM LINKS.



SO THE SOLUTION IS TO... UH...ELIMINATE PEOPLE? SEE, THAT'S WHY YOU GET THE BIG BUCKS...



2



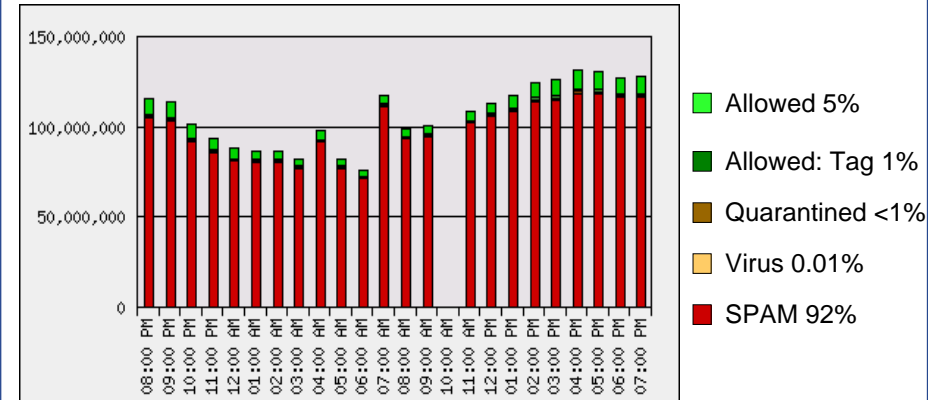
SPAM Erzeugung

- **Webmail**
 - Bots erzeugen ein Vielzahl von Benutzer-Konten
 - Captchas werden durch Social-Engineering umgangen
- **Open Mail Relay**
 - SMTP-Server schicken E-Mails von jedem an jedem
 - Lösung: Eintrag in DNSBL (DNS black list)
- **Open Proxy**
 - Vermittlung von Verbindungen von jeden Rechner an jeden Server
 - Vorteil für den Spammer: Verschleierung der Verbindung
 - Lösung: Eintrag in DNSBL (DNS black list)

3

- Feedback Forms
 - CGI Scripts konnten missbraucht werden, um an beliebige Adressaten E-Mails zu verschicken
- Spammer Virus
 - Sobig oder Mmail
 - Installation von Spam Werkzeuge auf PCs
 - ▶ Versand von SPAM
 - ▶ Address Harvester
 - ▶ DDoS Angriffe auf DNSBLs

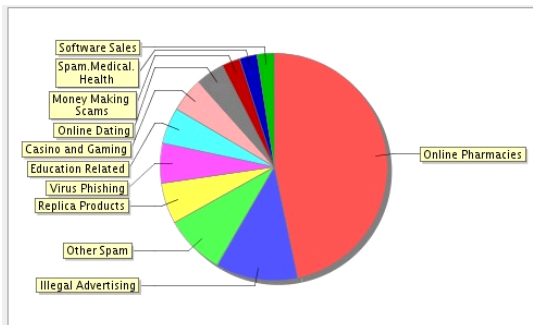
4



Von <http://www.barracudacentral.com/index.cgi?p=spam>

Stand: 03.04.2008

5



Von <http://www.barracudacentral.org/data/spam>

Stand: 20.04.2009

| Country | Percent of Total Spam |
|---------------|-----------------------|
| United States | 23.58% |
| Brazil | 6.77% |
| Russia | 5.66% |
| Canada | 4.69% |
| Turkey | 4.24% |
| Netherlands | 3.77% |
| Germany | 3.52% |
| China | 3.38% |
| UK | 2.48% |
| Poland | 2.25% |

6

- Domain Keys
 - Mail-Provider führt „strenge“ Identifizierung der Benutzer durch
 - Mail-Provider fügt Signatur ein
 - Vertrauen der Mail-Provider untereinander
- Sender Policy Framework
 - Neuer DNS-Eintrag SPF: definiert autorisierte Domäne für einen SMTP-Sender
 - Empfangender SMTP-Server prüft ob E-Mail Adresse aus autorisierte Domäne stammt

7

• Domain Keys

- Jeder Mail-Provider führt „strenge“ Identifizierung der Benutzer durch
- Vertrauen **aller** Mail-Provider untereinander
- Trojaner auf Endsystemen, Impersonifizierung
- Angreifer registriert Mail-Account, Domains, ...

• Sender Policy Framework

- Weiterleitung von E-Mails problematisch
- Keine direkte SMTP-Verbindung zu externen SMTP-Servern möglich, z.B. für private E-Mail
 - ▶ Lösung: SMTP submission
- Kein Schutz vor „Einweg“-Domains
 - ▶ Mehrzahl der Spammer-Domains enthält korrekten SPF Eintrag

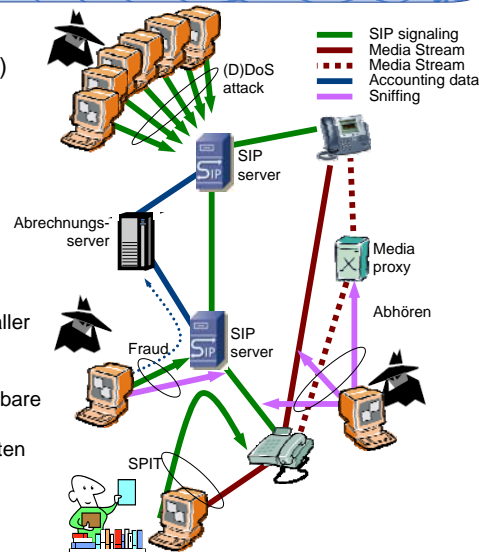
8

Übertragen Sie das Spam-Konzept auf andere Kommunikationsformen?

- Welche Voraussetzungen müssen erfüllt sein?
- Technische Herausforderungen
- Reichweite

9

- **Social attacks**
(SPam over Internet Telephony, SPIT)
 - Störung und Unterbrechung der Arbeit durch ungewollte Anrufe
- **Interruption of Service (DoS)**
 - Angriffe auf die Infrastruktur oder Endgeräte
- **Abhören und Modifikation**
 - Fehlende Vertraulichkeit der Kommunikation
 - Fehlende Integrität der Signalisierung
 - Offenlegung privater Informationen (caller ID, DTMF password/accounts, etc.)
- **Missbrauch der Dienste (Fraud)**
 - Nicht-Autorisierte oder Nicht-abrechenbare Ressourcen Nutzung
 - Impersonifizierung, gefälschte Identitäten



10

• Vergleichbar mit E-Mail SPAM

- Großteil des E-Mail-Verkehrs ist SPAM
- Entwickelt sich VoIP ähnlich, werden die meisten VoIP-Anrufe SPIT sein
 - ▶ Dauerklingeln des Telefons

• Konsequenzen gravierender als bei SPAM

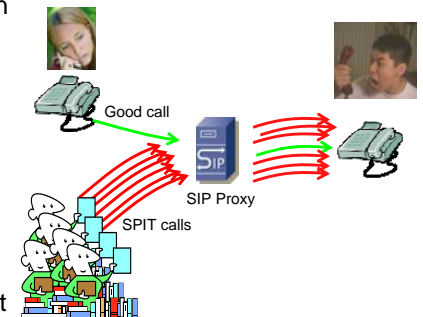
- Anruf stört den Benutzer sofort

• Email Spam Filter-Techniken nicht anwendbar

- SPIT ist Echtzeit
- Vorfilterung anhand des Inhalts nicht möglich

• Innovation notwendig

- Entwicklung neuer SPIT-blocking Methoden



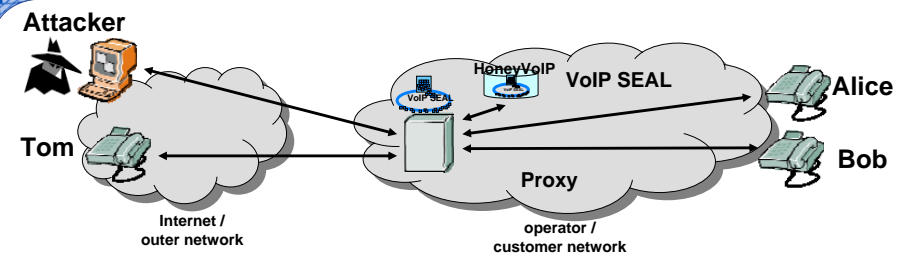
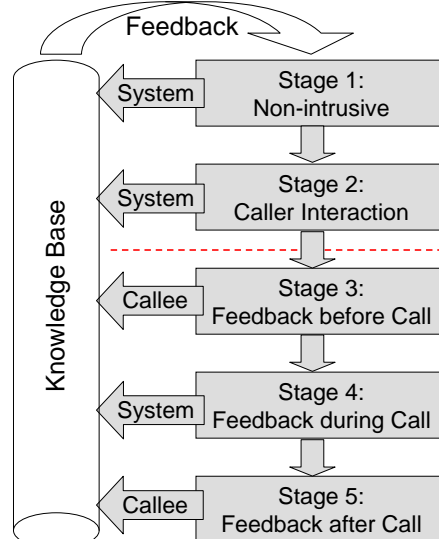
11

| SPAM | SPIT |
|---|---|
| Asynchrone Übertragung | Echtzeit-Kommunikation |
| Speicherung bis Abruf | Sofortige Auslieferung: Klingeln |
| Inhaltsanalyse vor Auslieferung | Inhaltsanalyse erst möglich nachdem der Empfänger bereits gestört wurde |
| Text-Analyse einfach | Sprach-Analyse sehr aufwendig |
| Einfache, schnelle und kostengünstige Erzeugung durch Bot-Netze | Einfache, schnelle und kostengünstige Erzeugung durch Bot-Netze |
| Benutzt für Marketing und Betrug | Kann für Marketing oder Betrug genutzt werden |
| Beherrscht den E-Mail-Verkehr, belästigt Benutzer, erzeugt Kosten und verringert die Produktivität weltweit | Wird hoffentlich nicht den VoIP-Verkehr beherrschen |

- **Annahmen**
 - Angriffe werden sich ähnlich entwickeln, wie Viren, Würmer und Trojaner in den letzten Jahren
 - SPIT wird eine erheblich Gefahr für SIP darstellen
- **Anforderungen**
 - Flexibler Schutz
 - Verschlüsselung und Authentifizierung reicht nicht aus
 - Schutz kann nicht auf einer einzigen Methode beruhen
- **NEC Solution: VoIP SEAL™: VoIP Secure Application Level Firewall**
 - SPIT Erkennung und Vermeidung
 - ▶ Modulare und erweiterbare Plattform
 - ▶ Kooperation verschiedener Schutzmodule
 - ▶ On-line plug-and-play Integration neuer Module
 - ▶ On-line Konfiguration der Module
 - ▶ On-line Update

SPIT Erkennung

1. Klassifizierung des Anrufers
 - Black- & Whitelist
2. Interaction mit Anrufer
 - Turing Test
3. Angerufene gibt Feedback vor dem Anruf
 - Signalisierung
4. Angerufener gibt Feedback während des Anrufs
 - Spezieller Auflegeknopf
5. Angerufener gibt Feedback nach dem Anruf
 - Service Nummer



- **VoIP SEAL (basic)**
 - Schutz des SIP-Betreiber Netzwerks
 - ▶ (D)DoS attacks
 - ▶ Nachrichten mit Formatfehlern
 - ▶ Unauthorisierte Nachrichten
 - Global-blacklist
 - Umleitung unbekannten Verkehrs für weitere Analyse
 - ▶ HoneyVoIP
- **VoIP SEAL (advanced)**
 - Personalisierung
 - ▶ Einstellungen und Profile
 - Erkennung von Angriffen anhand Benutzervorgaben
 - ▶ Personal-black&white list
 - ▶ Touringtests
 - ▶ DTMF check
 - ▶ Greylisting

- [2.1] **“Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1”**, M. Wong , W. Schlitt , RFC 4408
- [2.2] **“DomainKeys Identified Mail (DKIM) Signatures”**, E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, RFC 4870
- [2.3] **“SPam over Internet Telephony (SPIT) Prevention Framework”**, R. Schlegel, S. Niccolini, S. Tartarelli; M. Brunner; Global Telecommunications Conference, 2006. GLOBECOM'06. Nov. 2006 Page(s):1 - 6