Lo spam via Voip e metodi di prevenzione tramite Web of Trust

Marco Cornolti

Seminario per TIP, 19 maggio 2009

Lo SPam over Internet Telephony (SPIT)

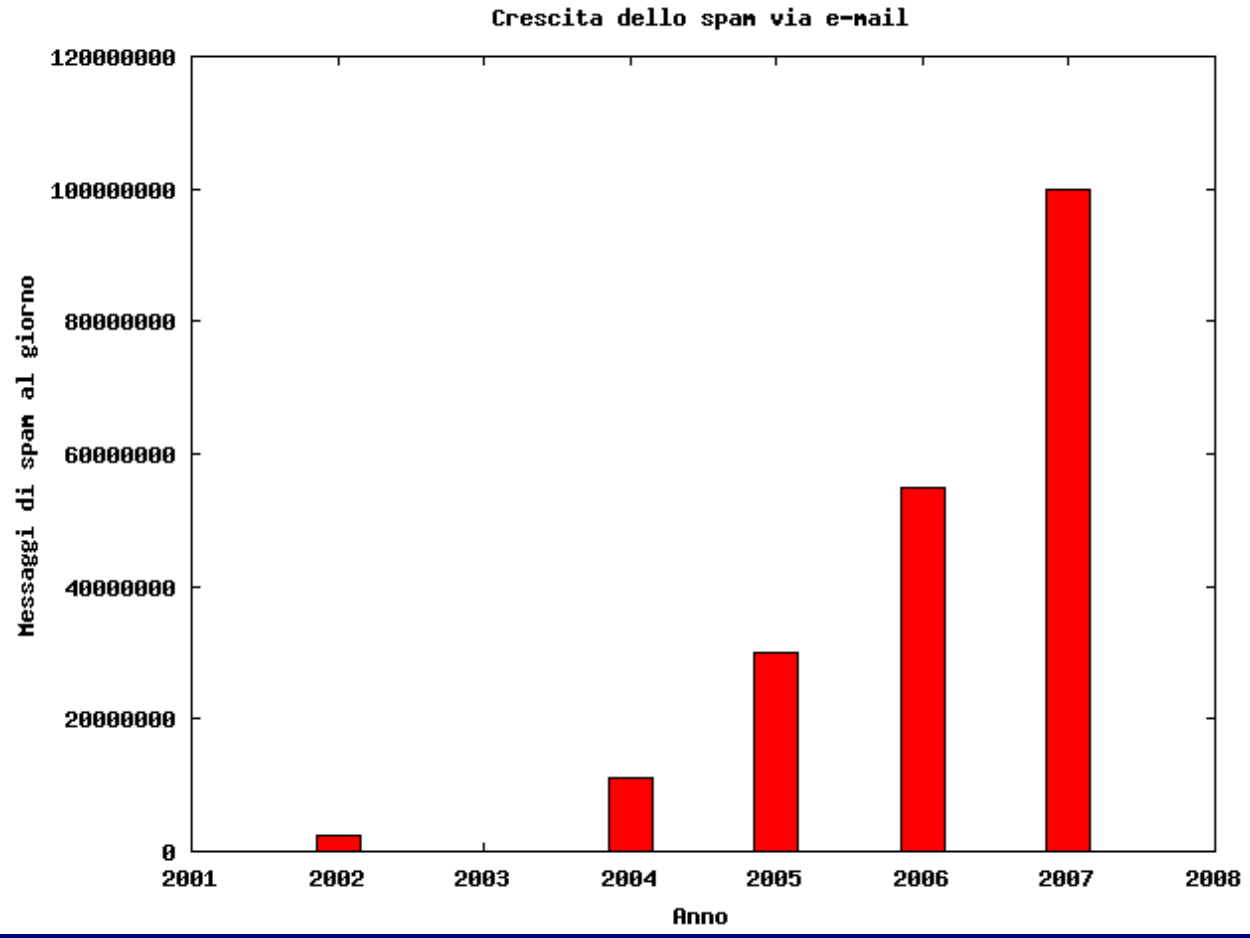
- Telefonate non richieste
- Puo' creare piu' danni al voip di quanto lo spam ne abbia provocato all'e-mail
- Fenomeno per ora inesistente
- Prendiamo in considerazione solamente SIP

Spam via e-mail

- Ha molti tratti in comune con lo SPIT
- Problema di progettazione in SMTP
  - Che non prevede alcuna forma di autenticazione del mittente
  - Difficilmente estendibile (caso DomainKeys)
  - L'eterogeneita' dei sistemi SMTP e' la forza e la debolezza

Spam via e-mail - proporzioni

- Nel 2002, 2,4 miliardi di messaggi al giorno, crescita esponenziale



Tipi di spam via e-mail

- Pubblicita'
- Phishing
- Advance-fee scam
- Diffusione Virus
  - W32.Sobig.F@mm Ha infettato milioni di computer
- ecc

Come funziona lo spam via e-mail

- Invio dei messaggi
  - 5kb l'uno (diciamo 8kb=64kbit tra overhead di tutti i protocolli), un'adsl a 640kbit/sec ne puo' spedire 10 msg/sec (~1m in 24h)
  - Una T3 (44.736 Mbit/sec) porta 700 msg/sec (~60m in 24h)
- Problema acquisizione indirizzi
  - Crawler
  - Virus

Punti a favore dello spam

- Basso costo trasferimento dati via Internet
- Alta velocita' dei dati
- Difficolta' di scoprire la fonte fisica dello spam
- Relativa facilita' di trovare fonte fisica dello spam
- Automazione del processo
- Ad ogni modo:
  spam esiste => c'e' del guadagno

SPIT mantiene le proprieta' di convenienza

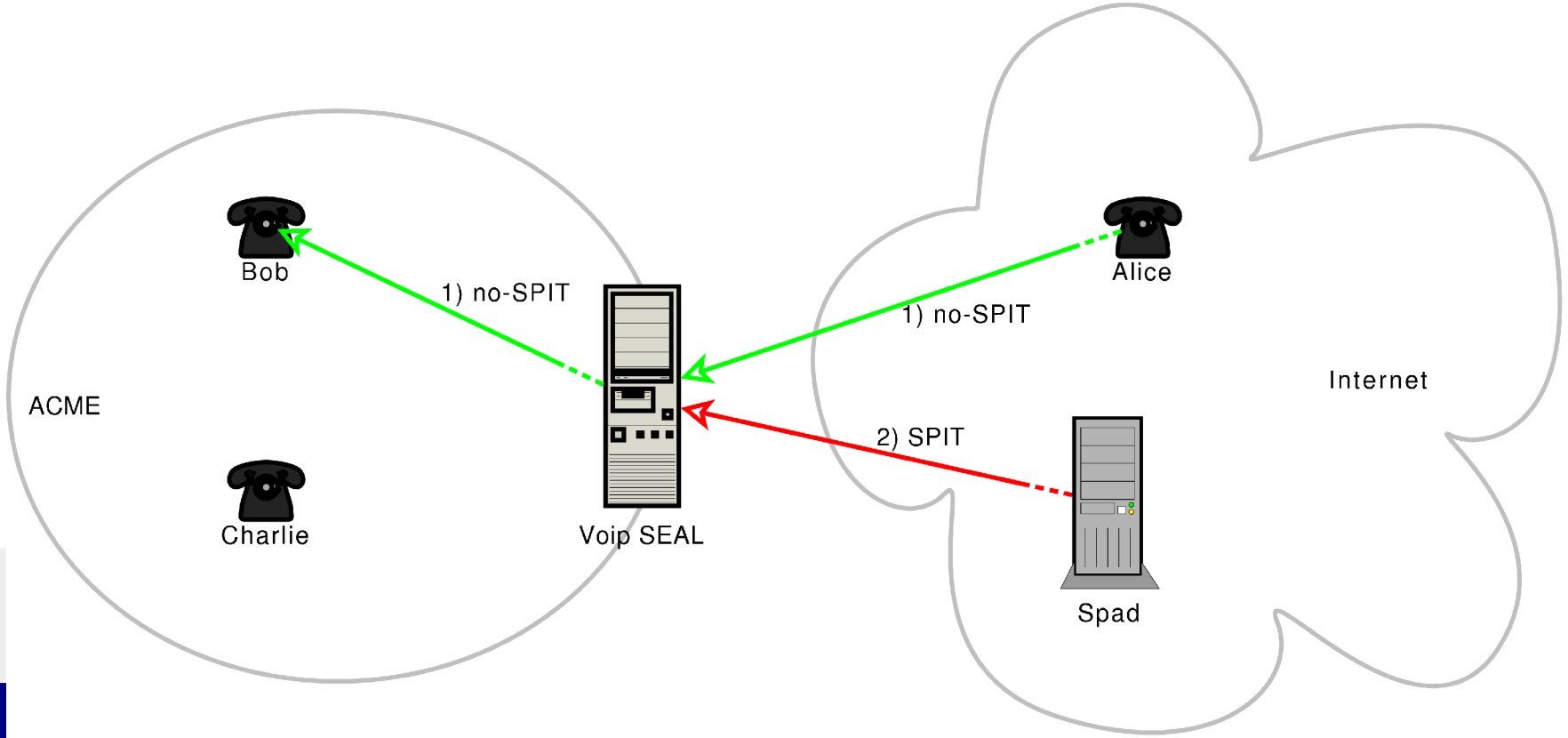
- Invio dei messaggi:
  G729 (8kbit/sec + 8kbit/sec di overhead). Da un'adsl a 640kbit/sec e' possibile inviare 40 telefonate contemporanee.
- Acquisizione degli indirizzi:
  Ancora piu' semplice. Per retro-compatibilita' con PSTN, gli indirizzi sono numerici e tipicamente assegnati in modo progressivo
- Automazione resta possibile; nascondere la fonte fisica anche

Differenze tra SPIT e e-mail spam

- SPIT e' sincrona, Spam e' asincrona
  - Impossibile l'analisi di un messaggio

Il sistema anti-SPIT Voip SEAL

- Presentato nel febbraio 2007 al 3GSM World Congress da NEC Network Lab Europe
- Difesa perimetrale (indipendente dai terminali)



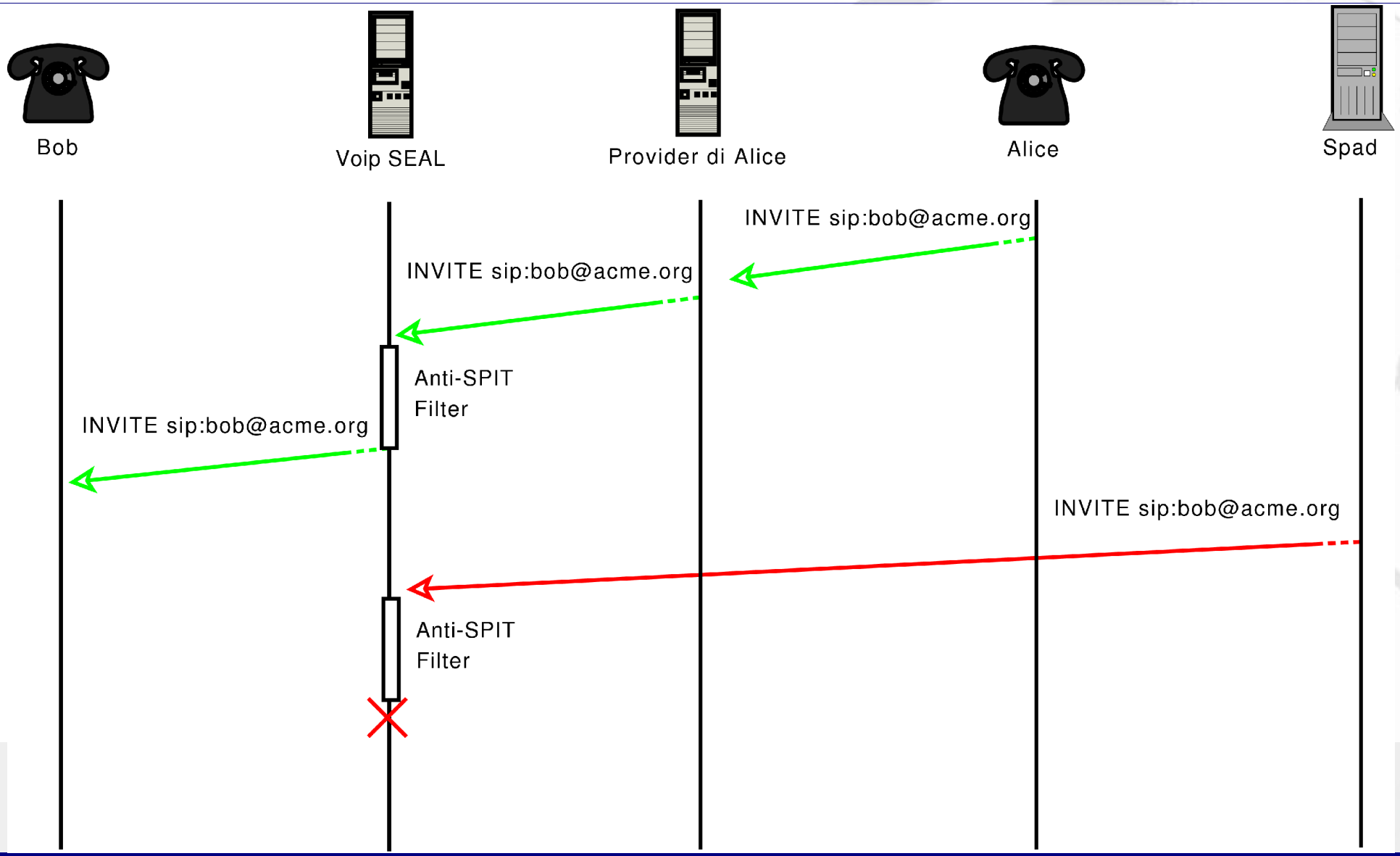
Voip SEAL - Elementi chiave

- Minimizzare le telefonate legittime scartate
- Minimizzare le telefonate illegittime che fanno squillare il telefono destinatario
- E' preferibile appesantire il sistema con calcoli piuttosto che chiedere l'interazione umana
- Nel caso di necessita' dell'interazione dell'utente, si preferisce appesantire il chiamante
- Tutto cio' in tempo reale!

Voip SEAL – Test e Stage

- Ogni test restituisce un punteggio [-1, 1]
- Organizzazione in Stage successivi:
  - Stage 1: test non-intrusivi (es. WoT, blacklist)
  - Stage 2: interazione della persona chiamante (turing test)
  - Stage 3: interazione della persona chiamata, prima che la telefonata venga stabilita.
  - Stage 4: durante la telefonata.
  - Stage 5: feedback dalla persona chiamata per potenziare la knowledge base del sistema.

Voip SEAL – Scambio di messaggi



Voip SEAL – Un po' di test - 1/3

- Black/Whitelist (Stage 1)
  - Semplice, anche computazionalmente
  - BL facilmente aggirabili generando indirizzi fasulli, WL troppo statica
- Turing Test (Stage 2)
  - Comporre una sequenza di numeri stile CAPTCHA
  - Invio segnale «attendere in linea mentre la chiamata viene inoltrata»

Voip SEAL – Un po' di test - 2/3

- Comunicazione basata sul consenso (Stage 3)
  - ~ lista dei contatti di skype
  - Troppo rigido
- Filtro sui contenuti (Stage 4)
  - Ricerca di pattern di SPIT
  - Computazionalmente costosi
  - Molti falsi positivi/negativi

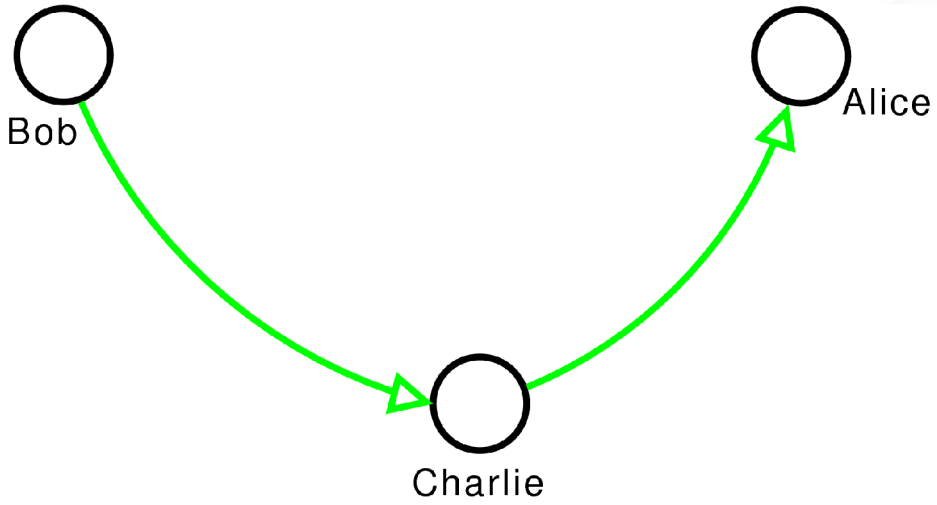
Voip SEAL – Un po' di test - 3/3

- Sistema di reputazione (Stage 5)
  - Al termine della chiamata, il destinatario da un giudizio sull'affidabilita' del mittente.
  - Serve solo a migliorare la KB usata dai test dello Stage 1
  - E' necessaria un'associazione solida tra indirizzo SIP mittente e persona fisica (altrimenti crolla il sistema di reputazione)
- Tutti questi test possono essere dislocati sul server anti-SPIT, no hardware particolare.

La Web of Trust di OpenPGP

- PGP introduce il concetto di firma
- Problema di PGP: scambiare in modo sicuro la chiave pubblica, e attribuire ad essa la corrispondenza con una persona fisica
- Per questo nasce la WoT
  - Rete che contiene le chiavi PGP e le relazioni di fiducia tra queste chiavu

WoT: esempio



- Es: Bob si puo' fidare di Alice tramite Charlie (esiste un Trust Path lungo 2 passi di fiducia da Bob ad Alice)
- La WoT e' un grafo orientato: Bob si fida di Alice, ma Alice non si fida di Bob

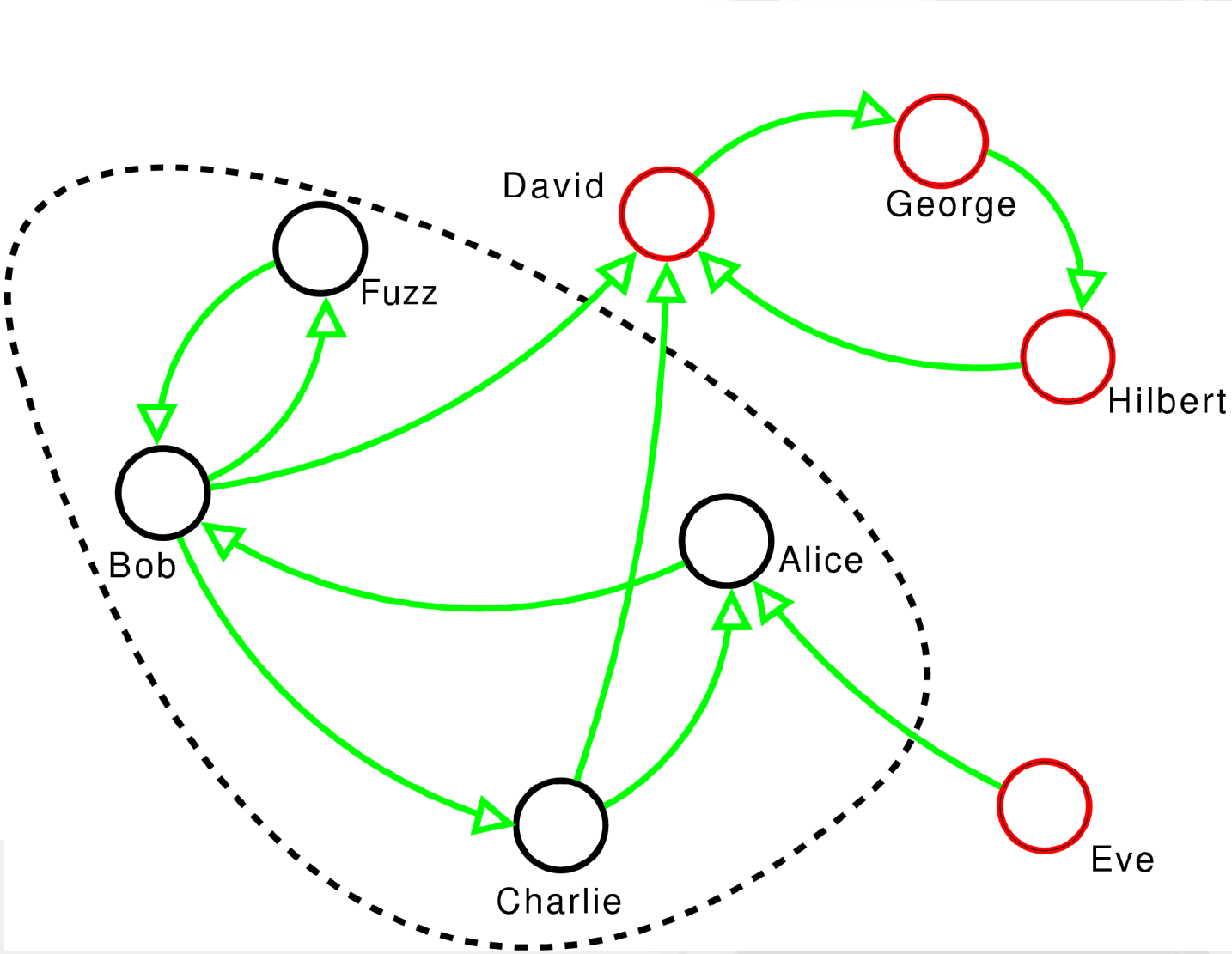
La WoT contro lo SPIT

- Gli elementi della WoT sono indirizzi SIP
- I messaggi di INVITE sono firmati
- All'arrivo di una chiamata, il server anti-SPIT cerca un percorso di fiducia dal destinatario al mittente

SIP Signed message

- INVITE sip:500@ekiga.net SIP/2.0
  Date: Tue, 19 May 2009 07:20:20 GMT
  CSeq: 1 INVITE
  Via: SIP/2.0/UDP
  192.168.100.184:5061;branch=z9hG4bKc0da292e-b342-de11-805c-000e35b7383e;rport
  From: "Alice" <sip:alice@xavier.org>;tag=b4bb1d2e-b342-de11-805c-000e35b7383e
  Call-ID: d4af1d2e-b342-de11-805c-000e35b7383e@makita
  To: <sip:bob@acme.com>
  Authentication:iEYEARECAAYFAkoSXoQACgkQzCa5QmSKyRGpwgCbBoI0HI4FXTLezl4FfS4KOurnEgoAoIeaUI57BgGxLFzQamLqzmyCARCf=kLWQ
  Contact: <sip:alice@xavier.org:5061;transport=udp>
  Content-Type: application/sdp
  Content-Length: 393
  Max-Forwards: 70
  [...]

Un altro esempio di WoT



WoT e Whitelist

- In pratica, WoT e' una Whitelist dinamica che usa anche l'informazione sulla fiducia di altre persone, per cui e' molto piu' potente:
  - Se, di media, un'identita' esprime fiducia in altre *m* identita', il numero di indirizzi SIP raggiungibili da tutti i path di lunghezza *l* sara' *r=m^l*
  - Ovvero, potenzialmente WoT raggiunge molte piu' persone di una Whitelist
  - WoT, come WL, da' solo giudizi positivi o incerti (deve essere combinato con altri test)

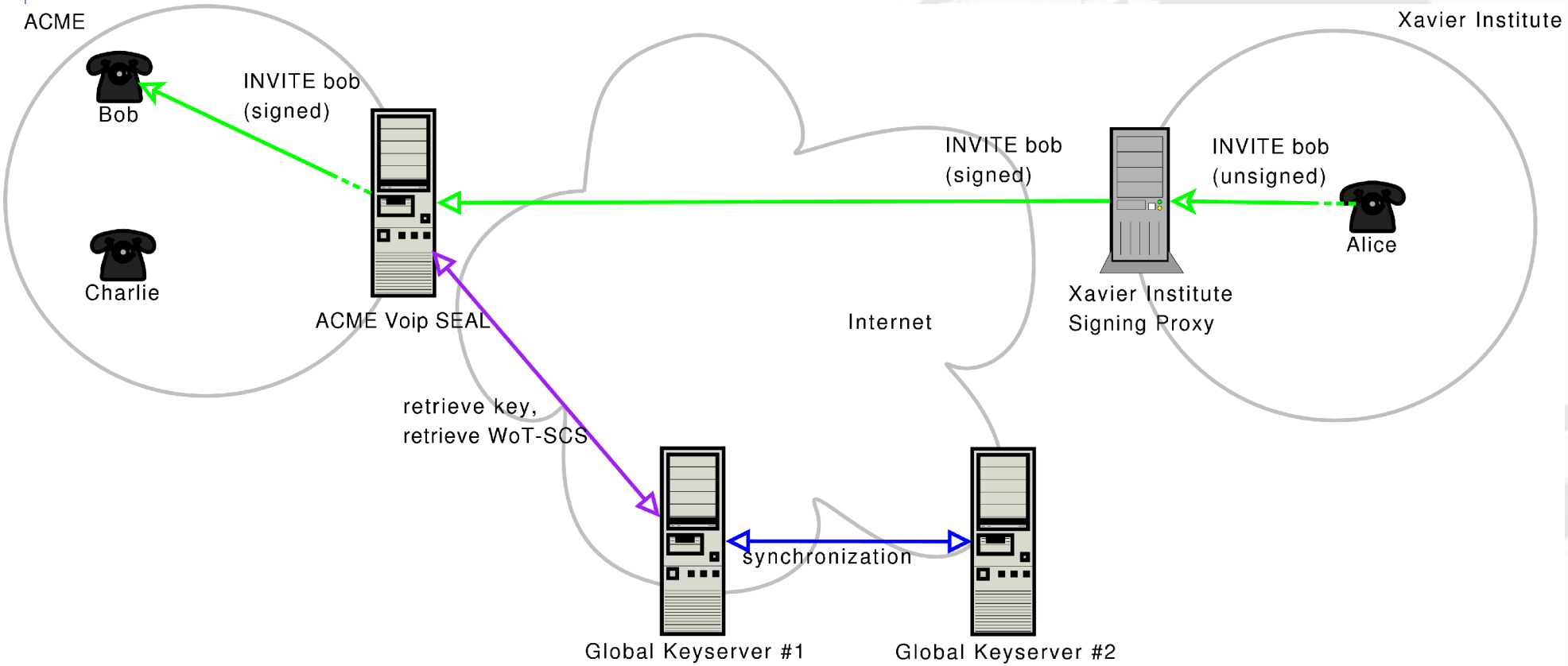
La lunghezza dei Trust Path

- Small World Experiment: ogni persona puo' raggiungere in 6 passi di amicizia qualunque persona sulla terra
- Come visto, numero di persone raggiungibili nella WoT e' exp. rispetto alla lunghezza del TP
- Non basta che esista un TP, la lunghezza del TP minimo dal destinatario al mittente della chiamata determina il livello di fiducia.

Deployment di WoT

- Terminali non fanno niente: necessita' di un'infrastruttura che apponga le firme al messaggio: Signing Proxy
- SP deve essere certo dell'identita' del chiamante: SIP supporta autenticazione
- Il modulo WoT ha bisogno nella propria KB della WoT, la cui generazione non e' un sistema banale
- C'e' bisogno di Keyserver per le k pubbliche

Deployment di WoT – schema



Sicurezza e Privacy

- Chiavi private concentrate nel SP: un problema?
- Pubblicazione delle relazioni di fiducia: un problema?

Come si costruisce la WoT

- Non ha senso usare la WoT di PGP (problema semantico)
- Necessario un metodo perche' gli utenti possano esprimere la fiducia
  - Vincolo: niente HW particolare (altrimenti, basterebbe un bottone)
  - Inserimento con interfaccia Web/audio
  - Inserimento automatico per telefonate > 5 minuti