XConnect

SPIT Prevention

September 23, 2008

XConnect

Spam over Internet Telephony (SPIT)

- The Threat of SPIT
- Solution Space
- The SPAM Score approach
  - Acme and XConnect test joint approach

XConnect

The Threat - Overview

- Bulk unsolicited communications are seen as largest threat to open IP communication

- With Email we “missed the boat”

With VoIP There is still a chance to deploy ubiquitous solutions before problem becomes widespread

XConnect

The Threat - Definition

- Defined as the transmission of bulk unsolicited…
  - SPAM – email
  - SPIM – **I**nstant **M**essages or presence requests
  - SPIT – **I**nternet **T**elephony call attempts
  - SPIDEO – Vi**deo** calls

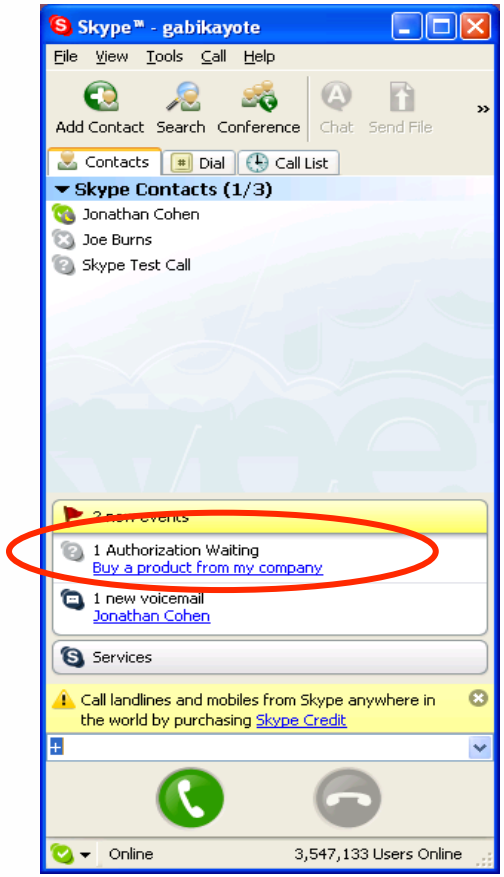
XConnect

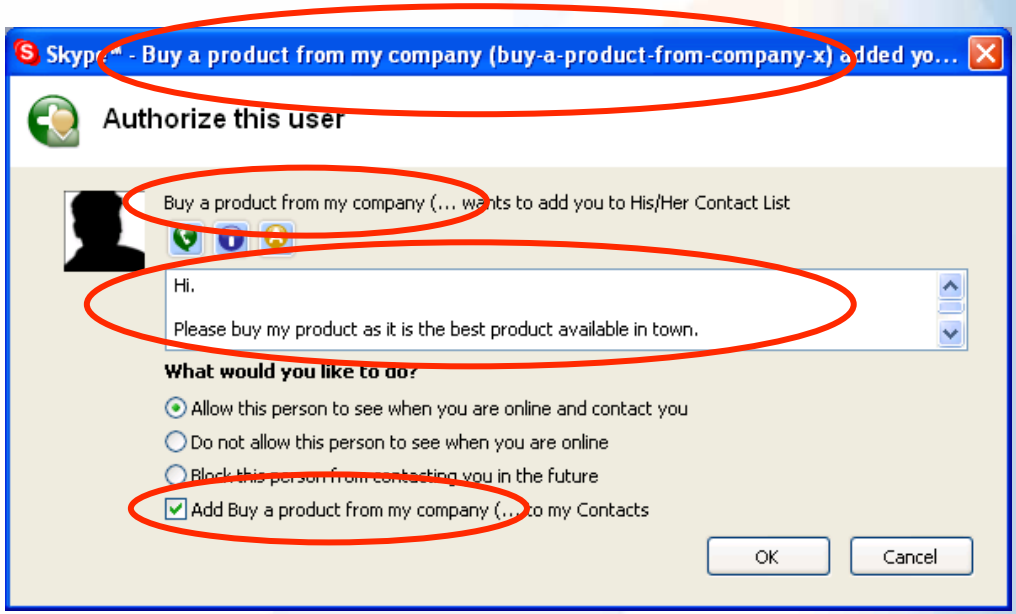
The Threat - How do they get my number?

- SPAM bots scour the web
  - email addresses appearing on a web page
  - Screen scraping
- Trial and error
  - Not so complicated with email addresses
    - Reuse existing email namespace for VoIP spam
  - Trivial with “virtual” phone numbers
    - Finite number space

XConnect

The Threat - IM/Presence Example





XConnect

The Threat - Is the threat real?

- It occurs in the existing telephone network
  - 18M telemarketing calls are generated daily*
- It occurs on the internet (email)
  - In 2004, 12.4B SPAM messages/day**

* http://www.privacycorps.com/pages/telemarketing-faq.htm.

** http://www.cybercity.com/business-email-content-filtering.asp

The difference is cost

XConnect

SPAM Cost Analysis Comparison

- one call at a time
- T1/T3 needed for large volume
- T1 line:
  - approximately US $250/month
  - about 1.5 ¢/minute for calls
  - at most 24 simultaneous calls
- Assuming about 10s/call attempt
  - 2.4 call attempts per second

$$\frac{0.015(\frac{\$}{\min})}{6(\frac{call}{\min})} = 0.0025(\frac{\$}{call})$$

SPAM

- Assume residential offering
  - 500K upstream
- Assume low compression codec
  - e.g. G.723.1 at 5.6 Kbps
  - ~ 90 simultaneous calls
- Assume about 10s of content/call
  - ~ 9 caps
  - broadband access ~ $50/ month

$$\frac{50(\frac{\$}{month})}{23.3M(\frac{call}{month})} = 0.00000215(\frac{\$}{call})$$

SPIT

XConnect

The Threat - Additional SPIT Considerations

- Name/Number space mining easier
  - username@domain space
    - SIP uses the same form of addressing as email
    - Reuse existing email lists to reduce costs
  - phone number space
    - finite address space
    - one that is fairly densely packed
    - Sequential phone #'s likely to produce high hit rate
- Pending stronger identity - Blacklisting is ill-advised
  - Legitimate user unable to use VoIP
- Bayesian content filtering not applicable
  - Content is available only once the call is answered

XConnect

The Solutions

- Make it harder to access namespace
- Reduce Automation
- Make cost prohibitive
- Limit “Openness” of communications

XConnect

The Solutions - Make it harder to mine #s

- **Address Obfuscation**
  - Spam lists are gathered from web sites
    - make your address impossible to gather
    - user@domain.com → u s e r a t d o m a i n d o t c o m
  - Public sources of info (e.g. ENUM) can be mined as well
    - Private ENUM trees, policy based DNS
- **Limited Use Addresses**
  - Give different addresses/numbers to different people
    - Once spam is detected on one account it is discontinued
- **Limited Use Addresses + presence**
  - Instead of email addresses user gives presence URI instead
  - Friends “subscribe” to presence info when wanting to send email
  - Presence data can include an email where user can be reached
    - One time use, obfuscated, different for each requesting buddy

Buddy list represents an automatically updating address book

XConnect

The Solutions - Reduce Automation

- Sender of message is given a “human only” puzzle
  - When solved correctly sender is placed on white list

- **Turing Tests**
  - sender connected to IVR and needs to enter spoken digits
    - Dependent on strong identity mechanisms
    - Language dependent
    - Can pay cheap human labor to take the test

XConnect

The Solutions - Make it cost prohibitive

- **Computational Puzzles –** Can't be solved by humans - expensive enough (computationally) to limit spam
  - Wide variation in computing power of potential clients wishing to communicate
  - Zombie machines help spammer reduce this cost
  - Active area of research (e.g. combining with white lists)

- **Payments at risk –** Sender puts money into receivers account prior to call - returned at end of call if not spam
  - Occurs only first time communicating with a given party
  - Relies on cheap micro payments techniques on the Internet
  - What is this "magical" amount?

- **Legal action**
  - Countries need to pass laws prohibiting spam – hard to enforce
  - Couple with existing laws (e.g. Habeas http://www.habeas.com header)
  - Peering agreements (e.g. http://www.dundi.com/PEERING.pdf)

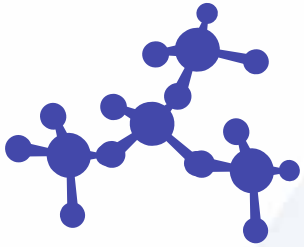
XConnect

The Solutions - Limit “Openness”

- Black lists/White lists

- Consent-based communications

- Reputations systems



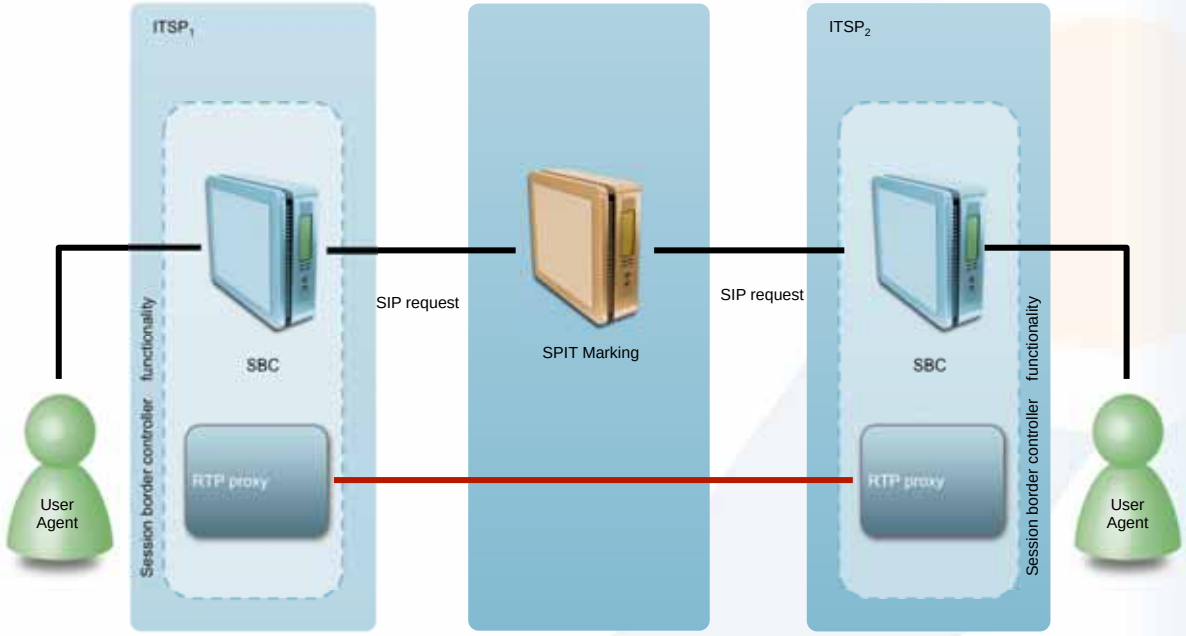
- Circles of trust (peering)

- Centralized providers (managed peering)

XConnect

The Solutions - Peering Enabled Solutions

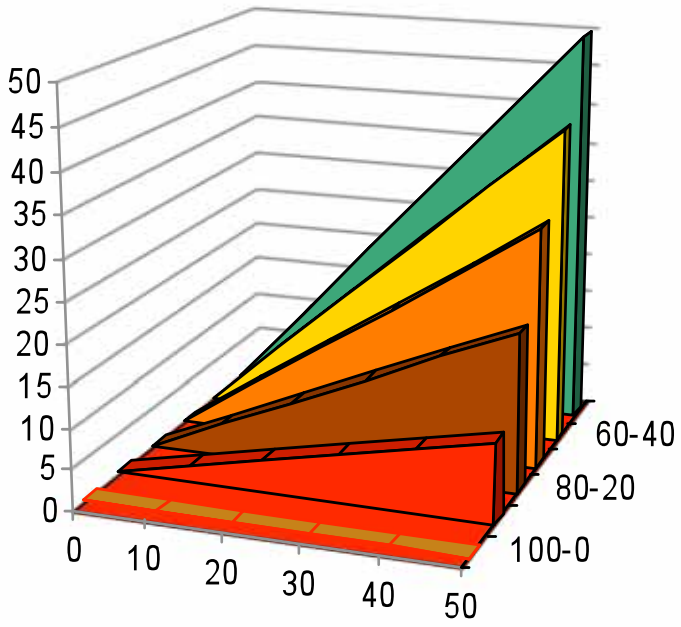
- Rating of Service Providers and individual call originators
  - Identity based
  - Assign a SPAM reputation or score



- SPIT threshold can be adjusted by each SBC enabled service provider

XConnect

SPIT Metric Examples



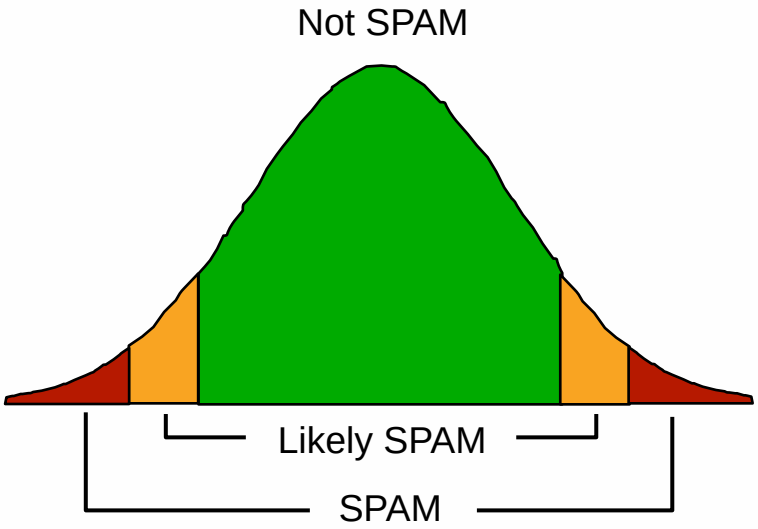
Symmetric Traffic
Incoming Vs. Outgoing

- Concurrent calls
- Call Attempts Per Second
- Call duration relative to average
- % of call attempts to invalid numbers
- Call spread (unique new numbers)
- Call distribution throughout the day

Other Metrics…

XConnect

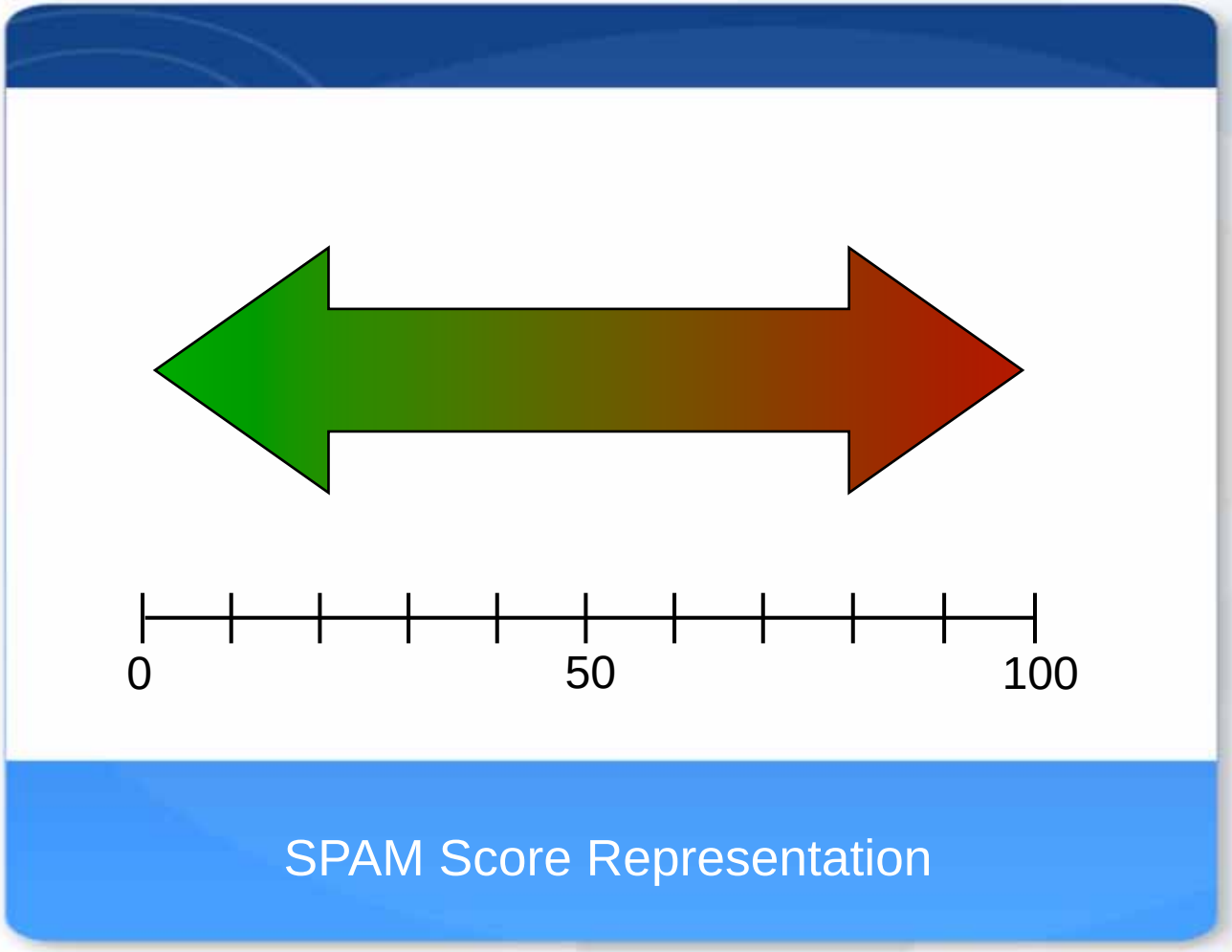
SPAM Metric Normalization



Algorithm for calculating individual metrics

XConnect

SPAM Score



XConnect

Spam-Score Header

```
INVITE …
Via: …
To: …
From: …
…
Spam-Score: Sym=0.7 ACD=0.4 Algo=SPAM1 Score=65
…
Cseq: …
Content-Length: …
```

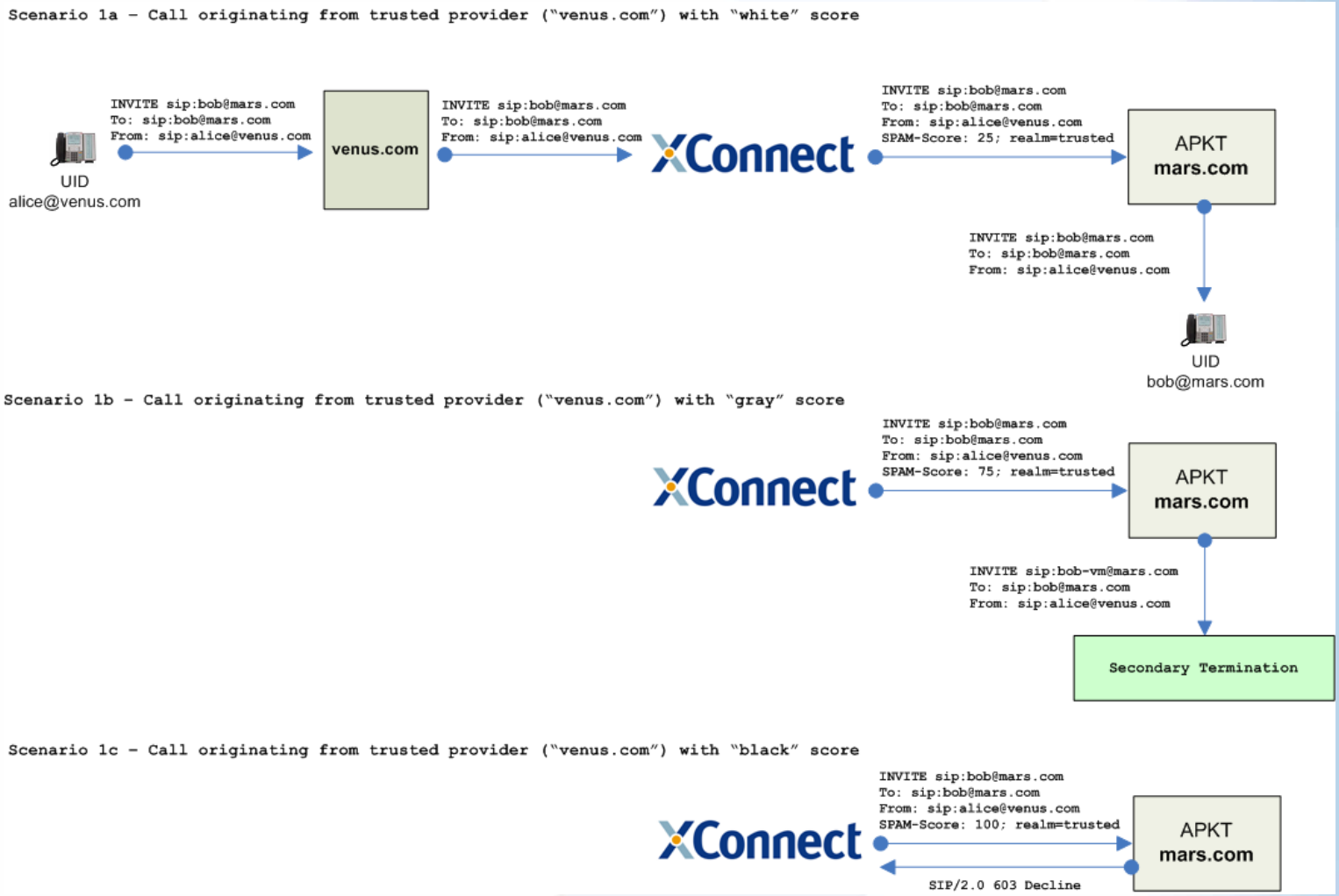
draft-wing-sipping-spam-score-02.txt

XConnect

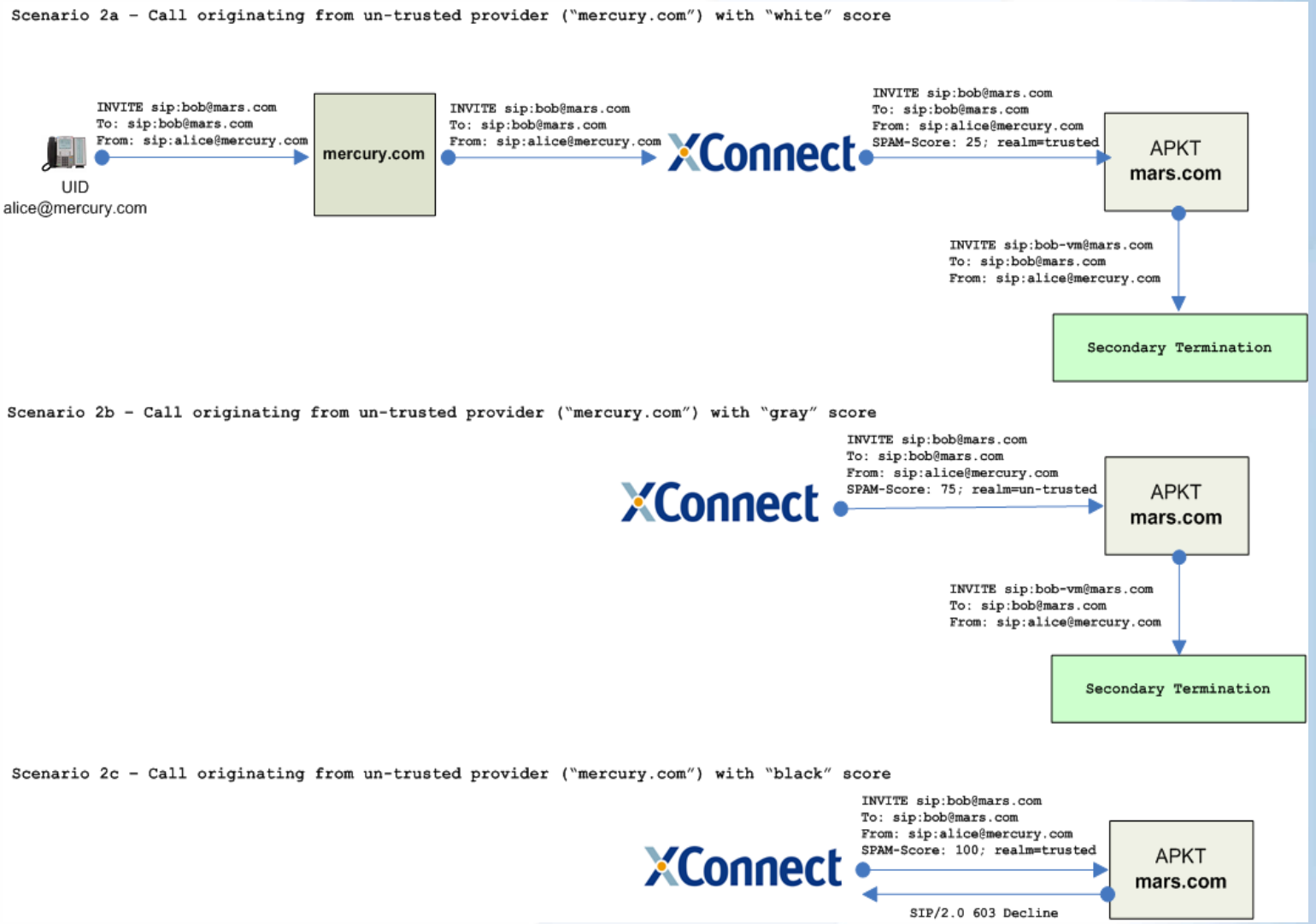
AcmePacket and XConnect Cooperate to test and deliver SPIT solutions

- Acme and XConnect technical executives participate in IETF standards initiatives for the design and functionality of the SPAM score concept
- Several drafts are introduced to the IETF including RUCUS Test Cases in July 08
  - http://tools.ietf.org/pdf/draft-schwartz-rucus-test-cases-00.pdf
- Proof of concept testing was conducted in Spring and Summer 2008
- Functionality now available in
  - latest Acme Packet NetNet SBC releases
  - XConnect Private Federations

Scenario 1: Call Flow from Trusted Provider



Scenario 2: Call from Un-Trusted Provider



XConnect

Additional References

- The Session Initiation Protocol (SIP) and Spam
  - RFC 5039
- SPAM Score For SIP
  - draft-wing-sipping-spam-score-02
- Policy based ENUM
  - draft-lendl-sip-peering-policy-00
- General background
  - draft-lendl-speermint-background-01

XConnect

Eli Katz

+1 914 487 2461

press@xconnect.net

www.xconnect.net