

***VoIP security
– myths & realities***

acme  packet

***Ishai Rosmarin
Sales Director – EMEA
IRosmarin@acmepacket.com***



**in IP
we don't
trust
anyone!**

VoIP security in the news



** VoIP Security Alert: Hackers Start Attacking For Cash (June 2006)*



** Two Men Charged With Hacking Into VoIP Networks (June 2006)*



** The Internet's a Scary Place for Voice (May 2006)*



** Is Your VoIP Phone Vulnerable? (June 2006)*

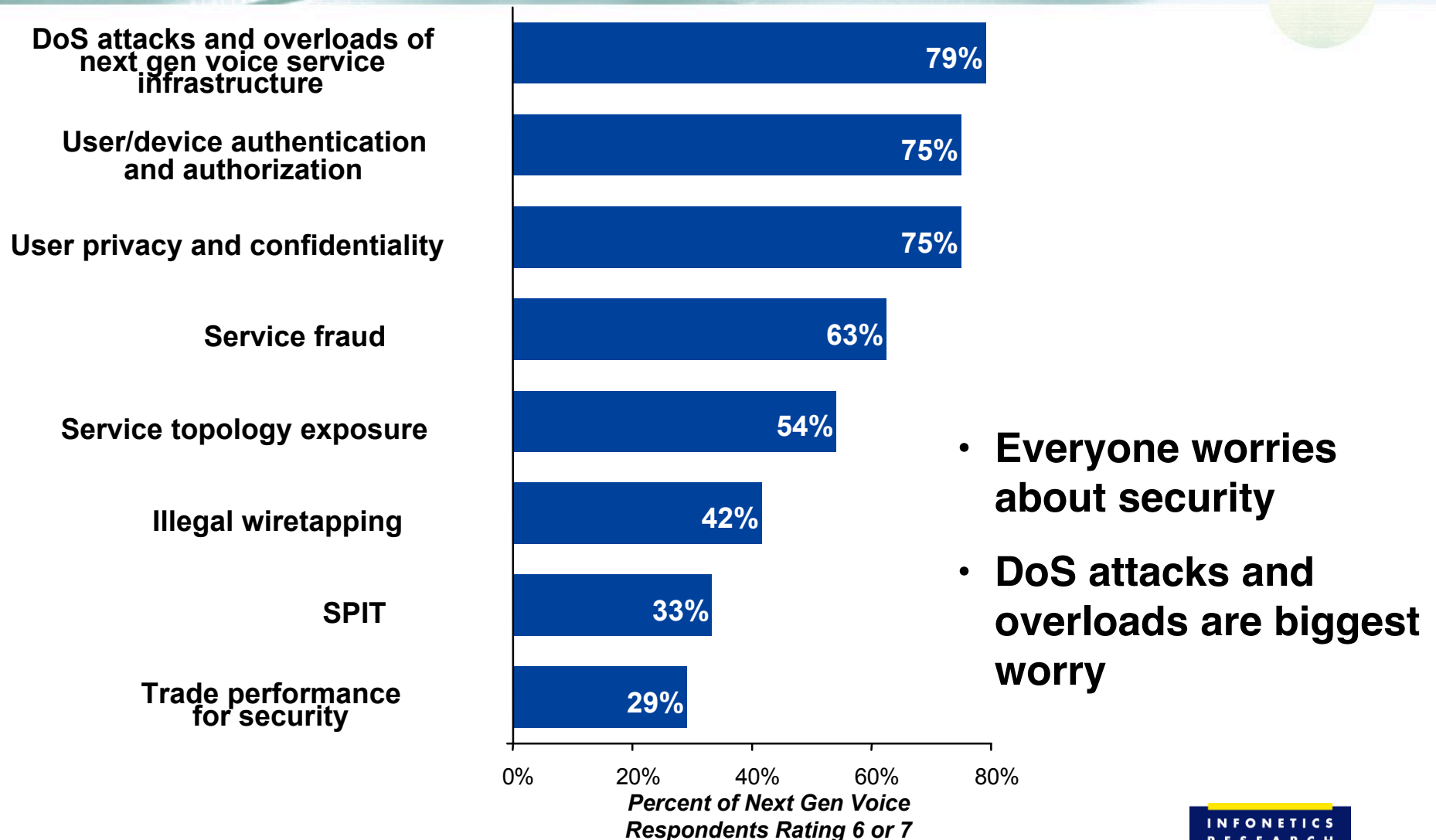


** Are Hackers Eyeing your VoIP Network? (Sept. 2006)*



** VoIP Security: It's More Than Data Security (Aug. 2006)*

Security Concerns



VoIP security threats & solutions



Security Threat	Comments	Impact	Probability			Security Solution
			VoIP over Internet - free, anonymous	VoIP over Internet - fee, not anonymous	VoIP over managed network	
DoS and DDoS attacks (service provider infrastructure)	-Requires sophisticated attack capable of covering tracks; -Catastrophic impact as all subscribers are impacted	10	1	3	2	-Access control and packet filtering; -Topology hiding and disintermediation; -Rate limiting and call gapping; -Dynamic attacker detection and blocking
Viruses and malware	-Impact varies based on service provider infrastructure, enterprise IP PBX or residential PC	3 to 8	5	5	5	-Authentication & authorization; -Deep packet inspection; -Signature detection; -Authenticated encryption
Service fraud	-Requires technical sophistication; -Impact depends on business model	5	N/A	5	5	-Bandwidth policing; -QoS marking/ mapping; -Admission control; -Authentication & authorization; -Intrusion detection
Identity theft (phishing, not man-in-the-middle)	-Requires slightly more technical sophistication than SPIT; -Man-in-the-middle requires same degree of technical capabilities; -Information can be used for other attacks with various impacts	2 to 5	8	6	4	-Authentication & authorization; -Authenticated encryption
Eavesdropping/ user privacy	-Requires technical sophistication and access to wiring closets	2	5	5	2	-Authenticated encryption; -Anonymize user information
SPIT	-Requires little sophistication; -Annoying more than harmful	1	10	8	6	-Authentication & authorization; -Call screening and filtering; -Access control; -Topology hiding; -Intrusion detection

Note: probability and impact ratings on 1 to 10 scale with 1 being low and 10 being high

IMS: Is Missing Security



Security feature requirement	IMS function/feature	DoS/DDoS attacks	Traffic overloads	Viruses & malware	Service fraud	Identity theft	Eves - dropping	SPIT
Access control - static IP address list	Core IMS functions, not applicable for UE							
Access control - dynamic IP address list	Not addressed				x			
Topology hiding (NAPT at L3 & L5)	I-BCF only, THIG sub-function							
Authentication - subscriber & CSCF	IPSec, SIP digest							
Authorization - subscriber	HSS function							
Signaling encryption	IPSec							
Media encryption	Not addressed							
Admission control - I/S-CSCF constraints	Not addressed							
Admission control - network bandwidth constraints	PDF/RACS function							
Admission control - user limits: sessions (#)	Not addressed							
Admission control - user limits: bandwidth	Not addressed							
SIP message & MIME attachment filtering/inspection	Not addressed							
Signaling rate monitoring & policing	Not addressed							
Bandwidth monitoring & policing	Not addressed							
Call gapping - destination number	Not addressed							
Call gapping - source/destination CSCF or UE	Not addressed							
QoS marking/mapping control	Not addressed							

DoS/DDoS attacks threaten subscriber retention and revenue



* Types

- Malicious attacks
- Non-malicious – poor behaving endpoints, power outages

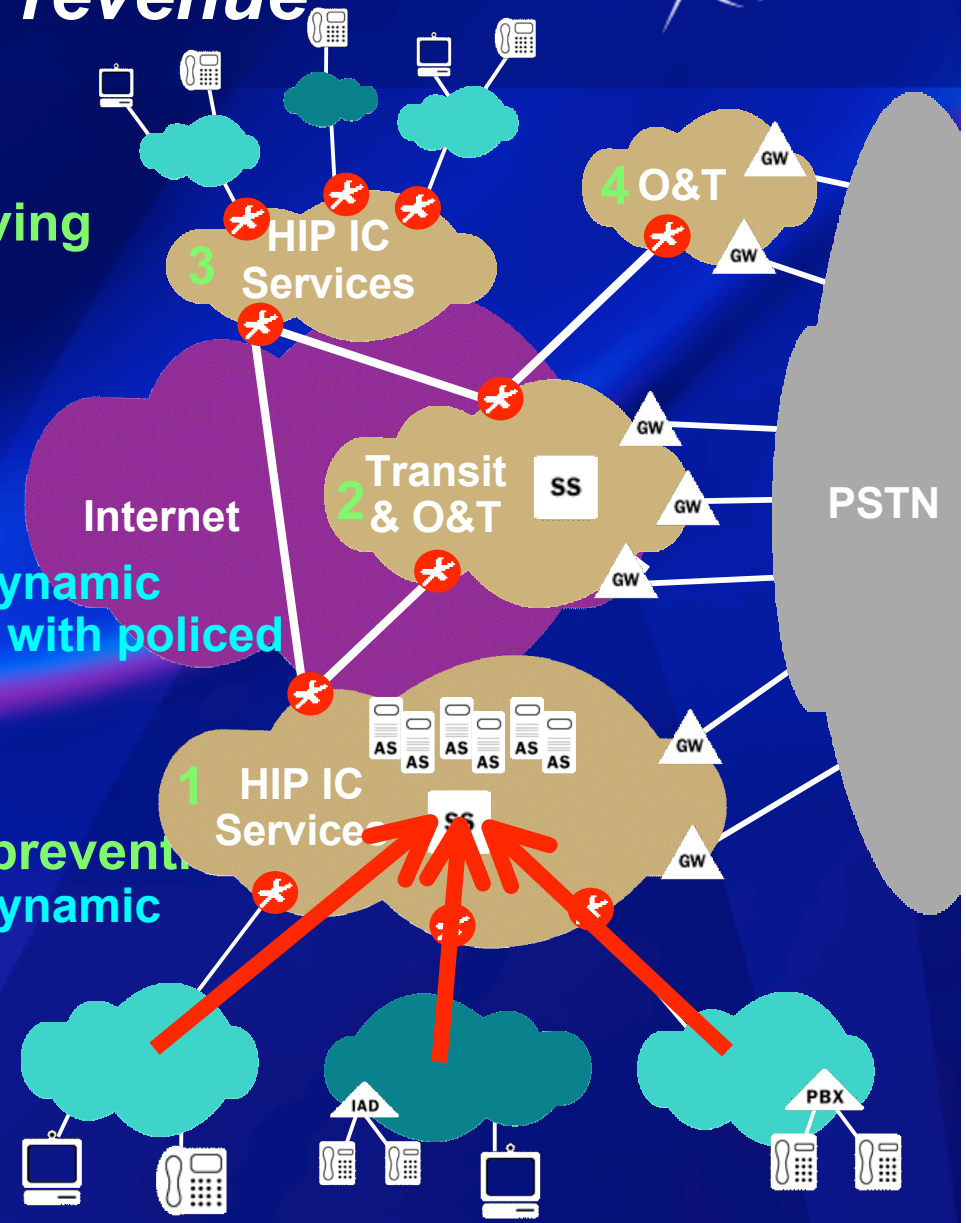
* Solution requirements

- SBC DoS self-protection

- Access control - static & dynamic
- Trusted & untrusted paths with policed queues
- IDS capabilities

- Service infrastructure DoS prevention

- Access control - static & dynamic
- Topology hiding
- Signaling rate plicing
- Bandwidth policing



Viruses & malware can threaten IC endpoints and service infrastructure



* SIP MIME attachments are powerful tool for richer call ID
- vcard text, picture or video

* Potential Trojan horse for viruses and worms to general-purpose server-based voice platforms

- SIP softswitch, IMS CSCF, SIP servers, app servers
- SIP PBX
- SIP phones & PCs

* New endpoint vulnerabilities

- Embedded web servers - IP phones
- Java apps – liability or asset?

* Solution requirements

- Authentication
- SIP message & MIME attachment filtering
- Secure OS environment

Code Red Sobig



Nimda

SQL

Slammer



Melissa

Klez

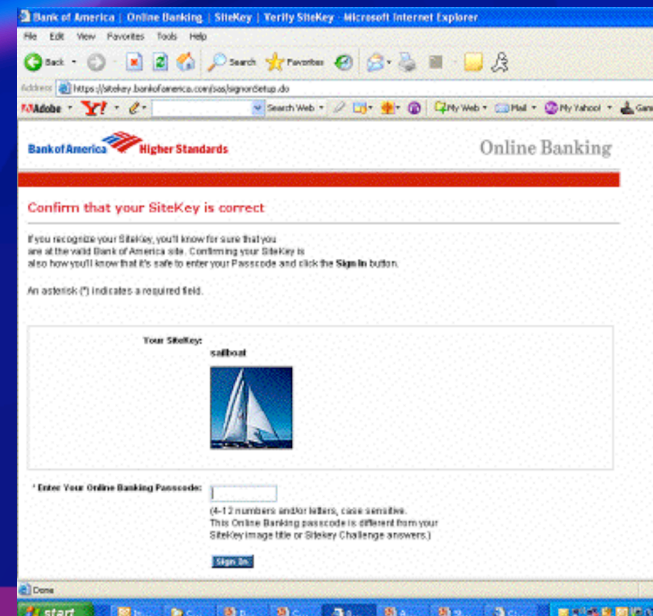
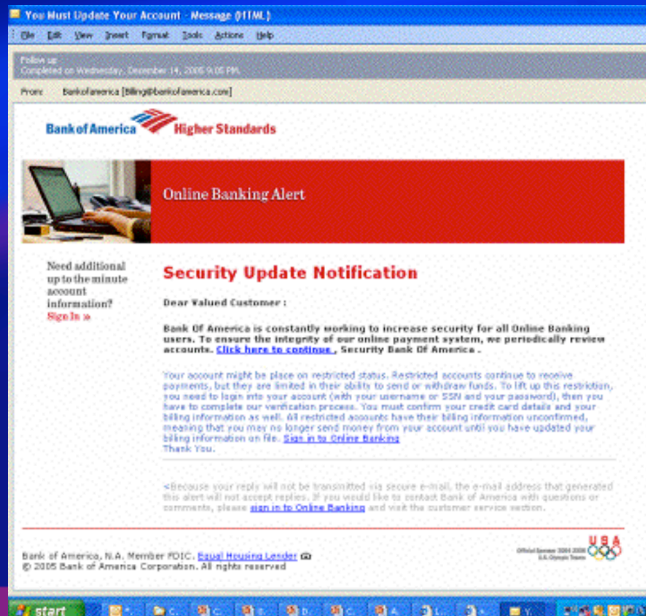
Michelangelo

Love Bug

Identity theft can't be prevented entirely by technology



- * How do you know you are talking to Bank of America?
- * Web site techniques don't work for IC
 - work for many-one, not many-many
- * Solution requirements
 - Authentication, access control
 - Trust chains - pre-established technical & business relationships



Eavesdropping threat is over hyped



* Less risk than email, who encrypts email?

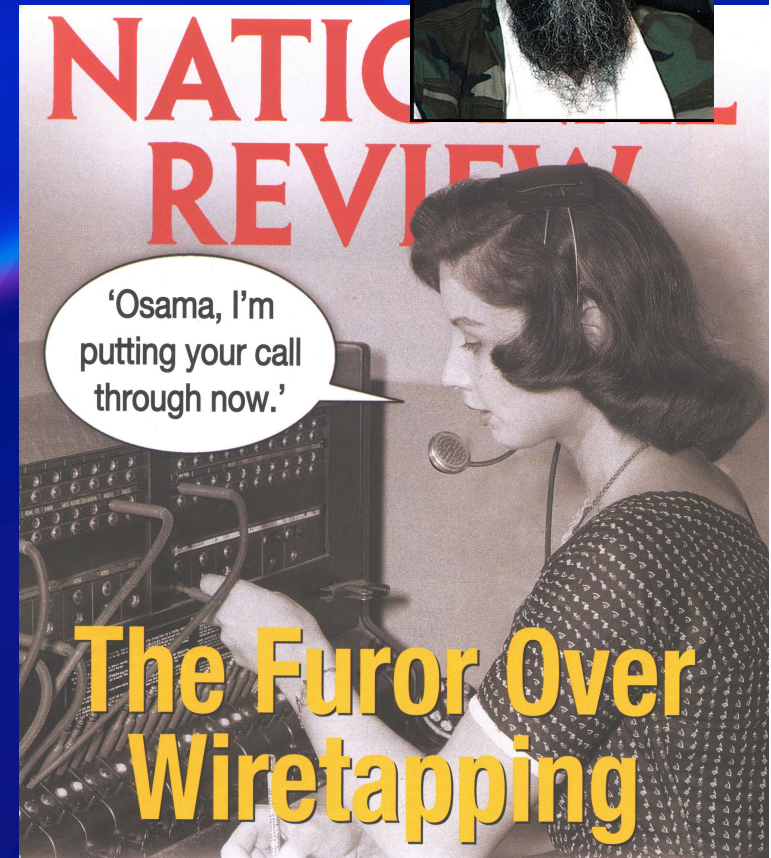
- Email is information rich (attachments), voice not
- Email always stored on servers, only voice mail
- Email always stored on endpoints, voice not

* Who is at risk?

- Bad guys - Osama, drug cartels, pedophiles, etc.
- Law enforcement
- Money, love, & health-related
 - insider trading, adultery, ID theft,

* Solution requirements

- Authentication – subscriber
- End-to-end encryption (EXPENSIVE)
 - Signaling (TLS, IPsec)
 - Media (SRTP, IPsec)



SPIT will be annoying, & possible tool for ID theft



* Will anonymous, cheap Yahoo subscriber (aka SPITTER) be able to call money-paying Verizon subscriber to solicit - phone sex, penis enlargement, Viagra pill purchase?

* Techniques that won't work

- Access control – static
- Content filtering
- Charging - \$/call
- Regulation

* Solution requirements

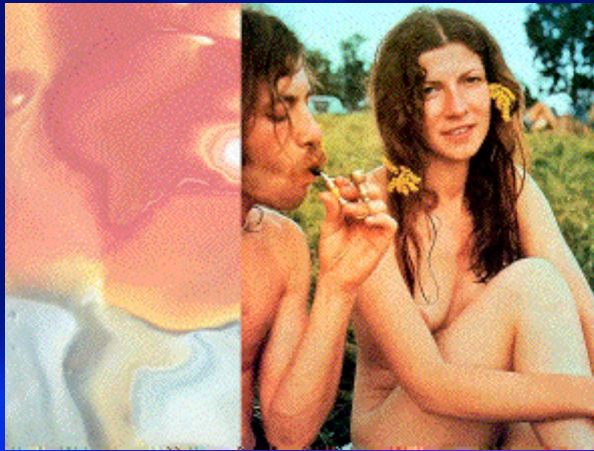
- Access control
 - dynamic, IDS-like
- Authentication
- Admission control
 - subscriber limits (#)
- Trust chains - pre-established technical & business relationships



Who is responsible for security?



The individual

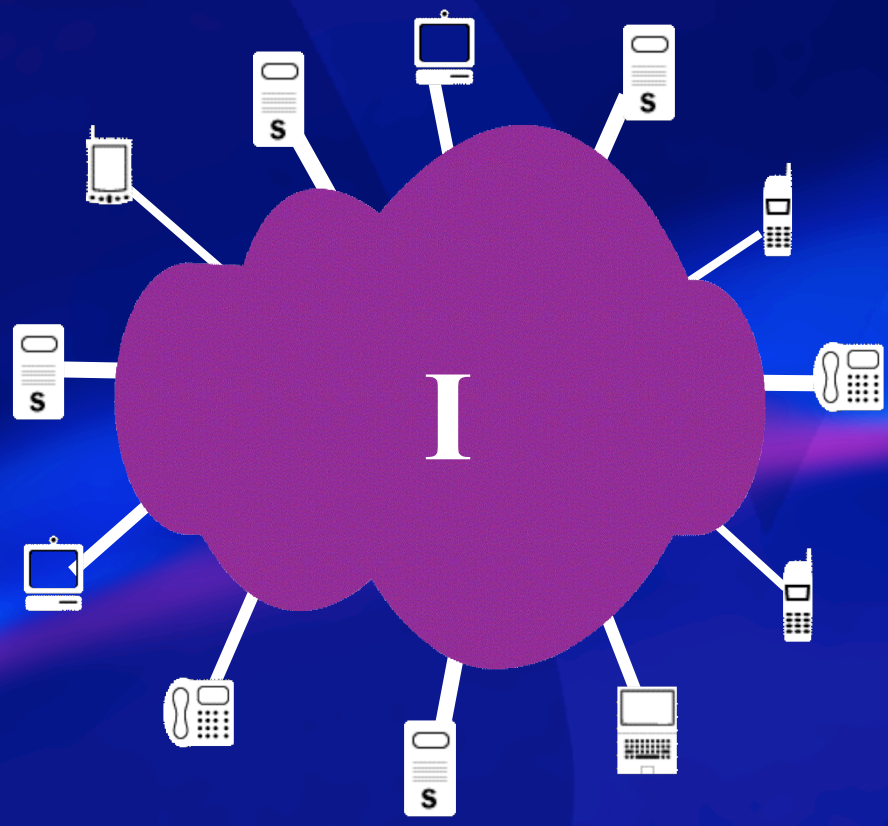


The organization

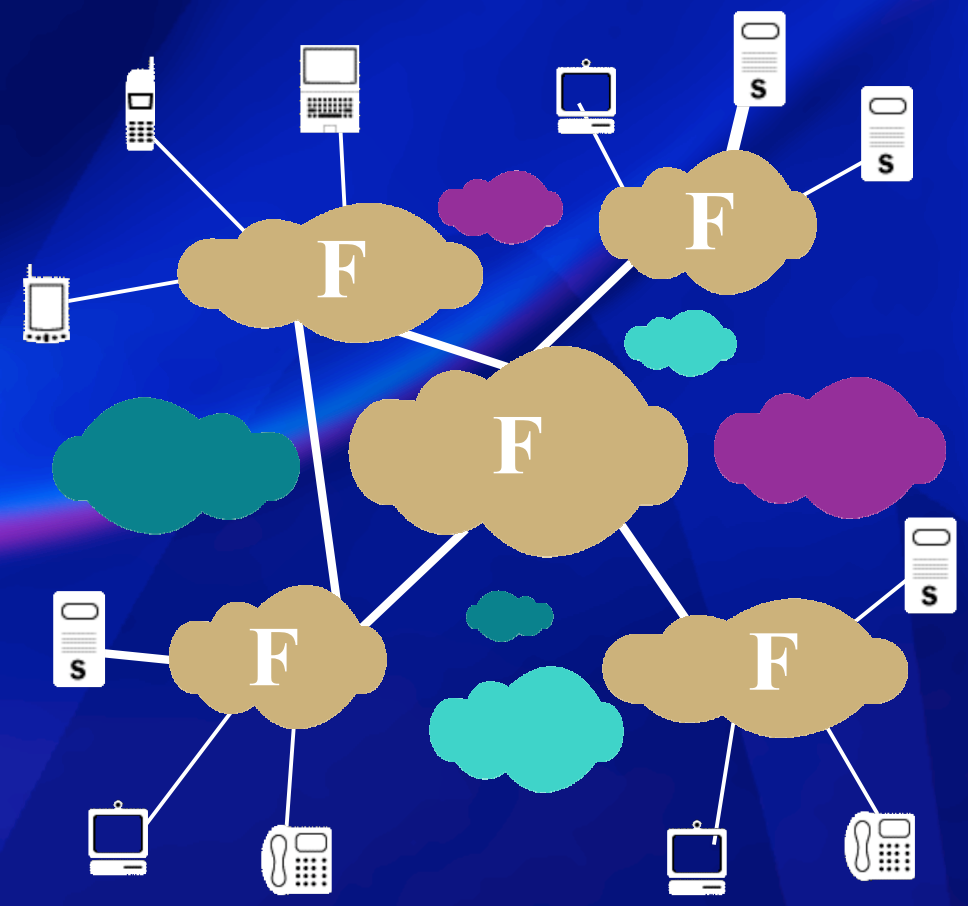


The future IC net?

The Internet



The Federnet



Net-Net



* Security issues are very complex and multi-dimensional

* Security investments are business insurance decisions

- Life – DoS attack protection
- Health – SLA assurance
- Property – service theft protection
- Liability – SPIT & virus protection

* Degrees of risk

- Internet-connected ITSP
- Facilities-based HIP residential services
- Facilities-based HIP business services
- Peering

High
↑
↓
Low

- NEVER forget disgruntled Malcom, OfficeSpace

* Session border controllers enable service providers to insure their success

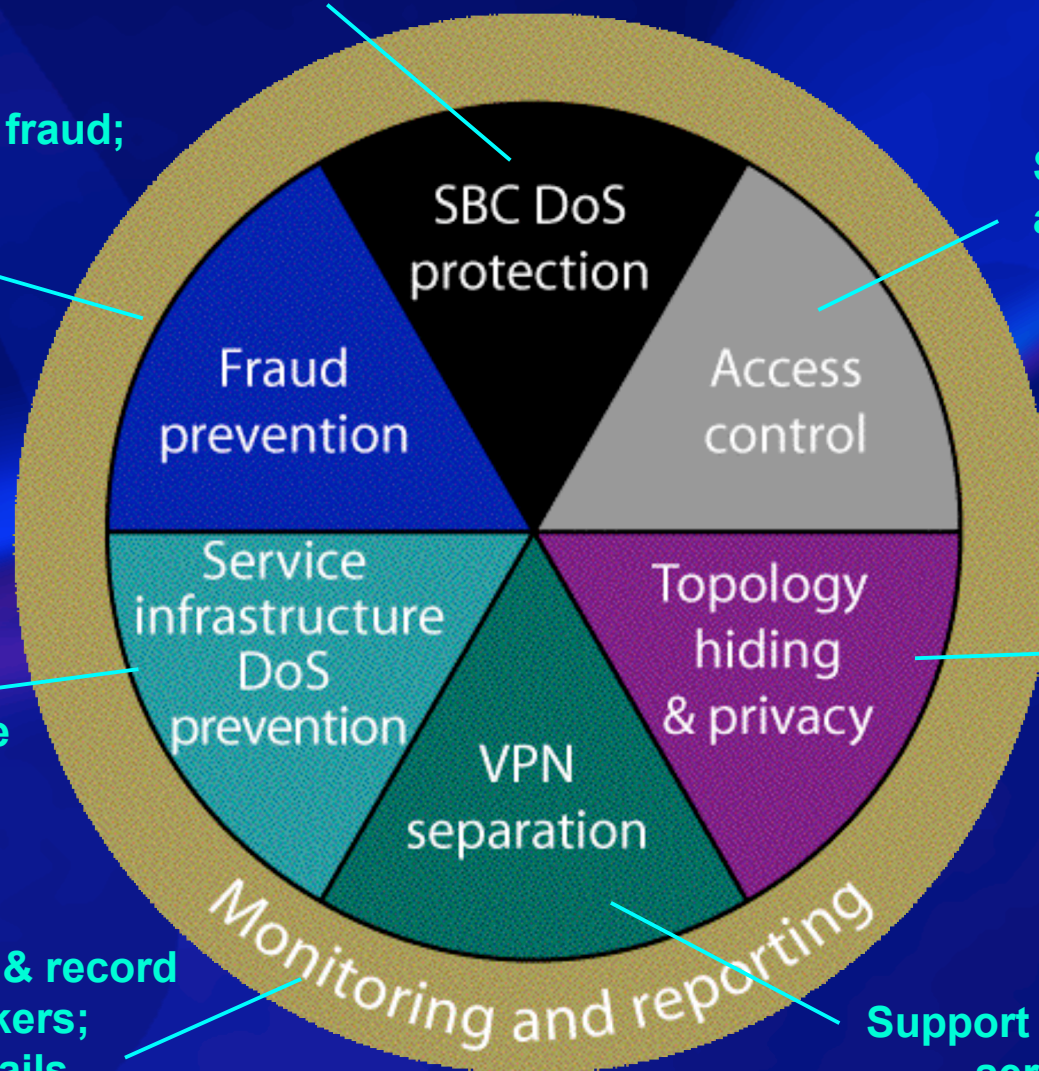
Net-SAFE – security requirements framework for session border control



Protect against SBC DoS attacks & overloads
(malicious & non-malicious)

Prevent misuse & fraud;
protect against
service theft

Session-aware
access control
for signaling
& media



Prevent DoS
attacks on service
infrastructure &
subscribers

Complete
service
infrastructure
hiding & user
privacy support

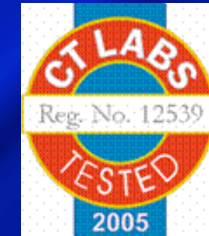
Monitor, report & record
attacks & attackers;
provide audit trails

Support for L2 and L3 VPN
services and security

Acme Packet Net-Net SD “flawlessly passed all of CT Labs’ grueling attack tests”

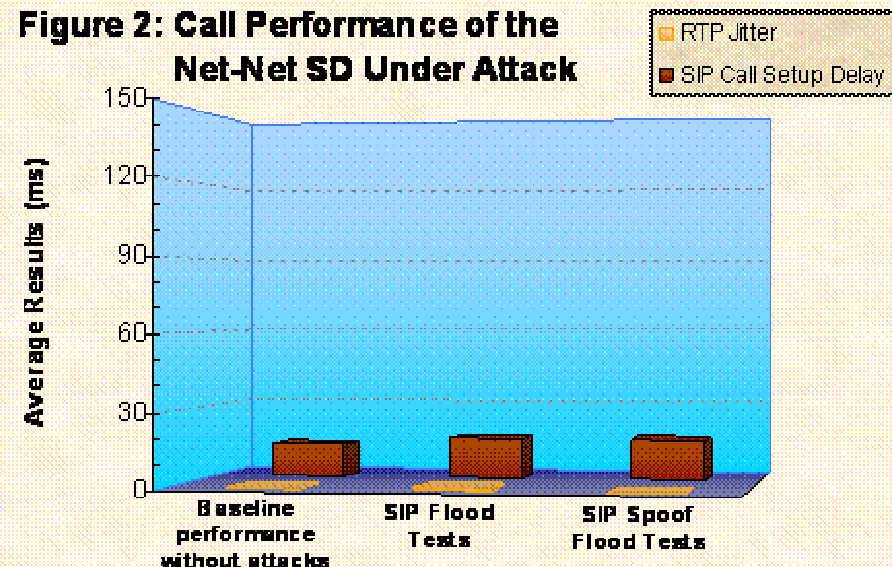


- ★ Total of 34 different test cases, using over 4600 test scripts
- ★ No failed or dropped calls, even for new calls made during attacks
- ★ No lost RTP packets during attacks
- ★ Protected the service provider equipment – did not allow flood attacks into core, stopped packets at edge
- ★ SD performance not impacted during attack



- SD CPU utilization - only 10% increase
- Signaling latency - only 2 ms average increase
- RTP jitter – less than 1 ms increase (not measurable by test equipment)

Figure 2: Call Performance of the Net-Net SD Under Attack



Acme Packet SBC DoS/DDoS protection

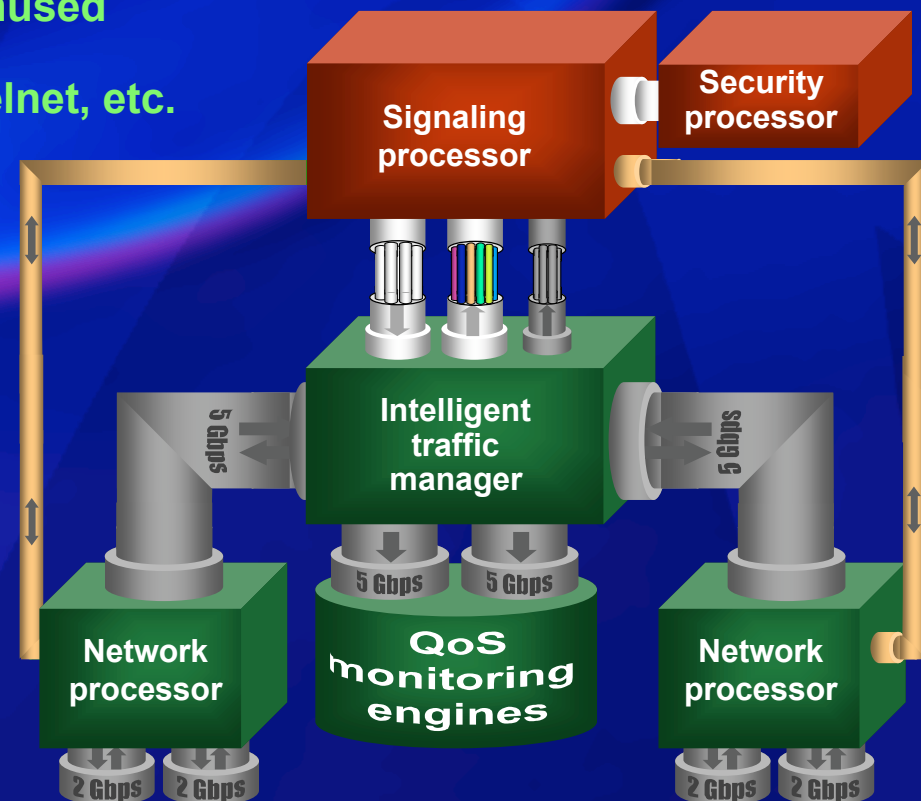


* Network processor (NPU) -based protection

- L3/4 (TCP, SYN, ICMP, etc.) & signaling attack detection & prevention -
- Dynamic & static ACLs (permit & deny) to SPU
- Trusted & untrusted paths to SPU w/configurable bandwidth allocation & bandwidth policing per session
- Trusted devices - guaranteed signaling rates & access fairness
- Untrusted devices – can access unused trusted bandwidth
- Separate queues for ICMP, ARP, telnet, etc.
- Reverse Path Forwarding (uRPF) detection - signaling & media
- Overload prevention - 10 Gbps NPUs > 8 Gbps network interfaces

* Signaling processor (SPU) -based protection

- Overload protection threshold (% SPU) w/graceful call rejection
- Per-device dynamic trust-binding promotes/demotes devices



*The leader
in session border control*

acme  packet

*for trusted, first class
interactive communications*