Black Box Analysis and Attacks of Nortel VoIP Implementations

Richard Gowman, CISSP
Eldon Sprickerhoff, CISSP CISA
www.esentire.com

e•sentire
Critical Security Solutions

Who we are...

- eSentire, Inc.
- Based out of Cambridge, ON.
- Collaborative Threat Management (Ongoing Security Analysis, Penetration Testing)
- Established in 2001.

Why Are We Speaking?

- Engaged in VoIP Security Analysis
- Nortel always seemed to get off easy (most attention paid to Cisco and Avaya?)
- We have several clients that use Nortel IP Telephony.

Overview

- Misconceptions about Nortel IP Telephony
- Physical Traffic Capture Configuration
- Protocols
- Attack Tree
- Implementation Weaknesses
- Remedies Against Attacks
- Nortel's Responses
- Tidbits

Misconceptions

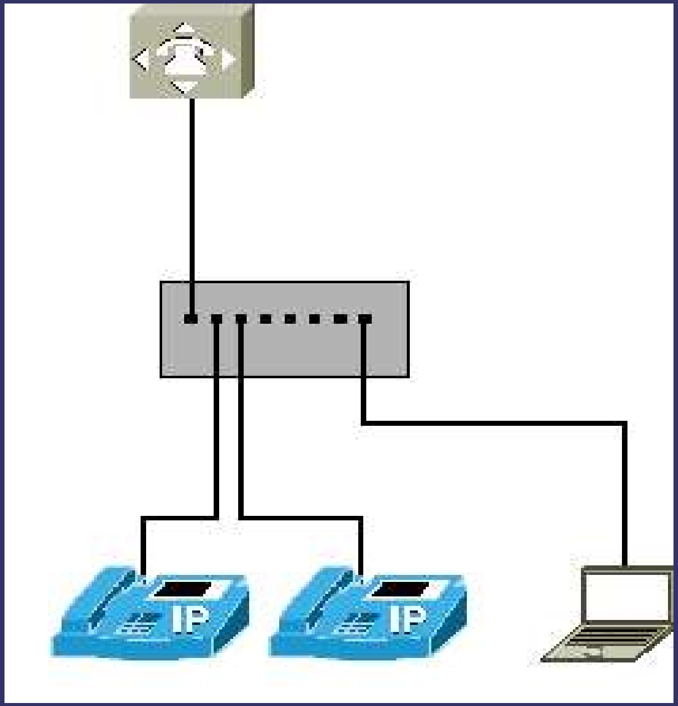
- Voodoo
- Implemented by external consultants
- Not fully understood by Voice group
- Not fully understood by Network group
- Security == Chicken Little

Misconceptions

- “Nortel uses a proprietary protocol and it's impossible to eavesdrop or extract the conversation.”
- “I did a packet capture and only got VLAN tagged data.”
- “We're OK - it's segregated from the data network.”
- “Haven't seen any tools on the Net.”
- “nCircle didn't find anything.”
- “We're getting a SIP firewall.”

On The Wire

- Hub/Bridge combo
- VLAN if necessary
- We used OpenBSD bridge/vlan combo.



e•sentire
Critical Security Solutions

Run Through Possible Traffic

- reboot_phone
- offhook_and_hangup
- offhook_onedigit_hangup
- call_internal_no_answer
- call_internal_answer
- internal_call_us
- internal_call_no_pickup
- internal_call_us_answer
- speakerphone_nocall
- speakerphone_call
- speakerphone_call_answer
- redial
- redial_answer
- change_volume
- disconnect_server_cable
- disconnect_server_cable_in_conversation
- disconnect_client_cable_in_conversation
- nmap_client
- external_call_in
- call_external
- And so on....

Protocols (1)

- It sure ain't SIP, baby.
- Unified Networks IP Stimulus (UNIStim)
- US Patent 7068641
- Canadian Patent 2273657

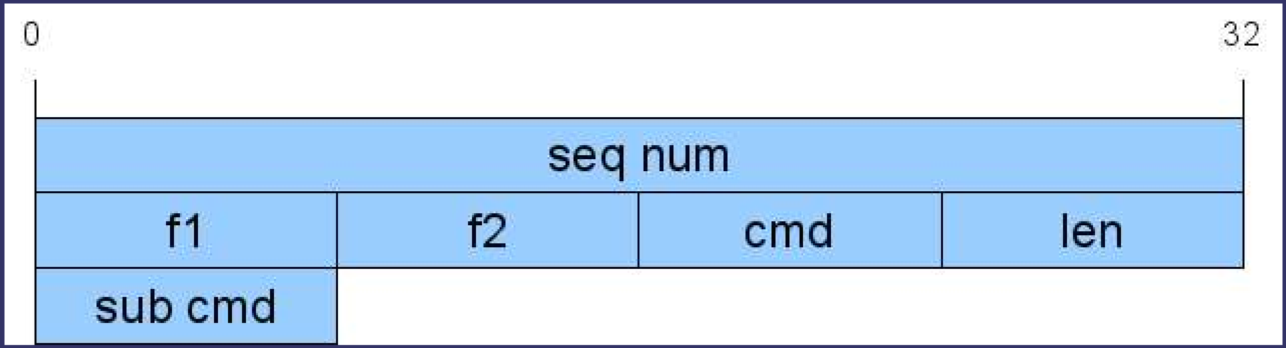
UNIStim

- Some details can be found in Asterix doc'n
- But didn't seem to necessarily mesh with what we found (possibly an older version?)

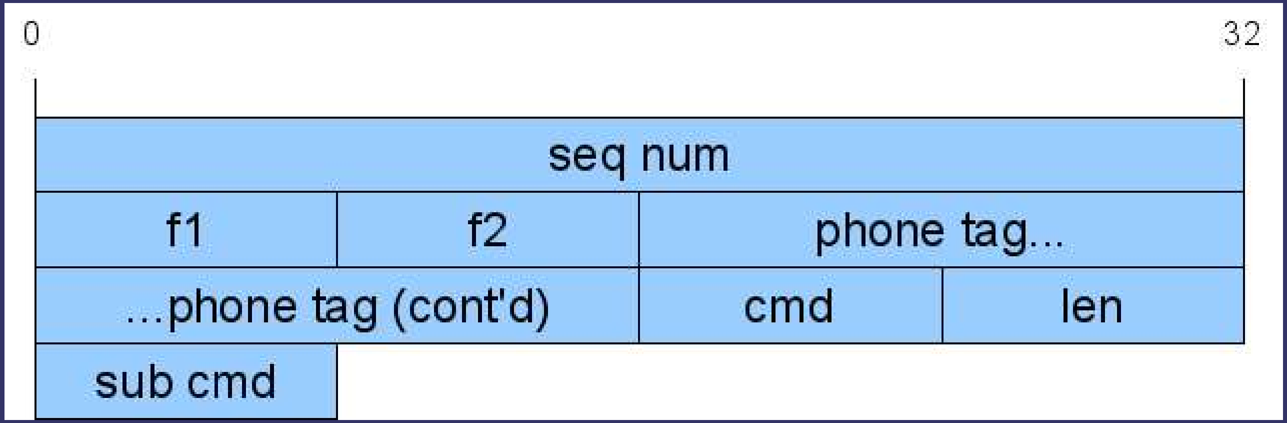
e•sentire
Critical Security Solutions

UNIStim

- UDP protocol
- Contains a sequence number, a few flags, and commands/parameters



0			32
seq num			
f1	f2	cmd	len
sub cmd			



0			32
seq num			
f1	f2	phone tag...	
...phone tag (cont'd)		cmd	len
sub cmd			

e•sentire
Critical Security Solutions

UNIStim Sequence Number

- Sequence number increments by 1 for each packet.
- Both client and server appear to ignore packets with incorrect sequence number (although they still send an ACK back)

UNIStim Flags

- Flag1: 0x00 – Error, 0x01 – ACK, 0x02 - PUSH
- Flag2: 0x00 – ServerACK/Irrelevant, 0x01 – server (to client), 0x02 – client (to server)
- Tag: (Client only) 4 bytes that the server will instruct the client to use
- cmd/sub cmd: These fields are combined to give the instruction to the client/server.

Network Capture

- Headset boots up (DHCP)
- Initial conversation with PBX (UNIStim)
- RTP packets sent directly between two phones

UNIStim

- Again, not SIP.
- Nortel will tell you that they support SIP and H.323
- IP sets themselves only speak UNIStim.
- SIP functionality “available” through UNIStim Terminal Proxy Server
- Not “Open Source”
- UNIStim channel driver exists for Asterix.

Security Considerations

- Confidentiality
- Integrity
- Availability

Confidentiality

- For Phone Call
  - Easy to sniff and reassemble phone conversations. (Ethereal/Wireshark can do it right out of the box for any RTP stream.)

- For Control Stream
  - Also easy to sniff UNISTim packets, so you can see exactly who the phone is calling.

Integrity

- For Phone Call
  - RTP also has a sequence number, so must sniff it before being able to inject.
  - Nothing prevents you from modifying packets as they pass through...

- For Control Stream
  - Seq number (in theory!) means that you must sniff an RTP packet first, and then can take over the stream.
  - Again, nothing prevents you from modifying the packets in transit...

Availability

- For Phone Call
  - Determine seq number and spoof some packets. The other end now hears what you want (which could be nothing at all.)

- For Control Stream
  - Determine seq number and tell the phone to do whatever you want it to do (including hanging up.)

Availability (2)

- For Phone
  - Start sending it packets (with a valid sequence number.) If you don't do everything properly, you'll confuse the phone and cause it to reboot (which takes a few minutes.)

- For Call Manager
  - Of course, nothing works if you can take down the Call Manager. (More on this later... :)

Attacks/Recon

- SYN Floods
- Network Mapping
- Fuzzing
- Brute Force Pass

- UNISTim seq num brute force
- Pickup/Hangup
- Media Card
- RTP injection
- ChangeDisplay
- Dial
- Terminate Conn
- Force Conn Open

“This is UNIX. I know this!”

- nmap shows:
- tcp/21
- tcp/23
- tcp/80
- tcp/111
- tcp/513
- udp/5060
- udp/161
- icmp

e•sentire
Critical Security Solutions

What else?

- SNMP: OID 1.3.6.1.2.1.1.1 (sysDescr, sysUptime, Software Release)
- SNMP community name: public
- FTP, HTTP: VxWorks
- ICMP: Timestamp

SYN Floods

- Server well-defended against flood of half-open packets.
- But the protocol appears to be weakly defended against fuzzing attacks.

“Atemi”

- Send random crap to ports
- Create a broadfisted DoS (works well against TCP).
- Take down the Primary, helps to find Secondary and Tertiary servers.

Pickup/Hangup

- Send many (100k) Pickup/Hangup packets
- Servers not well defended against this (fall down, go boom).
- Some firmware appears to defend against this attack.

RTP Packet Injection

- Inject tone (square waveform)
- Ouch!
- Works both in-band and out-of-band (caveat about sequence numbers).

UNISTim Seq Num Brute Force

- Sequence number for UNISTim packets appears to be 32bits. Unless you can sniff a packet, you must guess and 32bits is too large (due to hardware limitations on the phones themselves.)
- However, from observation, the first 16 bits always seem to be 0. This makes a brute force attack on the sequence number very feasible. (About a minute or so.)

Dial

- Cause a phone to dial any number you want.
- Want to get that annoying co-worker fired? Just about any 1-900 number will do (unless they're blocked).
- Keep initiating calls from your boss to the CEO (or their spouse – marital discord).

Terminate Connection

- Causes a connection to be closed.
- Inject one packet towards server saying client has hung up.
- Also inject one packet towards client saying other side has hung up.

Force Conn Open

- Initiate a phone call without recipient knowing.
- Why wait for a phone call in order to listen in to your victim?

Brute Force Admin Password

- ADMIN1
- Telnet is probably your best bet.
- Try “1111” as the password first.

Media Card Tidbits

- Tertiary IP telephony provisioning
- 32 phones per card
- Doesn't require a separate PBX (apparently).
- Only has UDP ports open (not susceptible to TCP SYN attacks).
- But appears to be particularly susceptible to protocol-sensitive fuzzing attacks.

Media Card One-Packet DoS Hex Example

- UDP
- SRC Port: 5000, DST Port: 5100
- HEX DATA DELETED UNTIL ISSUE RESOLVED

Official Nortel Position

- Securing Multimedia & IP Telephony
- “Instant” Secure Multimedia Zone Secure Multimedia Controller 2450 (SMC)
- Virtual “moat” around servers
- Stateful filters (SIP, H.323, etc.)
- Denial of Service defence engine
- Secure UNIStim encryption proxy
- 802.1X with EAP
- SRTP
- Gratuitous ARP Denial, Switch Lockdown

Security is a PITA

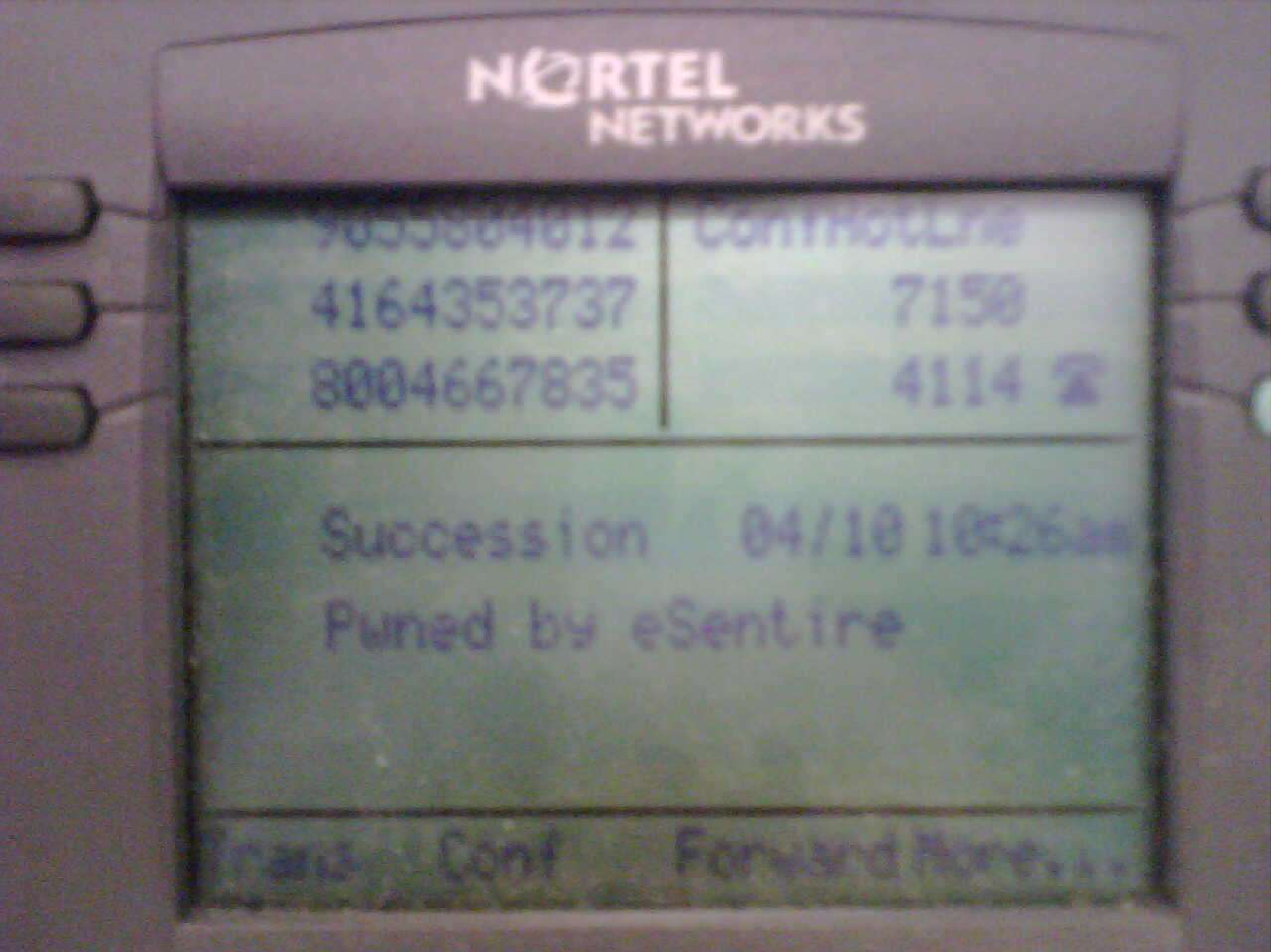
- Easy to ignore (Just get it working!)
- Adds overhead
- Can limit debugging capability
- Compatibility issues (conference calls, etc.)
- Major PITA to add after-the-fact

Configuration

- Limit administration access.
- Lock down protocols (some firewall functionality exists in the product itself).

Finally... ChangeDisplay

- Tell the phone what to display
  - Could use to display caller-id name/number
  - Plus, it's a lot of fun...



NORTEL NETWORKS

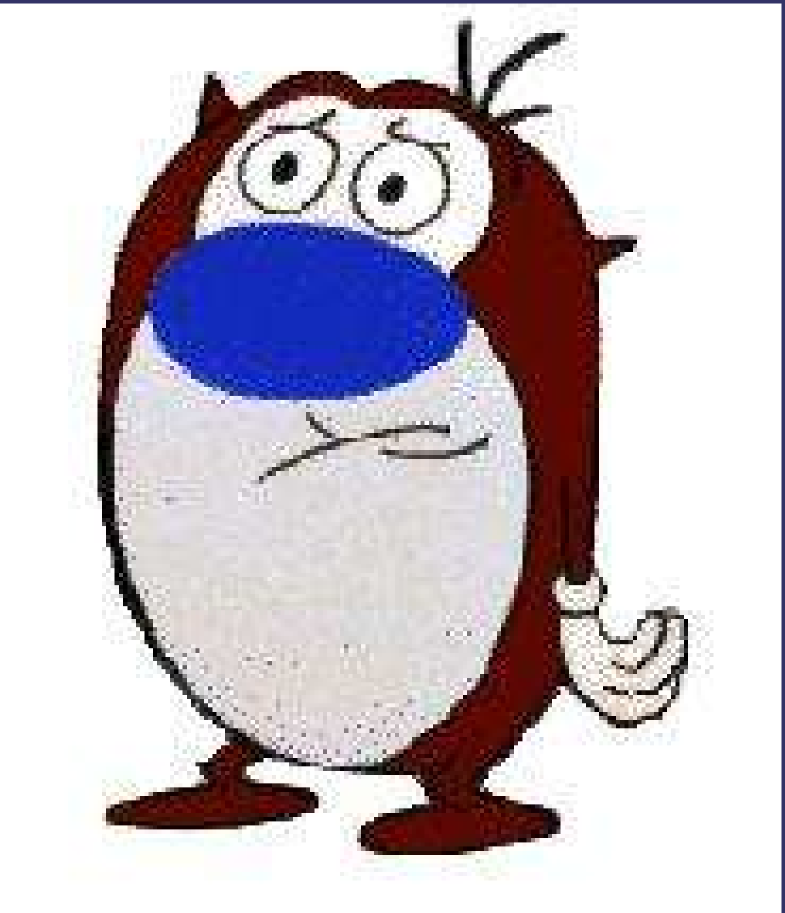
```
[illegible]   ConfHotLine
4164353737           7150
8004667835         4114 ☎

Succession   04/10 10:26am
Puned by eSentire

Trans   Conf   Forward More...
```

UNIStimpy: Slides and Code

- http://www.esentire.com/unistimpy
- Code coming soon!
- Shameless Plug: We consult!



e•sentire
Critical Security Solutions