

NGN – Next Generation Nightmare ?

What telco 2.0 really
means

Nicolas FISCHBACH

Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - <http://www.securite.org/nico/>

Internet-wide Security Issues

- So, what kept us up at night ?
- SNMP
- SQL Slammer (and friends)
- Cisco wedge bug <- 2003. Remember ?
 - State of upgrades today ?
 - State of transit ACLs today ?
- BGP TCP window [not really actually]
- Botnets and DDoS

Internet-wide Security Issues

- What have we done about it ? A lot. Too much maybe ?
 - Route/prefix filtering
 - DDoS detection: Netflow
 - DDoS mitigation: BGP (+ MPLS (+ Cleaning))
 - xACLs and MPLS Core hiding
 - QoS and Control Plane Policing (CoPP)
 - BGP TTL trick (GTSM) and BGP TCP md5
 - Unicast RPF (uRPF)
 - Router security 101
- UPGRADES. A LOT OF UPGRADES

Security – which future ?

- No “big” “nation-wide” “critical infrastructure” issue recently (OK, root DNS servers get some packet love sometimes)
- IP/Data network infrastructure has become a commodity (until it's down)
- No focus on infrastructure security anymore (but the wake up call will be “funny”)

So where do people put security
research and resources into ?

NGN

(Next Generation Networks)



What are NGNs ?

- NGN = Next Generation Networks
- Everything seems to be NGN at the moment
 - Ethernet
 - IP DSLAMs
 - 3G/4G - WiMax
 - VoIP
 - Virtualization
 - IPv6 (just kidding, too bad today isn't April 1st)
- Mostly a marketing driven term
- But impact on industry:
 - “Legacy” technology being phased out
 - End-of-sale, end-of-support, etc.
 - “Forced” to look into NGN
 - CAPEX vs OPEX

NGNs because of web 2.0 ?

- Not really
- Web 2.0 doesn't have a real impact on the telco/SP industry
- Most visible impact:
 - Bandwidth usage
 - Features on clients (software, hardware, etc)
 - Always on(line)
- More flash crowd effects: how do you deal with this?
 - DDoS / Impact on service
- One interesting impact on the security border: the CPE/end device is TRUSTED

What's changing with NGN

- Everything is IP and Ethernet now
- More interfaces and protocols exposed to customers
- Local craft terminals moving from proprietary consoles to Ethernet/IP/DHCP/HTTP
- Lots of security features still/back in software (not in hardware)
- How to get those features across product ranges and vendors ?
- Shift of features towards edge, access, last/first mile
- But these features are not (often) security features

What's changing with NGN

- Lots of devices that never “saw” the “bad” Internet
- Hardware limitations (FPGA, ASIC, NP)
- Features vs power vs cooling
- We're moving up and down the protocol stack at the same time
 - More and more large layer 2 networks
 - Growing complexity at layer 7 (and above :)
 - Unclear Service Access Points (demarcation)
- Pen-testing/auditing is so '97
 - LAN technologies in the WAN
 - Carrier and enterprise products now “IP enabled”

Good/bad things with NGN security

- Some people have learned the lesson: you need security involved and looked at from day one
- Reality kicks in quickly:
 - First you need to make the solution “work”
 - It takes more time than expected
 - Non-key testing shifts in the calendar
 - You only end-up doing a high level assessment:
 - Paper based
 - Launch nmap/Nessus/IMPACT/etc
 - Sometimes you may run specific tools
 - Risk of DoS during other tests
 - Fuzzers
 - Network layer attacks
 - Etc.

Voice over IP

- What's the path to full-VoIP ?
 - VoIP in the entreprise
 - VoIP on the Internet
 - VoIP in the access layer
 - IMS core
 - What will really replace TDM ? And when ?
- New attack surface for legacy TDM networks
 - Reach SS7 over IP

IMS

- IMS = IP Multimedia Subsystem
- SIP “only” VoIP architecture (logical/physical)
- Try to converge 3G/4G, VoIP and Unified Messaging
- Edge-only security
 - SBC (Session Border Controllers)
 - WebApp Fws
- Core is open
 - Poor OS hardening
 - COTS OSes
- WebApps usually easier to take over than to try to get around the SBCs Back-to-Back User Agent (real TCP/UDP proxy)

IMS

- WebApps usually easier to take over than to try to get around the SBCs Back-to-Back User Agent (real TCP/UDP proxy)
- Expect more people to look into SBC security real soon
 - Key to the kingdom
 - All traffic (signaling and media) crossing them
 - May even handle CDRs (Call Detail Records)

IPv6

- IPv6 – part of NGN ? Not really.
- Source of nightmare for sure (today and to come)
- A global research lab
- Is there a real commercial driver yet ?
- Expect 6PE (IPv6 in IPv4 MPLS VPNs) to be more common (and Teredo of course ;-)
- Nice firewall piercing ahead
- From a Service Provider security point of view you can't, today, enforce the same security in v6 as in v4

IP/Ethernet DSLAMS

- Legacy DSLAMs
 - DSL termination
 - ATM backhaul
- Today
 - IP and Ethernet enabled DSLAMs
 - Considered an IP access router
- But
 - Less security features
 - ACLs, uRPF, etc
 - Plane separation
 - Limited TCAM size
 - Supports VLANs and trunks
 - Not

MSPP

- MSPP = Ethernet Multi-Service Provisioning Platform
- Goal is to replace legacy SDH networks and cross-connects
- End-to-end multi-point Ethernet, with point&click end-to-end provisioning
- Some people even think it could replace the Internet ;-)
- Just think of all layer 2 attacks you know. One will fit. We really need dugsong to finish dsniff-ng(n) :)
- Vendors are still focusing on making it work (think 50ms wrap time and co)

Virtualization

- We use VMware
- Entreprises start to virtualize their Data Center
- Service Providers virtualize networks, systems and firewalls
 - MPLS VPNs
 - MSPP (Ethernet)
 - Shared PBX hosting
 - Shared firewalls
 - Multi-tenant web front-ends for new services
 - Managed services portals
- Main issue: traffic and domain separation
- Especially in WebApps today
- In Ethernet-based networks tomorrow

Change Management

- What is really having an impact on your overall security with NGN ?
- CHANGE MANAGEMENT
- Decision makers are scared of allowing changes (upgrades/downgrades/workaround deployment)
- Today most of the deployed NGN-type solutions are never patched
- Workarounds are sometimes deployed
- Most of the vulnerable systems “hidden” behind first line of defense at the edge of the network

Summary / Conclusion

- Next Generations Networks are the future. There's no way back. Full stop.
- Governments seem more interested in NGN security as part of critical infrastructure protection efforts than vendors and some SPs
- NGN will keep security people busy for quite some time
- Q&A