SÉCURITÉ.ORG

JSSI 2007

L'opérateur passe au 2.0 : La sécurité des réseaux de nouvelle génération

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

COLT

La sécurité d'Internet

- Réseaux “historiques” (voix, FR/ATM, ligne louée) : sécurité par l'obscurité et/ou séparation physique (ex: 2600->SS7)
- Qu'est-ce qui nous empêchait de dormir...
- SNMP
- SQL Slammer (et ses amis)
- Cisco wedge bug <- 2003. Vous vous souvenez ?
  - Qui a vraiment déployé des mises à jour ?
  - Les filtres de transit (tACLs) sont-ils encore déployés ?
- BGP TCP window [pas vraiment]
- Botnets et DDoS

La sécurité d'Internet

- Qu'avons nous fait ? Beaucoup de choses. Trop peut-être?
  - Filtrage de route/préfixes
  - Détection de DDoS: Netflow
  - Réduction de DDoS: BGP (+ MPLS (+ Cleaning))
  - xACLs et MPLS Core hiding
  - QoS et Control Plane Policing (CoPP)
  - BGP TTL trick (GTSM) et BGP TCP md5
  - Anti-spoofing Unicast RPF (uRPF)
  - Sécurisation du routeur (rACL, services inutiles)
- DES MISES A JOUR. BEAUCOUP DE MISES A JOUR

Quel futur pour la sécurité réseau ?

- Pas d'incident de portée (multi)-nationale touchant une infrastructure critique récemment (les serveurs racines reçoivent des semblants de DDoS tout le temps)
- Le vol d'identité est plus à la mode et les botnets des fonctions “commerciales”
- Les réseaux IP/données sont devenus une commodité (jusqu'à ce qu'ils plantent)
- La sécurité des infrastructures réseaux n'est plus vraiment une priorité (mais le réveil risque d'être drôle voire douloureux)

Sur quoi travaillent donc tous les chercheurs et ingénieurs en sécurité ?

NGN

(Next Generation Networks)

Que sont les NGNs ?

- NGN = Next Generation Networks
- Toute technologie est proclamée NGN en ce moment:
  - Ethernet
  - DSLAMs IP
  - 3G/4G - WiMax
  - VoIP
  - Virtualisation
  - IPv6 (pas vraiment, le 1er avril est loin :-)
- Principalement un terme marketing
- Mais avec un impact fort sur l'industrie
  - Les technologies “anciennes” sont enlevées
  - Arrêt des ventes, fin de support, etc
  - L'industrie est “forcée” de s'orienter vers les NGNs
  - CAPEX vs OPEX

NGNs à cause du web 2.0 ?

- Pas vraiment
- Le web 2.0 n'a pas vraiment d'impact sur les FAI/opérateurs
- L'impact le plus visible se traduit par:
  - L'utilisation de bande passante
  - Les fonctionnalités côté client (logiciel et matériel)
  - Le mode “toujours connecté”
- ”Effet Slashdot” plus courant: comment le gérer ?
  - Détecté comme un DDoS / impact sur le service
- Un impact “intéressant”: le CPE (équipement côté client) fait partie du domaine de confiance (problème de frontière) surtout dans le domaine de l'ADSL

Ce qui change avec les NGNs

- Tout devient Ethernet et IP
- Plus d'interfaces et de protocoles exposés au client
- Les terminaux “local craft” (console locale) ne sont plus propriétaires mais supportent Ethernet/IP/DHCP/HTTP
- Beaucoup de fonctionnalités sécurité sont encore/de retour en logiciel (et non directement dans le matériel): performances dégradées
- Comment faire pour avoir ces fonctionnalités dans toute les gammes de produits et les différents vendeurs ?
- Les fonctionnalités se déplacent vers le réseau d'accès
- Mais malheureusement se sont rarement des fonctionnalités de sécurité

Ce qui change avec les NGNs

- Beaucoup d'équipements n'ont jamais “vécu” le “méchant” Internet
- Limitations matérielles (FPGA, ASIC, NP)
- Fonctionnalités vs consommation vs climatisation
- On monte et descend la pile OSI:
  - De plus en plus de grands réseaux Ethernet
  - Augmentation de la complexité à la couche 7 (et au dessus :)
  - Démarcation floue (Service Access Points)
- Un pen-test/audit ressemble à 1997
  - Technologies LAN dans le WAN
  - Produits opérateurs et d'entreprise auxquels on rajoute une interface IP

Sécurité NGN: le bon et le mauvais

- La leçon a été retenue: la sécurité doit faire partie du projet, et celà à partir du 1er jour
- Mais la réalité nous rattrape rapidement:
  - L'objectif devient de faire fonctionner la solution
  - Ce qui souvent prend plus de temps que prévu
  - Les tests qui ne sont pas critiques sont retardés
  - Et finalement l'audit sécurité devient très limité:
    - Sur papier uniquement
    - Un rapide test avec nmap/Nessus/IMPACT/etc
    - Quelque fois des outils spécifiques sont utilisés
    - Rarement des tests en parallèle: le risque de déni de service et/ou de perturbation d'autres tests est trop grand:
      - Injection aléatoire
      - Attaques réseau, etc.

La Voix sur IP

- Quel est le chemin pour atteindre le tout VoIP ??
  - VoIP dans l'entreprise
  - VoIP sur Internet
  - VoIP au niveau du réseau d'accès
  - IMS core
  - Remplacement du réseau TDM/PSTN ? Quand ?
- Nouvelle surface d'attaque pour les réseaux TDM
  - SS7 over IP
  - WebApps (IN, PABX, etc)

IMS

- IMS = IP Multimedia Subsystem
- Architecture physique et logique reposant sur SIP
- L'objectif est de faire converger les réseaux 3G/4G/VoIP
- La sécurité se limite aux frontières
  - SBC (Session Border Controllers)
  - WebApp Fws
  - Lien entre les WebApps et le back-end
  - Attaques au niveau applicatif (confiance dans les utilisateurs et les fournisseurs de services)
- Le coeur est ouvert
  - Systèmes d'exploitation peu patchés
  - S.E. COTS

IMS

- Il est souvent plus simple d'abuser d'une application web plutôt que d'essayer de contourner le Back-to-Back User Agent du SBC (vrai proxy TCP/UDP)
- De plus en plus de personnes vont étudier la sécurité des SBCs:
  - Porte d'entrée dans le royaume
  - Gère tout le trafic (signalisation et média)
  - Peut même gérer les CDRs (Call Detail Records)
  - Evolue pour devenir un modèle distribué

IPv6

- IPv6 – un NGN ? Pas vraiment.
- Une source de problèmes (aujourd'hui et dans le futur)
- Un laboratoire de dimension internationale
- Existe-t-il une demande commerciale ?
- 6PE (IPv6 dans des VPNs MPLS IPv4) sera sans doute plus courant (ainsi que Teredo ;-)
- Contournement de pare-feux
- Du point de vue du FAI il est impossible aujourd'hui de déployer les mêmes mécanismes de sécurité en IPv6 qu'en IPv4

DSLAMs IP/Ethernet

- DSLAMs historiques
  - Terminaison DSL
  - Concentration ATM (backhaul DSL)
- Aujourd'hui
  - DSLAMs avec IP et Ethernet
  - Comparable à un routeur d'accès IP
  - Mais moins de fonctionnalités de sécurité
    - ACLs ? uRPF ? etc
    - Séparation des plans
  - Limite de la taille de la TCAM
  - VLANs et trunks

MSPP

- MSPP = Ethernet Multi-Service Provisioning Platform
- L'objectif est de remplacer les réseaux SDH
- Service de bout-en-bout multi-point Ethernet, avec une interface de configuration permettant un déploiement point&click
- Certains pensent que MSPP pourrait remplacer l'Internet ;-)
- Réflechissez à quelques attaques de niveau 2, l'une d'elle fonctionnera. Dug Song devrait finir dsniff-ng(n) :)
- Les équipementiers focalisent leurs efforts sur les mécanismes de base (protection en moins de 50ms, etc)

Virtualisation

- Nous utilisons VMware
- Les entreprises commencent à virtualiser leurs serveurs
- Les opérateurs virtualisent les réseaux, les systèmes et les pare-feux
  - VPNs MPLS
  - MSPP (Ethernet)
  - Hébergement partagé de PBX
  - Pare-feu partagé
  - Applications web multi-utilisateurs/clients
  - Portails pour services gérés
- Problèmes principaux: la séparation de trafic et de domaines
- Dans les applications web aujourd'hui
- Dans les réseaux Ethernet demain

Gestion des changements

- Qu'est-ce qui a un impact important sur la sécurité des éléments NGN ?
- La gestion des changements
- Les décideurs ont peur d'autoriser les changements (mise à jour, retour à d'anciennes configurations, solutions temporaires)
- Aujourd'hui les réseaux NGN déployés sont rarement patchés
- De temps en temps des solutions temporaires sont déployées
- La majorité des systèmes vulnérables sont “cachés” derrière une première ligne de défense

Conclusion

- Les Next Generations Networks sont le futur. Il n'y a pas de retour possible en arrière.
- Les gouvernements semblent plus intéressés par la sécurité des réseaux NGNs que certains opérateurs et vendeurs
- Les déploiements de technologies NGN vont nous occuper pour un bon moment
- Et le client ? Peut-il encore faire “confiance” à son opérateur ? Doit-il s'en protéger ?
- Q&R