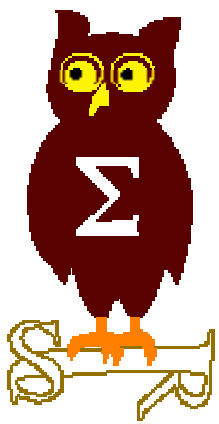
OSSIR
Groupe SUR

Réunion du 13 septembre 2005



Sécurité IOS

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Plan

- Introduction
- Historique des attaques sur IOS
- Etat de l'art
- Présentation de Mickael Lynn
- Evolutions futures de IOS
- La polémique
- Questions / réponses

Introduction

- Les attaques sur les routeurs ont toujours été l'objet de fantasmes
  - Les protocoles de routage (BGP, etc.)
  - Mais également les équipements eux-mêmes
- Jusqu'à présent, les seules attaques vues se limitent à
  - Du "brute force" de mot de passe …
  - Du DoS
    - Attaques TCP-RST, ICMP
    - Exploitation des failles zlib, SNMP, OpenSSH dans IOS
    - Vol de NetBlock
  - Du détournement de trafic après compromission
    - Phrack #56 – 0x0A : "things to do in Ciscoland when you're dead" (2000)
      - Etablissement d'un tunnel GRE
  - Et des attaques via HTTP
    - Le fameux /level/16/exec
- Les seuls incidents graves reportés publiquement découlent de bogues ou de mauvaises configurations
  - Ex. incident AS 7007 (1997), Cisco Wedge Bug

Introduction

- **Plusieurs facteurs contribuent à la crédibilité des rumeurs d'attaques**
  - **Monoculture "Cisco"**
  - **Rôle critique des routeurs dans les infrastructures**
  - **Absence d'outils de protection natifs pour routeurs**
    - **Protections externes type TripWire sur la configuration**
- **Des développements récents ont eu lieu sur le sujet des attaques du système d'exploitation Cisco : IOS**
  - **C'est le sujet de cette présentation**
- **Le projet HoneyNet s'est équipé de "HoneyRouters" ☺**

Historique des attaques sur IOS

- **Premier papier notable sur le sujet**
  - **Auteur : FX du groupe Phenoelit**
    - **http://www.phenoelit.de/**
  - **Date : 2002 (BH US 2002, Defcon X)**
  - **Principe de fonctionnement du *heap* et exploitation**
    - **http://www.phenoelit.de/ultimaratio/**
  - **Exploitation en combinant par exemple :**
    - **"HTTP GET" BoF**
      - **http://www.cisco.com/warp/public/707/cisco-sn-20030730-ios-2gb-get.shtml**
    - **"UDP Data Leak"**
      - **http://www.cisco.com/warp/public/707/cisco-sn-20030731-ios-udp-echo.shtml**

Historique des attaques sur IOS

- **Puis …**
  - **Auteur : toujours FX …**
  - **Date : fin 2002 (CCC 2002, BH US 2003)**
  - **Une exploitation complète :**
    - **"Heap Overflow" dans le protocole OSPF**
      - **http://www.cisco.com/warp/public/707/cisco-sn-20030221-ospf.shtml**
    - **Code d'exploitation disponible**
      - **http://www.phenoelit.de/ultimaratio/OoopSPF.c**
    - **Ecrase la NVRAM (et change les mots de passe)**
  - **Note : requière une configuration matérielle particulière sur le routeur pour fonctionner**

Etat de l'art

- **Avec le temps, des informations ont fui**
  - **Code source IOS**
    - **Le code source s'est retrouvé dans la nature au moins 2 fois de manière certaine**
      - **IOS 11.2 : se trouve sur eMule …**
      - **IOS 12.3 : http://www.securitylab.ru/news/213852.php**
    - **Note : "il parait" que le code source se trouve sur les portables de tous les *senior engineers* Cisco …**
  - **Documents**
    - **Officiels**
      - **"Inside Cisco IOS Software Architecture" (Cisco Press)**
      - **Note : certains documents anciens sont très détaillés !**
    - **Ou non …**
      - **"Cisco IOS Programing Guide"**

Etat de l'art

- Analyse logicielle
  - Possibilité de débogage à distance via GDB*
    - * En fait : rommon, IOS lui-même, et "remote gdb"
    - http://www.xfocus.net/articles/200307/583.html
    - IOS 11 est compatible "gdb" mais les fonctions disponibles sont plutôt limitées
      - Read / Write [reg | mem]
      - Continue / Step / Kill
      - Last signal
      - Toggle Debug
    - IOS 12 : pas mieux
  - Analyse de firmwares
    - http://packetstormsecurity.org/cisco/
      - Cisco6509_Reverse.tar.bz2
  - Analyse de coredumps
    - Très peu d'informations disponibles
    - Analyse en ligne par Cisco

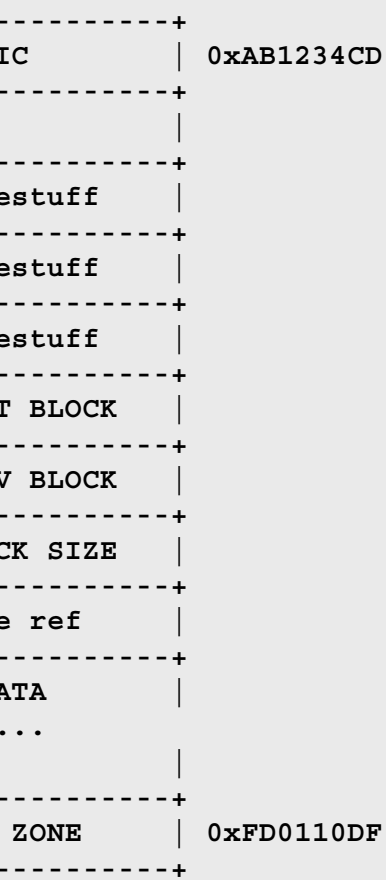
Etat de l'art

- Au niveau matériel
  - Un cœur Motorola 68000 (m68k), MIPS ou PPC
    - Evolution vers x86 ?
  - Des ASIC et des FPGA autour
  - De la Flash, de la NVRAM, de la RAM, …
- La plupart des données sont stockées dans le tas (*heap*)
  - IOS utilise très peu la pile (*stack*)
- Le problème du m68k : absence de MMU !
  - Il est impossible de protéger des pages mémoire contre l'écriture
  - Donc IOS effectue une vérification d'intégrité des pages mémoire toutes les 30 secondes !
    - Reload du système en cas de problème détecté
- Attaques possibles
  - Exploitation de "Heap Overflow" dans IOS (fenêtre 30 secondes)
  - Exploitation de Mini-IOS au reboot (fenêtre 5-7 secondes)

Etat de l'art

Structure du tas (d'après FX)

Bloc alloué



Header additionnel pour les blocs libres

Présentation de Michael Lynn

- **Au départ : un "heap overflow" dans le support IPv6 ou une faille plus ancienne ?**
  - **http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml**
- **Ensuite : un "shellcode" exécuté sur la machine**
  - **"Connect back shell" complet !**
- **Les nouveautés :**
  - **Fiabilise l'exploitation des "Heap Overflow" par rapport à la technique de FX**
  - **En faisant croire au routeur que la réinitialisation est en cours, il est possible de franchir la barrière des 30 à 60 secondes**
  - **Désactiver les interruptions hardware pour gagner encore du temps**
  - **La corruption générale du tas laisse 2 à 5 minutes avant le crash**
- **Michael Lynn estime que 1 bogue sur 10 est exploitable**
- **Et surtout … les technologies de virtualisation prévues dans les prochains IOS vont rendre les adresses beaucoup plus prédictibles !**

Evolutions futures de IOS

- **L'avenir d'IOS : modularité, virtualisation**
  - **IOS-XR tourne sur QNX-Neutrino**
    - **A destination des séries 12000 pour le moment**
    - **Développement en cours pour séries 6000 et 7600 (?)**
  - **Les images Cat6k vont être vendues avec une liste d'options**
    - **http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd80313e09.shtml**

- **Evolution des avis de sécurité Cisco**
  - **"Impact : successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device *or execution of arbitrary code*. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices."**

La polémique

- Quelques semaines avant BH US 2005, Cisco s'affole
  - 2000 CDs contenant les supports sont détruits
  - Des dizaines de gens envoyés par Cisco pour arracher les 20 pages de présentation
    - Opération filmée : une mauvaise opération de PR …
    - http://downloads.oreilly.com/make/cisco.mov
  - Michael accepte de faire une présentation sur VoIP à la place
    - Mais change son fusil d'épaule au dernier moment !
    - Il démissionne d'ISS et effectue sa présentation
- Les transparents se retrouvent évidemment sur Internet quelques jours après
  - http://cryptome.org/lynn-cisco.zip
- Les questions
  - Michael Lynn a-t-il violé le NDA qui liait ISS et Cisco ?
  - Est-il un chevalier du Bien ou travaille-t-il à sa carrière ? ☺

La polémique

- 5 jours après, McAfee prétend avoir une signature dans son IDS
  - http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050803_181545.htm
  - Mais pour quelle attaque ???
- Compromission de la base d'utilisateurs du site Cisco.com
  - http://software.silicon.com/security/0,39024655,39150991,00.htm
  - Peu de temps après la conf' ☺
  - Vol (?) de tous les login / mot de passe du site support
    - Permet ainsi de télécharger *toutes* les versions de IOS
  - Les utilisateurs doivent téléphoner au support pour réactiver leur compte

Questions / réponses

- **Questions / réponses**
- **Remerciements**
  - **Nicolas Fischbach**
  - **L'équipe EADS / DCR / SSI**
    - **Et particulièrement Philippe Biondi**