« Couvrez ces protocoles que je ne saurais voir.
Par de pareils objets, l'IoT est vulnérable,
Et cela fait venir de coupables pensées »

(Le Tartuffe, Molière, kind of)

Marc Dacier

marc.c.dacier@gmail.com

A propos du travail présenté aujourd'hui

- Résultat d'un projet de semestre et d'un stage de l'étudiant Dhia Farrah (Sup Telecom Tunis) sous ma supervision, et d'un autre stage en cours avec Elyssa Boulila (Sup Telecom Tunis)
- Le travail sur les attaques MITM a été accepté pour publication à WOOT 2021, colocalisé avec IEEE S&P.
- La présentation est prévue pour le 27 mai 2021 (par Dhia Farrah).
- Les détails techniques sont dans la publication.

Plan de l'exposé

- ***Introduction***
  - Fonctionnement des protocoles « zeroconf »
  - 4 attaques et leurs conséquences
  - WPAD, DHCP et ICMP V6
- Conclusions et futures directions

Nos fondations sont elles solides?

- « Network is the computer » … de Sun Microsystems à Cloudflare
- Nombre de protocoles datent d'une époque « sans attaque »
- Aujourd'hui, ils sont redécouverts et réutilisés par des applications cherchant la simplicité, ignorant les risques sous jacents.
- Personne ne peut pousser sur le bouton « Pause »

Zeroconf, WPAD, DHCP, IPV6 RA

- Notre point de départ: les protocoles zéro conf
- … puis WPAD …
- Et les interactions entre eux .. Et DHCP …

Plan de l'exposé

- Introduction
  - ***Fonctionnement des protocoles « zeroconf »***
  - 4 attaques et leurs conséquences
  - WPAD, DHCP et ICMP V6
- Conclusions et futures directions

Zeroconf Protocols

- Transposition au monde IP du « Name Binding Protocol » (NBP) utilisé dans les années 1980 dans Appletalk!
- Plusieurs variantes existent basées sur les mêmes principes: IPV4ALL, LLMNR, mDNS, DNS-SD, Bonjour …
- Février 2013, 2 RFCs par S. Cheshire et M. Krochmal: mDNS (RFC 6762) et DNS-SD (RFC 6763)

Principes (1/2)

- Permettre aux machines arrivant dans un réseau de se configurer sans l'aide de serveurs extérieurs, en particulier sans serveur DHCP ou DNS.
- Concrètement:
  - Choisir une adresse IP
  - Choisir un nom (FQDN)
  - Choisir un nom pour les services qu'elles offrent

Principes (2/2)

- Etape 1: demander si l'attribut désiré est déjà utilisé par quelqu'un sur le réseau
- Etape 2: en l'absence de réponse, annoncer cet attribut comme étant le sien.

- En cas de conflit: protocole de résolution de conflit

- Exemples:
  - requête ARP pour l'adresse IP W.X.Y.Z puis utilisation de cette adresse en cas d'absence de réponse
  - Requête sur le canal multicast pour l'adresse IP associée au nom NNN et, en cas d'absence de réponse, annonce de sa propre adresse associée à ce nom.

3 attributs essentiels

- L'adresse IP d'une machine

- Son nom local (local domain name)
  - HP_XXX.local

- Le(s) nom(s) de service(s):
  - HP [34B70]._ipp._tcp.local
    - Selon la nomenclature de définition de services publiée dans le RFC 6763

Appairage des attributs

- Un nom de domaine est associé à une adresse IP
- Tout nom de service est associé à un nom de domaine
- Pour imprimer il faut donc:
    1) Trouver les services d'impression offerts
    2) En choisir un et obtenir ses caractéristiques
    3) Obtenir le nom de la machine qui fournit ce service
    4) Obtenir l'adresse IP associé à cette machine
    5) Etablir la connection avec l'adresse IP obtenue

3 Modes de fonctionnement

1. Phase d'initiation:
    1. Une nouvelle machine cherche à obtenir et annoncer son IP, nom de domaine et nom de service
    2. En cas de conflit, le nouvel entrant est le seul à devoir le résoudre
2. Phase de fonctionnement:
    1. Toute machine écoute sur le canal multicast et répond aux demandes de découvertes de service (DNS-SD)
        1. Si la requête est de type « QM », la réponse est en multicast
        - Si la requête est de type « QU », la réponse est en unicast
    - Si deux machines répondent avec des informations conflictuelles, les deux doivent démarrer le protocole de résolution de conflit

3ème mode de fonctionnement: résolution de conflit

A. 1 machine en phase d'initiation et l'autre en fonctionnement:
   - Seule la machine en phase d'initiation modifie les infos conflictuelles

B. 2 machines en phase de fonctionnement:
   - Les deux machines reviennent en mode phase d'initiation

C. 2 machines en phase d'initiation:
   - L'ordre lexicographique des informations conflictuelles détermine la machine qui doit changer ses attributs et celle qui les conserve:
     - La plus faible valeur perd

Définition du conflit (RFC 6762)

[…] A conflict occurs when a Multicast DNS **responder** has a unique record for which it is currently **authoritative**, and it receives a Multicast DNS response message containing a record with the same name, rrtype and rrclass, but inconsistent rdata. […]

Whenever a Multicast DNS responder receives any Multicast DNS response (solicited or otherwise) containing a conflicting resource record […] the Multicast DNS responder MUST immediately […] go through the start up steps […]. The protocol used in the Probing phase will determine a winner and a loser, and the **loser MUST cease using the name**, and reconfigure.

It is very important that any host receiving a resource record that conflicts with one of its own **MUST take action** as described above.

Plan de l'exposé

- Introduction
  - Fonctionnement des protocoles « zeroconf »
  - ***4 attaques et leurs conséquences***
  - Discussion semi philosophique
- Conclusions et futures directions

Plan de l'exposé

- Introduction
  - Fonctionnement des protocoles « zeroconf »
  - ***4 attaques et leurs conséquences***
  - WPAD, DHCP et ICMP V6
- Conclusions et futures directions

Marc Dacier, 11/05/2021

Principes des attaques MITM

- Un client désire utiliser un service distant (cible) sur son réseau local (impression, streaming, stockage, scan, etc.…)
- Il utilise mDSN et DSN-SD pour trouver les infos nécessaires à l'initiation de la connection TCP
- L'attaquant parvient à substituer son adresse IP à l'adresse IP valide et se positionne en proxy entre client et cible
- Si la connection n'est pas chiffrée *de bout en bout*, toutes les manipulations possibles sont permises sur le flux, sans que la victime puisse s'en rendre compte.

4 familles d'attaques

1. **Convaincre le client** d'associer une fausse adresse IP à un nom de domaine existant (attaque ciblée)
2. **Convaincre le client** d'associer un faux nom de domaine à un nom de service existant (attaque ciblée)
3. **Convaincre la cible** de changer son nom de service pour le lui voler (attaque globale)
4. **Induire l'utilisateur final** en erreur dans son choix de service (attaque globale)

YAKA, FOKON, TAKA, etc….

- Le diable se cache dans les détails
- Eléments qui entrent en compte dans la réussite d'une attaque:
  - OS du client et/ou de la cible
  - Application fonctionnant sur le client et/ou la cible
  - L'état du client et/ou de la cible au moment de l'attaque
  - L'implémentation de l'attaque (cache flush bit, weight, etc.)
  - Un peu de réussite pour gagner les courses critiques

Expériences réalisées

- 2 clients:
  - Ubuntu 18.04 LTS
  - Windows 10
- 1 attaquant:
  - Kali Linux 5.8.0
- 2 cibles:
  - Apple TV (3rd gen model A1469), soft version 7.2.2
  - HP Office Jet Pro 6230 printer

- 300 expériences distinctes réalisées et documentées dans le papier WOOT 2021

Leçon : 1) QU vs QM

- Le protocole de résolution de conflit n'est enclenché que par le propriétaire de l'information
  - Si il ne voit pas l'information, le conflit n'est ni détecté ni résolu
- Le protocole prévoit de pouvoir poser des questions en multicast tout en acceptant des réponses envoyées en unicast (question QU)
    - La possibilité d'écraser des informations précédentes (cache flush bit) complète l'histoire.

Leçon : 2) QU vs QM (suite)

- Certaines implémentations acceptent des réponse en unicast alors qu'elles ont envoyé des requêtes de type QM

Leçon : 3) réponses non demandées

- Le protocole prévoit que des réponses multicast non demandées peuvent être envoyées et doivent être prises en considération (ex. paquets goodbye)
- Certaines implémentations acceptent de telles réponses non seulement en multicast mais aussi en unicast !

Leçon 4: Non-conformité et sécurité

- Lorsque 2 machines détectent un conflit entre eux, ils DOIVENT passer en mode de fonctionnement d'initiation afin de résoudre le conflit.
- Si un des deux refuse de changer de mode, l'autre, par définition du protocole, sera obligé de changer ses informations pour résoudre le conflit.

Leçon 5: Non-conformité et sécurité (suite)

- Lorsque 2 machines détectent un conflit entre eux, ils DOIVENT passer en mode de fonctionnement d'initiation afin de résoudre le conflit.

- Si le perdant du protocole de résolution refuse de changer les attributs en conflit, il s'en suit un déni de service.
  - `RFC6762: […] After one minute of probing, if the Multicast DNS responder has been unable to find any unused name, it should log an error message to inform the user or operator of this fact. This situation should never occur in normal operation. […]`

Plan de l'exposé

- Introduction
  - Fonctionnement des protocoles « zeroconf »
  - 4 attaques et leurs conséquences
  - ***WPAD, DHCP et ICMP V6***
- Conclusions et futures directions

L'arbre qui cache la forêt

- Les protocoles zeroconf ne sont pas l'exception qui confirme la règle, bien au contraire.

- Exemple:
  - WPAD et ses interactions avec DHCP et DNS

WPAD

- Web Proxy Auto Discovery:
  - Défini dans un « Internet Draft » qui a expiré en décembre 1999 !
  - Néanmoins implémenté dans la plupart des browsers et OS !

- Le protocole permet de trouver un serveur WPAD d'où télécharger un fichier javascript pour configurer les proxys….

- Dès 2005, la « bonne idée » du javascript est mise en lumière.
- En 2017, le « project zero » de google en fait une analyse systématique:
  - **aPAColypse now: Exploiting Windows 10 in a Local Network with WPAD/PAC and JScript**

https://googleprojectzero.blogspot.com/2017/12/apacolypse-now-exploiting-windows-10-in_18.html

WPAD et DHCP

- Comment trouver ce serveur ?
  - 1ère option: DHCP, option 252
- L'option 252 n'est pas officiellement associée à WPAD (!) car aucun RFC n'y correspond.
- DHCP est lui-même vulnérable à de nombreuses attaques réseaux.
- Windows, et non les browsers, gère cette option
  - Info stockée dans le registry
  - L'info survit à un reboot … !!!

WPAD et SLP

- Comment trouver ce serveur ?
  - 2ème option: SLP
- SLP: Service Localisation Procotol (RFC 2608, 1999)
  - protocole équivalent à MDNS et DNS-SD tombé en désuétude mais encore supporté par certains OS.
- Exercice: appliquez à SLP toutes les attaques contre MDNS et DNS-SD

WPAD et SLP

- Comment trouver ce serveur ?
  - 3ème option: DNS
- Recherche d'un serveur dont le nom serait :
  - wpad.<nom de réseau>
    - Bonjour la fuite des requêtes sur l'Internet
  - Wpad.local
    - Bonjour les attaques de MITM MDNS et DNS-SD … ☹

WPAD: synthèse

Une autre illustration d'un protocole très vulnérable, très utilisé et qui fonctionne en s'appuyant sur d'autres protocoles très vulnérables et très utilisés

Et tout cela sans que l'immense majorité des utilisateurs et d'administrateurs s'en doutent le moins du monde

Encore … ?

- CVE 2020 16898: Router Advertisement in IPV6
- Excellent blog Quarkslab dédié au sujet :
  - https://blog.quarkslab.com/beware-the-bad-neighbor-analysis-and-poc-of-the-windows-ipv6-router-advertisement-vulnerability-cve-2020-16898.html
  - "… a stack-based buffer overflow in the IPv6 stack of Windows, which can be remotely triggered by means of a malformed Router Advertisement (RA) packet…"

Plan de l'exposé

- Introduction
  - Fonctionnement des protocoles « zeroconf »
  - 4 attaques et leurs conséquences
  - WPAD, DHCP et ICMP V6
- ***Conclusions et futures directions***

Réseaux et sécurité

- Les attaquants ont, historiquement, ciblé les systèmes hôtes
- Les hôtes commencent à mieux se protéger
- La « softwerisation des réseaux » explose (IoT, OT, voiture autonome, cloud, SDN, NFV, 5G, …)
- Elle constitue le ventre mou de la sécurité.
  - Cet exposé en est un exemple.
- Elle va bientôt connaitre (à nouveau) son heure de gloire.

Marc Dacier, 11/05/2021

Merci pour votre attention

« Par ma foi! Il y a plus de vingt ans que nos machines usent des protocoles zeroconf sans que j'en susse rien, et je vous suis le plus obligé du monde de m'avoir appris cela »

(libre appropriation de
« Le Bourgeois gentillhome » de Molière)

Marc Dacier, 11/05/2021