École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

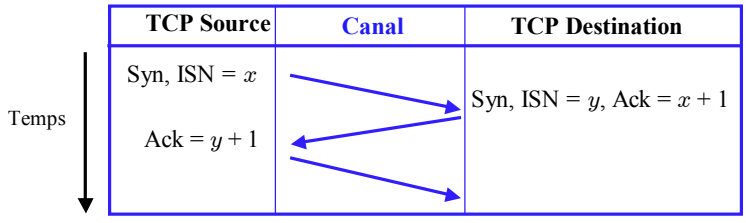
Politique de disponibilité du protocole TCP-IP

Frédéric Cuppens *Nora Cuppens-Boulahia*
www.enst-bretagne.fr

get

Le protocole TCP-IP

- Protocole connecté
- Utilisation d'un numéro d'ordre
  - ISN : Initial Sequence Number
- L'ISN est incrémenté pendant les échanges d'établissement de la session



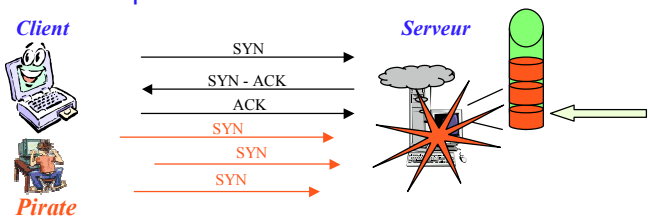
nora.cuppens@enst-bretagne.fr

ENST Bretagne

get

L'attaque SYN-FLOODING

- Attaque DoS sur les réseaux IP
- Connexion à moitié ouverte : le serveur insère les informations d'ouverture dans sa pile
- Le serveur attend la réponse (ack) du client et conserve dans sa pile des connexions à moitié ouvertes



- Le client n'envoie pas de ack pour ouvrir la connexion
- Trop de connexions à moitié ouvertes conduisent à un déni de service
- Besoin de définir une taille limite de la pile pour éviter un crash système : Backlog

Objectifs

- Spécification du protocole TCP-IP
- Étude des mécanismes de protection
  - Backlog
  - Timer pour éliminer les demandes non acquittées
  - SYN-COOKIE
- Application de Nomad
  - Expression de la politique de disponibilité
- Mise en œuvre des mécanismes de protection
  - Expression sous forme d'aspects

Spécification du protocole

- Gestion des sources
  - N sources différentes
  - Messages possibles
    - → SYN_i : la source i envoie un message SYN
    - → $SPOOFED\_SYN_i$: une source envoie un message SYN en se faisant passer pour i
    - → SYN_ACK_i : la source i reçoit un message SYN_ACK
    - → ACK_i : la source i envoie un message ACK
    - → $RESET_i$: la source i envoie ou reçoit un message RESET
  - Source non malveillante
    - → $HONNEST_i$: la source i est honnête
    - → Une source honnête n'enverra pas de messages de la forme $SPOOFED\_SYN_i$

Spécification du protocole

- Gestion de la pile
  - MAX = taille de la pile
  - $FREE_k$: la case k de la pile est libre
  - $BUSY_{k,i}$: la case k de la pile est occupée par la source i
  - $FREE_{\leq k}$: l'une des k premières cases de la pile est libre
  - $FREE_{=k}$: la case k est la première case libre de la pile

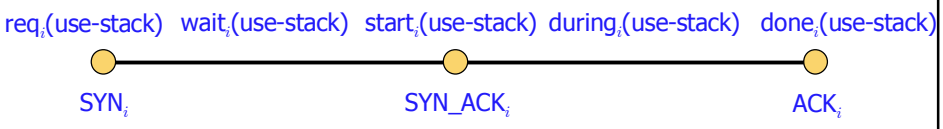
  - Axiomes
    - → $FREE_{\leq 1} \leftrightarrow FREE_1$
    - → $k > 1 \rightarrow (FREE_{\leq k} \leftrightarrow (FREE_{\leq k-1} \vee FREE_k))$
    - → $FREE_{=1} \leftrightarrow FREE_1$
    - → $k > 1 \rightarrow (FREE_{=k} \leftrightarrow (\neg FREE_{\leq k-1} \wedge FREE_k))$
    - → $\neg\, FREE_k \leftrightarrow \exists i,\, BUSY_{k,i}$

Spécification du protocole

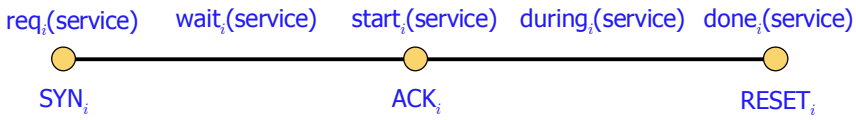
- Axiomes côté serveur
  - $(SYN_i \wedge FREE_{=k}) \rightarrow \oplus(SYN\_ACK_i \wedge BUSY_{k,i})$
  - $(SPOOFED\_SYN_i \wedge FREE_{=k}) \rightarrow \oplus(SYN\_ACK_i \wedge BUSY_{k,i})$
  - $(ACK_i \wedge BUSY_{k,i}) \rightarrow \oplus(FREE_k)$
  - $(RESET_i \wedge BUSY_{k,i}) \rightarrow \oplus(FREE_k)$
- Axiome côté client
  - $(SYN\_ACK_i \wedge HONNEST_i) \rightarrow \oplus(ACK_i \vee RESET_i)$

Application de Nomad

- Utilisation des ressources de la pile



- Exécution du service



  - $(SYN\_ACK_i \wedge HONNEST_i \wedge wait_i(service)) \rightarrow \oplus(ACK_i)$
  - $(SYN\_ACK_i \wedge HONNEST_i \wedge \neg\, wait_i(service)) \rightarrow \oplus(RESET_i)$

Politique de sécurité

- Prévention du débordement de pile
  - Côté client
    - $F(\text{SYN}_i \mid \neg\ \text{FREE}_{\leq MAX})$
  - Contre-partie côté serveur
    - $O(\oplus\text{REJECT}_i \mid (\text{SYN}_i \wedge \neg\text{FREE}_{\leq MAX}))$
    - REJECT_i: le serveur rejette le message envoyé par la source i
  - Aspect
    - $\text{SYN}_i \wedge \neg\text{FREE}_{\leq MAX} \rightarrow \oplus\text{REJECT}_i$
    - Tissage du backlog dans la spécification du protocole TCP-IP

Politique de sécurité

- Suppression des demandes qui ne sont pas acquittées après un certain délai
  - Côté client
    - $O(\bigcirc^{\leq d}\ \text{ACK}_i \mid \text{SYN\_ACK}_i)$
  - Contre-partie côté serveur
    - $O(\bigcirc^{d}\ \text{RESET}_i \mid \text{SYN\_ACK}_i \wedge \neg\bigcirc^{\leq d}\text{ACK}_i)$
  - Aspect
    - $\text{SYN}_i \wedge \neg\bigcirc^{\leq d}\ \text{ACK}_i \rightarrow \bigcirc^{d}\ \text{RESET}_i$
    - Tissage d'un timer dans la spécification du protocole TCP-IP

Politique de sécurité

- Disponibilité du service pour les sources non malveillantes
  - $O(\bigcirc^{\leq d} \text{ACK}_i \mid \text{SYN}_i \wedge \text{HONNEST}_i)$
    - ➔ $O(\bigcirc^{\leq d} \text{start}_i(\text{service}) \mid \text{req}_i(\text{service}) \wedge \text{HONNEST}_i)$
  - Aspect côté serveur
    - ➔ $(\text{SYN}_i \wedge \neg \text{FREE}_{\leq MAX}) \rightarrow \oplus \text{SYN\_COOKIE}_i$
    - ➔ $(\text{SPOOFED\_SYN}_i \wedge \neg\ \text{FREE}_{\leq MAX}) \rightarrow \oplus \text{SYN\_COOKIE}_i$
  - Aspect côté client
    - ➔ $(\text{SYN\_COOKIE}_i \wedge \text{HONNEST}_i \wedge \text{wait}_i(\text{service})) \rightarrow \oplus \text{ACK}_i$
  - Propriété de sécurité à prouver
    - ➔ $(\text{SYN}_i \wedge \text{HONNEST}_i) \rightarrow \bigcirc^{\leq d} \text{ACK}_i$
  - Remarque
    - ➔ Il faut supprimer l'aspect : $(\text{SYN}_i \wedge \neg\ \text{FREE}_{\leq MAX}) \rightarrow \oplus \text{REJECT}_i$

nora.cuppens@enst-bretagne.fr

Conclusion … et suite des travaux…

- Prise en compte implicite des rôles et des ressources
- Nomad pour exprimer la politique de dispo
- Identifications des aspects dispo pour la mise en œuvre

- Prise en compte explicite des ressources critiques
- La disponibilité dans les réseaux ad-hoc
- Application de la logique alternée et mise en œuvre RML

nora.cuppens@enst-bretagne.fr