Non classifié

Correspondance de règles sécurisée et confidentielle

Février 2020

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Plan de présentation

- Contexte
- Vision à long terme
- Le défi
- Questions

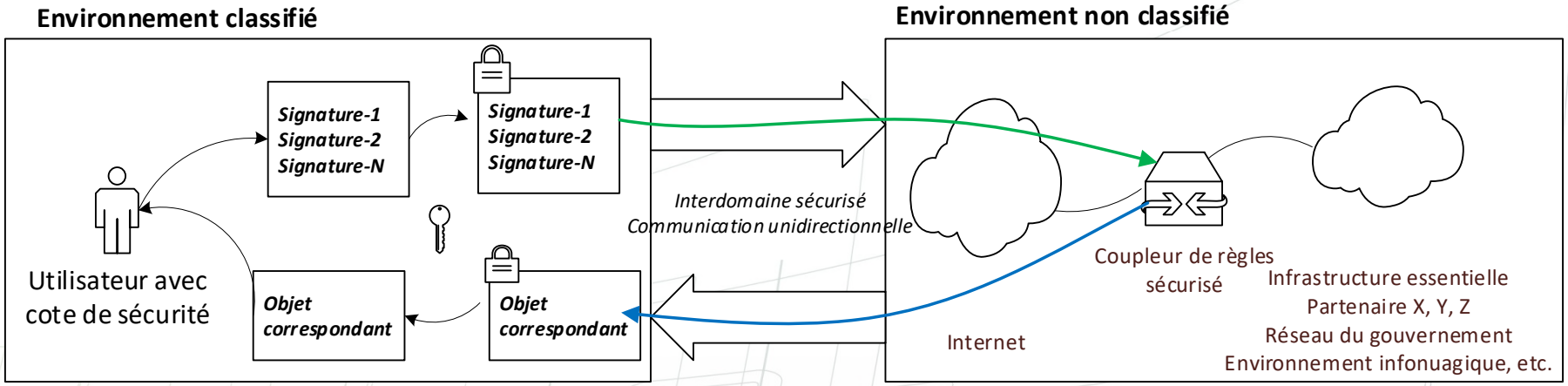
Contexte

- La collectivité de la sécurité et du renseignement (S&R) a accès à de l'information sensible, qui a trait aux cybermenaces, qu'il n'est pas toujours possible de diffuser auprès du public.
- Cette information peut être codée avec un degré de précision suffisant pour détecter et surveiller la présence d'auteurs malveillants dans le trafic réseau ainsi que dans la télémesure de systèmes, ce qui permet d'identifier lesdits auteurs ainsi que leur mode d'opération
- Cette information sensible sera classifiée (pour une période de temps)
- Nous aimerions intégrer des signatures de cybersécurité classifiées dans des équipements qui pourraient être déployés dans les réseaux non classifiés, notamment ceux du gouvernement ou ceux des infrastructures nationales essentielles.

Vision à long terme

Être en mesure d'évaluer des signatures sur des paquets réseau dans des environnements non sécurisés, de telle façon que ni les signatures ni le trafic réseau correspondant à ces signatures ne seront révélés

Système envisagé (1)



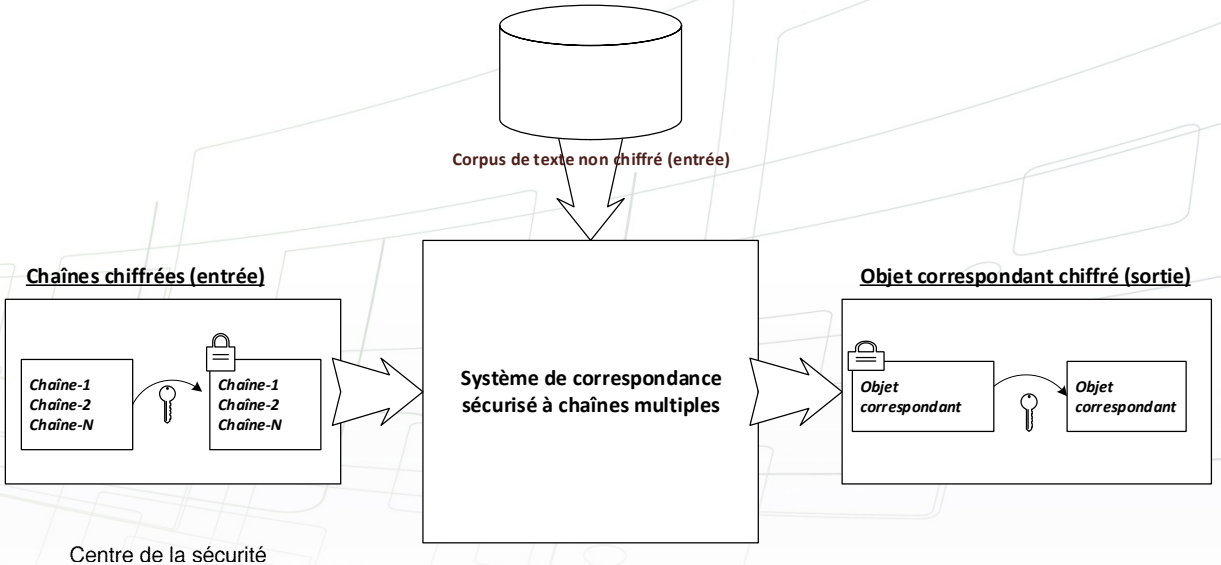
Système envisagé (2)

- Les signatures sont similaires au signatures que nous retrouvons dans les système de détection d'intrusions comme Suricata et SNORT (https://suricata-ids.org, https://www.snort.org)

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick
in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK ";
pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124;
classtype:trojan-activity; sid:2008124; rev:2;)
```

Le défi

- Le défi proposé est une version simplifiée du système futur idéal. Les signatures sont de simples chaînes de caractère et le trafic réseau est remplacé par un corpus de texte



Résultats essentiels

- Être en mesure d'appliquer la correspondance d'un ensemble de règles simples pour un corpus de texte non chiffré.
- Comporter des règles aussi élémentaires que de simples chaînes de caractères.
- Garantir la confidentialité des règles (chiffrement) pendant le processus de correspondance (*matching*).
- Empêcher toute possibilité de déduction des règles suivant l'analyse de l'exécution des instructions du système correspondant pendant la durée d'exécution.
- Garantir la confidentialité (chiffrement) des objets correspondants (objets qui indiquent la correspondance entre les règles et les portions de corpus). En d'autres termes, les observateurs non autorisés ne pourraient jamais savoir quelle règle correspond à quelle portion du corpus.
- Fournir des mécanismes permettant de chiffrer/de déchiffrer les signatures ainsi que les « objets correspondants » au moyen d'une clé qui ne serait accessible qu'aux intervenants titulaires de l'habilitation de sécurité requise.
- Fournir un système de correspondance de règles qui s'exécute en toute intégrité. Les règles correspondent sans erreur, exactement comme si le système devait s'exécuter sans chiffrement.
- S'intégrer à un espace réduit équivalent à quatre espaces dans le bâti standard d'un centre de données.

Résultats additionnels

- Être extensibles pour parvenir à prendre en charge un nombre accru de signatures (la cible est de 20 000).
- Permettre la spécification de règles à complexité accrue. Le but est de parvenir à répliquer le langage de spécification des règles Suricata (SDI de source ouverte).
- Développer l'aptitude à prendre en charge les signatures particulièrement complexes. Par exemple, la correspondance de chaînes avec des caractères de remplacement (*wild cards*), les règles booléennes simples à plusieurs variables et les expressions régulières.
- Être en mesure d'appliquer la correspondance des signatures dans un trafic réseau mis en paquets et non chiffré (par opposition à un simple corpus de texte non chiffré).
- Afficher un degré de performance, malgré la taille réduite, permettant d'appliquer la correspondance de 20 000 signatures à un débit de 1 Go/s de trafic réseau mis en paquets.
- Disposer d'une extensibilité (sur le plan des algorithmes) qui soit relative au nombre de chaînes; leur longueur et le nombre d'appariements dans le corpus doivent donc correspondre à la complexité des algorithmes de correspondace multichaîne qui s'exécutent sans chiffrement.
  O(size_of_text + number_of_match_occurences_in_corpus).

Questions et réponses anticipées

- Q: Quel est le niveau de sécurité requis?
  - R: Pour un niveau de confidentialité TOP SECRET, nous requérons l'équivalent sécuritaire à AES (Voir FIPS Pub 197) avec des clés de 256 bits
- Q: Quel information devrait être retournée lors d'une correspondance?
  - R: Nous devons savoir quelle signature à été localisée à quel endroit dans le texte ou dans quel paquet (IP 5-tuple pour les paquets)
- Q: Quel volume de donné est acceptable pour la sortie du système?
  - R: Nous devons tenter de minimiser le volume de donné en sortie (la taille des objets correspondants). L'utilisation du « batching » est acceptable lors de l'implémentation du système.
- Q: Est-ce que toutes les signatures seront classifiées ou seulement un sous-ensemble?
  - R: Toutes les signatures seront classifiées
- Q: Quelle est la taille assumée des paquets? (Combien de paquets par seconde dans le flux de 1 Gbps, ou quelle est la taille maximale d'une chaîne de caractères comparée?)
  - R: Dans le cas du trafic réseau en paquets, nous pouvons assumer que les paquets auront une taille maximale de 1500 octets.

Questions?