Faire face aux **cybermenaces** $\Rightarrow$ **détecter** (les attaques) $\wedge$ **former** (des experts en SSI)

Ludovic Mé
ludovic.me@supelec.fr
http://www.rennes.supelec.fr/ren/perso/lme/

7 juin 2013

Supélec

Livre blanc 2013 [1]

Cyberattaques == une menace majeure à forte probabilité

- Les intrusions visant l'état, les opérateurs d'importance vitale, ainsi que les grandes entreprises nationales ou stratégiques du pays sont aujourd'hui quotidiennes [p4]
- Des informations sont méthodiquement collectées pour rendre possible, dans une situation de conflit, une attaque de grande envergure [p4]

Livre blanc 2013 [2]

Cyberespace == champ de confrontation à part entière

- S'agissant de la protection du territoire national et des ressortissants français, les risques et les menaces pris en compte par la stratégie de défense et de sécurité nationale sont [p47] :
  - les agressions par un autre état contre le territoire national
  - les attaques terroristes
  - les cyber-attaques
- La capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale [p105]

Livre blanc 2013 [3]

Protection, détection/identification ... et riposte

- Mettre en place une posture robuste et résiliente de protection des systèmes d'information de l'état, des opérateurs d'importance vitale et des industries stratégiques [p106]
- Produire en toute autonomie nos dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque [p105]
- Capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'ampleur variées
  - faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers
  - sans s'interdire l'emploi gradué de moyens relevant du ministère de la Défense [p106]
    Les frappes à distance, le cas échéant cybernétiques, pourraient devenir plus fréquentes [p30]

Livre blanc 2013 [4]

Moyens

- L'organisation opérationnelle des armées intégrera ainsi une chaîne opérationnelle de cyberdéfense [p94]
- L'état fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles [p106]
- L'état doit soutenir des compétences scientifiques et technologiques performantes [pour protéger/détecter/identifier auteurs des cyberattaques] [p105]

Livre blanc 2013 [5]

Moyens (suite)

- Montée en puissance de nouvelles composantes de la réserve opérationnelle, spécialisées dans des domaines dans lesquelles les forces de défense et de sécurité sont déficitaires [p120]
- De manière plus générale, la sécurité de l'ensemble de la société de l'information nécessite que chacun soit sensibilisé aux risques et aux menaces et adapte en conséquence ses comportements et ses pratiques [p107]
- Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique [p107]

Livre blanc 2013 [6]

L'aspect offensif

- Comment interpréter la légitime défense de l'article 51 de la Charte de l'ONU face à des cyberattaques ?
  - Mise en cause de la « survie » de l'état ?
  - Saisie du conseil de sécurité : délai ?
  - Exigence de proportionnalité (non inscrit, mais coutumier) ...
- La capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité
  - Contribue à la caractérisation de la menace et à l'identification de son origine
  - Permet d'anticiper certaines attaques et de configurer les moyens de défense en conséquence

Objectif de la présentation

Vu ...

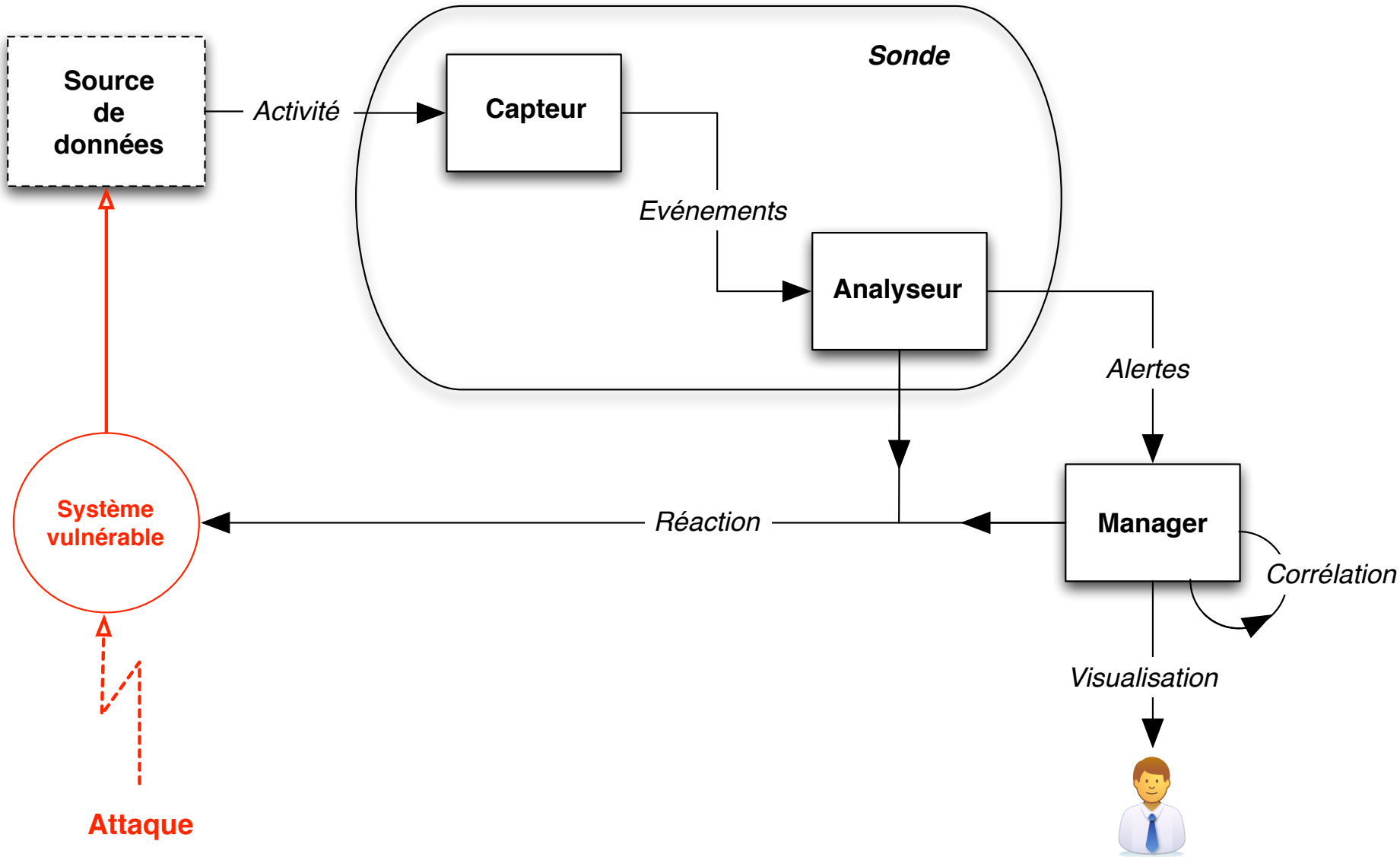
1. l'importance de la surveillance, de la détection, de l'alerte, de la supervision
2. l'importance de la sensibilisation et de la formation des experts
3. l'importance de la maîtrise des aspects offensifs (y compris en formation), ne serait-ce que pour caractériser et anticiper

... vous parler :

1. de détection d'intrusions
2. de formation en SSI

Détection des intrusions

Architecture de détection aujourd'hui ultra-classique



Propriétés attendues de l'analyse

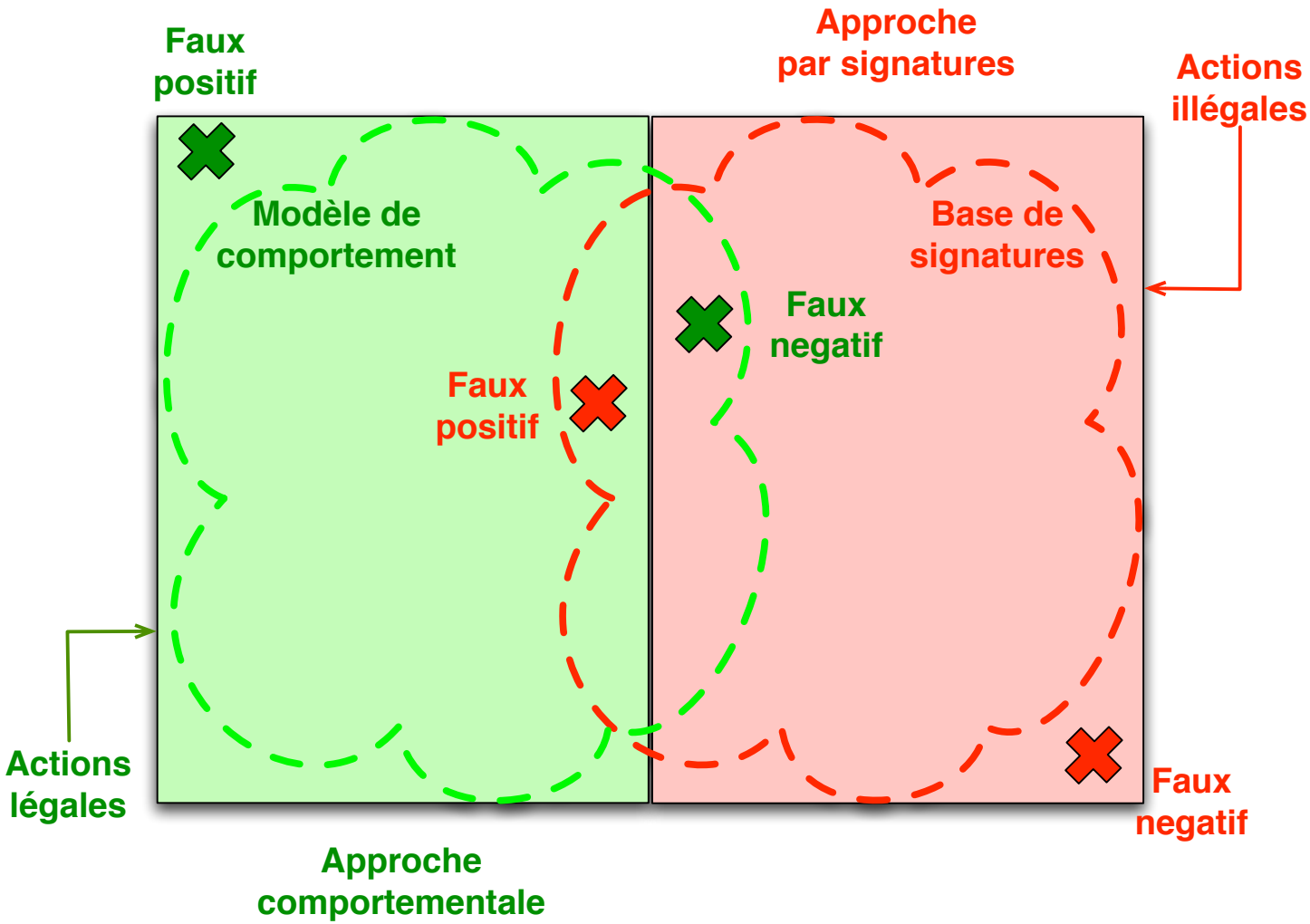
Fiabilité

- Attaque $\Rightarrow$ alerte
- Pas de faux négatif (attaque non détectée)
- TPR = nbr d'alertes correctes (TP) / nbr d'evt intrusifs (TP + FN)
- TPR idéalement égal à 1

Pertinence

- Alerte $\Rightarrow$ attaque
- Pas de faux positif (fausse alerte)
- FPR = nbr de fausses alertes (FP) / nbr d'evt sains (FP + TN)
- FPR idéalement égale à 0

TPR $\neq$ 1 et FPR $\neq$ 0



Comment gruger vos clients et/ou reviewers ?

Notre super algorithme/outils ...

- détecte 98% des attaques
- ne se trompe sur les événements normaux que dans 2% des cas

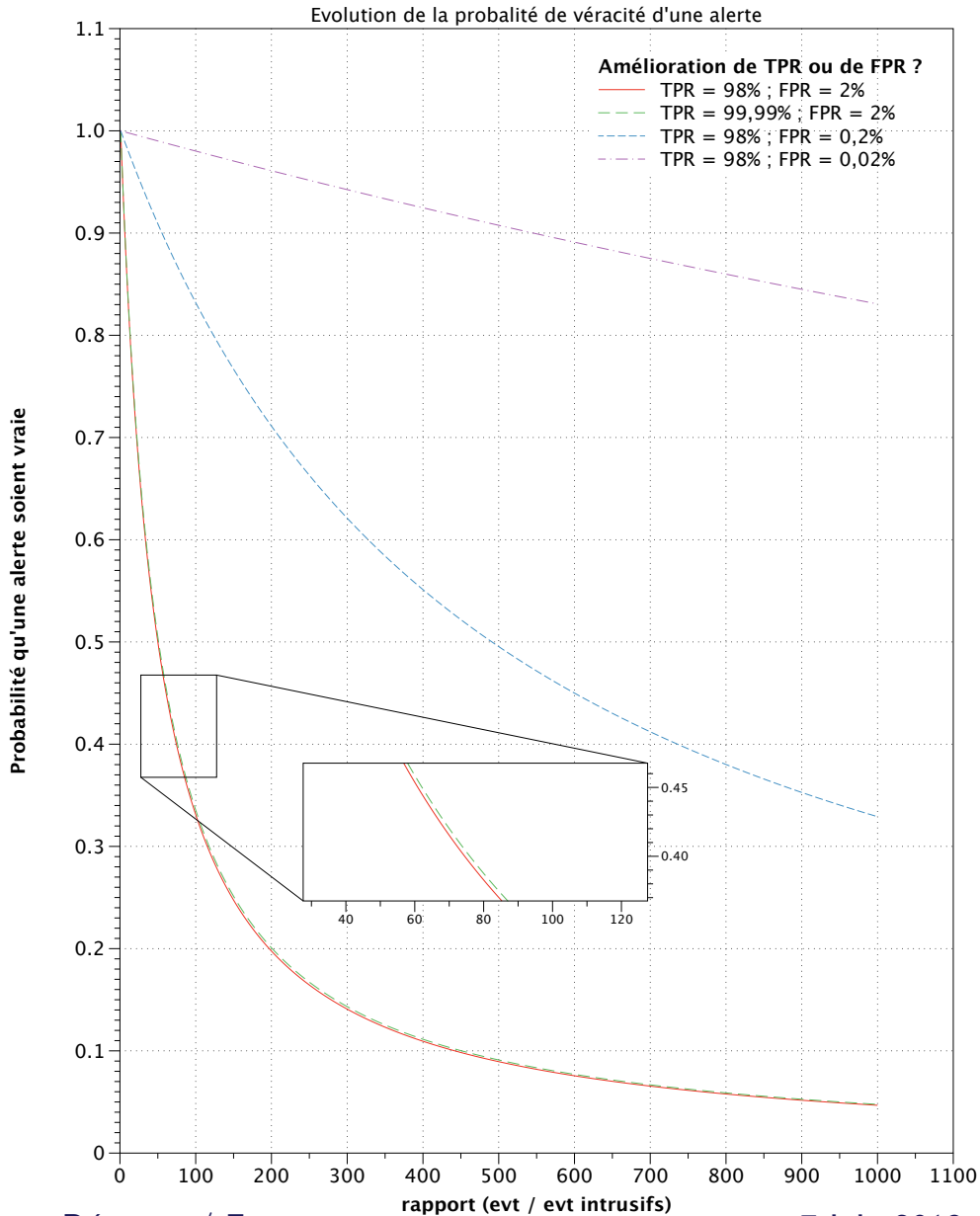
« Point de fonctionnement » classique (au moins dans la litterature)

- TPR = 0,98 et FPR = 0,02
- Ce qui parait pas si mal ...

FPR, TPR et probabilité de véracité d'une alerte

$$Prob_{TP} = \frac{TPR}{TPR+(r-1)FPR}$$

avec $r = \frac{\text{Qté évt}}{\text{Qté évt intrusifs}}$



Bref : trop de fausses alertes !

Le monitoring au niveau réseau par *pattern matching* peut-il être amélioré suffisamment pour réduire ce problème ?

- Meilleures couverture des signatures
- Améliorations incrémentales des moteurs d'analyse
- Lutte contre l'évasion
- Intégration d'aspects comportementaux (postscan, dos)
- Intégration de tests de conformité protocolaire

Mais ...

- Pas de baisse significative des vulnérabilités en vue
- Augmentation des débits et du trafic
- Usage plus large (?) de la crypto
- Verrou technologique et pas de rupture ces dernière années

Bref : trop de fausses alertes !

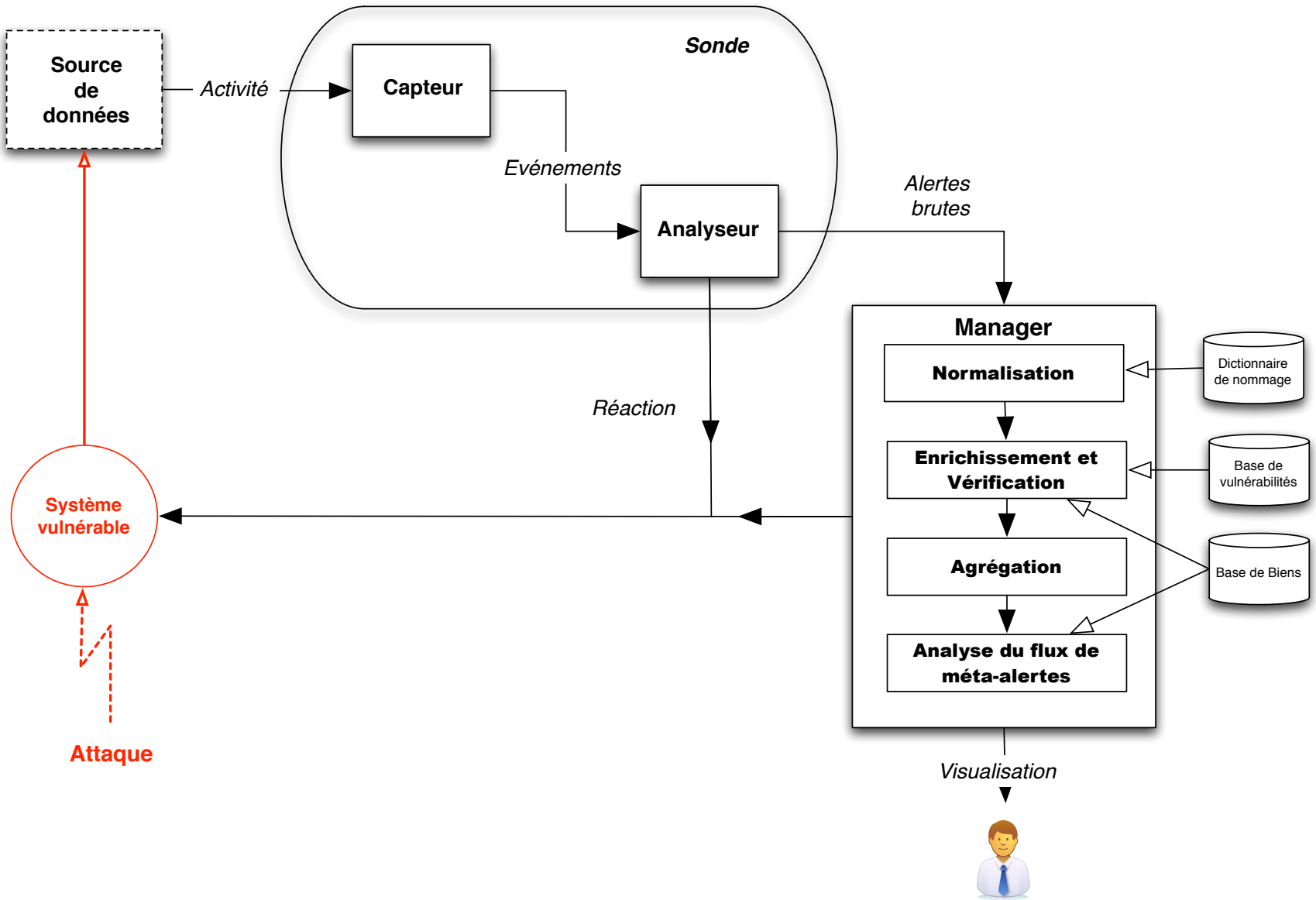
Le monitoring au niveau réseau par *pattern matching* peut-il être amélioré suffisamment pour réduire ce problème ?

- Meilleures couverture des signatures
- Améliorations incrémentales des moteurs d'analyse
- Lutte contre l'évasion
- Intégration d'aspects comportementaux (postscan, dos)
- Intégration de tests de conformité protocolaire

Mais ...

- Pas de baisse significative des vulnérabilités en vue
- Augmentation des débits et du trafic
- Usage plus large (?) de la crypto
- Verrou technologique et pas de rupture ces dernière années

Alors ? Post-traiter les alertes ? (1)



Alors ? Post-traiter les alertes ? (2)

Source : Gartner, 2013

Des outils, mais surtout des challenges

1. Mieux prendre en compte le contexte :
   - Trouver un meilleur format d'alerte
   - Mieux représenter les connaissances : vulné, biens, config., diag., contre-mesures
   - Créer/Partager des bases de scenarii d'attaque
2. Visualiser de grandes masses de données

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

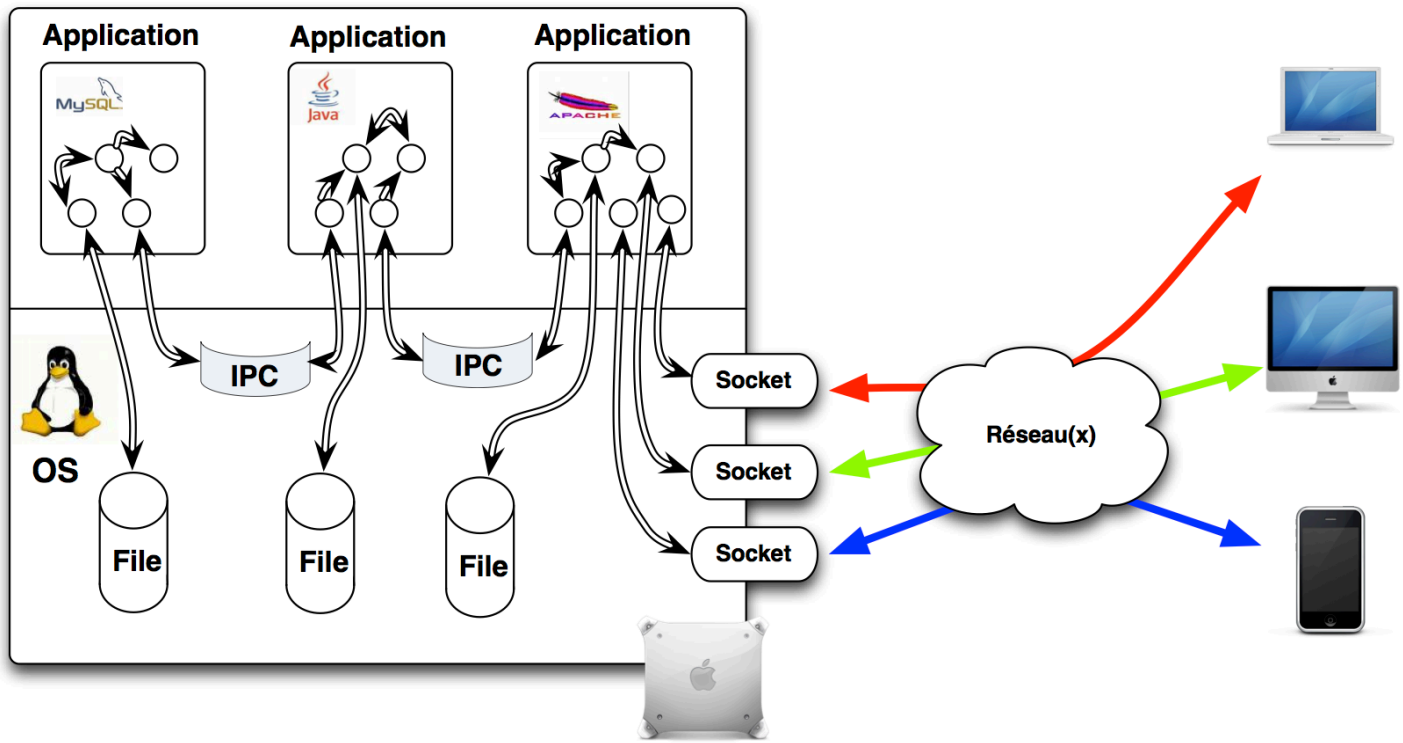
Alors ? Produire de meilleures alertes ? (1)

Nombreux challenges également ...

1. Améliorer l'analyse par les NIDS des protocoles applicatifs
2. Développer une offre d'HIDS : niveau OS, niveau applicatif
3. Prendre en compte la politique de sécurité (HIDS et NIDS)
4. Apporter des capacités de diagnostic aux IDS comportementaux
5. S'inspirer des techniques de la sureté de fonctionnement
6. Offrir un contrôle du FPR et/ou du TPR
7. Développer des environnements de test d'IDS

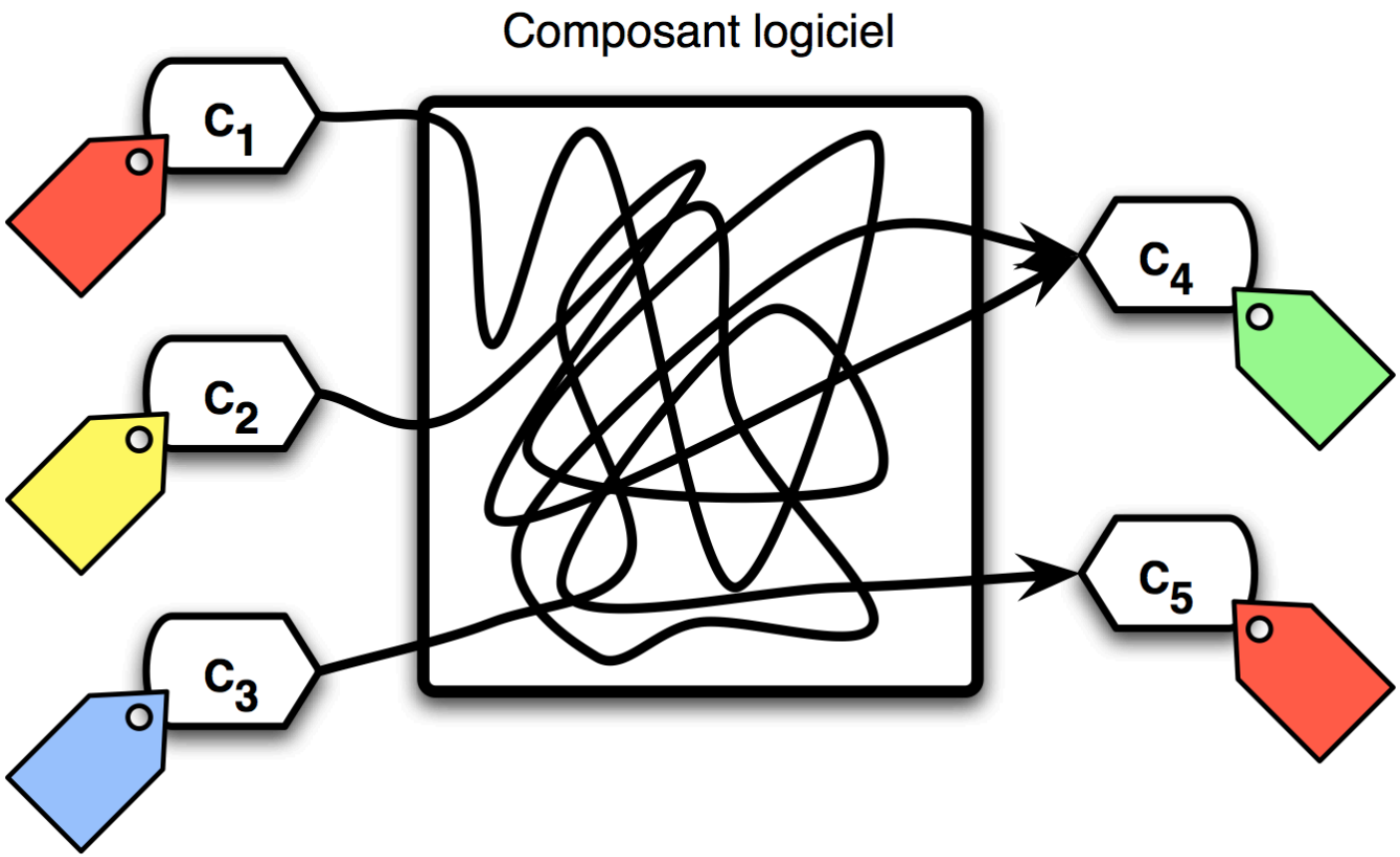
Alors ? Produire de meilleures alertes ? (2)

Ex 1 : paramètrer un HIDS par une politique de flux d'information



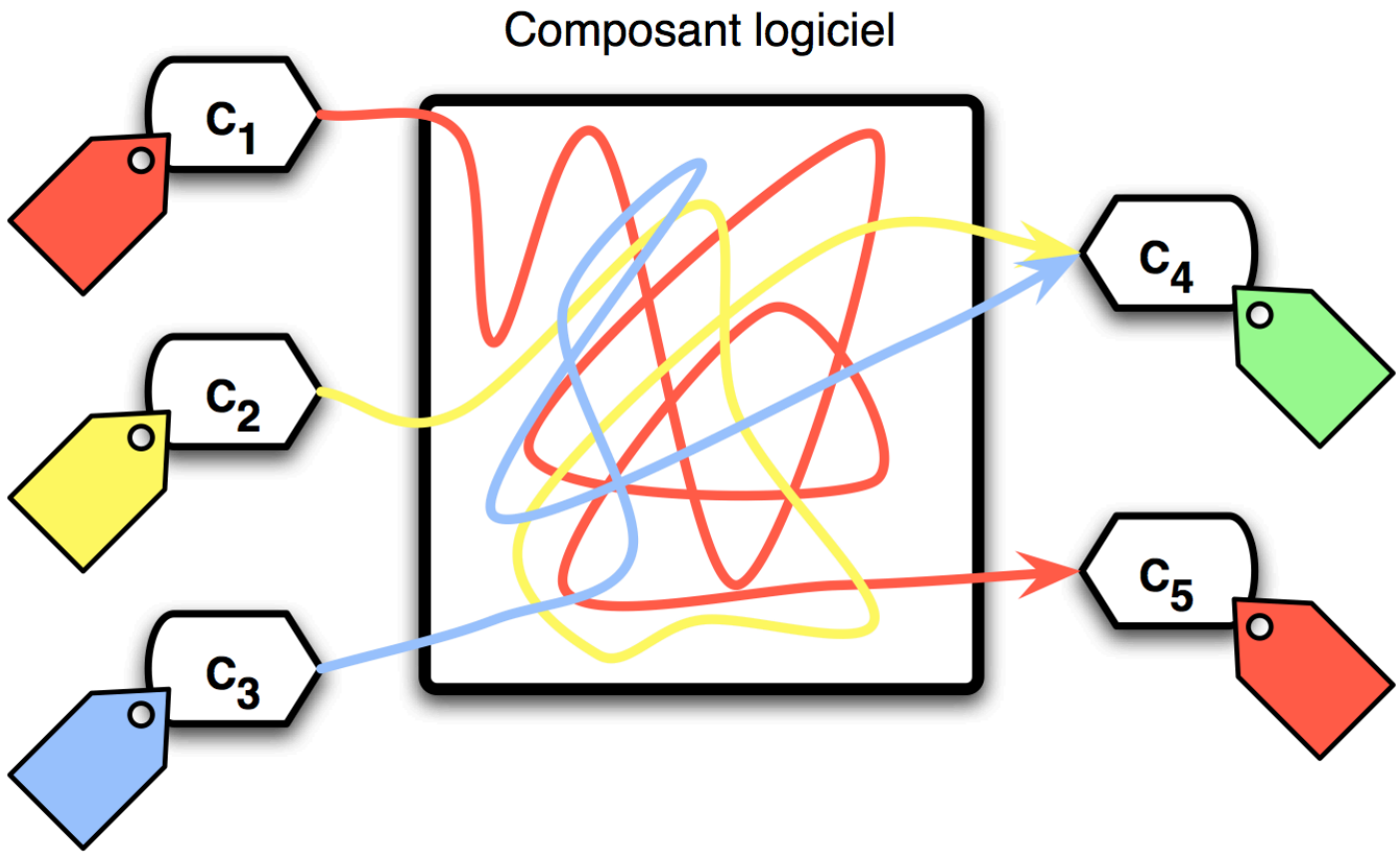
Alors ? Produire de meilleures alertes ? (2)

Ex 1 : paramètrer un HIDS par une politique de flux d'information



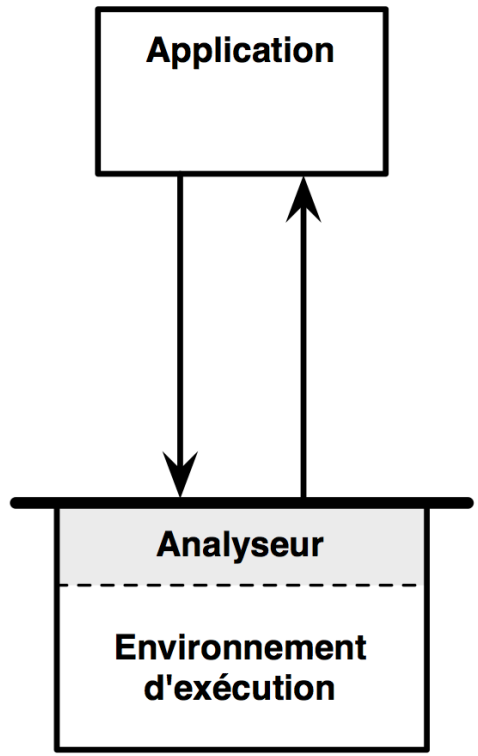
Alors ? Produire de meilleures alertes ? (2)

Ex 1 : paramètrer un HIDS par une politique de flux d'information



Alors ? Produire de meilleures alertes ? (2)

Ex 1 : paramètrer un HIDS par une politique de flux d'information



Blare : implantation Linux/Android s'appuyant sur LSM

www.blare-ids.org

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.   while(auth_ok != 1){
4.       type = packet_read(data);
5.       switch (type) {
6.           case SSH_CMSG_AUTH :
7.               auth_ok = auth(passwd, data);
8.               break; ...
9.    }
10. authenticated(uid);
```

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.   while(auth_ok != 1){
4.      type = packet_read(data);
       // bid 2347 : si pk trop gros et codage de sa taille sur 16 bits
       // ⇒ débordement d'entier
       // ⇒ par ex, passwd initialisé à chaîne vide ou auth_ok forcé à 1
5.      switch (type) {
6.          case SSH_CMSG_AUTH :
7.              auth_ok = auth(passwd, data);
8.              break; ...
9.    }
10. authenticated(uid);
```

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.   while(auth_ok != 1){
4.      type = packet_read(data);
       // bid 2347 : si pk trop gros et codage de sa taille sur 16 bits
       // ⇒ débordement d'entier
       // ⇒ par ex, passwd initialisé à chaîne vide ou auth_ok forcé à 1
5.      switch (type) {
6.          case SSH_CMSG_AUTH :
7.              auth_ok = auth(passwd, data); // retourne 1
8.              break; ...
9.    }
10. authenticated(uid);
```

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.   while(auth_ok != 1){
4.      type = packet_read(data);
       // bid 2347 : si pk trop gros et codage de sa taille sur 16 bits
       // ⇒ débordement d'entier
       // ⇒ par ex, passwd initialisé à chaîne vide ou auth_ok forcé à 1
5.      switch (type) {
6.          case SSH_CMSG_AUTH :
7.              auth_ok = auth(passwd, data); // retourne 1
8.              break; ...
9.    }
10. authenticated(uid);
```

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.   while(auth_ok != 1){
4.      type = packet_read(data);
       // bid 2347 : si pk trop gros et codage de sa taille sur 16 bits
       // ⇒ débordement d'entier
       // ⇒ par ex, passwd initialisé à chaîne vide ou auth_ok forcé à 1
5.      switch (type) {
6.          case SSH_CMSG_AUTH :
7.              auth_ok = auth(passwd, data); // retourne 1
8.              break; ...
9.    }
10.  authenticated(uid);
```

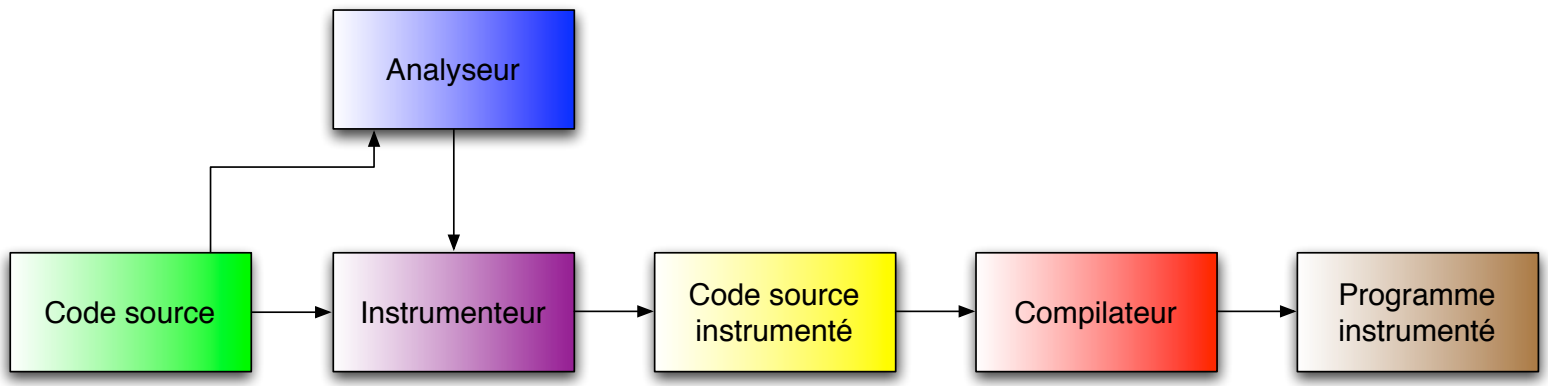
Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »

```
1.  int auth_ok = 0;
2.  if(passwd != NULL)
3.    while(auth_ok != 1){
4.      type = packet_read(data);
5.      switch (type) {
6.      case SSH_CMSG_AUTH :
7.        assert(passwd != NULL)
8.        auth_ok = auth(passwd, data);
9.        break;}
10. assert( (auth_ok == 1 && type == SSH_CMSG_AUTH)
    || auth_ok == 0 )
11. authenticated(uid);
```

Alors ? Produire de meilleures alertes ? (3)

Ex 2 : détecter les attaques contre les données de calcul par un « logiciel auto-testable »



Conclusion sur la détection

Livre blanc 2013

- Met en avant l'importance de la surveillance/détection/supervision
- Outils existants, mais outils à améliorer
- Des pistes existes
- IDS $\neq$ NIDS par signature ...

Remerciements

- Jacob Zimmermann, Christophe Bidan, Guillaume Hiet, Valérie Viet Triem Tong, Ben Morin, Andrew Clark, Christophe Hauser, Radoniaina Andriatsimandefitra, Fred Tronel, Guillaume Brogi
- Eric Totel, Fred Tronel, Jonathan Christopher Demay

Conclusion sur la détection

Livre blanc 2013

- Met en avant l'importance de la surveillance/détection/supervision
- Outils existants, mais outils à améliorer
- Des pistes existes
- IDS $\neq$ NIDS par signature ...

Remerciements

- Jacob Zimmermann, Christophe Bidan, Guillaume Hiet, Valérie Viet Triem Tong, Ben Morin, Andrew Clark, Christophe Hauser, Radoniaina Andriatsimandefitra, Fred Tronel, Guillaume Brogi
- Eric Totel, Fred Tronel, Jonathan Christopher Demay

Conclusion sur la détection

Pour en savoir plus sur les 2 approches esquissées ?

- Stéphane Geller and Christophe Hauser and Frédéric Tronel and Valérie Viet Triem Tong, Information Flow Control for Intrusion Detection derived from MAC policy, IEEE International Conference on Communications (ICC), 2011.
- Radoniaina Andriatsimandefitra and Stéphane Geller and Valérie Viet Triem Tong, Designing Information Flow Policies for Android's Operating System, IEEE International Conference on Communications (ICC), 2012.
- Valérie Viet Triem Tong, Andrew Clark, and Ludovic Mé. Specifying and Enforcing a Fine-Grained Information Flow Policy : Model and Experiments. Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JOWUA). Vol. 1 No 1. June 2010.
- Jonathan-Christofer Demay and Frederic Majorczyk and Eric Totel and Frederic Tronel, Detecting illegal system calls using a data-oriented detection model, Proceedings of the 26th IFIP TC-11 International Information Security Conference (IFIP SEC), 2011.

La formation en SSI

Former qui à quoi ?

Sensibiliser/former à divers niveaux

- Sensibilisation du grand public
- Sensibilisation de tous types de professionnels
- Sensibilisation de tous les ingénieurs
- Formation de tous les informaticiens
- Formation d'experts SSI : master et doctorat

Pluridisciplinarité

- Sécurité : logique + physique + organisationnel
- Importance du « facteur humain », ok, mais importance capitale du « facteur technique »

Former à quel niveau ?

Expériences étrangères

- Israël, au lycée depuis 1998
  - 270h : bases de l'informatique (2/3 obligatoires)
  - 450h : notions avancées (4/5 obligatoires)
- Finlande, Japon, Massachusetts, Ontario, Singapour : enseignement spécialisé en info entre 12 et 16 ans
- En Europe : objectif affiché de développer l'aptitude à la programmation en Allemagne, Grèce, Espagne, Italie, Pologne et Royaume-Uni

En France ?

- Informatique == un ensemble d'outils et pas une discipline autonome
- Fouillis sémantique : il faut arrêter d'appeler tout et n'importe quoi « informatique »

Encore un « problème français » ?

Le besoin

- Une formation démarrant bien plus tôt (dès le collège)
- Programmation (et algorithmie) certes, mais aussi architecture des machines, des réseaux, des SI + cultures (licences libres et commerciales, etc.)
- Formation des formateurs ?

Un espoir ?

- Spécialité « Informatique et Sciences du Numérique » créée en 2012 en S, étendue en E et L en 2014
- Cours de programmation (python) en prépa
- Rapport de l'Académie des sciences : « l'enseignement de l'informatique en France : il est urgent de ne plus attendre »

Formation technique des experts (1)

Prérequis

- Architecture des ordinateurs
- Systèmes d'exploitation : fonctionnement de Windows, Unix
- Réseaux : IP, TCP, UDP, certains protocoles applicatifs (DNS, HTTP, SMTP/IMAP)
- Processus et méthode de développent :
  - Bonne connaissance du C et de l'assembleur
  - Méthodes de développement dont méthodes formelles

Acquis en fin de L3 ?

Formation technique des experts (2)

Apports en M1/M2

- Politiques de sécurité
- Cryptographie
- Sécurité des OS : contrôle d'accès, anti-virus, détection d'intrusions
- Développement propre (du point de vue de la SSI), portable et documenté
- Sécurité des réseaux : techniques d'authentification (protocoles d'authentification cryptographique, SSO), pare-feu, VPN (IPSec, SSL/TLS), anti-virus, détection d'intrusions
- Sécurité logicielle : analyse statique et dynamique de source et de binaire, obscurcissement/désobscurcissement
- Sécurisation des applications (en particulier web)

Formation technique des experts (3)

Apports en M1/M2 (suite)

- Objet de sécurité : carte à puce, RFID
- Protection des données personnelles
- Méthodologie d'analyse de menaces et de gestion du risque
- Techniques pour l'informatique légale et l'analyse post-mortem (forensic)
- Méthode d'évaluation de la sécurité : CSPN, critères communs
- Les métiers de la SSI

Formation technique des experts (4)

Apports en M1/M2 (*last, but not least*)

- Lutte informatique offensive
  - Connaissance détaillée des vulnérabilités et de leur mode d'exploitation
- Précautions
  - Extension de la notion de « motif légitime » de l'art. 323-3-1 du code pénal
  - Centres de formation adaptés : certification, audit, contrôle
  - Formation à l'éthique
- Concours réguliers d'attaque/défense (*capture de flag*) $\Rightarrow$ montrer tout l'intérêt de la maitrise du volet offensif par les défenseurs

Qualité/reconnaissance des formations ?

Vers des « *Centers of Academic Excellence in Information Assurance Education* » ?

- Français ou européens ?
- Critère de labellisation ?
  - Volume de formation
  - Thème
  - Débouchés professionnels – et donc identification des métiers de la sécurité
  - Nombre et niveau des étudiants
  - Niveau des intervenants
  - etc.
- Lien avec les nombreux labels professionnels (CISM, CEH, CHFI, CISSP, CISA, etc.) ?
- Conférence annuelle à la *National Colloquium for Information Systems Security Education*

Conclusion

Faire face aux **cybermenaces** $\Leftrightarrow$
détecter (les attaques) $\wedge$ **former** (des experts en SSI) ?

Faire face aux **cybermenaces** $\Rightarrow$
détecter (les attaques) $\wedge$ **former** (des experts en SSI)

Faire face aux **cybermenaces** $\Rightarrow$ **détecter** (les attaques) $\wedge$ **former** (des experts en SSI)

Ludovic Mé
ludovic.me@supelec.fr
http://www.rennes.supelec.fr/ren/perso/lme/

7 juin 2013