Défis dans le génie sécurité des Systèmes de Systèmes

Vanea Chiprianov Laurent Gallon **Manuel Munier**
Philippe Aniorté Vincent Lalanne

LIUPPA, Université de Pau et des Pays de l'Adour, France

CIEL 2014

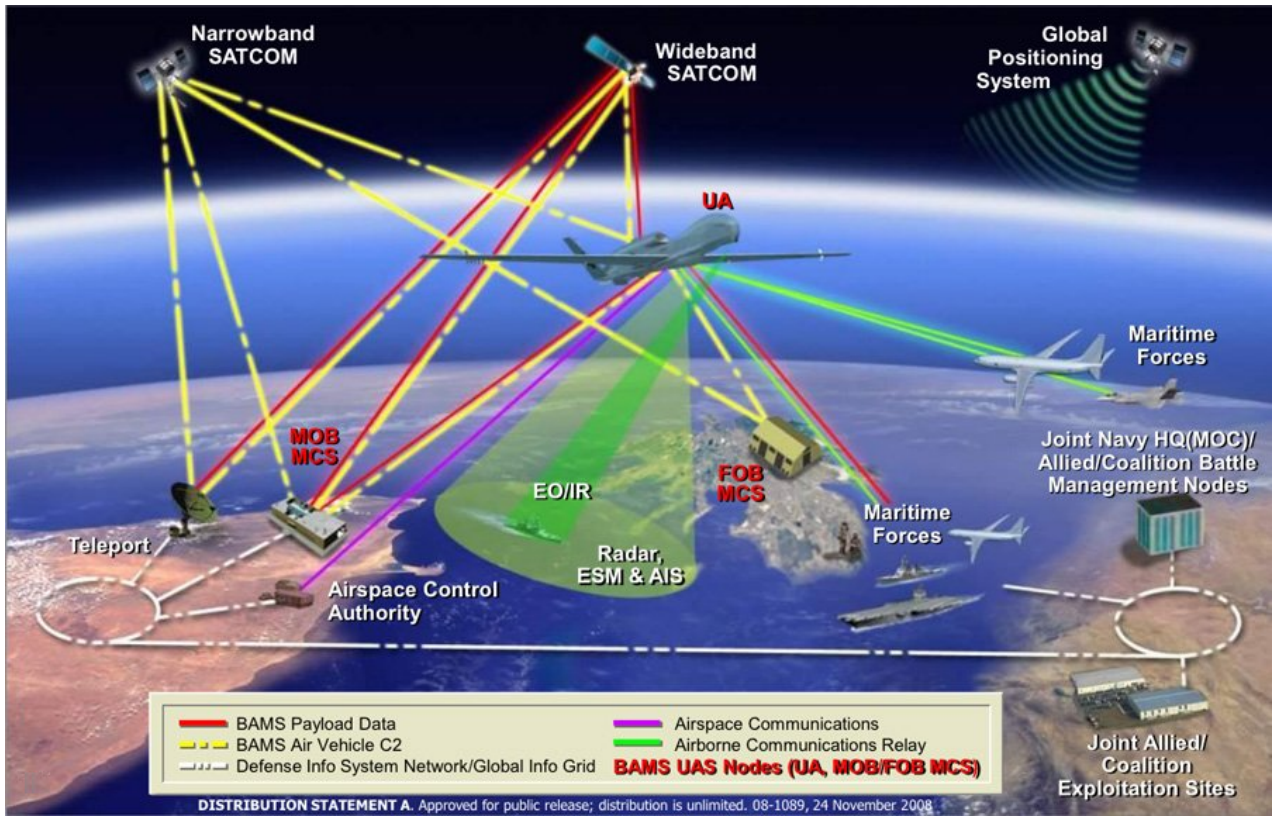
Paris, France, 10-13 juin 2014

Plan de la présentation

Systèmes de Systèmes (SdS)

Présentation

- Systèmes distribués, concurrents, à large échelle, composés de systèmes complexes, "indépendants" les uns des autres
- Ex: surveillance maritime



Systèmes de Systèmes (SdS)

Caractéristiques et sécurité des SdS

- Indépendance opérationnelle des éléments
  - Chaque système est conçu pour fonctionner de façon isolée
  - Politiques $\neq$, implémentations $\neq$, objectifs $\neq$

  $\Rightarrow$ Incompatibilités potentielles et conflits entre les différentes sécurités de chaque système

- Indépendance managériale des éléments
  - Chaque système est géré par sa propre organisation
  - Les activités d'un système peuvent impacter la sécurité des autres systèmes
  - Quels droits légaux pourrait/devrait avoir un système sur un autre système ?

Systèmes de Systèmes (SdS)

Caractéristiques et sécurité des SdS

- Développement évolutif
  - Ajout/retrait/modification de systèmes

  $\Rightarrow$ Comment assurer une sécurité qui n'a pas été prévue dès la conception ?

- Comportements émergents
  - De nouvelles fonctionnalités, imprévues, introduisent des vulnérabilités qui ne peuvent être détectées au niveau de chaque système pris individuellement
  - Quid des responsabilités ?

- Distribution géographique
  - Comment tenir compte de réglementations nationales différentes ?
  - Les cultures/approches peuvent elles aussi être différentes

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Identification des défis dans le génie sécurité des SdS
  - → Comment les classifier ?
  - → Approche "cycle de vie de la sécurité"
- "Framework" de sécurité des SdS
  - ▷ Analyse des besoins
  - ▷ Conception
  - ▷ Implémentation
  - ▷ Vérification
  - ▷ Release/Response
- Avec une particularité supplémentaire
  - → Longue vie (au sens GPL) des SdS

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **analyse des besoins**
  - ⇝ Identifier les besoins de sécurité des SdS
    - *besoins par rapport aux interactions entre les systèmes*
  - ⇝ Modéliser les besoins de sécurité
    - *court terme: contrôle sur les politiques et les interfaces*
    - *long terme: harmonisation des politiques et des mécanismes*
    - → *intégration de la sécurité dans la modélisation des besoins ?*
  - ⇝ Responsabilités
    - *tests, comportements émergents, utilisation malicieuse,. . .*
  - ⇝ Gestion des risques
    - *standards & processus pour 1 système, pas pour les SdS !*
  - ⇝ Métriques de sécurité

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **conception**
  - ⇝ Combler le trou entre les besoins et la conception
    - *interopérabilité → l'utilisation de standards & frameworks ne peut pas toujours garantir un certain niveau de sécurité*
  - ⇝ Intégrer la sécurité dans l'architecture
    - *sécurité souvent prise en compte à la fin du dév d'un système*
    - → *toute modification est coûteuse*
    - → *intégrer la sécurité au plus tôt dans la conception*
  - ⇝ Modéliser la sécurité des SdS et l'analyser (continuellement ?)
    - *SdS ≡ composition de systèmes*
  - ⇝ Analyser les interdépendances
    - *interdépendances (parfois "cachées") ⇒ impacts en cascade*
    - → *méthode d'évaluation des risques*
  - ⇝ Contrats de sécurité
    - *formalisation des relations entre systèmes*

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **implémentation** (1)
  - ⇝ Authentification
    - *interopérabilité, identités, contrats ?*
  - ⇝ Contraintes de temps
    - *insertion de composants ou de messages → impact sur les temps de réponse*
  - ⇝ Autorisations
    - *modéliser les autorisations d'un système sur un autre*
    - *qui gère ?*
  - ⇝ Audit
    - *traçabilité, responsabilités, délégations,. . .*
  - ⇝ Non-répudiation
    - *preuve (opposable en cas de litige), confiance,. . .*

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **implémentation** (2)
  - ⇝ Chiffrement
    - *fiabilité des connexions entre systèmes ?*
  - ⇝ Gestion des clés cryptographiques
    - *modèles/infrastructures actuels adaptés aux SdS ?*
  - ⇝ Composition des politiques de contrôle
    - *politiques sur chaque système, politique de composition,. . .*
  - ⇝ Politiques basées sur le contexte
    - *le partage de données entre les composants peut évoluer en fonction du contexte (quoi, qui)*
    - *politiques (règles) de sécurité dynamiques*

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **implémentation** (3)
  - ⇝ Métadonnées
    - *traçabilité → quelles métadonnées ? classification ?*
    - *sécurité, protection des données, vie privée,. . .*
  - ⇝ Hétérogénéité et multiplicité des plate-formes
    - *protocoles ≠, implémentations ≠, infrastructures ≠*

    ⇒ *vulnérabilités ? corrélation d'informations ?*
  - ⇝ Sécurité basée sur le hardware

    → *bénéfices également pour les SdS ?*

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

- Phase **vérification**
  - ⇝ Vérifier si l'architecture est conforme à l'analyse des besoins
  - ⇝ Vérifier si l'implémentation est conforme à l'architecture
  - ⇝ Vérifier si l'implémentation est conforme à l'analyse des besoins

Cycle de Vie de la Sécurité

"Framework" de sécurité des SdS

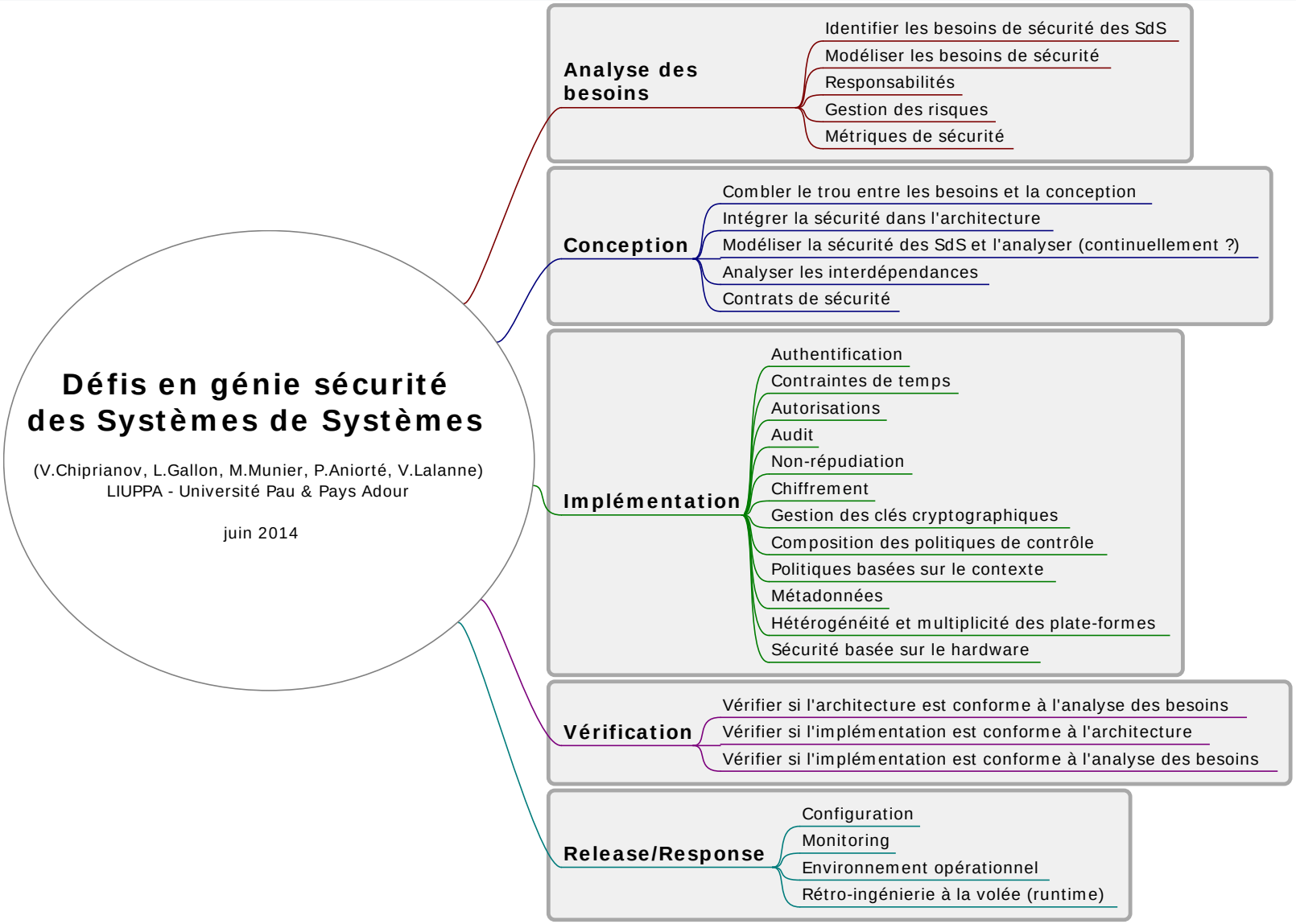
- Phase **release/response**
  - ⇝ Configuration
  - ⇝ Monitoring
  - ⇝ Environnement opérationnel
  - ⇝ Rétro-ingénierie à la volée (runtime)

⇒ Comment gérer ceci au niveau d'un SdS, i.e. à la couche "interactions entre systèmes" ?

- impacts sur les systèmes ?
- notion de niveau de sécurité ?
- ...

Conclusions

Défis du GPL 2025 "sécurité des SdS"



Conclusions

Défis du GPL 2025 "sécurité des SdS"

- Catalogue des défis à l'ingénierie de la sécurité des SdS

$\Rightarrow$ Milestones pour le développement d'un "framework" générique, d'une chaîne d'outils/approches pour adresser ces différents défis

Défis dans le génie sécurité des Systèmes de Systèmes

Invitation à collaborer avec nous pour adresser ces défis :)

Vanea Chiprianov, Laurent Gallon, **Manuel Munier**, Philippe Aniorté, Vincent Lalanne

Email: `prénom.nom@univ-pau.fr`