Workshop Entrain, Exploring New Territorial User Interfaces, November 2020

Security engineering for the design of new territorial user interfaces

Wilson E. Goudalo [1,2], Christophe Kolski [2], Frédéric Vanderhaegen [2]

[1] **ABERDI Inc.,** Westmount, Canada

[2] **LAMIH**-UMR CNRS 8201, Univ. Polytechnique Hauts-de-France (UPHF), Valenciennes, France

LABORATOIRE D'AUTOMATIQUE DE MECANIQUE ET D'INFORMATIQUE INDUSTRIELLES ET HUMAINES
LAMIH UMR CNRS 8201

INSTITUT CARNOT ARTS

cnrs

Université Polytechnique HAUTS-DE-FRANCE

From territoriality to security considerations

- Territorial user interfaces:

  - Possible analogies with geography and territorial considerations:

    Countries, regions, limits, frontiers, ressources, people, human rights (rules)…

- Security considerations:

  - May become the same in countries and territorial user interfaces:

    Data breach, Problems of Privacy, Confidentiality, Integrity, Availability, Authenticity, Accountability, Non-repudiation (Attacks or Errors)

- Necessity to be in line with current research ways considering:

  - Security & Usability & Resilience ([NIST, 2020], [ISO, 2018], [Vanderhaegen F, 2017], [Goudalo et al., 2017])

A recall about security: Three main considerations

Objectifs de protection	Impacts potentiels
Imputabilité	Perte des traces, des pistes d'audit et de la transparence. Perte d'image de marque et pénalités pour la non-conformité règlementaire.
Disponibilité	Perte d'exploitation directe et Perte de part de marché.
Confidentialité	Divulgation d'informations sensibles, Pénalités pour non-conformité, Perte d'image et de part de marché.
Intégrité	Corruption de données, Inconsistance des services, Perte d'image et de part de marché.

Objectifs de l'utilisabilité	Impacts potentiels
Coût d'utilisation (dans la réalisation d'une tâche)	Source d'erreurs
Efficacité de la réalisation des tâches	Source de contournement et/ou d'abandon
Efficience de la réalisation des tâches	Source d'erreurs et/ou de failles de sécurité
Satisfaction de l'utilisateur dans la réalisation des tâches	Source de rejet et/ou de recherche de contournement

Objectifs de Résilience	Techniques de résilience
Eviter des incidents inacceptables, du point de vue de la fréquence et du point de vue de la sévérité, en cas de changement	Évolutivité (adaptabilité)
Garantir la persistance de la prestation de services de confiance	Evaluation et vérification
Tenir compte des changements des systèmes	Utilisabilité (pour les utilisateurs humains et non-humain)
Tenir compte de la complexité des systèmes	Diversité (accroître la diversité de moyens et profiter des moyens alternatifs afin d'éviter le SPOF – *Single Point Of Failure*)

[Goudalo et al., 2020]

A recall about security: Motivations for Territoriality

- **Digital consumerism.** Digital consumerism has significantly led the evolution of IT paradigms over the last decade from traditional, perimeter-based monolithic structures to complex, “perimeter less” multi-cloud environments that are characterized by high interoperability, mobility, portability.
- **Changing attack vector and surface.** As the diversity of the security environment grows, new models of advanced security can help deliver greater efficiency in the context of territoriality (with changing attack vector and attack surface).
- **Business and IT objectives.** Rather than focus on only one functional area of security, we should shift into a business outcomes mindset, rooted in a unified strategy that accelerates business and IT objectives.
- **Zero Trust.** In secure territoriality context, users, data and resources should be securely connected through a deny-by-default policy and authorization, while providing expected business and IT value.

Key points for securing territorial user interfaces

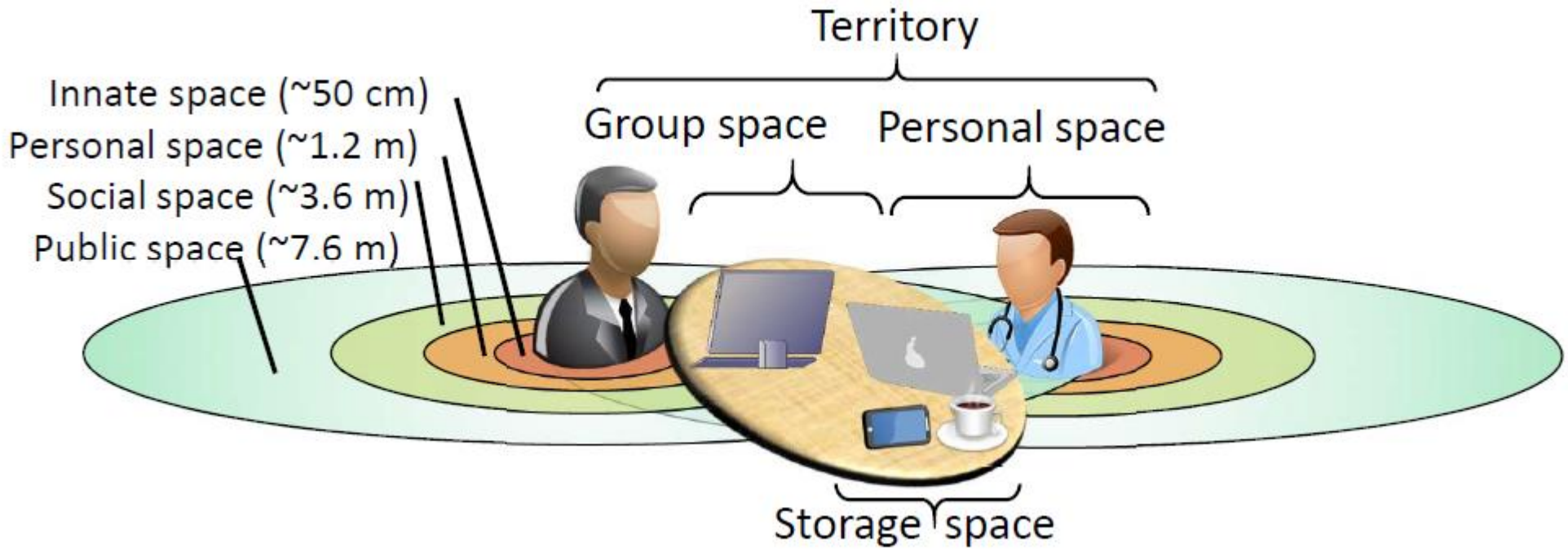
Proposition of the following four points in order to address security in territoriality context:

- **(a) Define Context** – Discover and classify resources based on risk. Coordinate actions across the territoriality ecosystem for consistency and context.
- **(b) Verify and Enforce** – Protect the territoriality actors and resources by quickly and consistently validating, enforcing and implementing advanced security models, policies and controls.
- **(c) Respond promptly** – Resolve and remediate security incidents with minimal impact to the business by taking targeted actions based on the territoriality context.
- **(d) Analyze and Improve** – Continually improve security posture by adjusting policies and practices to make faster more informed decisions to tighten security around each territoriality actor and resource.

Necessity to secure territorial user interfaces: illustrations

(a) Define Context

(b) Verify and Enforce



(c) Rapid Response

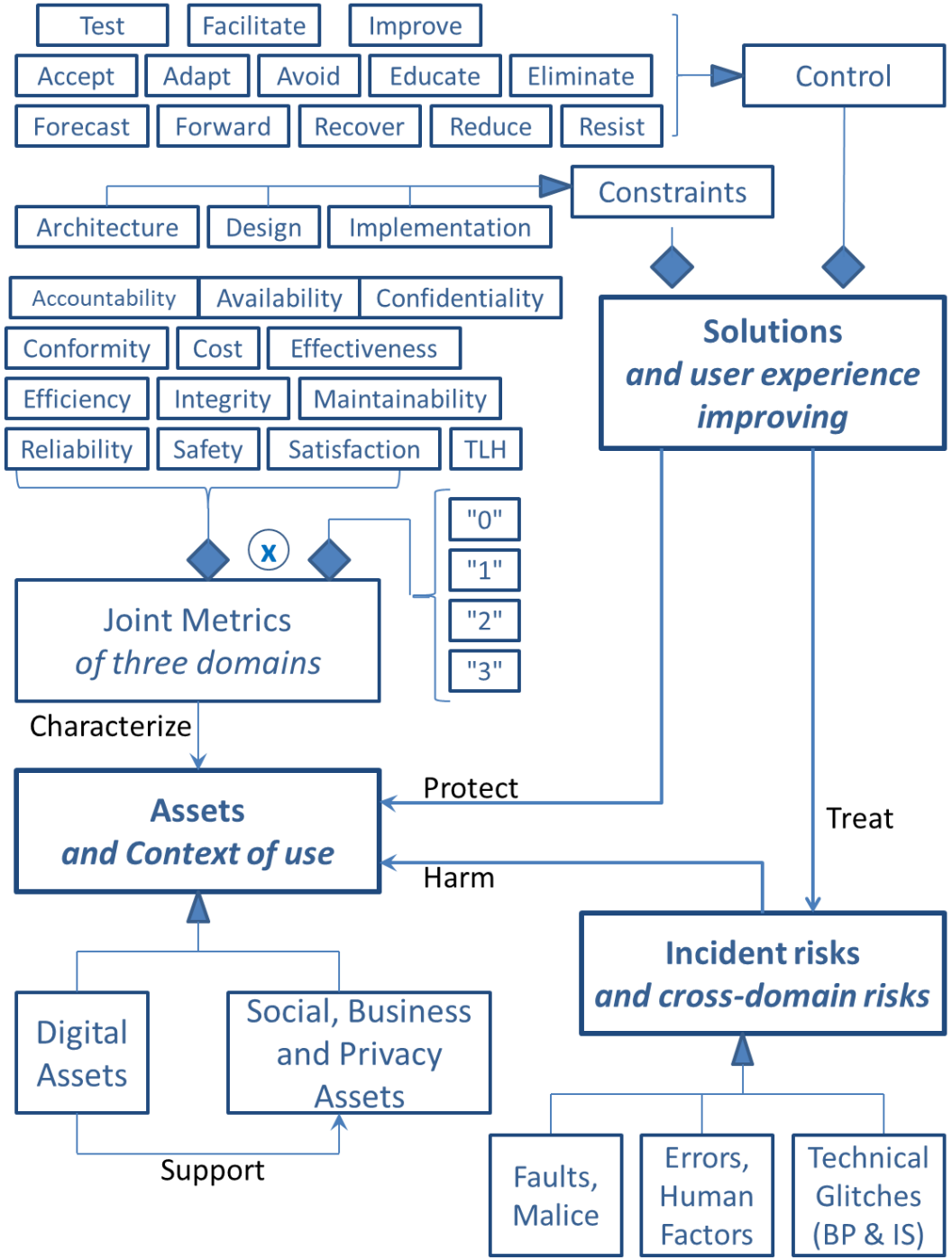
(d) Analyze and Improve

Advanced engineering based on (a) & (b) & (c) & (d) for treating Usability, Security and Resilience, jointly

Adapted from: [Scott et al., CSCW'2004]

Security engineering for the design of new territorial user interfaces: a first conceptuel framework

To address security in territoriality context, the proposed four points of the joint engineering treat together the three domains (Security, Usability and Resilience), in order to reach Business (*BP – Business Process*) and IT (*IS – Information System*) Objectives.



Advanced Conceptual Model of Joint Engineering of Security, Usability and Resilience

Conclusion

- Importance to ensure the security of new territorial user interfaces (*Security Motivations*)
- Proposition of four points from joint engineering of Security, Usability and Resilience (*Business and IT objectives together*)
- Research perspectives:
  - Develop a specific joint engineering for territoriality security
  - Apply to Distributed Mobile Multi-Agent Systems (*DMMAS*)

Questions / Answers / Remarks

FOR YOU ATTENTION

Workshop Entrain, Exploring New Territorial User Interfaces, November 2020

Security engineering for the design of new territorial user interfaces

Wilson E. Goudalo [1,2], Christophe Kolski [2], Frédéric Vanderhaegen [2]

[1] **ABERDI Inc.,** Westmount, Canada

[2] **LAMIH**-UMR CNRS 8201, Univ. Polytechnique Hauts-de-France (UPHF), Valenciennes, France

Future questions, comments, and advice are welcome

+1 514 978-8877

wgoudalo@gmail.com ; wilson.goudalo@abe-engineering.net

skype wgoudalo

www.aberdi.net (coming soon)

Wilson E. Goudalo,

ABERDI Inc. ***(Secure Digital Transformation and Intelligent Project Finance)***

INSTITUT CARNOT ARTS

cnrs

LAMIH LABORATOIRE D'AUTOMATIQUE DE MECANIQUE ET D'INFORMATIQUE INDUSTRIELLES ET HUMAINES UMR CNRS 8201

Université Polytechnique HAUTS-DE-FRANCE

References

- [Goudalo et al., 2017] - Goudalo W., C. Kolski et F. Vanderhaegen (2017a). Towards Advanced Security Engineering for Enterprise Information Systems: Solving Security, Resilience and Usability Issues Together Within Improvement of User Experience. In Enterprise Information Systems, ICEIS 2016, 291, LNCS, Springer, pp. 436-459.
- [Goudalo et al., 2020] - Goudalo W., Kolski C., Vanderhaegen F. (2020). "Vers une approche holistique pour l'amélioration de l'expérience des parties prenantes dans l'Hôpital 4.0". GISEH 2020 - 10ème Conférence Francophone en Gestion et Ingénierie des Systèmes Hospitaliers, Valenciennes, France. Publication acceptée en Mars 2020.
- [ISO, 2018] - ISO (2018). ISO 9241-11 : 2018, Ergonomie de l'interaction homme-système — Partie 11 : Utilisabilité — Définitions et concepts.
- [NIST, 2020] - NIST (2020). "Cybersecurity Framework" https://www.nist.gov/cyberframework
- [Scott et al., CSCW'2004] - Scott S.D., Carpendale M.S.T., Inkpen K. (2004). CSCW '04: Proceedings of the 2004 ACM conference on Computer supported cooperative workNovember 2004 Pages 294–303https://doi.org/10.1145/1031607.1031655
- [Vanderhaegen F, 2017] - Vanderhaegen F. (2017). Towards increased systems resilience: New challenges based on dissonance control for human reliability in Cyber-Physical & Human Systems. Annual Reviews in Control, 44, pp. 316-322.