REPUBLIQUE DU SENEGAL

UNIVERSITE CHEIKH ANTA DIOP

Ecole Supérieure Polytechnique de Dakar
Département Génie Informatique

MEMOIRE DE FIN DE CYCLE

Pour l'obtention du :

DIPLÔME D'INGENIEUR DE CONCEPTION EN INFORMATIQUE

Etude et mise en oeuvre d'une application conforme OWASP

Lieu de stage :
HubSo

Présenté et soutenu par :
Papa Latyr MBODJ

Maîtres de stage :
Ahmed Tidiane CISSE
Mouhamadou Mansour Sy SAMB

Professeur encadreur :
M. Ibra DIOUM

Année universitaire : 2017-2018

VISA

DÉDICACES

Remerciements

AVANT-PROPOS

RÉSUMÉ

Balancing of an inverted pendulum is a classical problem in the field of Control Theory and Engineering. It's balancing is always challenging for the beginners in control engineering. This thesis deals with stabilization and control of both the linear and rotary inverted pendulum systems. Simultaneous approach is applied to system analysis as well as controller synthesis. Great similarity of both the systems is pointed out during the derivation of the equations of motion using the Euler-Lagrange equation. Linear inverted pendulum system is analyzed in two experimental setups , pendulum on cart and two wheel self balancing vehicle. PID controller is used to control the system by trial and error based tuning. Potentiometer (pot) and gyroscopic sensor is used as feedback sensor of the controlled system. Rotary inverted pendulum system is analyzed in a experimental setup developed by $QUANSER$ and is balanced by Pole placement method. Rotary encoder is used as the feedback sensor of the controlled system. Later, Linear Quadratic Regulator (LQR) is designed for optimum control of the pendulum. System response and controller gains are simulated in $MATLAB$ environment and after applying controller in experimental prototype, actual response of the system is reported.

Keywords : Inverted pendulum, PID controller, Pole placement method, LQR.

ABSTRACT

Balancing of an inverted pendulum is a classical problem in the field of Control Theory and Engineering. It's balancing is always challenging for the beginners in control engineering. This thesis deals with stabilization and control of both the linear and rotary inverted pendulum systems. Simultaneous approach is applied to system analysis as well as controller synthesis. Great similarity of both the systems is pointed out during the derivation of the equations of motion using the Euler-Lagrange equation. Linear inverted pendulum system is analyzed in two experimental setups , pendulum on cart and two wheel self balancing vehicle. PID controller is used to control the system by trial and error based tuning. Potentiometer (pot) and gyroscopic sensor is used as feedback sensor of the controlled system. Rotary inverted pendulum system is analyzed in a experimental setup developed by $QUANSER$ and is balanced by Pole placement method. Rotary encoder is used as the feedback sensor of the controlled system. Later, Linear Quadratic Regulator (LQR) is designed for optimum control of the pendulum. System response and controller gains are simulated in $MATLAB$ environment and after applying controller in experimental prototype, actual response of the system is reported.

Keywords : Inverted pendulum, PID controller, Pole placement method, LQR.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE **Page**

TABLE DES FIGURES

FIGURE **Page**

Introduction

Première partie

Présentation Générale

Table des matières

CHAPITRE 1

LA STRUCTURE D'ACCUEIL

1.1 Présentation de HubSo

Hubso est une entreprise informatique crée en 2011. Elle oeuvre pour le développement de solutions sociales informatiques au Sénégal. Par l'usage des TIC, elle tente de matérialiser le concept d'actions sociales, d'aider les personnes et groupes les plus fragiles à mieux appréhender les domaines de la santé, de l'éducation, de la réduction de la pauvreté etc...
Hubso accompagne d'autres entreprises à mettre en place des solutions informatiques qui leur sont adaptées. Sur ce point, Hubso étant un grand adepte du manifeste agile, tient à cœur la collaboration avec ces entités pour bâtir des partenariats solides plus que tout. De même, elle collabore aussi avec d'autres entreprises de services du numérique. Parmi ces collaborateurs de Hubso, nous avons :
- Intouch, le plus proche partenaire
- Mazars
- Yux
- Performances Group
- 2SI
- entre autres

1.2 Domaines d'activités

Hubso propose les services suivants :
- Développement de solutions informatiques : Hubso est reconnue pour son expérience et ses références en matière de développement autour des technologies JEE et Android. Une équipe de plus de 15 ingénieurs de conception est à l'écoute de vos besoins ;
- Conseil en architecture d'entreprise : Les équipes de Hubso animent des ateliers avec ses clients pour concevoir leur architecture d'entreprise ;
- Tierce maintenance applicative :?
- Promotion de solutions innovantes pour la société : Hubso, c'est aussi l'innovation par la promotion de solutions.

1.3 Quelques Solutions

Hubso propose entre autres, les solutions suivantes :

- TONGTONG

TongTong est un site de vente en ligne basé sur les concepts d'achat groupé. TongTong, lancé par Hubso en 2014 , est aujourd'hui une référence dans le domaine de l'Ecommerce, notamment en matière de produits alimentaires manufacturés, de légumes, de produits locaux, etc. Il est possible de faire ses commandes sur www.tongtong.sn

- GRANT

GRANT est une solution permettant à une entreprise de subventionner un ou plusieurs services pour ses employés. Elle a été lancée par Hubso en 2017. Les subventions de tickets restaurant ont été intégrées à la plateforme et sont aujourd'hui utilisées par plusieurs entreprises.

- AVISJOURNAUX.COM

AVISJOURNAUX.COM diffuse quotidiennement tous les appels d'offres et autres avis parus au Sénégal à ses milliers d'abonnés. C'est aujourd'hui une solution de référence dans le domaine, plébiscitée par les nombreux messages d'encouragement. Les abonnements "Grand public" sont gratuits. Cependant, une offre dédiée est commercialisée pour les regroupements de professionnels désirant bénéficier d'un service plus adapté.

1.4 Organisation

Ici organigramme

Petite explication organigramme

CHAPITRE 2

LE SUJET

2.1 Présentation

2.2 Contexte

2.2.1 Evolution des applications Web

Aux premiers jours de l'internet, le World Wide Web [1] consistait en de simples pages web, des pages d'information constituée de ressources statistiques. Le flot d'informations était à sens unique, du serveur au navigateur. L'authentification des utilisateurs n'était souvent pas nécessaire car les mêmes informations étaient affichées à tous les utilisateurs. Les risques de sécurité découlaient exclusivement de l'hébergement des sites web, c'est-à-dire au niveau des serveurs web. En cas d'attaque, il n'y avait que peu de risques car l'information au niveau des serveurs était déjà accessible au grand public. Les attaques consistaient donc le plus souvent à des démaquillages des sites web.

Aujourd'hui, le World Wide Web est très différent de ce qu'il était à ses débuts. De nouveaux sites web plus poussés apparaissent : les applications Web. Ils ne se limitent plus à l'affichage de ressources statistiques. La majorité des sites web de nos jours, sont en réalité des applications web. Une application web est un site Web qui permet à ses utilisateurs de réaliser des tâches spécifiques. Le flux d'informations n'est plus à sens unique mais plutôt bidirectionnel entre le serveur et le client (navigateur, téléphone mobile, autre application). Le contenu présenté aux utilisateurs est spécifique à chaque utilisateur en fonction de préférences préalablement enregistrées ou d'autres paramètres de l'application.

En plus des applications web disponibles publiquement, nous avons les applications web internes aux entreprises qui soutiennent les entreprises dans l'accomplissement de tâches spécifiques : applications de gestion de ressources humaines et de la paie, applications de collaborations, applications de messagerie interne ainsi que les applications sur mesure propres au fonctionnement de l'entreprise (ERPs, applications de gestion des assurances, applications de gestion d'examens, etc.).

L'information traitée est très sensible de nos jours. Les applications web prennent en charge des fonctionnalités très délicates telles que les transactions financières ; il y a de cela quelques années, lorsqu'on voulait faire une transaction financière, il fallait aller à la banque et un agent le faisait

1. Système reliant des ressources hypertextes sur Internet grâce au protocole Http

pour vous alors qu'aujourd'hui, avec ces applications web, il est possible de faire ces transactions soit même en ligne en fournissant certaines informations. Ceci étant, si un attaquant arrivait à compromettre ce genre d'applications par exemple, il lui serait facile de faire des transactions frauduleuses et vider votre compte bancaire. De même, de nos jours, toute présence sur le net requiert la fourniture de données privées, il ne serait pas bien que ces informations tombent entre les mains d'individus malintentionnés. Il y a aussi la multiplication des sites marchands sur le net qui permettent de faire des achats en ligne. Qu'un individu malintentionné arrive à compromettre ce genre d'applications représenteraient de gros risques à la fois pour les propriétaires de ces applications dont le business repose essentiellement sur ces dernières mais aussi pour les utilisateurs qui auront fourni des informations très sensibles (mots de passe, numéros de carte de crédit entre autres).
Les applications Web manipulent aujourd'hui des données hautement sensibles et fournissent des informations très confidentielles.

2.2.2 Apparition des applications mobiles

Avec le développement fulgurant de l'industrie mobile au début des années 2000, les téléphones mobiles ne sont plus de vulgaires appareils dont l'utilité est limitée à la communication. Désormais, ils proposent des fonctionnalités plus poussées grâce à des systèmes d'exploitation embarqués ; nous avons notamment Android de Google et Ios de Apple. Ces systèmes d'exploitation mobiles font des appareils mobiles des mini ordinateurs offrant des fonctionnalités similaires à celles des ordinateurs. A partir de ce moment, ce fut l'explosion des applications mobiles dont les champs d'application sont infinis. Les spécificités techniques d'une application mobile lui confèrent de nombreux avantages par rapport aux applications mobiles :
- l'exécution est plus rapide : les éléments d'interface n'ont pas besoin d'être téléchargés depuis un serveur ;
- l'accès aux données de l'utilisateur est plus facile ; - l'utilisation est plus simple et plus intuitive ;
- certaines applications mobiles peuvent fonctionner hors ligne.
Bon nombre d'applications Web existent aussi en version mobile. Ces applications mobiles utilisent soit des navigateurs embarqués, soit des APIS exposées par l'application web. Les fonctions et les données manipulées par les applications mobiles sont généralement les mêmes que celles manipulées par les applications Web. Cela fait que les applications mobiles sont exposées aux mêmes risques que les applications web. Ainsi, pour une organisation, prendre en charge la sécurité de ses applications implique à la fois celles Web et celles mobiles.

2.3 Problématique

Software is at a tipping point. The rapid increase in connectivity, combined with a dramatic rise in the value of assets in our systems, and the increasing use of new protocols and technologies has resulted in applications that represent significant risk to the organizations that build and use them.

C'est dans cette optique que des initiatives ont été prises pour adresser les problèmes de sécurité rencontrés le plus souvent au niveau des applications Web et mobiles afin d'éveiller les organisations et les inciter à prendre ces problèmes à la source. Parmi ces initiatives, nous avons l'OWASP Top 10 et le Mobile 10 de l'OWASP qui publiés périodiquement et qui sont respectivement un classement des dix vulnérabilités les plus fréquentes au niveau des applications Web et des dix vulnérabilités les plus fréquentes au niveau des applications mobiles.
Hubso, étant une entreprise développeuse de solutions informatiques très sensibles pour des utilisateurs très variés et des clients souvent ciblés par des attaques informatiques,

2.4 Objectifs

Pour que Hubso puisse conserver sa compétitivité et faire face à ce problème de sécurité de ses applications, elle doit adopter

Deuxième partie

Etat de l’art sur la sécurité informatique

CHAPITRE 3

DÉFINITIONS

3.1 Sécurité informatique

La sécurité peut être définie comme étant une situation, un état dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque d'agression, de détérioration ou encore par le long processus visant à atteindre cet état. Lorsqu'on parle de sécurité dans le domaine des technologies de l'information et de la communication, on fait très souvent allusion à la sécurité de l'information. La sécurité de l'information, en anglais Information Security abrégé Infosec consiste en la mise en place d'un ensemble de stratégies pour gérer les processus, les outils et les politiques nécessaires pour prévenir, détecter, documenter et contrer les menaces à l'information. La sécurité de l'information recouvre donc toutes les techniques permettant d'assurer la protection de l'information. La sécurité de l'information se fonde sur 3 principes fondamentaux : - la confidentialité : c'est le fait d'assurer que l'information ne puisse être accessible qu'à ceux qui ont l'autorisation de la consulter. Cela sous-entend le fait de rendre inintelligible cette information aux personnes non autorisées ; - l'intégrité : assurer que l'information n'est pas modifiable par un tiers non autorisé. Elle consiste à certifier que les données n'ont pas été détruites ou altérées tant de façon intentionnelle qu'accidentelle ; - la disponibilité : assurer que l'information est accessible en temps voulu par ceux qui en ont l'autorisation. Ne pas pouvoir accéder à une information en temps voulu est semblable à la non-possession de celle-ci. Comme principes supplémentaire, nous notons :' - l'authentification : elle consiste à assurer l'identité d'un tiers et permet de garantir qu'un tiers est bien celui qu'il prétend être ; - la non-répudiation : le fait de ne pas pouvoir nier une action faite sur le système

3.2 Cryptographie

La sécurité informatique est un domaine pluridisciplinaire. En effet, pour arriver à ses buts, elle a, tout au cours utilisé, entre autres, la cryptographie. La cryptographie peut être définie comme un art et une science permettant de concevoir des techniques pour garder le secret des messages transmis. Voici les problèmes que doit résoudre la cryptographie : - la confidentialité - l'intégrité - l'authentification On voit ainsi que la sécurité informatique et la cryptographie partagent des objectifs similaires. Et c'est pour cette raison que tout au long de l'histoire, elle a été utilisée dans le domaine de la sécurité informatique. De même, les évolutions dans le domaine de la sécurité informatique ont souvent été rendus possibles grâce aux avancées de la cryptographie.

On distingue : - la cryptographie classique qui décrit la période d'avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle. Dans cette famille, on retrouve le chiffrement par substitution qui consiste, à remplacer, sans en bouleverser l'ordre les symboles d'un texte clair par d'autres symboles [1] et le chiffrement par transposition qui repose sur le bouleversement de l'ordre des symboles du message clair. Les techniques de chiffrement les plus connues dans cette famille sont le chiffrement de César et le chiffrement de Vigenère. - la cryptographie moderne qui utilise la puissance de calcul des ordinateurs pour affiner ces techniques de chiffrement. Dans cette famille, nous avons le chiffrement symétrique qui utilise une même clé pour le chiffrement et le déchiffrement (DES en est la technique la plus connue) et le chiffrement asymétrique qui utilise des clés différentes pour le chiffrement et le déchiffrement. RSA est l'algorithme de chiffrement asymétrique le plus utilisé

CHAPITRE 4

HISTORIQUE

4.1 Genèse

Le domaine de la sécurité des informations est très ancien. Déjà, dès l'antiquité, des techniques de chiffrement de l'information étaient utilisées. Vers 1900 av JC, le scribe de Khnumhotep II retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu'il dessinait. Vers 500 av. J.-C., les Spartiates ont développé un dispositif appelé Scytale, qui a été utilisé pour envoyer et recevoir des messages secrets. Plus récemment dans l'histoire, l'empereur romain Jules César utilisa la technique de chiffrement qui porte son nom (Chiffrement de César) afin de crypter ses messages personnels. Ces Expériences, Bien Que Ne Couvrant Que Le Principe De La Confidentialité, Sont Les Ancêtres De La Sécurité De L'information.
A cette époque, assurer la sécurité de l'information se résumait en un problème de cryptage de données. On utilisait alors la cryptographie classique avec le chiffrement par substitution[1] d'abord puis plus tard le chiffrement par transposition[2].

4.2 Seconde Guerre mondiale et guerre froide : tournant de l'histoire de la sécurité informatique

Avec le temps, les techniques permettant d'assurer la sécurité de l'information deviennent de plus en plus pointues. La seconde guerre mondiale et la guerre froide ont marqué un tournant dans l'histoire de nombreuses technologies, y compris celles qui ont façonné l'industrie de la sécurité de l'information.
En effet, durant cette période, de nouveaux moyens de communication apparaissent : la radio et le cinéma étaient les principaux vecteurs de l'information. Sur le champ de bataille, les différentes unités devaient coordonner leurs actions et pour ce faire des informations étaient échangées entre elles. Toutes ces communications étaient diffusées par radio et pouvaient être interceptées par l'ennemi. Il était d'une importance cruciale de rendre l'information inintelligible à l'ennemi puisqu'il s'agissait de communiquer sur les stratégies d'actions à mener. Pour protéger ces communications militaires, des systèmes très sophistiquées furent mises en place. Il s'agissait surtout de machines permettant de chiffrer l'information. Enigma était la machine de chiffrement la plus avancée de l'époque : elle sécurisait les communications des flottes et des troupes nazis en

leur permettant de chiffrer leurs messages par un chiffrement par substitution. Elle utilisait des algorithmes de chiffrement par substitution très poussés à l'époque. Elle avait la réputation d'être inviolable. Cependant, des experts en chiffrement polonais et britanniques ont réussi à trouver le moyen de casser Enigma en créant une machine connue sous le nom de « Bombe cryptographique » permettant de déchiffrer ses messages, donnant ainsi à la coalition antihitlérienne un avantage significatif ou « l'avantage définitif » selon Churchill et Eisenhower lors de la seconde guerre mondiale et soulignant du même pied l'importance capitale qu'a revêtu la sécurité de l'information lors de cette époque.

Puis, la seconde guerre mondiale laissa place à la guerre froide, une guerre d'opinion opposant deux blocs : d'un côté les états unis démocrates et de l'autre les russes, communistes. Ce fut la naissance d'une course à l'armement et à l'avancée technologique pour dominer le camp adverse. C'est durant cette période que les premiers ordinateurs sont créés. A cette époque, ils sont beaucoup plus utilisés comme outils de calcul pour des applications scientifiques et n'étaient pas très répandus. C'était des systèmes mono-utilisateurs logés dans de grande salle et il n'y avait pas communication entre ces différentes machines. La sécurité n'était pas une priorité et n'impliquait que le fait de sécuriser les salles où étaient installées ces machines. Du fait de leur puissance et de leurs nombreux avantages, de plus en plus d'ordinateurs et de systèmes d'exploitation furent créés. De même, la cryptographie entre dans une nouvelle ère : des techniques de chiffrement plus avancées sont mises en place grâce à la puissance de calcul des ordinateurs. C'est la naissance de la cryptographie moderne [1]. Avec la prolifération des terminaux distants sur les ordinateurs commerciaux, le contrôle physique de l'accès à la salle informatique n'était plus suffisant. En réponse à cela, des systèmes de contrôle d'accès logique ont été développés. (Un système de contrôle d'accès maintient une table en ligne des utilisateurs autorisés. Un enregistrement d'utilisateur type stocke le nom de l'utilisateur, son numéro de téléphone, son numéro d'employé et des informations sur les données auxquelles l'utilisateur était autorisé à accéder et les programmes qu'il était autorisé à exécuter. Un utilisateur peut être autorisé à afficher, ajouter, modifier et supprimer des enregistrements de données dans différentes combinaisons pour différents programmes.) Dans le même temps, les gestionnaires de système ont reconnu l'importance de pouvoir se remettre de catastrophes pouvant détruire le matériel et les données. Les centres de données ont commencé à faire régulièrement des copies sur bande de fichiers pour le stockage hors site. Les gestionnaires de centre de données ont également commencé à élaborer et à mettre en œuvre des plans de reprise après sinistre. Ce sont les premières politiques de sécurité entreprises. Cependant, même avec un tel système en place, de nouvelles vulnérabilités ont été reconnues au cours des années suivantes. Il fallait des systèmes plus fiables. Multics, un système d'exploitation multi utilisateurs fut créé en 1964. Ce fut la première fois que la problématique de la sécurité de l'information fut prise en compte en amont. En effet, dès la conception de Multics, les décisions prises (langages de programmation, architecture du noyau, etc.) prenaient en compte les exigences de sécurité. Les fonctions de sécurité de Multics comprenaient également le chiffrement des mots de passe, des audits de connexion et des procédures de maintenance logicielle. Les mots de passe dans Multics n'étaient jamais stockés en texte clair. Lorsqu'un utilisateur entrait son mot de passe, ce mot de passe était chiffré, puis comparé au mot de passe stocké sur le système. Cela permit de garder les mots de passes des utilisateurs en cas de dump système. De même, un journal d'audit de connexion enregistrait

l'heure, la date et le terminal de chaque tentative de connexion, et notifiait à l'utilisateur le nombre de tentatives de mot de passe incorrectes sur son compte depuis la dernière connexion réussie. Enfin, des procédures de maintenance logicielle, telles que la vérification du nouveau logiciel permettaient de maintenir le système sûr et épargné des régressions de sécurité. Au début des années 1970, alors que l'armée américaine était à la recherche de systèmes informatiques multi utilisateurs capables de protéger les informations classifiées, Multics lui fut recommandé. A cette époque, pour éprouver la sécurité des systèmes en place, il était très courant de faire appel à des Tiger Team. Il s'agissait d'experts rassemblés pour gérer des situations spéciales, régler des problèmes spécifiques le plus rapidement possible. Au début, leur travail consistait surtout en des revues manuelles de code pour détecter la source des bugs. Un peu plus tard, ils ont commencé à utiliser le « pentest » ou test d'intrusion.(C'est une méthode permettant d'évaluer la sécurité d'un système informatique à travers des tentatives d'intrusion à la manière d'un attaquant.) Dès 1969, l'ARPA (Advanced Research Project Agency), une agence dédiée aux projets de recherche avancée renommée plus tard en DARPA (Defense Advanced Research Project Agency) arriva à interconnecter les ordinateurs de quatre universités en un réseau afin de leur permettre de partager leurs résultats de recherche : ce réseau fut nommé l'Arpanet. Dans Arpanet, les utilisateurs se connaissaient plus ou moins et étaient pour la majorité des académiciens : la sécurité n'était pas un problème majeur dans ce « réseau d'amis ». C'est ce simple réseau de quatre nœuds sans aucune préoccupation de sécurité qui conduisit plus tard à la naissance d'Internet et du World Wide Web. Vers la fin des années 1970, l'analyse de codes source, qui était faite manuellement, vit une révolution. Lint, le premier outil d'analyse de codes source automatisée apparut. Initialement, il était destiné aux codes sources écrits en langage C. Lint était pratique pour trouver des bugs potentiels, mais était très lent et n'était pas équipé de la vue complète du programme. Il ne pouvait analyser qu'un seul fichier à la fois. Lint a ouvert la voie à la première génération d'outils destinés à la sécurité des applications informatiques qui, bien qu'ils aient été utiles pour trouver des bugs spécifiques, étaient assez maladroits et ne faisaient pas mieux que l'analyse manuelle. La décennie 1970 vit également l'apparition des premiers micro-ordinateurs. Au début, parce qu'ils étaient entièrement autonomes et généralement sous le contrôle d'un seul individu, il y avait peu de problèmes de sécurité. Très rapidement ils passent d'un passe-temps pour les passionnés d'informatique en un sérieux outil de travail. A partir de ce moment, des logiciels commencent à être créés pour les ordinateurs. L'on sait que pour cela, il fallait écrire du code source parfois enclin à des bugs et à des vulnérabilités de sécurité.

4.3 Evolutions récentes

CHAPITRE 5

CONTEXTE

5.1 Contexte juridique

5.2 Contexte organisationnel

Troisième partie

Etat de l’art sur la sécurité des applications Web

Quatrième partie

Analyse et Conception

Cinquième partie

Réalisation

Sixième partie

Bilan et Perspectives

CONCLUSION

Ce stage a été une étape très importante dans notre insertion dans le monde professionnel. Il a été l'occasion pour nous de mettre en pratique nos connaissances théoriques acquises tout au cours de notre cycle. Tout d'abord, nous avons eu besoin de faire l'étude du système existant. Cela a été la partie la plus difficile parce qu'il fallait avoir au moins une certaine compréhension des aspects électriques tels que les types de puissances. Ensuite, nous avons eu à faire une analyse et une conception du nouveau système En outre, il faudra aussi noter que la phase d'analyse a été la phase la plus longue car permet de mieux comprendre et de bien cerner les besoins. Aussi il nous faut dire qu'il reste a implémenter la solution proposée car le temps ne nous l'a pas permis.