IFT6271–Sécurité Informatique
(Solution de l'exemple, Hiver 2014)

Louis Salvail[1]

Université de Montréal (DIRO), QC, Canada
salvail@iro.umontreal.ca
Bureau: Pavillon André-Aisenstadt, #3369

3 Exemple–politique de sécurité

3.1 Les menaces.

Voici une liste de menaces supplémentaires au bon déroulement d'un examen donné dans les conditions de l'énoncé. Rappelons simplement le fait que les examens autorisent ou nécessitent l'utilisation d'un ordinateur portable pour essentiellement trois choses:

1. Pour l'accès à des notes de cours, des notes personnelles, à des manipulation de données (i.e. via des logiciels), l'énoncé de l'examen,
2. pour rédiger l'examen et
3. pour la remise de l'examen vers un serveur prévu à cet effet.

Dans cette section, nous décrivons les nouvelles attaques qui sont rendues possibles par l'ajout des éléments 1, 2 et 3 au déroulement normal des examens. Nous ne traitons donc pas des menaces qui existent déjà dans le cadre normal des examens à moins que leur déploiement en soit facilité par le nouvel environnement.

Nous donnons une liste de menaces selon la classification STRIDE. Nous choisissons cette classification puisqu'une classification par les effets semble préférable à ce point. Puisque la politique de sécurité qui suivra devra s'inspirer des menaces identifiées ici, une identification par effet est une façon simple de diriger sa rédaction.

Spoofing Identity: Dans le cas qui nous intéresse, la personnification d'un autre usager permettrait de soumettre un examen au nom d'un autre étudiant. La personne malveillante peut être:
1. Un étudiant présent à l'examen, ou
2. un adversaire externe (situé à l'extérieur de la salle d'examen).

L'effet d'une telle attaque est l'attribution d'un examen remis à autre que celle/celui qui l'a fait. Ceci peut éventuellement mener à une mauvaise attribution des notes pour des étudiants honnêtes. Une attaque avec ces effets peut être lancée avant ou pendant le déroulement de l'examen.

Tampering: L'adversaire peut manipuler des données sans qu'il n'y soit autorisé. Le résultat étant des modifications des réponses d'un examen données par un étudiant ou même des modifications à l'énoncé de l'examen récupéré par certains étudiants. L'effet d'une telle attaque dans notre situation est:
1. L'annulation d'un examen mené honnêtement,

2. une note plus basse ou plus haute que méritée attribuée à un étudiant honnête, ou
3. une note plus haute attribuée à un étudiant malhonnête.

Une attaque avec ces effets doit être lancée pendant ou avant le déroulement de l'examen.

Repudiation: Dans notre situation, un étudiant malhonnête pourrait nier avoir remis un exament lui étant attribué correctement. Dans notre scénario, il s'agirait de nier qu'une remise ait été faite après que celle-ci soit transmise au serveur de réception L'effet pourrait être une entrave au déroulement normal d'un examen et/ou et une mauvaise attribution des notes. Une attaque avec ces effets doit prendre place pendant ou après le déroulement de l'examen.

Information disclosure: Dans notre situation, le résultat d'une telle menace est ou bien le plagiat ou bien un avantage non légitime à la réalisation d'un examen. Une telle menace peut se décliner de trois façons:

1. Un étudiant malhonnête réussi à accéder à des données relatives à l'examen en cours qui sont du domaine d'un autre étudiant à son insu,
2. Un étudiant malhonnête transmet des données relatives à l'examen en cours à un autre étudiant et
3. Un étudiant réussit à obtenir le questionnaire de l'examen avant la tenue de l'examen.

Encore une fois, les conséquences peuvent se faire sentir dans l'attribution juste des notes. Les attaques avec ces effets doivent être conduites pendant le déroulement de l'examen pour les points 1 et 2 et avant l'examen pour les points 3.

Denial of service: Un adversaire peut interférer avec le déroulement normal d'un examen en empêchant la remise vers le serveur de réception. Une telle attaque peut être lancée de l'intérieur ou de l'extérieur pendant le déroulement de l'examen. L'effet d'une telle attaque peut aller jusqu'à l'annulation d'un examen.

Élévation des privilèges: Une telle attaque permettrait à l'adversaire d'obtenir les droits de l'un ou l'autre des usagers avec privilèges supérieurs suivants:

1. les droits d'un étudiant inscrit sur son portable,
2. les droits d'administrateurs sur le serveur de réception et
3. les droits des étudiants inscrits à un examen EXAPORTABLE.

L'effet pourrait aller d'une mauvaise attribution des notes jusqu'à une annulation de l'examen. Une telle attaque peut être menée pendant ou avant l'examen à partir de l'intérieur ou de l'extérieur de la salle.

3.2 Politique de sécurité pour les usagers du système

Préambule.† La présente politique porte sur le bon déroulement des examens EXAPORTABLE tenus dans les salles prévues à cet effet (i.e. *les salles* EXAPORTABLE). Elle établit les règles qui doivent être suivies par tous les usagers impliqués. Elle énonce les règles d'utilisation du matériel informatique rendu disponible ou autorisé pendant le déroulement des examens EXAPORTABLE. Elle doit être interprétée en complément aux règles en vigueur lors des examens traditionnels. Cette politique ne traite pas des règles déjà en vigueur lors des examens traditionnels. Pour ces règles déjà établies, consultez la politique des examens de l'université.

Objectifs. Les objectifs principaux de cette politique sont:

- Contribuer au déroulement équitable d'examens EXAPORTABLE.
- Assurer un déroulement normal de ces examens en évitant que les systèmes mis à disposition ne soient perturbés.
- Encadrer les mesures de protection pour qu'elles soient efficaces et deployées de façon uniforme dans toutes les salles EXAPORTABLE.

Définitions.† Les termes suivants seront utilisés par la suite:

EXAPORTABLE: Le nom donné aux examens où le portable est autorisé et où un serveur de réception est mis à disposition des étudiants pour la remise de leur examen. Ces examens se déroulent dans une salle préparées à cet effet que l'on nomme *salle* EXAPORABLE.

EXAMEN: Désgine l'énoncé pour lequel les étudiants doivent apporter des réponses dans le cadre d'un examen EXAPORTABLE.

USAGER(S) EXAPORTABLE: Le professeurs ou chargé de cours qui donne un examen EXAPORTABLE et les étudiants inscrits à un examen EXAPORTABLE.

TECHNICIEN: Toute personne qui par sa fonction est amenée à installer des ressources informatiques dans une salle EXAPORTABLE.

TECHNICIEN EN CHEF: Toute personne qui par sa fonction a la responsabilité des ressources informatiques dans les salles EXAPORTABLE.

DIRECTEUR DE LA SÉCURITÉ INFORMATIQUE: Personne en charge des politiques de sécurité pour les systèmes de TI dans cette université.

SERVEUR **ou** SERVEUR DE RÉCEPTION: Désigne le serveur de remise des examens tenus dans les salles EXAPORTABLE.

PORTABLE: Désigne un ordinateur portable qui n'est pas un téléphone mobile.

BLUETOOTH: Désigne les techniques radio courte distance qui peuvent être utilisées par les portables pour s'interconnecter.

WIFI: Désigne les techniques basés sur les ondes radios permettant aux portables de se connecter en réseau.

RÉSEAU DE L'UNIVERSITÉ: Les équipements de télécommunication et le câblage qui sont installés dan les bâtiments de l'université.

RÉSEAU LOCAL: Désigne le réseau sur lequel les usagers se branchent dans une salle EXAPORTABLE. Aussi appelé réseau EXAPORTABLE.

AUTHENTIFIANT: L'information confidentielle qu'un étudiant reçoit pour avoir accès aux ressources mis à disposition dans les salles EXAPORTABLE.

Champ d'application. Cette politique s'applique aux usagers EXAPORTABLE. Elle ne s'applique pas lors des examens qui ne sont pas tenus dans une salle EXAPORTABLE.

Dispositions générales.

1. Toutes les règles qui s'appliquent aux examens traditionnels s'appliquent aussi aux examens EXAPORTABLE.
2. Tous les usagers doivent s'authentifier pour accéder au réseau local.
3. Si le déroulement normal de l'examen EXAPORTABLE est compromis alors un technicien doit être contacté pour prendre les dispositions à cet effet.

Dispositions pour les étudiants.

1. Aucun étudiant n'est autorisé à nuire au bon déroulement de l'examen. Ceci inclut toute tentative d'interférence avec le bon fonctionnement du serveur.
2. Aucun étudiant n'est autorisé à divulguer son authentifiant EXAPORTABLE à quiconque.
3. Aucun étudiant ne peut se connecter à l'internet durant l'examen.
4. Aucun étudiant n'est autorisé à tenter d'établir une connexion avec l'extérieur de la salle EXAPORTABLE que ce soit vers l'internet ou n'importe quel autre réseau disponible.
5. Aucun portable n'est autorisé à utiliser une connexion WiFi ou BlueTooth durant le déroulement de l'examen. Les émetteurs pour ces signaux doivent être désactivés avant d'entrer dans la salle EXAPORTABLE.
6. Aucun étudiant n'est autorisé à tenter d'espionner le travail d'un autre étudiant que ce soit de façon physique ou informatique.
7. Aucun étudiant n'est autorisé à transmettre de l'information à un autre étudiant durant l'examen en cours que ce soit de façon physique ou informatique.
8. Les étudiants ne doivent d'aucune façon faciliter le plagiat.
9. L'étudiant accède au questionnaire de l'examen à partir de la salle EXAPORTABLE pendant la période de l'examen. Celui-ci est téléchargeable en utilisant son authentifiant sur le serveur de réception à l'adresse `https://www.exaport.umontreal.ca/iftxyzw/`, où xyzw est le numéro du cours.
10. La taille maximale d'un fichier transmis au serveur de réception est de 3.0Mo.
11. L'étudiant ne doit communiquer qu'une seule fois avec le serveur de réception durant le déroulement d'un examen EXAPORTABLE.
12. Le seul type de fichier qui puisse être transmis au serveur de réception est PDF.
13. Lorsque l'étudiant a remis son examen au serveur de réception, la remise est faite et est irrévocable. Aucune autre remise ne peut être faite. L'étudiant doit alors quitter la salle et n'est plus autorisé à y revenir durant l'examen.

Dispositions pour les professeurs.

1. Le professeur doit informer le support technique pour les salles EXAPORTABLE de la quantité de données à télécharger sur le serveur de réception ainsi que le nombre d'étudiants inscrits. Cette information doit être donnée au moins 3 jours avant la tenue de l'examen.
2. L'énoncé de l'examen doit être en format PDF, déposé par le professeur sur le serveur de réception au plus 24 heures d'avance. Le professeur dépose son examen à l'adresse: `https://www.exaport.umontreal.ca/iftxyzw-profs`
3. Le professeur ne doit jamais dévoiler à quiconque son authentifiant pour le serveur de réception.
4. Le professeur doit autant que possible s'assurer que les étudiants ne communiquent pas entre eux par WiFi ou BlueTooth.
5. Le professeur doit rappeler aux étudiants de désactiver les émetteurs Wifi et BlueTooth avant le début de l'examen.
6. L'examen doit être conçu pour que l'examen complété puisse toujours être remis dans un fichier d'au plus 3.0Mo.
7. Le professeur doit distribuer cette politique aux étudiants d'un cours où un examen EXAPORTABLE aura lieu. La distribution doit se faire avec la plan de cours.

Rôles et responsabilités.†

1. **Usager:** Chaque usager doit se conformer à la présente politique.
2. **Étudiant:** L'étudiant ne doit en aucune façon atténuer ou contourner les dispositifs de sécurité qui s'appliquent aux ressources informatiques mis à disposition dans les salles EXAPORTABLE. L'étudiant est aussi responsable de son propre matériel informatique (portable). En particulier, il est responsable des violations éventuelles des dispositions aux étudiants lorsqu'elles originent de sa machine.
3. **Professeur:** Le professeur, en plus de se conformer à la présente politique, doit faire de son mieux pour que le déroulement de l'examen soit équitable. Il doit s'assurer que les examens peuvent être conduits selon les règles énoncées plus haut.
4. **Directeur de la sécurité informatique:** Sous l'authorité du bureau du recteur, le directeur de la sécurité est responsable de la gestion de cette politique pour qu'elle soit appuyée par la direction de l'université.

Non-respect de la politique. Si un étudiant ne se conforme pas à cette politique alors les pénalités sont les même qu'en cas de plagiat lors d'examens traditionnels. Si l'étudiant n'a pas l'énoncé de l'examen lors de sa tenue, il en est tenu responsable.

Un professeur qui ne se conforme pas à cette politique peut voir son examen annulé. Les étudiants peuvent déposés une plainte qui sera étudiée par un comité formé par le directeur du département du professeur ainsi que l'ombudsman de l'université.

3.3 Politique pour les techniciens

Préambule.† La présente politique porte sur la sécurité des salles EXAPORTABLE où des examens EXAPORTABLE peuvent être tenus. Elle énonce les règles qui doivent être suivies par les techniciens informatiques lors de l'installation des salles EXAPORTABLE ainsi que lors de la configuration du serveur de réception. Ces salles mettent à disposition un réseau filaire sur lequel les portables des étudiants peuvent se brancher pour avoir accès au serveur de réception.

Objectifs. Les objectifs principaux de cette politique sont:

- Contribuer à la mise en place des systèmes mis à disposition dans les salles EXAPORTABLE.
- Assurer un déroulement normal des examens EXAPORTABLE en évitant que les systèmes mis à disposition ne soient perturbés par des actions malveillantes ou accidentelles.
- Permettre la détection de certaines tentatives malveillantes.
- Encadrer les mesures de protection techniques pour qu'elles soient efficaces et deployées de façon uniforme dans toutes les salles EXAPORTABLE.
- Assurer le bon fonctionnement du serveur de réception et sa résistance aux attaques.

Définitions.† Voir les définitions données dans la politique de sécurité pour les usagers.

Champ d'application. Cette politique s'applique aux techniciens responsables de la préparation des salles EXAPORTABLE. Elle s'applique également aux techniciens avec des droits d'administrateur sur le serveur de réception.

Dispositions générales.

1. Les salles EXAPORTABLEs demeurent vérouillée en tout temps.
2. Un authentifiant EXAPORTABLE est donné à chaque usager du système. Cet authentifiant permet le téléchargement des examens complétés par les étudiants sur le serveur de réception: `https://www.exaport.umontreal.ca/iftxyzw`. Cet authentifiant peut être le même que celui permettant aux étudiants d'avoir accès au réseau de l'université.
3. Un technicien du support technique doit être disponible pour la résolution des problèmes pour chaque examen EXAPORTABLE.

Dispositions pour les techniciens.

1. Le support technique pour les examens EXAPORTABLEs doit s'assurer que le serveur de réception est complètement fonctionnel avant la tenue de chaque examen.
2. Avant la tenue d'un examen dans une salle EXAPORTABLE, un technicien doit s'assurer que la salle est configurée en accord avec cette politique.
3. L'accès aux réseaux WIFI doit être rendu difficile sinon impossible à partir d'une salle EXAPORTABLE.
4. Le réseau EXAPORTABLE n'est connecté à aucun autre réseau que ce soit l'internet ou le réseau local de l'université.
5. Le serveur de réception n'accepte que des connexions à partir d'une salle EXAPORTABLE, d'un professeur donnant un examen EXAPORTABLE et un administrateur système.
6. Le réseau EXAPORTABLE ne permet de communiquer qu'avec le serveur de réception. L'accès au réseau local de l'université ou à l'internet doit être rendu impossible.
7. Le réseau EXAPORTABLE est un réseau filaire ethernet qui ne permet aux étudiants que de communiquer avec le serveur de réception. Cette connexion est de type HTTPS (serveur WEB qui roule sur le serveur de réception) pour la remise de l'examen complété ainsi que pour le téléchargement de l'énoncé.
8. Le serveur de réception pour un examen en ift-xyzw est disponible à l'adresse: `https://www.exaport.umontreal.ca/iftxyzw/`. L'énoncé est disponible à cette adresse et il est possible d'y déposer un examen complété. Seuls les étudiants inscrits à un examen EXAPORTABLE peuvent s'y connecter.
9. Les connexions au serveur de réception par les étudiants ne sont possibles que durant le déroulement de l'examen.
10. La seule façon de se connecter au serveur de réception est sur le port 80 (i.e. port WEB) à moins d'être un administrateur système.
11. Le serveur de réception n'accepte pas le téléchargement d'une examen complété de plus de 3.0 Mo.
12. Le serveur de réception n'accepte que les fichiers de type PDF pour les énoncés ainsi que les examens complétés.

13. Le serveur de réception doit mettre à jour un fichier log de toutes les requêtes faites au serveur de réception durant un examen EXAPORTABLE.
14. Le serveur de réception re-transmet à l'étudiant l'examen qu'il est sur le point de remettre pour qu'il soit certifié par celui-ci. Si l'étudiant ne certifie pas le fichier alors la requête est annulée.
15. Un système de détection de tentative de connexion sans fil doit être installé dans chaque salle EXAPORTABLE (sniffer) même aucun signal WIFI n'est perceptible la plupart du temps.
16. Chaque remise doit clairement indiquer l'identité de son auteur. Le serveur de réception ajoute le nom de l'étudiant, son code permanent, l'heure à laquelle l'examen a été reçu, l'ordre de la remise et une emprunte authentifiant le fichier reçu.
17. Les fichiers transmis au serveur de réception sont conservés sur le serveur.
18. Les fichiers sauvés correspondants à un examen EXPORTABLE sont conservés pour deux trimestres. Le support peut détruire ces données qu'après ce délai.

Dispositions pour la fiabilité et en cas de problèmes.

1. Un technicien en chef doit pouvoir intervenir rapidement en cas de problème. Il doit être disponible pendant le déroulement de chaque examen EXAPORTABLE.
2. La configuration des salles EXAPORTABLE doivent être testées régulièrement pour s'assurer de leur bon fonctionnement.
3. La mauvaise qualité des receptions WiFi doit être testée régulièrement (et juste avant chaque examen) dans les salles EXAPORTABLE.

Rôles et responsabilités.[†]

1. **Technicien:** Il doit faire son travail dans le respect de cette politique.
2. **Technicien en chef:** Doit vérifier que chaque installation est faite en conformité avec cette politique. Le technicien en chef est responsable de la bonne préparation des salles EXAPORTABLE. Le technicien en chef est aussi responsable de faire en sorte que cette politique soit décrétée par le directeur de la sécurité informatique de l'université.
3. **Directeur de la sécurité informatique:** Le directeur de la sécurité est responsable de la gestion de cette politique pour qu'elle porte l'appui de la direction de l'université.

3.4 Mécanismes

Voici une liste non-exhaustive des mécanismes qui peuvent être mis en place pour satisfaire les objectifs de la politique de sécurité. Cette politique est énoncée aux sections précédentes. Nous distinguons les mécanismes selon leur type: physique/technologique ou non. Nous ne donnons que quelques mécanismes sans prétendre qu'il s'agisse d'une liste exhaustive. En particulier, nous laissons de côté les mécanismes pour la résolution des problèmes techniques.

Non-physique. Voici quelques mécanismes qui ont pour but de sécuriser les salles EXAPORTABLE ainsi que le déroulement d'un examen.

1. Les émetteurs WiFi de l'université situés près d'une salle EXAPORTABLE sont éteints.
2. Le professeur (qui organise des examens EXAPORTABLE) doit reçevoir une formation au sujet des fonctions du serveur de réception EXAPORTABLE.
3. Le professeur s'assure que tous les mécanismes soient fonctionnels au moins 15 minutes avant le début de l'examen et au plus 60 minutes avant.
4. Les étudiants doivent signer une déclaration du respect des dispositions relatives aux étudiants de la politique de sécurité pour les usagers.
5. La politique de sécurité pour les usagers est remise à chaque étudiant avec le plan de cours au premier cours du trimestre. La politique est décrite par le professeur ainsi que la disposition précédente (i.e. disp. 4).

Physique et Logiciel. En premier lieu, nous énumérons des mécanismes de sécurité physiques, excluant le réseau EXAPORTABLE en tant que tel. Ces mesures tentent de rendre les communications (sans passer par le réseau filaire) entre les portables des étudiants le plus difficile possible.

1. La salle est munie d'un brouilleur WiFi/BlueTooth si autorisé, autrement des *sniffers* peuvent être utilisés.
2. Chaque table peut aussi être dotée d'une antenne Bluetooth pour détecter les connexion de ce type.

Les mécanismes qui suivent visent à sécuriser le réseau.

1. Le serveur de réception refuse toutes les connexions qui ne sont pas initiées par des étudiants inscrits à un examen EXAPORTABLE pendant le déroulement de celui-ci.
2. Chaque place d'étudiant dispose d'un cable ethernet lui permettant de se connecter au réseau EXAPORTABLE. Pour s'assurer que les étudiants ne peuvent communiquer entre eux, nous utilisons un commutateur avec filtrage de paquets. En outre, le filtrage de paquets ne laisse passer que les paquets provenant d'une adresses IP d'un étudiant vers le port 80 du serveur de réception. Ce filtrage rejète toutes les autres connexions comme celles entre étudiants. Utiliser un commutateur est préférable à un concentrateur (i.e. hub) car ce dernier transmet les messages à chaque port, ce n'est pas le cas des commutateurs qui ne transmettent qu'au port de réception. Le serveur de réception est également connecté au commutateur.
3. Le serveur de réception est également un serveur DNS permettant aux étudiants de s'y connecter en utilisant l'adresse `http://www.exaport.umontreal.ca` plutôt que son adresse IP.
4. Le commutateur refuse les connexions multiples des étudiants vers le serveur de réception (i.e. déni de service interne). Le commutateur peut se comporter comme un mur coupe-feu.
5. Un mur coupe-feu est placé entre le serveur de réception et le réseau local de l'université. Il n'accepte que les connexions sur le port 80 du serveur. Aucune autre connexion n'est possible à moins d'en être un administrateur système.

6. Le mur n'accepte que les connexions à partir d'une machine enregistrée de l'université.
7. Le mur coupe-feu est capable de filtrage applicatif pour la protection contre les attaques qui visent un déni de service (déni de service externe).
8. Puisque SSL est utilisé pour transmettre un fichier serveur, son authenticité ainsi que sa confidentialité sont garanties. Ceci s'applique aux examens complétés ainsi qu'à l'énoncé.
9. Le serveur peut annuler une connexion lorsque le fichier (lu par paquets) est plus grand que 3.0Mo. Il peut également annuler une connexion lorsque le fichier n'est pas de type PDF. La même chose lorsqu'un énoncé y est déposé. Si le type n'est pas PDF alors la connexion est annulée.
10. Le serveur peut tenir un log de toutes les connexions.
11. L'activité sur le réseau local peut aussi être monitorée par des logiciels qui roulent sur le serveur de réception. Un exemple est `ActivityMonitor4.4` qui permet de voir ce que les usagers d'un réseau local exécutent.

3.5 Politiques, Mécanismes et Menaces

Discutons finalement de la façon dont les menaces identifiées sont evitées par les politiques et les mécanismes identifiés. Cette liste n'est pas exhaustive. Certaines dispositions des politiques ne sont pas discutées ici.

Spoofing identity: La remise des examens se fait via une connexion SSL puisque le serveur WEB est accessible seulement à travers une connexion HTTPS. La connexion nécessite une authentification de l'usager par un mot (phrase) de passe comme énoncé dans la politique aux techniciens. Si les authentifiants des usagers sont privés alors un étudiant ne pourra pas personnifier un autre étudiant. Un adversaire externe ne pourra pas se connecter en usurpant l'identité d'un étudiant à son insu si ce dernier désactive ses connexions WiFi comme énoncé dans la politique aux usagers. Ces techniques permettent d'éviter les attaques montées pendant l'examen. Pour les attaques lancées avant l'examen, la politique de sécurité pour les usagers accorde la responsabilité à l'étudiant. Il doit absolument garder secret son authentifiant.

Tampering: Les données importantes (l'examen complété) transmises au serveur de réception par les usagers sont sécurisées par SSL (HTTPS). Il en résulte que les données ne peuvent être manipulées sans être détectées. En supposant le réseau à l'abris de l'élimination des paquets par un tiers, il en résulte que ces manipulations devraient être difficiles à exécuter. Les dispositions prisent dans la politique aux usagers permettent de décourager l'étudiant à entreprendre de telles actions.

Repudiation: Les connexions SSL au serveur sont documentées. Ceci permet de s'assurer qu'un étudiant a bien déposé son examen sur le serveur WEB. Les logiciels qui monitorent les connexions peuvent aussi aider à détecter les actions suspectes. Puisque la connexion SSL peut seulement être établie avec un usager qui a donné son authentifiant, les signatures ne sont pas utiles ici. Sous l'hypothèse que les authentifiants demeurent privés (voir politique aux usagers), le dépôt de l'examen indique son propriétaire d'une façon qui ne puisse être niée. En fait, toutes les communications SSL sont authentifiées par CAM. Ils ne peuvent donc pas être répudiés et imputés à un autre étudiant (i.e. seul le prof ou le serveur pourrait avoir remis cet examen, sans confiance dans le prof tout le système est bien inutile...).

Information disclosure: SSL permet de sécuriser les communications d'un usager honnête. Les communication avec l'extérieur sont quant à elles rendus difficiles par l'utilisation d'un brouilleur. Les communications de l'intérieur sont rendus difficiles par l'architecture du réseau et les règles du commutateur. La politiques décourage de telles actions. Le fait d'utiliser un commutateur avec règles qui empêchent les communications entre participants permet d'éviter les communications entre les étudiants.

Denial of service: Le mur coupe-feu permet une protection contres ces attaques comme énoncé dans la politique de sécurité aux techniciens. Le point 7 des mécanismes physiques indiquent comment ce genre d'attaques peut être évité par le mur coupe-feu. La politique aux usagers énonce aussi des mesures de découragement. Les fichiers sont toujours vérifiés quant à leur taille et format.

Élévation des privilèges: La protection contre l'élévation des privilèges dépend des défenses du serveur de réception. Le mur coupe-feu permet une protection avant l'examen, pendant et après l'examen. Une disposition de la politique pour techniciens assure aussi que le serveur n'est pratiquement pas accessible lorsqu'il n'y a pas d'examen. Le serveur de réception est également sécurisé par les dispositions générales des serveurs WEB de l'université.