Génie Logiciel
3IF-GL

Security by design

Omar Hasan

Génie logiciel et la sécurité

Génie logiciel

Le génie logiciel est une science qui étudie les méthodes de travail et les bonnes pratiques des ingénieurs qui développent des logiciels.

Le génie logiciel s'intéresse en particulier aux procédures systématiques qui permettent d'arriver à ce que des logiciels de grande taille correspondent aux attentes du client, **soient fiables**, aient un coût d'entretien réduit et de bonnes performances tout en respectant les délais et les coûts de construction. [1]

[1] Marylène Micheloud et Medard Rieder, *Programmation orientée objets en C++: Une approche évolutive*, PPUR presses polytechniques, 2002

Fiabilité (dependability)

La **disponibilité (availability)** est exprimée par la probabilité que le système délivre le service attendu à un instant donné.
Uptime / Total time (Uptime + Downtime). Exemple : 54 min / 60 min = 90 %

La **fiabilité (reliability)** est la caractéristique du système exprimée par la probabilité qu'il délivre le service attendu pendant une durée déterminée.
Mean Time Between Failure (MTBF) : total time in service / number of failures.
Exemple : 1 heure / 2 = 30 minutes

La **maintenabilité (maintainability)** caractérise l'aptitude du système à être réparé quand il est défaillant, ou à évoluer.

La **sécurité-innocuité (safety)** caractérise l'aptitude du système a ne pas encourir de défaillances catastrophiques.

La **sécurité-confidentialité (security)** caractérise l'aptitude du système a se prémunir contre les accès ou manipulations non autorisées (virus, attaques,...)

Sécurité

Sécurité ∈ Fiabilité ∈ Exigences d'un logiciel

La sécurité est un attribut non fonctionnel d'un logiciel qui le permet de se défendre contre des attaques.

Objectifs de la sécurité

Objectifs de la sécurité

Objectif	Description
Confidentialité	La confidentialité est un élément nécessaire de la vie privée. C'est un attribut de notre capacité de protéger nos données à l'accès non autorisé.
Intégrité	L'intégrité se réfère à la capacité d'empêcher nos données d'être modifiés de manière non autorisée ou indésirable.
Disponibilité	La disponibilité fait référence à la capacité d'accéder nos données lorsque nous en avons besoin. Une attaque qui mène à la perte de disponibilité s'appelle une attaque de « Denial of Service (DoS) ».

D’autres objectifs de la sécurité

Objectif	Description
Authentification	L'authentification désigne le processus visant à confirmer qu'un commettant est bien celui qu'il prétend être. Quelques facteurs d'authentification qui peuvent être utilisés pour confirmer l'identité d'un commettant: • Utiliser une information que seul le commettant connaît. • Utiliser une information unique que seul le commettant possède. • Utiliser une information que seul le commettant peut produire.
Non-Répudiation	La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.
Responsabilité « Accountability »	L’assurance de la traçabilité des événements permettant de remonter jusqu'à une personne ou un processus à l'origine d'une action.

Types d’attaque

Type of attack	Description	Objectives of security defeated
Interception	Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.	Confidentiality
Interruption	Interruption attacks cause our assets to become unusable or unavailable for our use.	Integrity Availability
Modification	Modification attacks involve tampering with our asset.	Integrity Availability
Fabrication	Fabrication attacks involve generating malicious data, processes, or messages.	Integrity Availability

Attaques contre la sécurité, exemples

Un système décentralisé pour additionner des nombres privés

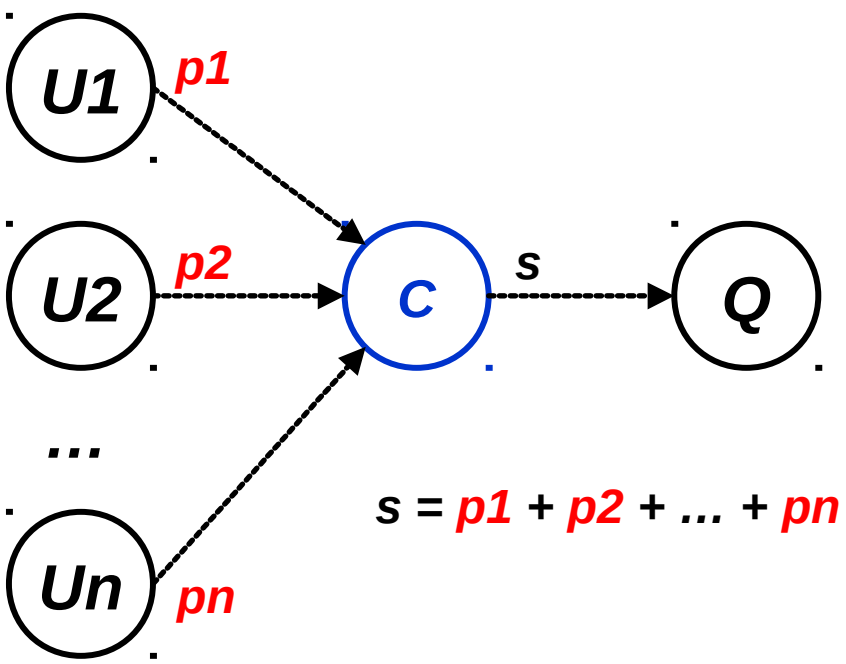
Utilisateur	Nombre
U1	5
U2	3
U3	-9
U4	4
Somme :	*3*

Respect de la confidentialité

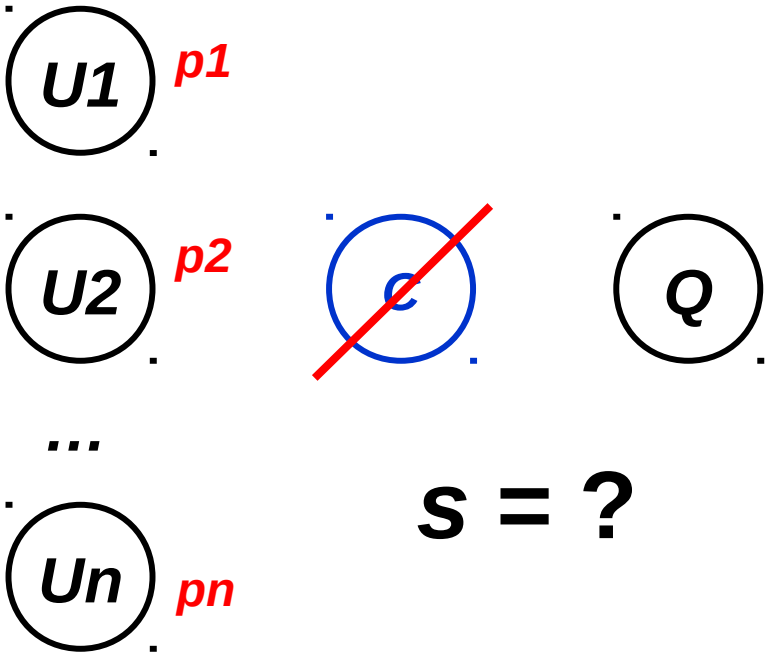
Utilisateur	Nombre privé
U1	X
U2	X
U3	X
U4	X
Somme :	*3*

Un système décentralisé pour additionner des nombres privés

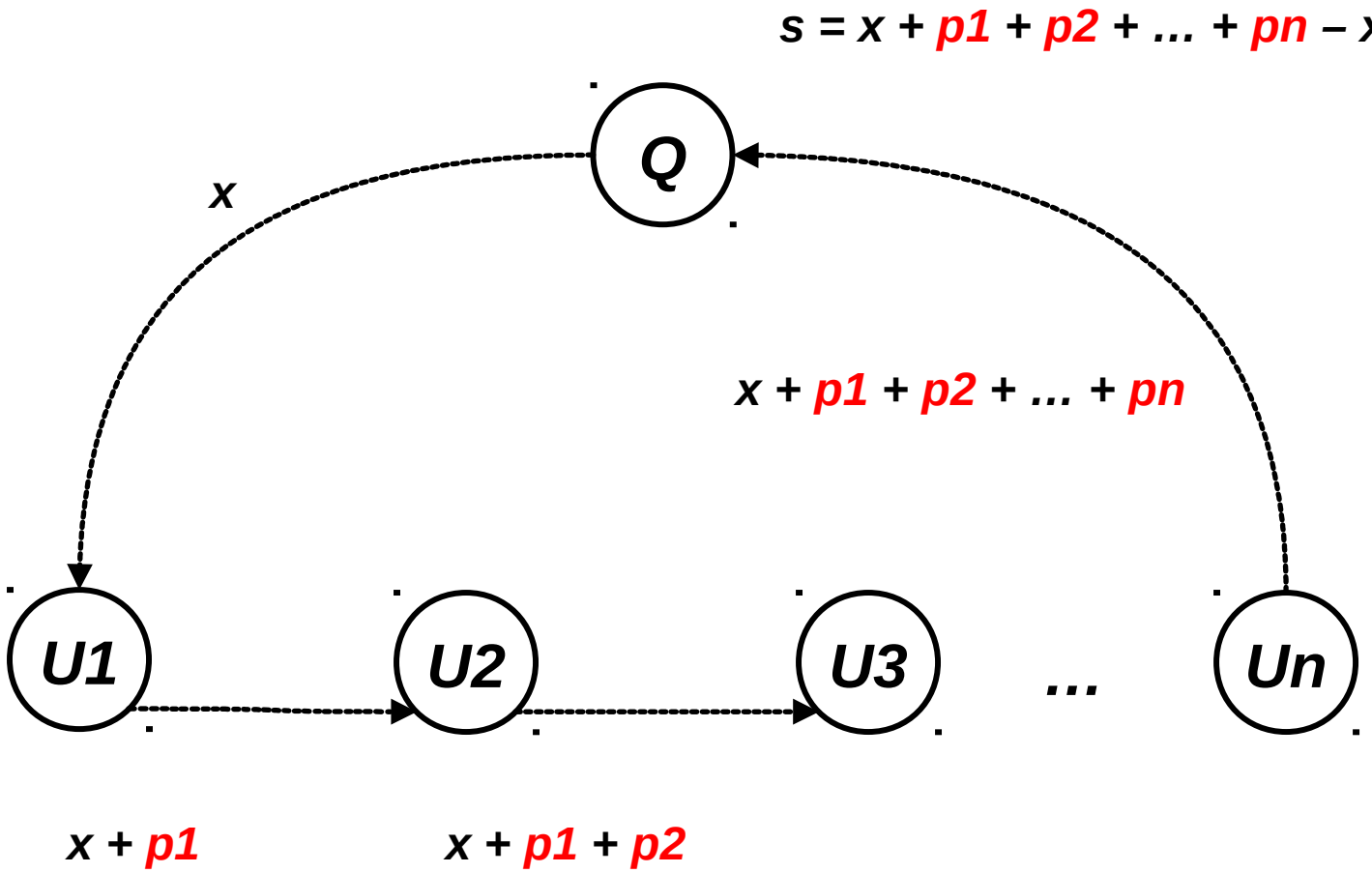
Centralisé



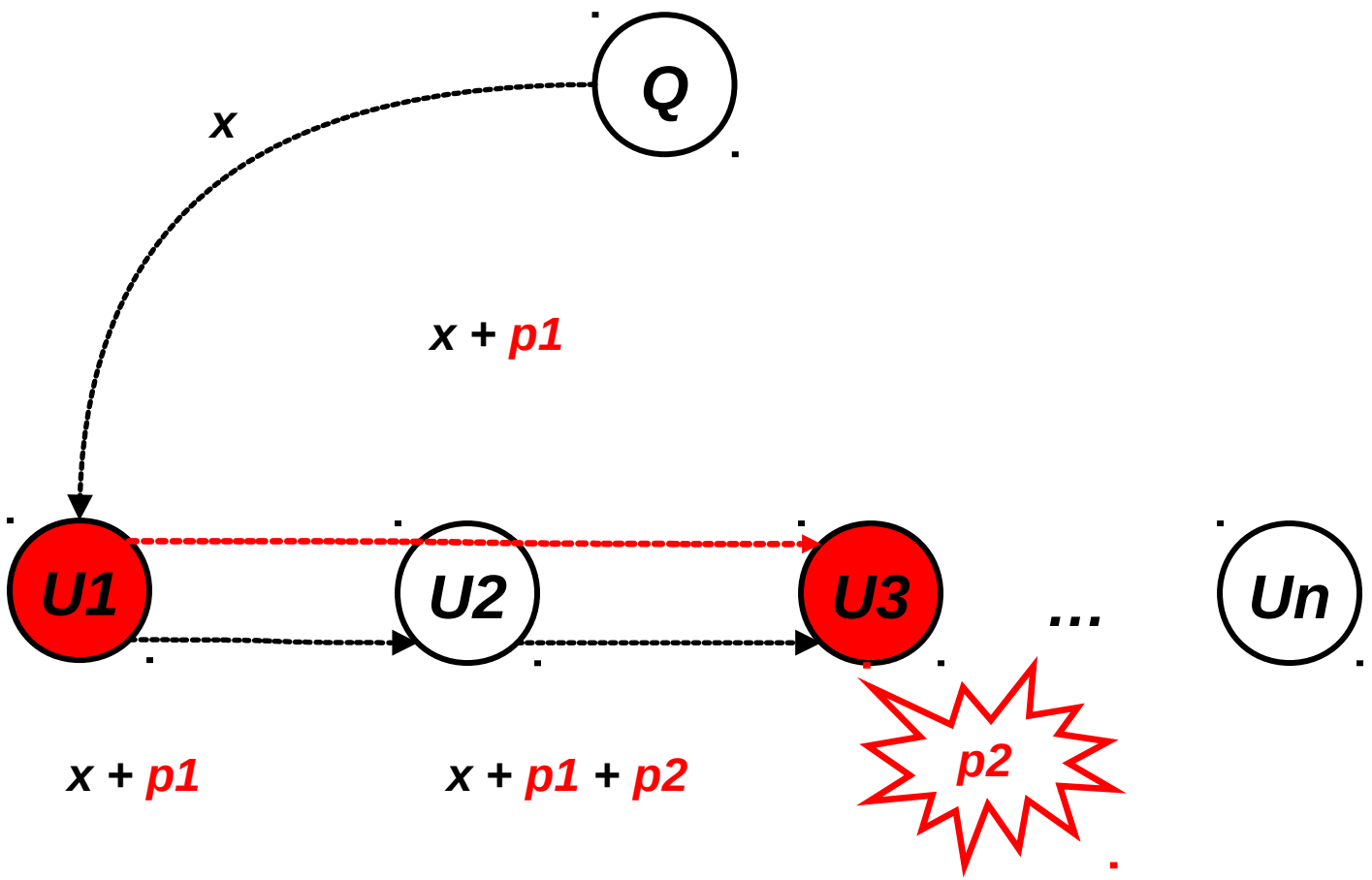
Décentralisé



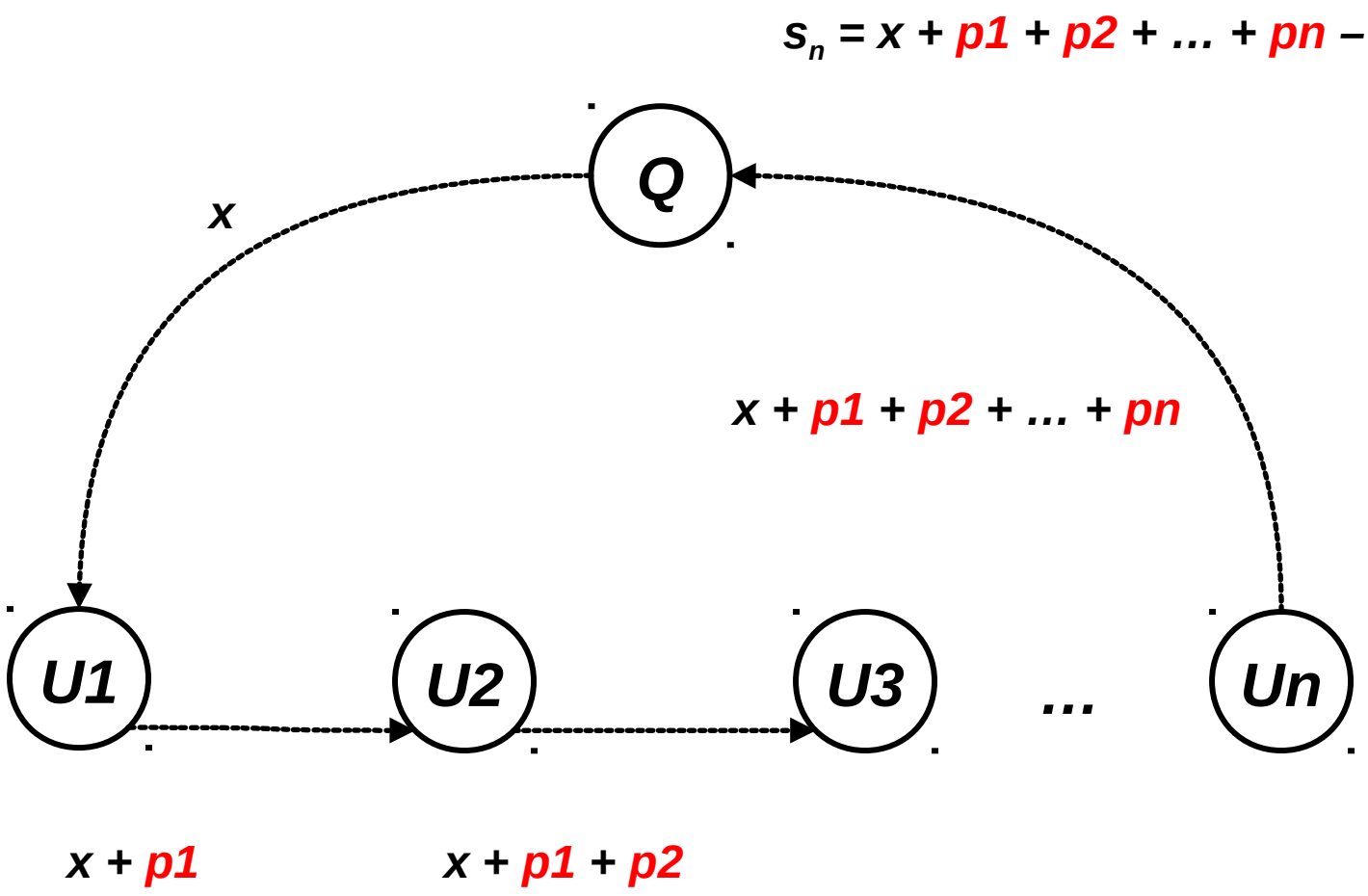
Un système décentralisé pour additionner des nombres privés



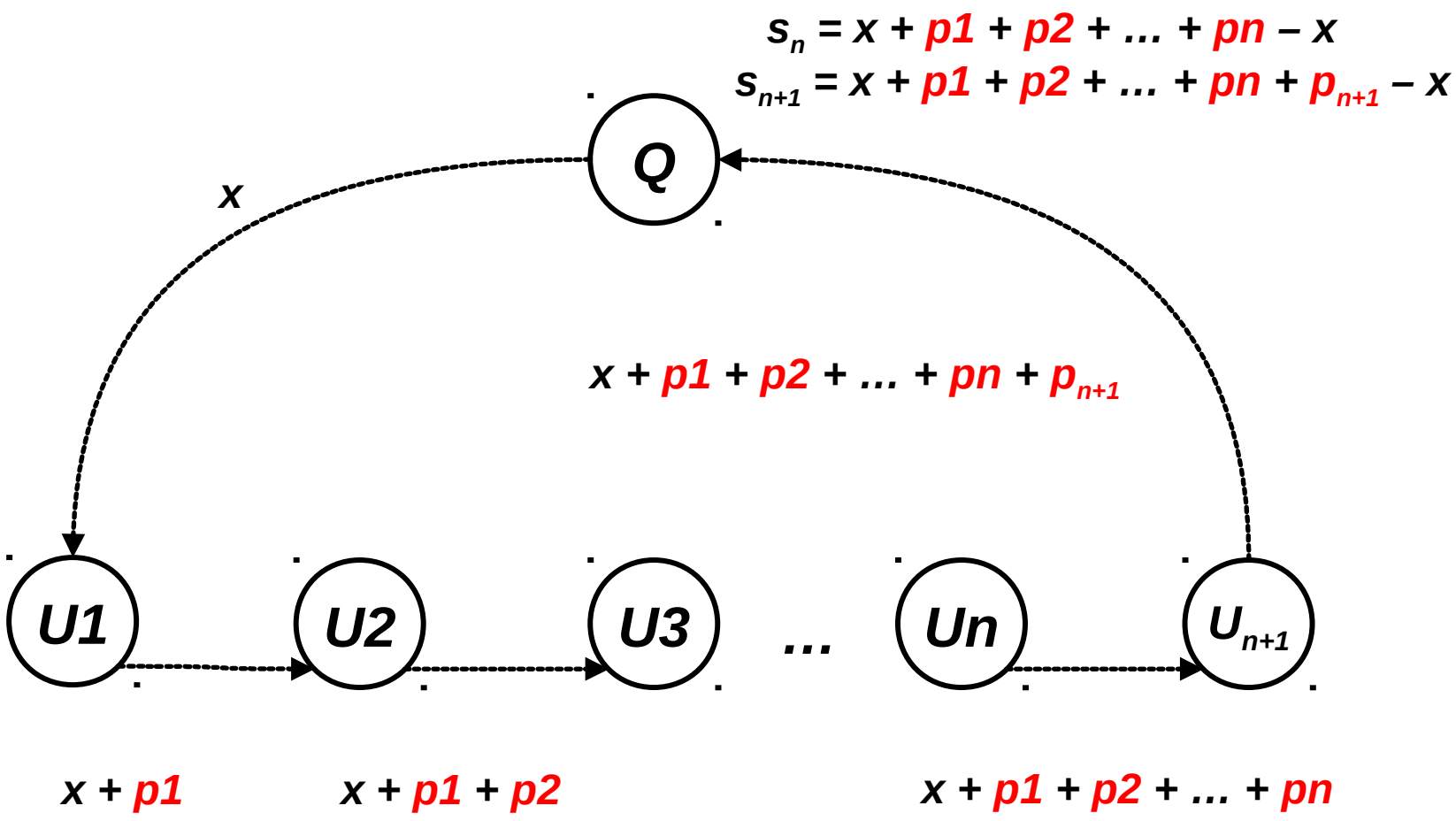
Attaque d’interception n° 1



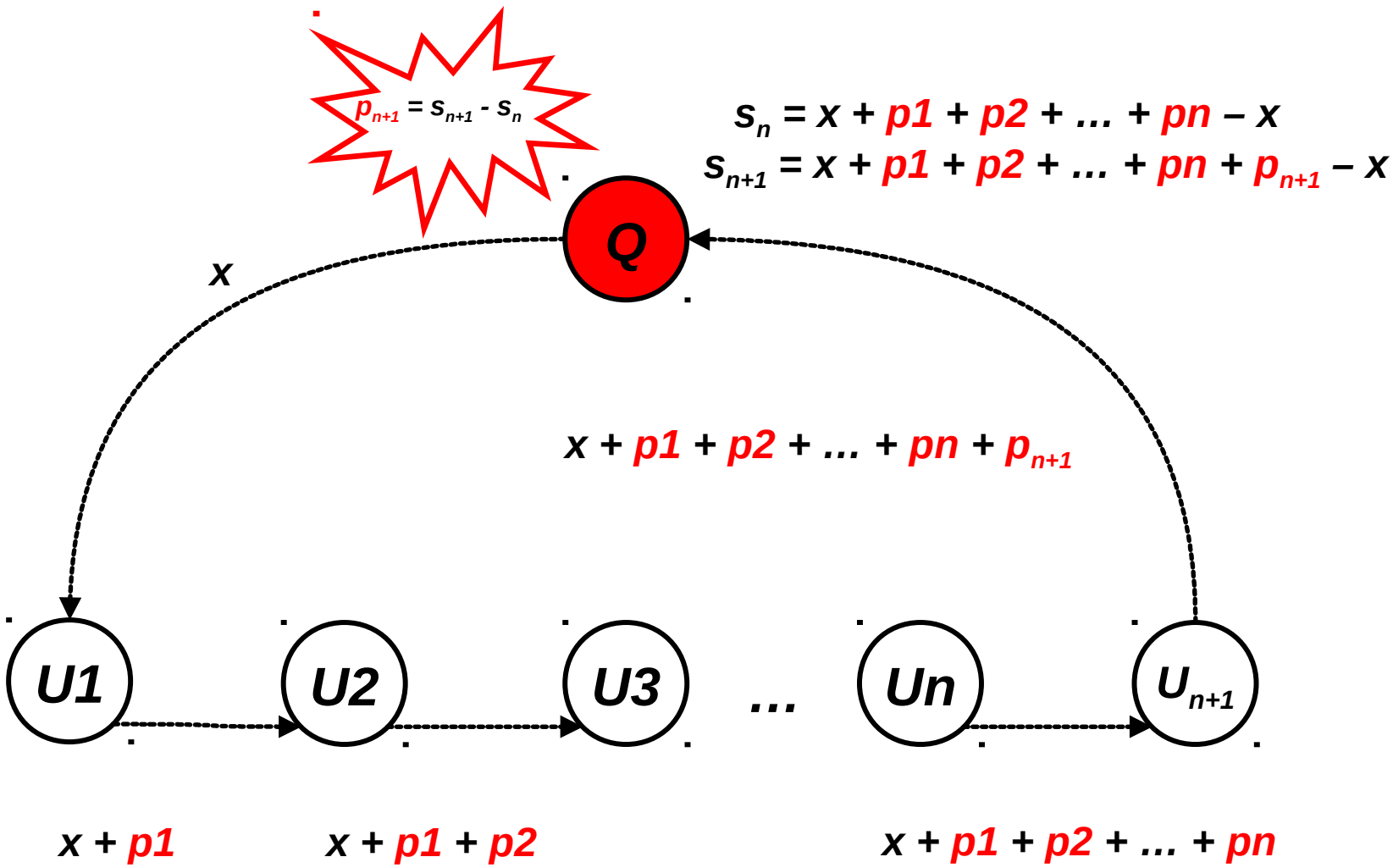
Attaque d'interception n° 2



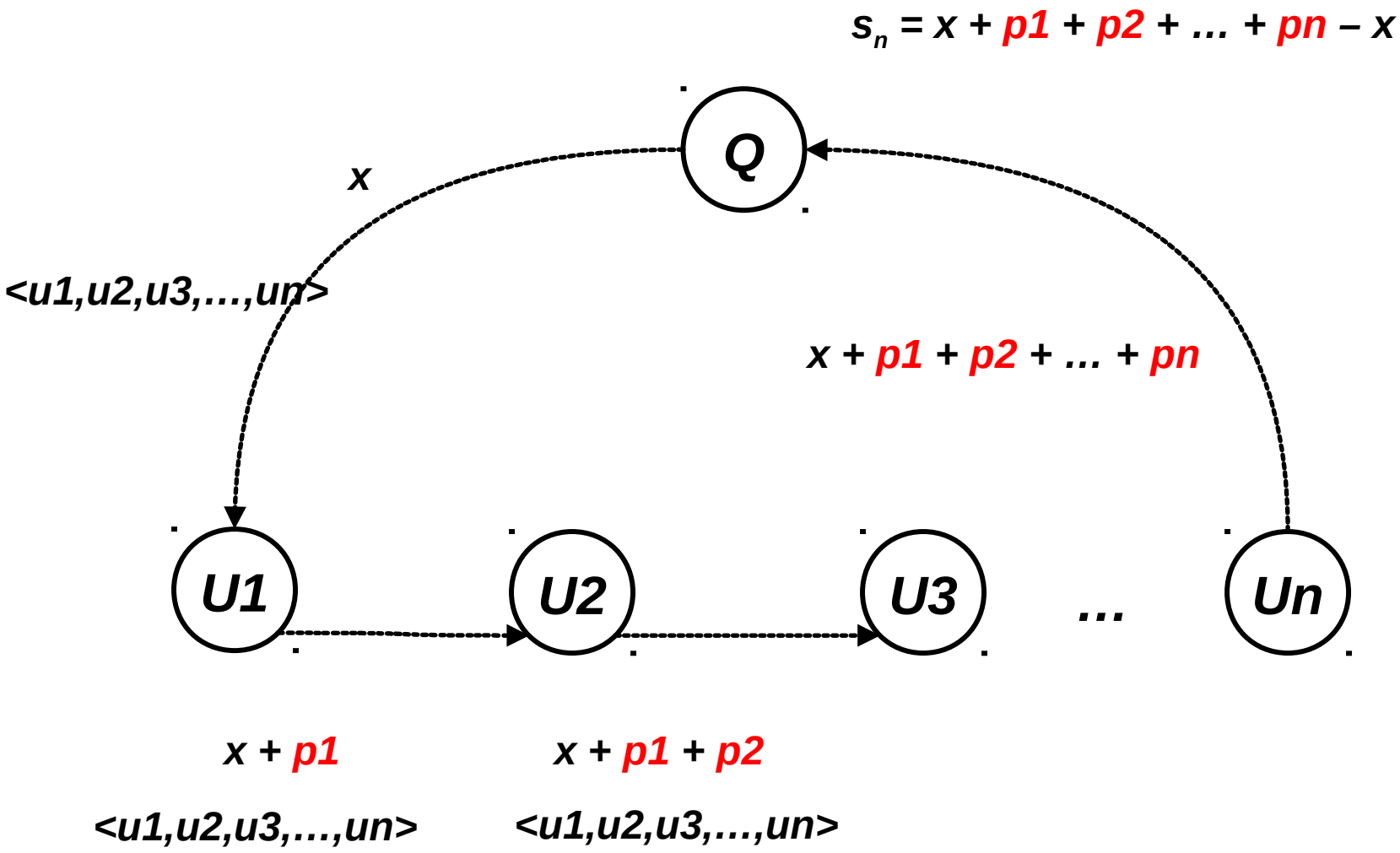
Attaque d'interception n° 2



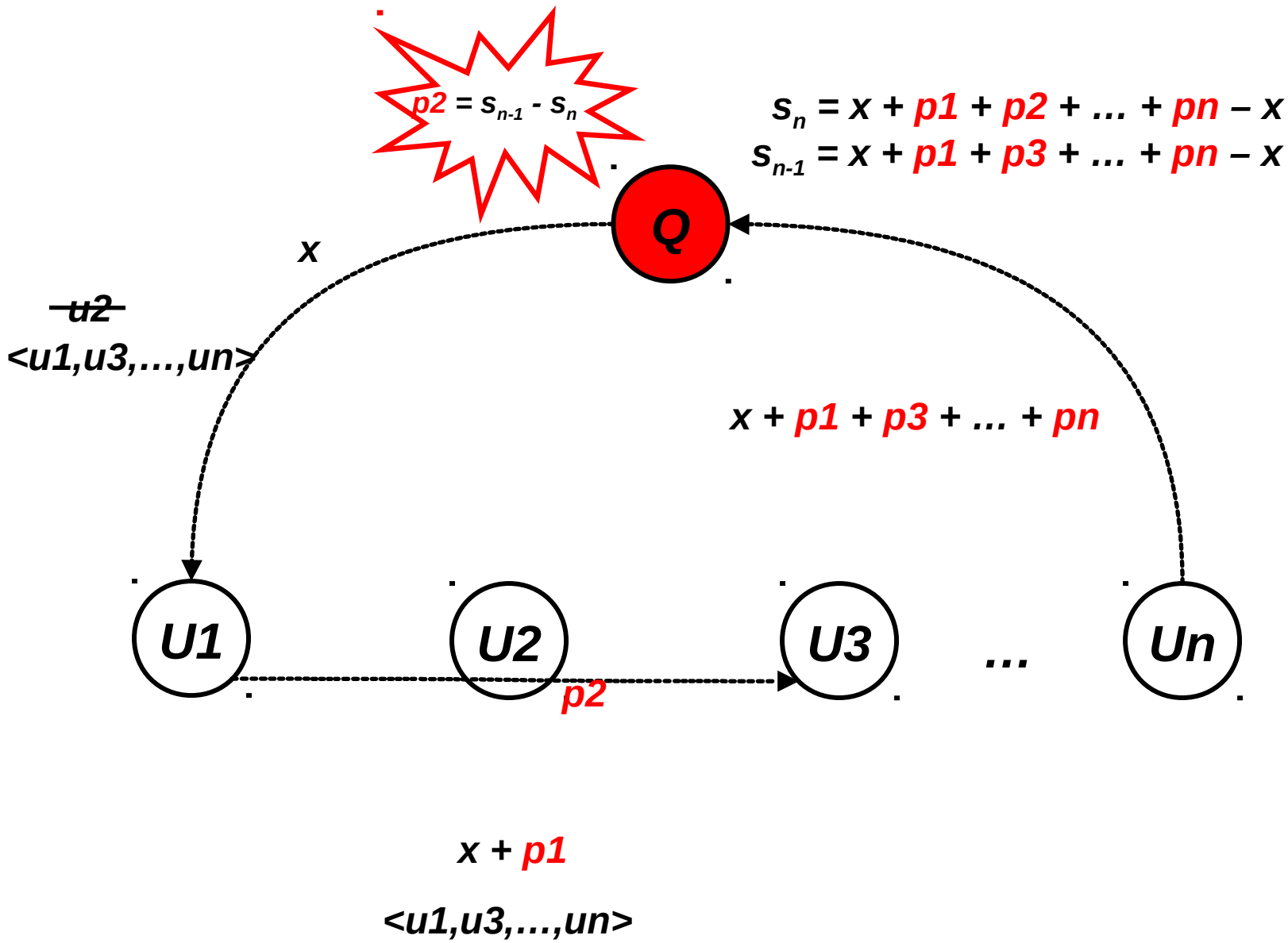
Attaque d'interception n° 2



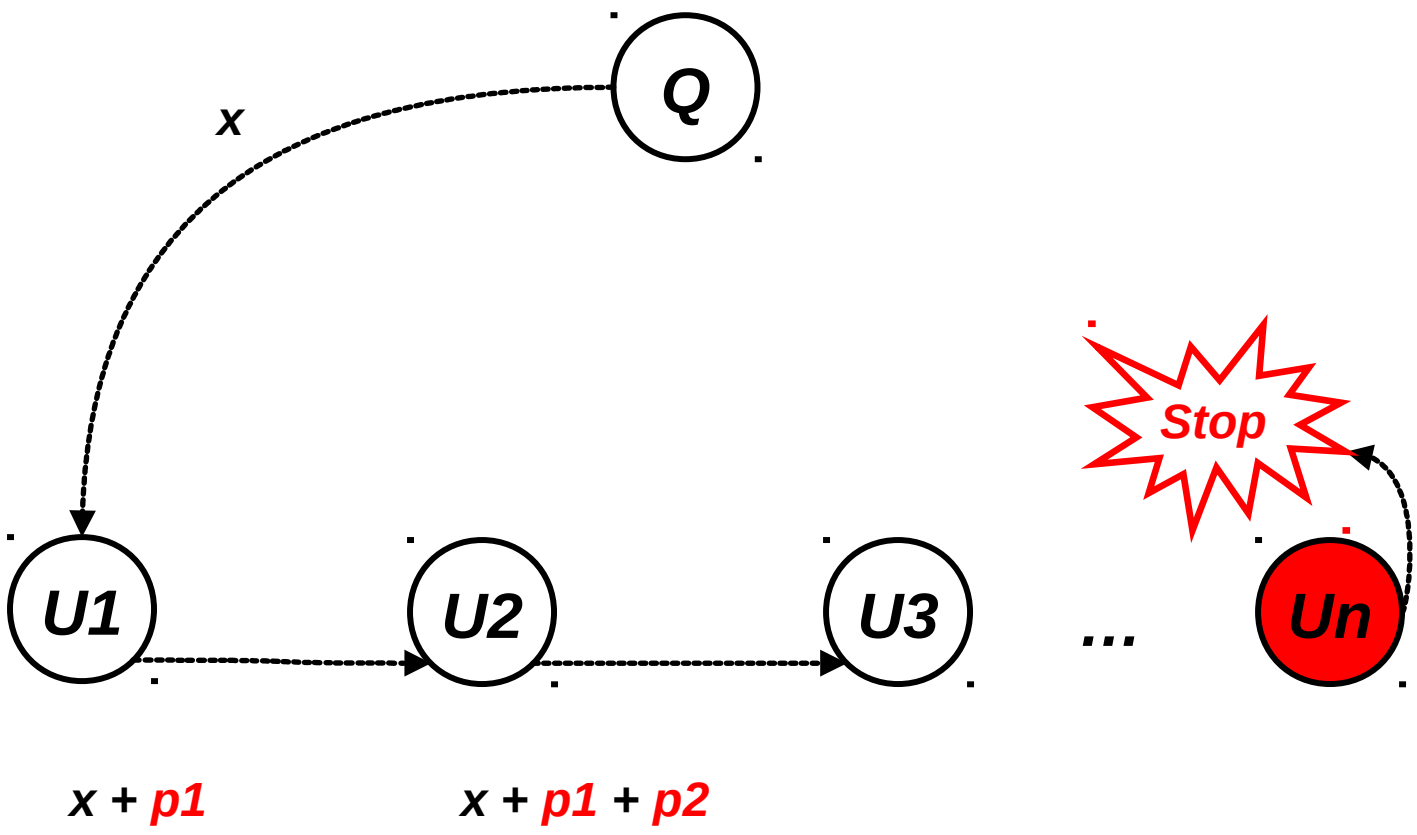
Attaque d'interception n° 3



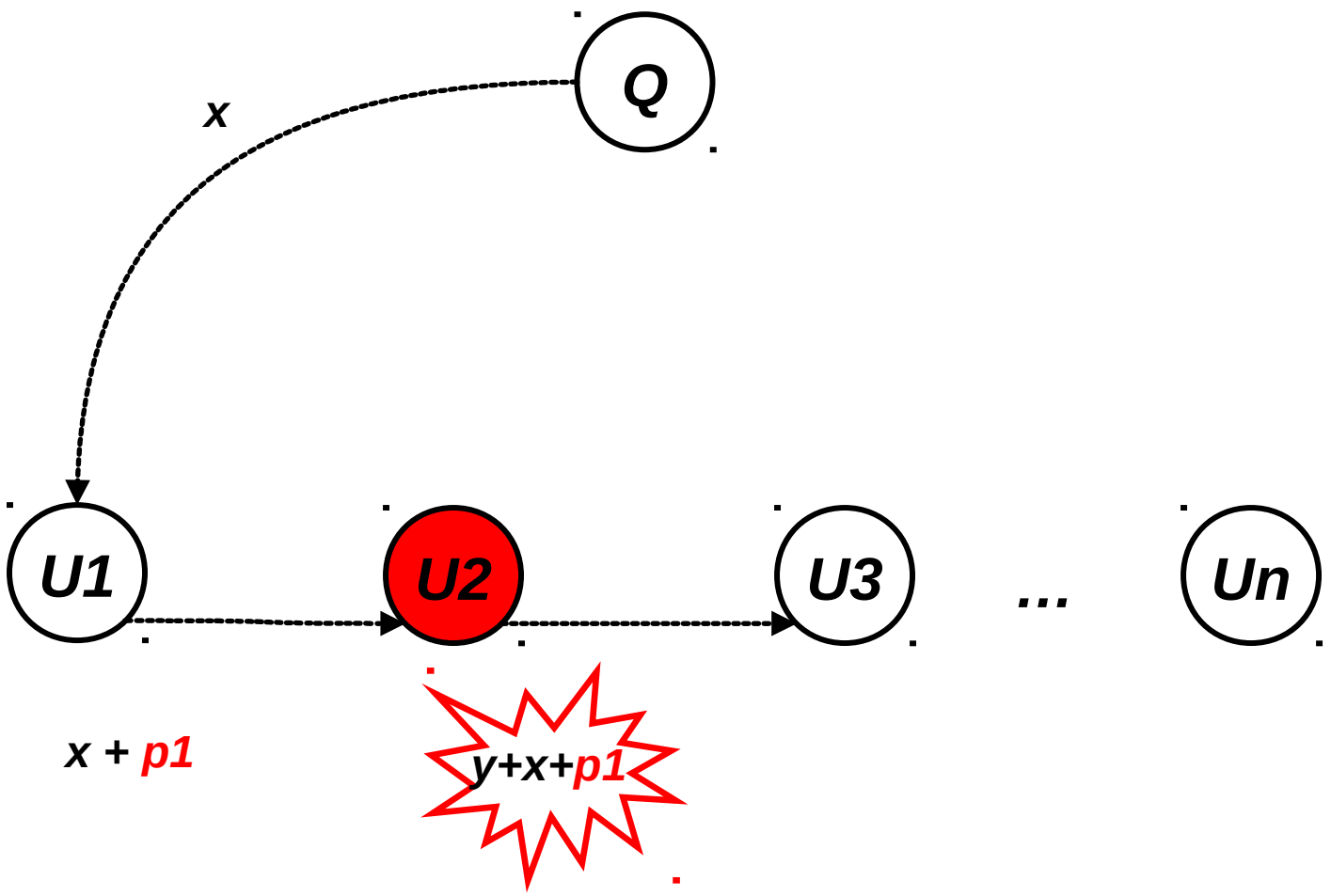
Attaque d'interception n° 3



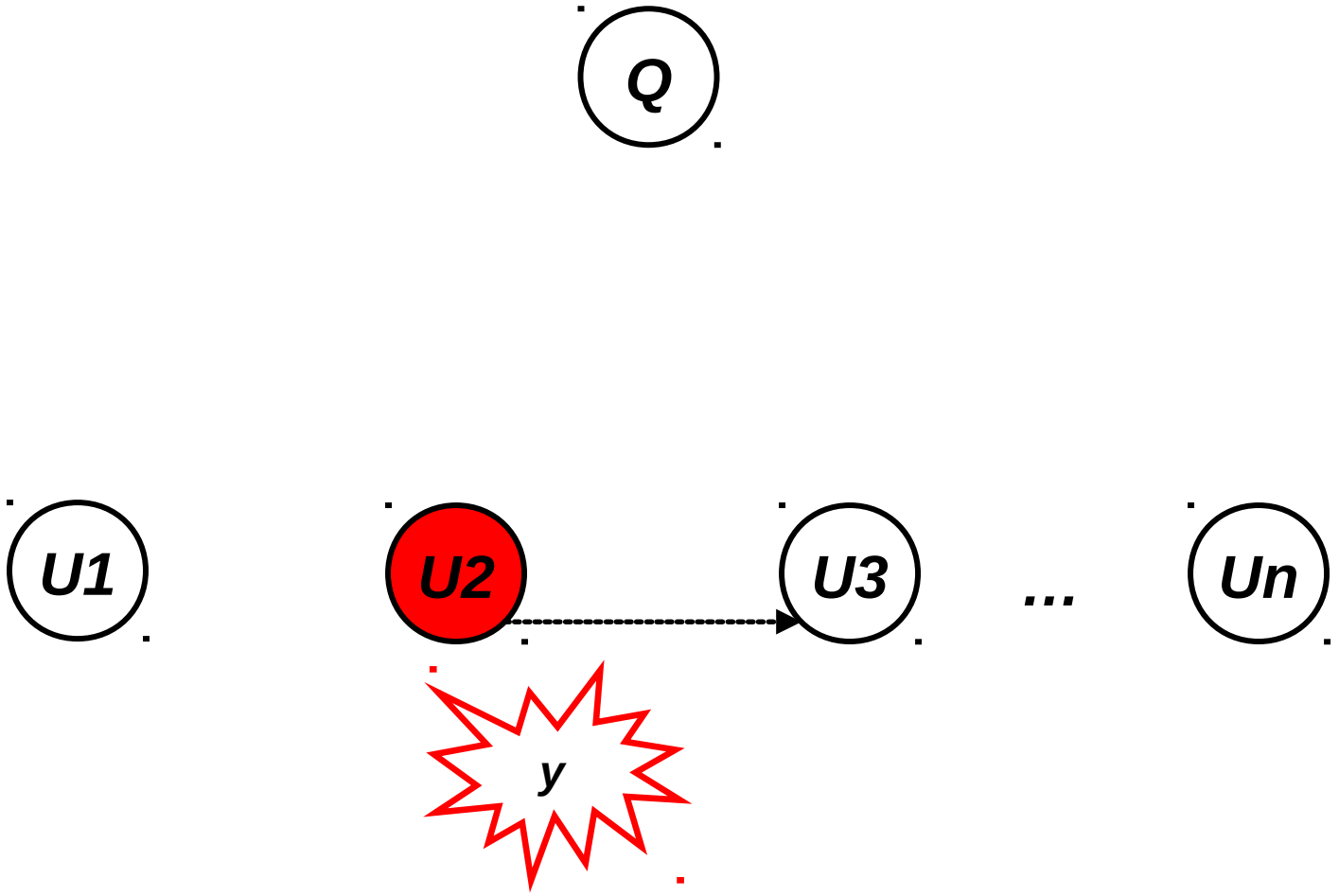
Attaque d'interruption



Attaque de modification



Attaque d’invention



Importance de la sécurité

Importance de la sécurité

La sécurité est une exigence non fonctionnelle. Cependant, la sécurité est souvent plus importante que les exigences fonctionnelles d'un logiciel.

Raison	Description
Les défaillances de la sécurité affectent tous les utilisateurs	Certaines fonctionnalités d'un logiciel sont utilisés par seulement quelques utilisateurs. Cependant, une défaillance de la sécurité, telle que celle qui réduit la disponibilité du logiciel affecte tous les utilisateurs.

Importance de la sécurité

La sécurité est une exigence non fonctionnelle. Cependant, la sécurité est souvent plus importante que les exigences fonctionnelles d'un logiciel.

Raison	Description
Les défaillances de la sécurité affectent tous les utilisateurs	Certaines fonctionnalités d'un logiciel sont utilisés par seulement quelques utilisateurs. Cependant, une défaillance de la sécurité, telle que celle qui réduit la disponibilité du logiciel affecte tous les utilisateurs.
Les utilisateurs rejettent des systèmes qui ne sont pas sécurisés	Si les utilisateurs trouvent que le système n'est pas sécurisé, ils refusent de l'utiliser. Ils peuvent aussi refuser d'utiliser d'autres logiciels de la même entreprise.

Importance de la sécurité

La sécurité est une exigence non fonctionnelle. Cependant, la sécurité est souvent plus importante que les exigences fonctionnelles d'un logiciel.

Raison	Description
Les défaillances de la sécurité affectent tous les utilisateurs	Certaines fonctionnalités d'un logiciel sont utilisés par seulement quelques utilisateurs. Cependant, une défaillance de la sécurité, telle que celle qui réduit la disponibilité du logiciel affecte tous les utilisateurs.
Les utilisateurs rejettent des systèmes qui ne sont pas sécurisés	Si les utilisateurs trouvent que le système n'est pas sécurisé, ils refusent de l'utiliser. Ils peuvent aussi refuser d'utiliser d'autres logiciels de la même entreprise.
Le coût d'une défaillance de la sécurité peut être énorme	Le coût des défaillances de la sécurité des systèmes critiques, par exemple, le système d'alimentation électrique d'une ville, peut être beaucoup plus coûteux que le système lui-même.

Importance de la sécurité

La sécurité est une exigence non fonctionnelle. Cependant, la sécurité est souvent plus importante que les exigences fonctionnelles d'un logiciel.

Raison	Description
Les défaillances de la sécurité affectent tous les utilisateurs	Certaines fonctionnalités d'un logiciel sont utilisés par seulement quelques utilisateurs. Cependant, une défaillance de la sécurité, telle que celle qui réduit la disponibilité du logiciel affecte tous les utilisateurs.
Les utilisateurs rejettent des systèmes qui ne sont pas sécurisés	Si les utilisateurs trouvent que le système n'est pas sécurisé, ils refusent de l'utiliser. Ils peuvent aussi refuser d'utiliser d'autres logiciels de la même entreprise.
Le coût d'une défaillance de la sécurité peut être énorme	Le coût des défaillances de la sécurité des systèmes critiques, par exemple, le système d'alimentation électrique d'une ville, peut être beaucoup plus coûteux que le système lui-même.
Un système non sécurisé peut entraîner la perte d'informations précieuses	Les données sont très coûteuses à collecter et à entretenir. Les données sont aussi généralement privées. Les dommages à cause de la perte de données peuvent être irréversibles.

Les facteurs qui contribuent au problème de la sécurité

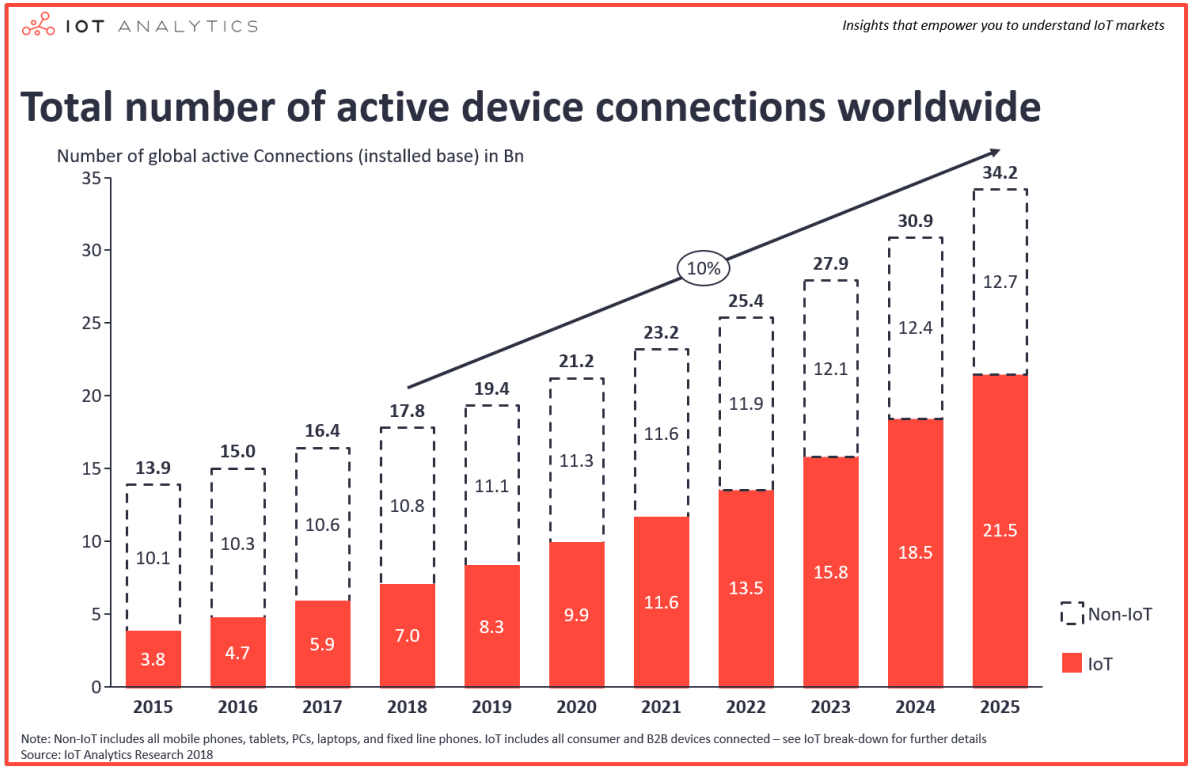
Les facteurs qui contribuent au problème de la sécurité

- Connectivité
- Extensibilité
- Complexité

Connectivité

De plus en plus d'ordinateurs (les PCs, tablettes, smartphones, ainsi que les systèmes qui gèrent les infrastructures essentielles, par exemple les systèmes SCADA) sont connectés à l'Internet.

La connectivité signifie qu'un attaquant peut accéder les logiciels à distance et tenter d'exploiter ses vulnérabilités.



Extensibilité

Un logiciel extensible accepte des extensions afin que la fonctionnalité du système peut être évolué de façon progressive. Exemple : le mécanisme de modules d'extension des navigateurs web.

Un attaquant peut exploiter l'extensibilité du logiciel en introduisant du code malveillant.

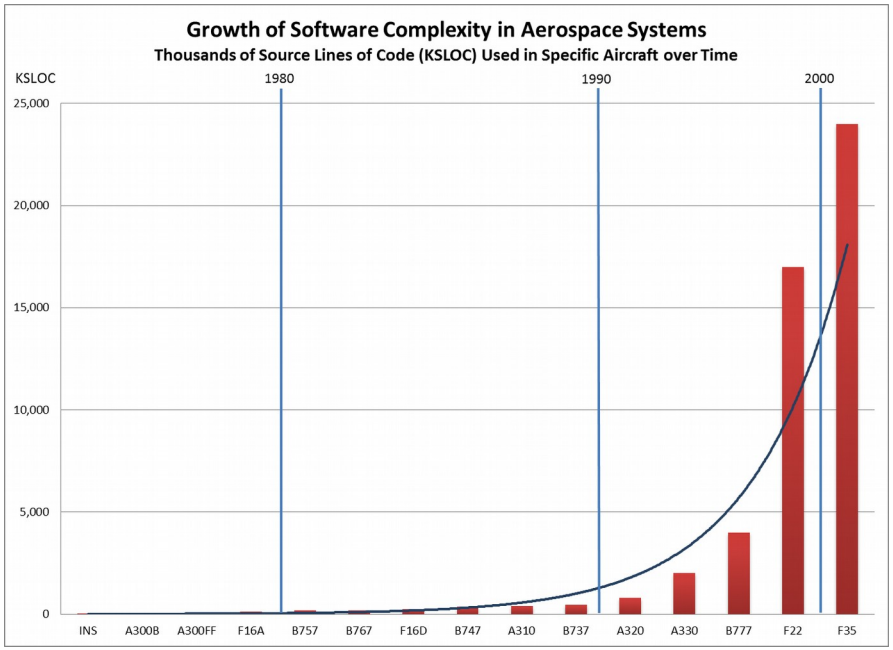
Les logiciels sont de plus en plus extensible.

Complexité

La taille d'un logiciel en termes des lignes de code indique la complexité du logiciel.

Les logiciels ont la propension d’augmenter en taille avec le temps.

Plus de lignes de code a la tendance d’entraîner plus de défaillances et plus de problèmes de sécurité.



https://savi.avsi.aero/about-savi/savi-motivation/

Analyse des risques contre la sécurité des logiciels

Analyse des risques contre la sécurité des logiciels

Identification des éléments suivants :

- Attaquant
- Atout
- Vulnérabilité
- Attaque
- Probabilité d’attaque
- Menace
- Risque
- Impact
- Contre-mesure

Analyse des risques – Scénario 1

Dossier Médical Personnel

Un logiciel avec des exigences fortes de la sécurité

« Le Dossier Médical Personnel (DMP) est un dossier médical, informatisé et sécurisé qui accompagne le patient tout au long de sa vie. Il est accessible sur internet. »
www.dmp.gouv.fr

Dossier Médical Personnel

Les informations regroupées dans un dossier médical personnel :
- traitements et soins
- comptes-rendus
- imagerie médicale
- analyses de laboratoire
- données de prévention
- certificats ou déclarations

- Les informations sont **partagées**
  - Les médecins et les autres professionnelles de santé peuvent partager les informations d'un patient afin de coordonner les soins du patient

- Les informations sont **sécurisées**
  - Le patient choisit les médecins et les autres professionnelles de santé avec les quels il veut partager ses informations
  - Confidentialité, intégrité, disponibilité

Objectifs de la sécurité

Objectif	Dossier Médical Personnel
Confidentialité	Un dossier médical personnel doit rester confidentiel. Seulement les médecins autorisés doivent avoir l'accès.
Intégrité	Un attaquant ne devrait pas être en mesure de modifier ou supprimer un dossier médical personnel.
Disponibilité	Une personne doit avoir accès à son dossier médical personnel à tout moment.

Attaquant

Un attaquant, c'est quelqu'un qui veut battre la confidentialité, l'intégrité ou la disponibilité du système.

Quelques propriétés d’un attaquant :

- Utilisateur externe ou interne (par exemple, un médecin dans le cas de DMP)
- Les moyens de calcul
- Les ressources de stockage
- Le nombre de machines en réseau sous contrôle

Atout

Un atout, c’est quelque chose de valeur qui doit être protégé contre l’attaquant. L’atout peut être le système logiciel lui-même ou les données gérés par le système.

Les documents dans un dossier médical personnel :
- traitements et soins
- comptes-rendus
- imagerie médicale
- analyses de laboratoire
- données de prévention
- certificats ou déclarations

Système	**Atout**
Logiciel e-santé	Les documents dans un dossier médical personnel

Vulnérabilité

Les vulnérabilités sont des faiblesses qui peuvent être utilisés pour nous faire du mal. Essentiellement, ils sont des trous qui peuvent être exploitées par l'attaquant.

Système	Atout	Vulnérabilité
Logiciel e-santé	Les documents dans un dossier médical personnel	• Des mots de passe faibles sont permis, par exemple, les mots de passe comme 123456, motdepasse, etc. • Les données saisies ne sont pas validées • Transmission et stockage de donnés sans chiffrement

Vulnérabilité

Exemple : des mots de passe faibles

Les mots de passe les plus fréquents

http://matchableapp.wordpress.com/page/2/

How secure is my password?
http://howsecureismypassword.net/

Vulnérabilité

Password Entropy

- Password entropy predicts **how difficult** a given **password** would be **to crack** through **guessing**, **brute force cracking**, **dictionary attacks** or other common methods.

- Entropy essentially measures **how many guesses** an attacker will need to make to guess your password.

Source: https://generatepasswords.org/how-to-calculate-entropy/

Vulnérabilité

How to Calculate Password Entropy?

L = Password Length; Number of symbols in the password

S = Size of the pool of unique possible symbols (character set).

For example:

Numbers (0-9): 10
Lower Case Latin Alphabet (a-z): 26
Lower Case & Upper Case Latin Alphabet (a-z, A-Z): 52
ASCII Printable Character Set (a-z, A-Z, symbols, space): 95

Number of Possible Combinations = S^L

Entropy = $\log_2$(Number of Possible Combinations)

Source: https://generatepasswords.org/how-to-calculate-entropy/

Vulnérabilité

Complexity	Entropy Calculation
4 characters consisting of: • Letters of the same case	• **Length:** 4 • **Possible Symbols:** 26 • **Possible combinations:** 26^4 = 456,976 • **Bits of Entropy:** $\log_2(26^4)$ = 18.80 • **Strength:** Very Weak
8 characters consisting of: • Letters of the same case	• **Length:** 8 • **Possible Symbols:** 26 • **Possible combinations:** 26^8 = 208,827,064,576 • **Bits of Entropy:** $\log_2(26^8)$ = 37.60 • **Strength:** Weak
8 characters consisting of: • Letters (upper and lower case)	• **Length:** 8 • **Possible Symbols:** 52 • **Possible combinations:** 52^8 = 9.1343852e+46 • **Bits of Entropy:** $\log_2(52^8)$ = 45.60 • **Strength:** Reasonable

Source: https://generatepasswords.org/how-to-calculate-entropy/

Vulnérabilité

Common Vulnerabilities and Exposures Database
http://cve.mitre.org

Attaque / Menace / Mauvaise utilisation

Une attaque, c’est une exploitation des vulnérabilités d'un système pour endommager un atout.

On peut également identifier les cas de mauvaise utilisation.

Système	**Atout**	**Vulnérabilité**	**Attaque**
Logiciel e-santé	Les documents dans un dossier médical personnel	• Des mots de passe faibles sont permis, par exemple, les mots de passe comme 123456, motdepasse, etc. • Les données saisies ne sont pas validées • Transmission et stockage de donnés sans chiffrement	• l’attaquant devine le mot de passe • l’attaquant saisit des données inattendues • l’attaquant intercepte la communication • l’attaquant utilise du code malveillant : Virus, Worm, Trojan

Attaque / Menace / Mauvaise utilisation

Exemple

- **l'attaquant saisit des données inattendues**
- **SQL code injection**

```
String query = "SELECT * FROM traitements
        WHERE patientID='" + request.getParameter("id") +"'";
```

Attendue :
http://www.dmpexemple.com/app/patientView?id=9

Inattendue :
http://www.dmpexemple.com/app/patientView?id=' or '1'='1

SELECT * FROM traitements WHERE patientID='' or '1'='1'

Types d’attaque

Type of attack	Description	Objectives of security defeated
Interception	Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.	Confidentiality
Interruption	Interruption attacks cause our assets to become unusable or unavailable for our use.	Integrity Availability
Modification	Modification attacks involve tampering with our asset.	Integrity Availability
Fabrication	Fabrication attacks involve generating malicious data, processes, or messages.	Integrity Availability

Risque

Un risque est le résultat potentiel d'une attaque réussie. Un risque se pose en raison de la présence à la fois d’une menace et d’une vulnérabilité que la menace peut exploiter.

Système	Atout	Vulnérabilité	Attaque	Risque
Logiciel e-santé	Les documents dans un dossier médical personnel	• Des mots de passe faibles sont permis, par exemple, les mots de passe comme 123456, motdepasse, etc. • Les données saisies ne sont pas validées • Transmission et stockage de donnés sans chiffrement	• l’attaquant devine le mot de passe • l’attaquant saisit des données inattendues • l’attaquant intercepte la communication • l’attaquant utilise du code malveillant : Virus, Worm, Trojan	• l’attaquant obtient accès au DMP • l’attaquant supprime le DMP • l’attaquant modifie le DMP, par exemple, le groupe sanguin du patient

Impact

Le niveau d'impact est la gravité de la perte ou les dommages causés lorsque le risque se réalise.

Level of Impact	Description
High	(1) Very costly loss of major tangible assets or resources (2) Significant violation of, or harm or impediment to, an organization's mission, reputation, or interest
Medium	(1) Costly loss of tangible assets or resources (2) Violation of, or harm or impediment to, an organization's mission, reputation, or interest
Low	(1) Loss of some tangible assets or resources (2) A noticeable effect on an organization's mission, reputation, or interest

Software Security: Building Security In. Gary McGraw.

Impact

Attaque	Risque	Niveau d'impact
• l'attaquant devine le mot de passe • l'attaquant saisit des données inattendues • l'attaquant intercepte la communication • l'attaquant utilise du code malveillant : Virus, Worm, Trojan	(1) l'attaquant obtient accès au DMP (2) l'attaquant supprime le DMP (3) l'attaquant modifie le DMP, par exemple, le groupe sanguin du patient	(1) Élevé (2) Élevé (3) Élevé

Contre-mesure

Afin d’atténuer les risques, nous pouvons mettre en place des contre-mesures pour s'assurer que des menaces et des attaques sont prises en compte. Une contre-mesure, c’est une solution défensive pour empêcher une attaque.

Risque	**Contre-mesure**
• l’attaquant obtient accès au DMP • l’attaquant supprime le DMP • l’attaquant modifie le DMP, par exemple, le groupe sanguin du patient	• Les mots de passe sont vérifiés et les mots de passe faibles ne sont pas acceptés • Un CAPTCHA est utilisé pour vérifier que les réponses sont donnés par un humain • Les données saisies sont vérifiés et validées • Transmission et stockage de donnés avec chiffrement

Analyse des risques – Scénario 2

Museum information system

https://cdt31.media.tourinsoft.eu/upload/Augustins.jpg

- An information system for a **museum**, which holds **valuable exhibits**.
- The information system must manage information about the **exhibits**, the museum **employees**, as well as research and analysis **data**.

Source

- **Security Patterns: Integrating Security and Systems Engineering** by Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad. Wiley, 1st edition. February 2006.

Evaluation of assets

1. Determine the security value.
The importance of guaranteeing the asset's information security properties: confidentiality, integrity, availability and accountability.

Table 6.5 Security requirements rating

RATING	QUALITATIVE	DESCRIPTION
6	Extreme	The asset requires an extreme degree of confidentiality, integrity, and availability. Compromise of these security properties would expose massive amounts of confidential information and endanger public safety.
5	Very high	The asset requires a very high degree of confidentiality, integrity, availability or accountability. Compromise of one or more of these properties would expose sensitive information and possibly endanger public safety
4	High	The asset requires a high degree of confidentiality, integrity, availability or accountability. Compromise of these properties would expose sensitive information, violating local or federal legislation.
3	Medium	The asset has a moderate requirement for information security controls. Compromise of the security properties would violate corporate policy and possibly local or federal legislation.
2	Low	The asset has a low requirement for security. Compromise of the asset would expose only non-critical information or data.
1	Negligible	The information is publicly available or the asset has no information security value for the enterprise.

Evaluation of assets

2. Determine the financial value.
The financial value of the enterprise asset based on the cost of repair or replacement.

Table 6.6 Financial value rating

RATING	QUALITATIVE	DESCRIPTION
6	Extreme	The asset has an extreme monetary value for the enterprise. Loss or damage of the asset would probably bankrupt the enterprise.
5	Very high	The asset has a major monetary value. Loss or damage of the asset would impose a substantial financial burden on the enterprise.
4	High	The asset has a significant monetary value. Repair or replacement would require significant funds.
3	Medium	The asset has moderate financial value. Loss or damage of the asset would require financial repurposing.
2	Low	The asset has low financial value to the company.
1	Negligible	The asset has no monetary value.

Evaluation of assets

3. Determine the impact to business.
The value of the asset in relation to the impact a compromise of the asset would have on the enterprise's business processes.

Table 6.7 Business impact rating

RATING	QUALITATIVE	DESCRIPTION
6	Extreme	The enterprise cannot function without this asset. Its compromise or loss would result in immediate termination of critical business services.
5	Very high	This asset represents a major service of the enterprise. Its loss would result in termination of a critical service or severe degradation of many services.
4	High	This asset supports many enterprise services. Its loss would results in termination of a major service or degradation of services.
3	Medium	This asset supports a fair number of customers, or supports a major service of the enterprise. Its loss would result in degradation of more important services.
2	Low	This asset supports an ancillary enterprise service. Its compromise would have a slight impact on business services.
1	Negligible	The loss of asset would have no impact to the business.

Evaluation of assets

4. Determine the overall value and build an asset valuation table. Combine the results of the security, financial and business valuations and determine the overall value the enterprise places on the asset.

Table 6.8 Overall asset value scale

RATING	QUALITATIVE	DESCRIPTION
6	Extreme	The enterprise places the highest possible value on this asset. Its compromise results in human deaths, immediate and total loss of business services or financial bankruptcy.
5	Very high	The asset represents or supports a critical business function for the enterprise. Loss or damage of it results in severe financial, security or health repercussions.
4	High	The asset is highly valued because of its security requirements or customer focus. Its loss would result in considerable harm to customer services and reputation.
3	Medium	The asset is of moderate value. It has some security needs and financial value. Compromise of it would impede the enterprise's mission.
2	Low	This asset is of minor financial value. Compromise of it results in little business impact.
1	Negligible	The asset has insignificant importance for the enterprise. It is easily replaced or repaired. It has little to no security requirements and represents no health impact.

Evaluation of assets

4. Determine the overall value and build an asset valuation table.

Table 6.10 Information asset valuation table

ASSET	SECURITY VALUE	FINANCIAL VALUE	BUSINESS IMPACT	OVERALL
Museum employee data	5	3	5	5
Museum financial/insurance data, partner financial data	4	3	4	4
Museum contractual data and business planning	4	3	4	4
Museum research and associated data	3	2	3	3
Museum advertisements and other public data	1	2	2	2
Museum database of collections information	3	3	4	4

Evaluation of threats

1. Create a likelihood scale.
Create a scale for rating the frequency of attempted events, or likelihood for events occurring.

Table 6.13 Event likelihood

RATING	LIKELIHOOD	DESCRIPTION
6	Extreme	The threat action is continually occurring
5	Very high	The threat action occurs very often
4	High	The threat action regularly happens
3	Medium	The threat action occurs infrequently
2	Low	This threat action rarely takes place
1	Negligible	The occurrence of this threat action is extremely unlikely within a human lifetime

Evaluation of threats

2. Identify threats

Identify major threat sources that could potentially impact the assets defined by the scope of the risk assessment and trace their threat actions and consequences.

3. Build a threat table, rate each threat

Table 6.14 Threats to information assets

THREAT ACTION (FREQUENCY)	THREAT CONSEQUENCE
Natural	
Electrical spike in computer room (3)	Incapacitation, corruption of informational assets
Loss of electronic documents (3)	Incapacitation of informational assets
Professional criminals	
Theft of information assets (3)	Misappropriation, incapacitation, misuse, exposure, corruption of informational assets
Employees	
Unauthorized access to informational assets (5)	Exposure, falsification, incapacitation, misappropriation of informational assets
Data entry errors (5)	Corruption of information assets
Leaking confidential information (3)	Exposure of information assets

Evaluation of vulnerabilities

1. Create a severity scale.
This scale will represent the degree to which an asset is susceptible to a vulnerability, and the potential impact should the vulnerability be exploited.

2. Identify vulnerabilities.
Using the threat table, identify the vulnerabilities of the assets.

3. Build a threat-vulnerability table.
Extend the threat table by associating each vulnerability with a threat action.

5. Rate each vulnerability.
Rate each vulnerability according to the severity scale and update the threat vulnerability table to reflect this rating.

Evaluation of vulnerabilities

Table 6.17 Threat-Vulnerabilities table for information assets

THREAT ACTION (FREQUENCY)	VULNERABILITY (SEVERITY)
Natural	
Electrical spike in computer room (3)	Lack of surge protection, uninterruptible power system (UPS) (4)
Loss of electronic documents (3)	Incomplete or corrupt data backups (4)
Professional criminals	
Theft of information assets (3)	Susceptibility of employees to bribery (3) Lack of proper physical controls for document storage (locks, safe) (4)
Employees	
Unauthorized access of informational assets (5)	Weak information security controls enabling unauthorized access (3)
Data entry errors (5)	Lack of data validation during form input (2)
Leaking confidential information (3)	Exposure of information assets (3)

Evaluation of risks

***1*. Associate threat-vulnerability pairs with assets.**
Using the threat-vulnerability table, identify all threat-vulnerability pairs that pose a direct risk to each asset separately.

2. Evaluate risk.
Evaluate a risk equation using the numerical values for asset valuation, threat likelihood and vulnerability severity.

$$\text{Risk}(A) = \text{SUM}[\text{Threat} * \text{Vulnerability}](A) * \text{Asset Value}(A)$$

3. Present the results.
Sort the results in order of decreasing risk.

Evaluation of risks

Table 6.19 Threat-vulnerability pairs for museum building

THREAT ACTION (FREQUENCY)	VULNERABILITY (SEVERITY)
Natural	
Museum fire (3)	Failure of fire alarm system (6) Failure of fire suppression system (5)
Fatigue of support fixtures, building structural failure (3)	Lack of regularly scheduled inspections (4)

$$\text{Risk} = (3*6 + 3*5 + 3*4) * 6$$
$$\text{Risk} = (18 + 15 + 12) * 6$$
$$\text{Risk} = (45) * 6$$
$$\text{Risk (museum building)} = 270$$

Evaluation of risks

Table 6.21 Threat-vulnerability pairs for museum employee data

Natural	
Electrical spike in computer room (3)	Lack of surge protection, uninterruptible power system (UPS) (4)
Loss of electronic documents (3)	Incomplete or corrupt data backups (4)
Professional criminals	
Theft of information assets (3)	Susceptibility of employees to bribery (3) Lack of proper physical controls for document storage (locks, safe) (4)
Employees	
Unauthorized access of informational assets (5)	Weak information security controls enabling unauthorized access (3)
Data entry errors (5)	Lack of data validation during form input (2)
Leaking confidential information (3)	Exposure of information assets (3)

$$\text{Risk} = (12 + 12 + 21 + 15 + 10 + 9) * 5$$
$$\text{Risk} = 79 * 5$$
$$\text{Risk (museum employee data)} = 395$$

Evaluation of risks

Table 6.22 Prioritized risks for museum assets

ASSET	RISK VALUE
Museum collections and exhibits	786
Museum employee data	395
Museum staff	342
Museum financial/insurance data, partner financial data	316
Museum building	270
Museum contractual data and business planning	232
Museum database of collections information	232
Museum research and associated data	147
Museum transport vehicles	120
Museum advertisements and other public data	98

Sécurité assuré dès la conception
« Security by design »

Sécurité assuré dès la conception « Security by design »

L’approche de la sécurité assurée dès la conception pour les logiciels garantit que la sécurité est traitée au moment de la conception.

Quelques principes importants de « Security by design » :

- Défense en profondeur
- Point unique de défaillance
- Moindre privilège
- Compartimentage
- Défaillance sécurisée

Défense en profondeur

Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will, ideally, prevent a full breach.

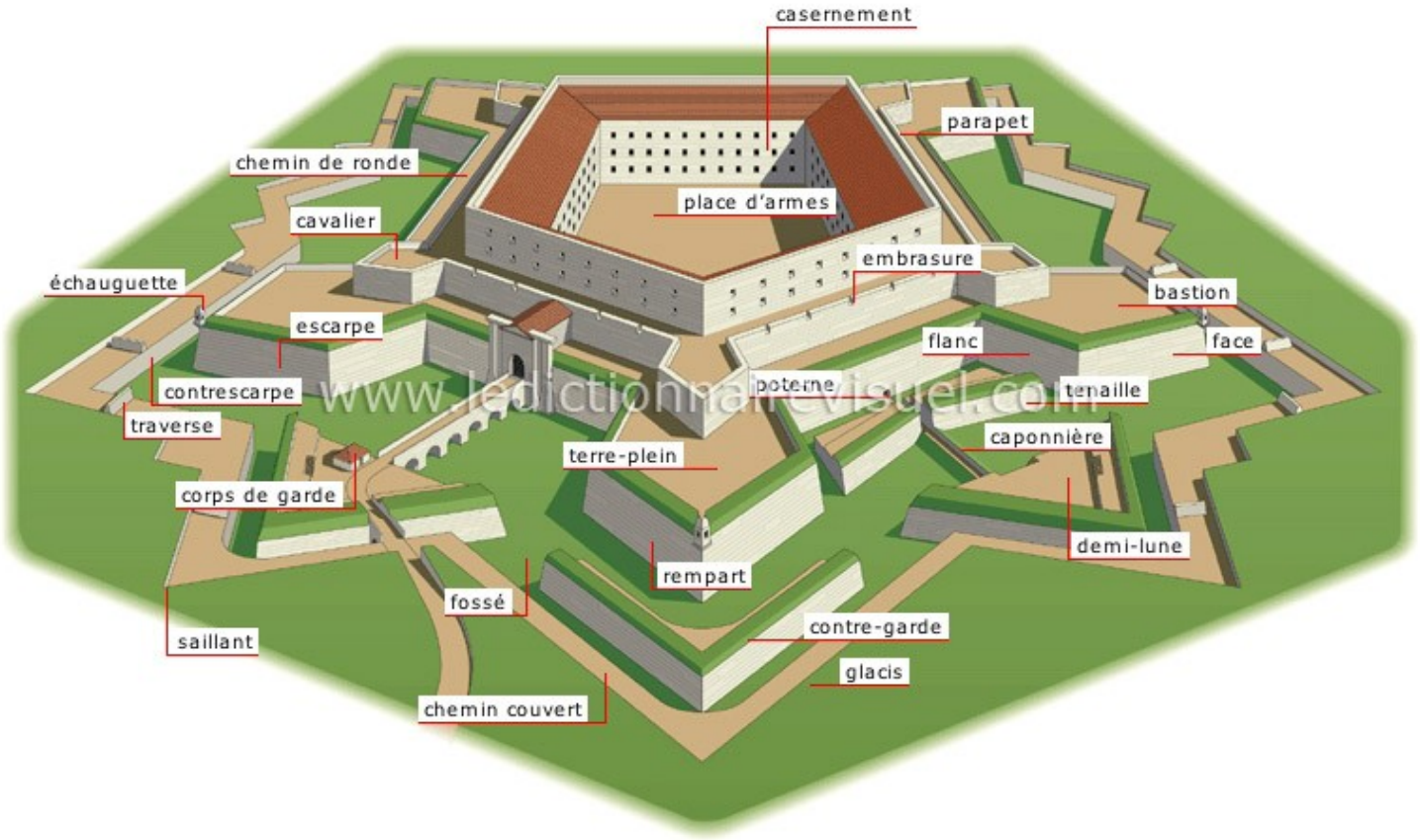
Security Engineering for Software. CS996 –CISM. JiaAn Chen. 03/31/04

La défense en profondeur, terme emprunté à une technique militaire destinée à retarder l'ennemi, consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant.

http://fr.wikipedia.org/wiki/Defense_en_profondeur

Défense en profondeur

Fortification à la Vauban



Défense en profondeur

Fortification à la Vauban

Les concepts sous-jacents de la construction des fortifications à la Vauban :

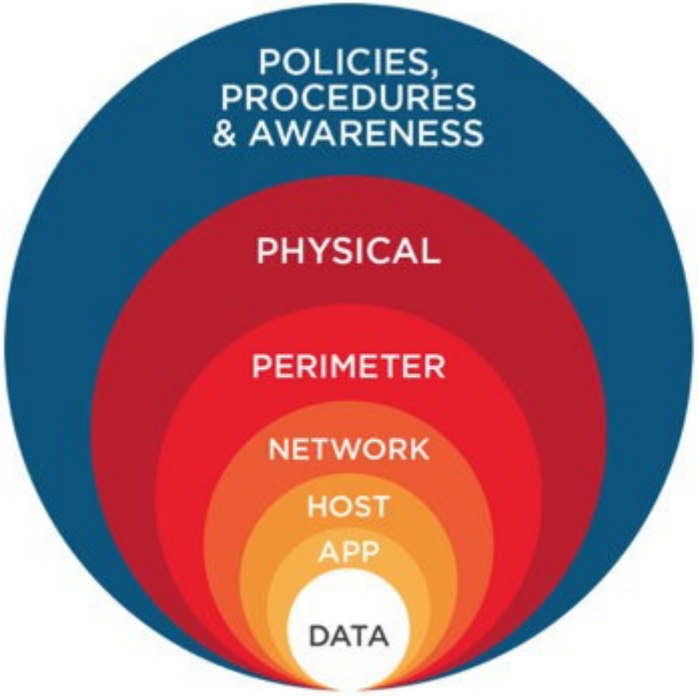
- les biens à protéger sont entourés de plusieurs lignes de défense ;
- chaque ligne de défense participe à la défense globale ;
- chaque ligne de défense à un rôle à jouer : affaiblir l'attaque, la gêner, la retarder

- chaque ligne de défense est autonome (la perte de la ligne précédente est prévue pour éviter un effet château de cartes) : la perte d'une ligne de défense affaiblit la suivante mais celle-ci dispose de ses propres moyens de défense face aux différentes attaques (chaque processus d'attaque possible entraîne une défense correspondante).

Mémento sur le concept de la défense en profondeur appliqué aux SI. Direction centrale de la sécurité des systèmes d'information, Bureau conseil (SGDN / DCSSI / SDO / BCS). Version 1.1 – 19 juillet 2004.

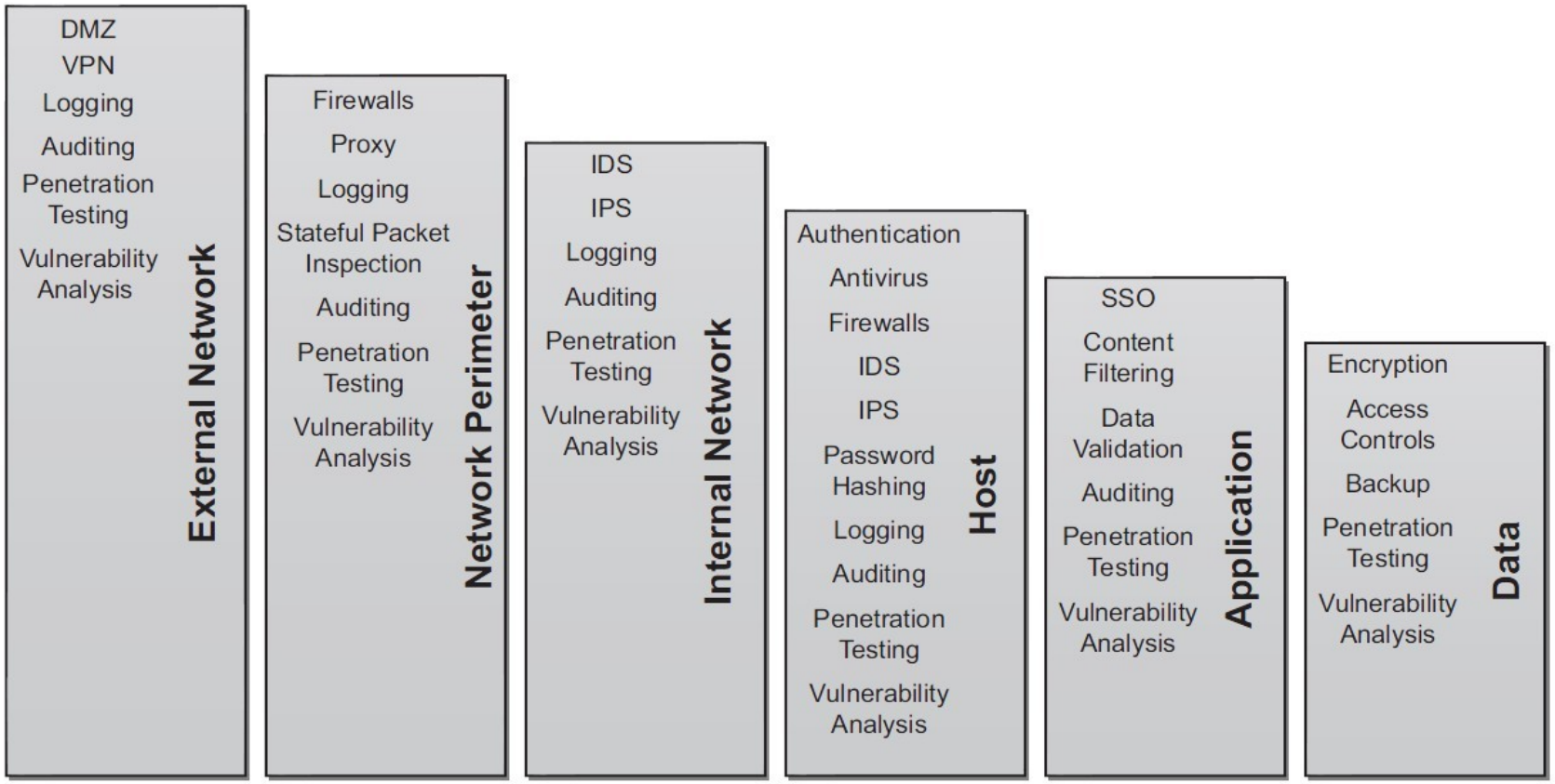
Défense en profondeur

Sécurité des logiciels



https://www.gotyoursixcyber.com/portfolio-item/defense-in-depth/

Défense en profondeur



Point unique de défaillance

Un point unique de défaillance est un point d'un système informatique dont le reste du système est dépendant et dont une panne entraîne l'arrêt complet du système.

Le point unique de défaillance est un risque pour la disponibilité du système. La présence d'un point unique de défaillance dans un système augmentant la probabilité d'apparition d'une attaque de déni de service.

http://fr.wikipedia.org/wiki/Point_individuel_de_defaillance

Moindre privilège

Only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

Security Engineering for Software. CS996 –CISM. JiaAn Chen. 03/31/04

- Tout ce qui n'est pas explicitement autorisé est interdit
- Autoriser uniquement ce qui est utile et justifié
- Cependant, attention à ne pas trop gêner les utilisateurs

Jean-Pierre Lips. Sécurité des Systèmes d'Information. 2011-2012. Université de Nice.

Compartimentage

Break the system up into as many isolated units as possible, in order to minimize the amount of damage that can be done to a system when a unit is compromised.

Défaillance sécurisé

• When a **system fails**, it should do so **securely**. This typically involves several things: secure defaults (default is to **deny access**); on failure **undo changes** and restore to a **secure state**; always check return values for failure; and in conditional code/filters make sure that there is a default case that does the right thing.

• The **confidentiality and integrity** of a system should remain even though **availability** has been **lost**.

• **Attackers** must not be permitted to gain access **rights to privileged objects** during a failure that are normally inaccessible.

• Upon failing, a system that reveals **sensitive information** about the failure to potential attackers could supply additional knowledge for creating an attack.

• Determine what may occur when a system fails and be sure it does not threaten the system.

https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/351-BSI.html

Security by Design – More Guidlines

- **Balance security and usability**
  - Try to avoid security procedures that make the system difficult to use. Sometimes you have to accept weaker security to make the system more usable.
- **Log user actions**
  - Maintain a log of user actions that can be analyzed to discover who did what. If users know about such a log, they are less likely to behave in an irresponsible way.
- **Use redundancy and diversity to reduce risk**
  - Keep multiple copies of data and use diverse infrastructure so that an infrastructure vulnerability cannot be the single point of failure.

Source : Software Engineering 9th / 10th Edition, Ian Sommerville