CGI : RGPD

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

Mars 2018

Programme

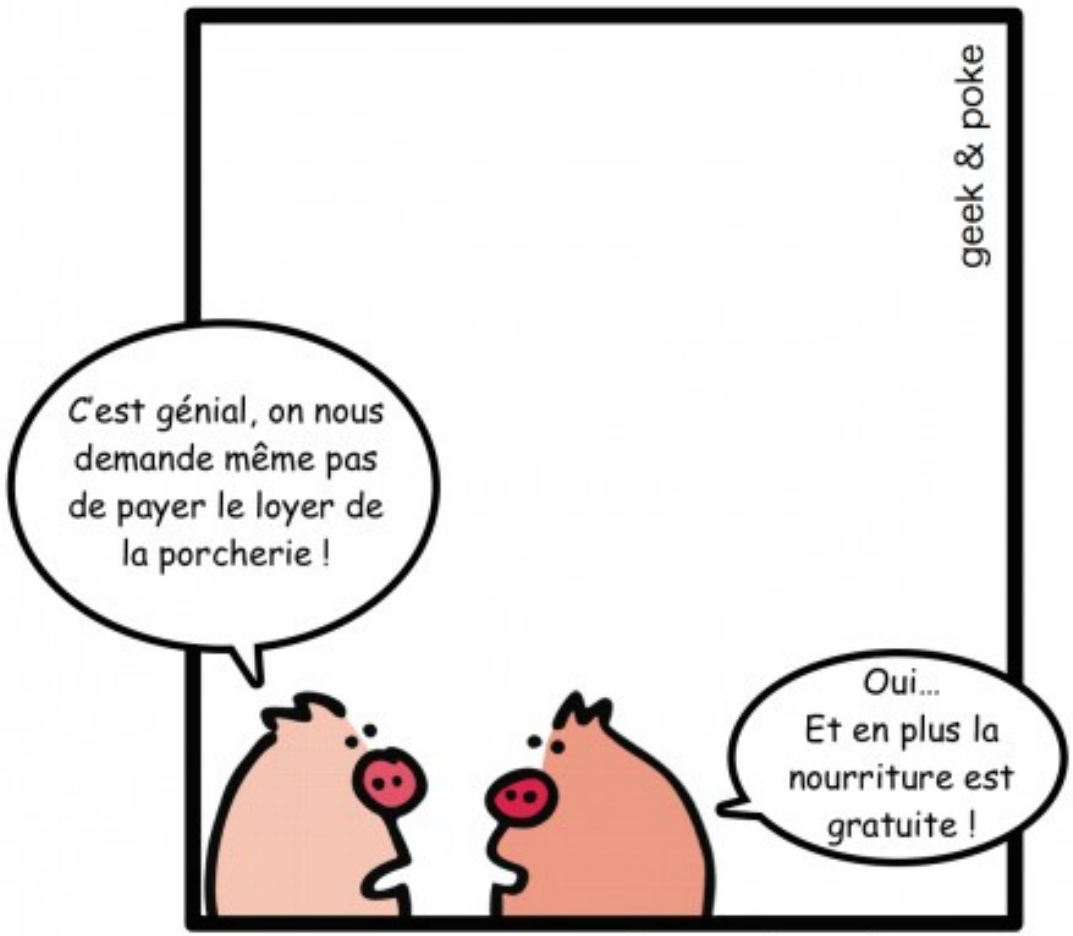
3 jours !

- Cadre juridique : RGPD
- Introduction à la cryptographie
- Mission Crypto

Outline

Big Data and Security

Free ?



Deux cochons discutant du modèle « gratuit »

Free ?

If it is free then you are the product

Data Privacy ?

Outline

CNIL créé en 1978

Commission nationale de l'informatique et des libertés

BUT

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

ANSSI créée le 7 juillet 2009.

STAD

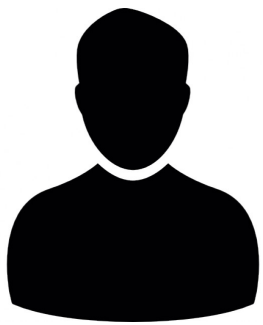
Système de Traitement Automatisé de Données

"Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

Aucune définition précise dans la loi

Dans les faits c'est presque tout :

3 acteurs

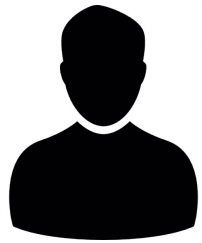


Utilisateur

Responsable

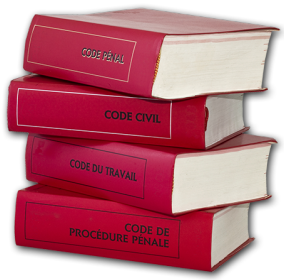
Pirate

L'utilisateur



Droits

- D'accès : demander directement au responsable d'un fichier s'il détient l'intégralité de ces données
- De rectification
- D'opposition dêtre dans un fichier
- Déréférencement sur le web par rapport au nom et prénom



Le responsable

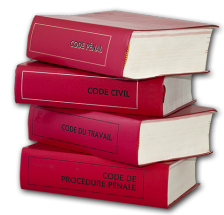
Et le sous-traitant via le contrat.

Devoirs

- Déclarer les traitements de données personnelles
  5 ans & 300 000
- Prendre toutes précautions pour la sécurité des données selon
  - la nature des données
  - les risques présentés par le traitement

  5 ans & 300 000

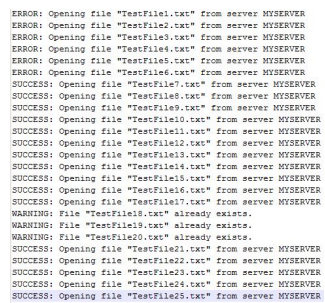
Lois informatique et libertés : Article 22 et Article 34.
Guide de la CNIL : La sécurité des données personnelles



Conservation des logs

LCEN 2004

- 1 an pour les logs (jurisprudence de la BNP Paribas)
- Décret 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne:
  - ip, url, protocole, date heure, nature de l'opération
  - éventuellement les données utilisateurs
  - éventuellement données bancaires
  - accédées dans le cadre d'une réquisition
  - conservées un an
  - données utilisateurs pendant un an après la clôture



Article 226-20 : les logs ont une date de péremption

Le pirate

Risques (STAD (Article 323-1))

- accès frauduleux ou maintien frauduleux de l'accès **2 ans & 60 000**
- suppression ou modification des données **3 ans & 100 000**
- si données à caractère personnel **5 ans & 150 000**
- altération du fonctionnement **5 ans et de 75 000**
- si données à caractère personnel **7 ans & 100 000**

Risques encourus

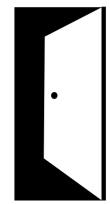
En pratique

- Atteintes aux intérêts fondamentaux de la nation (Sécurité nationale) Article 410-1 à 411-6
- Secret des communication pour l'autorité publique et FAI **3 ans et 45 000** Article 432-9
- Usurpation d'identité **5 ans et de 75 000** Article 434-23
- Importer, détenir, offrir ou mettre à disposition un moyen de commettre une infraction est puni

Sauf si

Pas de condamnation si

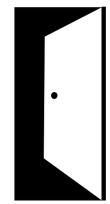
- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Sauf si

Pas de condamnation si

- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Il est donc important de protéger ces données

Outline

Réglement européen : 25 mai 2018

Règlement Général sur la Protection des Données RGPD

Histoire

Invalidation du “safe harbor” par la Cour de Justice de l’Union européenne : une décision clé pour la protection des données, 07 octobre 2015
Quel niveau de protection des données personnelles transférées aux Etats-Unis ?

Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

Guichet unique

Protection des mineurs

Portabilité

Objectifs?

Renforcer la transparence:

- Quelles données sont collectées?
- Dans quels buts?
- Pour combien de temps?

Faciliter l'exercice des droits

- droit à la rectification
- droit à la portabilité : récupération et communication à un autre traitement
- droit à l'oubli : suppression de données personnelles
  - dès qu'elles ne sont plus nécessaires au traitement
  - dès que le consentement de l'utilisateur a été retiré
  - dès que la personne s'y oppose

Règles d'or de la CNIL

1. Licéité du traitement
2. Finalité du traitement
3. Pertinence et proportionnalité des données; principe de minimisation
4. Conservation limitée des données
5. Exactitude, intégrité et confidentialité des données : principe de sécurité
6. Renforcement de la transaparence et exercice des doits facilité

Nouveautés

RESPONSABILITATION de TOUS les acteurs !
Outils de la confirmité

- Registre des traitements
- Registre sous-traitant
- Analyse d'impact PIA (CNIL)

Archivage et RGPD : à des fins statistiques.

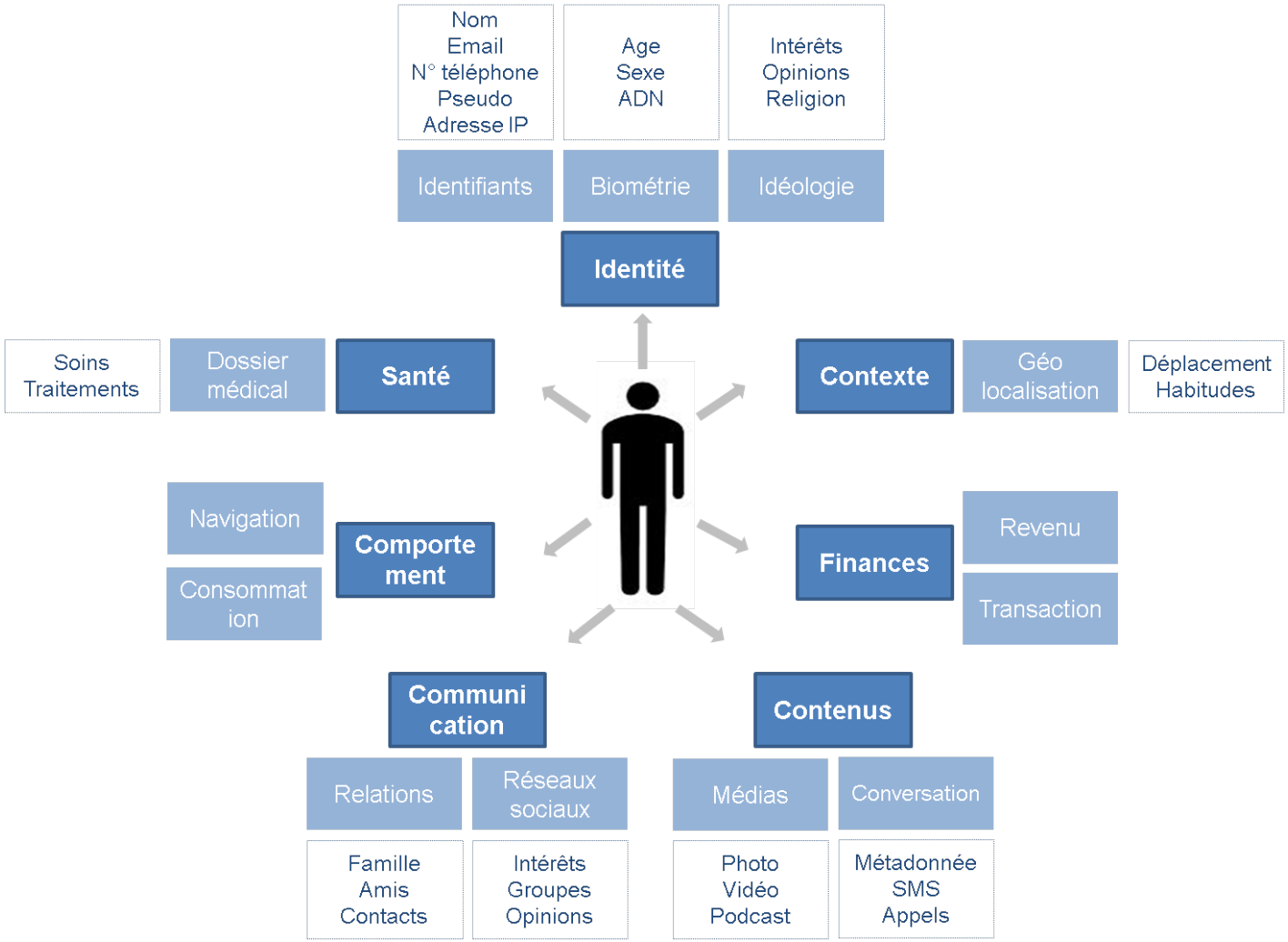
Principes

Tous responsables et tous auditables
Privacy by design
Security by default
DPO (Data Protection Officer)

- conformité au RGPD
- Point de contact avec les autorités

Analyse d'impact (PIA: Privacy Impact Assessment)

Qu'est-ce qu'une donnée personnelle ?



Qu'est-ce qu'une donnée personnelle ?

Information qui permet d'identifier une personne physique, directement ou indirectement.

- un nom,
- une photographie,
- une adresse IP,
- un numéro de téléphone,
- un identifiant de connexion informatique,
- une adresse postale,
- une empreinte,
- un enregistrement vocal,
- un numéro de sécurité sociale,
- un mail, etc.

Qu'est-ce qu'une donnée personnelle **sensible**?

Données liés à de la discrimination ou des préjugés :

- Une opinion politique,
- une sensibilité religieuse,
- un engagement syndical,
- une appartenance ethnique,
- une orientation sexuelle,
- une situation médicale ou des idées philosophiques sont des données sensibles.

Toute collecte sans consentement préalable écrit, clair et explicite est interdite !

RPGD : en 6 étapes @CNIL

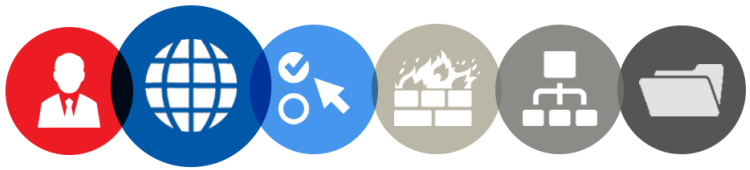
1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

Étape 1 : Désigner un pilote

Délégué à la protection des données

Mission d'information, de conseil et de contrôle en interne.
Conformité au RGPD.

Étape 2 : Cartographier

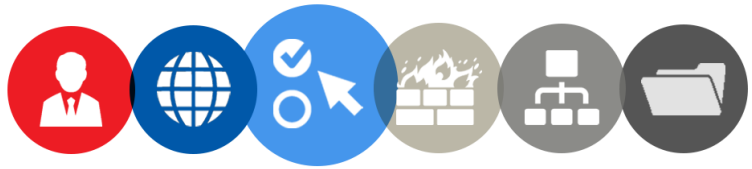


Tenir une documentation interne complète sur leurs traitements de données personnelles

- Catégories les données traitées
- Recenser précisement vos traitements de données personnelles (**Registre des traitements**)
- Lister les objectifs
- Identifier les acteurs
- Identifier les flux des données

But : Assurer que ces traitements respectent bien le règlement.

Étape 3 : Prioriser



1. Collecter et traiter **que les données nécessaires**.
2. **Base juridique du traitement** : consentement de la personne, contrat, obligation légale ...
3. Révisez vos **mentions d'information** : articles 12, 13 et 14: droits de la personne concernée : Transparence, Information et Transitivité
4. Vérifier vos **sous-traitants** et clause des contrats
5. Prévoyez les **modalités d'exercice des droits** des personnes concernées : droit d'accès, de rectification, droit à la portabilité, retrait du consentement...
6. Vérifiez les **mesures de sécurité** mises en place.

Étape 3 : VIGILANCE, des **types** de données

- origine prétendument **raciale ou ethnique**, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- la **santé** ou l'orientation sexuelle,
- génétiques ou **biométriques**,
- infraction ou de condamnation **pénale**,
- sur les **mineurs**.

Étape 3 : VIGILANCE, votre traitement

- la surveillance **systématique** à grande échelle d'une zone accessible au public
- l'évaluation **systématique** et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

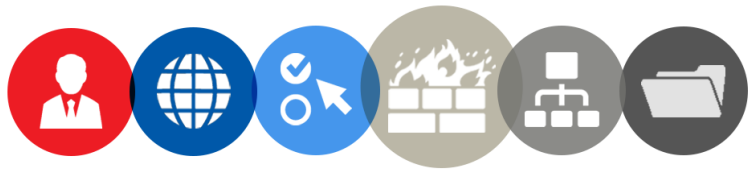
Étape 3 : VIGILANCE **transfert** des données hors UE

- Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne ;
- Dans le cas contraire, encadrez vos transferts.

Étape 4 : Gérer les risques

Privacy Impact Assessment (PIA)

Data protection impact assessment



- Principes et droits fondamentaux, **non négociables**, de la loi
- Gestion des **risques sur la vie privée** des personnes concernées, pour déterminer les mesures techniques et d'organisation pour protéger les données personnelles.

Un PIA contient :

- Une **description** du traitement étudié et de ses **finalités**.
- Une **évaluation de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- Une **évaluation des risques** pour les droits et libertés des personnes, les mesures envisagées pour faire face aux risques.

Étape 4 : Qui participe au PIA?

- **Le responsable de traitement** : valide et applique le PIA.
- **Le délégué à la protection des données** : élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s)** : fournit les informations nécessaires à l'élaboration du PIA ;
- **Les métiers (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre)** : aident à la réalisation du PIA en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

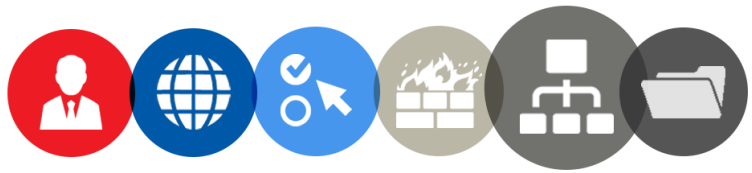
Étape 4 : **PIA obligatoire** Art. 35

Pour tout traitement susceptible d'engendrer des **risques élevés** pour les droits et libertés des personnes concernées.

1. Evaluation ou notation;
2. Décision automatisée avec effet juridique significatif;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si **au moins 2 de ces critères**, alors faire un PIA.

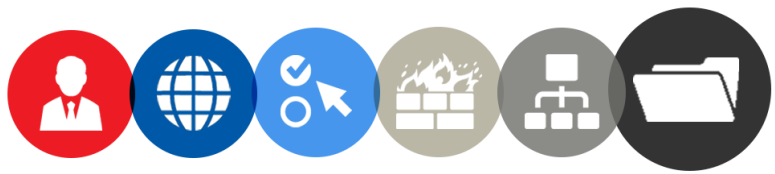
Étape 5 : Organiser



- Protection des données personnelles **dès la conception**
- **Sensibiliser et d'organiser la remontée d'information**
- Traiter les **réclamations et les demandes** des personnes concernées quand à l'exercice de leurs droits
- **Anticiper les violations de données**, dans les 72 heures aux autorités et personnes concernées

Étape 6 : Documenter

Prouver la conformité = Avoir la documentation nécessaire



- Traitements
- Information des personnes
- Contrat pour les acteurs

Étape 6 : Documenter les traitements

- Le **registre des traitements** (pour les responsables de traitements) ou des **catégories d'activités de traitements** (pour les sous-traitants)
- **PIA** pour les traitements à risque
- L'**encadrement des transferts** de données hors de l'Union européenne.

Étape 6 : Documenter l'information

- Les **mentions d'information**
- Les modèles de **recueil du consentement** des personnes concernées,
- Les procédures **mises en place** pour l'exercice des droits

Étape 6 : Documenter les contrats

- Les **contrats avec les sous-traitants**
- Les **procédures internes** en cas de violations de données
- Les **preuves** que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Objectif

Responsabilisation de tous les acteurs impliqués dans le traitement des données personnlles dès lors qu'elle concernent des résidents européens.

- Obligation de transparence et traçabilité
  - Contrtat écrit entre les acteurs
  - Autorisation écrite des traitement
  - Démontrer le respect de vos obligations
  - Ternir un **registre des traitements**
- Protection by design et by default (paramètres, accès, purge)
- Obligation de garantir la sécurité des données traitées
- Obligation d'assistance, d'alerte et de conseil (immédiate)

Registre des catégories d'activités de traitement

- nom et les coordonnées de chaque client
- le nom et les coordonnées de chaque sous-traitant
- le nom et les coordonnées du délégué à la protection des données
- les catégories de traitements effectués
- les transferts de données hors UE
- une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place

Qui est touché ?

TOUT LE MONDE !

- les prestataires de services informatiques
- les agences de marketing ou de communication
- tout organisme offrant un service ou une prestation
- Un organisme public ou une association

qui traite les données personnelles.

Sanctions

Jusqu'à 10 ou 20 millions d'euros, ou 2% ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent.
En France la CNIL devient autorité de contrôle

Sanctions pour le sous-traitant

- si vous agissez en dehors des instructions licites de votre client ou contrairement à ces instructions ;
- si vous n'aidez pas votre client à respecter ses obligations
- si vous ne mettez pas à la disposition de votre client les informations permettant de démontrer le respect des obligations ou pour permettre la réalisation d'audits
- si vous n'informez pas votre client qu'une instruction constituerait une violation du règlement européen
- si vous sous-traitez sans autorisation préalable de votre client
- si vous fait es appel à un sous-traitant qui ne présente pas de garanties suffisantes
- si vous ne désignez pas un délégué à la protection des données
- si vous ne tenez pas de registre des catégories d'activités de traitement

Bilan après 4 mois

- 24500 organismes ont 1 DPO: 13000 DPO contre 5000 CIL
- 600 notifications de violations, environ 7 par jour
- 3 millions de visites sur le site de la CNIL
- 150 000 téléchargements du registre simplifié de la CNIL
- 3767 plaintes soit une augmentation de 64%
- plus de 200 plaintes transfrontalières

24 Juillet 2018 : Sanction de 50 000 € de la CNIL à l'encontre de la société DAILYMOTION, mot de passe stocké en clair temporairement.
15 Aout 2018 : Sanction de 30 000 € par la CNIL à l'encontre de l'Office Public de l'Habitat de Rennes Métropole

4 Croyances sur le RGPD par Florence BONNET

I. La probabilité de faire l'objet d'un contrôle de la CNIL est faible

- obligation de notifier et de communiquer les violations de données personnelles à l'autorité et aux personnes concernées le cas échéant.
- toute personne a le droit de réclamer auprès d'une autorité de contrôle et d'exercer son droit d'obtenir réparation.

4 Croyances sur le RGPD par Florence BONNET

II. En cas de contrôle, il suffira de collaborer avec la CNIL et de faire preuve de réactivité pour éviter une sanction

Absence de mesures élémentaires de sécurité = non-conformité.

- Mise en ligne d'un site sans test
- Exposition aux données sans authentification (mot de passe suffisamment robustes)
- Ne doivent pas être conservés ou transmis en clair mais de manière sécurisée
- Les connexions et flux de données doivent être sécurisés
- Les connexions à une plateforme des paiements doivent être tracés
- Le dispositif de communication bluetooth doit être sécurisé
- La connexion à distance doit être sécurisée (VPN, IP)
- Les données les sensibles doivent être conservées et sécurisées
- Le chiffrement doit être à l'état de l'art ! Pas de MD5 !

4 Croyances sur le RGPD par Florence BONNET

II.

- Protection du secret : le sel doit être conservé dans un espace distinct de celui où sont stockés les mots de passe ;
- Les numéros de carte bancaire ne doivent pas être conservés en clair avec les cryptogrammes .
- Les accès aux données doivent être strictement limités aux seules personnes ayant besoin d'en connaitre
- il appartient au responsable de traitement, d'adapter les conditions d'usage de ce logiciel à sa propre population

4 Croyances sur le RGPD par Florence BONNET

III. Se croire à l'abri parce qu'il existe forcément une politique de sécurité dans l'entreprise

- il est vain pour la société de chercher à se dégager de sa responsabilité en invoquant de supposées procédures préventives en la matière (procédure sécurité conforme ISO 27001, exigences du Règlement CRBF 97-02)

4 Croyances sur le RGPD par Florence BONNET

IV. c'est le sous-traitant qui sera responsable

- Il convient de tracer et de documenter les échanges avec le prestataire
- L'intervention d'un prestataire crée une responsabilité supplémentaire de contrôle effectif des agissements du prestataire et des solutions utilisées par ce dernier.
- La prestation de service doit obligatoirement faire l'objet d'un contrat encadrant les obligations du sous-traitant en matière de sécurité et de confidentialité des données à caractère personnel

Note: 70%

Faire un PIA pour votre entreprise ou une partie de votre entreprise.

Outline

Démarche

Publiée en octobre 2005 et révisée en 2013.

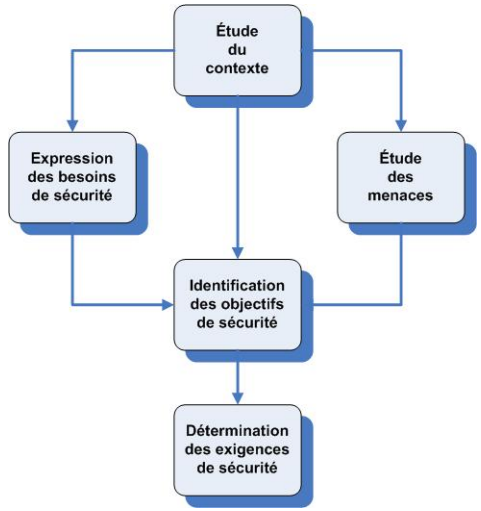
1. Phase d'établissement
2. Phase d'implémentation
3. Phase de maintien
4. Phase d'amélioration

SMSI : Système de management de la sécurité de l'information

Phase d'établissement (PLAN)

1. Définir la politique et le périmètre du SMSI
2. Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité (EBIOS)
3. Traiter le risque et identifier le risque résiduel par un plan de gestion (Évitement, réduction, transfert, acceptation)
4. Choisir les mesures de sécurité à mettre en place

EBIOS



1. Identifier les actifs ;
2. Identifier les personnes responsables ;
3. Identifier les vulnérabilités ;
4. Identifier les menaces ;
5. Identifier leurs impacts sur les actifs à défendre ;
6. Èvaluer la vraisemblance ou potentialité du risque ;
7. Estimer les niveaux de risque, fonction de leur potentialité et de leur impact.

Phase d'implémentation (DO)

1. Établir un plan de traitement des risques
2. Déployer les mesures de sécurité
3. Générer des indicateurs:
   - De performance pour savoir si les mesures de sécurité sont efficaces
   - De conformité qui permettent de savoir si le SMSI est conforme à ses spécifications
4. Former et sensibiliser le personnel

Phase de maintien (Check)

Gérer le SMSI au quotidien et à détecter les incidents

- Le contrôle interne (s'assurer en permanence que les processus fonctionnent normalement)
- Les audits internes (vérifier la conformité et l'efficacité du système de management.
- Les revues (ou réexamens) qui garantissent périodiquement l'adéquation du SMSI avec son environnement.

Phase d'amélioration (Act)

Actions correctives, préventives ou d'amélioration pour les incidents et écarts constatés lors de la phase Check.

Outline

Définition

La maîtrise et la protection de l'information stratégique utile pour tout acteur économique.

3 piliers

- Maîtrise de l'information, management des connaissances
- Protection du patrimoine informationnel
- Stratégie d'influence et lobbying

La compétitivité est la finalité de l'IE
(Intelligence = renseignement)

Maîtriser l'Information

- Identifier les sources
- Collecter l'information (veille, reseaux sociaux ...)
- Exploitation : analyse et aide à la décision
- Diffusion :

Protection de l'Information

"Seuls les paranoïaques survivent", Andy GROVE, Cofondateur d'Intel en 1968

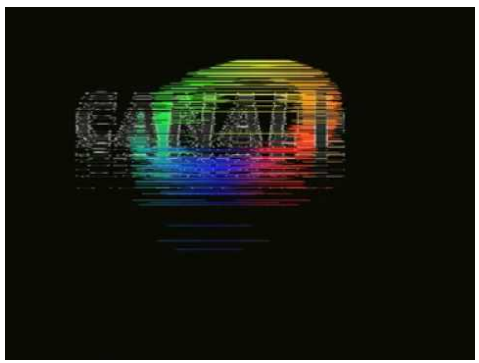
1. Classification de l'information
2. Diagnostic
3. Protection des accès
4. Sensibilisation
5. Surveillance, détection

Stratégies d'Influence

- Presse, média
- Blog, réseaux sociaux
- Communication en cas de crise infomration/désinformation

Outline

La sécurité numérique est déjà là



Mais prendre de bonnes habitudes ça prend du temps ...

même quand c'est important

Devenir acteur de sa sécurité numérique

Devenir acteur de sa sécurité numérique

car la sécurité c'est pas automatique.

Sécurité de mes mots de passe

Sécurité de mes mots de passe

Top 25 en 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

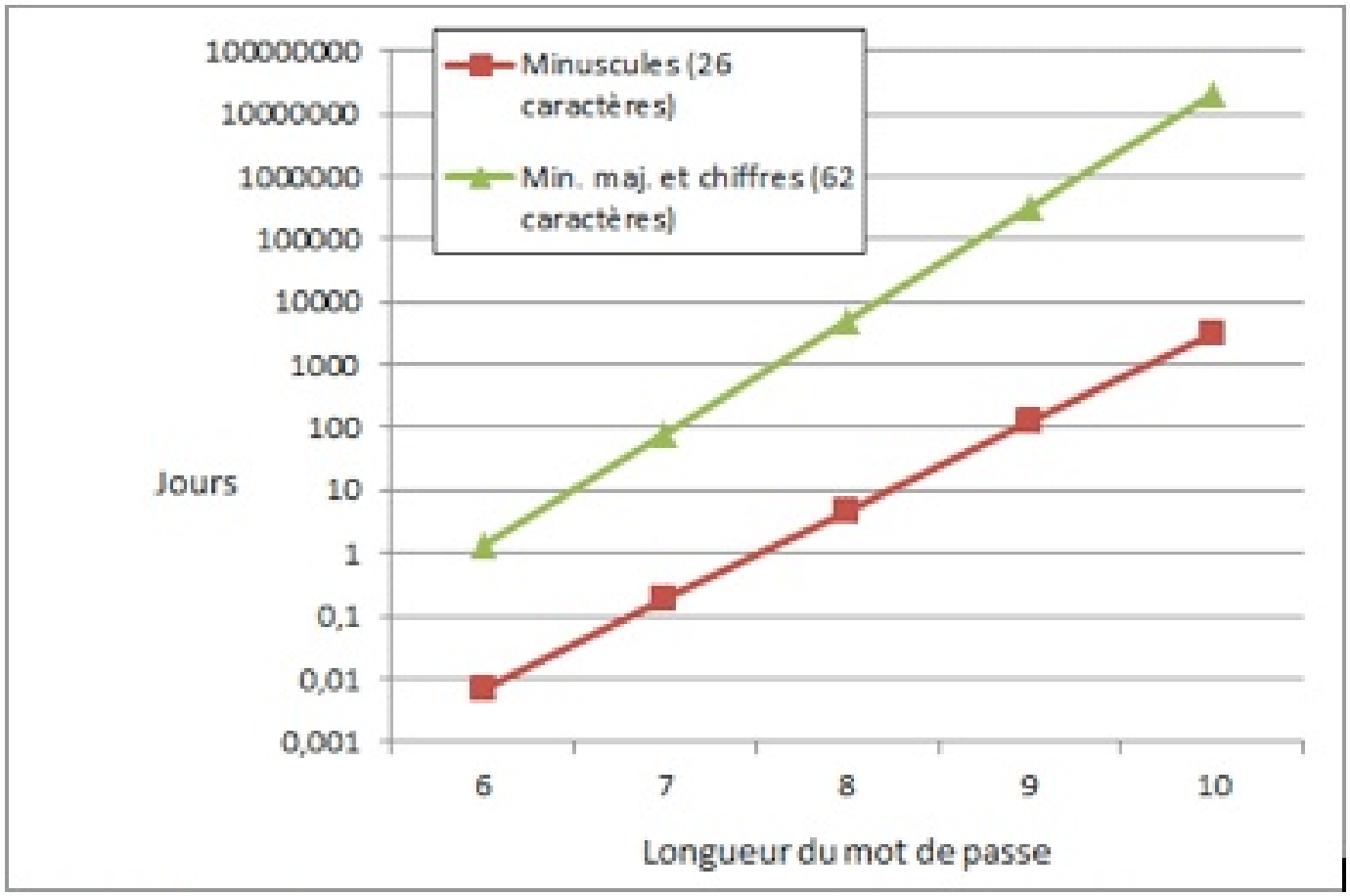
Top 25 en 2015

1. 123456 (Unchanged)
2. password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 1)
5. 12345 (Down 2)
6. 123456789 (Unchanged)
7. football (Up 3)
8. 1234 (Down 1)
9. 1234567 (Up 2)
10. baseball (Down 2)
11. **welcome**
12. **1234567890**
13. abc123 (Up 1)
14. 111111 (Up 1)
13. **1qaz2wsx**
14. dragon (Down 7)
15. master (Up 2)
16. monkey (Down 6)
17. letmein (Down 6)
18. **login**
19. **princess**
20. **qwertyuiop**
21. **solo**
22. **passw0rd**
23. **starwars**

Top 25 en 2016

1. 123456 (Unchanged)
2. 123456789 (Up 5)
3. qwerty (Up 1)
4. 12345678 (Down 1)
5. 111111 (Up 9)
6. **1234567890**
7. 1234567 (Up 1)
8. password (Down 6)
9. **123123**
10. **987654321**
11. **qwertyuiop**
12. **mynoob**
13. **123321**
14. **666666**
15. **18atcskd2w**
16. **7777777**
17. **1q2w3e4r**
18. **654321**
19. **555555**
20. **3rjs1la7qe**
21. **google**
22. **1q2w3e4r5t**
23. **123qwe**
24. **zxcvbnm**
25. **1q2w3e**

Passwords: Brute force



Quelques chiffres

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

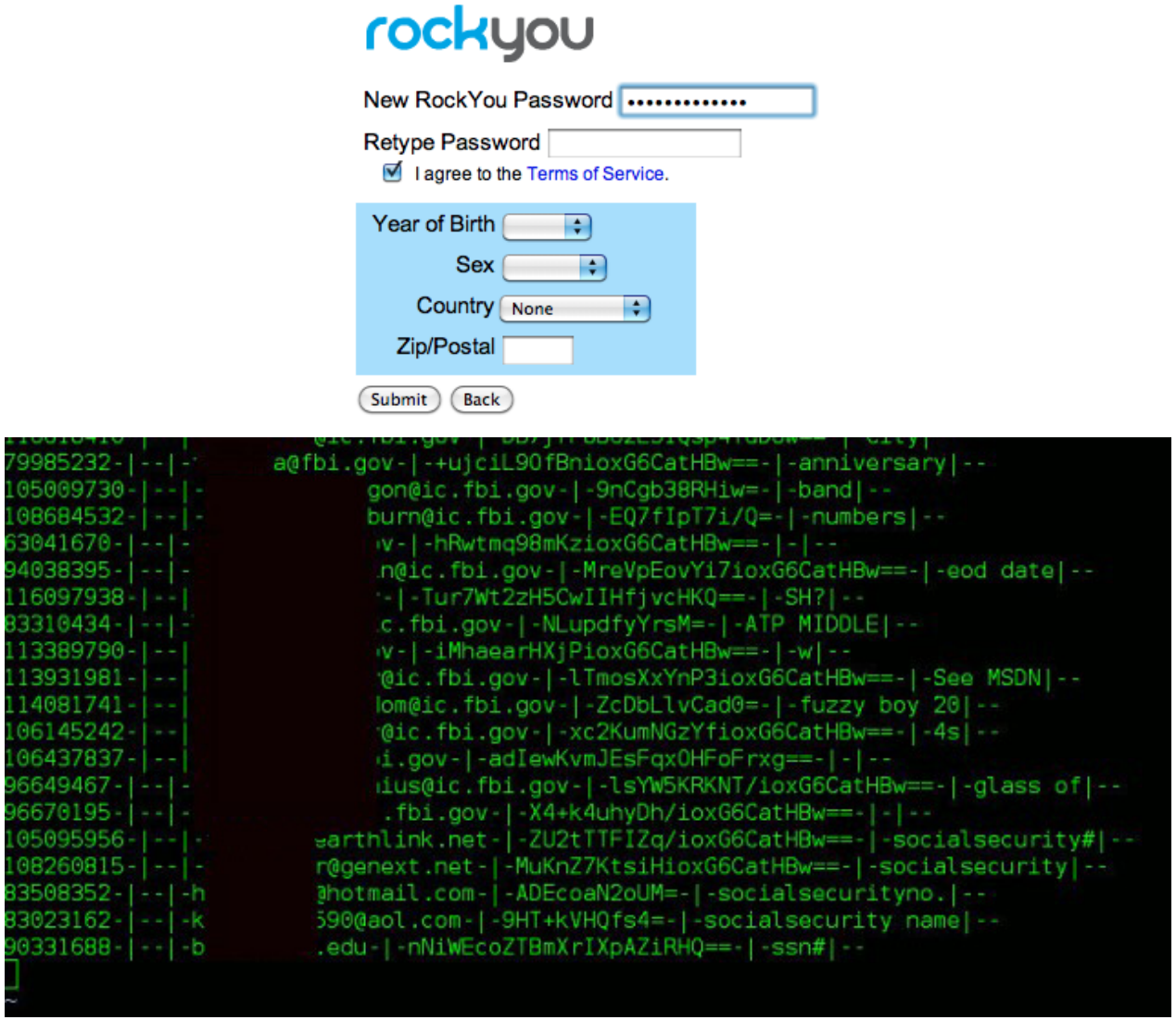
Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Calculer la « force » d'un mot de passe

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots d plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l' de chiffrement standard AES (128 bits).

Suite aux fuites ...



Suite aux fuites ...

... j'ai changé mes mots de passe !

En réalité

En réalité


©Crown Copyright, 2012
www.dukeandduchessofcambridge.org


MilFlip Logon Details
RMS
ATTENTION ALL RMS STUDENTS

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Remarques:

- Il est difficile pour un humain de mémoriser 12 caractères aléatoires.
- Passphrase.

Comment stocker les mots de passe ?

Stockage

- En clair
- Haché (pwd) $\Rightarrow$ Rainbowtables !
- Haché (pwd + Salt)
- Haché (pwd + Salt-user)
- bcrypt(pwd + Salt-user) (bcrypt = hachage plus lent ou PBKDF2)
- AES(bcrypt(pwd + Salt-user), SecretKey)

`http://linuxfr.org/users/elyotna/journaux/l-art-de-stocker-des-mots-de-passe`

Résumé

- Comment les mots de passe sont-ils choisis ?
- Comment sont-ils transmis entre l'utilisateur et le vérificateur ?
- Comment sont-ils stockés/protégés par l'utilisateur ?
- Comment sont-ils stockés/protégés par le vérificateur ?

Contre-mesures

- Challenge / Response:
  - C to S : hello
  - S to C : r
  - C to S : $H(r||pwd)$
- Limiter le nombre de tentatives en bloquant par exemple le système pour une certaine durée après un certain nombre d'essais.
- S'assurer que chaque essai est bien mené par un humain (et non pas un ordinateur) en utilisant des techniques de type CAPTCHA "Completely Automated Public Turing test to tell Computers and Humans Apart"
- OTP avec SMS en plus pour confirmer.

John the Ripper

`www.openwall.com/john/`

Keep Pass

`http://keepass.info/`

KeePass

Wireshark

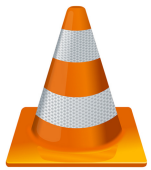
https://www.wireshark.org/

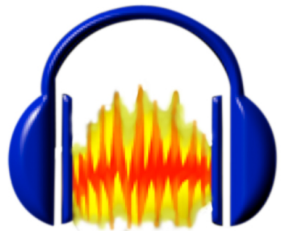
Homeworks

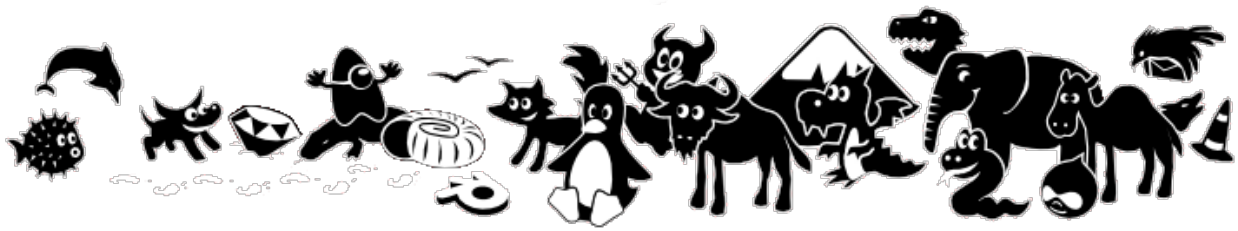
Préparation du TP du lundi 10 décembre:
Réaliser en python un stockage de mot de passe du moins au plus sécurisé.

Outline

Exemples







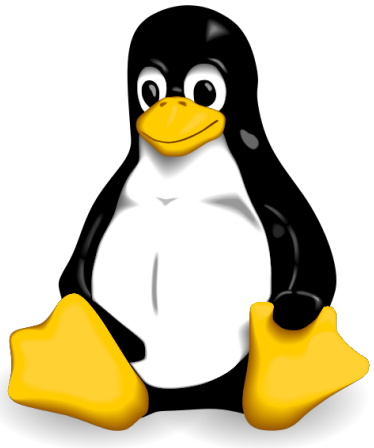
Logiciel LIBRE

"free software" $\neq$ 

Exemples

- **libre, gratuit** : Linux, FreeBSD, perl, python ...
- **libre, non gratuit** : achéter un CD, payer des développeurs...
- **non libre, gratuit** : Acrobat Reader, Chrome, Flash ...
- **non libre, non gratuit** : no comment.

Free as in freedom



4 Freedoms

- Freedom 0: **Run** the program as you wish, for any purpose.
- Freedom 1: **Modify** the program to suit your needs. (you

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Que font les programmes binaires téléchargés suivants ?

`http://sancy.univ-bpclermont.fr/~lafourcade/Helloworld`

`http://sancy.univ-bpclermont.fr/~lafourcade/Hellworld`

Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
  system("wget -q http://sancy.univ-bpclermont.fr/
         ~lafourcade/Helloworld");
  system("chmod 777 Helloworld");
  system("clear");
  system("./Helloworld");
  return 0;
}
```

Outline

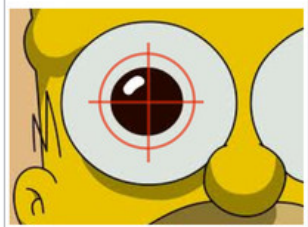
Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

Example: e-voting

- An e-voting system should ensure that
  - only registered voters vote,
  - each voter can only vote once,
  - integrity of votes,
  - privacy of voting information (only used for tallying), and
  - availability of system during voting period

Outline

Definition

Malware

A set of instructions that run on your computer and make your system do something that an attacker wants it to do.

Virus (Fred Cohen 1983)

A program that can infect other programs by modifying them to include a, possibly evolved, version of itself.

Polymorphic : uses a polymorphic engine to mutate while keeping the original algorithm intact (packer)
Methamorpic : Change after each infection

Classification

Propagation (codes auto-reproductor)

- Virus: human-assisted propagation (e.g., open email attachment)
- Worm: automatic propagation without human assistance.

Concealment

- Logic Bombs : wait an event to attack
- Rootkit: modifies operating system to hide its existence
- Trojan: provides desirable functionality but hides malicious operation

Botnet:

- Programs running autonomously and controlled remotely
- Can be used to spread out worms, mounting DDoS attacks

Backdoors

History Virus

- 1972 sci-fi novel "When HARLIE Was One" features a program called VIRUS that reproduces itself
- First academic use of term virus by PhD student Fred Cohen in 1984, who credits advisor Len Adleman with coining it
- In 1982, high-school student Rich Skrenta wrote first virus released in the wild: Elk Cloner, a boot sector virus
- (c)Brain, by Basit and Amjood Farooq Alvi in 1986, credited with being the first virus to infect PCs

History Worms

- First worms built in the labs of John Shock and Jon Hepps at Xerox PARC in the early 80s
- CHRISTMA EXEC written in REXX, released in December 1987, and targeBng IBM VM/CMS systems was the first worm to use e-mail service
- The first internet worm was the Morris Worm, written by Cornell student Robert Tappan Morris and released on November 2, 1988

Virus Phases

- Dormant phase
- Propagation phase.
- Triggering phase.
- Action phase.

Viruses

- Encrypted virus :
  - Decryption engine + encrypted body
  - Randomly generate encryption key
  - Detection looks for decryption engine
- Polymorphic virus
  - Encrypted virus with random variations of the decryption engine (e.g., padding code)
  - Detection using CPU emulator.
- Metamorphic virus
  - Different virus bodies
  - Approaches include code permutation and instrucBon replacement
  - Challenging to detect

Cryptolocker

Wannacry ...

Antivirus

Antivirus = Vaccin

IDS Intrusion Detection System

Anaylisis of log, activities...

Signatures: A Malware Countermeasure

Scan compare the analyzed object with a database of signatures

- A signature is a virus fingerprint
  - E.g.,a string with a sequence of instructions specific for each virus
  - Different from a digital signature
- A file is infected if there is a signature inside its code
- Fast pattern matching techniques to search for signatures
- All the signatures together create the malware database that usually is proprietary

White/Black Listing

Maintain database of cryptographic hashes for

- Operating system files
- Popular applications
- Known infected files
- Compute hash of each file
- Look up into database
- Needs to protect the integrity of the database

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis:
  - Based on the instrucBons, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,

  Execution emulation
  - Run code in isolated emulation environment
  - Monitor actions that target file takes
  - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Online AntiVirus

Software Online

- Free browser plug-in
- Authentication through third party certificate (i.e. VeriSign)
- No shielding
- Software and signatures update at each scan
- Poorly configurable
- Scan needs internet connection
- Report collected by the company that offers the service

Offline AntiVirus

Software Offline

- Paid annual subscription
- Installed on the OS
- Software distributed securely by the vendor online or a retailer
- System shielding
- Scheduled software and signatures updates
- Easily configurable
- Scan without internet connection
- Report collected locally and may be sent to vendor

Quarantine

- A suspicious file can be isolated in a folder called quarantine :
  - E.g ,. if the result of the heuristic analysis is positive and you are waiting for db signatures update
- The suspicious file is not deleted but made harmless:
  - the user can decide when to remove it or eventually restore for a false positive
  - Interacting with a file in quarantine it is possible only through the antivirus program
- The file in quarantine is harmless because it is encrypted
- Usually the quarantine technique is proprietary and the details are kept secret

Static vs. Dynamic Analysis

Static Analysis

- Checks the code without trying to execute it
- Quick scan in white list
- Filtering: scan with different antivirus and check if they return same result with different name
- Weeding: remove the correct part of files as junk to better identify the virus
- Code analysis: check binary code to understand if it is an executable, e.g., PE
- Disassembling: check if the byte code shows something unusual

Static vs. Dynamic Analysis

Dynamic Analysis

- Check the execution of codes inside a virtual sandbox
- Monitor:
  - File changes
  - Registry changes
  - Processes and threads
  - Networks ports

Virus Detection is Undecidable

Theorem by Fred Cohen (1987)

Virus abstractly modeled as program that eventually executes infect Code where infect may be generated at runtime

Proof by contradiction similar to that of the halting problem.
Suppose isVirus (P) determines whether program P is a virus
Define new program Q as follows:
Q: if (not isVirus (Q)) then Q infects else Q stops
Running isVirus on Q achieves a contradiction, two cases

- isVirus(Q) is true $\Rightarrow$ Q does nothing
- isVirus(Q) is false $\Rightarrow$ Q infects

Other Undecidable Detection Problems

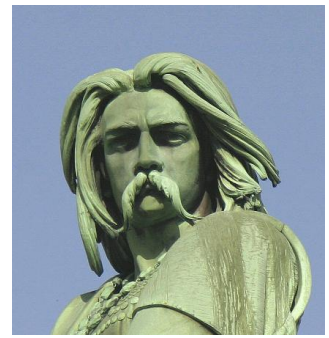
- Detection of a virus:
  - by its appearance
  - by its behavior
- Detection of an evolution of a known virus
- Detection of a triggering mechanism
  - by its appearance
  - by its behavior
- Detection of a virus detector
  - by its appearance
  - by its behavior
- Detection of an evolution of
  - a known virus
  - a known triggering mechanism
  - a virus detector

Outline

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something
without revealing any information

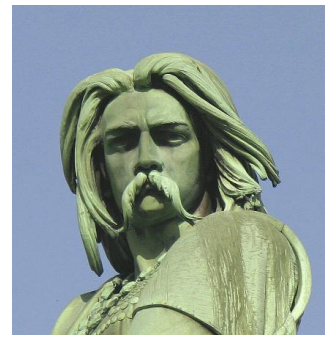


Verifier (V)

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something
without revealing any information

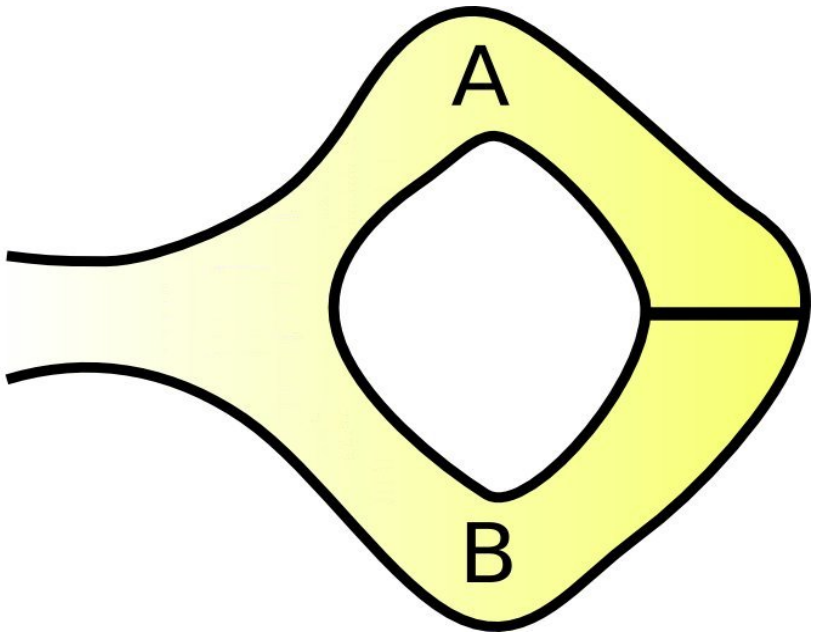


Verifier (V)

Applications:

- Authentication systems: prove its identity to someone using a password without reavealing anything about the secret.
- Prove that a praticipant behavior is correct according to the protocol (e.g. integrity of ballots in vote).
- Group signature, secure multiparty computation, e-cash ...

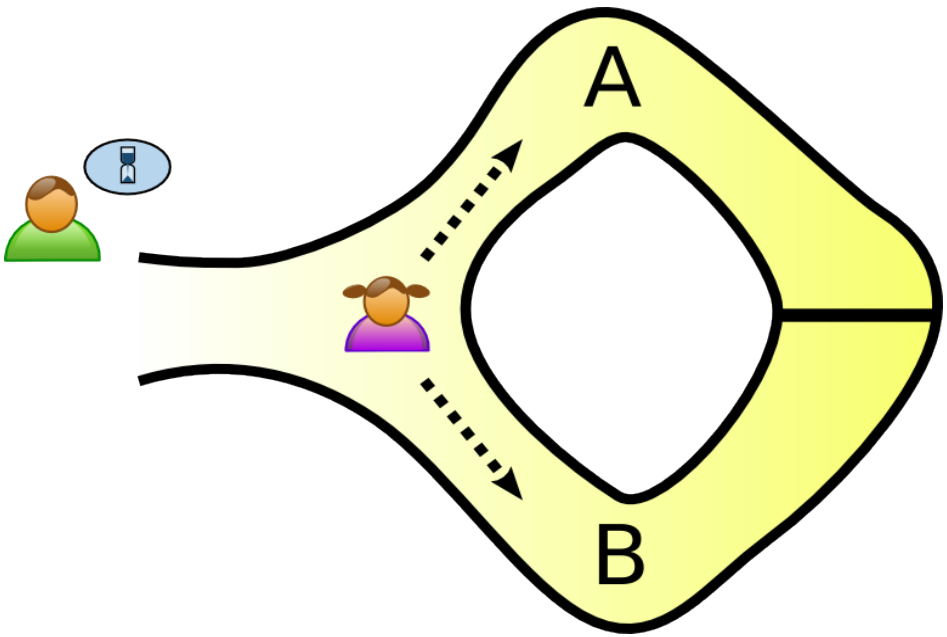
Cave example (0)



Door with a secret code

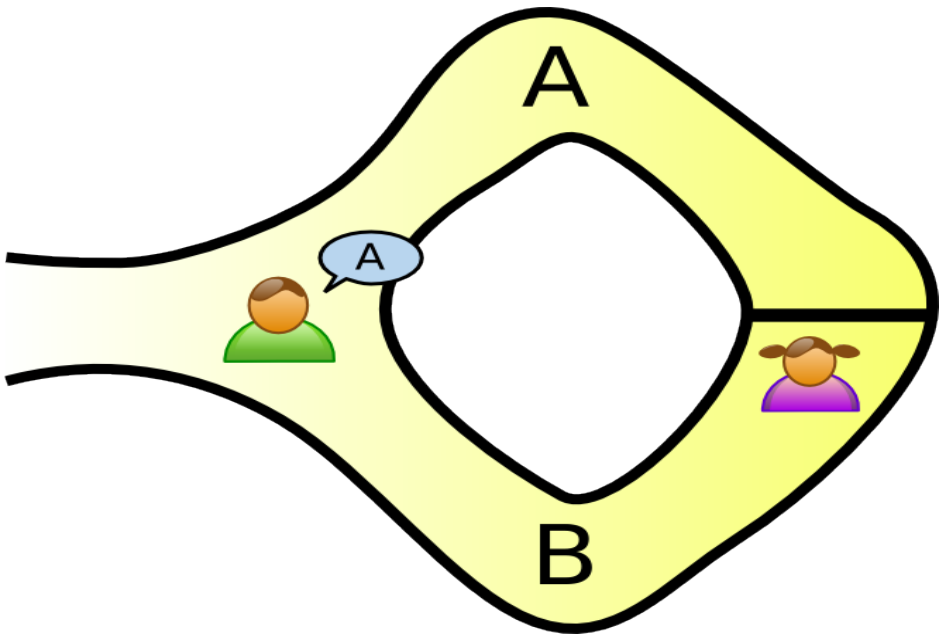
Cave example (I)

V waits outside while P chooses a path



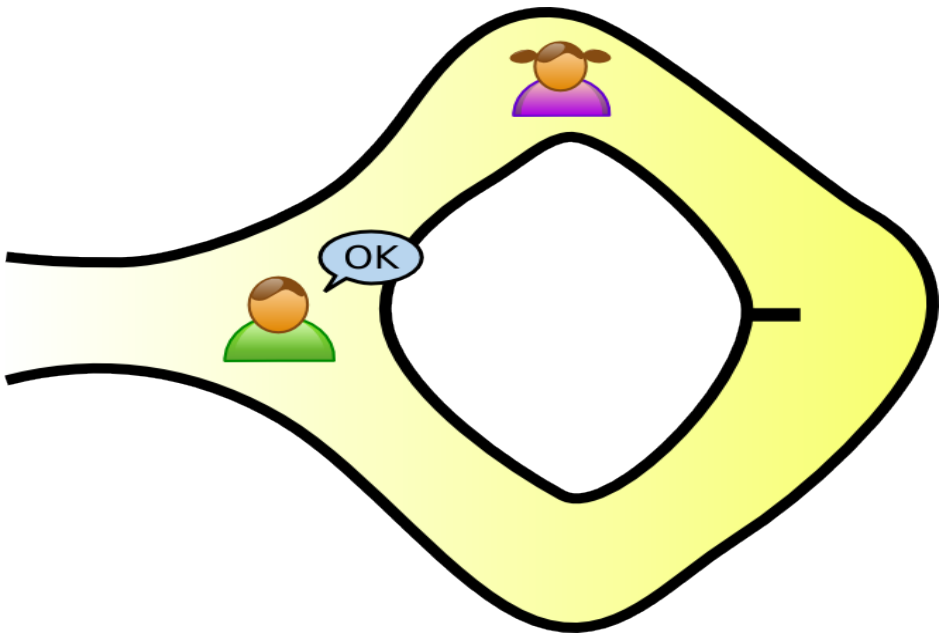
Cave example (II)

V enters and shouts the name of a path



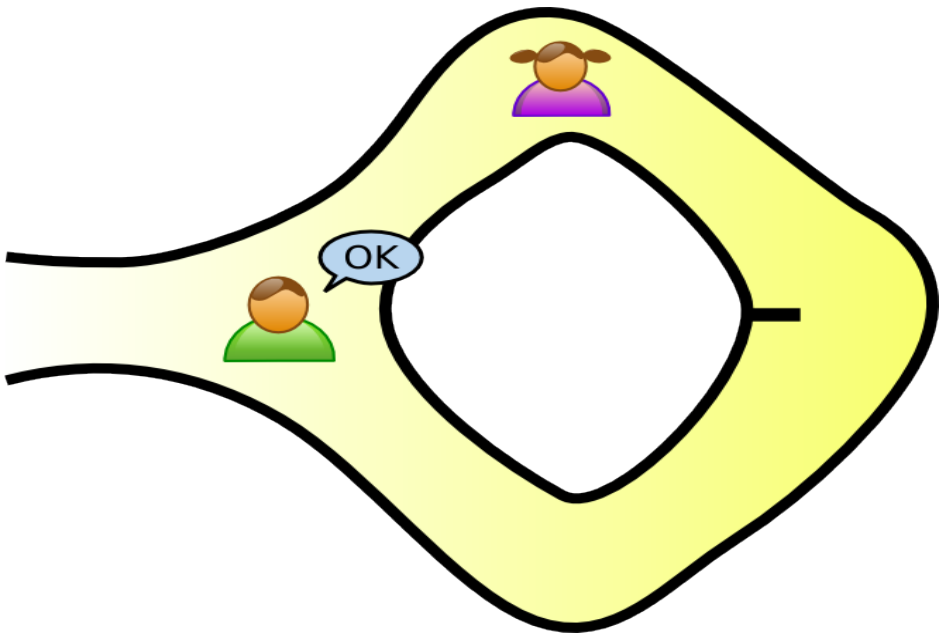
Cave example (III)

P returns along the desired path (using the secret if necessary)



Cave example (III)

P returns along the desired path (using the secret if necessary)

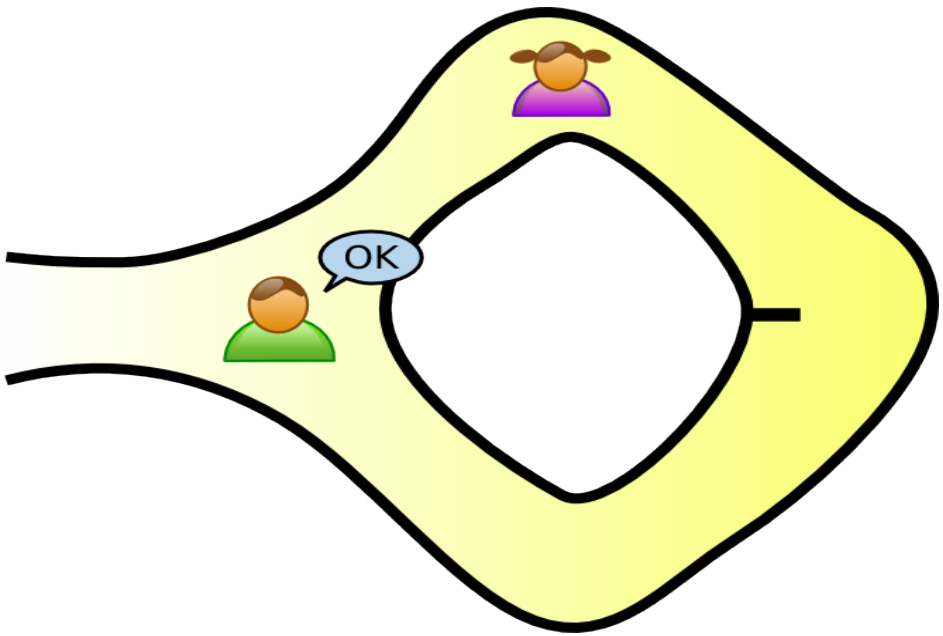


$A =$ "P does not know the secret"
is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

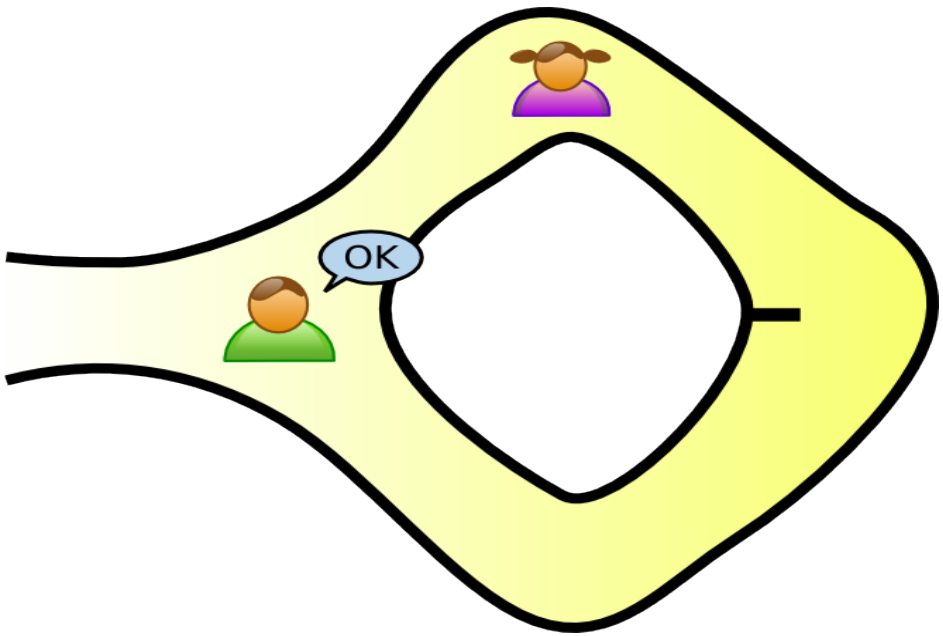
$$Pr[A] = \frac{1}{2}$$

After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

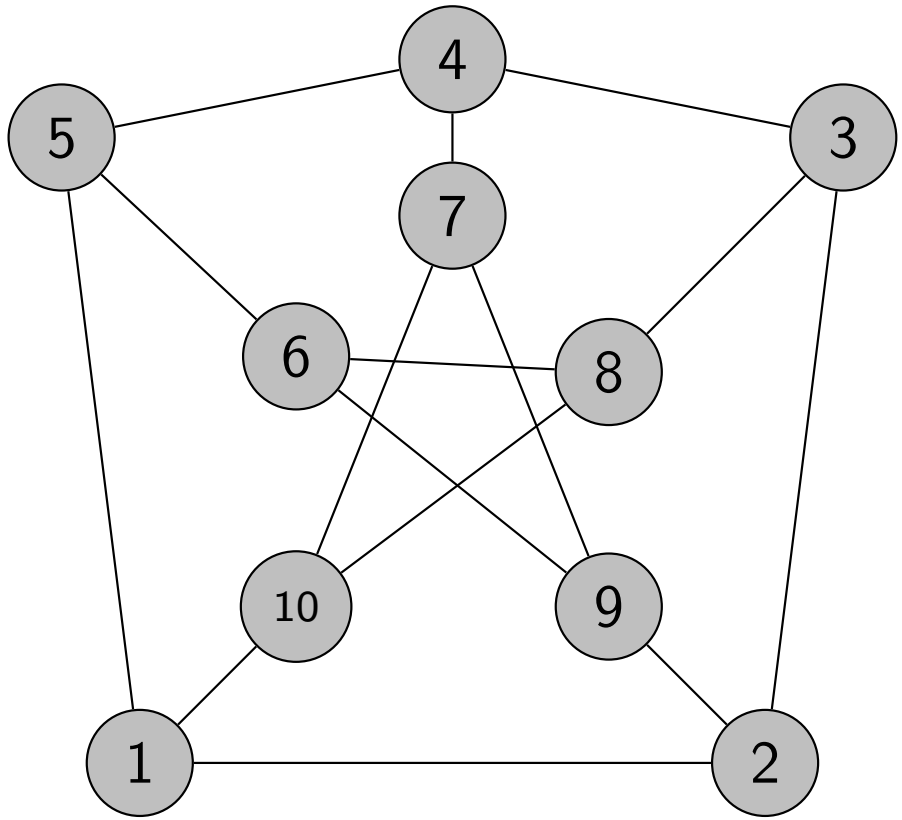
After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

$\overline{A} =$ "P knows the secret", then

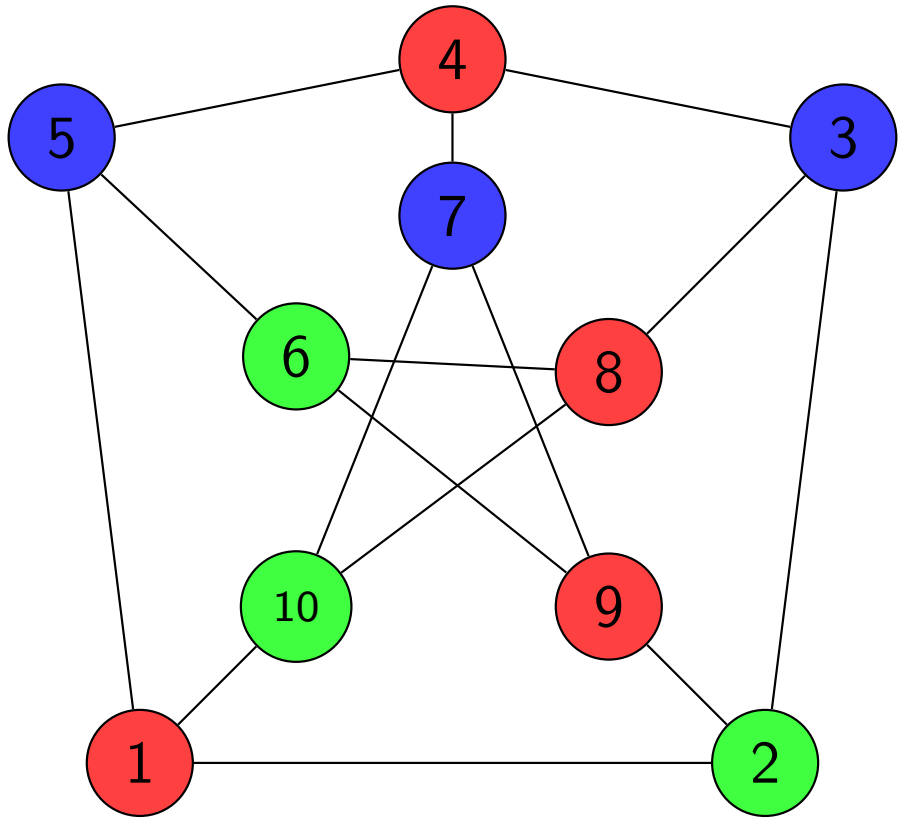
$$Pr[\overline{A}] = 1 - Pr[A] = 1 - (\frac{1}{2})^k$$

Graph 3-coloring is NP-complete: ● ● ●



Petersen graph

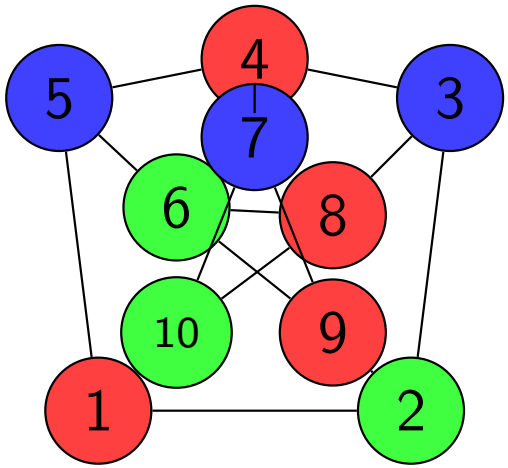
Graph 3-coloring is NP-complete: ● ● ●

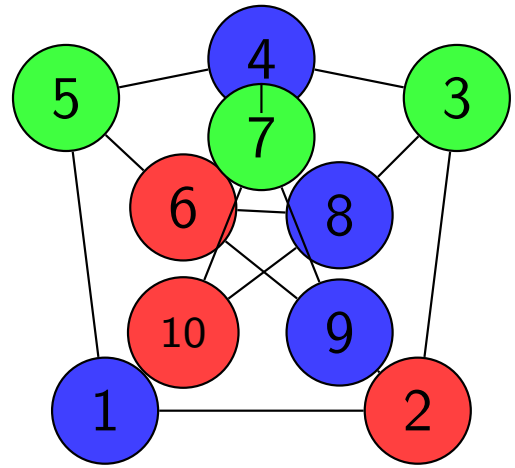


Petersen graph

P wants to prove to V his 3-coloring of $G = (E, V)$

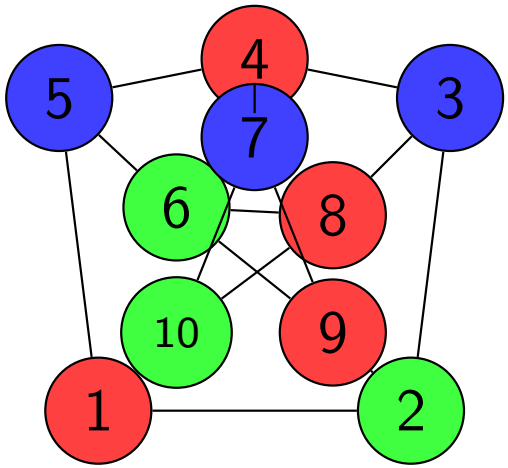
P selects a permutation π of the 3 colors.

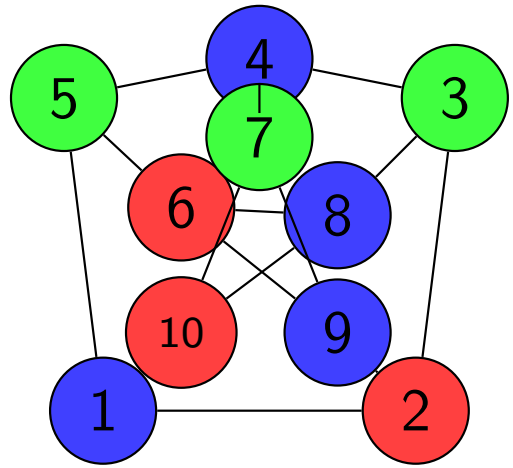
$\pi($ 

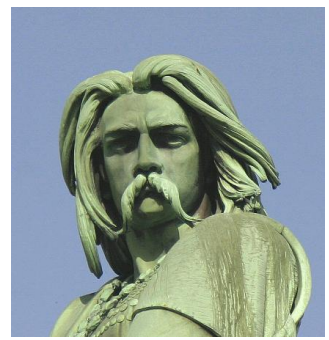
$)=$ 

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

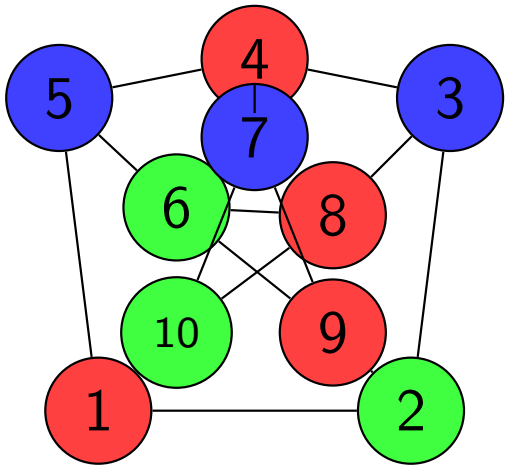


Chooses $\forall u \in V, r_u$

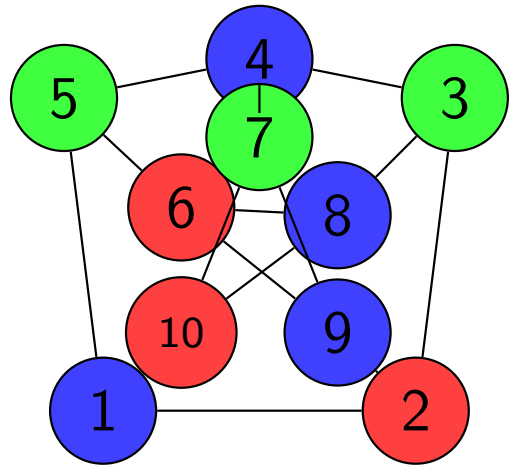
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

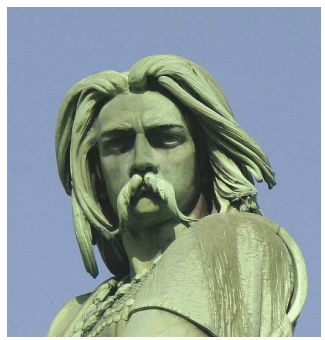
$\pi($



$)=$



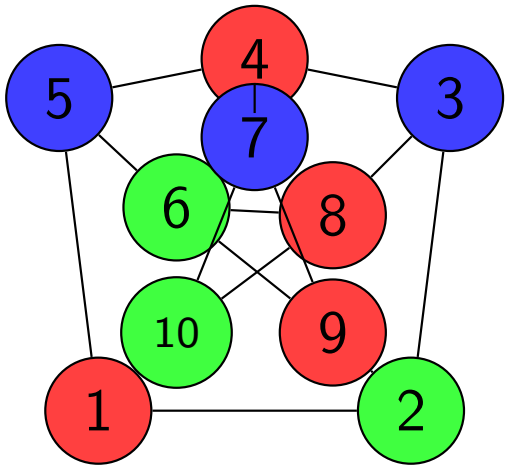
$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

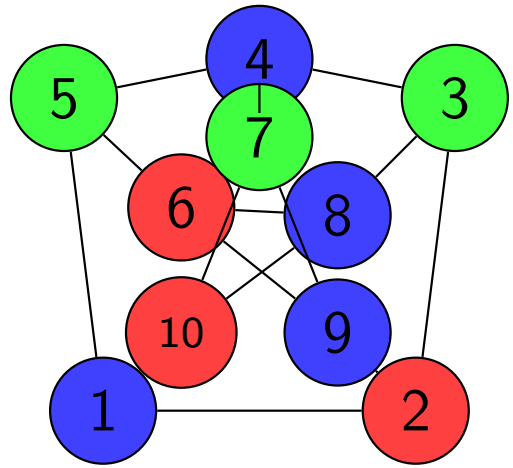


Chooses $\forall u \in V, r_u$

P wants to prove to V his 3-coloring of $G = (E, V)$

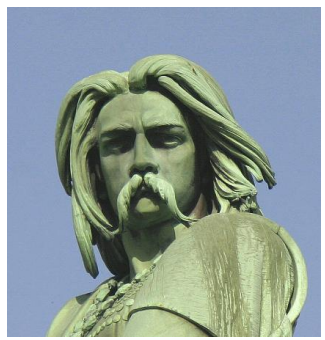
P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

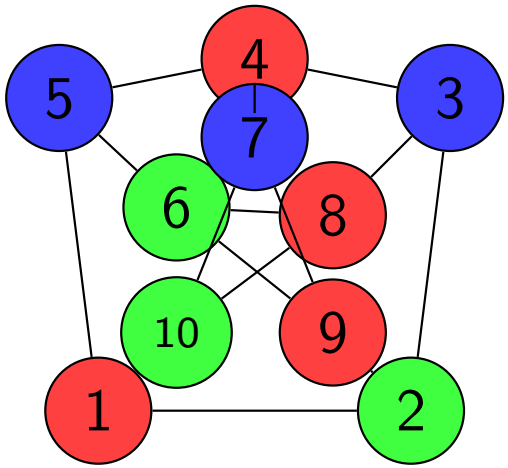
$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$

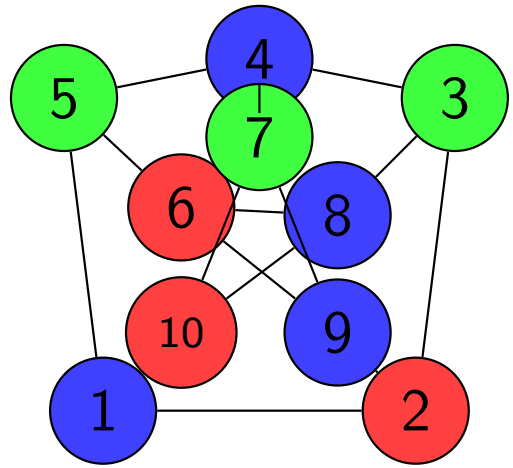


Chooses i and j

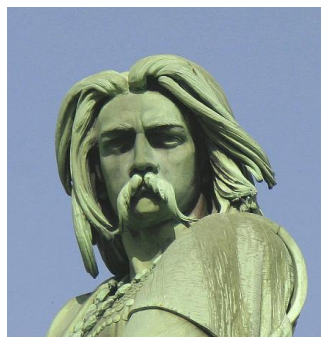
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$

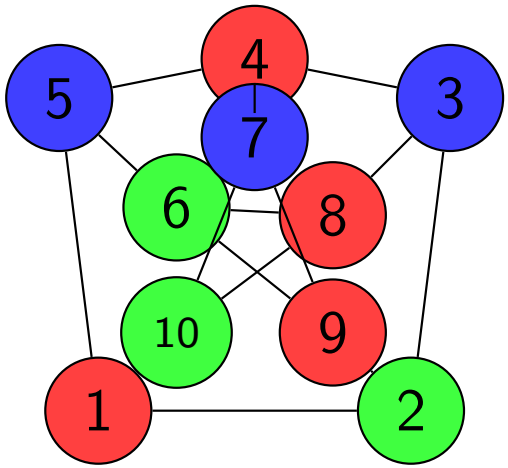


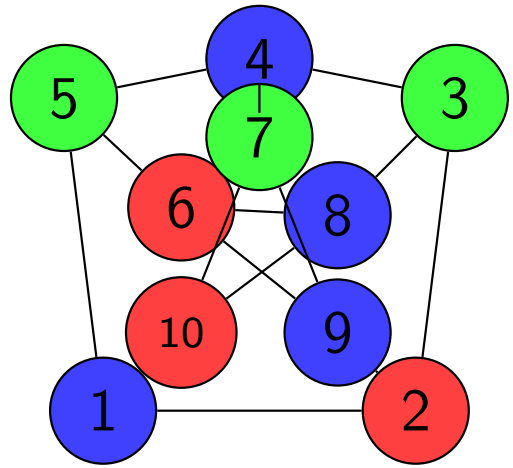
Chooses $\forall u \in V, r_u$

Chooses i and j

P wants to prove to V his 3-coloring of $G = (E, V)$

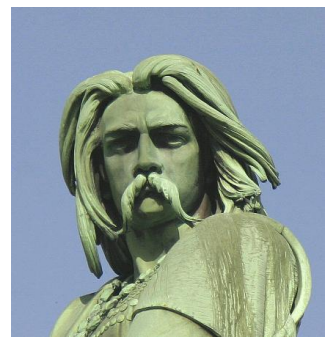
P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

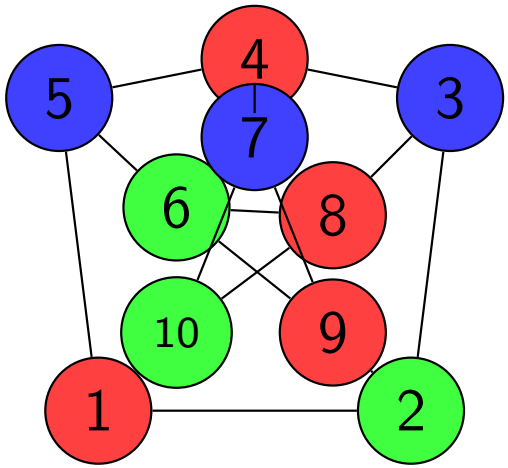
$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

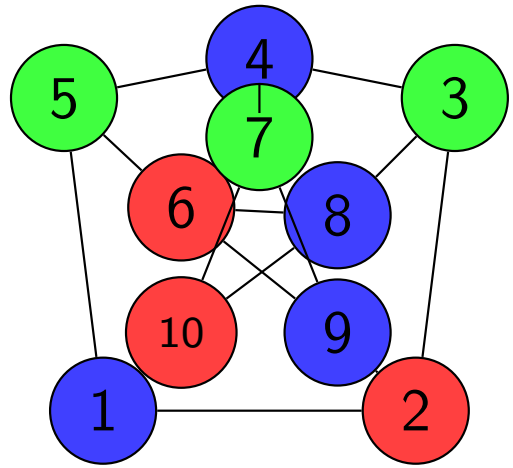


Chooses i and j

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

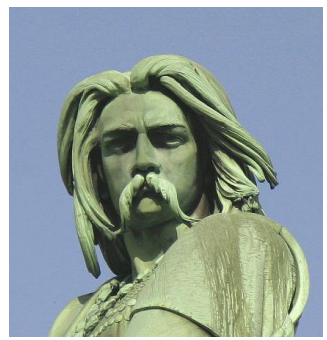
$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

V accepts, if $e_{u_i} = H(\pi(c(u_i))||r_{u_i})$ and $e_{u_j} = H(\pi(c(u_j))||r_{u_j})$



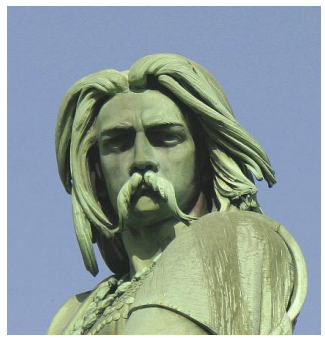
Chooses i and j

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

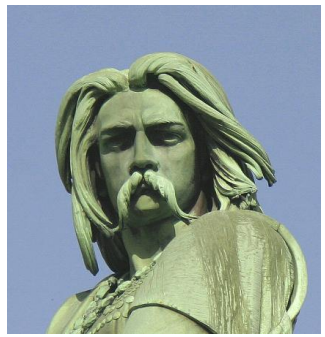


Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$



Chooses a random r

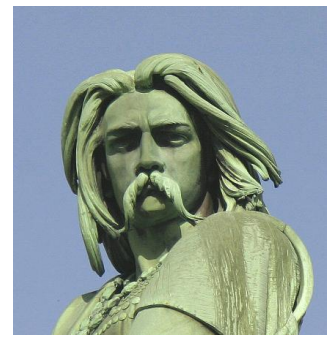
Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

$$\longrightarrow t = g^r \longrightarrow$$



Chooses a random r

Schnorr Protocol, 1991

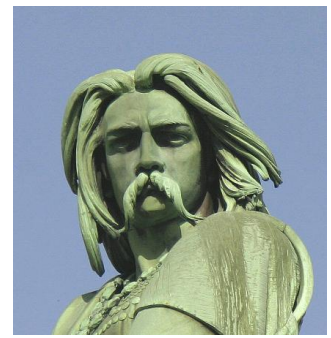
Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

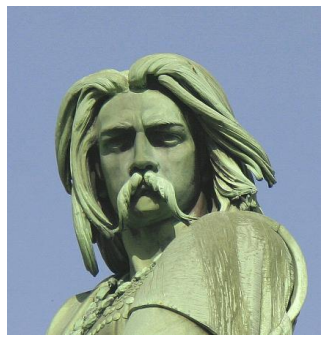
Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

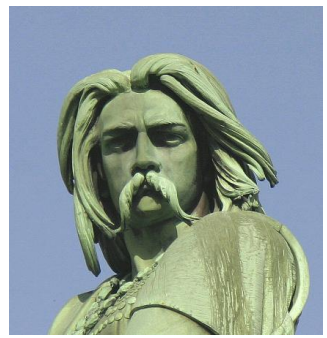
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

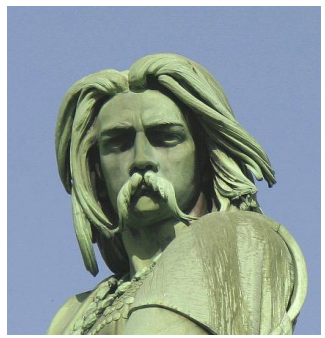
Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$

V accepts, if $t \cdot y^c = g^s$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

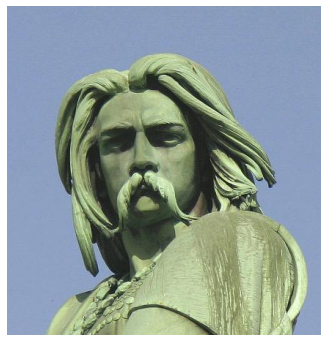
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

V accepts, if $t \cdot y^c = g^s$

$$t \cdot y^c = g^r \cdot (g^x)^c = g^{r+x \cdot c} = g^s$$

Outline

XSS : "Cross Site Scripting"

Principe : Injection de code HTML ou JavaScript dans des variables mal protégées

Exemple

Saisie dans un formulaire de type POST.

```
<script>alert('bonjour')</scrypt>
```

1. XSS reflected : Stolen data are sent to the attacker once
2. XSS permanent : Injection of piece of code on the server

```
<img src=''toto'' onerror=''injection bad script''  hidden
```

XSS : Contre mesures

Vérifier toutes les entrées, en php : `htmlspecialchars()`

Outline

Things to bring home

- Security should be done by experts!
- Security should be taken from the design and not after!



$$\textit{Protocol} + \textit{Properties} + \textit{Intruder} = \textit{Security}$$

Thank you for your attention.

Questions ?