Homologation ARJEL : Retour d'expérience

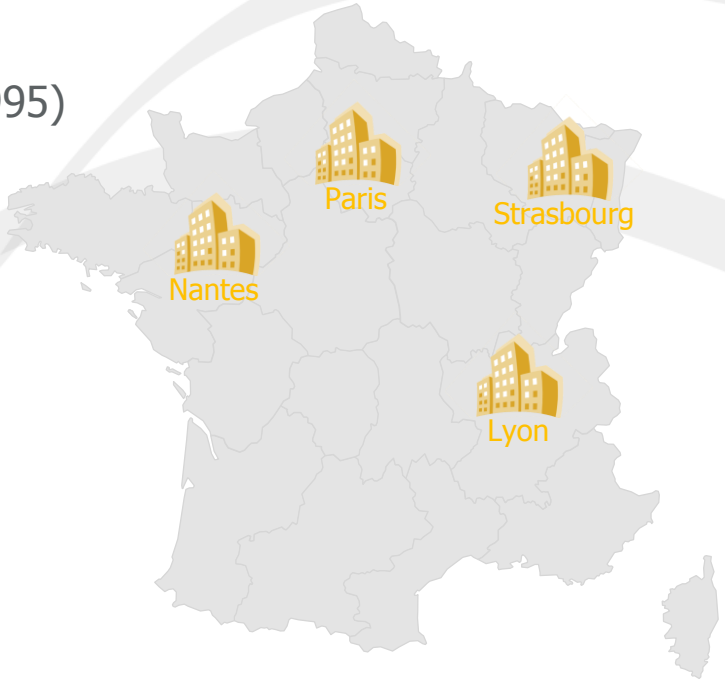
Ossir Paris / Juin 2013

Thibaud Binétruy – Consultant Sécurité
Thibaud.Binetruy@intrinsec.com

Intrinsec ? Petite présentation !

Intrinsec - Présentation

- Thibaud Binétruy
  - Consultant Sécurité
  - Travaille pour Intrinsec depuis 3 ans ½
  - Spécialisé en sécurité applicative
- Intrinsec : acteur historique de la sécurité des SI (1995)
  - Vieux briscard du pentest ☺
- Métiers
  - Hébergement & infogérance de SI
  - Sécurité de l'information ~30 personnes
  - Certificateur ARJEL depuis le 16/12/2010
- Réalisations ARJEL
  - Certifications
  - Homologations



Et l'ARJEL ? Qu'est ce que c'est ?

ARJEL – Définition / Présentation

- ARJEL : Autorité de Régulation des Jeux en Ligne
  - Concerne les paris sportifs, les paris hippiques et les jeux de cercle (Poker)

- Création en 2010
  - Ouverture du marché des jeux en ligne
  - LOI n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne

- 5 missions principales
  - Délivrer des agréments et s'assurer du respect des obligations par les opérateurs
  - Protéger les populations vulnérables, lutter contre l'addiction
  - S'assurer de la sécurité et de la sincérité des opérations de jeux
  - Lutter contre les sites illégaux
  - Lutter contre la fraude et le blanchiment d'argent

- Sélection de certificateurs agréés (16 déclarés officiellement) chargés de
  - Réaliser les certifications annuelles des opérateurs
  - Réaliser les homologations des logiciels de jeux

ARJEL – Définitions

- Capteur Frontal
  - Elément enregistrant toutes les actions des joueurs (inscription, paris, …)
  - Positionné en coupure entre le joueur et la plateforme de jeu
  - Chargé de vérifier les interdits de jeu en interrogeant un référentiel avec le protocole DNS
  - Enregistrement des événements au format XML suivant une grammaire spécifique
  - Stockage des données dans un coffre fort numérique accessible directement par l'ARJEL
  - Doit être développé par l'opérateur
- Coffre Fort
  - Entrepôt pour les traces des joueurs
  - Doit avoir obtenu une CSPN
- Logiciel de jeu
  - Application ou programme mis à disposition par l'opérateur aux utilisateurs afin d'interagir avec la plateforme de jeux
  - Peut être de type : client léger (Web), client lourd, mobile (Android, iOS…)
  - Tout nouveau logiciel doit être homologué
  - Toute modification importante doit entrainer une nouvelle homologation

Certification vs Homologation

Certification vs Homologation

- La première certification est réalisée à 6 mois
  - → Audit de configuration de la plateforme d'hébergement du frontal
  - → Test d'intrusion et audit de code du capteur
  - → Analyse de la conformité des traces stockées dans le coffre-fort
- Les certifications doivent ensuite être réalisées tous les ans
  - → Pour la 1ère certification (6 mois après) et uniquement pour celle-ci
    - ✓ Analyse du suivi des recommandations de la certification à 6 mois
  - → Pour les autres certifications
    - ✓ Audit de configuration / Audit de code « intrusif » sur le frontal
    - ✓ Analyse de la conformité des traces
    - ✓ Audit de configuration de la plateforme de jeu
    - ✓ Audit de code « intrusif » des applications présentes dans le périmètre
      - ○ Sauf des applications possédant une homologation
    - ✓ Audit financier et légal par un cabinet d'avocat et un cabinet de comptabilité
- En cas d' « oubli » l'opérateur peut perdre son agrément
  - → Ex: France-Pari-Sportif décision N°2012-06 du 16 avril 2013 de la Commission des sanctions

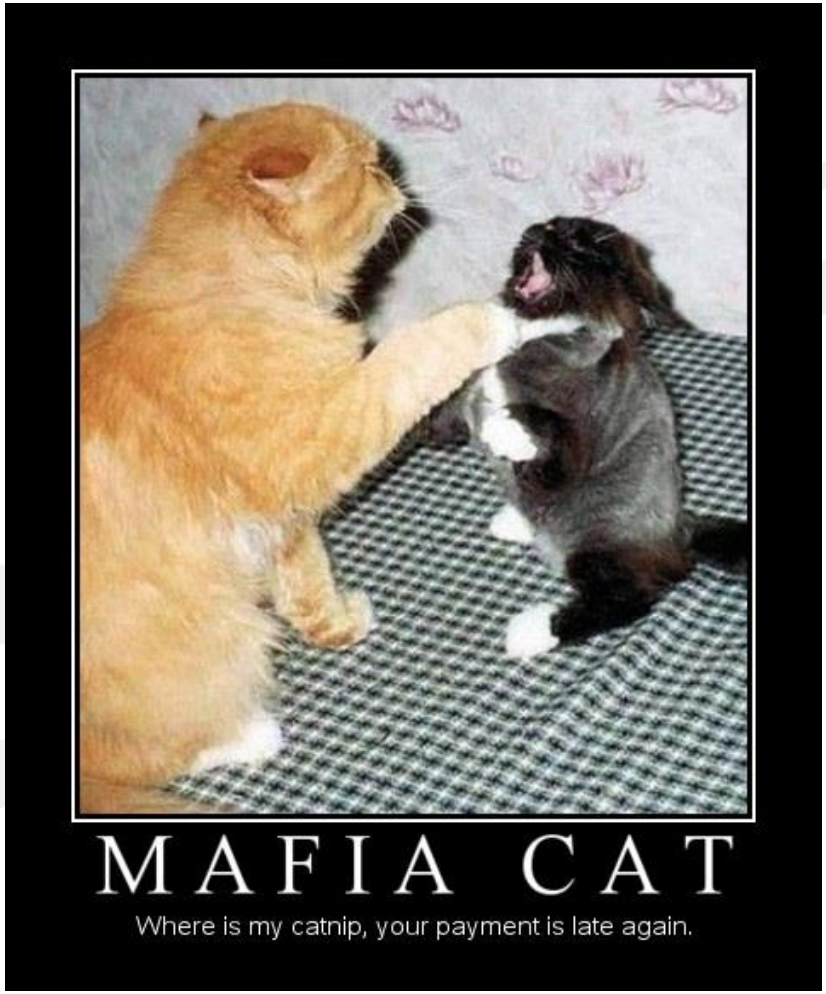
Certification vs Homologation

- Les homologations concernent tous les logiciels de jeu
- **Ce sont des prestations TECHNIQUES**
  - « Trop de rapports réalisés par des prestataires opportunistes »
- En cas de modification, l'ARJEL décide ou non de procéder à une nouvelle homologation
- Un logiciel de jeu spécifique à un support (tablette, mobile…) doit être considéré comme un nouveau logiciel de jeu
- D'après le DET:
  - « les vulnérabilités des logiciels de jeu détectées lors des différents audits des certifications annuelles devront impérativement être corrigées ou leur exploitation rendue impossible »
- Les actions à réaliser sont les suivantes
  - Un audit de code « intrusif » de l'application
  - Une analyse du PRNG si concerné
  - Une analyse de la bonne implémentation des règles de jeu si concerné (ex: Poker)

Certification vs Homologation

- Les logiciels de jeux doivent communiquer avec le frontal
  - → Pour enregistrer les événements de jeux des utilisateurs
  - → Pour assurer la gestion des interdits de jeux
- Les logiciels de jeux doivent afficher les messages de sensibilisation
  - → Pour rappeler aux joueurs que « jouer comporte des risques »
- Les logiciels de jeux doivent implémenter des limites de paris
  - → Pour éviter limiter les joueurs compulsifs
- Les logiciels de jeux ne doivent pas être vulnérables à des failles techniques

Dallas ton univers impitoyable



Dallas ton univers impitoyable

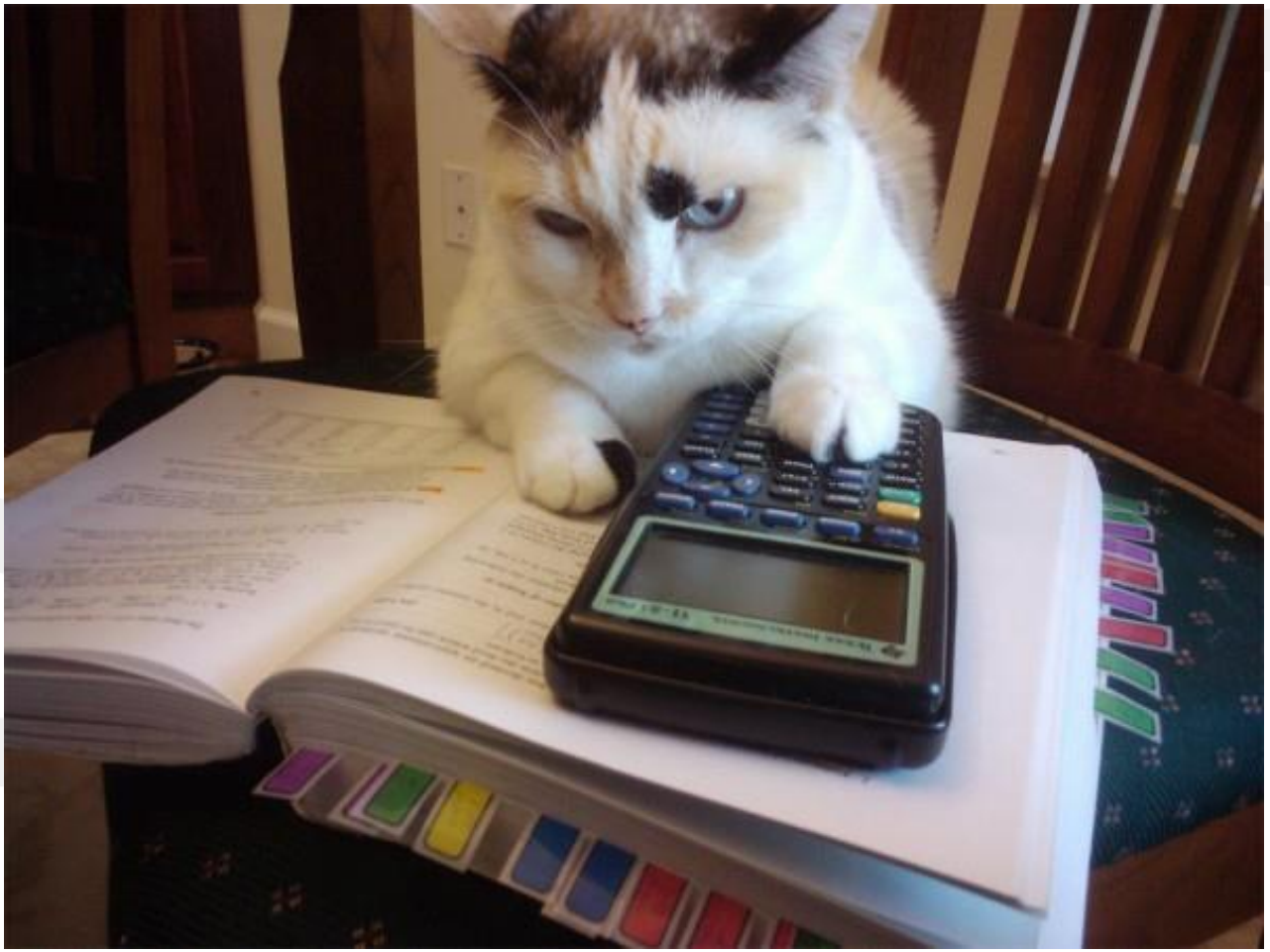
- Possibilité d'utiliser des logiciels de jeux développés par des prestataires étrangers
  - Exemple d'un prestataire dont les équipes sont basés dans des pays de l'Europe de l'Est
  - Difficulté afin d'accéder aux sources des applications (secret de fabrication, etc.)
  - Barrière de la langue
- « On les soupçonne d'être un peu trop dans l'univers gris du jeu »
- Les audits ARJEL sont imposés par la loi
  - Les opérateurs tentent souvent de négocier toutes les vulnérabilités identifiées
  - « Si je corrige vite on est obligé de le mentionner dans le rapport ? »
- Des clients qui refusent de payer si les livrables ne sont pas validés par l'ARJEL

Contraintes « légales »

Certification vs Homologation

- Intrinsec n'a jamais constaté de manquement aux contraintes de base
- Les logiciels de jeux communiquent correctement avec le frontal
  - → Les architectures sont conçues pour qu'il ne soit pas possible de faire autrement
- Les messages de sensibilisation sont toujours affichés sur les logiciels
  - → Permet de rassurer les utilisateurs en affichant le logo ARJEL
- Les logiciels de jeux implémentent tous les limitateurs
  - → Aucun défaut permettant de contourner ces limites n'a été constaté

Tests sur le PRNG



Tests sur le PRNG

- Ce qu'Intrinsec réalise actuellement
  - Génération d'un très grand nombre de « seeds » collectées à la sortie du PRNG
  - Utilisation de la suite DieHarder de Robert G. Brown sur ces « seeds »
  - Transformation des seeds en tas de cartes mélangés (réduction sur 52 cartes)
  - Analyse en utilisant l'algorithme X^2 (Khi carré)
- Analyse du code source de la transformation des « seeds »
  - Parfois difficile d'obtenir des captures du code
- « C'est bien mais pas suffisant » © Groland
  - L'ARJEL, soucieuse sur ce point là, ne se satisfait pas de ces tests
  - Khi^2 ne teste que l'équiprobabilité de la 1ere carte d'un tas mais pas la suite du tas
  - Mais pas d'autres solutions proposées par l'ARJEL…
  - Le certificateur doit proposer des tests lui même

Analyse des règles de jeu

Analyse des règles de jeu

- Concerne les applications de Poker

- Validation des règles de jeu énoncés dans les CGU
  - Analyse des CGU puis réalisation des tests sur l'application
  - Le consultant doit « jouer » au poker (peut paraitre fun mais…)
  - Difficulté pour recréer certains cas bien précis
    - ✓ Split des pots
    - ✓ Relance dite « invalide »
    - ✓ …

- Défauts principalement rencontrés
  - Pas de violation flagrante des règles de jeu
  - Bug d'affichage empêchant un jeu normal (les applications testées sont souvent non finies)
    - ✓ Cartes ne s'affichant pas correctement ou pas du tout…
    - ✓ Plantage en cours de jeu
    - ✓ …

Audit de code intrusif

Audit de code intrusif : possibilité de triche

- Vulnérabilité la plus critique identifiée par Intrinsec sur le backend d'une application mobile
  - Les web services, non modifiés depuis la dernière homologation, étaient hors scope
- Possibilité de triche
  - Possibilité de « rebuy » en tournoi de manière infinie
  - Facile de gagner à tous les coups en faisant tapis systématiquement
- Vulnérabilité « backend »
  - Deux web services: 1 pour les rebuy en « cash game » et 1 pour les rebuy en tournoi
  - Appel du mauvais web service lors des tournois
  - Défaut de vérification coté backend
- Défaut non identifié lors de l'homologation des web services
  - Comment l'a-t-on identifié ?

Audit de code intrusif : possibilité de triche

- Un peu comme ça ☺

Audit de code intrusif : SSL mon amour…

The Most Dangerous Code in the World:
Validating SSL Certificates in Non-Browser Software

Martin Georgiev
The University of Texas at Austin

Subodh Iyengar
Stanford University

Suman Jana
The University of Texas at Austin

Rishita Anubhai
Stanford University

Dan Boneh
Stanford University

Vitaly Shmatikov
The University of Texas at Austin

- Etude montrant que beaucoup d'applications mobiles ne valident jamais les certificats
  - → https://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- Les applications mobiles de jeux en ligne ne sont pas épargnées
- La totalité des applications mobiles auditées par Intrinsec étaient vulnérables
  - → Possibilité d'intercepter les flux à l'insu de l'utilisateur

Audit de code intrusif : SSL mon amour…1

- Première raison : l'utilisation de certificats auto-signés sur les environnements de recette
  - Implémentation d'un « bypass » des erreurs de certificat pour le développement
  - Oubli de cette implémentation lors de la livraison de l'application

```
//settings depended of HttpMehod. For now only GET setting there should be depend method
if (m_HttpMethod == MethodGet)
{
    curl_easy_setopt(m_Curl, CURLOPT_URL, m_Url);
    curl_easy_setopt(m_Curl, CURLOPT_WRITEFUNCTION, CRequest::GotData);
    curl_easy_setopt(m_Curl, CURLOPT_WRITEDATA, (void *)this);
    //curl_easy_setopt (m_Curl, CURLOPT_ERRORBUFFER, Error );
    curl_easy_setopt(m_Curl, CURLOPT_SSL_VERIFYPEER, 0L);
    curl_easy_setopt(m_Curl, CURLOPT_SSL_VERIFYHOST, 0L);
    curl_easy_setopt(m_Curl, CURLOPT_USERAGENT, "NetLibGet/1.0");   //not needed
    //curl_easy_setopt(m_Curl, CURLOPT_CONNECTTIMEOUT, 15);
    //curl_easy_setopt(m_Curl, CURLOPT_TIMEOUT, 30);
}

if (m_HttpMethod == MethodPost)
{
    curl_easy_setopt(m_Curl, CURLOPT_URL, m_Url);
    //curl_easy_setopt (m_Curl, CURLOPT_ERRORBUFFER, Error );
    curl_easy_setopt(m_Curl, CURLOPT_SSL_VERIFYPEER, 0L);
    curl_easy_setopt(m_Curl, CURLOPT_SSL_VERIFYHOST, 0L);
    curl_easy_setopt(m_Curl, CURLOPT_POSTFIELDS, p_Data);
    curl_easy_setopt(m_Curl, CURLOPT_POSTFIELDSIZE, p_DataLength);
    curl_easy_setopt(m_Curl, CURLOPT_POST, 1L);
    curl_easy_setopt(m_Curl, CURLOPT_USERAGENT, "NetLibPost/1.0");  //not needed
    curl_easy_setopt(m_Curl, CURLOPT_WRITEFUNCTION, CRequest::GotData);
    curl_easy_setopt(m_Curl, CURLOPT_WRITEDATA, (void *)this);
    //curl_easy_setopt(m_Curl, CURLOPT_CONNECTTIMEOUT, 15);
    //curl_easy_setopt(m_Curl, CURLOPT_TIMEOUT, 30);
}
```

Audit de code intrusif : SSL mon amour…2

- Deuxième raison : on recopie un bout de code trouvé sur le net…
  - Comment on gère le chiffrement SSL avec Apache HTTPClient ?
  - Regarde donc sur Stack Overflow ☺

```
public HttpClient getNewHttpClient(Context context) {

    try {

        KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
        trustStore.load(null, null);

        CustomSSLSocketFactory sf = new CustomSSLSocketFactory(trustStore);
        sf.setHostnameVerifier(SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);

        HttpParams params = new BasicHttpParams();
        HttpProtocolParams.setVersion(params, HttpVersion.HTTP_1_1);
        HttpProtocolParams.setContentCharset(params, HTTP.UTF_8);
        HttpProtocolParams.setUserAgent(params, getUserAgent(context, ""));

        SchemeRegistry registry = new SchemeRegistry();
        registry.register(new Scheme("http", PlainSocketFactory.getSocketFactory(), 80));
        registry.register(new Scheme("https", sf, 443));

        ClientConnectionManager ccm = new ThreadSafeClientConnManager(params, registry);

        HttpClient client = new DefaultHttpClient(ccm, params);
        addCustomHeaders(context, client);

        return client;

    } catch (Exception e) {

        return new DefaultHttpClient();

    }

}
```

Audit de code intrusif : SSL mon amour…3

- Troisième raison: utilisation d'une bibliothèque douteuse
  - → « La validation des certificats c'est useless surtout sur mobile » ☺

Audit de code intrusif : SSL mon amour…3

Audit de code intrusif : SSL mon amour…3

MugunthKumar commented — 5 months ago

I added a new property called shouldContinueWithInvalidCertificate
This is "NO" by default and MKNK will not accept invalid certs. Did this help?

Audit de code intrusif : SSL mon amour…3

- Validation des certificats pour le moins étrange…
  - Si le certificat est invalide soit l'utilisateur accepte le défaut et tout est envoyé normalement
  - Soit la requête est effectuée mais sans les « credentials » (authent HTTP != FORM)

```
self.serverTrust = challenge.protectionSpace.serverTrust;
SecTrustResultType result;
SecTrustEvaluate(self.serverTrust, &result);

if(result == kSecTrustResultProceed ||
   result == kSecTrustResultUnspecified || //The cert is valid, but user has not explicitly accepted/denied. Ok to proceed (Ch 15: iOS PTL :Pg 269)
   result == kSecTrustResultRecoverableTrustFailure //The cert is invalid, but is invalid because of name mismatch. Ok to proceed (Ch 15: iOS PTL :Pg 269)
   ) {

  [challenge.sender useCredential:[NSURLCredential credentialForTrust:challenge.protectionSpace.serverTrust] forAuthenticationChallenge:challenge];
}
else if(result == kSecTrustResultConfirm) {
    if(self.shouldContinueWithInvalidCertificate) {

    // Cert not trusted, but user is OK with that
    DLog(@"Certificate is not trusted, but self.shouldContinueWithInvalidCertificate is YES");
    [challenge.sender useCredential:[NSURLCredential credentialForTrust:challenge.protectionSpace.serverTrust] forAuthenticationChallenge:challenge];
  } else {

    DLog(@"Certificate is not trusted, continuing without credentials. Might result in 401 Unauthorized");
    [challenge.sender continueWithoutCredentialForAuthenticationChallenge:challenge];
  }
}
else {
  // invalid or revoked certificate
  if(self.shouldContinueWithInvalidCertificate) {
    DLog(@"Certificate is invalid, but self.shouldContinueWithInvalidCertificate is YES");
    [challenge.sender useCredential:[NSURLCredential credentialForTrust:challenge.protectionSpace.serverTrust] forAuthenticationChallenge:challenge];
  } else {
    DLog(@"Certificate is invalid, continuing without credentials. Might result in 401 Unauthorized");
    [challenge.sender continueWithoutCredentialForAuthenticationChallenge:challenge];
  }
}
```

Audit de code intrusif : SSL mon amour…3

tclayson commented — a month ago

Unfortunately this isn't working for me. Our SSL certificate has expired, however we are still about to communicate with our API using MKNetworkKit. Even manually setting [op setShouldContinueWithInvalidCertificate:NO] doesn't seem to work.

What am I doing wrong? How can I make sure it doesn't allow expired certificates?

Many thanks.

Closed

8 comments

Audit de code intrusif : « Aie confiance »

- Le paiement « in-app » au sein d'une WebView
  - L'utilisateur ne peut pas vérifier l'URL
  - L'utilisateur ne peut pas vérifier le certificat
  - Va à l'encontre de toutes les sensibilisations réalisées par les banques…

Audit de code intrusif : « Aie confiance »

- Problématique reconnue mais tolérée par l'ARJEL

Audit de code intrusif : les mots de passe ?

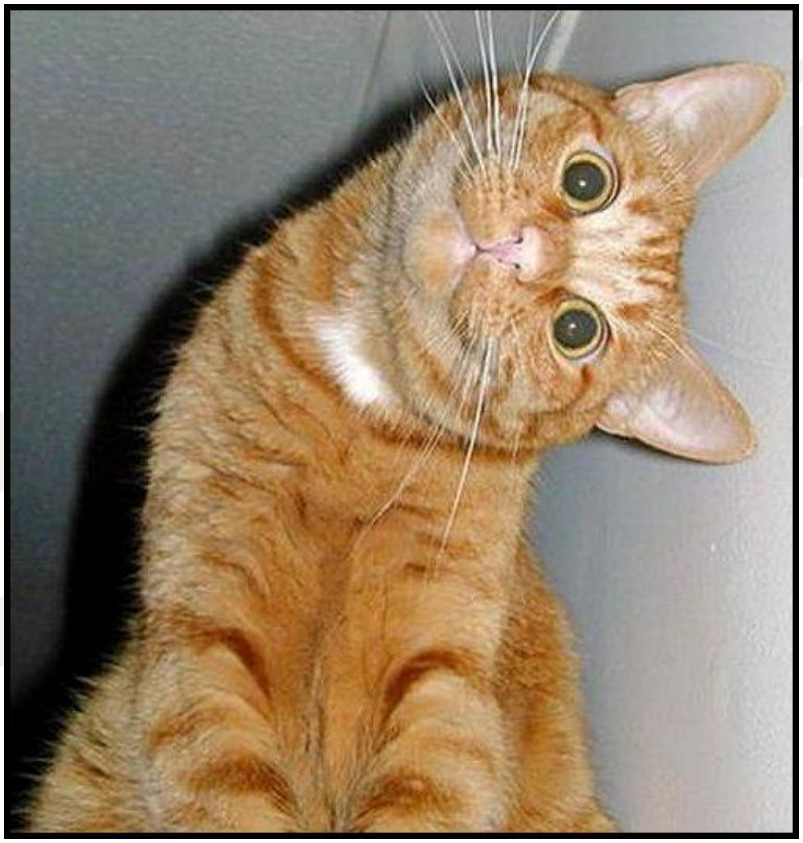
- « Les mots de passe c'est chiant à retenir » © Madame Michu
- Sur un secteur à forte concurrence on a tendance à prendre soin des clients
- On propose donc d'enregistrer les identifiants sur le terminal
- **Problème**: un mobile ça se vole facilement…

Audit de code intrusif : les mots de passe ?

- Question de l'auditeur chiant au développeur de l'application
  - « Comment vous stockez les mots de passe sur le terminal ? »

Audit de code intrusif : les mots de passe ?

- Réponse du développeur à l'auditeur chiant
  - « Boah, dans le truc standard où on stocke les machins des applications ! »
  - Intrinsec n'a jamais constaté de chiffrement des identifiants sur les terminaux mobiles…



Audit de code intrusif : les mots de passe ?

- Pas de « keychain » sur Android
  - Désactivation de la fonction de stockage des identifiants sur le terminal
  - Certains opérateurs appliquent cette recommandation
- iOS met à disposition un keychain chiffré avec une clé dérivée du PIN du terminal
  - Le keychain est difficile à utiliser, Apple met à disposition un « wrapper » pour l'utiliser
  - Wrapper non inclus dans la bibliothèque « CoreFoundation »
  - Peu utilisé par les développeurs…

Audit de code intrusif : les mots de passe ?

- Le stockage des identifiants de manière non « sécurisée » est toléré par l'ARJEL

Bonus

Bonus

- Les jeux d'argent et de hasard ne sont pas autorisés sur le Play Store Android

  - **Jeux d'argent et de hasard** : nous n'autorisons pas les contenus ou services qui visent à faciliter l'accès à des sites de jeux d'argent, notamment, et sans s'y limiter, les casinos en ligne, les sites de paris sportifs et les loteries.

- Est-ce que ça arrête les opérateurs ?

Non ☺

Android™ est une marque commerciale de Google Inc.

Bonus

- Cette problématique est également autorisée par l'ARJEL

Conclusion: « La sécurité est un échec ? » ©

Conclusion

- Les risques de fraude et de blanchiment d'argent sont plutôt limités
  - La traçabilité des actions utilisateur est plutôt dissuasive
  - Les audits permettent d'identifier les cas de triches possibles
  - L'ARJEL est pointilleuse concernant la validation du PRNG
- La protection des personnes vulnérables est plutôt bien gérée
  - L'ARJEL est très pointilleuse sur les interdits de jeux
  - Des messages de sensibilisation imposés dans les logiciels de jeu
- La sécurité informationnelle des utilisateurs est plutôt légère (pour le moment)
  - Toutes les vulnérabilités identifiées ne sont pas forcément corrigées
  - Difficulté pour tout faire appliquer d'un coup
  - La criticité des défauts de sécurité est revue chaque année par l'ARJEL
  - Nécessité de tenir compte des exigences des utilisateurs et des opérateurs

intrinsec
BUSINESS CONTINUITY AND SECURITY

Merci de votre attention
Questions ?