Cryptage de données moderne avec approfondissement dans l'industrie militaire

Le cryptage est le processus d'encodage d'un texte lisible en un code sécurisé. Il s'agit d'une technologie fondamentale pour sécuriser les informations contre l'accès extérieur.

Historiquement, il a été utilisé dans l'espionnage et en temps de guerre pour les communications sensibles (nous avons vu beaucoup d'exemples dans le fichier qu'on a dû lire)…

XVIe siècle **Le chiffre de Vigenère**

À partir du XIXe siècle, on utilise des machines mécaniques à cylindres de plus en plus complexes basées sur le principe de **substitution polyalphabétique** comme le chiffre de Vigenère. La plus connue de ces machines est la **machine Enigma,** utilisée par les Allemands durant la 2de guerre mondiale, et cassée par les Alliés.

Les informations personnelles, les données financières et les documents confidentiels partagés en ligne doivent être cryptés pour les protéger correctement contre la cybercriminalité.

Plusieurs types d'algorithmes de chiffrement existent pour différentes circonstances. Mais ça reste toujours que chaque algorithme nécessite un nombre spécifique de clés, déterminant le type de cryptage en place.

Une application de messagerie sécurisée garde vos conversations privées. Sauf si vous utilisez une application de messagerie non cryptée, vous laissez toutes les portes ouvertes.

Les applications de messagerie sécurisée utilisent **le chiffrement de bout-en-bout** pour sécuriser le transit des données depuis leur expéditeur vers leur destinataire. Comme d'habitude les données sont chiffrées à l'envoi et déchiffrées à leur arrivée. Au cours de la transmission, personne ne peut accéder à ces données.

Bien que le cryptage et la confidentialité jouent un rôle essentiel dans le choix de l'application de messagerie à utiliser, il est également nécessaire d'utiliser les applications de messagerie que nos amis utilisent. Ici, nous voyons des statistiques des utilisateurs actifs chaque mois . Selon Statista (2022), WeChat, WhatsApp et Facebook Messenger restent les applications de messagerie les plus populaires au monde. WeChat est utilisé par la majorité des gens en Chine, car les applications comme WhatsApp et Facebook Messenger sont bloquées.

Tableau

Problème –Telegram

Les serveurs de Telegram sont très différents. Malheureusement, ils stockent toutes les conversations et données les concernant (localisation géographique, fichiers, cookies, photos etc) sur leurs serveurs.

Le peuple ukrainien a été rapidement informé du contenu qui ne pouvait pas être affiché sur le réseau. …voir pp

Ces informations peuvent attirer des pirates informatiques ou des employés qui sont sous pression ou prêts à coopérer avec le gouvernement russe.

Les travailleurs des médias pouvaient seulement afficher des photos avec de la fumée là où il n'y avait pas de zone spécifique avant de recevoir l'information officielle

Cependant, il y a aussi eu la création de canaux où tout le monde pouvait signaler le déplacement des équipements russes.

Le **Signal** en Ukraine est bien connu pour ceux qui sont en communication avec l'armée ukrainienne ou qui sont proches de l'armée. Par exemple, pour les bénévoles qui livrent des médicaments et de la nourriture à la défense territoriale. Pour ceux qui érigent des barricades et envoient des photos à leurs amis avec les résultats. Ou aussi pour ceux qui sont dans les territoires occupés et ne veulent pas être trouvés par des soldats russes et être forcés de prendre un passeport et numéro de téléphone russe.

Signal est le gagnant pour les utilisateurs iOS et Android. Signal a créé un protocole de cryptage qui est maintenant reconnu comme le protocole d'application de messagerie le plus sécurisé disponible. Il offre tout ce dont la plupart des utilisateurs ont besoin – SMS, appels vidéo et vocaux, chats de groupe, partage de fichiers et messages disparus – sans bourrer l'application de publicités et de collecte de données utilisateur. Il s'agit également d'une plate-forme open source permettant à tout le monde de vérifier les vulnérabilités.

tableau

En Ukraine, il y a beaucoup de services numériques d'État que chaque Ukrainien utilise chaque jour.

L'objectif du ministère de la Transformation numérique était de créer une application qui permettrait à chaque Ukrainien de se sentir comme un citoyen du pays le plus progressive et le plus pratique au monde. De nos jours, un passeport électronique est un document légalement reconnu avec la même force juridique qu'une version papier et plastique. Et l'Ukraine a été le premier pays au monde à le faire.

Une semaine avant l'invasion à grande échelle la loi sur les services cloud a été adoptée. Il a permis de transférer officiellement des registres à l'étranger et de stocker des données. C'était une décision stratégique. Un missile russe a frappé l'un des principaux centres de données de Kiev au début de l'invasion. Bien sûr, ces services souffrent d'attaques de pirates informatiques tout le temps, mais ils n'ont jamais réussi.

Lorsque les chars russes sont entrés sur notre territoire, les Ukrainiens ont photographié l'équipement russe, les soldats, le mouvement des colonnes. On a commencé à avoir besoin d'un outil sécurisé pour la transmission sûre et rapide des informations à l'armée. Pendant 2 semaines, Ministère de la Transformation numérique de l'Ukraine a lancé le chatbot eEnemy. La principale différence par rapport aux autres bots est l'autorisation via l'application Diya. Pendant 10 mois de travail, le chatbot eEnemy est devenu un outil efficace de renseignement public. Un demi-million d'Ukrainiens l'ont utilisé.

De l'autre côté du front, des dizaines d'applications, des systèmes d'exploitation à usage militaire ont déjà été inventés. Tout comme dans la vie civile, les gens choisissent un programme en fonction de leurs goûts et de leurs besoins, de sorte que les militaires utilisent des programmes qui conviennent mieux à leurs tâches.

J'en ai présenté plusieurs, de petites notes à côté pour montrer le but du logiciel. tels que les cartes numériques, l'environnement tactique, l'orientation, les calculs pour le tir, le contrôle des subdivisions

Je souhaite d'aller en détail sur le système d'exploitation Kropyva (Orties) , car il est maintenant utilisé par 90% des artilleurs. Army SOS est l'une des principales organisations bénévoles qui aident le personnel militaire ukrainien pendant la guerre depuis 2014

En 2014, les militaires ont demandé aux volontaires des cartes papier ordinaires mais modernes. L'équipe de ArmySOS n'a pas imprimé de nouvelles cartes. Au lieu de cela, ils ont acheté des tablettes avec Google Maps, mais très rapidement, la fonctionnalité des cartes civiles sur les tablettes n'était pas suffisante pour les militaires. Ils ont demandé d'ajouter des mesures de distance, des calculs automatiques, etc. Les militaires ont vu que ce produit change simplement le cours de la guerre et la qualité de la guerre, alors ils

ont refusé les vêtements et les armures corporelles et ont demandé plus de tablettes. En 2017, le fonds a transféré l'Ortie à l'État gratuitement.

Mainetenant l'Ortie est une application de renseignement cartographique tournant sous Android permettant à une personne dotée d'un terminal, le plus souvent une tablette, de marquer aisément une position ennemie. Le logiciel transmet ensuite l'indication aux pièces d'artillerie à proximité tout en permettant la coordination de leurs feux.

Dans l'Ortie, il est utilisé des stations de radio numériques à ondes courtes et très haute fréquence compatibles avec la norme OTAN. Il est également possible d'utiliser d'autres canaux de communication utilisant la technologie IP (satellite, fibre optique, etc.)

- Pourquoi pas les satellites? - Les documents militaires américains disent : "La première priorité est la communication à ondes courtes, satellite - priorité numéro deux."

L'origine volontaire des programmes ne signifie pas open source. Les développeurs de toutes les applications assurent qu'il n'est pas facile d'accéder au logiciel. "Même si quelqu'un télécharge un fichier, le déploie sur une tablette, tout ce qu'il peut faire est de nous laisser tomber la demande" "Il n'y a même pas deux facteurs, mais une authentification multifactorielle." Presque toutes les applications ont décentralisé le stockage de l'information. "Il n'y a pas de la ligne de front entière dans une tablette. Chaque unité voit les données de son site. Par conséquent, même la capture de l'appareil par l'ennemi n'est pas critique.

La Russie possède également ses propres drones, satellites et espions. Mais l'image de la guerre montre que cela ne suffit pas, alors les plans pour capturer l'Ukraine en quelques jours, détruire la défense aérienne et d'autres ont échoué.