V1.1 06 Nov 2020
CYBERSECURITY SERIES

Le long arc de l'histoire de la cybersécurité et INTERnet

Anthony M. Rutkowski, <mailto:trutkowski@netmagic.com>

le résumé

L'auteur décrit le long arc de l'histoire des internets, de la cybersécurité et de la manière dont ils ont été liés au fil des décennies à mesure que la technologie et les déploiements ont évolué.

La façon dont l'Agence de sécurité nationale a commencé à identifier les défis émergents en matière de cybersécurité à partir de la fin des années 1960, alors que la nouvelle technologie Internet commençait à émerger et à évoluer de manière inattendue, a été traitée en profondeur.

Les calendriers entrelacés au cours des cinquante prochaines années sont explorés à mesure que les nouvelles technologies et déploiements Internet évoluent, et que la NSA a dû répondre aux besoins de cybersécurité pour authentifier, protéger et analyser les informations et les services dont nous dépendons tous..

Les bases

- Qu'est-ce que la cybersécurité?
  - L’authentification, la protection et l’analyse des informations
    - au repos, ou
    - en mouvement, ou
    - qui générent plus d'informations
- Qu'est-ce qu'INTERnet?
  - Le déplacement des messages d'information
    - d'une source vers une ou plusieurs destinations
  - à travers différents supports de communication interconnectés
    - ces dernières années, le terme est devenu presque vide de sens

À partir du début de l'arc

- Les bases sont restées les mêmes depuis que les gens ont décidé de communiquer
- Les premiers paquets de communication étaient des humains, puis des objets physiques (par exemple, des lettres), puis visuels (sémaphore) puis des objets électroniques
- Le chiffrement a été utilisé très tôt pour
  - Authentifier et
  - protéger les messages
- Les premiers internets de réseau numérique avec cryptage ont vu le jour dans les années 1840 (télégraphe électrique)
- Le changement le plus important était la radio en tant que média à la fin des années 1890
- Le président Grover Cleveland a géré Internet par radio depuis la Maison Blanche à la fin de 1898 pour communiquer avec les ambassades américaines à l'étranger et recueillir des renseignements.
- Les internets radio ont considérablement amélioré le développement et l'utilisation des technologies de cryptage
- L'interception et le décryptage des messages par la France ont gagné la Première Guerre mondiale et favorisé l'origine de l'Agence nationale de sécurité
- L'histoire s'est répétée au Royaume-Uni pendant la Seconde Guerre mondiale
  - Turing et l'ordinateur Colossus ont montré l'avenir

Le long de l'arc

- Les satellites géostationnaires ont mis à l'échelle les internets mondiaux dans les années 1960
- L'idée de Baran et Davies d'utiliser des ordinateurs pour créer et acheminer des paquets numériques a changé la technologie de transport des communications dans les années 1960 et construite par Larry Roberts sous le nom d'ARPANET
- Le potentiel pour les réseaux de paquets de créer de nouvelles vulnérabilités a abouti à une initiative de sensibilisation à la cybersécurité par la NSA en 1969
- Peggy Karp du MITRE développe un protocole de nommage d'hôte réseau en 1971
- Pouzin en France en 1971 décrit l'utilisation de "datagrammes" sur des réseaux "sans connexion" - lancement du concept de base des internets contemporains
- De multiples initiatives pour différents «protocoles Internet» commencent à progresser dans les années 70 et 80
  - Metcalfe au MIT a décrit le protocole Ethernet de réseau local en 1973 basé sur le protocole satellite ALOHAnet
  - Kahn de la DARPA a décrit le protocole Internet d'hôte à hôte en 1974 (TCP / IP)
  - Bell-Labs a publié le protocole Internet UUCP en 1979
  - Fuchs à Princeton a développé Internet basé sur IBM nommé BITNET en 1981

Evolution

  - Marque déposée du consortium bancaire pour son Internet pour les distributeurs automatiques de billets
  - Bell-labs a développé le protocole Internet téléphonique (SS7) dans les années 1980 pour la signalisation et la messagerie (SMS)
  - NCS et DOD ont développé le protocole Internet OSI mondial (CLNP) dans les années 1980
  - GSM a développé des protocoles Internet mobiles mondiaux dans les années 1980-90
- L'intégration à très grande échelle (VLSI) a réduit la taille des ordinateurs tandis que la technologie de fibre optique a augmenté la bande passante de communication (loi de Robert)
- La NSA a lancé publiquement une initiative révolutionnaire de cybersécurité sur Internet en 1986 connue sous le nom de Secure Data Network System (SDNS) et comprenait une suite de protocoles Internet sécurisés.
- Morris Worm a causé la première interruption massive d'Internet pendant trois jours en novembre 1988
- Un traité international sur Internet a été conclu à Melbourne, en décembre 1988, avec des dispositions en matière de cybersécurité

Défis et changement

- Les interfaces utilisateur graphiques ont été popularisées en tant que navigateurs Web et ont conduit à une utilisation publique et professionnelle
- Les internets ont convergé au milieu des années 1990 sur les protocoles Kahn et GSM
- La convergence + les réseaux ouverts ont abouti à l'Internet des objets (IoT)
- Tout ce qui est connecté au réseau devient vulnérable aux attaques
- La Convention sur la cybercriminalité est approuvée en 2001
- Les téléphones portables et les ordinateurs ont convergé dans les années 2000
- La NSA et le CIS ont développé de nouveaux outils de cyberdéfense dans les années 2000
- Les réseaux ouverts ont créé des cybermenaces persistantes dans le monde dans les années 2010
- Une bande passante massive + une connectivité Internet + une intégration informatique ont abouti à des architectures de centre de données dans le cloud à la fin des années 2010

Opportunité et chaos au bout de l'Arc

- Le décor est planté pour une virtualisation extraterritoriale rapide et dynamique d'Internet et des ressources à la demande dans le monde entier (5G / F5F / S5G / NFV / SDN / MEC)
- Les sources de communication, les architectures et les terminaux sont de plus en plus dynamiques
- Un cryptage rapide, omniprésent et bon marché cache tout et diminue la confiance
- L'intelligence artificielle (IA) et les réalités alternatives créent à la fois des opportunités et des menaces
- Le piratage informatique augmente
- Les contrôles de sécurité critiques évoluent
- Les cyberattaques basées sur le contenu créent des menaces et des dilemmes économiques, politiques et sociétaux
- Les besoins de cyberdéfense produisent une virtualisation holistique d'Internet
- L'informatique quantique reste une perturbation potentiellement majeure

Lectures complémentaires

- https://www.nsa.gov/about/cryptologic-heritage/museum/
- https://www.bletchleypark.org.uk/
- https://www.arcsi.fr/
- https://www.deutsches-museum.de/en/exhibitions/communication/computers/cryptology/
- https://www.sciencemuseum.org.uk/what-was-on/top-secret
- https://hackaday.com/2017/03/02/great-hacks-of-history-the-marconi-radio-hack-1903/
- https://en.wikipedia.org/wiki/Colossus_computer; https://www.tnmoc.org/
- https://en.wikipedia.org/wiki/Louis_Pouzin
- https://en.wikipedia.org/wiki/Paul_Baran
- https://en.wikipedia.org/wiki/GSM#History
- http://www.circleid.com/posts/20200415-a-short-history-of-internet-protocol-intellectual-property/
- http://www.circleid.com/posts/20190715_the_untold_history_of_the_first_cyber_moonshot/
- https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/
- https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824,856#/
- https://www.cisecurity.org/controls/cis-controls-list/