HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

OSSIR

Compte rendu 29C3

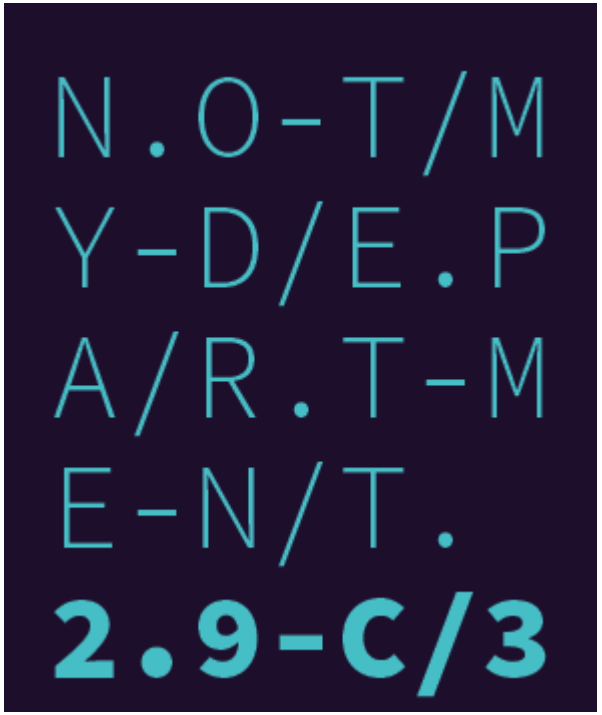
Hambourg – du 27 au 30 décembre 2012

- Mardi 8 janvier 2013 -

Steeve Barbeau <Steeve.Barbeau@hsc.fr>
Jérémy Rubert <Jeremy.Rubert@hsc.fr>

Chaos Communication Congress 2012

- 29ème édition du CCC
  - « *Not my departement* »
- Chiffres
  - 6600 participants
  - 4 jours (27 au 30 décembre)
  - 3 salles + *streaming*
  - 93 conférences + 3 *ligthning talk*
  - 60 % des conférences en anglais, 40 % en allemand
- Congress Center Hambourg
  - Couverture wifi sur l'ensemble du site
  - Présence d'un réseau GSM dédié



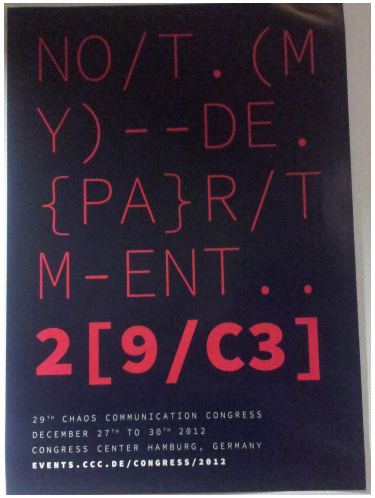
Chaos Communication Congress 2012

- Stands présents
  - Électronique (led, quadcoptère, robots, arduino)
  - Crochetage de serrure
  - Jeux vidéos vintages
- Sur place
  - Très bonne ambiance
  - Profils humains très variés
  - Beaucoup de jeux de lumières
  - Possibilité de restauration sur place
  - Organisation très « allemande »

Keynote : Not my departement
Jacob Appelbaum

- Introduction par une vidéo de la construction d'un centre informatique pour la NSA (UTAH) destiné à l'interception des communications

- Plusieurs thèmes abordés
  - Respect de la vie privée
  - Liberté numérique => perte des démocraties à travers le monde
  - Hacktivisme
  - Logiciel libre



- Recommandations de Jacob
  - Implication dans le domaine du libre
  - Ne pas travailler pour des technologies telles que la DPI

ISP Black blox
Luka Perkov

- Comment un FAI peut gérer de nombreux CPE (*Customer Premises Equipement*) ?
- Fonctionnement du protocole CWMP (*CPE WAN Management Protocol*)
  - Gestion de la configuration des CPE depuis un ACS (*Auto Configuration Server*)
  - Bidirectionnel SOAP/HTTP
  - Communique en XML
  - Utilisation d'objets (*Device.ManagementServer.password*)
- Quatre outils permettant d'analyser et de simuler cette gestion
  - libfreecwmp, freecwmp, mod_cwmp (nginx proxy), freeacs-ng
  - Développés pour openWrt

Setting mobile phones free
Mark van Cuijk

- Projet Limesco (2 ans, 3 fondateurs)
  - Opérateur téléphonique hollandais se revendiquant libre
- Présentation des différents acteurs du monde téléphoniques
  - MNO (*Mobile Network Operator*) -> gestion des antennes
  - MVNO (*Mobile Virtual Network Operator*) -> marketing et relation clients
  - MVNE (*Mobile Virtual Network Enable*) -> architecture pour les MVNO
  - Aperçu de leurs modèles économiques
- Présentation des équipements réseaux
- Deux offres Limesco
  - Offre téléphonie classique
  - Offre technophile -> utilisation d'un serveur SIP privé connecté à Limesco

Re-igniting the Crypto Wars on the Web
Harry Halpin

- Javascript obligatoire au sein d'un navigateur
  - Nécessaire pour de nombreux sites
- Plugins non recommandés pour cet usage
  - Vulnérabilités fréquentes
- Usages
  - Authentification multi-facteur
  - Signature de documents
  - Chiffrement de documents, communications ...
- Besoin d'une API web de cryptographie qui répond aux mêmes besoins que PGP

Privacy and the Car of the Future
Christie Dudley

- DSRC (*Digital Short Range Communication*)
  - Communication de véhicule à véhicule
  - Communication de véhicule à infrastructure
  - Distance ~ 380m
  - But -> réduction du nombre d'accidents
  - 5.9Ghz réservé pour l'Europe et les États-Unis -> IEEE 802.11p

- Problèmes
  - Envoie des messages en diffusion à tous -> atteinte à la vie privée + possibilité de traçage d'une voiture
  - Pas encore de méthodes pour délivrer des certificats servant à signer les messages
  - Coupler des caméras sur les routes avec ce système pour la répression des conducteurs

The Ethics of Activist DDOS Actions
Molly Sauter

- Critiques des DDOS
- Les DDOS ne sont pas illégaux partout
- Exemples
  - IGC/Euskal Herria Journal (1997)
  - EDT/Lufthansa (2001)
  - etoy/toywar (1999)
- Types d'attaques
  - Manuelles / automatiques
  - Automatiques -> botnet d'ordinateurs volontaires / botnet d'ordinateurs infectés à leur insu
- La méthode utilisée pour faire passer un message contredit souvent celui-ci

Hacking Cisco phones
Ang Cui & Michael Costello

- Ils ont présenté l'an dernier l'exploitation d'imprimantes HP
- Les serveurs sont protégés par des pare-feux, mais on peut passer par les imprimantes ou les téléphones

- Les téléphones CISCO sont partout -> hôpitaux, bureau d'Obama, Airforce One, département de la défense, etc.
- Protections
  - Logiciels signés
  - Chiffrement certifié FIPS
  - Système d'exploitation sécurisé
  - Surface d'attaque minimale
  - Java !

Name	Date Modified	Size	Kind
CuiCostelloStolfo_29c3	Today 8:53 AM	1.92 GB	Microsoft PowerPoint presentation

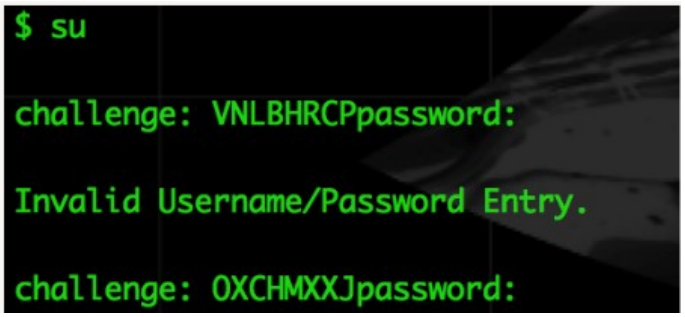
Hacking Cisco phones
Ang Cui & Michael Costello

- Caractéristiques
  - Sommes de contrôles partout
  - Système type UNIX
  - Séparation des processus
  - Isolation de la mémoire
  - Espaces mémoires non inscriptibles et non exécutables
  - Seul le processus d'initialisation s’exécute en tant que root

- Faiblesses
  - Vérification des signatures et des sommes de contrôle uniquement au démarrage
  - Une fois démarré, on peut modifier le code !

Hacking Cisco phones
Ang Cui & Michael Costello

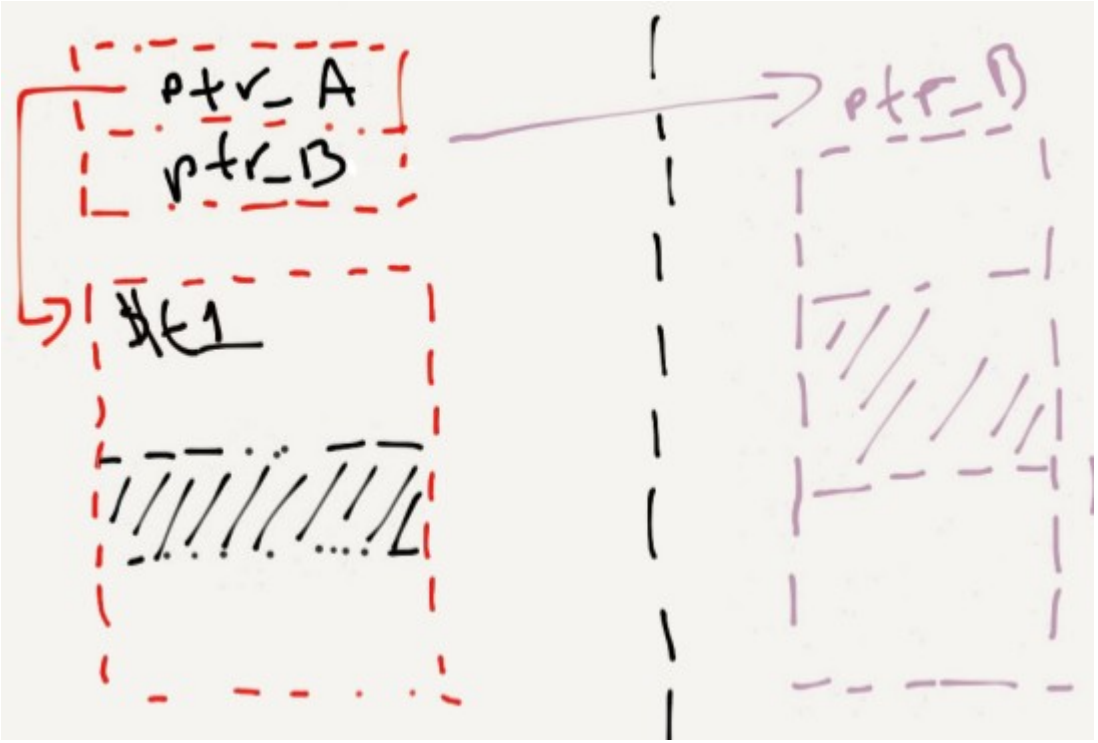
- Scénarios d'attaque
  - Root via SU
    - Utilisation des identifiants par défaut
    - Présence d'un mécanisme de challenge / réponse

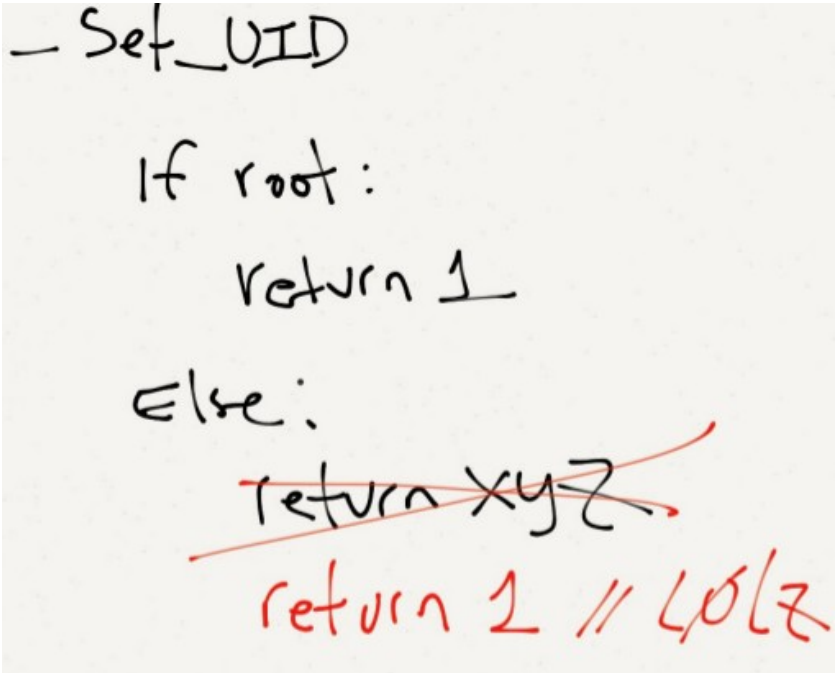


  - Utilisation d'IDA pour casser le mécanisme de challenge / réponse
    - Mécanisme cassé
    - Ne fonctionne quand même pas -> mécanisme différent d'un UNIX classique
  - Utilisation d'un *fuzzer* d'appels systèmes
    - Génération des appels depuis un ordinateur distant puis transmission au téléphone via SSH qui va effectuer les appels systèmes
    - Beaucoup de paniques noyaux !
    - 364 entrées d'appels systèmes -> 173 appels systèmes implémentés -> 60 erreurs triviales !

Hacking Cisco phones
Ang Cui & Michael Costello

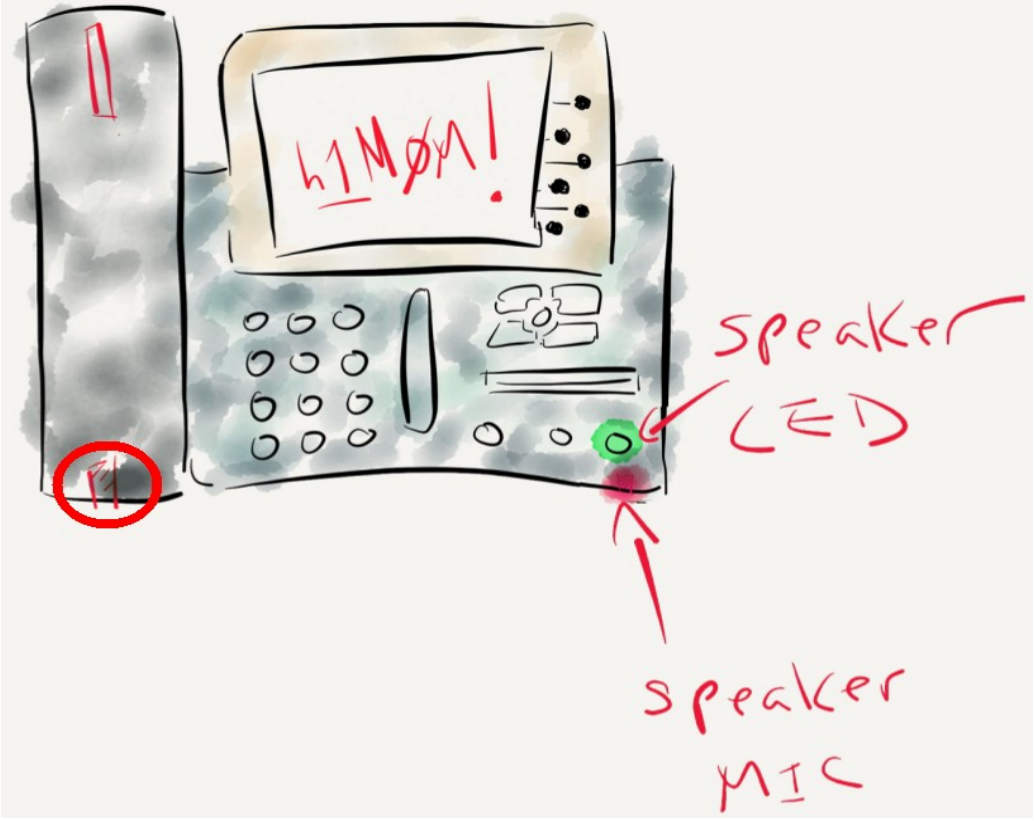
- La vulnérabilité exploitée
  - Lors d'un appel système, celui-ci copie les données de A vers B représenté dans une structure par des pointeurs
  - Fail -> l'adresse pointée par B n'est pas vérifiée !!
  - Exploitation -> faire pointer B vers une adresse dans le noyau

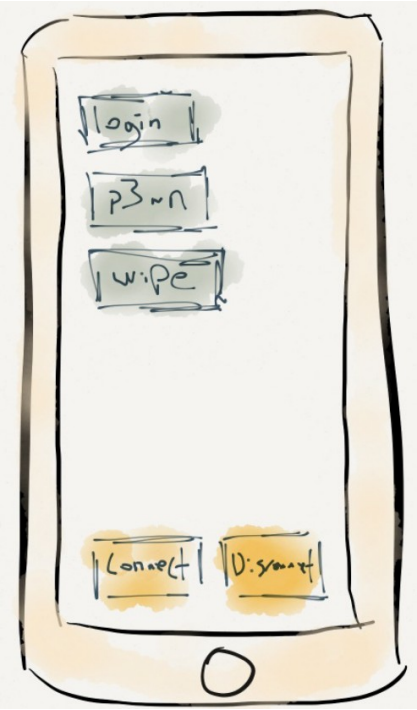




Hacking Cisco phones
Ang Cui & Michael Costello

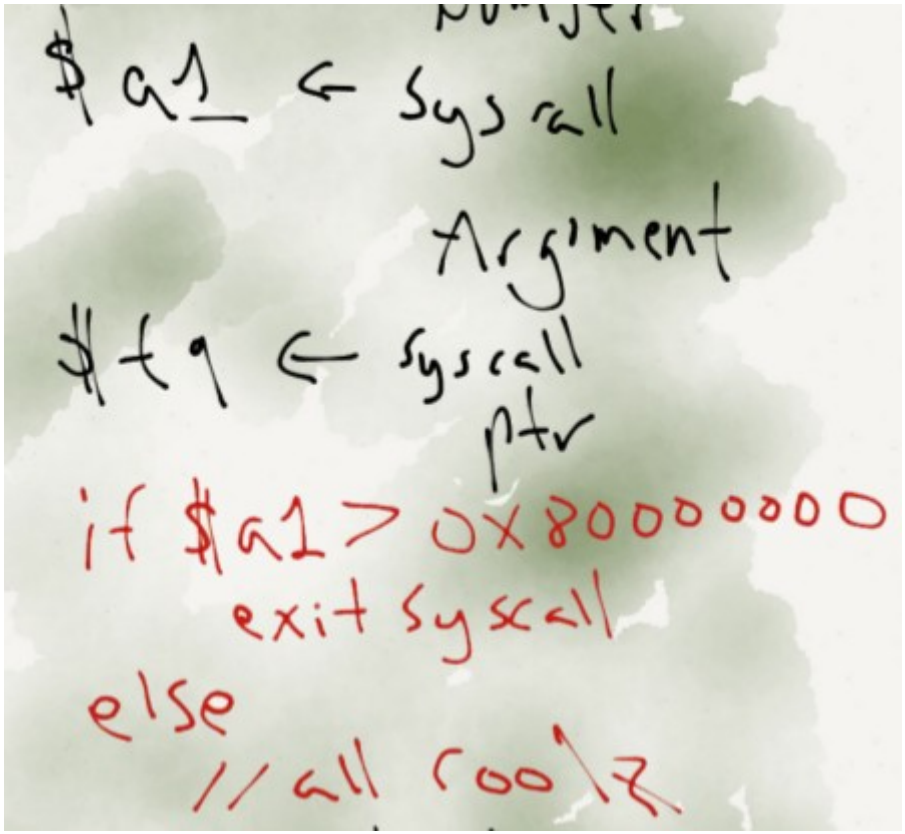
- Démonstration
  - Connexion d'un module Bluetooth au téléphone
  - Activation de la vulnérabilité depuis un téléphone portable
  - Retransmission des conversations avoisinantes sous forme textuel

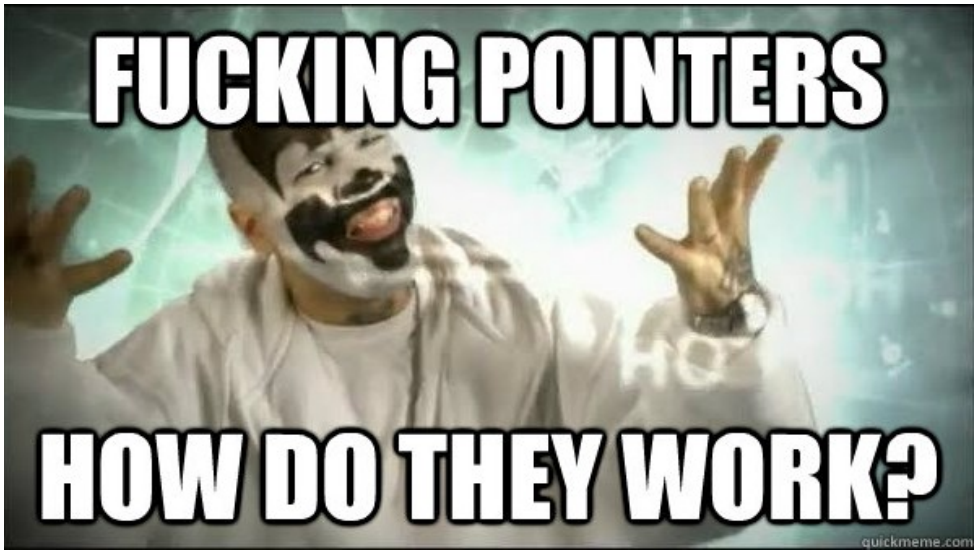




Hacking Cisco phones
Ang Cui & Michael Costello

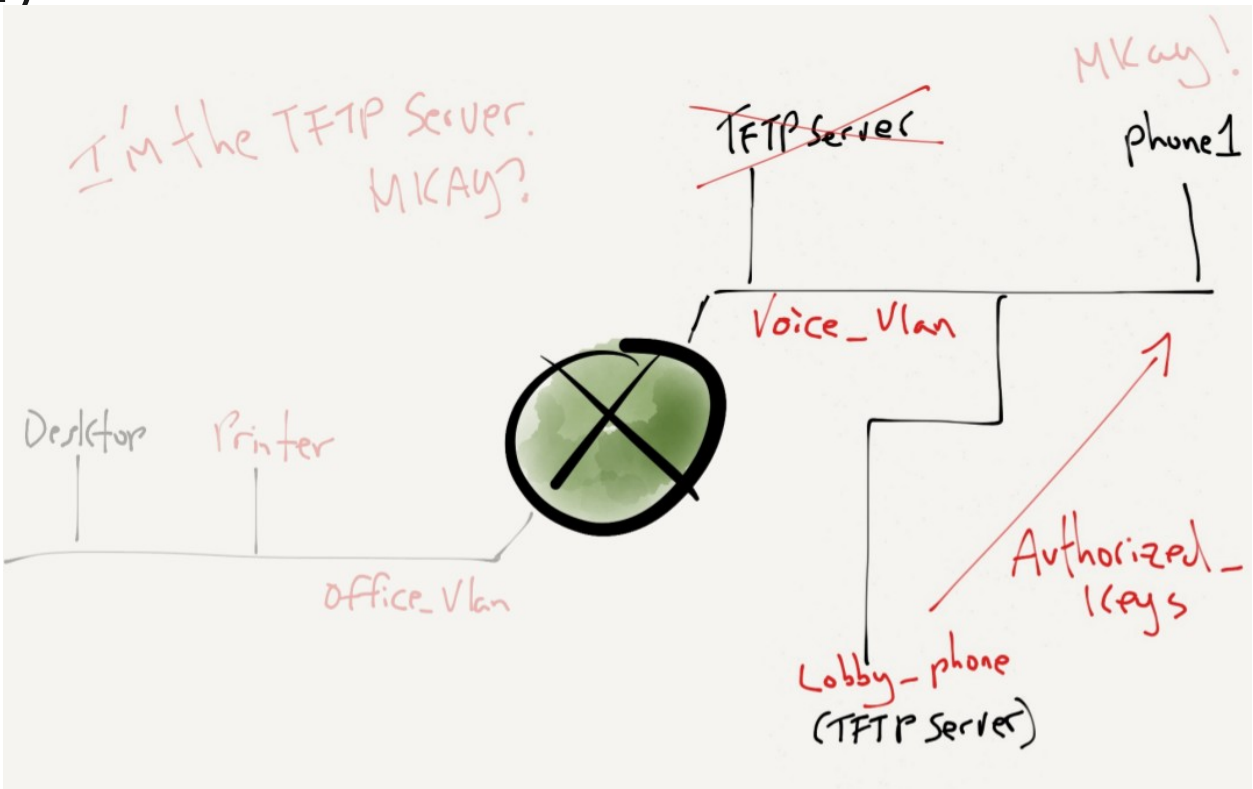
- Correctif





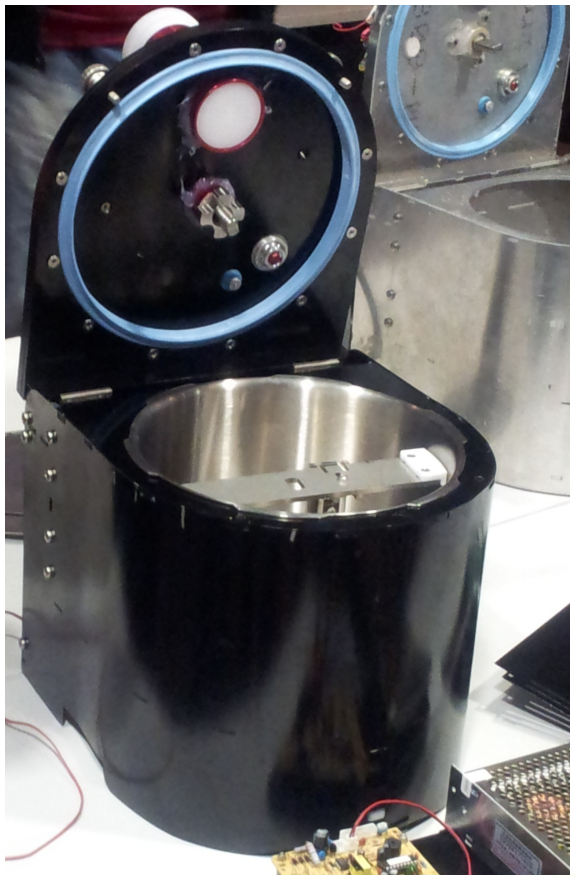
Hacking Cisco phones
Ang Cui & Michael Costello

- Autres attaques
  - Empoisonnement de cache ARP du téléphone avant une connexion SSH pour se faire passer pour le serveur TFTP légitime
  - Envoi de la réponse avant le serveur TFTP légitime (un paquet UDP à envoyer)



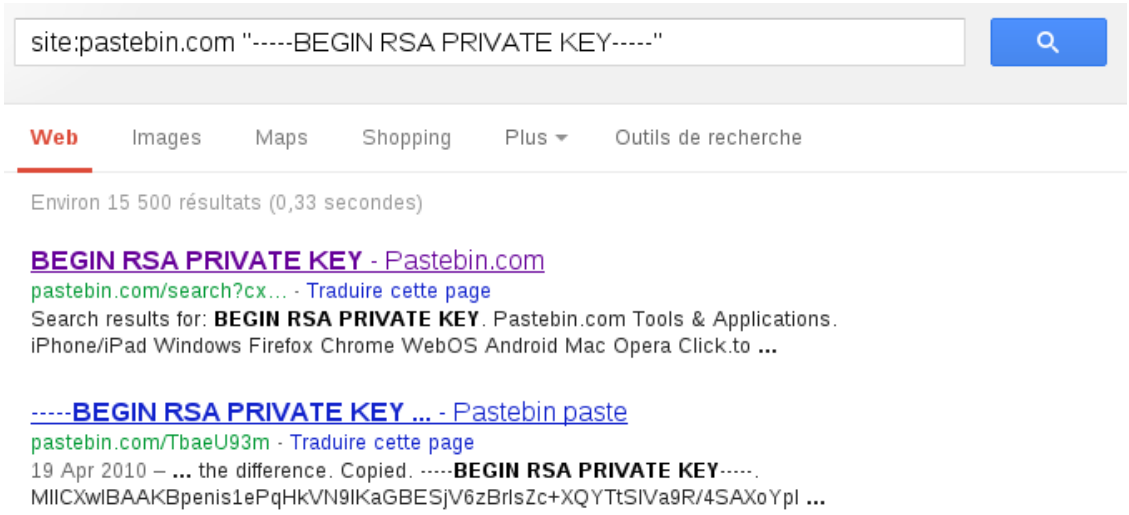
EveryCook
Alexis Wiasmitinow

- Machine de cuisine autonome
  - Gestion de la température, pression, quantité d'ingrédients
  - Utilisation de recettes (informations diététiques, régime alimentaire...)
- 2008 : Début du projet
- 2011 : Premier prototype
  - Arduino + EEEpc
  - Code en PHP
  - Moteur de récupération, Casserole …
- Dernier prototype :
  - Ajout du Wifi, d'un serveur Web



FactHacks
djb Nadia Heninger Tanja Lange

- Énumération des différentes méthodes pouvant affaiblir RSA
  - P et q petits
  - P et q trop près
  - Mauvais générateur de nombres aléatoires
- Clefs 1024 bits déconseillées
  - Cassable par des botnets ou des états
  - Nouveau centre informatique de la NSA



Defeating Windows memory forensics
Luka Milkovic

- Inforensique mémoire de plus en plus populaire
  - Recherche d'objets cachés par un rootkit
  - Fichier dépacké, déchiffré
- Corrompre l'acquisition de la mémoire
  - Arrêt du processus d'acquisition
  - Empêcher l'installation du driver
- Point faible
  - Écriture de la mémoire sur le disque

Defeating Windows memory forensics
Luka Milkovic

- Présentation de son outil : Demantia
  - Remplacement de NTWriteFile()
  - Dissimulation de structures lors de l'acquisition
  - Caché uniquement dans l'acquisition et non en mémoire
  - http://code.google.com/p/dementia-forensics/
- Permet de cacher
  - Processus
  - Threads
  - Connexions réseaux
  - Handles Objets
  - Drivers

Let Me Answer That for You
Nico Golde

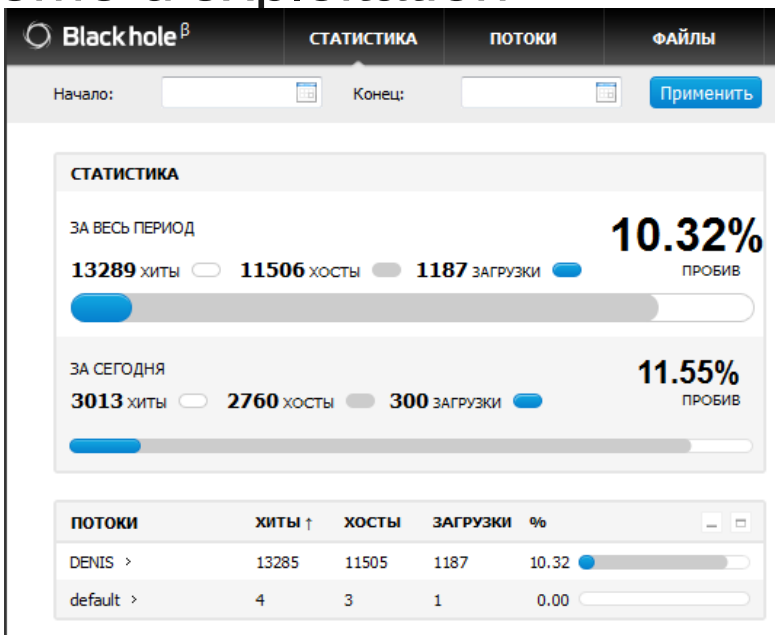
- Présentation du canal de radiomessagerie (*Paging Channel*)
  - Utilisé à des fins de notification
  - Messages transmis à tout le monde
  - Messages non chiffrés et rarements authentifiés
- Possibilité de réaliser un déni de service
- Attaques possibles si réponse avant le téléphone légitime
  - Déni de service : Non réception SMS ou appel
  - Interception de SMS d'une victime : Nécessaire de connaître le TMSI (*Temporary Mobile Subscriber Identity*)
  - Déconnexion d'un téléphone du réseau : message « *IMSI Detach* »

Stylometry and Online Underground Markets
Aylin Caliskan Islam et Sadia Afroz

- Sources
  - Canaux IRC, Forums multi-langues : anglais, russe, indien, allemand
  - Carding, Spam, Exploits, Logiciels malfaisants
- Identification de suspects et de sujets prédominents
- Identification grâce à
  - Mots, verbes, lettres
  - Ponctuation
  - Motifs répétés
- Outils développés (présentés au 28c3)
  - Jstylo : identification de l'auteur de messages
  - Anonymouth : anonymisation de texte

Analytical Summary of the BlackHole Exploit kit - Julia wolf

- Première version découverte en septembre 2010
- Écrit en PHP donc indépendant du système d'exploitation
- Requiert MySQL et IonCube
- Qui ?
  - « Naron » a codé la v1.0 et 1.1
  - « Legacy » a vendu la version 1.0
  - « Paunch » s'occupe de tout aujourd'hui
  - Probablement des Russes



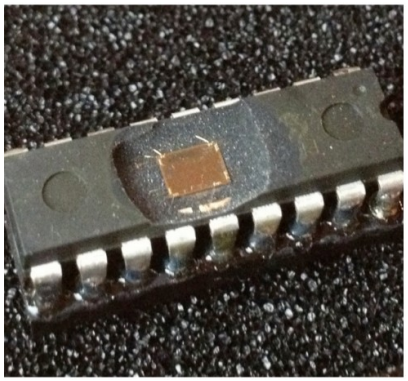
- Les exploits viennent de tierces personnes
- Début mai 2011 le code source à fuit
  - Protégé par IonCube
  - Certains fichiers manquants

Writing a Thumbdrive from Scratch
Travis Goodspeed

- Facedancer
  - Module électronique permettant d'émuler un périphérique USB
  - Développement en Python
  - Utile pour le développement d'exploits de drivers USB
- Techniques anti-inforensiques
  - Manipulation de l'acquisition (accès linéaires sur le disque)
  - Identification du type de système d'exploitation sous-jacent
  - Détection de la présence d'un bloqueur en écriture

Low cost chip microprobing
Philipp Maier & Karsten Nohl

- Introduction à l'ingénierie inverse de cartes électroniques
- Utilisation d'un microscope
- Explication du décapage des puces électroniques
  - A la main
  - Utilisation de produits chimiques
  - Utilisation de lasers
- Explication de protection courante contre ce type d'analyse
  - Filet de protection en fils électriques
  - S'ils sont cassés alors le composant ne fonctionne plus
- Prix du matériel (~ 2500 €)

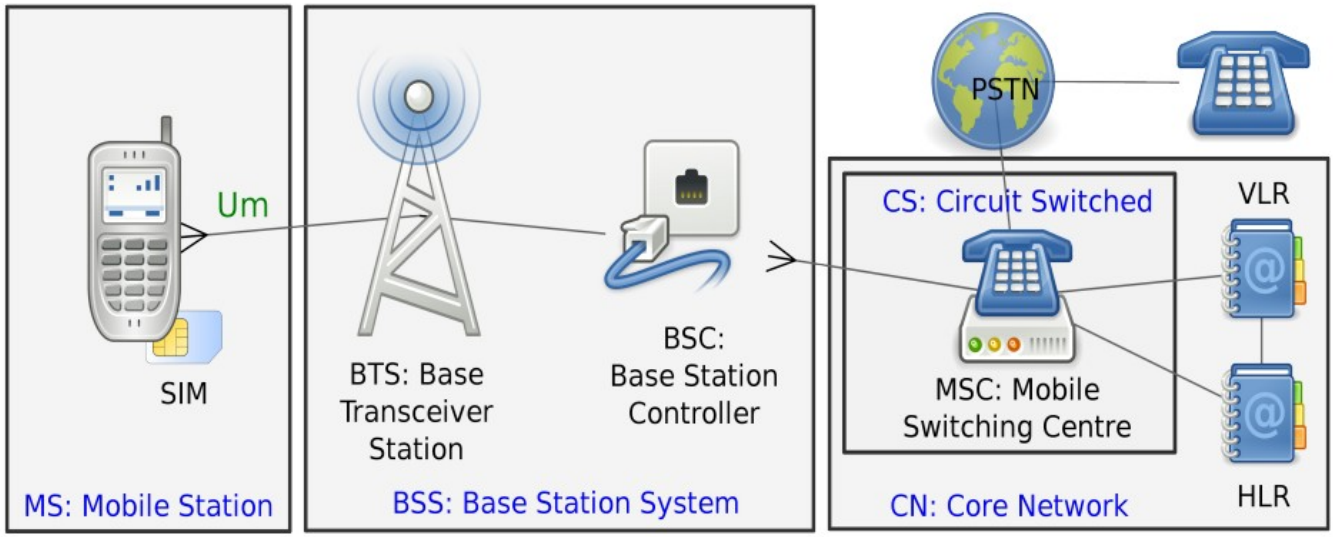


Security Evaluation of Russian GOST Cipher - Dr. Nicolas T. Courtois

- GOST
  - Système de chiffrement officiel en Russie
  - Chiffrement symétrique
  - Développé en 1970
  - Malgré 20 ans de recherches, aucune vulnérabilité majeure trouvée
- Meilleure attaque possible
  - Retrouver la clé de 256 bits avec une complexité de 2^101
  - Combinaisons de nombreuses attaques différentes pour réduire la complexité
  - Certaines attaques présentées proviennent du conférencier
- Certaines techniques non reconnues par la Russie

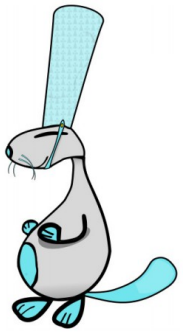
Further hacks on the Calypso platform
Sylvain Munaut

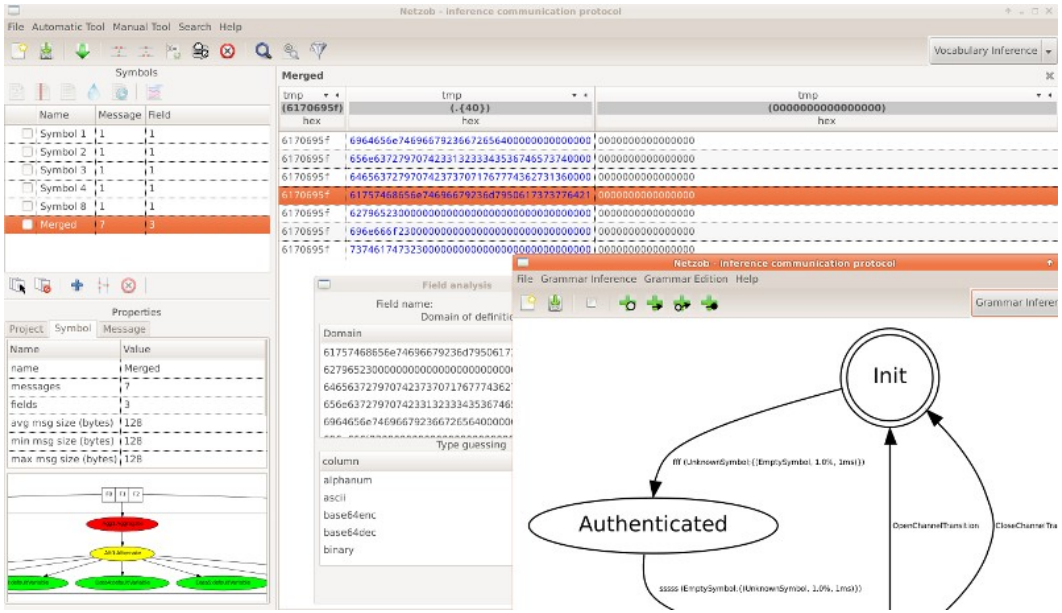
- Transformation d'un téléphone en élément du réseau
- Motorola C123
  - OsmocomBB
  - OpenBTS
- Démonstration
  - Interception de SMS ayant transité par ce BTS



Protocol reversing and simulation
Frédéric Guihéry &Georges Bossert

- Création d'un outil d'analyse de protocoles inconnus : Netzob
- Pas d'analyse de fichiers binaires
- Trois approches
  - Passives
  - Actives
  - Semi-automatique
- Quatre composants
  - Import
  - Inférence avec le protocole
  - Simulation
  - Export





Protocol reversing and simulation
Frédéric Guihéry &Georges Bossert

- L'outil
  - Uniquement une interface graphique (GTK3)
  - Principalement écrit en python et en C
  - Architecture sous forme de plugins
  - Libre : https://dev.netzob.org/git/netzob.git/
- Utilisation de NetZob contre le botnet ZeroAccess
  - Protocole pair à pair pour commander le botnet
  - Communication chiffrée mais chiffrement cassé par une tierce personne
  - Certaines traces réseaux proviennent du site « contagio »
  - Après analyse, la simulation du trafic permet d'obtenir des réponses cohérentes du serveur

Conclusion

- Une ambiance unique ?
- Sujets des conférences très divers
  - Trop de conférences sur l'hackivisme
  - Conférences techniques intéressantes

- Informations complémentaires
  - Planning et supports de présentations
    - http://events.ccc.de/congress/2012/Fahrplan/
  - Vidéos
    - http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/
    - Https://www.youtube.com/playlist?list=UUG4QMB95FR6Df6XdQwn8gSg

Merci de votre attention

Questions ?

Merci à l'OSSIR pour sa participation