OSSIR
CR BlackHat 20/Defcon
Las Vegas – 22 au 30 Juillet 2017

Charles-Edmond Bihr
<Charles-Edmond.Bihr@hsc.fr>

Olivier Houssenbay
<Olivier.Houssenbay@hsc.fr>

Blackhat 2017 – 20ème édition

- Deux parties
  - 22 au 25 juillet
    - Trainings
  - 26 au 27 juillet
    - Briefings
- 18 tracks ou “thèmes”:
  - Cryptography, Enterprise, Exploit development, Hardware/Embedded, IoT, Mobile, Reverse engineering, Web AppSec, etc.
- Mandalay Bay

Defcon 25

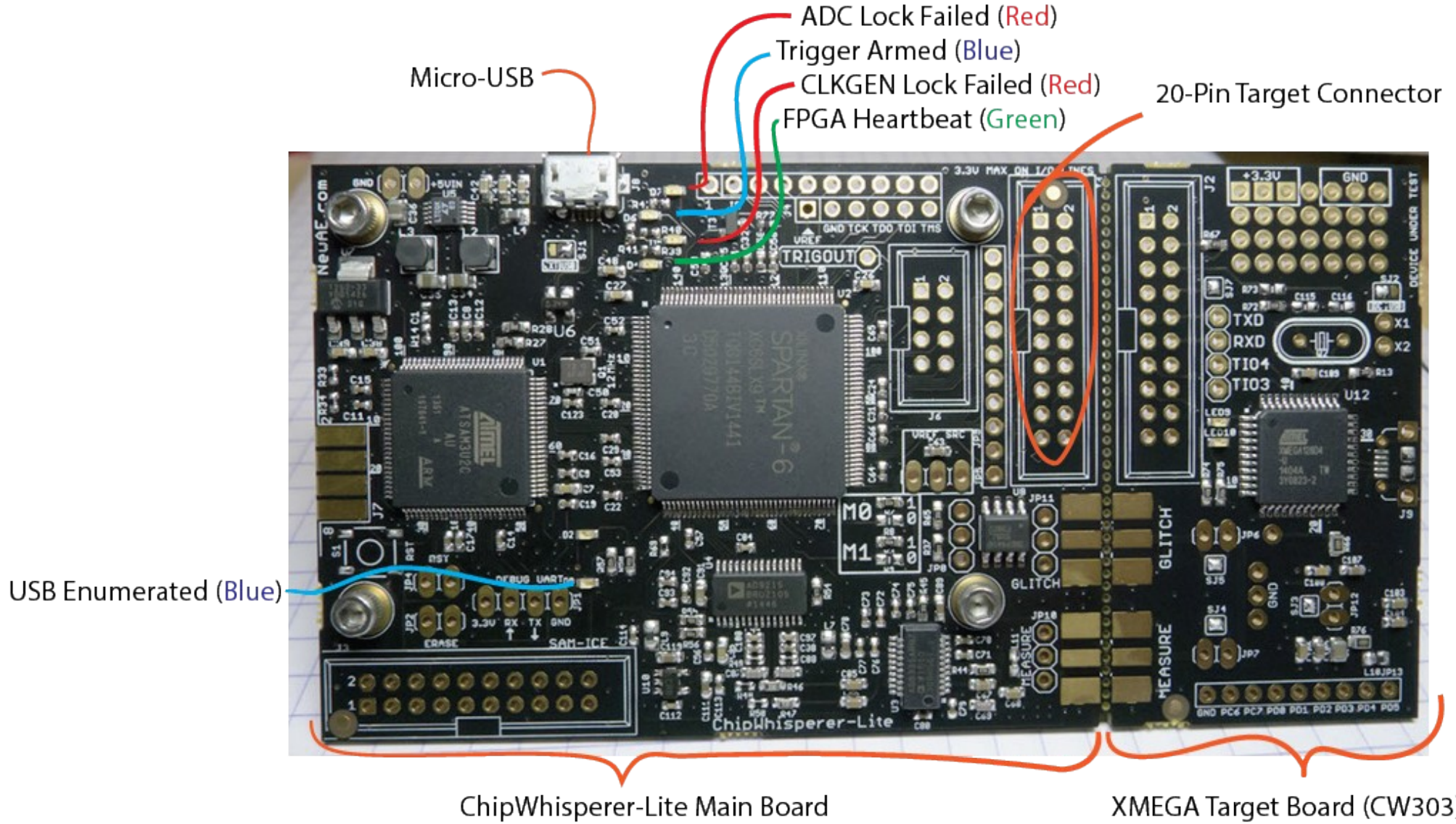
- Conférences
  - 27 au 30 juillet
- Premier jour (Dernier jour de Blackhat)
  - Deux tracks
- Deuxième et troisième jours
  - Quatre tracks
- Caesars Palace
- CTF, Workshops, Demo labs and Villages (Biohacking, Car hacking, Crypto and privacy, Hardware hacking, ICS, IoT, Lockpick, etc.)

Formation - ADVANCED HARDWARE HACKING: HANDS-ON POWER ANALYSIS & GLITCHING WITH THE CHIPWHISPERER

Par Colin O'Flynn, NewAE Technology

- Prise en de main de ChipWhisperer-Lite
  - plateforme matérielle open source
- Analyse de consommation électrique par canaux auxilaires
  - captures de plusieurs traces
  - extraction de clef AES 128
- Glitching, Injection de faute
  - modification d'horloge

Formation - ADVANCED HARDWARE HACKING: HANDS-ON POWER ANALYSIS & GLITCHING WITH THE CHIPWHISPERER



Formation - ARM IoT exploit lab

(Par Saumil Shah, 2 jours)

- Exploitation de vulnérabilités sur architecture ARM
- Extraction du firmware d'un routeur dans une VM ARM
- Lancement des services minimaux requis et du serveur HTTP
- Exploitation d'une faille sur le serveur HTTP: ROP, ASLR, Shell.

Formation – Malware analysis crash course

(Par Flare team of Mandiant, a Fireeye company)

- Introduction à l'assembleur
- Principalement l'utilisation d'une VM et d'outils comme Ollydbg, IDA pro.
- Où regarder quand on analyse un malware
- Un peu court...

FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

(Par Sen Nie, Ling Liu, Yuefeng Du de Keen Security Lab of Tencent)

- Compromission complète:
  - Wifi
    - Connexion automatique en wifi au SSID “Tesla Guest” avec psk “abcd123456”
    - QtCarBrowser, le navigateur intégré recharge sa page courante automatiquement
    - Vieille version de WebKit utilisée → Vulnérabilité dans la fonction JSArray::sort()
    - CVE-2011-3928: Use-after-free vulnerability in Google Chrome before 16.0.912.77
    - Écriture/Lecture d’adresses arbitraires
    - Exécution de code arbitaire

FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS (suite)

- Élévation de privilèges
  - Utilisateur sans privilèges, protégé par AppArmor, règles Iptables interdisant l'accès aux services locaux.
  - Un vieux kernel Linux est utilisé (2.6.36.3)
  - CVE-2013-6282 (put_user/get_user)

    "allows attackers to read or modify the contents of arbitrary kernel memory locations"
  - Exécution de code arbitraire: Remplacement d'un appel système dans la table des appels sytèmes
- Échappement de Apparmor
  - Appel de la fonction reset_security_ops()
- Obtention des droits roots non restreints: Patch de setresuid()
- Compromission du bus CAN

SONIC GUN TO SMART DEVICES: YOUR DEVICES LOSE CONTROL UNDER ULTRASOUND/SOUND

(Par Wang Zhengbo, Wang Kang et Pan, Aimin de Alibaba Security, Yang Bo de CAICT et Li Shangyuan de Tsinghua University)

- Attaque sur les MEMS (gyroscopes, accéléromètre)
- Ces types de capteurs ont des parties mobiles
- Des ultrasons sont utilisés pour entrer en résonnance avec ces parties mobiles
- Cibles:
  - Téléphones, drones, robots, hoverboards
  - Tout ce qui contient un MEMS.
- Démos:
  - Téléphone: https://www.youtube.com/watch?v=McNM29Zk1O8
  - Self Balancing robot: https://www.youtube.com/watch?v=tO5OxbbA1hU

SONIC GUN TO SMART DEVICES: YOUR DEVICES LOSE CONTROL UNDER ULTRASOUND/SOUND (suite)

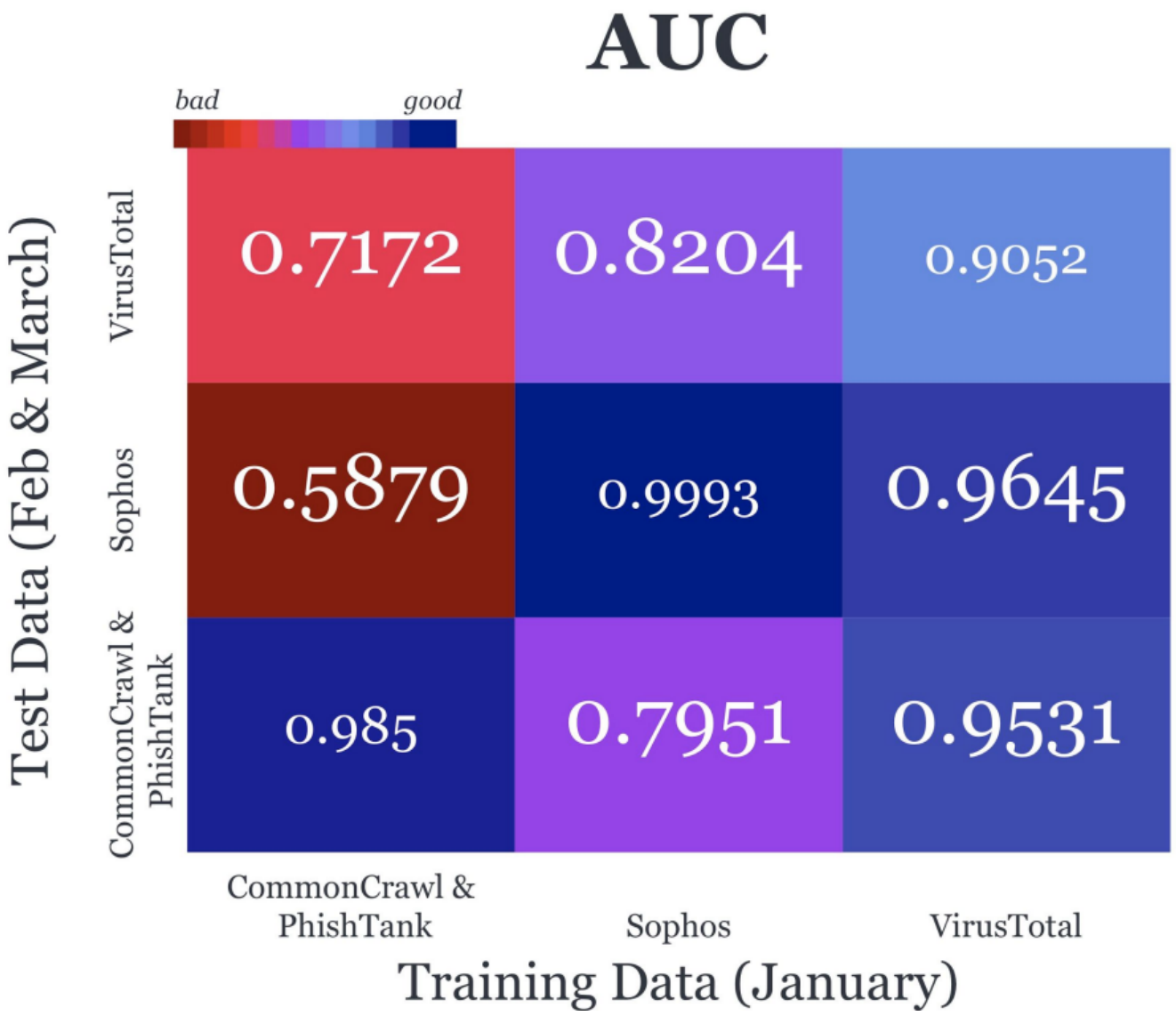
- Paraît peu applicable dans la vie réelle pour l'instant:
  - Distance entre capteur et "pistolet"
  - Poids et volume du matériel nécessaire

GARBAGE IN, GARBAGE OUT: HOW PURPORTEDLY GREAT MACHINE LEARNING MODELS CAN BE SCREWED UP BY BAD DATA

(Par Hillary Sanders)

- Test de trois modèles d'apprentissage automatique permettant de noter des URLs:
  - Sophos
  - VirusTotal
  - CommonCrawl & Fishtank
- Objectifs de ces modèles:
  - *f* (http://www.trustus.evil.ru/paypal/login/) = .944780
  - *f* (https://www.facebook.com/) =.019367
- Ces modèles sont en premier lieu entrainés. Chaque moteur a été entrainé avec les données d'entraînement des autres.
- Leur efficacité a ensuite été testée avec des données de test.

GARBAGE IN, GARBAGE OUT: HOW PURPORTEDLY GREAT MACHINE LEARNING MODELS CAN BE SCREWED UP BY BAD DATA (suite)



- Conclusion:
  - La précision d'un modèle est **extrêmement** dépendante des données utilisées pour l'entraînement et le test

BOT VS BOT: EVADING MACHINE LEARNING MALWARE DETECTION

(Par Hyrum Anderson)

- Modèle d'intelligence artificielle
  - Pour obfusquer des programmes malveillants
  - Afin de contourner des modèles d'apprentissage automatique de détection de malware en "blackbox" (pas d'accès au modèle).
- Le compare à une IA jouant seule au jeu "Atari breakout":

BOT VS BOT: EVADING MACHINE LEARNING MALWARE DETECTION (suite)

- Atari breakout:
  - Entrée : Environnement (screenshot du jeu à un instant donné)
  - Sortie : Un mouvement, déplacer la barre à gauche/droite
  - Feedback : Le score (points quand on casse une brique)
- Anti-malware evasion IA:
  - Entrée : Environnement (Octets du malware)
  - Sortie : Une transformation sur le binaire (nouveau point d'entrée, nouvelle section, imports aléatoires, upx pack/unpack, etc.)
  - Feedback : Le score retourné par VirusTotal

BOT VS BOT: EVADING MACHINE LEARNING MALWARE DETECTION (suite)

- Entraînement:
  - 15h pour 100k itérations (10k malwares avec 10 tours chacun)
  - Utilisation d'échantillons de VirusShare
- Résultats:
  - Le modèle est appliqué à 62 malwares dont 35 sont initialement détectés
  - Une fois modifiés, seuls 25 malwares sont détectés
- Recommandations:
  - Attaquer son propre modèle
  - Limiter l'exposition du score

BROADPWN: REMOTELY COMPROMISING ANDROID AND IOS VIA A BUG IN BROADCOM'S WI-FI CHIPSETS

(Par Nitay Artenstein de Exodus Intelligence)

- REMOTE EXPLOIT != BROWSER EXPLOIT
- Attaque du chipset Wifi broadcom:
  - Peu ou pas de protections (Pas de DEP, ASLR, etc.)
  - Mémoire RWX
  - (Contrairement au baseband chipset) chipset wifi (broadcom) est utilisé pour énormément de téléphones
- Code source trouvé sur github (github.com/elenril/VMG1312-B)

BROADPWN: REMOTELY COMPROMISING ANDROID AND IOS VIA A BUG IN BROADCOM'S WI-FI CHIPSETS (suite)

- Wireless Media Extension (WME)
  - Extention QoS de 802.11
  - L'information est parsée dans les paquets "probe resquests", "probe response", et "association response" → pas besoin d'être associé
- Overflow de seulement 24 octets → Egghunter
- Puis envoie du shellcode complet dans des paquets "beacon probes" (rappel: les paquets sont RWX)
- Prochaine étape → un ver
  - Wifi! : un téléphone infecté en infecte un autre automatiquement
- Pas d'exécution de code privilégiée (mais Project Zero a déjà montré la possibilité d'écrire dans la mémoire kernel en utilisant PCIe)

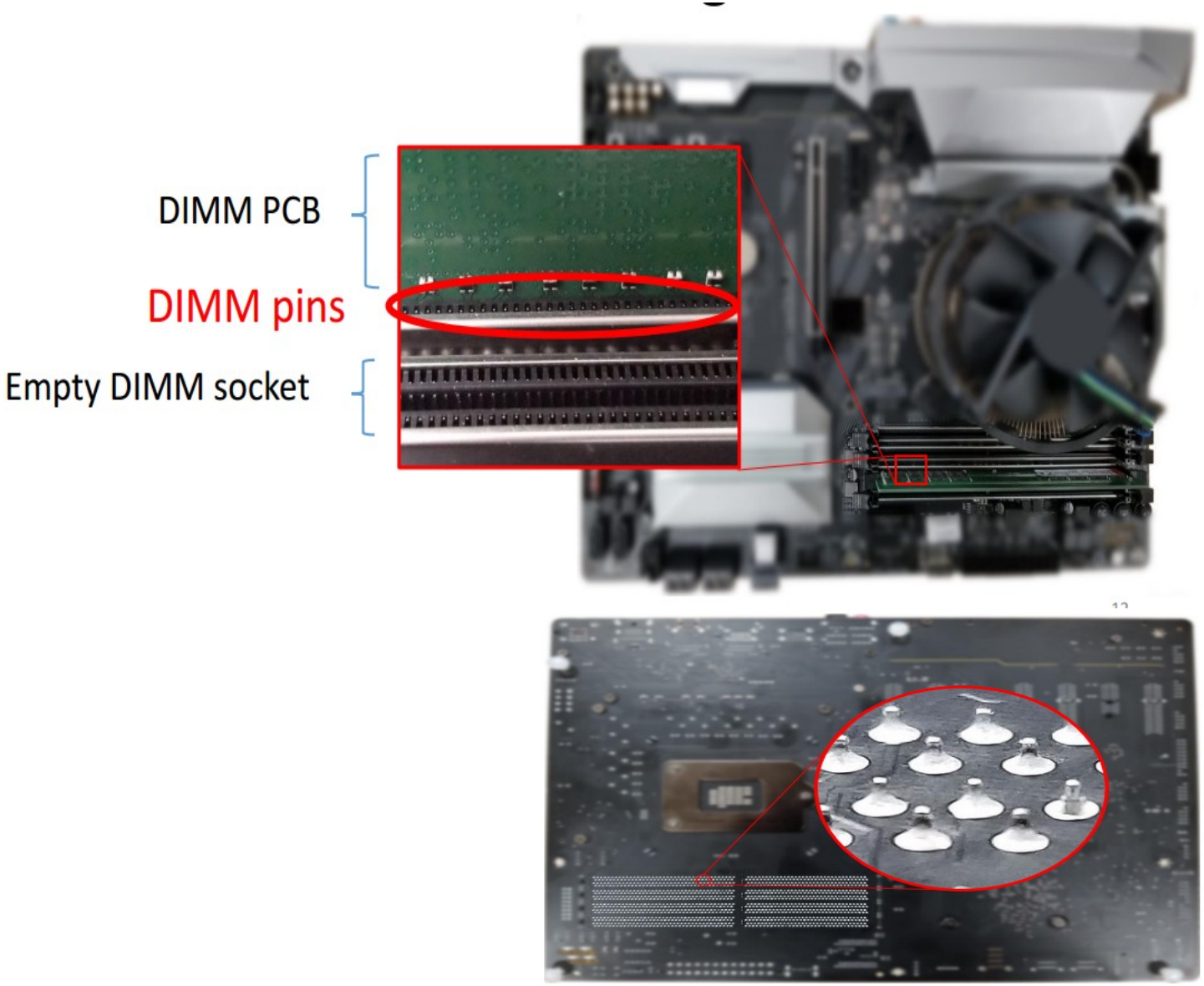
Taking DMA Attacks to the Next Level...

Hardware/Sécurité des composants

- Par Anna Trikalinou & Dan Lake (Intel)
- Attaque physique sur la DRAM (Dynamic Random Access Memory)
  - Objectifs
    - Extraire les secrets (clefs de chiffrement du disque dur)
    - Contourner les politiques de sécurité (modification de *page tables*)
- Attaque DMA indétectable
  - Exploite le design des DIMMs
  - Nécessite un accès physique

Taking DMA Attacks to the Next Level...

Hardware/Sécurité des composants

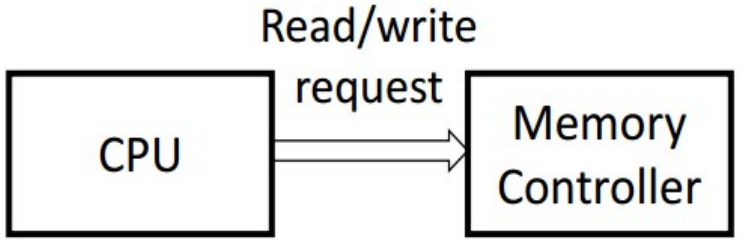


Taking DMA Attacks to the Next Level...

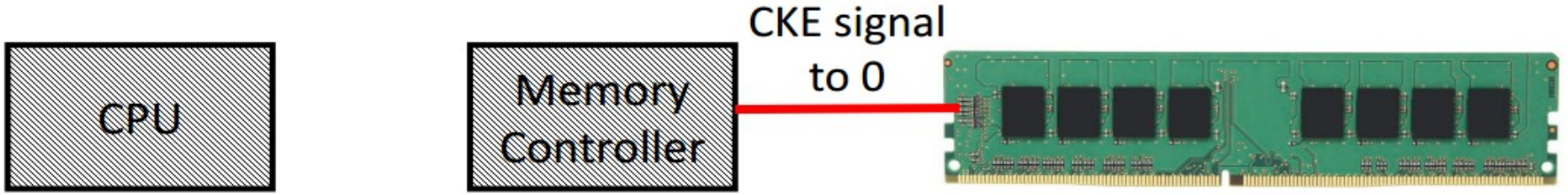
Hardware/Sécurité des composants

- 288 pins de chaque DIMMs exposées
  - Demande de R/W
- Étude des normes JEDEC (Joint Electron Device Engineering Council)
  - Application universelle, protocole Hardware
  - Définit les pré-requis des modules mémoires et architectures
- Contrôleur de mémoire
  - Intermédiaire entre le CPU et la DIMM
  - Agnostique
  - Opérations
    - Calibration, configuration des registres, ordonancement, rafraichissement

- Fonctionnement de la DRAM
  - État normal
    - CKE (clock enable) '1'



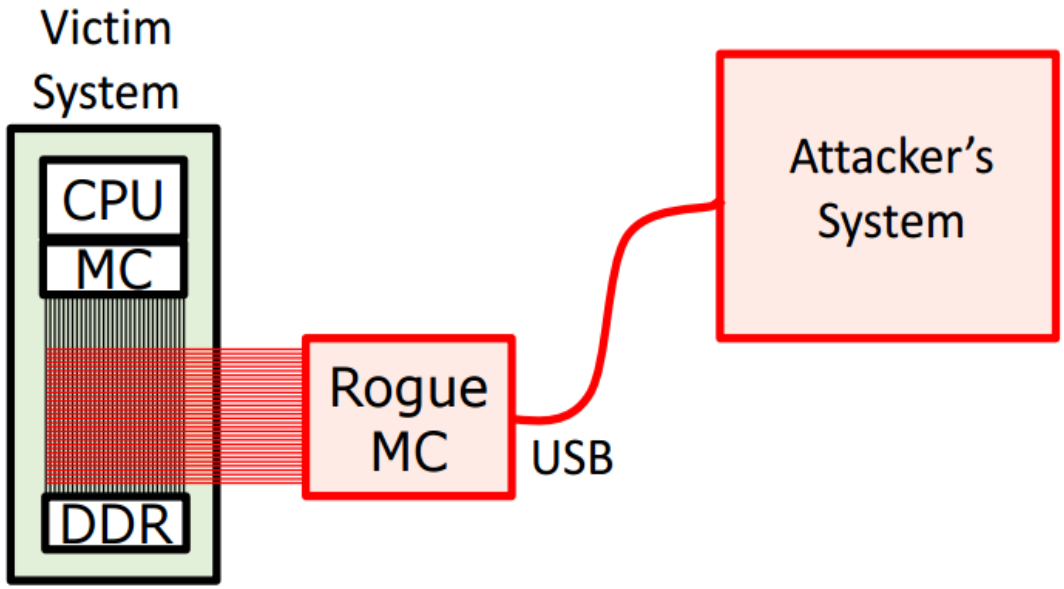
  - En veille (sleep)
    - CKE '0'
    - CPU et contrôleur de mémoire éteints
    - DIMM en gestion autonome



Taking DMA Attacks to the Next Level...

Hardware/Sécurité des composants

- Limitations
  - Calibration et fréquence d'horloge géré par le contrôleur de mémoire
  - Pas d'authentification entre le contrôleur et la DIMM
  - Aucune protection contre l'usurpation de contrôleur de mémoire
- Conception d'un contrôleur de mémoire malveillant (rogue)



- PoC sur un fil
- Perpectives
  - Passer sur le bus entier
  - Réduire le bruit ajouté par les connecteurs
- Contre-mesures
  - Court terme : mise en veille prolongée (hibernation)
  - Long terme : Modifier le design des cartes mères, ajout d'un mécanisme d'authentification dans JEDEC

Breaking the x86 Instruction Set Arch

Hardware/Sécurité des composants

- Par Christopher Domas @xoreaxeaxeax (Batelle Memorial Institute)
- Outil de scan des instructions x86
  - Sandsifter : https://github.com/xoreaxeaxeax/sandsifter
- Objectifs
  - Auditer le processeur
  - Trouver les instructions cachées
- Approche
  - Recherche d'instructions par « tunneling »
    - réduction de l'espace de recherche ~100 000 instructions contre $1.3x10^{36}$
  - Taille des instructions (en x86 longueur variable)
    - Analyse des pages fault

- Recherche d'instructions
  - Deux pages mémoire consécutives
    - RWX et RW

  - On saute à l'instruction à décoder
    - Vérification par le décodeur d'instruction
  - Nécessite un octet supplémentaire ?
    - Exception PF (page fault)
      - Adresse de « faute » dans le registre CR2 = adresse seconde page
  - Ajout d'un octet

- Instruction décodée
  - Exécution possible
  - Levée d'exception différente
  - Page fault avec une adresse différente dans CR2
  - Taille de l'instruction déterminée
- L'instruction existe ?
  - Non
    - UD exception => *invalid opcode exception*
  - Oui
    - Pas d'exception

Breaking the x86 Instruction Set Arch

Hardware/Sécurité des composants

- Spécificité
  - Exécution depuis le « ring 3 »
- Composants
  - Injector
    - analyse de pages fault et génération des instructions (tunneling)
  - Sifter
    - analyse les résultats de l' « injector »
    - utilise capstone pour vérifier l'existence des instructions
  - Summarizer
    - regroupe les instructions identifiées par famille

Breaking the x86 Instruction Set Arch

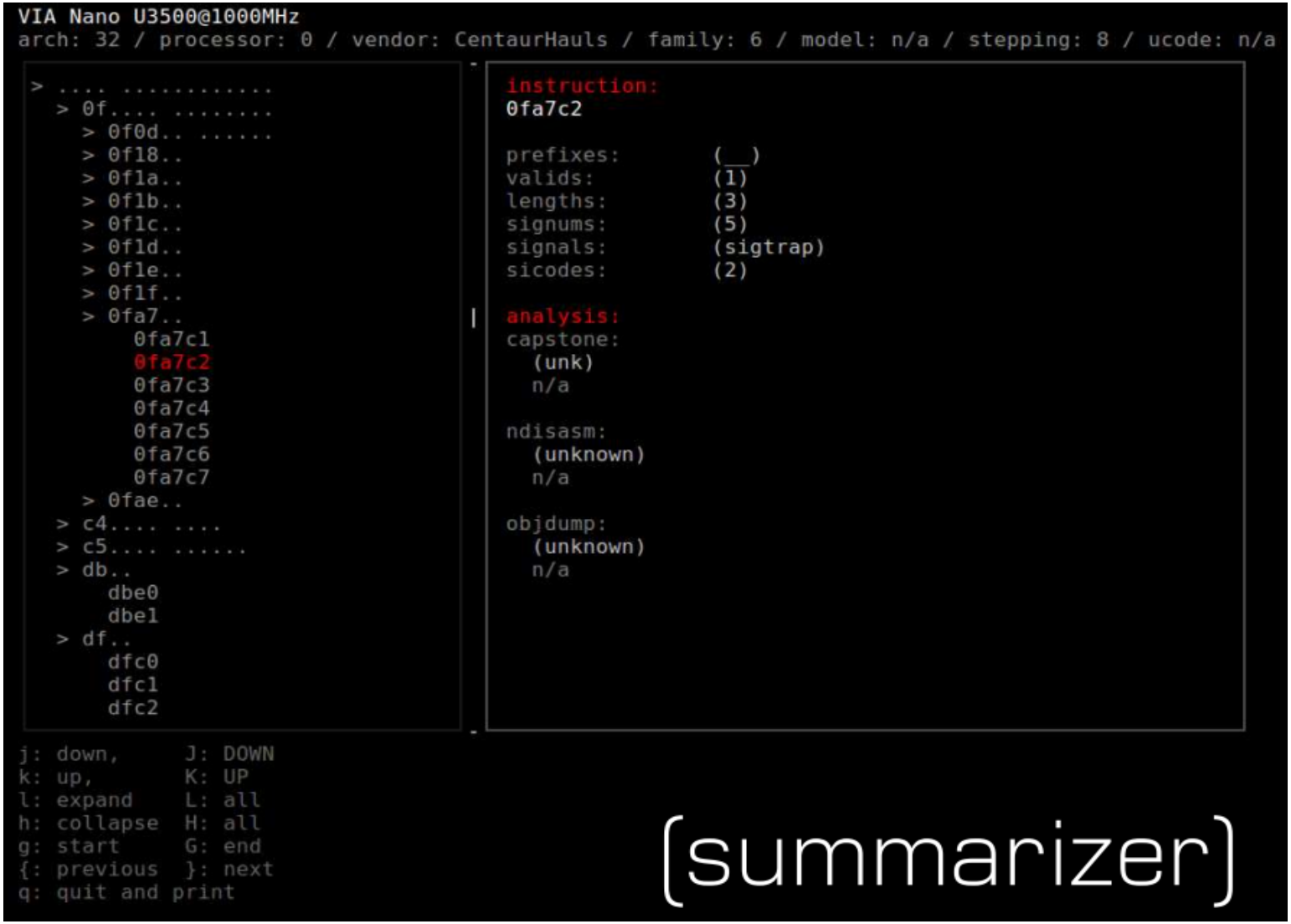
Hardware/Sécurité des composants

- Démo

Breaking the x86 Instruction Set Arch

Hardware/Sécurité des composants

- Démo



- Résultats
  - Instructions cachées
  - Bogues logiciels
  - Défauts dans les hyperviseurs
  - Bogues matériels
- Killer poke ou Halt and catch fire
  - Instruction malformée depuis le « ring 3 »
  - Testé depuis 2 noyaux Windows et 3 noyaux Linux
  - Aucune information sur le model, la marque ou l'instruction exécutée
    - à ce jour
  - Première attaque du même type il y a 20 ans : Pentium f00f

Infection the enterprise abusing office 365+powershell for covert c2

Malware/Défense réseau

- Craig Dods (Juniper)
- Exfiltration de données avec PowerShell et Office365
- PoC en 4 phases
  - SE : utilisation de macros Word/Excel
  - Récupération du token SAML
    - persistance pour la connexion vers Office365
  - Ajout du domaine malfaisant dans les trusted sites et montage d'un partage invisible
  - Contournement des resctrictions PowerShell et exfiltration des données

Infection the enterprise abusing office 365+powershell for covert c2

Malware/Défense réseau

- Avantages de Office365 pour l'attaquant
  - Autorisation de communication chiffrées vers 0365
  - Liaison réseau performante (10Gbps)
  - Volume de données et confiance importante
    - pas de revue du traffic
  - Solutions DLP considère un partage réseau comme ressource locale
  - Cmdlet New-PSDrive
    - Invisible pour l'explorateur de fichier
      - Détection plus difficile

- Contre-mesures
  - Déchiffrer les communications SSL/TLS
  - Base de signatures qui n'autorise que le/les domaines O365 connus
  - Activer la journalisation sur les terminaux et envoyer vers un SIEM
    - Surveiller les instances New-PSDrive
  - Utiliser un pare-feu pour mesurer la quantité de données envoyées et un SIEM pour détecter les upload vers l'extérieur