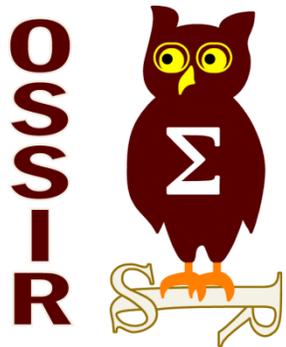


13 janvier 2015



BlackHat Europe 2014 : Compte-rendu

OSSIR 13/01/2015

La BlackHat Europe

- Petite sœur de la BlackHat Las Vegas
- 1000 personnes présentes cette année
- A Amsterdam
- 3 « *tracks* » de conférences
- L'Arsenal



Le programme de ce compte-rendu

Focus sur 3 interventions

- **Firmware.re: unpacking, analysis, and vulnerability discovery as a service**
Jonas Zaddach
- **Practical attacks against VDI solutions**
Dan Koretsky
- **DTM Components : Shadow keys to the ICS kingdom**
Alexander Bolshev & Gleb Cherbov



Sans oublier

- Keynote présentée par Adi Shamir : Side channel attacks – Past, Present and Future
- Lights off! The darkness of the Smart Meters
- Hack your ATM with friend's Raspberry Pi
- Session identifiers are for now, passwords are forever – XSS based abuse of browser password manager
- Industrial Control Systems : Pentesting PLCs 101

Firmware.re: unpacking, analysis, and vulnerability discovery as a service

- **Problème majeur des systèmes embarqués** : l'analyse de ces systèmes requiert beaucoup de temps et ne peut pas être faite manuellement à grande échelle
- **Idee de la recherche** : faire une analyse à grande échelle afin de voir si les systèmes embarqués possèdent les mêmes vulnérabilités
- **Difficultés de cette analyse à grande échelle** : les systèmes embarqués ont des systèmes d'exploitation et des architectures différentes et les enjeux de sécurité sont différents
- **Solution** : site web www.firmware.re permettant d'automatiser les actions suivantes :
 - Télécharger le firmware
 - Faire une analyse statique basique
 - Faire une corrélation avec les autres firmwares
- **Avantage** : caractère non intrusif de l'analyse
- **Plusieurs challenges non encore résolus**
 - Comment obtenir le firmware ?
 - Comment les identifier ? Comment détecter un firmware parmi des milliers de fichiers ?

Présenté par Jonas Zaddach



Pour résumer

- Très beau projet, plutôt ambitieux
- **Première étape franchie** avec la possibilité d'extraire de façon automatisée un firmware et d'analyser ses différents fichiers

Firmware.re: unpacking, analysis, and vulnerability discovery as a service

Challenge: Unpacking & Custom Formats

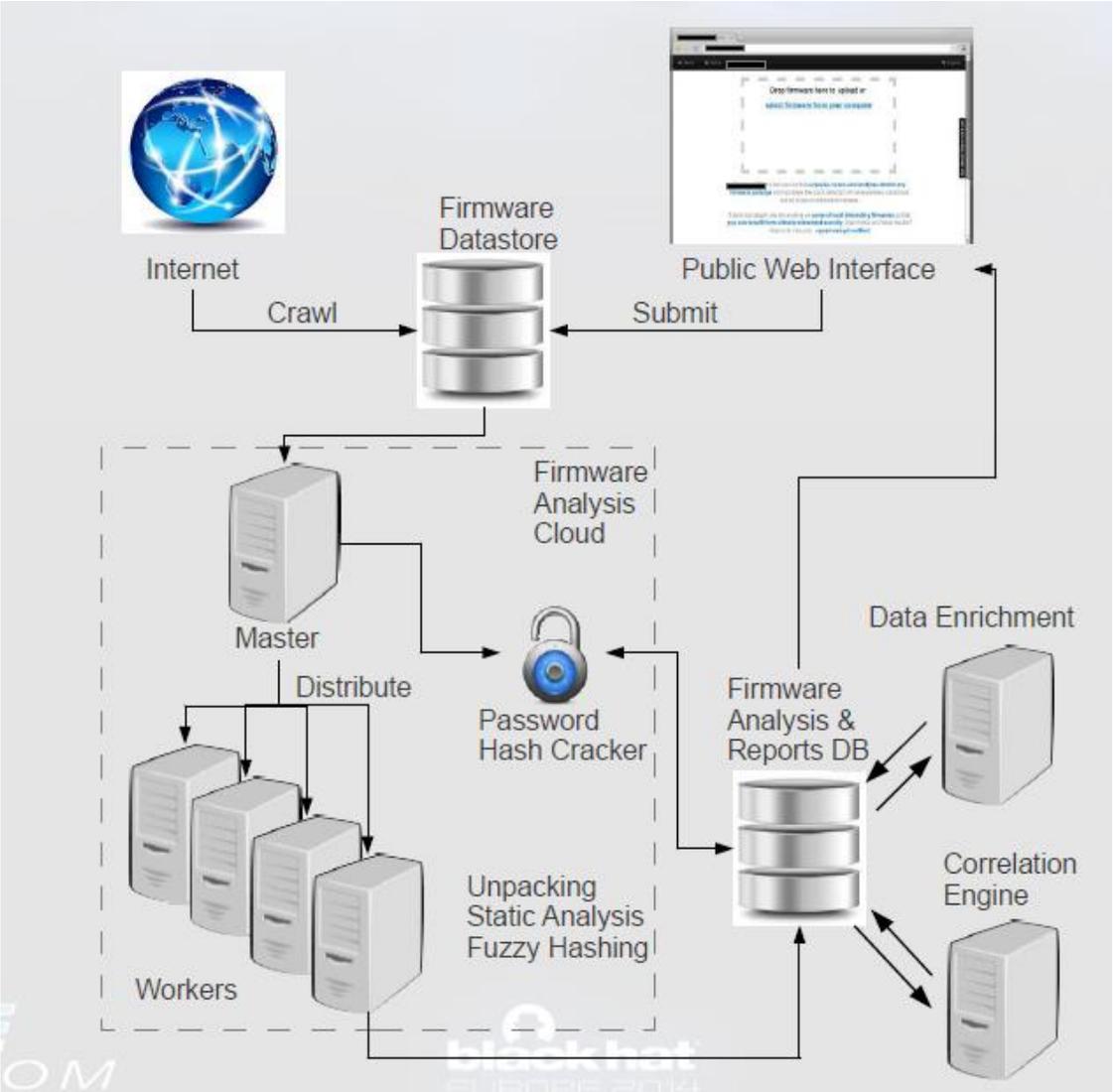
- How to reliably unpack and learn formats?

Update executable?
Binary patch?
Whole FW image?

EURECOM logo
blackhat EUROPE 2014 logo

Challenge: Firmware Identification

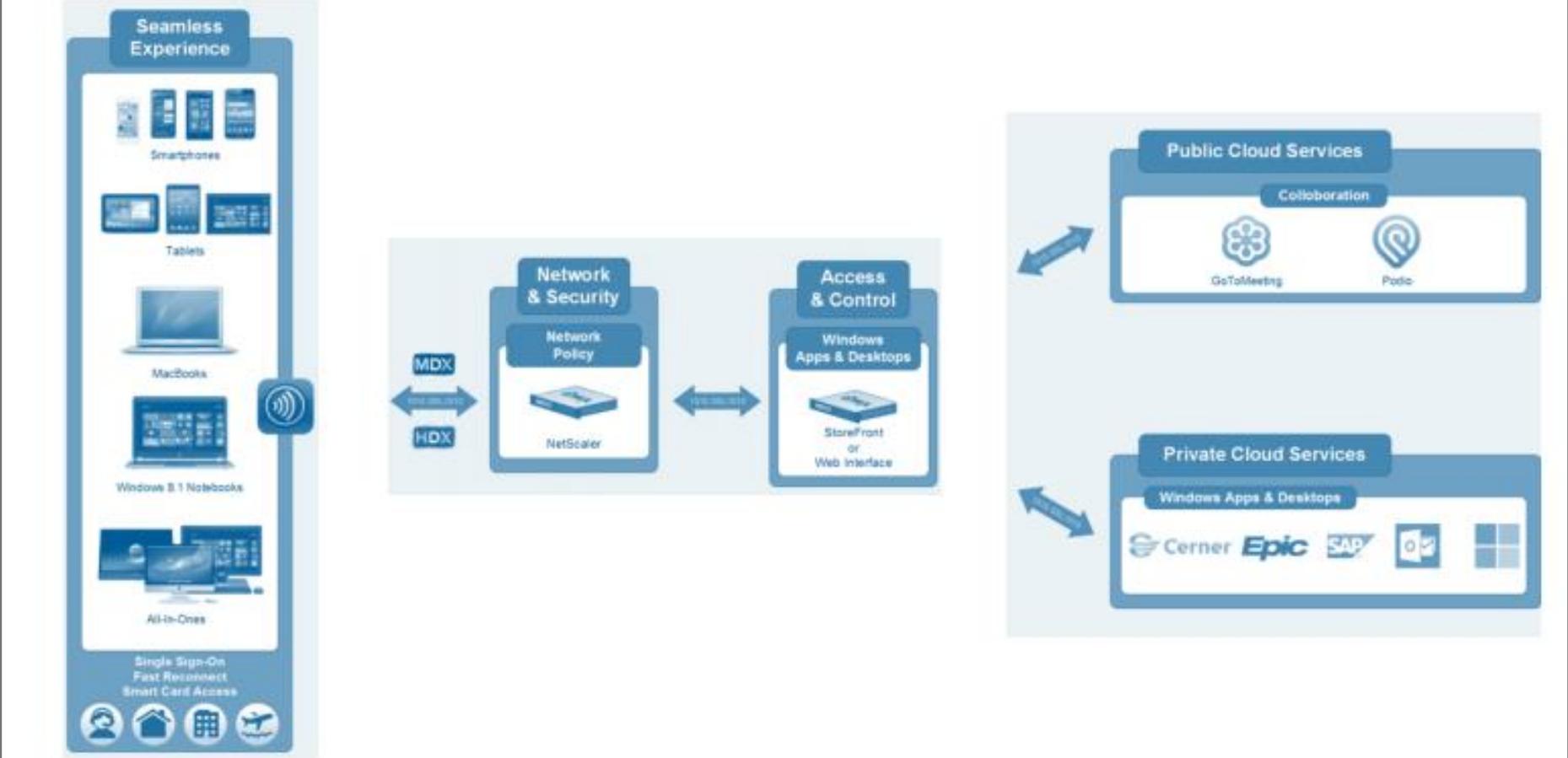
← Clearly a Firmware Clearly not a Firmware →



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Zaddach-Firmware-re-Firmware-Unpacking-Analysis-And-Vulnerability-Discovery-As-A-Service.pdf>

Practical attacks against VDI solutions

VDI Architecture - Example



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf>

Practical attacks against VDI solutions

What is a Mobile Remote Access Trojan (mRAT)



15

- Key Logger
- Screen Scraper
- Memory Scraping
- Files and Photos
- Microphone and Camera
- Track Location
- Emails
- App Data
- Contact Lists, Call & Text Logs

The diagram illustrates the capabilities of a Mobile Remote Access Trojan (mRAT). It features a central blue area with a white border. On the left, there are three icons: a speech bubble for 'Emails', a cube for 'App Data', and a document for 'Contact Lists, Call & Text Logs'. A bracket groups these three items and points to three capabilities: 'Key Logger', 'Screen Scraper', and 'Memory Scraping'. On the right, there are three icons: a document for 'Files and Photos', a microphone for 'Microphone and Camera', and a location pin for 'Track Location'.

<https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf>

Practical attacks against VDI solutions



mRAT Spectrum

FinSpy Mobile

]HackingTeam[

DROPOUTJEEP
ANT Product Data

Gov / Mil mRATs

\$300K-\$12M
Government -> Terrorists / Activists

Darknet mRATs

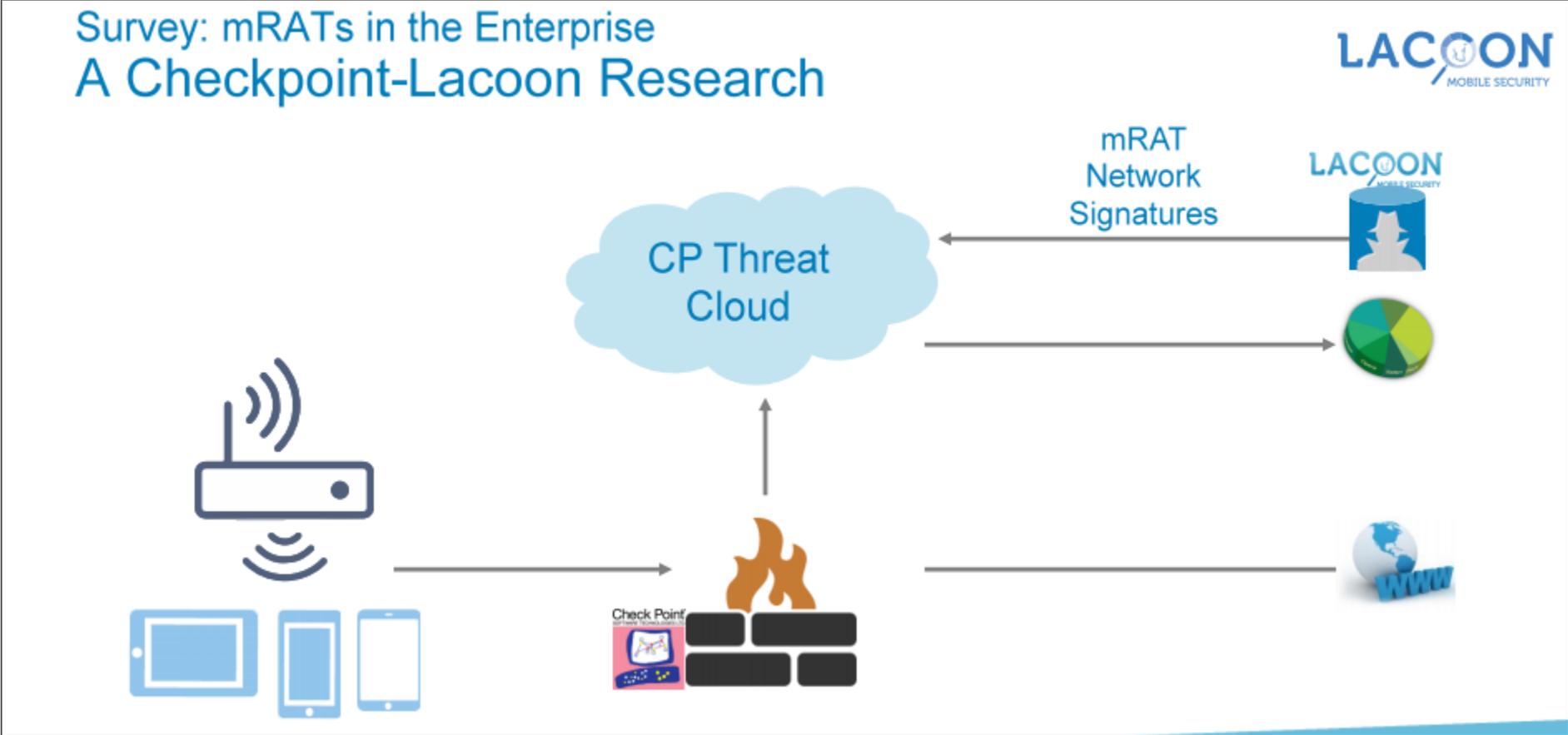
Free - \$300
Cybercriminal -> ?

Surveillance /
Monitoring Tools

Free - \$100
Everyone -> Everyone

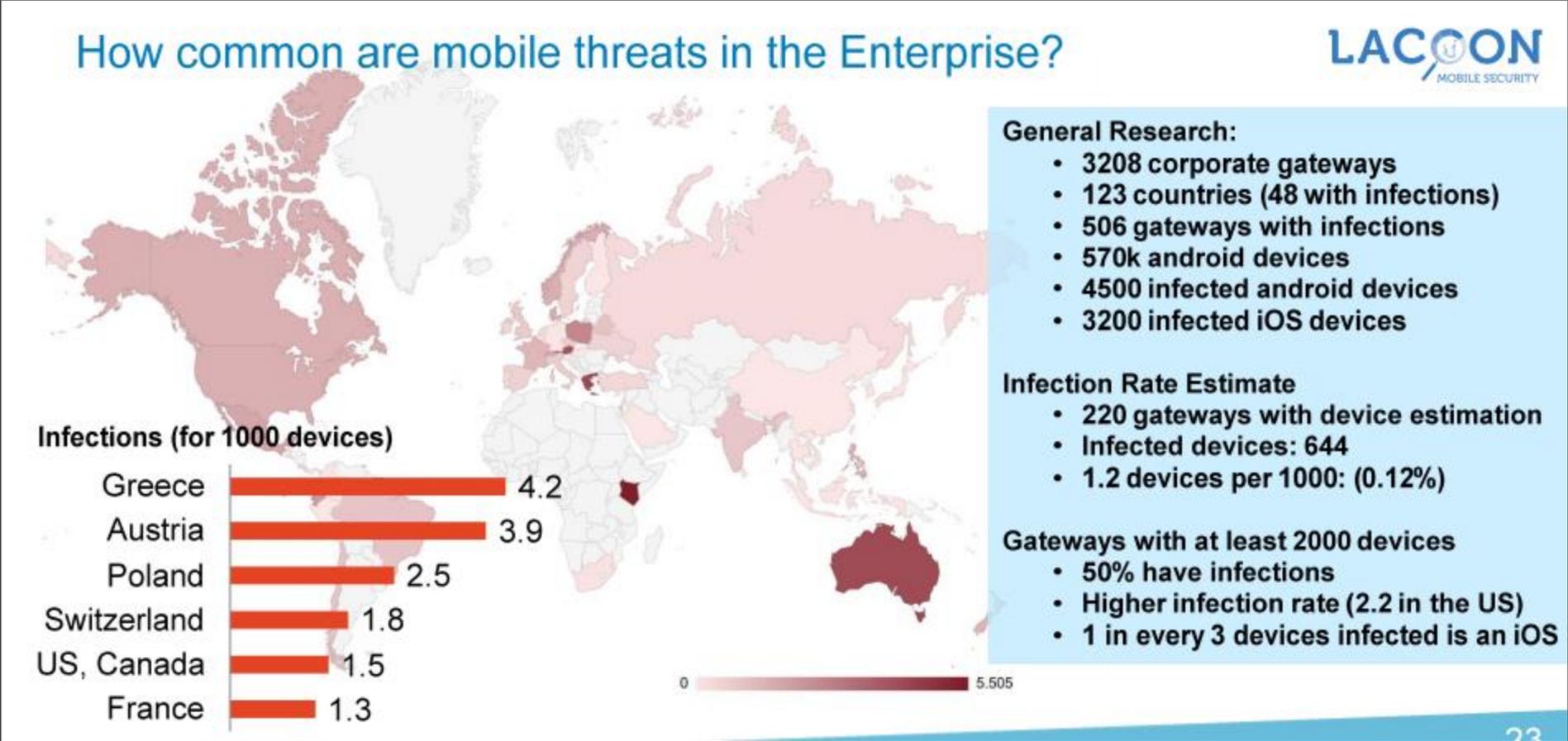
<https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf>

Practical attacks against VDI solutions



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf>

Practical attacks against VDI solutions



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf>

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

ICS 101

- ICS stands for Industrial Control System.
- Today, ICS infrastructures are commonly used in every factory and even in your house, too!
- ICS collects data from remote stations (also called field devices), processes them, and uses automated algorithms or operator-driven supervisory to create commands to be sent back.
- Thousands of field devices could exist at one facility.
- To control them, Plant Asset Management Systems (PAS or AMS) were invented.
- **Plant Assets Management Software = tools for managing plants assets, that lie on the upper/medium levels of ICS and control/monitor/configure field devices.**

DTM COMPONENTS: SHADOW KEYS
TO THE ICS KINGDOM

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

What is FDT/DTM?

- “The FDT concept defines the interfaces between device-specific software components provided by the device supplier and the engineering tool of the control system manufacturer. The device-specific software component is called DTM (Device Type Manager).” © FDT Group, maintainer of FDT/DTM specification

In short:

- FDT standardizes the communication and configuration interface between all field devices and host systems
- DTM provides a unified structure for accessing device parameters, configuring and operating the devices, and diagnosing problems

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

<https://www.blackhat.com/docs/eu-14/materials/eu-14-Bolshev-DTM-Components-Shadow-Keys-To-The-ICS-Kingdom.pdf>

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

CoCreateInstance
IUnknown:Release (final)
IUnknown:Release
up
IPersistInNew
IPersistLoad
combine
IPersistXXX
new
existing

FDT/DTM architecture

Developers dream... vs. ...cruel reality.



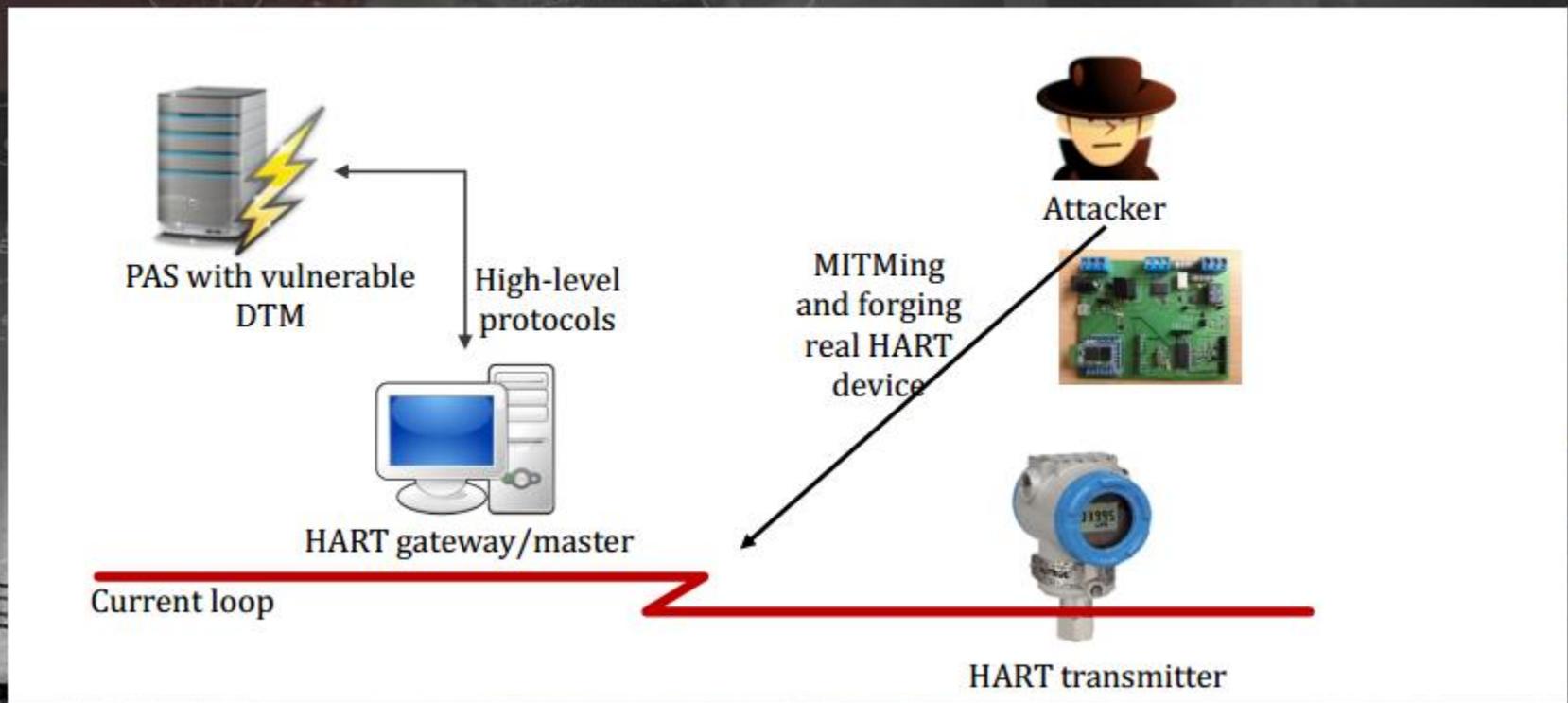
IDtm:ReleaseCommunication
IDtm:SetCommunication
communication set

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

<https://www.blackhat.com/docs/eu-14/materials/eu-14-Bolshev-DTM-Components-Shadow-Keys-To-The-ICS-Kingdom.pdf>

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

Attack model 1: through current loop



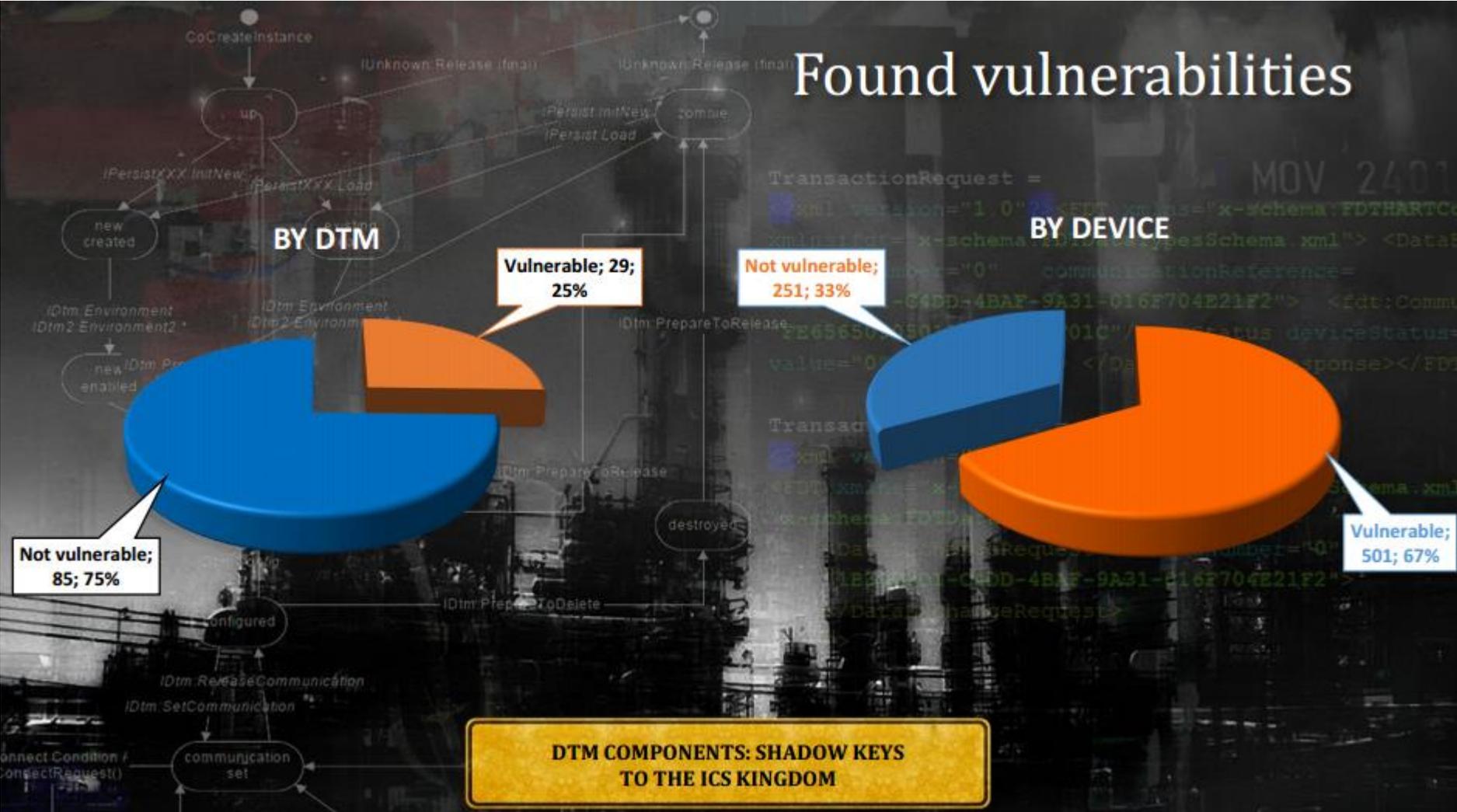
DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Bolshev-DTM-Components-Shadow-Keys-To-The-ICS-Kingdom.pdf>

DTM COMPONENTS: SHADOW KEYS TO THE ICS KINGDOM



<https://www.blackhat.com/docs/eu-14/materials/eu-14-Bolshev-DTM-Components-Shadow-Keys-To-The-ICS-Kingdom.pdf>

Hack your ATM with friend's Raspberry Pi

- **Problématique** : à quel point il est difficile d'accéder à l'intérieur d'un distributeur automatique de billets ?
- ATM avec **deux zones principales** : une zone de service et une zone « safe »
- Possible de crocheter la serrure facilement et d'introduire un **Raspberry Pi** directement dans le distributeur de billets. Le Raspberry Pi est connecté à l'ordinateur et est accessible à distance.
- **Démo** : l'ordinateur qui gère le distributeur est un PC standard sous Windows XP, sur lequel aucune mise à jour n'est installée
 - Possible d'**exploiter des failles connues** s'il existe un accès réseau
 - **Compréhension du protocole utilisé** pour dialoguer avec le coffre-fort et ainsi **déclencher la distribution d'argent**.

Présenté par Alexey Osipov et Olga Lochetova



Pour résumer

- Attaque moins alambiquée qu'elle n'y paraît, et qui peut rapporter gros
- **Windows XP** n'est pas prêt de disparaître

Hack your ATM with friend's Raspberry Pi



SSL validation checking vs Go(ing) to fail

- **Faible « go to fail »** sur les terminaux iOS : une simple erreur dans le code a entraîné un **manque de validation des certificats SSL**
- **Exploitation** de cette faille : réaliser des attaques du type Man-in-the-middle en utilisant de faux certificats SSL
- **Solution pour vérifier l'implémentation** de la vérification des certificats SSL sans avoir accès au code source : « **SSL validation fuzzer** »
 - Outil placé entre la cible et un serveur de test
 - Certificats invalides générés à la volée afin d'évaluer si la vérification des certificats SSL est bien implémentée ou non côté client
- **De nombreuses applications bancaires testées** : nombre d'entre elles n'implémentent pas correctement la validation des certificats SSL

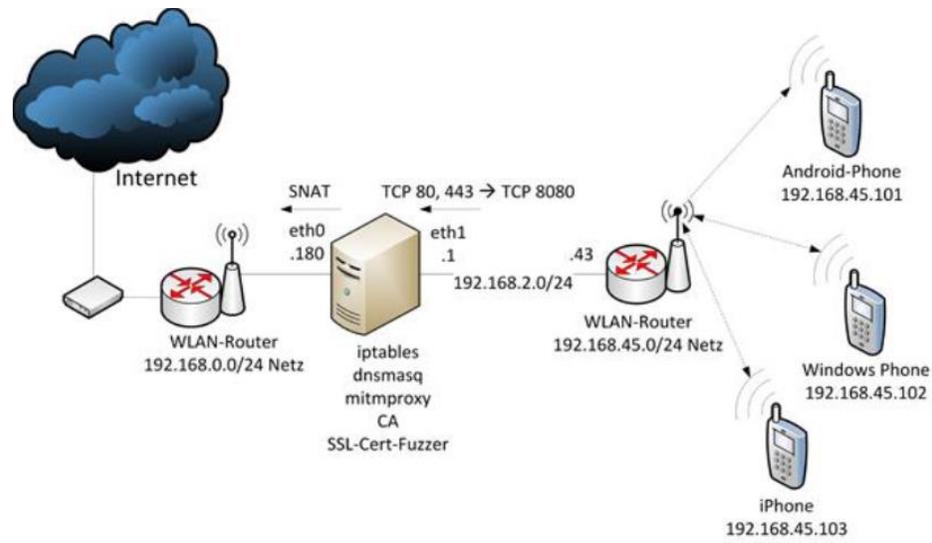
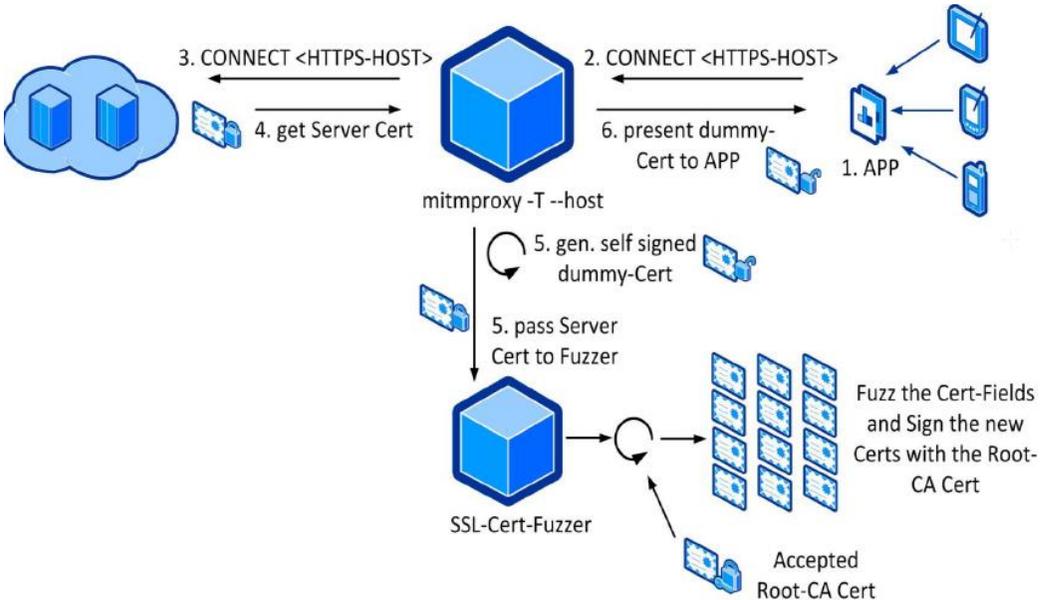
Présenté par Thomas Brandstetter



Pour résumer

- **Démarche** utilisée est **très intéressante**
- **Les développeurs** ne sont pas des spécialistes en cryptographie et **disposent de peu d'outils** ou guides complets pour implémenter correctement le protocole SSL

SSL validation checking vs Go(ing) to fail



LIMES SECURITY

Test cases! But which ones do make sense?
How twisted can a developer's mind be?

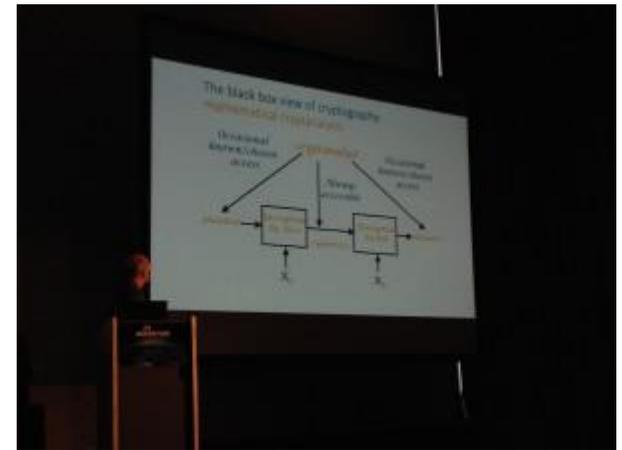
Ifh
st. pölten

| | | | |
|--|---|---|--|
| Case 1: arbitrary certificate | Case 2: valid certificate | Case 3: invalid notAfter | Case 4: invalid notBefore |
| Case 5: invalid Hostname, original serial no | Case 6: invalid signature, modified serial no | Case 7: invalid signature, original serial no | Case 8: not signed with key of CA |
| Case 9: issuer field of certificate does not match subject of CA | Case 10: hostname in subject field modified | Case 11: no hostname in subject field, subjectAltNameExtension on changed | Case 12: version 2 certificate with wrong hostname in subject field, correct one in subjectAltName-Extension |
| Case 13: certificate chain is extended with intermediate certificate | Case 14: incorrect intermediate-certificate (basicConstraints = CA:FALSE) | Case 15: tbd | |

List Initial test cases based on x509 standard certificate fields, In addition:
- SSL stripping
- Certificate pinning

Keynote présentée par Adi Shamir : Side channel attacks – Past, Present and Future

- Présentation de ses derniers travaux, concernant la **communication bidirectionnelle de longue distance** avec un ordinateur totalement isolé du réseau
- **Problématique** : comment communiquer avec un ordinateur compromis, mais totalement isolé du réseau ?
 - Utilisation d'une simple **imprimante/scanner** et d'un **laser** afin de communiquer à plus de 1200m de distance
 - Écriture d'un programme permettant au malware d'utiliser un scanner pour communiquer, via **l'émission et la réception de signaux lumineux**
- Possible **scénario d'attaque** : attendre que la victime lance un scan pour envoyer le message qui est alors scanné et visible sur les bords de la page. La malware est en mesure d'interpréter ce message et d'exécuter la commande demandée
- L'imprimante peut aussi être utilisée pour envoyer des données : technique « **SCANGATE** ».



Pour résumer

- Attaque relativement **difficile à implémenter** en pratique
- Pas nécessaire de jeter tous les scanners à la poubelle

Lights off! The darkness of the Smart Meters

Présenté par Garcia Illera et Javier Vazquez Vidal

- Sécurité des **compteurs intelligents** (*smart meters*) qui facilitent les opérations à distance et permettent d'adapter la production électrique à la demande en temps réel
 - Peuvent être accessibles à distance en utilisant les lignes électriques
 - Peuvent recevoir des commandes
 - Peuvent servir de relai pour transmettre des commandes à d'autres compteurs environnants
- **Analyse d'un compteur intelligent** déployé en Espagne et identification de l'utilisation de composants standards
 - De nombreux mécanismes de sécurité absents : SWD (*Serial Wire Debug*) activée
 - Clé AES identique pour l'ensemble des compteurs (sa connaissance permet l'envoi de commandes arbitraires aux compteurs)
- **Démo** : possibilité de modifier le contenu d'une puce mémoire permettant ainsi de désactiver une alarme qui se déclenche en cas d'ouverture du compteur
- **Scénario d'attaque** : reprogrammation distante des compteurs et propagation de ce code tel un ver sur le réseau électrique, par exemple pour couper le courant à l'ensemble de la population

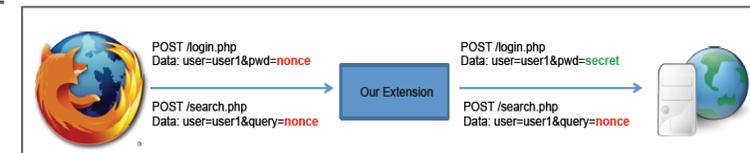
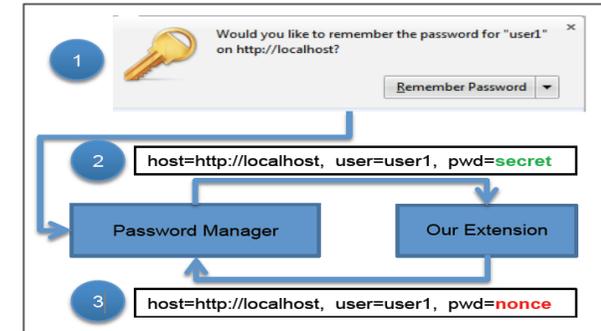
Pour résumer

- Évocation des problèmes liés aux **objets connectés** en général
- Vulnérabilités classiques, connues depuis des années et **trivialement exploitable**

Session identifiers are for now, passwords are forever – XSS based abuse of browser password manager

- Possibilité d'exploitation des XSS plus intéressante, permettant de **voler le mot de passe de l'utilisateur**
- **Cinq caractéristiques** des **password manager** testées sur cinq navigateurs différents (Internet Explorer, Google Chrome, Safari, Firefox et Opera) :
 - Correspondance de l'URL et du formulaire
 - Interaction de l'utilisateur
 - Attribut d'auto complétion
 - Remplissage automatique des champs
- Les comparatifs effectués ont montré qu'**Internet Explorer** implémentait les **restrictions les plus strictes**
- Impact de ces attaques d'autant plus grave que le mot de passe peut être récupéré **que l'utilisateur soit authentifié ou non**
- **Solution** : le mot de passe devrait être envoyé directement au serveur et ne devrait pas être inséré dans le formulaire. Un nonce devrait être utilisé dans les requêtes POST et l'URL devrait être vérifiée.

Présenté par Sebastian Lekies et Ben Stock



Pour résumer

- **Internet Explorer** qui sort du lot, et dans le bon sens du terme
- Les recherches ont montré que **50% des mots de passe** étaient **transmis en HTTP**
- Une question émerge de cette réflexion : vaut-il mieux **utiliser un unique mot de passe**, ou multiplier les mots de passe selon le site web utilisé moyennant **un password manager peu sécurisé** afin de gérer cet ensemble ?

Un peu d'autopromo : mon workshop



Industrial Control Systems : Pentesting PLCs 101

- Environ 1h d'intro sur les SI industriels et les problématiques de sécurité associées
- Puis 1h de TP sur une maquette constituée de deux automates, avec une machine virtuelle préparée pour l'occasion et distribuée en début de workshop
- Les slides sont en ligne
 - <https://www.blackhat.com/docs/eu-14/materials/eu-14-Soullie-Industrial-Control-Systems-Pentesting-PLCs-101.pdf>
 - <http://fr.slideshare.net/arnaudsoullie/introduction-to-industrial-control-systems-icsv11>

WHAT IS WRONG WITH CURRENT ICS SECURITY?

- ORGANIZATION & AWARENESS
- NETWORK SEGMENTATION
- VULNERABILITY MANAGEMENT
- SECURITY IN PROTOCOLS
- THIRD PARTY MANAGEMENT
- SECURITY SUPERVISION

LAB SESSION #2: MODBUSPAL

- Modbuspal is a modbus simulator
 - \$ > java -jar ModbusPal.jar
- Add a modbus slave
- Set some register values
- Query it with:
 - MBTGET Perl script
 - Metasploit module
- Analyze traffic with Wireshark

WHAT CAN WE DO ABOUT IT?

It's difficult, but not all hope is lost.

- NETWORK SEGMENTATION**
 - Do not expose your ICS on the Internet
 - Do not expose all of your ICS on your internal network
 - Use DMZ / Data diodes to export data from ICS to corporate network
- PATCH WHEN YOU CAN**
 - Patching once a year during plant maintenance is better than doing nothing.
- APPLY CORPORATE BEST PRACTICES**
 - Change default passwords
 - Disable unused services
- SECURITY SUPERVISION**
 - IPS have signatures for ICS
 - Create your own signatures, it is not that difficult

Y U NO SECURE ICS ?

THE COST IS TOO DAMN HIGH !

The power of simplicity
«*Ce qui est simple est fort*»



www.solucom.fr

Contact

Arnaud SOULLIE
Consultant sénior

Mail : arnaud.soullie@solucom.fr