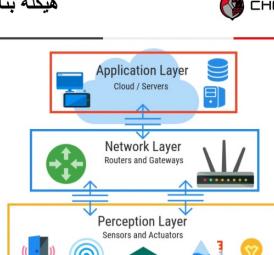
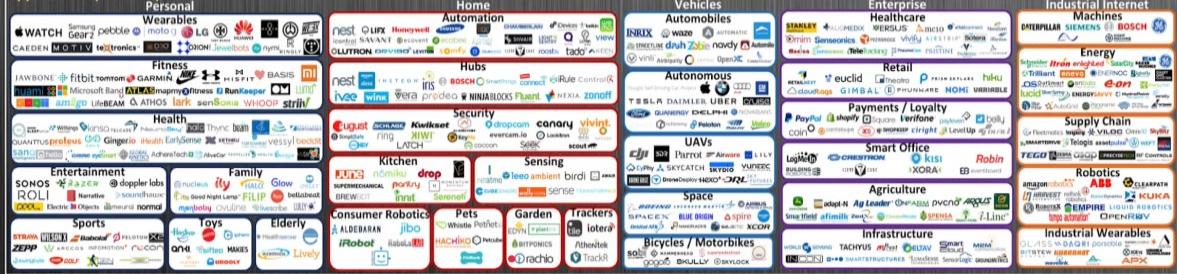


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دوره حیاة إنترنت الأشياء	
التحول	جمع البيانات
انشاء معلومات مفيدة من البيانات مثل تقارير.	جمع البيانات عن طريق الأجهزة وحساسات الاستشعار من اي مكان مثلًا من المنزل . السيارة، المكتب المصعد
تصنيف البيانات	
الغفل	التواصل
القائم بعمل معين بناء على البيانات والمعلومات المستلمة من الاجهزة مثل اتصال جهاز اخر.	ارسال البيانات عبر شبكات الاتصال لمراكز استقبال البيانات مثلًا داخل الحوسنة السحابية او مركز البيانات او شبكة المنزل الذكي
ارسال المعلومات الى جهاز معين تلقائيًا، تتضمن البيانات، إيقاف الطبيعة وغيرها	
هيكلة بناء إنترنت الأشياء	
التحول	CHC v2
نوع مجموعة مختلفة من التطبيقات المستخدمين	
تقنيات إنترنت الأشياء	
ادارة الاجهزة وادارة البيانات	
الاتصال بين الاجهزة	
بروتوكولات الارسال والترجمة	
اجهزه الاستشعار، الالات، الاجهزه، اجهزة التواصل التقنية بشكل عام	

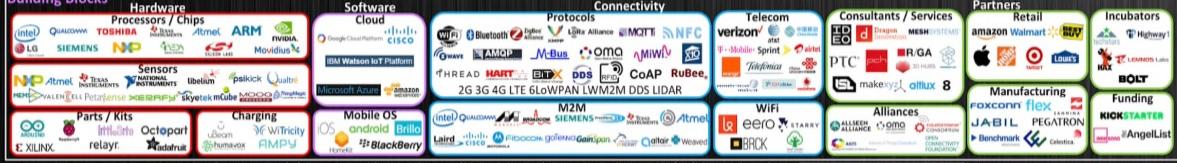
Applications (Verticals)



Platforms & Enablement (Horizontals)



Building Blocks



© Matt Turck (@mattturck), David Rogg (@davidjrogg) & FirstMark Capital (@firstmarkcap)

FIRSTMARK



أين يوجد إنترنت الأشياء

- التجارة والصناعة
- البيوت المراقبة
- البيوت الذكية والمعلمات
- الطاقة
- البنية والمعمار
- الصحة والعلوم
- النقل
- الزراعة وغيرها

مجالات إنترنت الأشياء في التطبيقات



تقنيات وبروتوكولات إنترنت الأشياء



العرب
بالإنجليزية

تقنيات وبروتوكولات إنترنت الأشياء

Major IoT Protocols

OSI Layers	Major IoT Protocols						
Application Presentation Session	HTTP + 5.25 + TCP based + Req/Resp	WebSocket + 52 + TCP based + Req/Resp + Pub/Sub	AMQP + 5.25 + TCP based + Pub/Sub	XMP + 5.25 + TCP based + Req/Resp + Pub/Sub	MOTT + DDS + TCP based + Req/Resp + Pub/Sub	CoAP + D2S + UDP based + Req/Resp	DDS + D2D + UDP based + Pub/Sub
Transport Network	http://						
Data Link Physical	TPC	IPv6	UDP	6LowPAN			
	Short Range	Long Range	Tethered				

تقنيات وبروتوكولات إنترنت الأشياء



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



العرب
بالإنجليزية



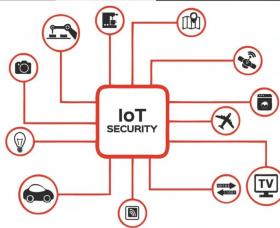
العرب
بالإنجليزية

العرب
بالإنجليزية

النحوات الذكى انتشاراً



OWASP Top 10 IoT Vulnerability and Obstacles

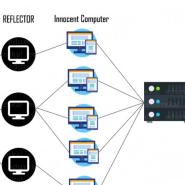


Insecure Web Interface

- معلومات الدخول الافتراضية
- عدم توفير إيقاف الحسابات المشبوهة
- CSRF, SQLI, XSS



OWASP Top 10 IoT Vulnerability and Obstacles



Insecure Network Services

- ثغرات هجوم Denial-of-Service
- UPnP اختراق منفذ
- المتلازمة المطلوبة الغير ضرورية



OWASP Top 10 IoT Vulnerability and Obstacles



Privacy Concerns

- الكثير من البيانات والمعلومات الشخصية يتم تجميعها
- بيانات المعلومات التي يتم تجميعها لا يتم إدارتها أو حفظها بشكل صحيح
- لابحث للمستخدمين السماح بجمع معلومات معينة فقط



OWASP Top 10 IoT Vulnerability and Obstacles



Insecure Mobile Interface

- عرض كلمات مرور ضعيفة
- عدم وجود ميزة إيقاف الحسابات المشبوهة
- عدم وجود تحفظ ثباتي



OWASP Top 10 IoT Vulnerability and Obstacles



Insufficient Authentication / Authorization

- طريقة استئناف كلمة المرور غير آمنة
- كلمات المرور الضعيفة
- عدم وجود التحقق الثنائي

Password *

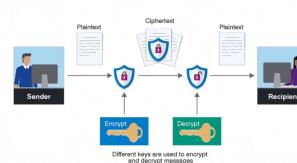
Password strength: Weak



OWASP Top 10 IoT Vulnerability and Obstacles



Lack of Transport Encryption/Integrity Verification



OWASP Top 10 IoT Vulnerability and Obstacles



Insecure Cloud Interface

- لا يوجد مراجعة لثغرات واجهات الحماية والأمان
- عرض كلمات مرور ضعيفة
- عدم وجود تحفظ ثباتي



OWASP Top 10 IoT Vulnerability and Obstacles



Insufficient Security Configurability

- عدم وجود خيارات لتحمية كلمة المرور
- عدم وجود خيارات التشفير
- عدم وجود خيار للدخول الآمن للحساب





Insecure Software/Firmware

- تحديثات الخوادم بشكل غير آمن
 - تحديثات الاجهزة الغير مسجلة
 - تحديثات الاجهزة الغير مشفرة



OWASP Top 10 IoT Vulnerability and Obstacles

Poor Physical Security

- منافذ لا حاجة لها مثل منفذ USB
 - الدخول على نظام التشغيل عبر التحكم بالوسائط
 - لا يوجد صلاحيات للحد من القراءة الإدارية

مُنظَّماتِ الدِّينِ

طرق اختراق IoT



الحفظ على الاختراق

لدخول على الجهاز

الجهوم

فحص الثغرات

جمع المعلومات

جمع المعلومات

الخطوة الأولى في اختراق أجهزة إنترنت الأشياء، هو جمع المعلومات مثل IP و الملفات المترافق، والبروتوكولات، وإنواع الأجهزة والتوكين، وشركة التصنيع ورقم التصنيع وغيرها ملخص معلومات

الجهات

طرق اختراق IoT



التدريب

بدر المصطفى



#CHC



digital footprint

عن طرق موجهة

www.CHC-course.com

52

#CHC_Course

فحص الثغرات

الخطوة الثانية في اختراق أجهزة إنترنت الأشياء، هي فحص الثغرات بمساعدة المخترق في التعرف على جهاز إنترنت الأشياء من خلال الضغط الموجود في اعدادات الجهاز مثل: الثغرات المفتوحة، خلل في المتصفح التطوير، ضعف في الاعدادات او كلمات المرور، ضعف في التشفير بالتوصل وغيرها

nmap . . .

www.CHC-course.com

54

#CHC



التدريب

بدر المصطفى

طرق اختراق IoT



#CHC_V2

الهجوم

الخطوة الثالثة في اختراق أجهزة إنترنت الأشياء، هي الثغرات التي يتم الوصول إليها يتم استغلالها في الهجوم ويوجد عدة أنواع للهجوم ومنها

,DDoS, Rolling code, Jamming Signal, Sybil, MITM

طرق اختراق IoT



التدريب

بدر المصطفى



#CHC

دخول على الجهاز



الخطوة الرابعة في اختراق أجهزة إنترنت الأشياء، هي حسب الهجوم الذي يتم عن طريق المخترق، سوف يقوم المخترق بتحويل الجهاز إلى لدخول الجهاز والوصول لنسيمة الشركة مع عدم التواصل أو التفاعل مع اي جهاز اخر تختوي على برامج حماية او جدار ناري او غيرها

www.CHC-course.com

57



التدريب

بدر المصطفى

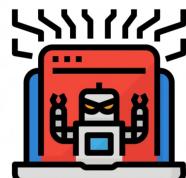
طرق اختراق IoT



#CHC_V2

الحفظ على الانترنت

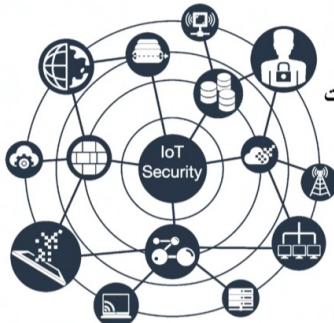
الخطوة الأخيرة في اختراق أجهزة إنترنت الأشياء، في هذه المرحلة يقوم المخترق في حذف الأنتر حتى لا يتم التعرف على وجوده داخل النظام او الشبكة، ويقوم باستخدام فيروسات سامحة على الحفاظ على الاختراق



www.CHC-course.com

58

#CHC_Course



- تطوير نظام الحماية للنظام
- تفعيل العنوان الآمن للوصول للجهاز من الانترنت
- تعطيل منفذ telnet على المنفذ 23
- تعطيل منفذ UPnP في الراوتر
- تحديث البرامج وإغلاق المنافذ وترقيع الثغرات
- متابعة حزم البيانات في المنفذ 48101
- إيقاف الحسابات التجريبية والدخول كزائر إلى نظام الجهاز إنترنت الأشياء
- استخدم ميزة القفل الآمن للحسابات في حالة تكرار محاولات الدخول المشبوهة
- تطوير وتفعيل طرق التحقق
- تفعيل الجدار الناري في شبكة العمل
- تفعيل برامج الحماية IPS و IDS في الشبكة
- تطوير طريقة التشفير end-to-end و Public Key Infrastructure
- استخدام VPN للتواصل الآمن

دليل الحماية لمصانع اجهزة IoT



- التأكد من الجهاز بشكل دوري بعدم وجود أي أدوات غير مستخدمة او عدم تفعيل التنصاصير الادوات والبرامج الغير هامة
- استخدام نظام أمن للتحقق من جميع البرامج المستخدمة في الجهاز
- استخدام SSL/TLS لحاجة التواصل
- التحفيز على استخدام كلمات المرور القوية
- التأكد من شهادة SSL
- تحديثات الجهاز يجب ان تكون بسيطة وآمنة للثقة المستفیدین
- تطوير نظام القفل الآمن بعد محاولات الدخول المتكررة للحسابات المشبوهة للحماية ضد brute force attack
- قفل الجهاز في اي حالة واي مكان معرض للهجوم