XGen™

萬物聯網之下的資訊安全隱憂

林政君 (Sylph Lin)
Solution Architect, Trend Micro

TREND MICRO™

關於我

林政君 (Sylph Lin)

Solution Architect

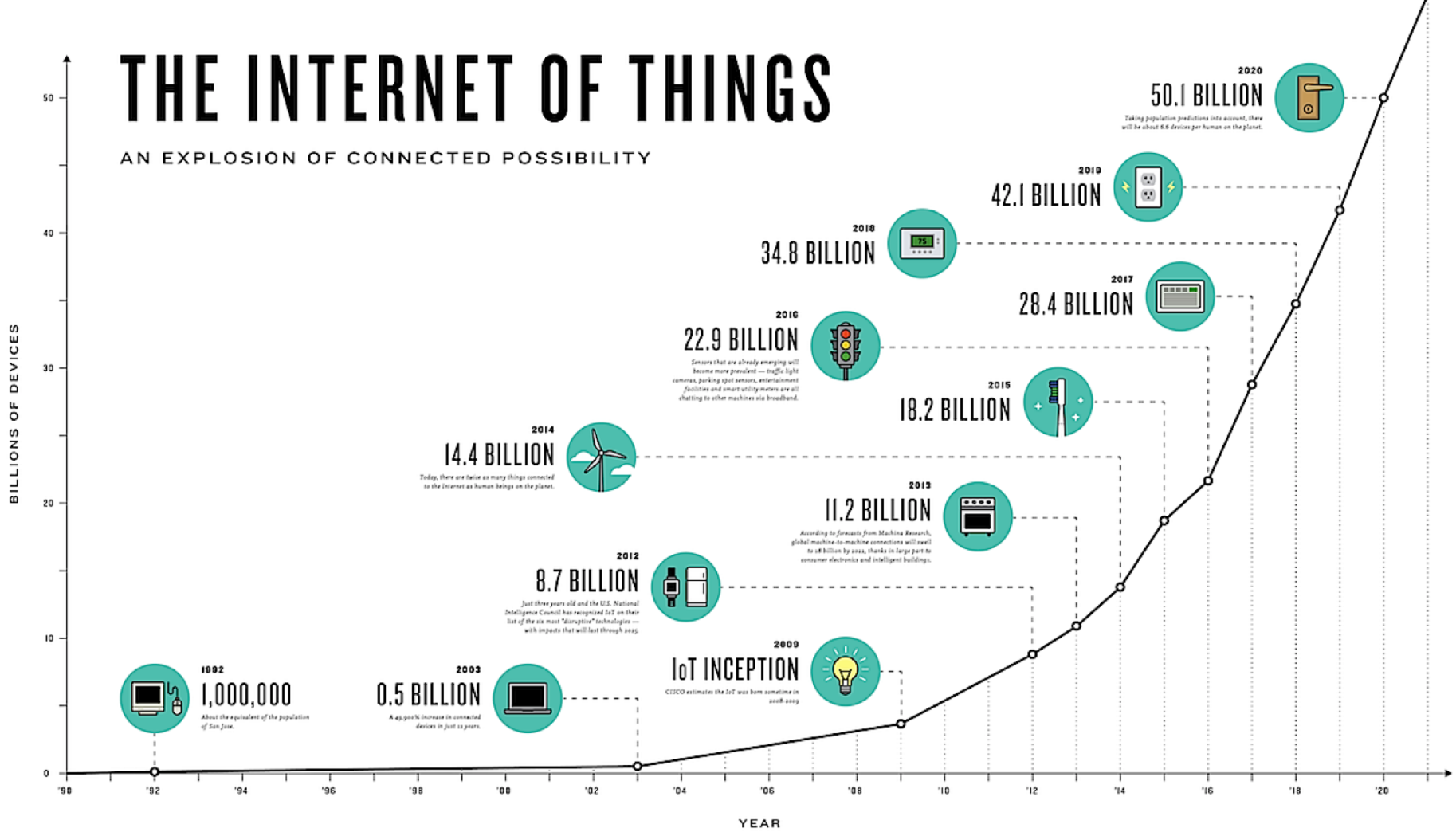
聯網設備產品經理

聯網設備軟體架構規劃

智慧裝置技術顧問

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY



美麗新世界！

你的一舉一動可能都暴露在別人的目光下

Insecam Project

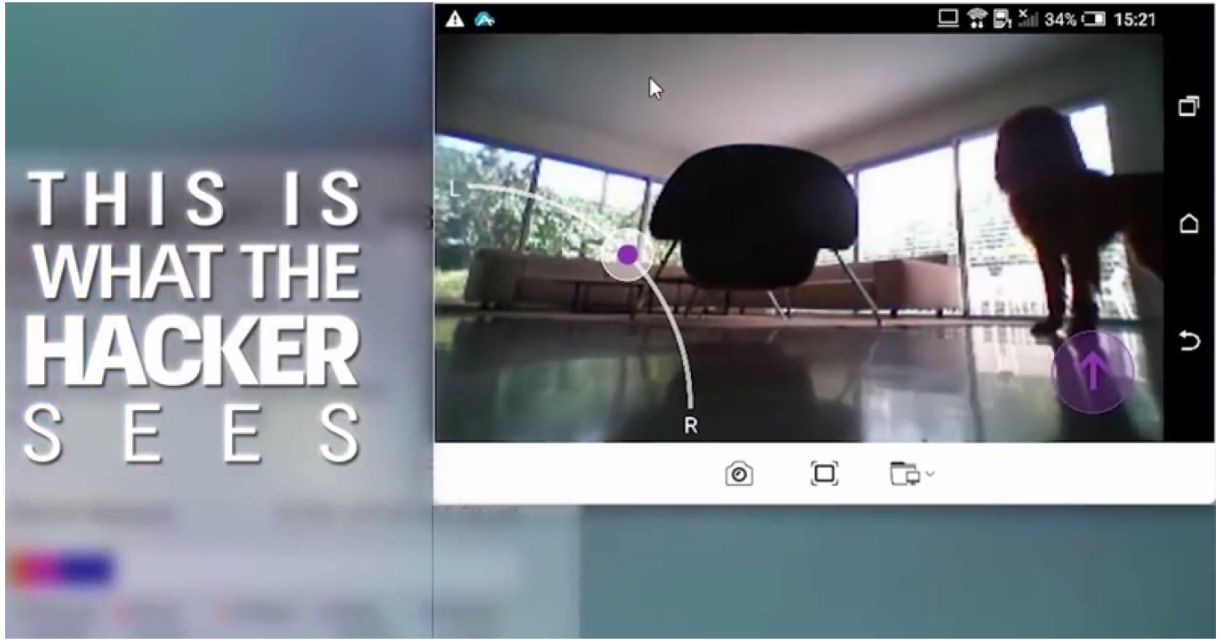
Watch Panasonic camera in Korea, Republic Of,Busan

Watch Panasonic camera in Japan,Tokyo

Watch Vivotek camera in Australia,Sydney

https://www.insecam.org

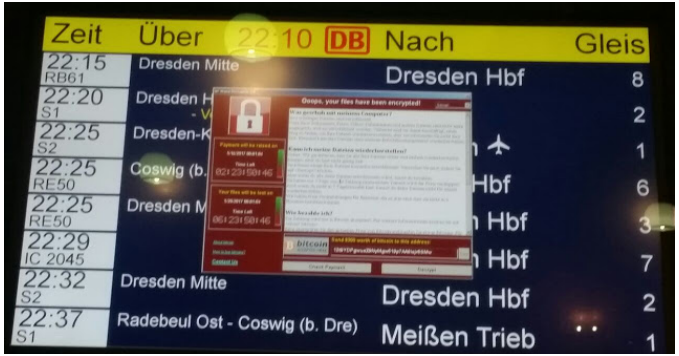
你的一舉一動可能都暴露在別人的目光下



也會造成生活上的不便

ATM

Digital Signage in Bangkok



Train Information Display

或造成財務上的損失 (ATM Jackpotting)

主頁 即時 日報 動新聞 搜尋

蘋果即時 最新 焦點 熱門 娛樂 愛播網 社會 國際 政治 生活 火線 3C 動物 副刊

步第一銀行盜領案後塵　美國也有ATM遭駭客入侵

3699 出版時間：2018/01/29 01:47

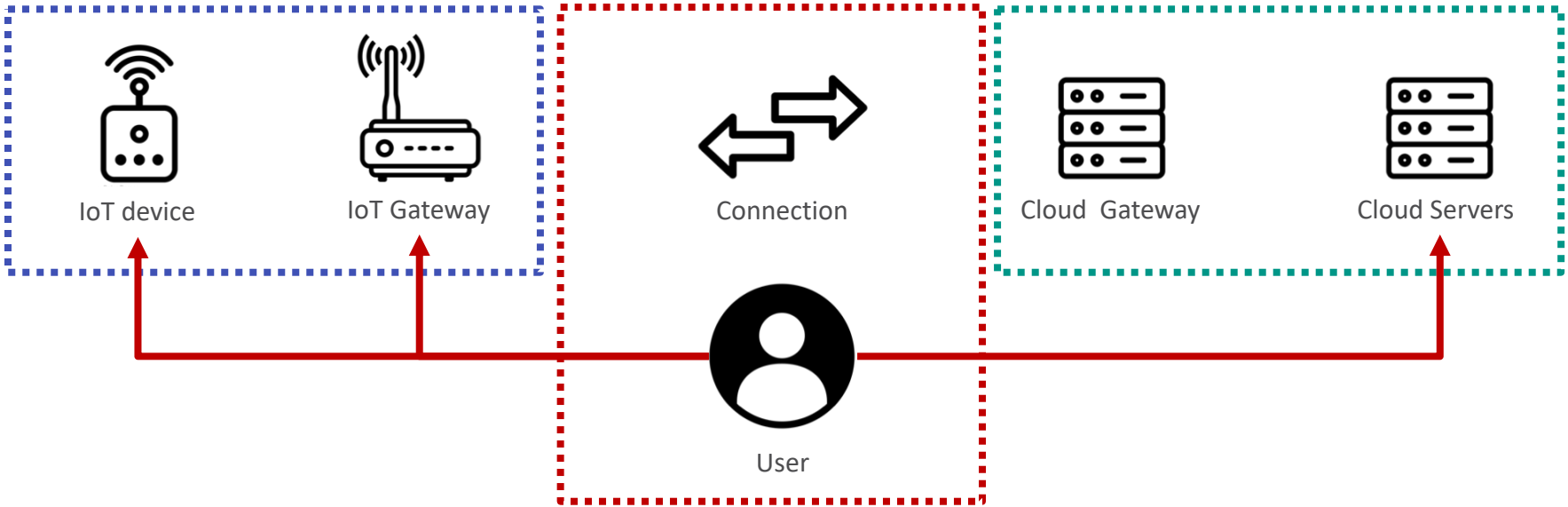
美麗新世界？

Internet of Things

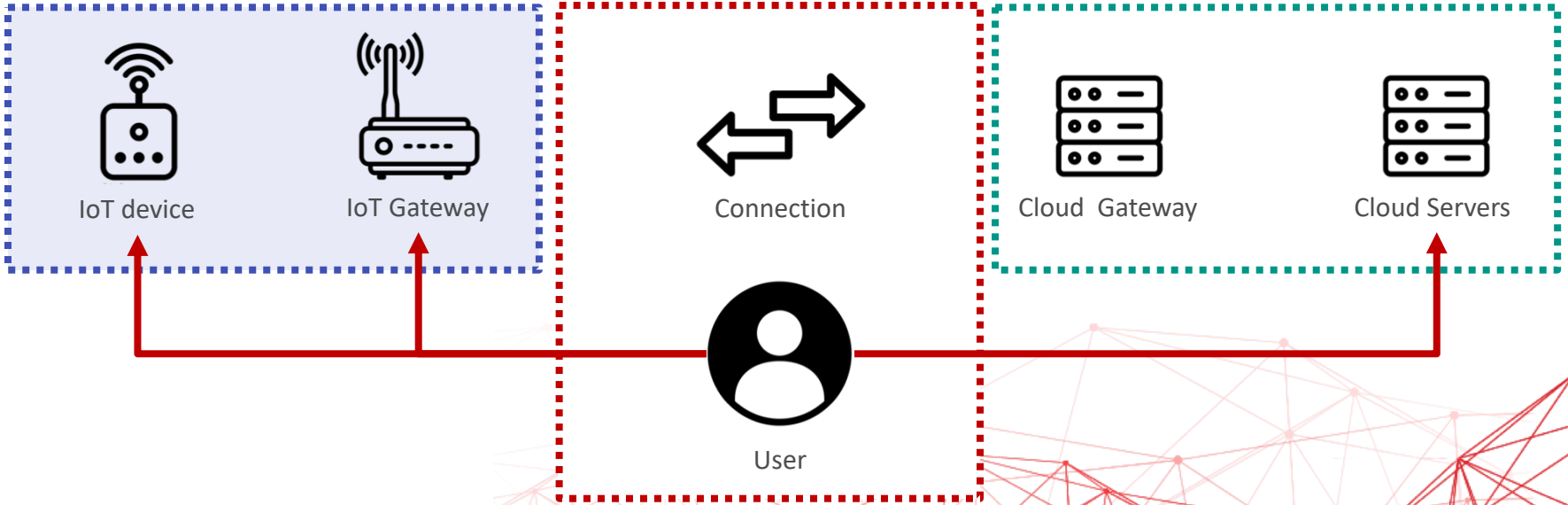
Threats

IoT Threat Modeling

物 聯 網



物 聯 網


IoT device
IoT Gateway
Connection
Cloud Gateway
Cloud Servers
User

裝置的預設密碼

Insecure Way

- 使用預設的系統密碼
  - admin / admin
  - cisco / sanjose
  - root / r00t
- 延伸問題
  - Insecam Project
  - Mirai

Suggested Way

- 強迫使用者必須在安裝流程裡變更系統密碼

Insecam

你的一舉一動可能都暴露在別人的目光下

Watch Panasonic camera in Korea, Republic Of,Busan

Watch Panasonic camera in Japan,Tokyo

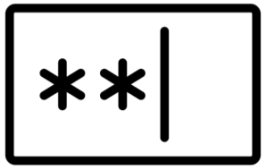
Watch Vivotek camera in Australia,Sydney

https://www.insecam.org

LG

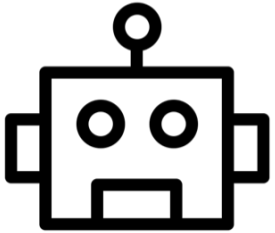
Mirai (ミライ)

IP Scan



Try Password by Telnet

Infection



Botnet

2016年10月21日
Dyn公司提供的DNS服務遭到了數次通過Mirai發起的大型DDoS攻擊，牽涉到的受感染物聯網裝置數量眾多。這次攻擊使得數個高瀏覽量的網站無法正常開啟，其中包括GitHub、Twitter、Reddit、Netflix和Airbnb等

永不更新的韌體

Insecure Way

- 不要去踢睡著的獅子
- 沒事不更新，不更新沒事

Suggested Way

- 手動升級的提醒介面
- OTA自動升級
- 保留完整的韌體升級路線
- 雙韌體設計，避免更新失敗
- 產品生命週期管理

沒有驗證收到的資訊或命令

Insecure Way

- GPS竄改
- 偽造伺服器端命令
- 惡意的韌體

Suggested Way

- 利用融合定位輔助
- 命令簽章
- 韌體驗證

沒有物理安全防護

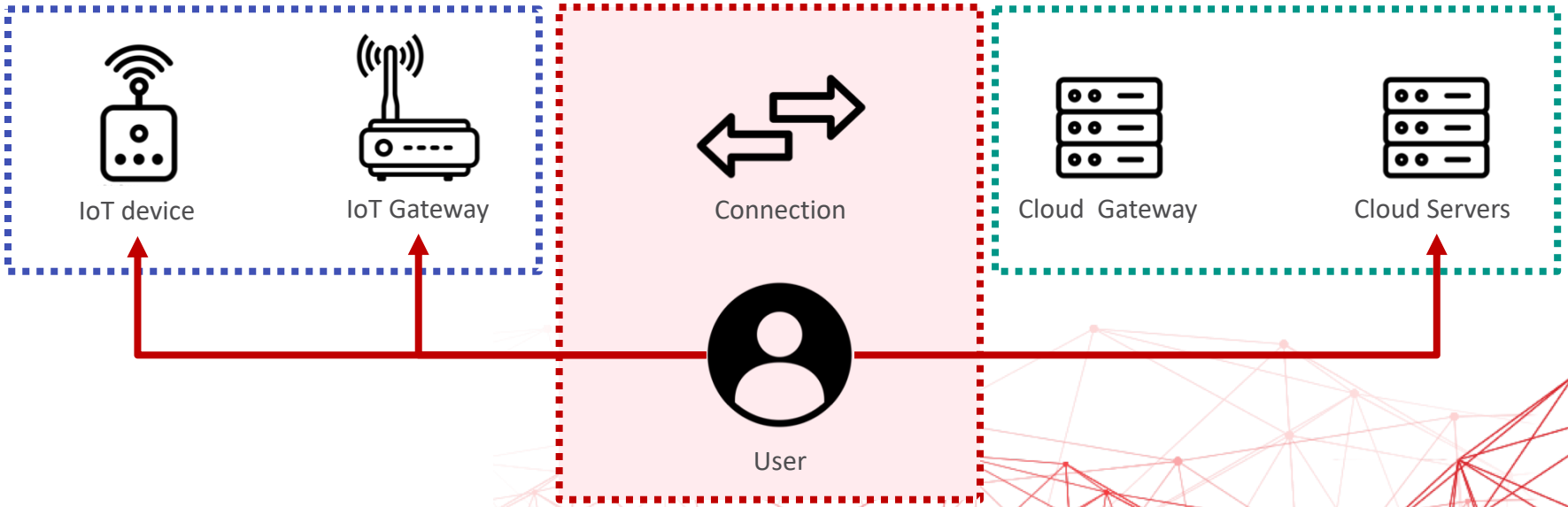
Insecure Way

- 不必要或外露的接口
- 容易被取下並竄改

Suggested Way

- 透過機構設計來保護接口
- 移動感應監測
- 自毀設計

物 聯 網


IoT device
IoT Gateway
Connection
Cloud Gateway
Cloud Servers
User

不安全的配對方法

Insecure Way

- MAC Address配對
- 貼在外包裝盒的配對ID
- 沒有檢查機制

Suggested Way

- UID+檢查碼
- 動態QR Code配對
- 設備憑證配對

使用未加密的傳輸通道

Insecure Way

- 使用沒有加密的通道傳輸設備操作命令 (Telnet, HTTP, SNMP)

Suggested Way

- 使用加密通道傳輸設備操作命令 (SSH, HTTPs, SNMPv3)
- TLS/SSL通道

使用不安全的加密演算法

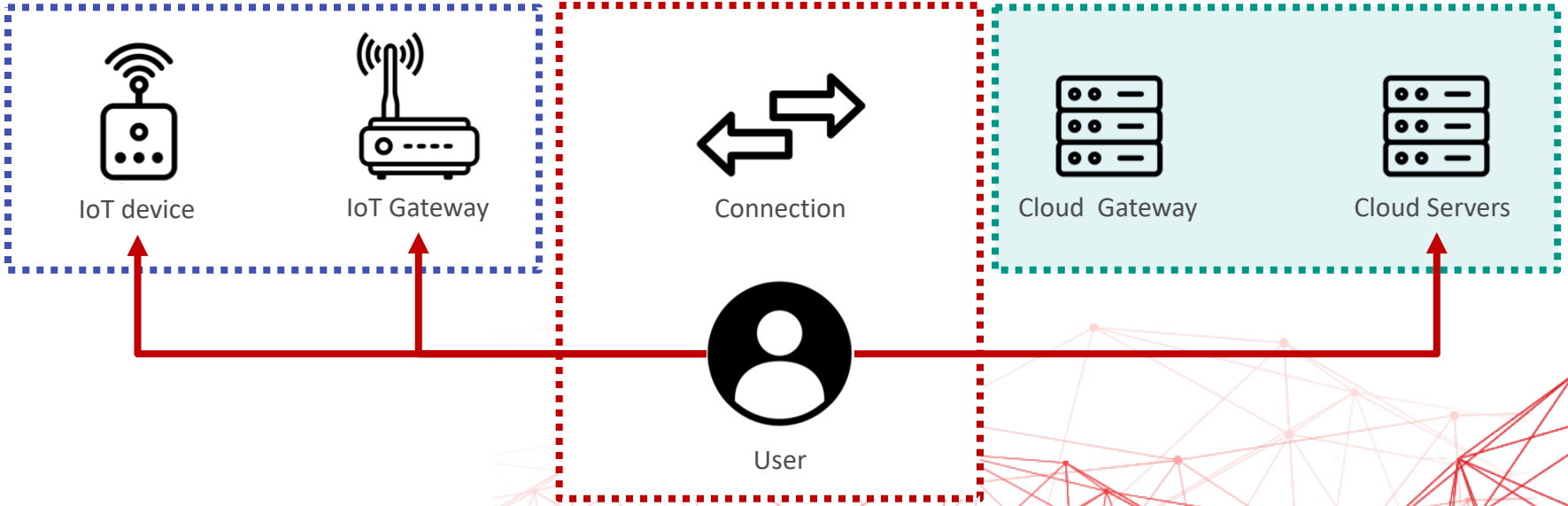
Insecure Way

- 使用已被攻破或已被證實不安全的加密和雜湊演算法

Suggested Way

- 使用正向表列的加密演算法
- **SSL and TLS Deployment Best Practices (SSL Lab)**
- **Recommendation for Applications Using Approved Hash Algorithms (NIST)**

物 聯 網


IoT device
IoT Gateway
Connection
Cloud Gateway
Cloud Servers
User

缺乏設備驗證

Insecure Way

- 沒有驗證設備身份
- 設備送上來的訊息照單全收

Suggested Way

- 透過設備憑證驗證
- 監控重複設備

脆弱的使用者密碼

Insecure Way

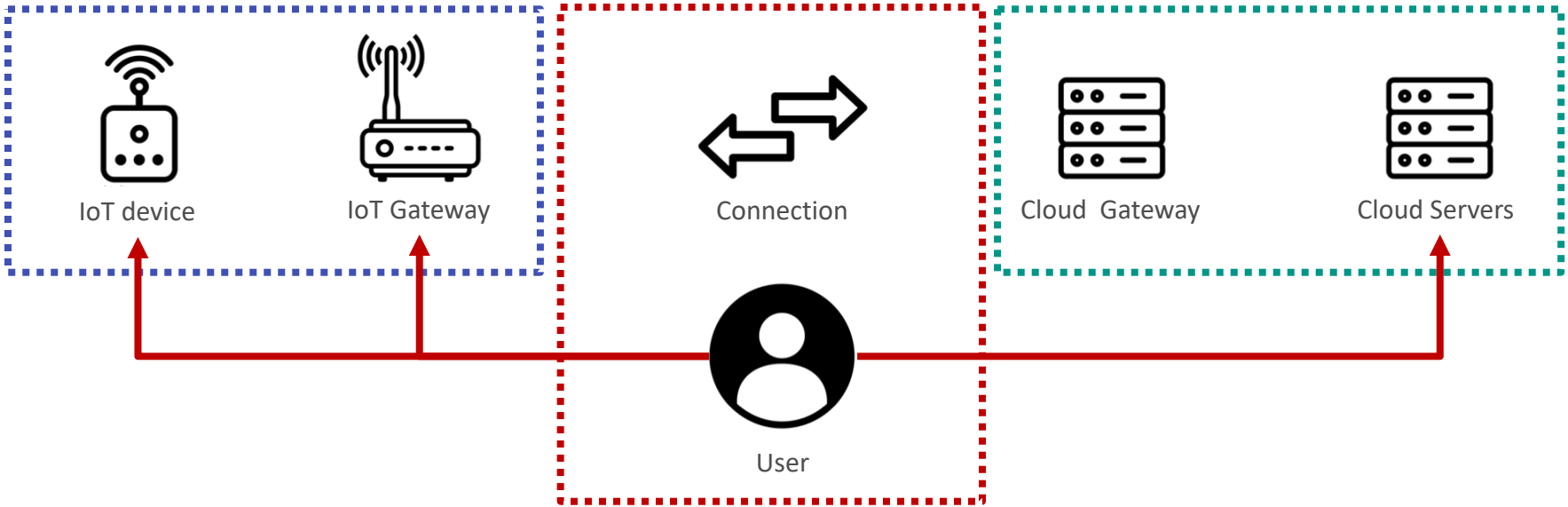
- 使用超短密碼
- 使用常見的已知密碼
- 延伸問題
  - 字典法攻擊
  - 暴力法攻擊

Suggested Way

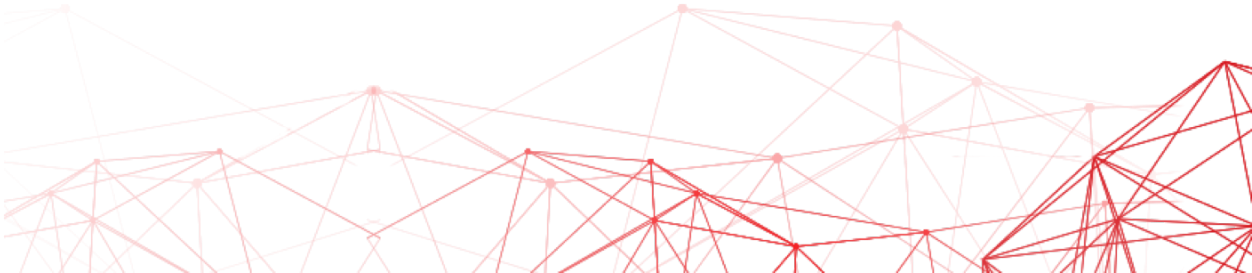
- 增加密碼長度
- 禁用常用的已知密碼
- 多重驗證 (MFA)
- Digital Identity Guidelines (NIST, 800-63B)

IoT Threat Modeling

物 聯 網



安全從來不是一件輕鬆的事
但是...



但這就是專業和業餘的差別...

專業的賽車駕駛，不但會繫上安全帶，還會穿上任何能夠保護他們的裝備

但是一般人卻會覺得安全帶很不舒服，而不想用

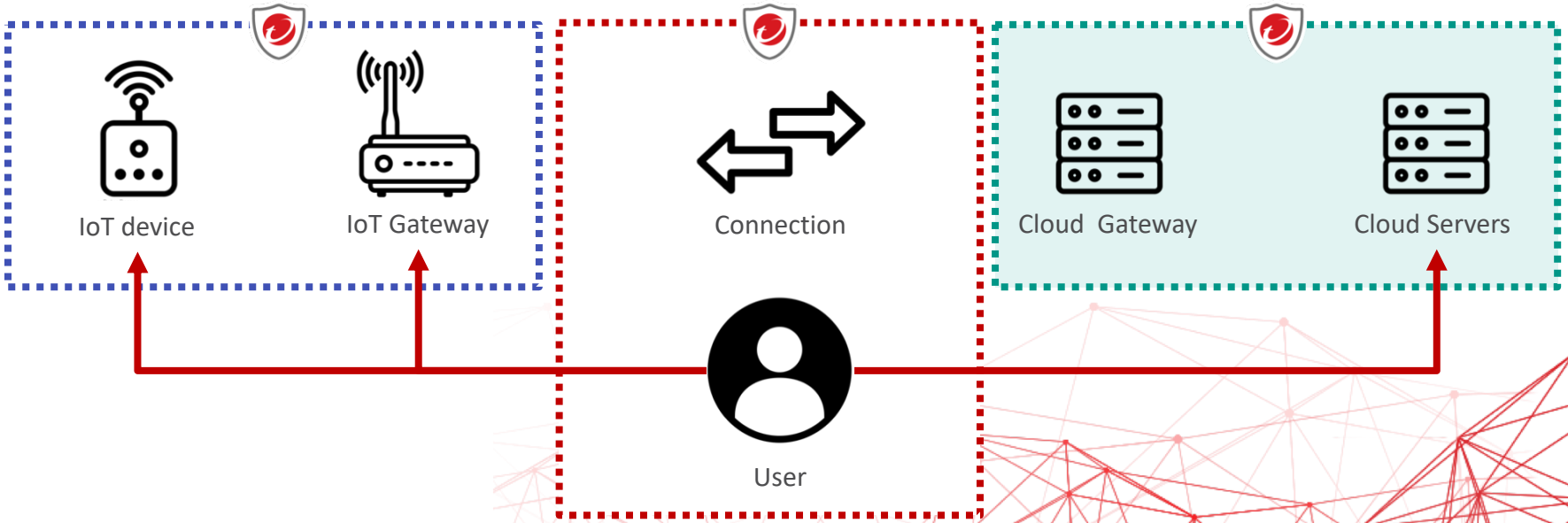
TREND MICRO

TMIS Agent/SDK

Tipping Point
Cloud Edge
Virtual Network Function Suite
Deep Discovery

Deep Security

物 聯 網



Thank You