讓物聯網安全「硬」起來 IoT裝置的資訊安全解方

高傳凱 博士

資策會資安所 副主任

資安檢測鑑識實驗室 技術主管

高傳凱

資策會 資安所 產業資安發展中心副主任
TAICS TC Network and Security WG1 組長
資策會 資安檢測鑑識實驗室 技術主管

+886-0955216185
marskao@iii.org.tw

國立成功大學 電腦與通信工程研究所 博士

專長：物聯網設備資安檢測、資安標準研擬

願景：期待資安所成為資安研發的前導角色、政府資安政策的先鋒，帶動國家資安產業量能

- **榮譽**
  - 2020 建構全國第一個資安國際交互認證體系(ISASecure)
  - 2019 資策會資安所績優人員 技術菁英獎
  - 2019 卓越計畫貢獻獎
  - 2017~present 影像監控系列、智慧巴士系列、智慧路燈系列資安標準制定
  - 2017 IEEE 論文審查委員

心法1：安全無絕對，只有風險高與低

Likelihood

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	>10^{-1} per year (High demand)
2	Likely	Likely to occur	10^{-1} to 10^{-3} per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^{-3} to 10^{-4} per year
4	Unlikely	Conce	
5	Remote	So unl	

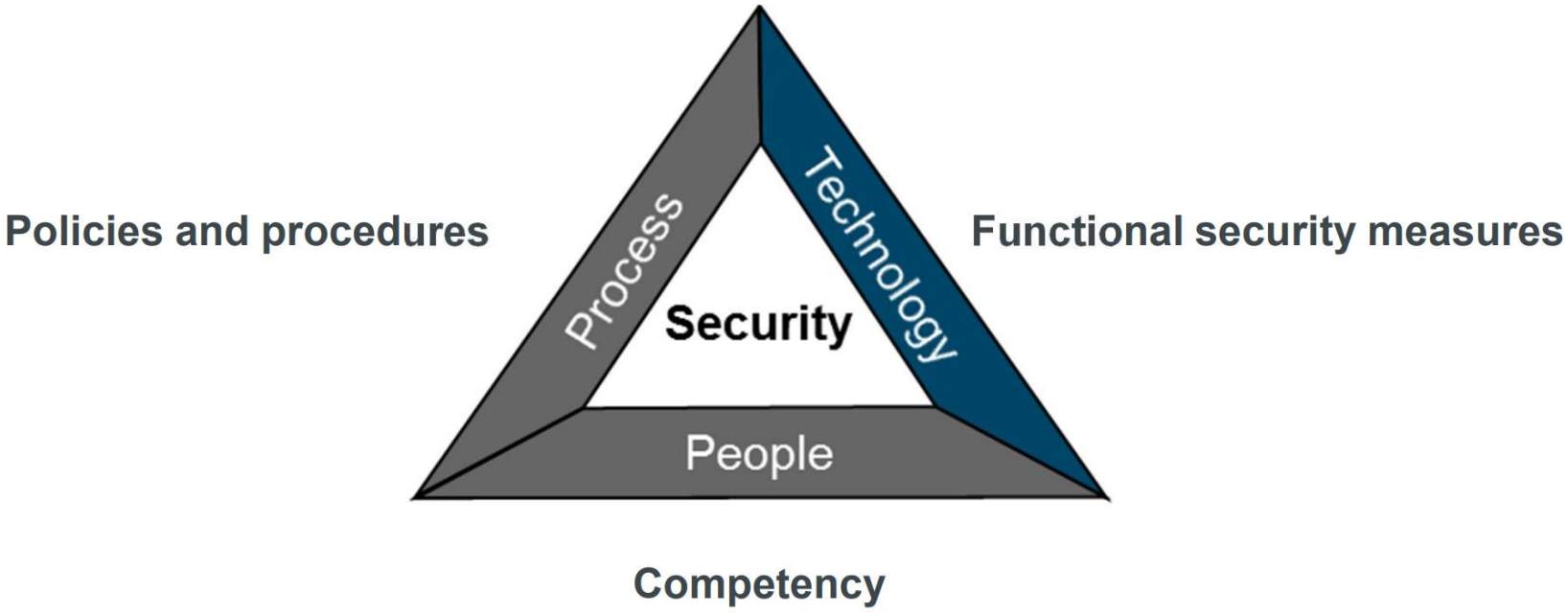
Impact

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or	No complaints	Small, contained

Risk

Likelihood				
	Highly likely	Medium	High	High
	Possible	Low	Medium	High
	Unlikely	Low	Low	Medium
		Negligible	Moderate impact	Severe

心法2：資安是技術、程序、人



Source: Siemens

心法3：比起防禦，韌性更適合資安

築高牆，防止惡意人士

隨侍在身，隨時監控

每個人心目中的資安事件

Twilio、Cloudflare員工遭網釣攻擊的事故，疑與鎖定Okta用戶的大規模攻擊行動有關

雲端服務業者Twilio、Cloudflare先後表示因員工遭到網釣簡訊攻擊，而導致公司遭到攻擊的情況，如今有資安業者指出，這很可能只是大規模攻擊行動的冰山一角。

資安業者Group-IB揭露名為0ktapus的網路釣魚攻擊，駭客自今年3月開始，鎖定使用Okta身分驗證解決方案的企業下手，駭客不只試圖取得用戶帳密，還有雙因素驗證（2FA）的驗證碼並用於第二階段的攻擊行動。

總共有130個組織受害，攻擊者竊得近1萬筆帳密資料，逾半數（5,503筆）在美國。研究人員指出，Twilio、Cloudflare遭到攻擊，以及行銷管理業者MailChimp、Klaviyo的事故，都與0ktapus攻擊行動有關。

Source: iThome

南歐蒙特內哥羅當地政府疑遭勒索軟體Cuba攻擊

8月26日，蒙特內哥羅的政府系統與關鍵基礎設施遭到網路攻擊，美國大使館指出這起事故可能會擾亂當地交通、公營事業、以及電信服務的運作，蒙特內哥羅指控俄羅斯駭客組織所為。

英國NHS的MSP業者Advanced證實遭到勒索軟體攻擊，111系統停擺

英國NHS的111緊急通報系統於8月5日傳出服務中斷，起因與代管服務業者Advanced遭到攻擊有關，此業者於10日提出進一步說明。Advanced表示，他們約於8月4日上午7時遭到勒索軟體攻擊，共有7款產品的用戶受到影響，該公司委

歐洲大型能源業者Encevo遭到勒

勒索軟體駭客組織BlackCat攻擊行動頻

據新聞網站Dark R

發布公告，旗下的

到網路攻擊，駭客

所為，總共竊得15

因網路攻擊而中斷

智利證實政府機關遭勒索軟體攻擊，部分服務被迫中斷

智利電腦緊急應變小組（CSIRT）發布資安通告，指出當地政府機關於8月25日遭到勒索軟體攻擊，駭客針對Windows伺服器與VMware ESXi伺服器下手，將事件記錄檔案LOG、可執行檔EXE、程式庫DLL，以及多種ESXi檔案（vmdk、vmsn、vmem等）進行加密，導致該國政府機構的營運受到影響。

而對於攻擊來源，智利電腦緊急應變小組認為有可能與勒索軟體RedAlert或是Conti有所關連，威脅情報分析師Germán Fernández表示，這很可能是過往未曾出現的勒索軟體駭客組織所為。

Source: iThome

7-11櫃臺後方數位看板的內容遭置換，刑事局調查指出是遭駭客入侵

美國聯邦眾議院議長裴洛西（Nancy Pelosi）昨晚抵臺後，今日早上許多民眾臉書分享在不同7-11便利商店，看到結帳櫃臺後方的廣告螢幕，播放「戰爭販子裴洛西滾出台灣」的影像，有民眾質疑是廣告還是被駭？對此事件，應是超商合作的聯播廣告商其檔案內容被置換，可能是數位電子看板的內容管理伺服器（CMR）主機遭入侵？或OPEN！CHANNEL聯播服務網權限遭接管？。後續，7-11表示由他們統一回應：「廠商受不明來源干擾播放訊息。」中央社報導指出，刑事局初步調查為駭客入侵。此外，新左營車站電子看板也遭駭客入侵備置換簡體中文內容。

Source: iThome

駭客究竟是怎麼做的?

＜因原資料機敏所以移除＞

晶片相關測項

安全功能/非安全功能保護

1. 在攻擊者損害任何安全功能及非安全功能前，可偵測或阻止具有物理存取的攻擊者的攻擊。
2. 測項： <基礎物理攻擊抵抗>、<進階物理攻擊抵抗>

封裝保護

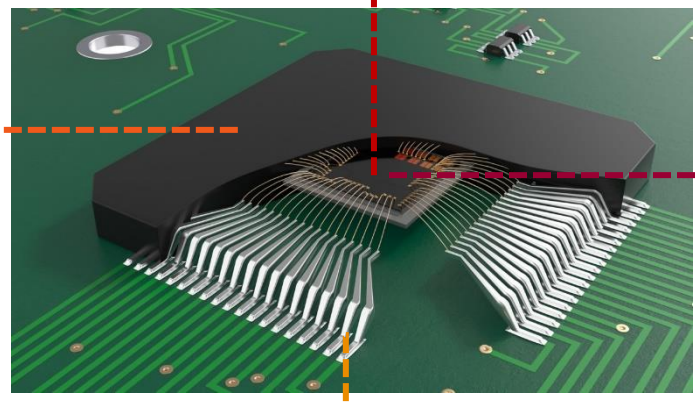
1. 驗證晶片密碼模組遭受竄改或移除時，是否保留竄改或移除之證據，及是否具有篡改回應紀錄。
2. 測項： <晶片密碼模組通用保護>、<晶片密碼模組基礎保護>及<晶片密碼模組進階保護>

除錯介面安全

1. 確保介面提供的服務不會遭到濫用，及除錯介面使用的身份驗證功能之安全性。
2. 測項： <安全除錯保護>、<安全除錯身份驗證>

晶片設計

1. 複雜的半導體供應鏈，可能導致晶片在設計過程中，遭受有心人士植入可疑電路，以便在某個時間點或條件下發動資安攻擊。
2. 測項： <可疑電路測試>



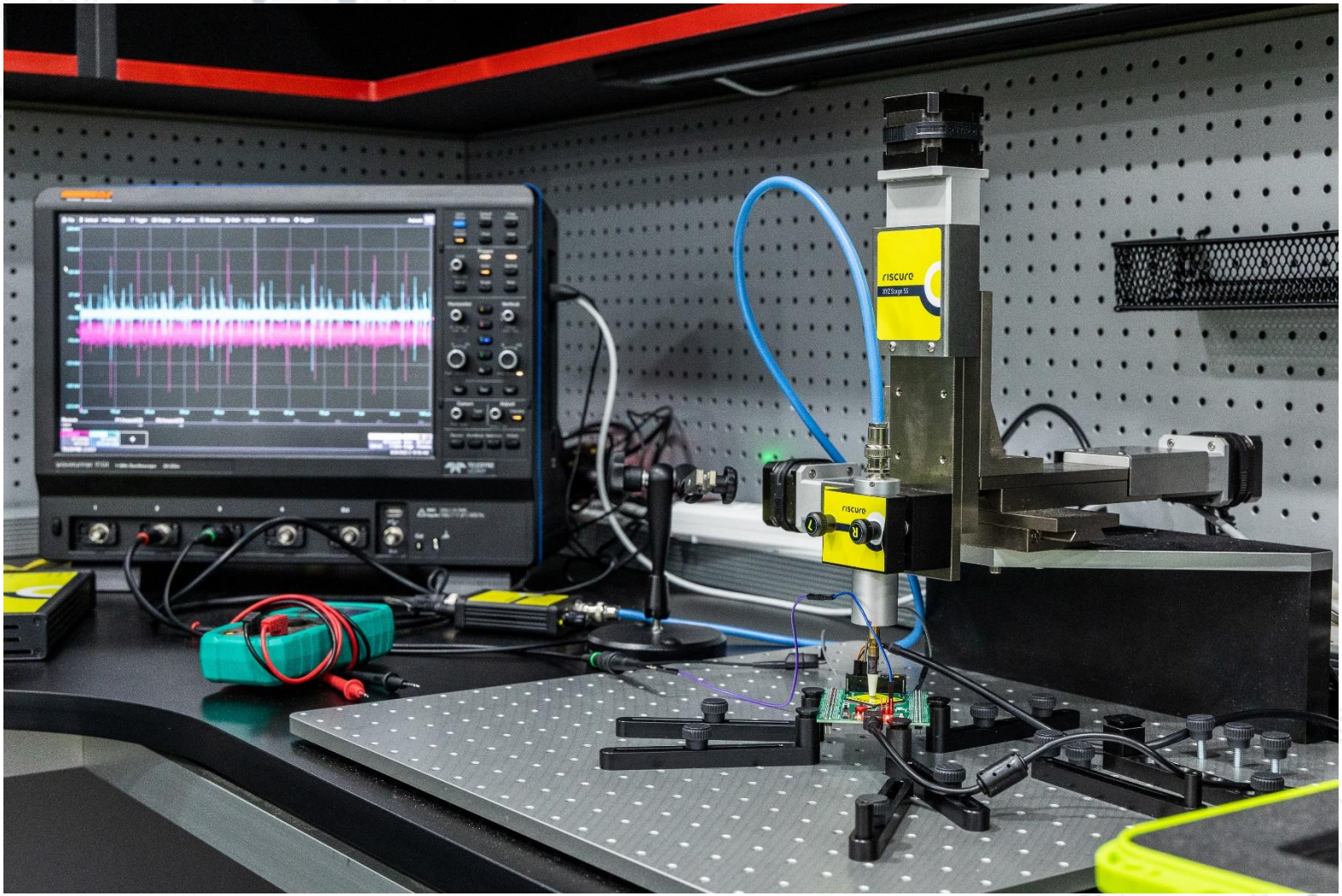
韌體安全

1. 驗證確認韌體檔案內沒有機敏資料，或機敏已經過妥善保護，並避免韌體內含有可疑連結與程式碼、源程式碼遭未經授權的揭露與修改等。
2. 測項： <機敏內容保護>、<可疑連結與程式碼檢測>及<韌體弱點檢測>、<韌體原始碼保護>、 <韌體完整性保護 >

晶片本體

1. 測試採用攻擊緩解技術的晶片，在執行密碼運算時，是否可以抵禦旁通道攻擊。
2. 利用在晶片上或周圍測量的物理量測量(如電磁場、耗電量、計算時差)中的隱藏偏差(latent bias)，嘗試找出密鑰等機敏資訊。這種偏差可能很細微，但通常持續存在，因此成為攻擊者覬覦的目標。
3. 測項：<TA測試>、<SPA/SEMA測試>及<DPA/DEMA測試>等旁通道測項。

旁通道攻擊 – 隔空抓取金鑰



STEP1: 知名國際指引導入資安best practice

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tool

TOPICS PUBLICATIONS TOOLS NEWS EVE

Home › Publications › Technical Guideline on Minimum Security Measures

Topic

Incident Reporting

For Telcos

Keywords

Resilience

Technical Guideline on Minimum Security Measures

In this document we give guidance to NRAs about the implementation of Article 13a and in particular about the security measures that providers of public communications networks must take to ensure security and integrity of these networks. It lists the minimum security measures NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

Published	October 24, 2014
Authors	ENISA
Language	English

Download
PDF document, 1.38 MB

yptography working group is a subgroup of TC CYBER; you can find out more about

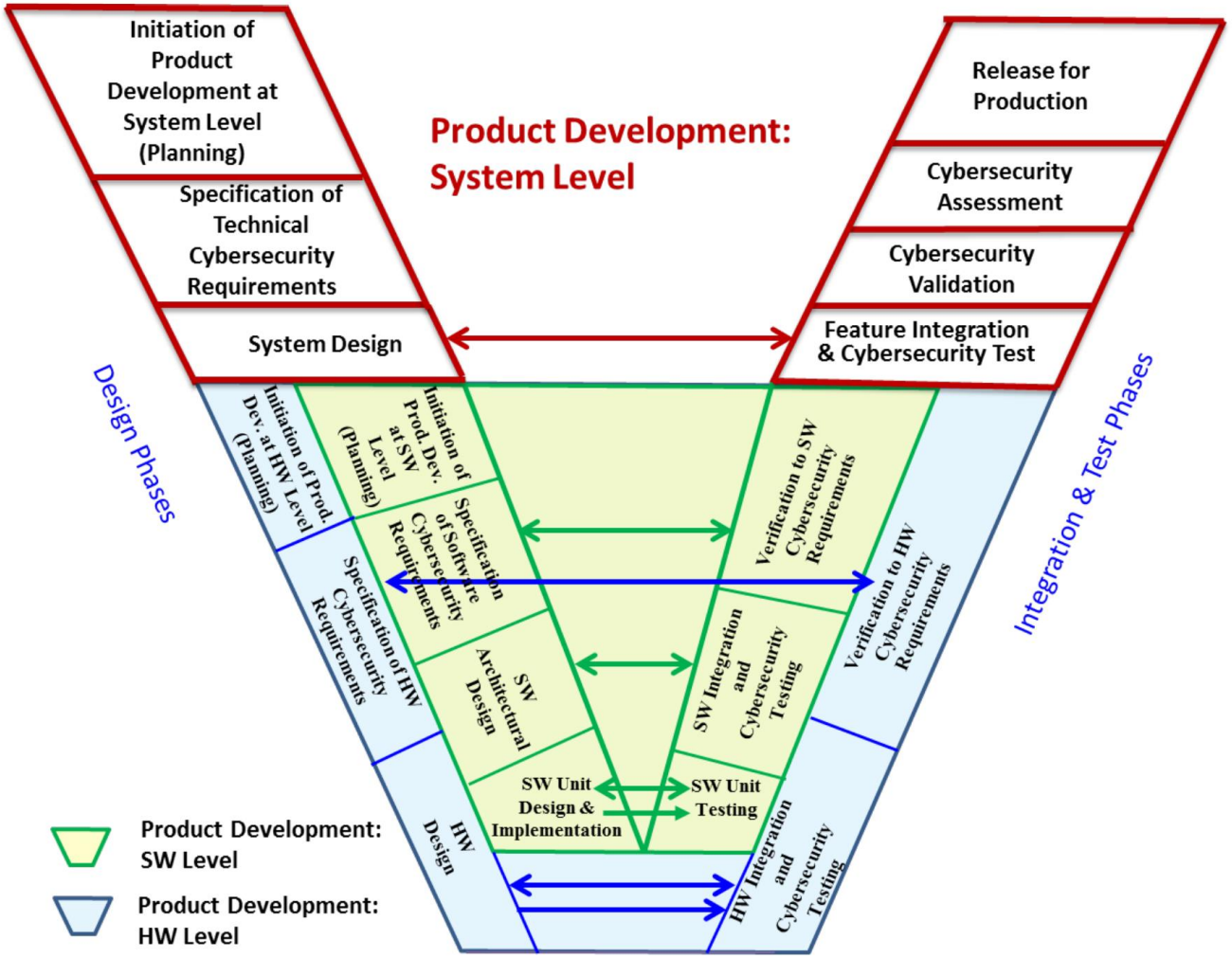
R, other ETSI groups also work on standards for cross-domain cybersecurity, the tures, devices, services and protocols and security tools and techniques. They address nd more information can be found in the related technologies pages:

- ybersecurity
- on Security Indicators
- d traffic integration
- ologies and systems
- ireless systems (5G, TETRA, DECT, RRS, RFID...)
- achine-to-Machine (M2M)
- Functions Virtualisation
- t Transport Systems, Maritime
- ting
- Artificial Intelligence
- nd techniques
- terception and Retained Data
- gnatures and trust service providers
- ements
- Security algorithms

ETSI

STEP2: 產品安全功能導入

安全開發



識別及認證

SL	Requirement Description
1	通過機制來防止未經身份認證的user，偶然或意外地存取系統/組件。
此級別重視(1)監控經由不信任網路的存取、(2)限制登入次數、(3)密碼認證強度、(4)所有介面都要有識別及認證、(5)必須具備更改預設authenticator的功能且安裝時要強制更改，並且要妥善保護authenticator、(6)帳號、ID、認證因子都要可管控。	
2	通過機制來防止未經身份認證的user，使用較少資源，通用技巧和低動機的簡單方法存取系統/組件。
此級別重視(1)除特定授權人士外，拒絕所有機敏資料的存取請求、(2)公鑰認證的使用及強度、(3)所有介面都要有識別及認證所有使用者，且ID都要唯一。	
3	通過機制來防止未經身份認證的user，使用中等資源，IACS特定技能和中等動機的簡單方法存取系統/組件。
此級別重視(1)PKI認證要搭配硬體解決方案、(2)人類使用者的密碼生命週期、(3)由hardware來保護authenticator。	
4	通過機制來防止未經身份認證的user，使用巨大資源、IACS特定技能和高動機的簡單方法存取系統/組件。
此級別重視(1)密碼生命週期(歷程紀錄)。	

授權

SL	Requirement Description
1	根據特定的權限來限制對產品的使用，防止由於偶然或意外的誤用。
此級別重視(1)要提供日誌功能、(2)日誌空間要充足、(3)日誌錯誤回報、(4)終止session、(5)病毒程式監控、(6)移動式裝置的監控、(7)無線使用控制、(8)授予人類使用者權限。	
2	根據特定的權限來限制產品的使用，防止user使用較少資源，通用技巧和低動機的簡單方法，以提升權限。
此級別重視(1)為了log需提供timestamp、(2)授予所有使用者權限、(3)更改角色權限對應、(4)無線裝置的識別。	
3	根據特定的權限來限制產品的使用，防止user花費中等資源，產品特定技能和中等動機的複雜手段，以提升權限。
此級別重視(1)日誌要集中控管、(2)日誌空間不足時要警示、(3)系統內部時間同步、(4)人類使用者的不可否認性、(5)session管理、(6)mobile code完整性驗證、(7) 高權限帳戶手動給予已授權帳戶臨時權限。	
4	根據特定的權限來限制產品的使用，防止user花費巨大資源、產品特定技能和高動機的複雜手段來，以提升權限。
此級別重視(1)時間資訊的完整性、(2)不只人類使用者的不可否認性、(3)Dual approval	

系統完整性

SL	Requirement Description
1	防止由於偶然或意外行為而導致產品完整性的遺失。
此級別重視(1)當攻擊使系統/組件無法維持正常功能，控制系統至少要能回復到預設狀態、(2)防止注入攻擊、(3)要能監控未授權改變軟體及資訊、(4)要提供安全功能驗證方法、(5)傳輸訊息完整性驗證。	
2	防止user使用較少資源，通用技巧和低動機的簡單方法，導致產品完整性的遺失。
此級別重視(1)log要有權限控管、(2)禁止不合法session id的使用、(3)除錯訊息洩漏機敏資訊、(4)zone的進出點監控malware。	
3	防止user花費中等資源，產品特定技能和中等動機的複雜手段，導致產品完整性的遺失。
此級別重視(1)使session id在session結束後無效、(2)session id的唯一性、(3)發現不完整時要主動告警、(4)要能提供自動安全功能驗證、(4)集中監控malware、(5)具安全強度的訊息完整性演算法。	
4	防止user花費巨大資源、產品特定技能和高動機的複雜手段來，導致產品完整性的遺失。
此級別重視(1)log用實體保護、(2)確保session Id的隨機性、(3)要能在正常運作下提供安全功能驗證	

資料保密

SL	Requirement Description
1	防止通過竊聽或偶然暴露，而導致未經授權地洩露訊息。
此級別重視(1)當加密是需要時，金鑰長度、金鑰建立與管理、加密演算法要使用安全可靠的做法。(2)機敏資料無論是儲存或傳送都要確保機密性。	
2	防止使用較少資源，通用技巧和低動機的簡單方法，未經授權將訊息洩露給主動搜索訊息的實體。
此級別重視(1)機敏資料要具備確實從系統/組件刪除的功能。(2)機敏資料無論是儲存或傳送在untrusted network都要加密。	
3	防止user花費中等資源，產品特定技能和中等動機的複雜手段，來未經授權將訊息洩露給主動搜索訊息的實體。
4	防止user花費巨大資源、產品特定技能和高動機的複雜手段，來未經授權將訊息洩露給主動搜索訊息的實體。
此級別重視(1) 機敏資料無論是儲存或傳送都要加密。	

限制資料流

SL	Requirement Description
1	防止由於偶然或意外行為而導致規避zone及conduit的分段。
此級別重視(1)要達到邏輯分段、(2)保護zone的邊界、(3)禁止使用個人聊天系統、(4)達到服務分段。	
2	防止user使用較少資源，通用技巧和低動機的簡單方法，故意規避zone及conduit的分段。
此級別重視(1)要達到實體分段、(2)只允許特定user流量能進入。	
3	防止user花費中等資源，產品特定技能和中等動機的複雜手段，來防止故意規避zone及conduit的分段。
此級別重視(1)將控制系統網路與非控制系統網路隔離、(2)將關鍵控制系統與非關鍵控制系統隔離、(3)禁止任何流入zone的通訊。	
4	防止user花費巨大資源、產品特定技能和高動機的複雜手段，來故意規避zone及conduit的分段。

事件回報

SL	Requirement Description
1	監視產品的運行並在發現事件時對事件做出響應，方法是在查詢時收集並提供鑑識證據。
此級別重視(1)要提供audit log的存取能力。	
2	監視產品的運行，並通過主動收集和定期報告鑑識證據對發現的事件做出響應。
此級別重視(1)持續監控資安事件。	
3	監視產品的運行，並通過主動收集和報告鑑識證據推送予適當權威。
此級別重視(1)可程式存取log，即透過API存取log。	
4	監視產品的運行，並通過主動收集和報告鑑識證據即時推送予適當權威。

資源可用性

SL	Requirement Description
1	確保系統/組件在正常生產條件下可靠運行，並防止由於偶然或意外行為而導致的拒絕服務(Denial-of-Service)情況。
此級別重視(1)要具備系統備份/還原功能、(2)遇使用緊急電源情況下，資安手段仍要能維持、(3)遇DoS event，仍要維持最低限度的運作。	
2	確保系統/組件使用較少資源，通用技巧和低動機的簡單方法，在正常和異常生產條件下可靠地運行，並防止拒絕服務的情況。
此級別重視(1) 備份完整性、(2)要能減緩流量攻擊的影響。	
3	確保系統/組件在正常、異常和極端生產條件下都能可靠地運行，並防止花費中等資源，產品特定技能和中等動機的複雜手段來拒絕服務。
此級別重視(1)限制去對別的系統/組件發動DoS攻擊、(2)自動化備份。	
4	確保系統/組件在正常，異常和極端生產條件下可靠運行，並防止花費巨大資源、產品特定技能和高動機的複雜手段來進行拒絕服務的情況。

STEP 3: 資安測試把關

資安檢測

白箱檢測

源碼檢測

Tool:
Checkmarx
Fortify

Pros:
High coverage
Find issues in early stage

黑箱檢測

弱點掃描

Tool:
Acunetix
Nessus
CMARS

滲透測試

Tool:
Kali
Burp Suite.
hashcat
…

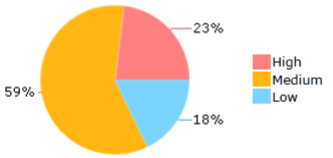
Pros:
No need source code
Low false rate

模糊測試

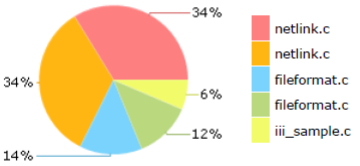
Tool:
Defensics

源碼檢測

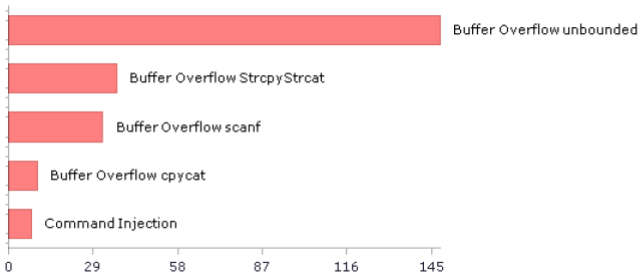
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



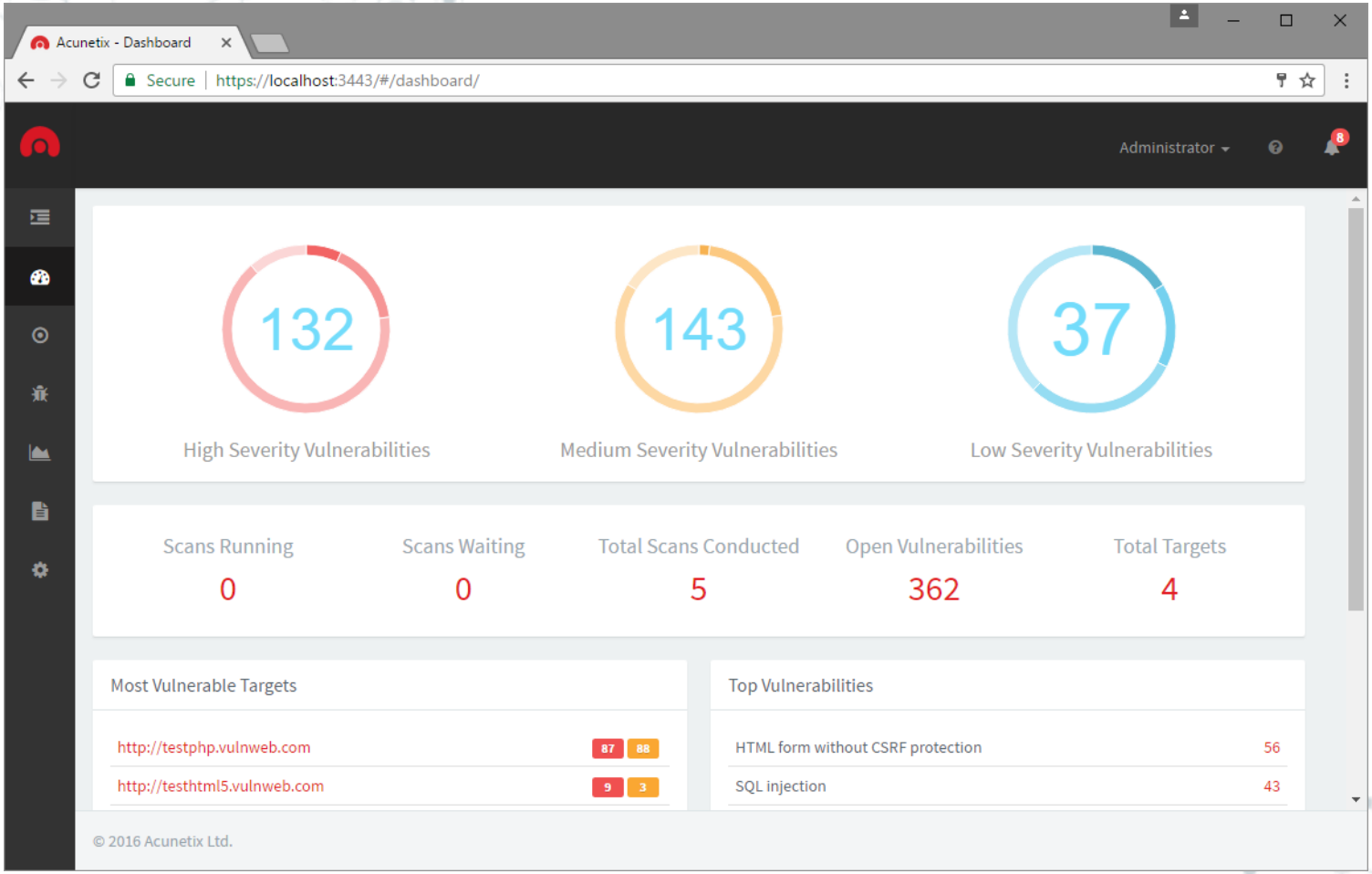
系統弱點掃描

192.168.1.236

Vulnerabilities Total: 39

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	57608	SMB Signing Disabled
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information

網站弱點掃描



行動APP資安檢測工具

行動APP常見重大資安威脅

- 憑證綁定
- 程式碼混淆
- 除錯訊息含敏感資料

模糊測試工具

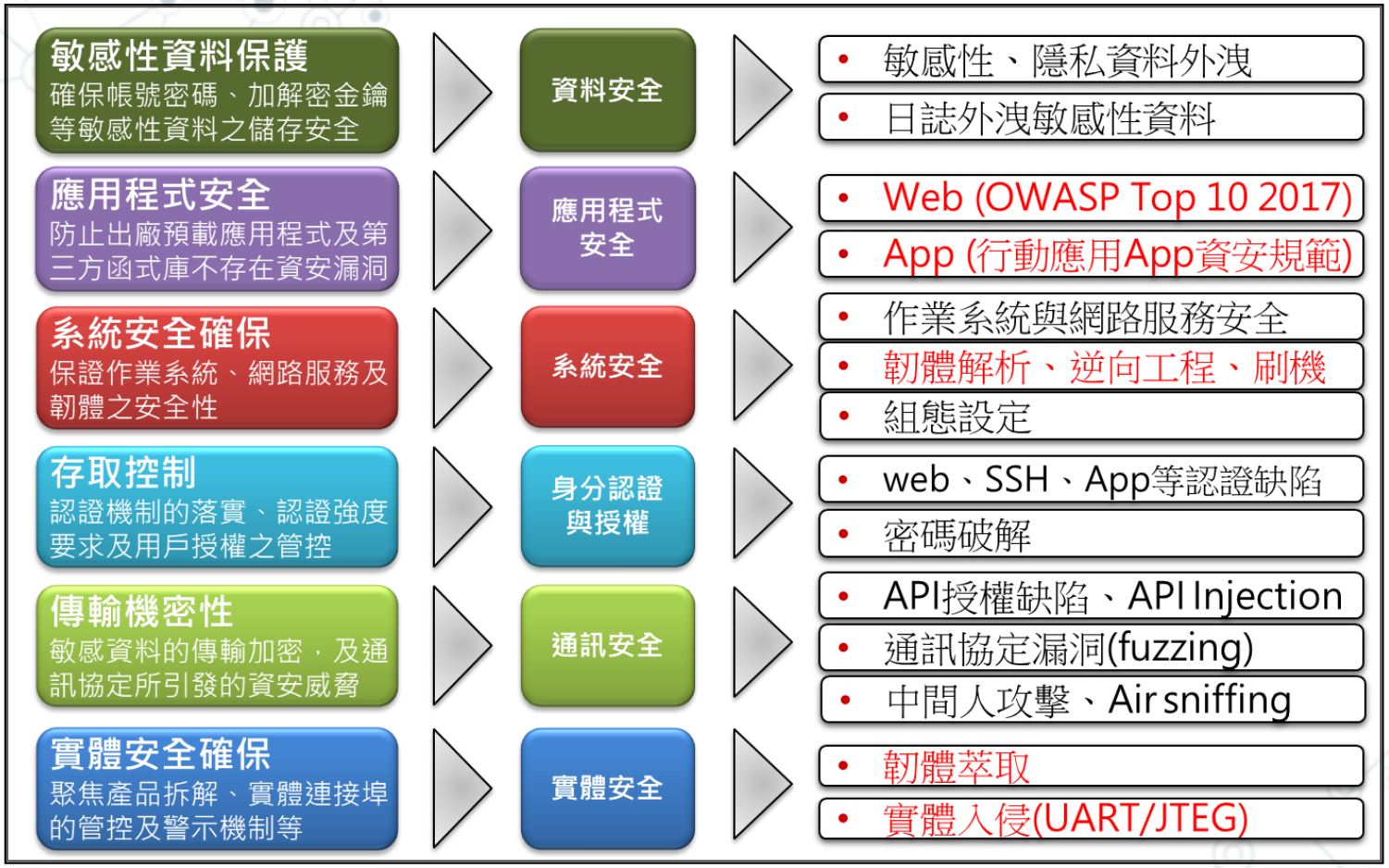
目前支援模糊測試之協定

- **Wi-Fi Protocol**
- **Ethernet-related Protocol**
- **S1AP**
- **SCTP**
- **Modbus**
- **DLMS/COSEM**

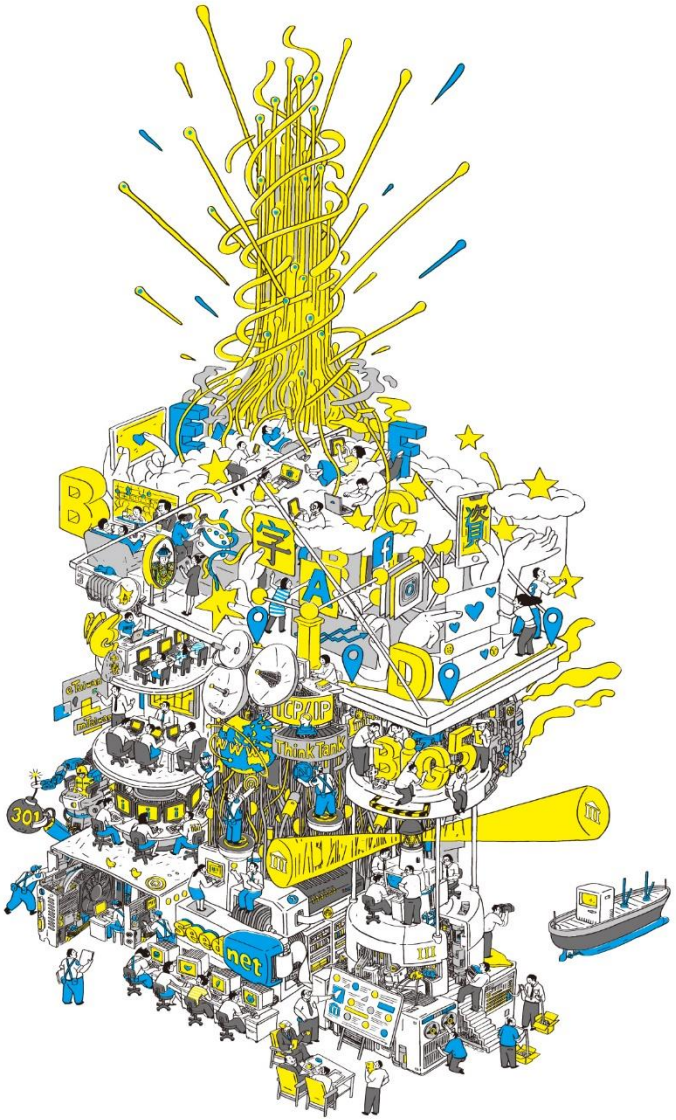
智慧資安模糊測試技術雛形，利用**人工智慧學習技術** (Long/Short-Term Memory, LSTM) 及**智慧選擇8種變異方法** (功能碼變異、暫存器變異、payload長度異常變異等)，創建模糊測試資料進行模糊測試

滲透測試

滲透測試框架



參考 NIST SP 800-115, OWASP Top 10 IoT Vulnerability



1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13策進 e-Taiwan / m-Taiwan 14精進5G智慧科技創新應用 15支援文創與設計產業奠基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉無線寬頻環境
19協助產業拓展商機並強化資安防護 20數位轉型化育者

THANK YOU