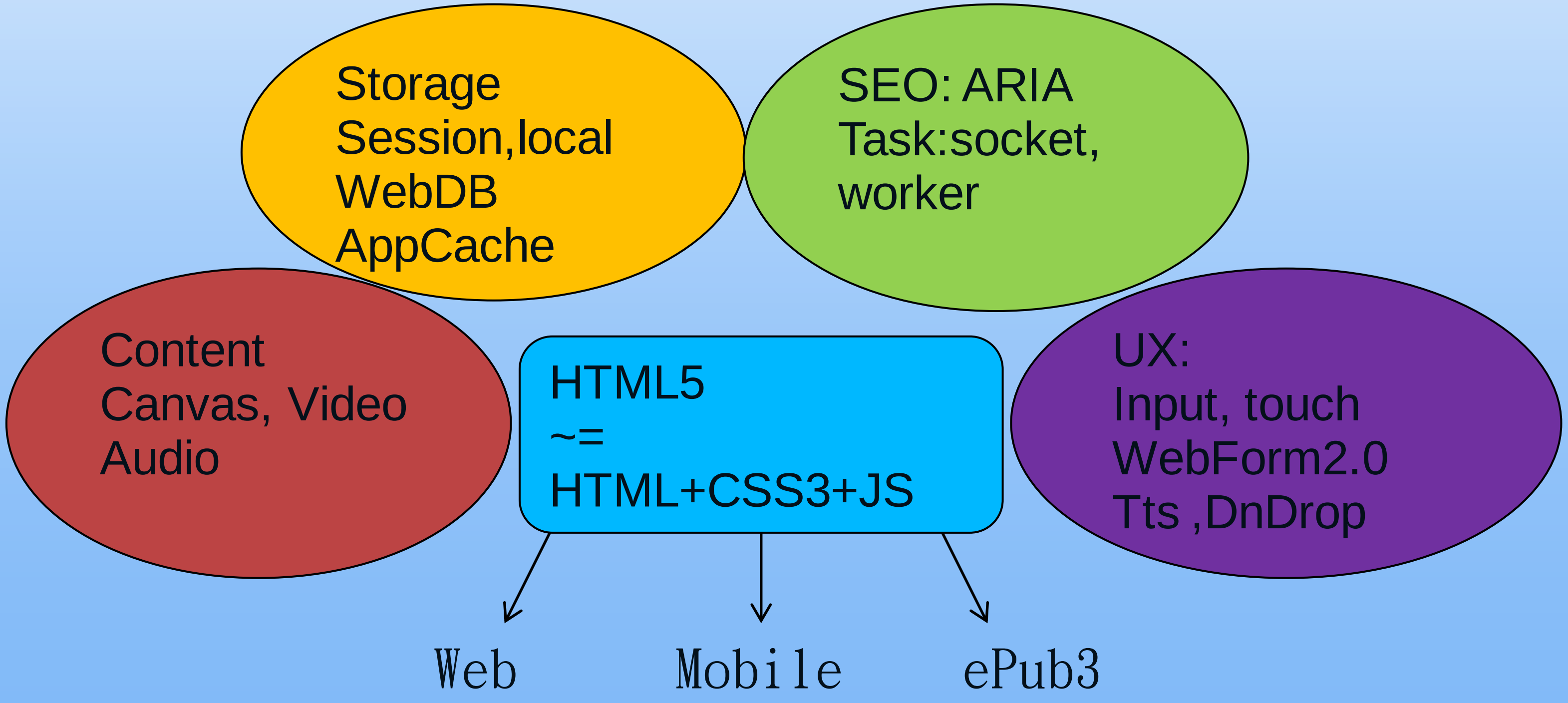
HTML5與Mobile安全威脅發展

Jack Yu

Agenda

- HTML5 安全威脅發展
- Mobile安全威脅發展
- Web Backend安全威脅發展

HTML5新功能與安全評估



Storage
Session,local
WebDB
AppCache

SEO: ARIA
Task:socket,
worker

Content
Canvas, Video
Audio

HTML5
~=
HTML+CSS3+JS

UX:
Input, touch
WebForm2.0
Tts ,DnDrop

Web

Mobile

ePub3

- localStorage 儲放XSS攻擊程式與shell code
- HTML5 Botnet
- 利用HTML5 達到內部網路掃描

OWASP Top 10 Mobile Risks

OWASP Top 10 Mobile Risks
M1 – Insecure Data Storage不安全的資料儲存於用戶端
M2 – Weak Server Side Controls伺服器端安全控制脆弱
M3 – Insufficient Transport Layer Protection傳輸層保護不足
M4 – Client Side Injection用戶端注入變造
M5 – Poor Authorization and Authentication身分鑑別與授權機制不嚴謹
M6 – Improper Session Handling 連線階段處理不適當
M7 – Security Decisions Via Untrusted Inputs對於不受信任輸入來源的檢測處置
M8 – Side Channel Data Leakage側通道的資訊洩漏
M9 – Broken Cryptography 加密方法不嚴謹或失效
M10 – Sensitive Information Disclosure 敏感資訊洩漏

補充：ENISA 智慧手機十大風險

No.	Title	Risk
1	Data leakage resulting from device loss or theft	High
2	Unintentional disclosure of data	High
3	Attacks on decommissioned smartphones	High
4	Phishing attacks	Medium
5	Spyware attacks	Medium
6	Network Spoofing Attacks	Medium
7	Surveillance attacks	Medium
8	Diallerware attacks	Medium
9	Financial malware attacks	Medium
10	Network congestion	Low

OWASP TOP 10 – 2010	OWASP TOP 10 – 2013 (New) RC1
A1-注入攻擊 (Injection)	A1-注入攻擊 (Injection)
A3-失效的驗證與連線管理 (Broken Authentication and Session Management)	A2-失效的身分驗證與連線管理 (Broken Authentication and Session Management)
A2-跨站腳本攻擊(Cross-Site Scripting, XSS)	A3-跨站腳本攻擊(Cross-Site Scripting, XSS)
A4-不安全的物件參考(Insecure Direct Object References)	A4-不安全的物件參考(Insecure Direct Object References)
A6-不當安全組態設定(Security Misconfiguration)	A5-不當安全組態設定(Security Misconfiguration)
A7-不安全的加密資料儲存--與A9合併→ (Insecure Cryptographic Storage)	A6-敏感資料暴露(Sensitive Data Exposure)
A8-限制網址存取失效--擴大為2013-A7→ (Failure to Restrict URL Access)	A7-缺少功能級別的存取控制(Missing Function Level Access Control)
A5-跨站請求偽造 (Cross-site Request Forgery, CSRF)	A8-跨站請求偽造 (Cross-site Request Forgery, CSRF)
<隱藏於A6: 不當安全組態設定> <buried in A6: Security Misconfigurtion>	A9-使用已知漏洞的元件(Using Known Vulnerable Components)
A10-未驗證的重新導向與轉發(Unvalidated Redirects and Forwards)	A10-未驗證的重新導向與轉送 (Unvalidated Redirects and Forwards)
A9-傳輸層保護的不足 (Insufficient Transport Layer Protection)	與2010-A7合併至2013-A6