7TH INTERNATIONAL COMMON CRITERIA CONFERENCE

TELECOM TECHNOLOGY CENTER

New Attack and CC v3.0

Author : Chao-Tung , Yang / Yao-Chang , Yu

Speaker : Yao-Chang , Yu / Chao-Tung , Yang

Advisor : Hsi-Lan, Hsu

Sponsor : National Communications Commission

20. September 2006 Spain

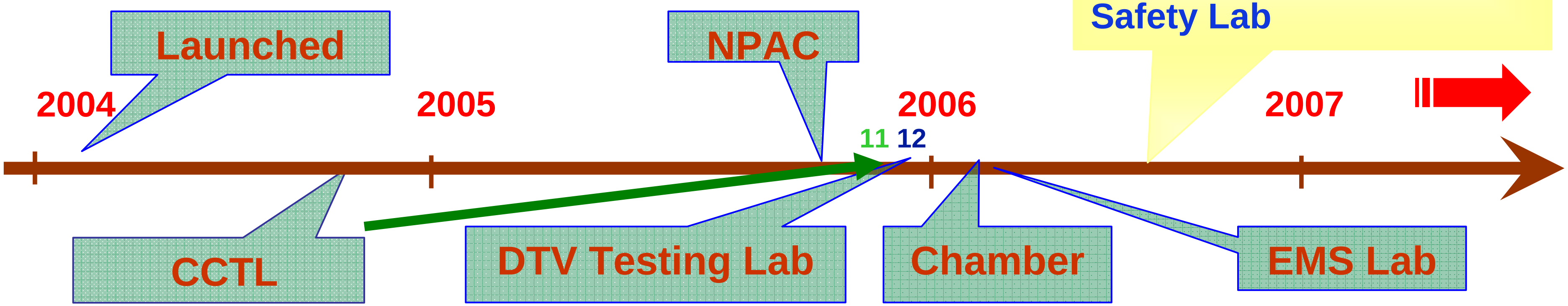
Contents

- ❑Introduction to TTC
- ❑Motivation
- ❑New Attack Issues
- ❑New Attack Example — Phishing
- ❑New Attack Example — Mobile Malicious Code

Introduction to TTC

TTC Roadmap

WiMAX Certification Lab
DVB-H Lab
MHP Lab
VoIP Exchange Center
CMTL
SAR & MPE Lab
EMI Lab
Safety Lab



Launched

NPAC

2004

2005

2006

2007

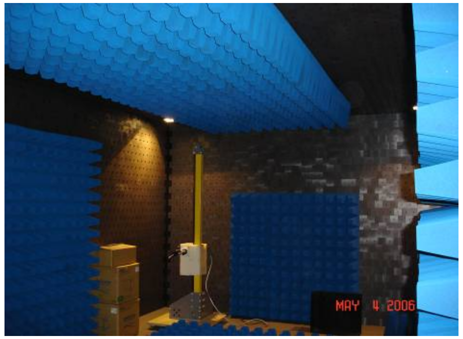
11 12

CCTL

DTV Testing Lab

Chamber

EMS Lab



Motivation

Introduction of Internet Growth

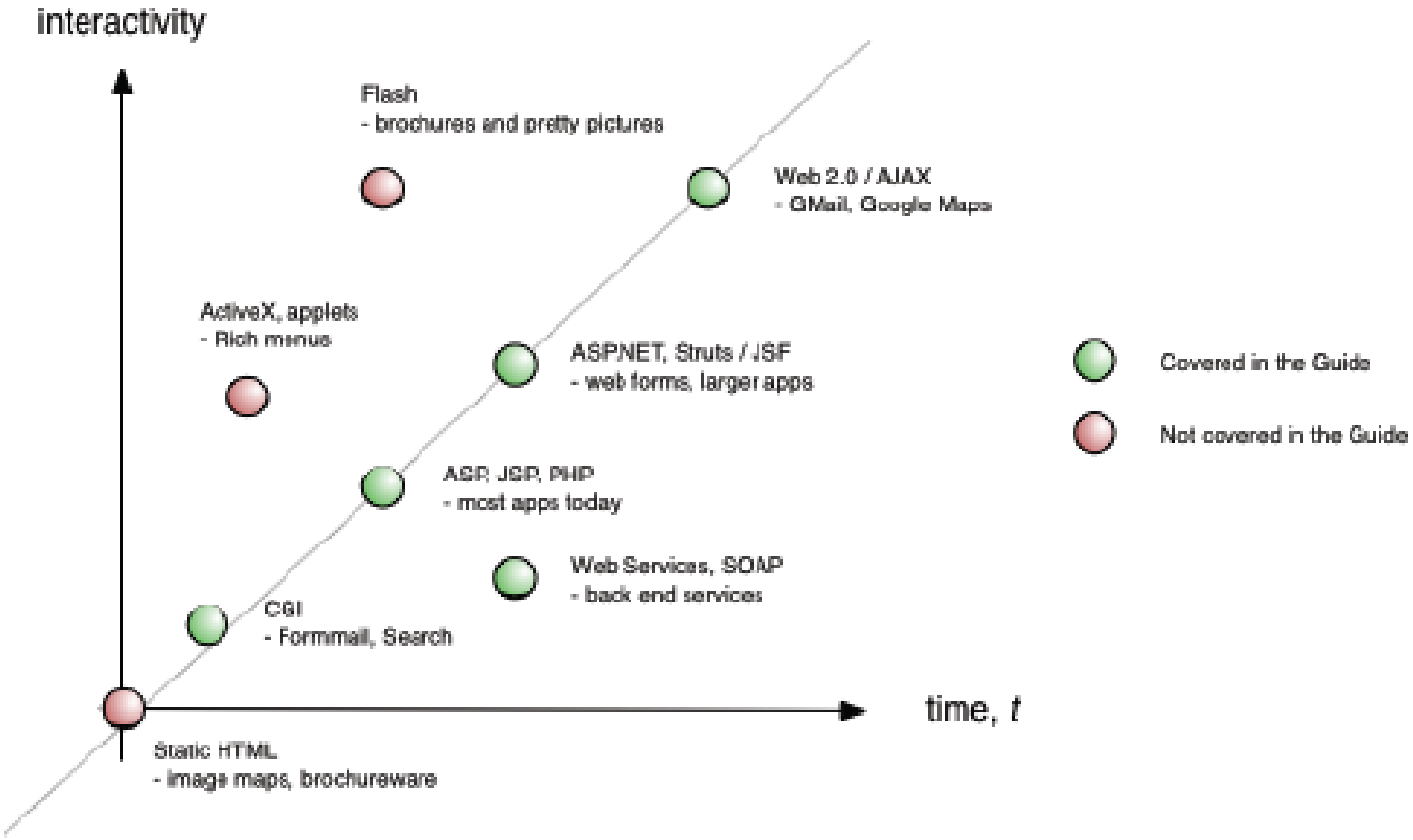
- ❑ Today there are more and more computer users connecting to the Internet. The Internet becomes popular for commercial communication, commerce, medicine, and other public services, such as, e-commerce (such as Amazon), web e-mail (Hotmail or GMail), Internet Banking, blogs, online share trading, web forums, communities Orkut and Friendster.
- ❑ The trend of web usage becomes increasing interactivity on apace with the advent of “Web 2.0”, a term that encompasses many existing technologies and heavily features highly interactive, user centric, and web-aware applications.

Motivation

- ❑In the meantime, the risk of unauthorized access and destruction of service by outsiders is increasing. The malicious usage, attacks, and sabotage have been on the rise as more and more computers are put into use.

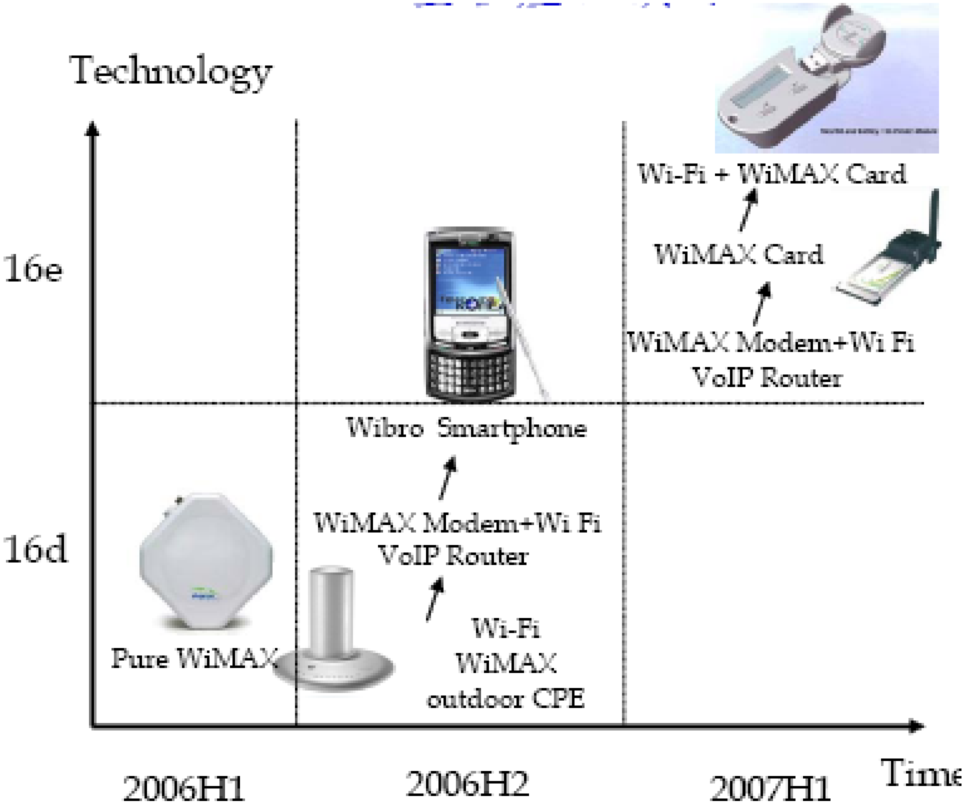
New Attack Issues

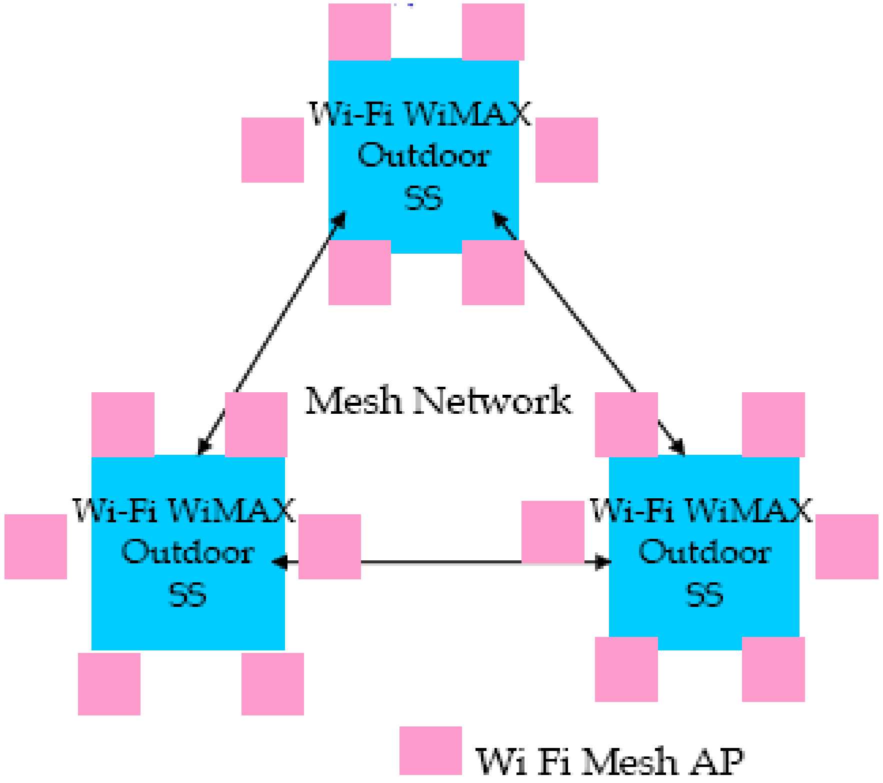
State of the Art Technical in Web



Source from : www.owasp.org

Next Wireless Generation





New Vulnerabilities in Web and Wireless application

- ❑ Invalid Input
- ❑ Broken Access Control
- ❑ XSS Flaws
- ❑ Buffer Overflows
- ❑ Injection Flaws
- ❑ Denial of Service
- ❑ Phishing
- ❑ Inherent Malicious Code
- ❑ Mobile Malicious Code
- ❑ ……

New Attack Example — Phishing

New Attack Example — Phishing

- ❑ Phishing is the misrepresentation of information which the criminal uses social engineering to appear as a trusted identity. The criminal abuses the trust to gain valuable information, such as, details of accounts. The criminal might gain the enough personal information to open accounts, obtain loans, or buy goods through e-commerce sites.
- ❑ Phising attacks are one of the highest visibility problems for banking and e-commerce sites. The attacks have the potential to destroy a customer's livelihood and credit rating.

Calculation of attack potential

Factor	Value
Elapsed Time	
<= one day	[✓ 0]
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> Six months	19
Expertise	
Layman	0
Proficient	3
Expert	[✓ 6]
Multiple experts	8

Factor	Value
Knowledge of TOE	
Public	[✓ 0]
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary/unlimited access	0
Easy	[✓ 1]
Moderate	4
Difficult	10
None	
Equipment	
Standard	[✓ 0]
Specialised	4
Bespoke	7
Multiple bespoke	9

Calculation of attack potential

- ❑ Elapsed Time
  - ➢ <= one day : 0
- ❑ Expertise
  - ➢ Expert : 6
- ❑ Knowledge of TOE
  - ➢ Public : 0
- ❑ Window of Opportunity
  - ➢ Easy : 1
- ❑ Equipment
  - ➢ Standard : 0
- ❑ Total : 0 + 6 + 0 + 1 + 0 = 7

Rating of Vulnerabilities and TOE Resistance

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4 AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1 AVA_VAN.2	AVA_VAN.3, AVA_VAN.4 AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3	AVA_VAN.4 AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=> 25	Beyond High	High	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4 AVA_VAN.5	-

Issue1: Phishing

- ❑Attack potential required to exploit scenario
  - ➢Only Basic

Phising — A new age weapon

Only Basic?

Issue2: Phishing

- ❑Phishing could be happened in Internet Banking or Portal Site.
- ❑According to “Calculation of attack potential”, there is the same value in rating of Vulnerabilities of Phishing.
- ❑Actually, there should be different risk at different web applications.

Could CC v3.0 solve this problem ?

Propose

Add new factor

- Protect asset value
  - Low : 4
  - Moderate : 10
  - High : 19

And/or

- Risk value
  - Low : 4
  - Moderate : 10
  - High : 19

New Attack Example — Mobile Malicious Code

New Attack Example — Mobile Malicious Code

- ❑Malicious code has been generally accepted as one of the top security threats to computer systems around the globe for several years now.
- ❑We are now seeing new innovation as mobile malicious code moves away from being a way to disrupt systems and communications. Today, it is a ‘crime-enabler’ for spammers, hackers and organized criminals.

Calculation of attack potential

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	[✓ 13]
<= five months	15
<= six months	17
> Six months	19
Expertise	
Layman	0
Proficient	3
Expert	[✓ 6]
Multiple experts	8

Factor	Value
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	[✓ 11]
Window of Opportunity	
Unnecessary/unlimited access	0
Easy	[✓ 1]
Moderate	4
Difficult	10
None	
Equipment	
Standard	0
Specialised	4
Bespoke	[✓ 7]
Multiple bespoke	9

Calculation of attack potential

- ❑ Elapsed Time
  - ➢ <= four months : 13
- ❑ Expertise
  - ➢ Expert : 6
- ❑ Knowledge of TOE
  - ➢ Critical : 11
- ❑ Window of Opportunity
  - ➢ Easy : 1
- ❑ Equipment
  - ➢ Bespoke : 7
- ❑ Total : 13 + 6 + 11 + 1 + 7 = 38

Rating of Vulnerabilities and TOE Resistance

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4 AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1 AVA_VAN.2	AVA_VAN.3, AVA_VAN.4 AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3	AVA_VAN.4 AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=> 25	Beyond High	High	AVA_VAN.1, AVA_VAN.2 AVA_VAN.3, AVA_VAN.4 AVA_VAN.5	-

Issue1: Mobile Malicious Code

❑ Attack potential required to exploit scenario

- ➢ More than **Beyond High**
- ➢ According to Attack potential definition, developer usually doesn't include this scenario.

Mobile Malicious Code — will be frequently happened

Doesn't consider this scenario ?

Issue2: Mobile Malicious Code

- ❑ADV_IMP.2 only looks at instantiation of SFRs, but how about inspection of the other parts???
  - ➢What's wanted is an exhaustive inspection
  - ➢In reality, this is not feasible, probably because of time-consuming

Could CC v3.0 solve this problem ?

Propose

- ❑ Refine ATE_DPT.4.1C to ATE_DPT.4.4C
  - ➢ Code coverage
    - Show code coverage by tests (ATE_FUN) by automated means
    - In case of uncovered code:
      - – Specify/perform additional tests
      - – Give rationale for non-covered parts
- ❑ Refine ADV_IMP.2
  - ➢ Evaluator can check that method to show code coverage works
  - ➢ IMP-evaluation, exhaustively look at code parts

Contact Information

Yao-Chang, Yu	Chao-Tung, Yang
Director	Evaluator
Phone +886-7-6955008	Phone +886-2-89535600 ext.217
Fax +886-7-6955009	Fax +886-289535655
E-mail yaochang@ttc.org.tw	E-mail spencer@ttc.org.tw
www.ttc.org.tw	
Common Criteria Testing Lab Telecom Technology Center	

Question ?

THANKS VERY MUCH FOR YOUR ATTENTION