Vulnerabilities go mobile

Marko Laakso, Mikko Varpiola

ouspg@ee.oulu.fi

Oulu University Secure Programming Group

Clash of two worlds

Information security incidents plague the Internet. Our society depends on phone networks. Today, the Internet has gone mobile.

There will be an inevitable clash of two worlds?

- Internet
  - Payload: Open, flexible, technically simple ...
  - Drag: Exposed, hostile, unreliable, ...
- Classic phone networks
  - Payload: Dependable, familiar, user friendly, ...
  - Drag: Closed, technically complex, ...

[Rocket Art ©http://www.discoveryschool.com]

The plot - for a brave new world?

Mobile phones have transformed into interconnected computing appliances and information about their security vulnerabilities begins to roll-in. We explored the vulnerability scene of the mobile phone networks.

1. Characteristics of the mobile phone network vulnerability scene
2. Sanity check through study of the WAP implementations
3. Analysis through a vulnerability scene maturity model
4. Wistful conclusions

Mobile vulnerability scene from actor perspective

- We assert that:
  - Since engineers constantly push the complexity barrier, all concurrent technology will have potential for information security and safety hazards
  - Vulnerabilities in technology (e.g. in software implementation) will be discovered, disclosed and abused
- Since this implies existence of a *vulnerability scene* we aim to identify such for the mobile telecom and attempt to compare it with its Internet counterpart. First as a collection of actor related observations ...

Evaluators of security

- Mobile telecom
  1. Some analytic papers on e.g. WTLS, GPRS and A5 weaknesses
  2. Initial vulnerability discoveries (Siemens SMS and Nokia SMS DoS), no vulnerability forums, no advisories, no vendor statements and no patch releases (rumoured I-Mode recall)
- Internet
  1. Numerous analytic papers and experiments on public cryptographic algorithms and protocols
  2. High volume of vulnerability disclosures on established forums, security advisories, vendor statements and patch releases

Developers

- Mobile telecom
  1. First mobile terminal virus scanners (e.g. F-Secure), encryption and VPN products (e.g. SSH Communications) are emerging
  2. Initial attempts to support patch-by-wireless for terminals instead of recall to firmware upgrade
- Internet
  1. Myriad of security solutions are available from multiple vendors: IDS, virus scanners, encryption products, VPN products, firewalls, content filters ...
  2. Support for patch announcement, deployment and automatic updates

Users and providers

- Mobile telecom
  1. Devices chosen based on personal preference
  2. Organisations may have no record of mobile device models, firmware levels and add-on applications
  3. No tools for computer forensics, no audit-trails (logs)
  4. No filtering by providers (not even horizontal)
- Internet
  1. Product choices controlled by company policy
  2. Organisations may have inventory of used products
  3. Many computer forensic tools, audit-trails collected
  4. Providers may sell filtering services

Mediators and controllers

- Mobile telecom
  1. Media is interested but news are either sensationalistic or discuss new “solutions”
  2. Telecommunication legislation and regulation may be old and strict, possibly even hindering information sharing during incident response
- Internet
  1. Media is more involved and sometimes even helps in “crisis communication” by distributing constructive information about vulnerabilities
  2. Cyber (crime) legislation slowly rolls in

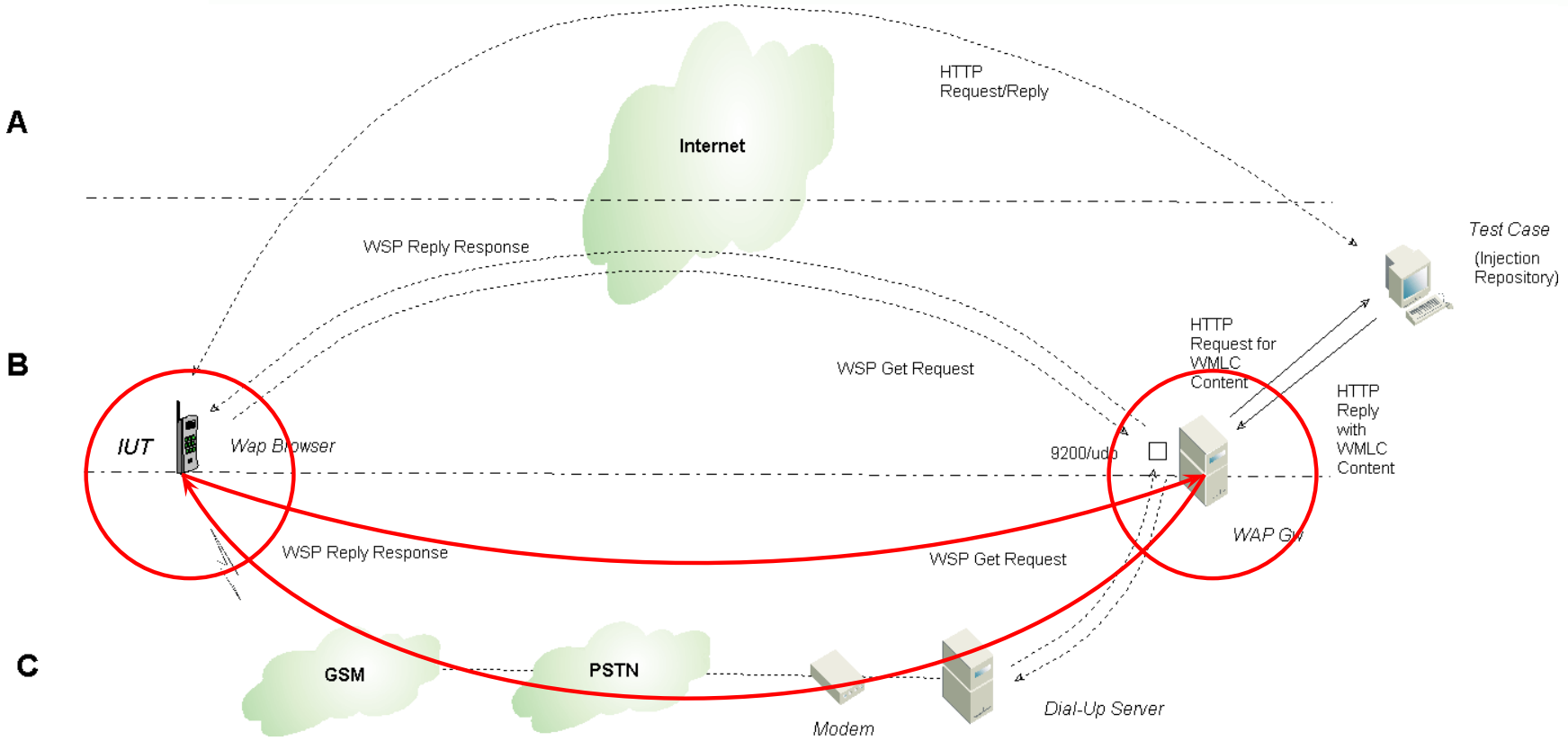
Mobile telecom vs. Internet - end of round one

"For 2001, Nokia estimates that web-enabled handset unit volumes will increase to around 200 million" [Nokia press release]

- Mobile devices and classic Internet devices are comparable in numbers
- Combined with usage scenarios this implies comparable importance
- Our initial analysis shows vulnerability related activity in mobile telecom context. Amount of it pales in comparison to similar activity in Internet scene.

Is this difference due to more robust and less vulnerable technology?

Sanity check through WAP vulnerability assessment



WAP gateways

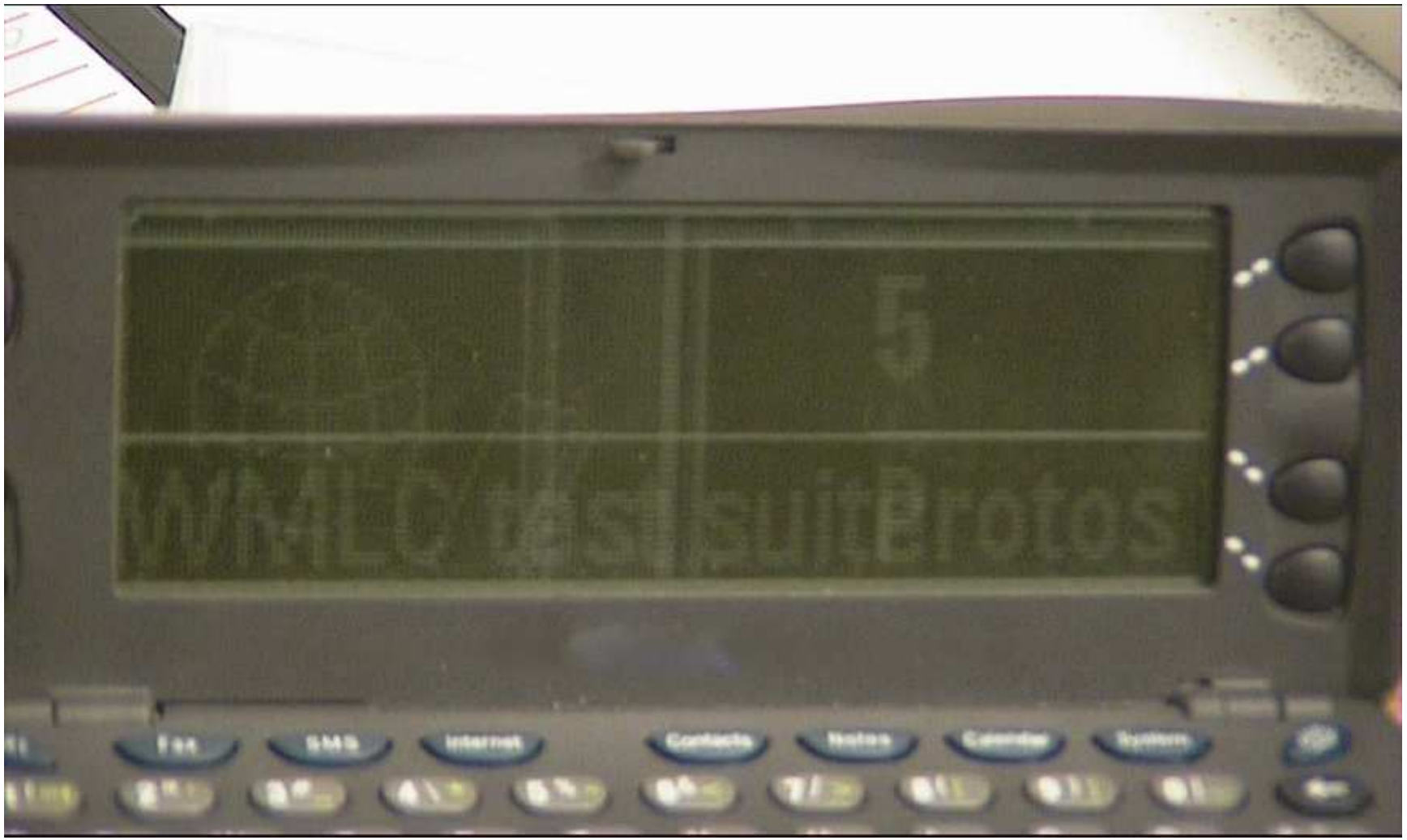
- In PROTOS c04-wap-wsp-request test-suite we constructed 4236 test-cases in 39 categories with malicious content to trigger WAP gateway flaws. All implementations we tested were equally vulnerable.

Implementation	Failed cases	Failure groups
Gateway 001	569	10
Gateway 002	141	18
Gateway 003	10	2
Gateway 004	385	16
Gateway 005	664	8
Gateway 006	622	14
Gateway 007	148	20

- Random Encounters: (a) WAP has peculiar peer-to-peer encryption concept. Decrypt and re-encrypt in the middle at the WAP gateway. (b) Companies did come and go during the test-suite vulnerability process.

We went mobile with WAP terminals (browsers)

A graphic crash



Asserting into a vegetable

Reformat and lose all data

No survivors

No survivors - in detail

In PROTOS c05-wap-wmlc test-suite we constructed 1033 test-cases in 84 categories with malicious content to trigger WAP browser flaws. All implementations we tested were equally vulnerable.

Implementation	Failed cases	Failure groups
Browser 001	26	4
Browser 002	189	43
Browser 003	8	2
Browser 004	4	2
Browser 005	34	4
Browser 006	21	9
Browser 007	25	2
Browser 008	31	11
Browser 009	9	1
Browser 010	34	15

Random Encounters: (a) Client software is not regarded security critical by the vendors. From our perspective it either holds the data or keys to the data to be potentially protected.

Mobile telecom vs. Internet - end of round two

- PROTOS test-suites - vulnerability assessment through syntax testing

Test-suite	Failed products	Vendor responses	Advisory
c04-wap-wsp-request	7 (7 tested)	5	n/a
c05-wap-wmlc	10 (10 tested)	1	n/a
c05-http-reply	5 (12 tested)	2	n/a
c06-ldapv3	6 (8 tested)	10	CA-2001-18
c06-snmpv1	12 (12 tested)	140	CA-2002-03

[http://www.ee.oulu.fi/research/ouspg/protos]

From robustness perspective both worlds are vulnerable. Since there is less fuzz, is the mobile telecom vulnerability scene more mature?

Vulnerability scene maturity model

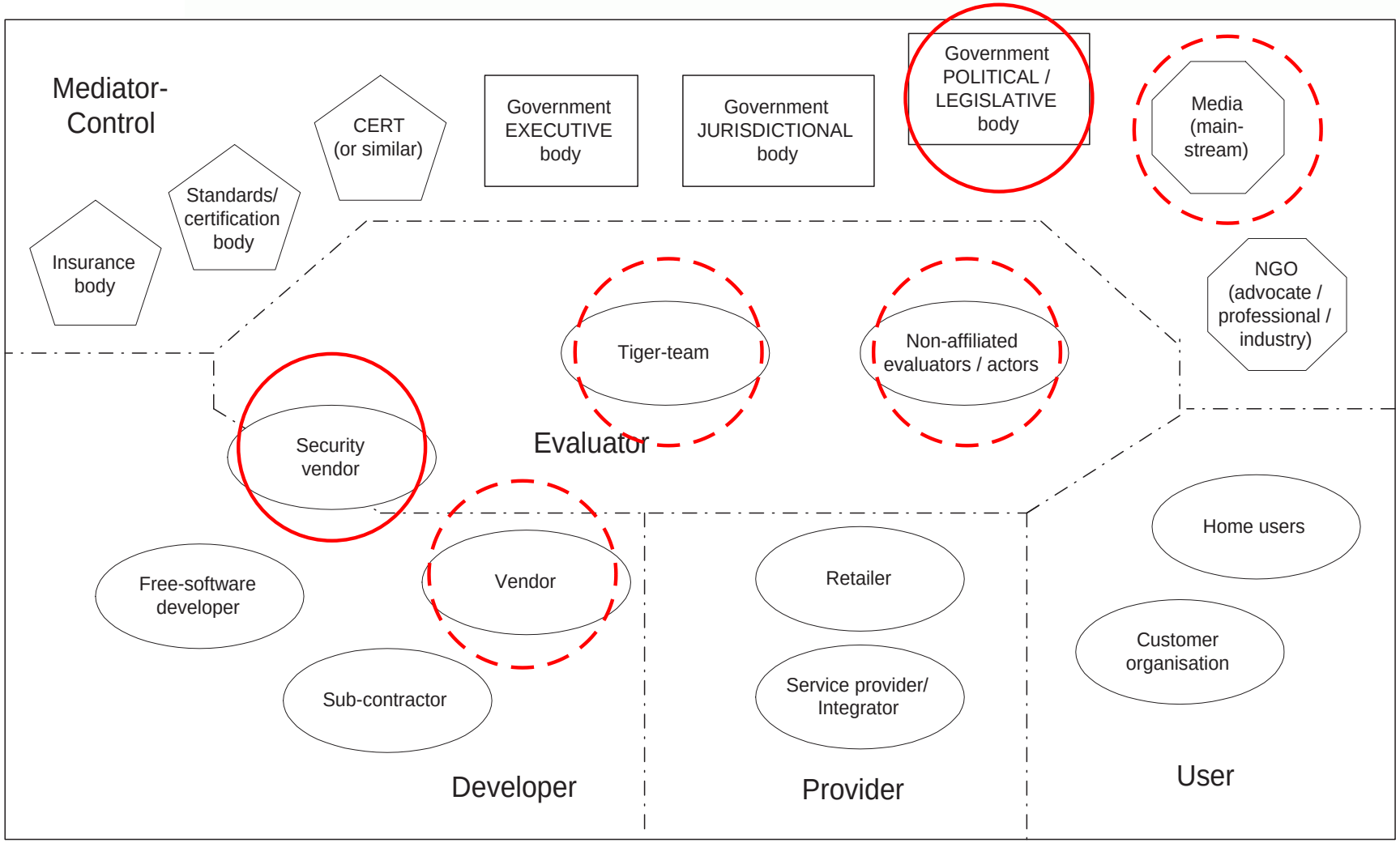
- We assert that there are three conceptual levels of vulnerability scene (process) activity:
  1. Infancy
     - Scattered and uncoordinated activity
  2. Developed
     - Most major players are involved, interconnections between actors are building up and processes evolve
  3. Mature
     - A process involving all major actors has developed and is self-tuning based on informed risk management

Vulnerability scene maturity model vs. CMM

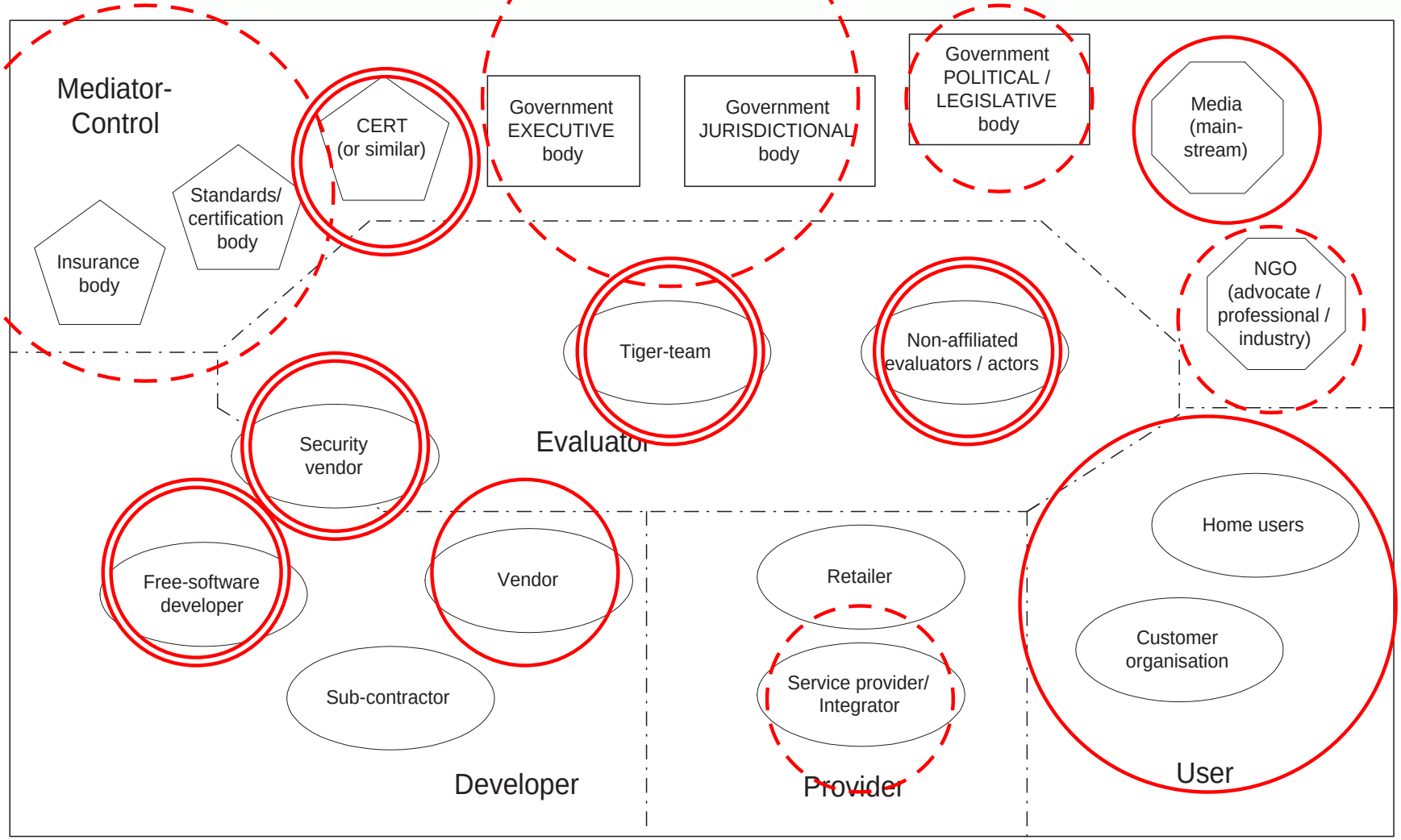
- Capability Maturity Model definitions can be applied in our vulnerability scene context:
  1. **Initial** - The software process is characterised as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
  2. **Repeatable** - Intuitive
  3. **Defined** - Standard and Consistent
  4. **Managed** - Predictable
  5. **Optimizing** - Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

[http://www.sei.cmu.edu/cmm/cmm.sum.html]

Activity in mobile vulnerability scene - infancy stage?



Activity in Internet vulnerability scene - developed stage?



Mobile telecom vs. Internet - end of round three

Mobile vulnerability scene is in its infancy. Even the Internet counterpart leaves much to desire for.

- Bugs (vulnerabilities) come and go, they are not the point
- We need quantitative measures for “vulnerability”, we need to understand the threats and do informed risk management. A gross simplification:
  $risk = vulnerability * threat$
- Due to almost uncanny resemblance between the two worlds we could avoid some vulnerability related mobile telecom growth pains and aim for a mature merger.

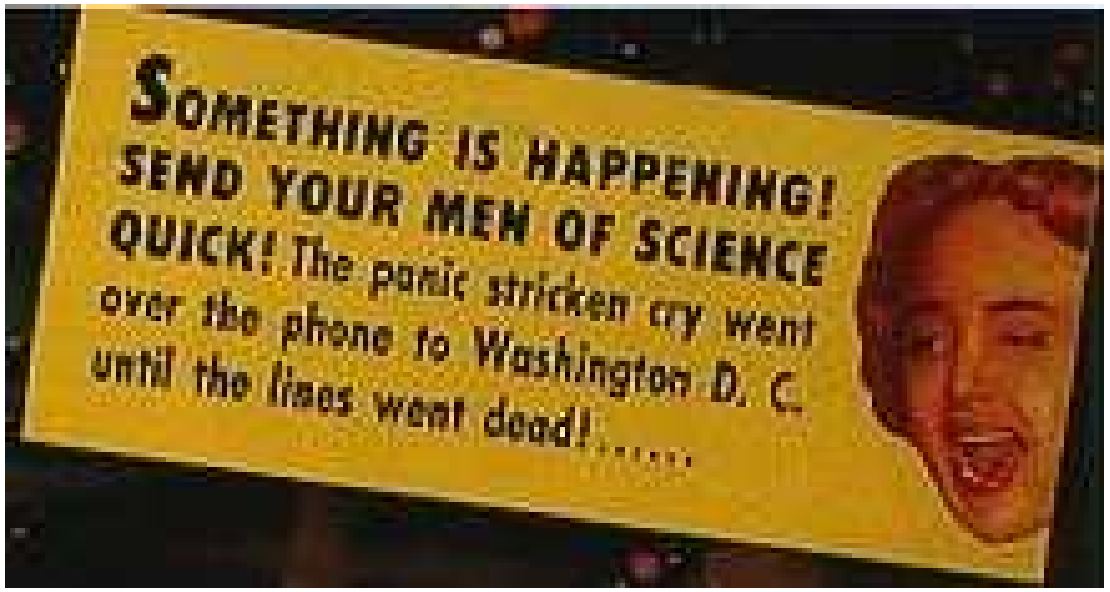
Wistful conclusions

- For mobile telecom there will:
  - be vulnerability disclosures (hype imminent)
  - be incidents (hype imminent)
  - not be silver bullets (hype imminent tho)
- For all of us there is just hard work: informed risk management, proactive and reactive measures, incident response, activating all actors, demanding more robust products ...

Fortunately it is familiar work, just like in the Internet context. Lets make these worlds merge into one mature scene.

The End

Lets muffle our panic stricken cries with reason



Any questions?

All this and more available from:

http://www.ee.oulu.fi/research/ouspg/protos/sota/AusCERT2002-mobile

[Panic art from movie poster “Invasion of the Body Snatchers”]