Towards secure Internet

TIVIT results and business forum, 12.4.2011

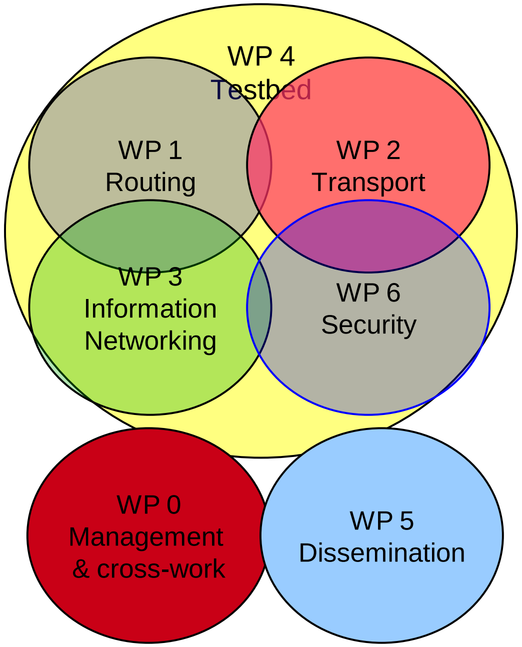
Prof. Mika Rautila
VTT Technical Research Centre of Finland

Tivit Future Internet Program 2008 - 2013

Vision: Future Internet = a mission critical backbone of global information society

Mission: Enhance the Internet technology and ecology as a *platform for innovation* while providing strong governance over the use of the network resources and information

4 yr Strategic Research Agenda: www.futureinternet.fi



WP 4 Testbed

WP 1 Routing

WP 2 Transport

WP 3 Information Networking

WP 6 Security

WP 0 Management & cross-work

WP 5 Dissemination

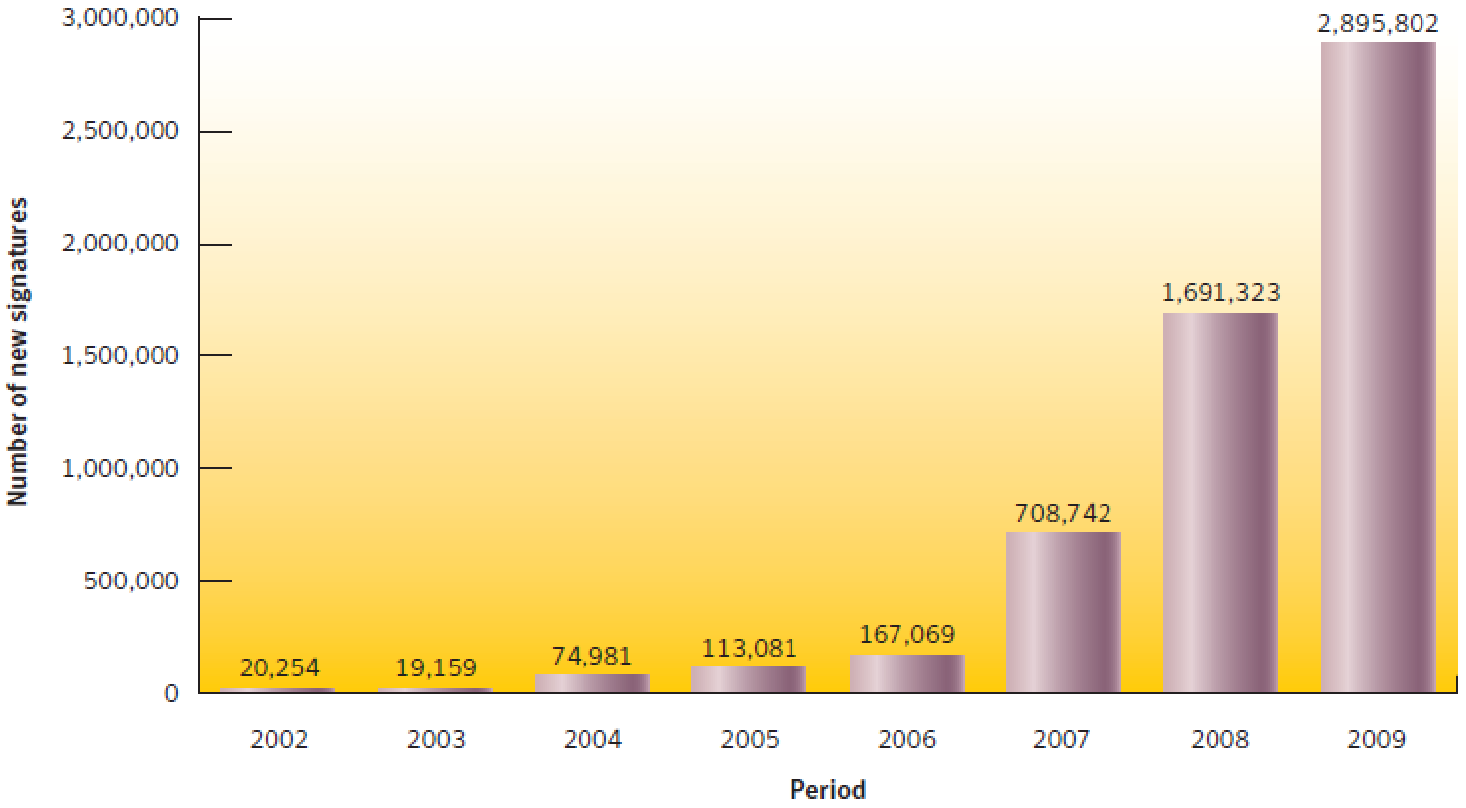
Phase 2 Partners (6/2009 – 3/2011):
CSC – IT Center for Science, Cybercube, F-Secure, Ericsson, Nokia, Nokia Siemens Networks, Stonesoft, TeliaSonera Finland, Aalto University, Universities of Helsinki, Jyväskylä and Turku, Tampere University of Technology, VTT Technical Research Centre of Finland, Tivit

Trends in security landscape

The following trends are characteristic for the development of security landscape of the Internet over the past few years:

- Amount of malicious activity has increased rapidly.
- Attacks have become web based.
- Attackers have moved away from nuisance towards activities that are motivated by financial gain.
- Professionalization and commercialization of malicious activities.

Trends in security landscape



New malicious code signatures

Symantec Internet security threat report XV, 2010

Trends in security landscape

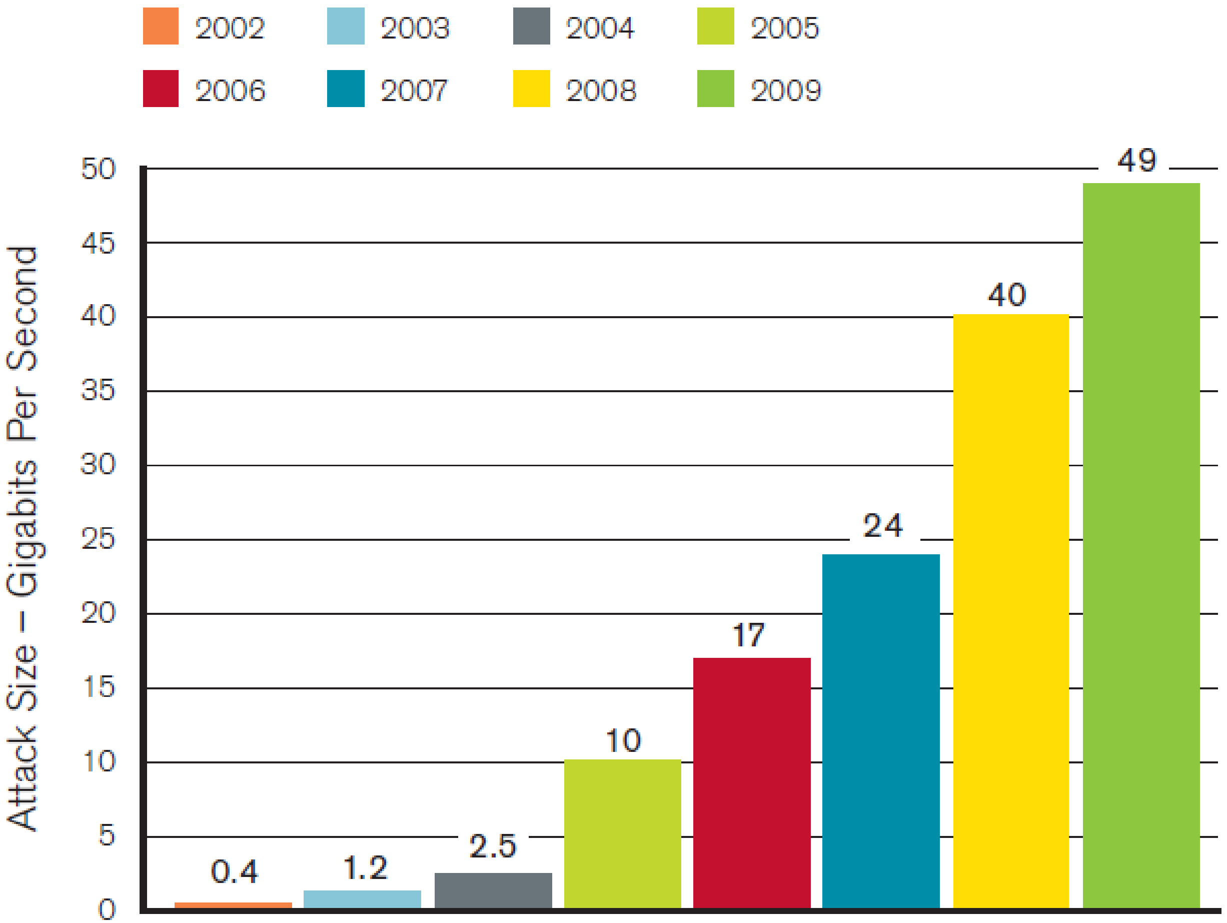


***Figure 1:** Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Trends in security landscape

Some typical goals of the attackers are as follows:

- **Theft of credit card and financial account information**
- **Theft of identity information**
- **Taking control of target computers**
- **Extortion**
- **Ruining critical systems and infrastructure**

Concrete research problems

How to improve security of Internet so that the society cannot be damaged through the Internet.

This goal translated to the following subproblems:

- how modern data analysis can be used to improve information security,
- how trust, trustworthiness and reputation of objects can be evaluated and used to protect users,
- how to mitigate the unwanted traffic problem.

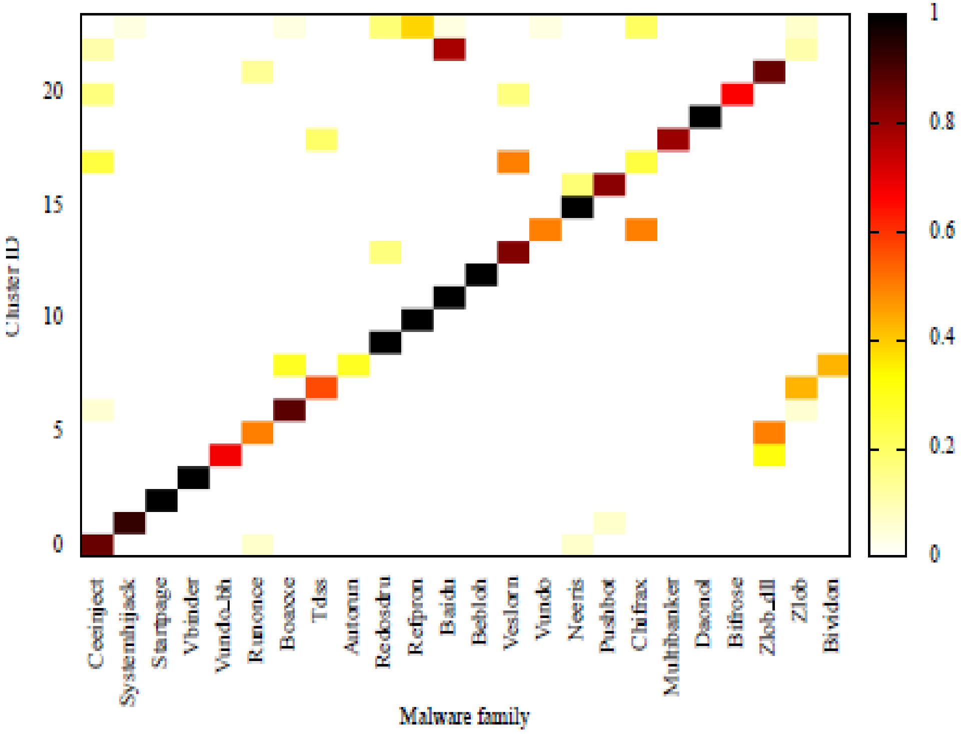
Data analysis for information security

- **Malicious programs are automatically created.**
- **Hence anti-virus software vendors receive tens of thousands of new potentially malicious program samples every day.**
- **Signature based detection must be augmented with new approaches.**

- **Two different machine learning based approaches:**
  - **Analysis based on dynamic properties of programs**
  - **Analysis based on static properties of programs**

Data analysis for information security
Call graph similarity based clustering

- One way to automatically generate new malicious samples is to slightly modify an existing one. Hence the static structure of the two versions are often similar.
- Measure distance between two call graphs by the number of elementary graph modifications required to make the call graphs isomorphic (graph edit distance).
- Cluster samples using graph edit distance.



(a) trained *k*-medoids clustering.

Data analysis for information security
Classification using SVM

- Behaviour of samples are described by textual fields, e.g., field containing name of created file.
- Aim at good precision with good enough recall, i.e.,
  - if a sample is classified as malicious it is malicious with high probability, and
  - big enough proportion of malicious samples are classified as malicious.

- An SVM based classifier using Gaussian kernel
- Evaluated with a dataset containg ~250k samples from a time span of about 2.5 years.

- Cumulatitive precision was 99.923% and recall 53.52%.

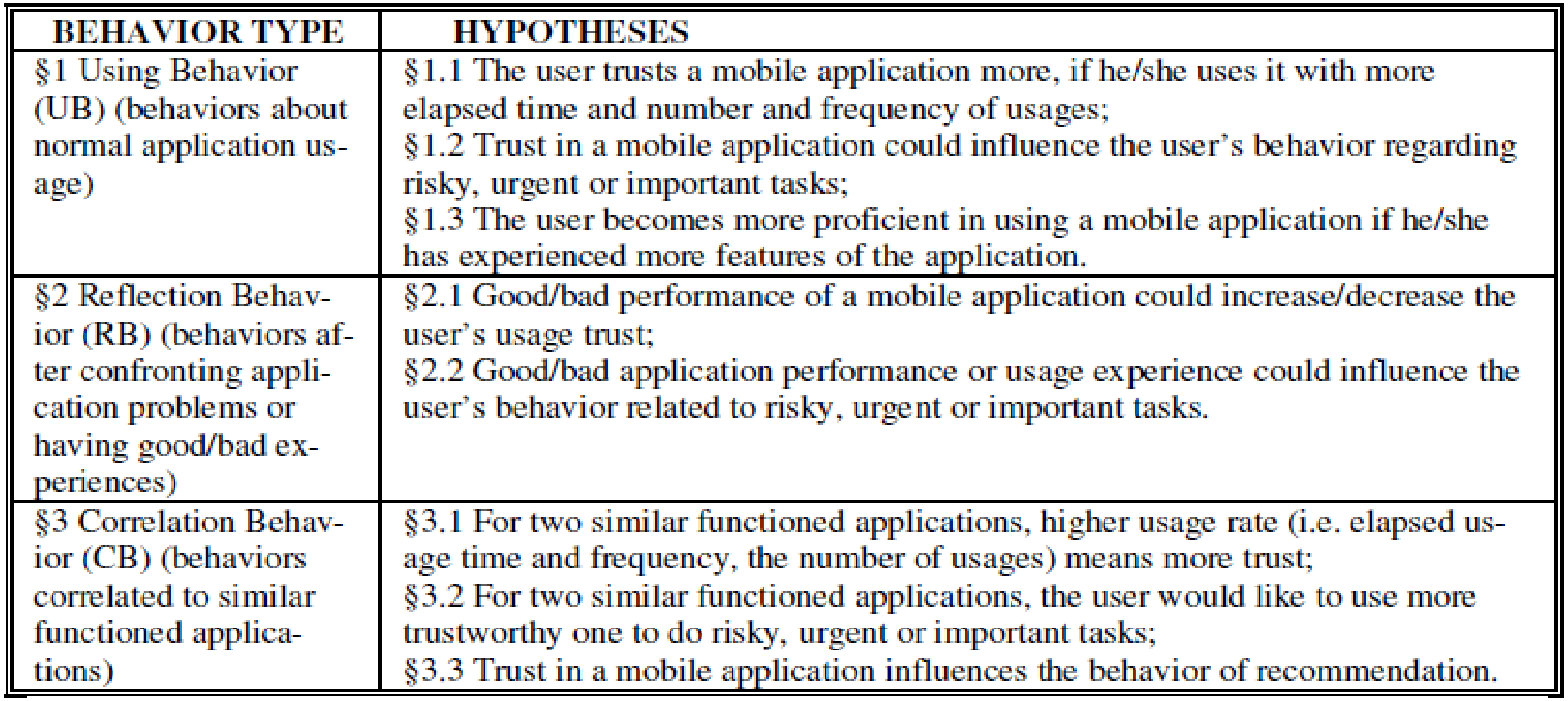
Trust and reputation

- Mobile devices have been becoming open platforms to install and execute various applications. Users’ trust to an application will become a crucial issue that impacts its success.
- Explore trust of mobile applications based on users’ behaviors, and propose a conceptual trust model

- Research question: what interaction behaviors are related to the user’s trust in a mobile application.
- Hypothesis: user’s trust in a mobile application can be studied during the appliaction usage.

Trust and reputation

- **Trust related behvior**



BEHAVIOR TYPE	HYPOTHESES
§1 Using Behavior (UB) (behaviors about normal application usage)	§1.1 The user trusts a mobile application more, if he/she uses it with more elapsed time and number and frequency of usages; §1.2 Trust in a mobile application could influence the user's behavior regarding risky, urgent or important tasks; §1.3 The user becomes more proficient in using a mobile application if he/she has experienced more features of the application.
§2 Reflection Behavior (RB) (behaviors after confronting application problems or having good/bad experiences)	§2.1 Good/bad performance of a mobile application could increase/decrease the user's usage trust; §2.2 Good/bad application performance or usage experience could influence the user's behavior related to risky, urgent or important tasks.
§3 Correlation Behavior (CB) (behaviors correlated to similar functioned applications)	§3.1 For two similar functioned applications, higher usage rate (i.e. elapsed usage time and frequency, the number of usages) means more trust; §3.2 For two similar functioned applications, the user would like to use more trustworthy one to do risky, urgent or important tasks; §3.3 Trust in a mobile application influences the behavior of recommendation.

Trust and reputation

UB1: normal usage behavior

1. The more times you use the messaging, the more you trust it.
2. The more frequently you use the messaging, the more you need it.
3. The longer time you use the messaging, the more you trust it.

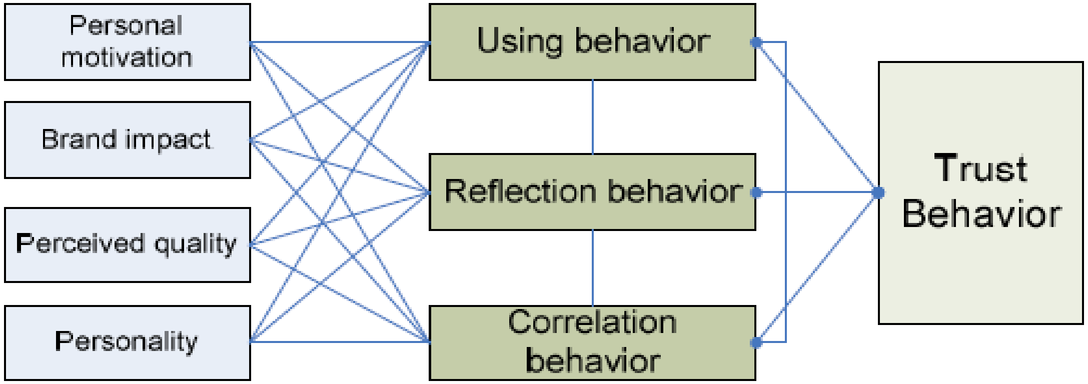


Fig. 1. Proposed trust model

Unwanted traffic

- Network level payload based access policy
  - In traditional firewalls access policy decisions are based on network address information in the packets
  - In payload based access policy application protocol or application is first identified and based on this information access policy decision is made.
  - This means that in the beginning of each connection traffic is first allowed and after the application protocol has been identified the policy decision is made.

VTT creates business from technology