COST WG 4 Meeting
April 27, 2009, Vienna, Austria

Network Management – Role of Risk and Security Management

Burkhard Stiller[1,2]

*[1] Communication Systems Group CSG,
Department of Informatics IFI, University of Zürich UZH
[2] associated with the D-ITET, ETH Zürich*

Assumptions

Knowledge and News!

Risk Management

Necessities and Gaps?

Assumptions: IP Remains* (Evolution)

- ❑ Core network
  - – Sufficient bandwidth available in the core network
    - Optical network technologies
  - – Operator of core network
    - Offers simple data forwarding interface
    - Does not expose management capabilities to its customers
- ❑ Access network
  - – Bandwidth of the access network may vary
    - E.g., in case of a wireless access network
  - – Additional functionality is needed for a node
    - To operate adequately, *e.g.*, with resource constraints or changes

** At least for some other hours in the next couple of days ...*

Knowledge in the Domain

- ❑ We “do know” about handling separate networking principles separately (partly incomplete):
  - Mobility, wireless, ad-hoc
  - Security (privacy, retention)
  - QoS, Traffic types/classification
  - Overlays
  - Virtualization
  - Error detection, dependability
  - Context-awareness
  - Accounting
  - Economics
  - …
- ❑ We “do know” about dealing with management “algorithms” (again, partly incomplete):
  - Network management (FCAPS)
  - Service management
  - Security (ID, privacy) management
  - Traffic/queue management
  - Address management (routing)
  - Bandwidth, policy management
  - Self-management (self-*)
  - Autonomic management
  - Layered NetMgt Architectures
  - …

Architecture* Effects — No News!

Observation: Almost all of this is conceptionally independent of the Internet today or basically any of the FI architectures.

- ❑ We “apply” research/engineering methodologies correctly:
  - Analysis, modeling, (cross-layer) design, engineering, simulation, implementation, operations
  - Use cases, statistics, evaluation, interpretation, discussion, conclusions

** Logical OR for current and Future Internet Architecture*

Next Features to Come (1)

- Self-management:
  - A device is capable of configuring itself based on guidelines
  - End users and access network devices equipped with autonomic capabilities:
    - *E.g.*, information sensing, decision making, and enforcement
  - Decision making based on programmability not restricted to device manufacturer
- Risk management:
  - Determination of risks for a network and its services offered in a (fully) distributed manner
    - Definition of a relation between infrastructure and economics

Risk and Definitions

- Risk: The combination of the probability of an event and its consequence

Accordig to ISO

- Risk assessment: The process by which risks are identified and the impact of those risks determined.
- Risk management: The process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to the acceptable level, and maintaining that level of risk.

Risk Management

According to Microsoft

- Reactive approach
  - Safety, damage, determination of cause of damage, repair damage, review response and update policies
- Proactive approach
  - Identify business assets
  - Determine what damage an attack against an asset could cause to the organization
  - Identify the security vulnerabilities that the attack could exploit
  - Determine how to minimize the risk of attack by implementing appropriate controls

Quantifications (1)

- Determining the monetary value of an asset is the important prerequisite:
  - Organizations maintain a list of asset values as part of their business continuity plans.
- Single Loss Expectancy (SLE)
  - The SLE is the total amount of revenue that is lost from a single occurrence of the risk.
  - Calculate the SLE by multiplying the asset value by the exposure factor, which represents the percentage of loss that a realized threat could have on a certain asset.

According to Microsoft

Quantifications (2)

- Annual Rate of Occurrence (ARO)
  - ARO is the number of times that you reasonably expect the risk to occur during one year.
- Annual Loss Expectancy (ALE)
  - Calculate ALE value by multiplying the SLE by the ARO.
  - The ALE is similar to the relative rank of a qualitative risk analysis.
- Return On Security Investment (ROSI)
  - Estimate the cost of controls by equation
    ROSI = (ALE before control) – (ALE after control) – (annual cost of control
- **Problem: Technicians and economists live in two independent worlds!**

Next Features to Come (2)

- Content + Services
  - Management of the data (not only the network any more)
  - Management of the service provisioning, the service offering, the service maintenance, and the service tear-down
- Revenue models of the FI
  - Advertisement (?)
  - Selling content *and* user information, for sure services
  - Various quality levels, quality of experience levels
  - Distinct reliability classes (risk-assessed, risk-certified?)

Management Necessities and Gaps?

❑ Key necessities of management aspects not met today:

- Determination of risk of service failure, unavailability – insurance
- Clear distinction of time and control loop generalities for short-/mid-/long-term actions – proven separation of automated/human-based management tasks
- Incentive-compatible, operationally-efficient, economically-viable, and application-independent traffic management (multi-player game)
- Non-voice QoE “measurements”

❑ Plus key management gaps seen today for the FI:

Design

- Well-restricted set of functionality and simple architecture to be considered – don‘t do all in NM!

Mod./Eng.

- Concrete mechanisms, algorithms, configurations required for (new) FI arch – principles are known/understood

Eval.

- Economic traffic management

Ana./Mod.

- Robust, non-self-destructive mgt. mechanisms (proven)
- Handling of network neutrality and regulatory requirements

Conclusions

1. Evolutionary (or even revolutionary) approaches of **security management** any FI architecture is NOT a problem, IFF security management algorithms are researched and engineered jointly.

2. **Risk management** is missing, but a **must**. Security aspects (HW, SW, FW, service), technology, and algorithms are known, but network management tasks embedded with risk management parameters are still a dream … to be made true*, soon.

** Effects on user behavior (social), economics of overhead, legal acts.*