

# A VISUALIZATION AND MODELING TOOL FOR SECURITY METRICS AND MEASUREMENTS MANAGEMENT

**Reijo M. Savola**

VTT Technical Research Centre of Finland



Teknologiasta liiketoimintaa

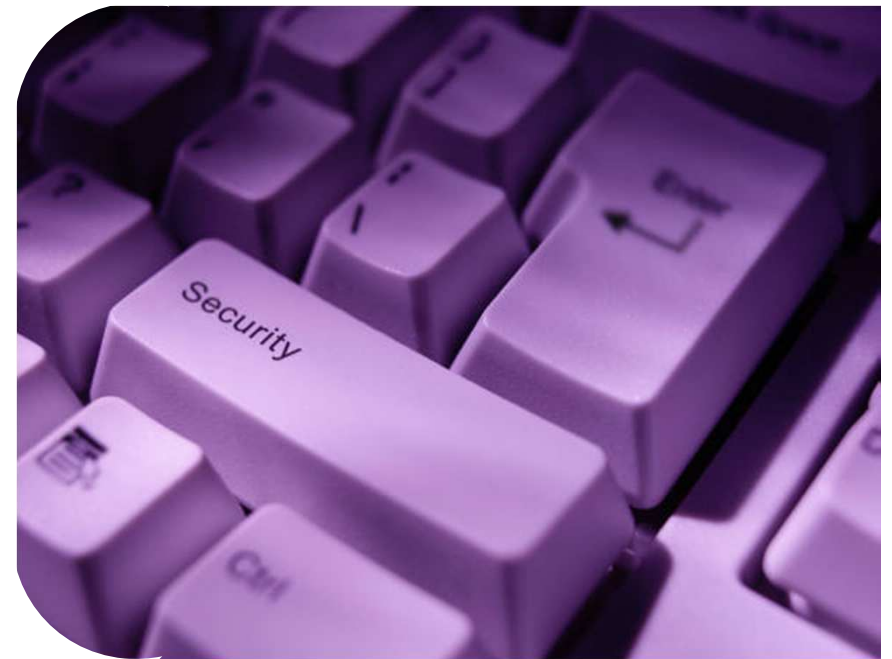


ISSA 2011

Johannesburg, South Africa

# CONTENTS

- Introduction to Security Metrics
- Metrics Visualization System
- Future Directions in Security Metrics
- Conclusions



"An activity cannot be managed well if it cannot be measured."

# INTRODUCTION TO SECURITY METRICS

## Measurement target, objectives, methods



Measurement Objectives



Measurement methods

*Target can be*

- *Organisation*
- *Product*
- *Operation of a technical system, service etc.*
- *Human behaviour*
- *Etc.*



# INTRODUCTION TO SECURITY METRICS

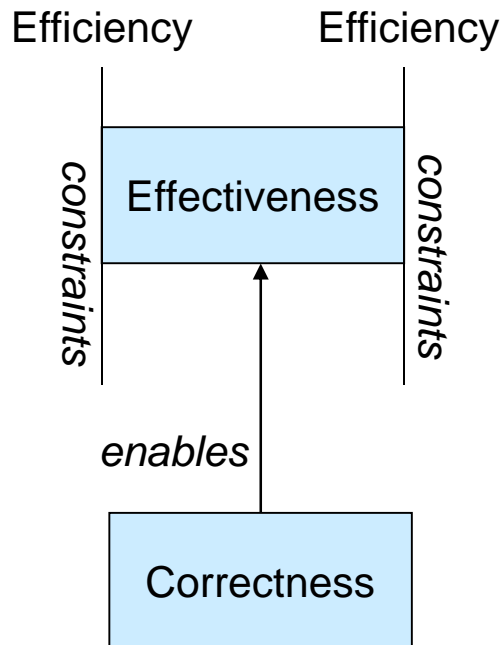
## Operational characteristics challenges of security and privacy metrics\*

- **Complexity of software systems:** all potential state transitions are not known
- **Uncertainty:** it is hard to assess how likely are transitions between states
- **Non-stationarity:** security risks can vary, even rapidly, over time
- **Limited observability:** it is hard to observe, measure and to correctly detect all events
- **Maliciousness:** security threat agents can be strategically intelligent
- **Security and privacy cannot be measured as a universal property!**
- **However, indicators based on security and privacy requirements are possible!**

\* Verendel, V. Some Problems in Quantified Security, Licentiate Thesis, Chalmers University of Technology, Göteborg, Sweden, 2010.

# INTRODUCTION TO SECURITY METRICS

## Fundamental measurement objectives



- **SECURITY CONTROL**

- **Security controls are means of managing privacy risk, which can be administrative, technical, management, or legal in nature** (based on ISO/IEC 27000's security control concept)

- **SECURITY CONTROL CORRECTNESS**

- **Security correctness denotes assurance that privacy controls have been rightly implemented in the SuI, and the system, its components, interfaces and the processed data meet privacy requirements.**

- **SECURITY CONTROL EFFECTIVENESS**

← THE MAIN OBJECTIVE!

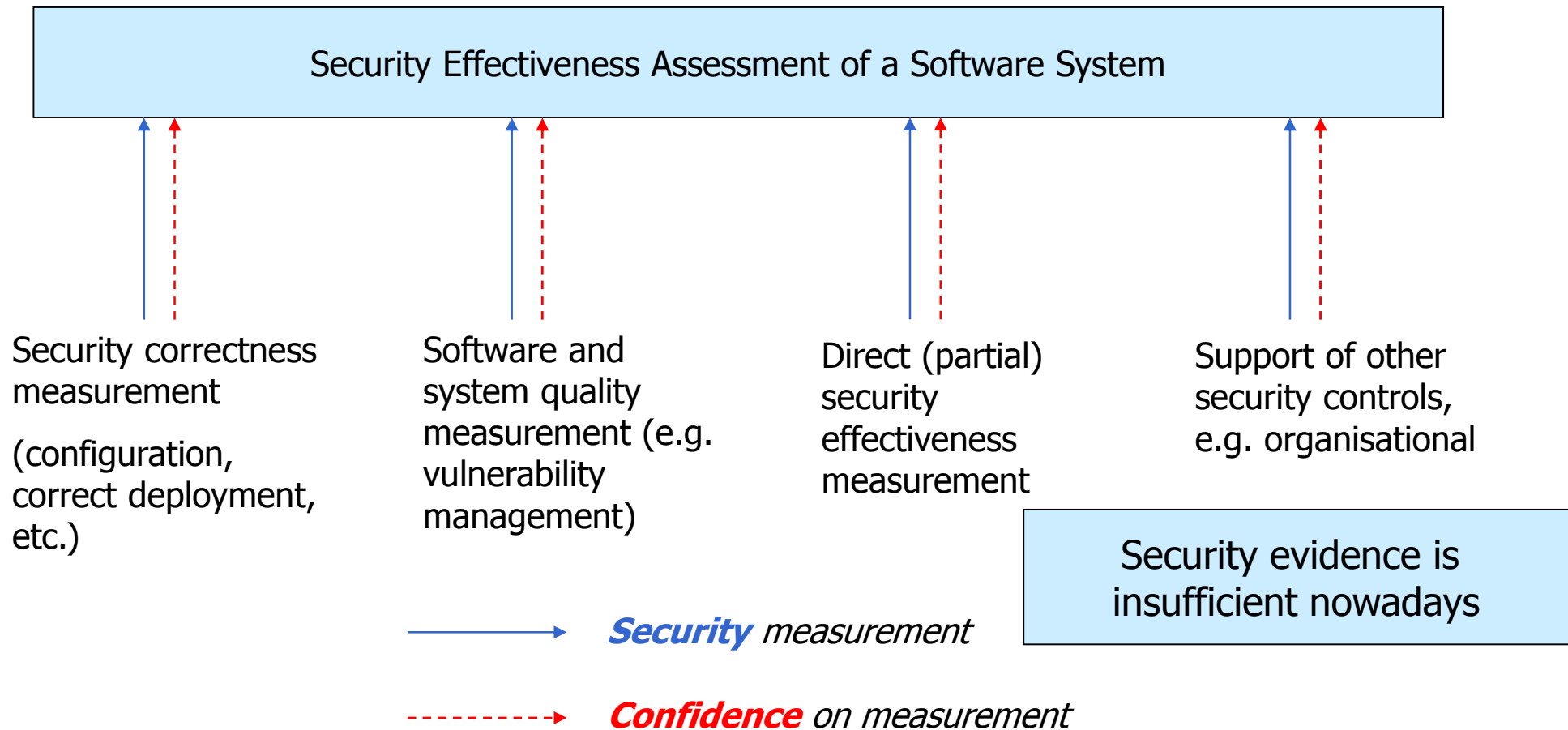
- **Security effectiveness denotes assurance that stated privacy objectives are met in the SuI and expectations for resiliency in the use environment are satisfied, while the SuI does not behave in any other way than what is intended.**

- **SECURITY CONTROL EFFICIENCY**

- **Security efficiency denotes assurance that the adequate privacy quality has been achieved in the SuI meeting resource, time and cost constraints.**

# INTRODUCTION TO SECURITY METRICS

## Factors contributing to security effectiveness



# INTRODUCTION TO SECURITY METRICS

## Interview Results from 2011 in Finland (24 Interviews)

### **Needs for Security Metrics and Measurements**

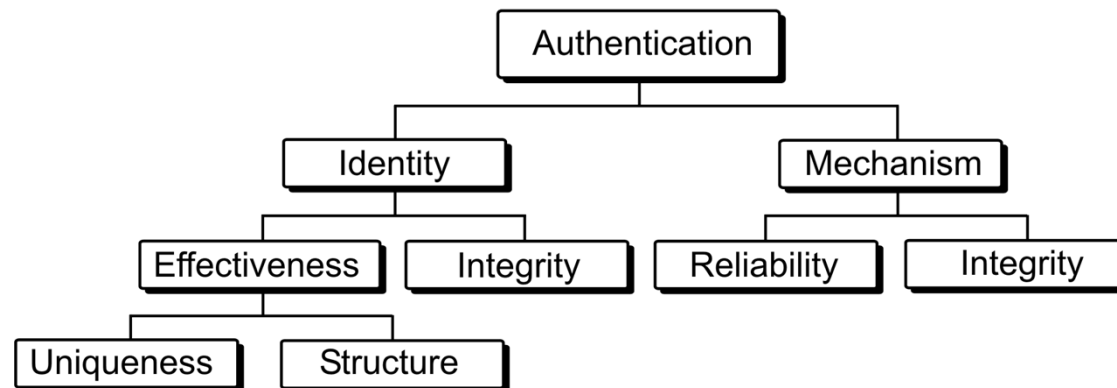
- Transparency emphasized
- Evidence about security management
- Evidence about security control deployment
- Evidence about operational security issues
- Accreditation, auditing, certification evidence and supporting test reports
- Metrics should be clear, meaningful and should have value to their user
- Risk-based metrics needed
- Security and business goal alignment
- Metrics for monitoring
- Standardized metrics
- Concentrating on the application layer
- Non-repudiation service for the measurements

# INTRODUCTION TO SECURITY METRICS

## Metrics development by decomposition

- (1) Identify successive components from each security requirement
- (2) Examine the subordinate nodes to see if further decomposition is needed. If so, repeat (1) and (2).
- (3) Terminate the decomposition when none of the leaf nodes can be decomposed any further.

### E.g. authentication:



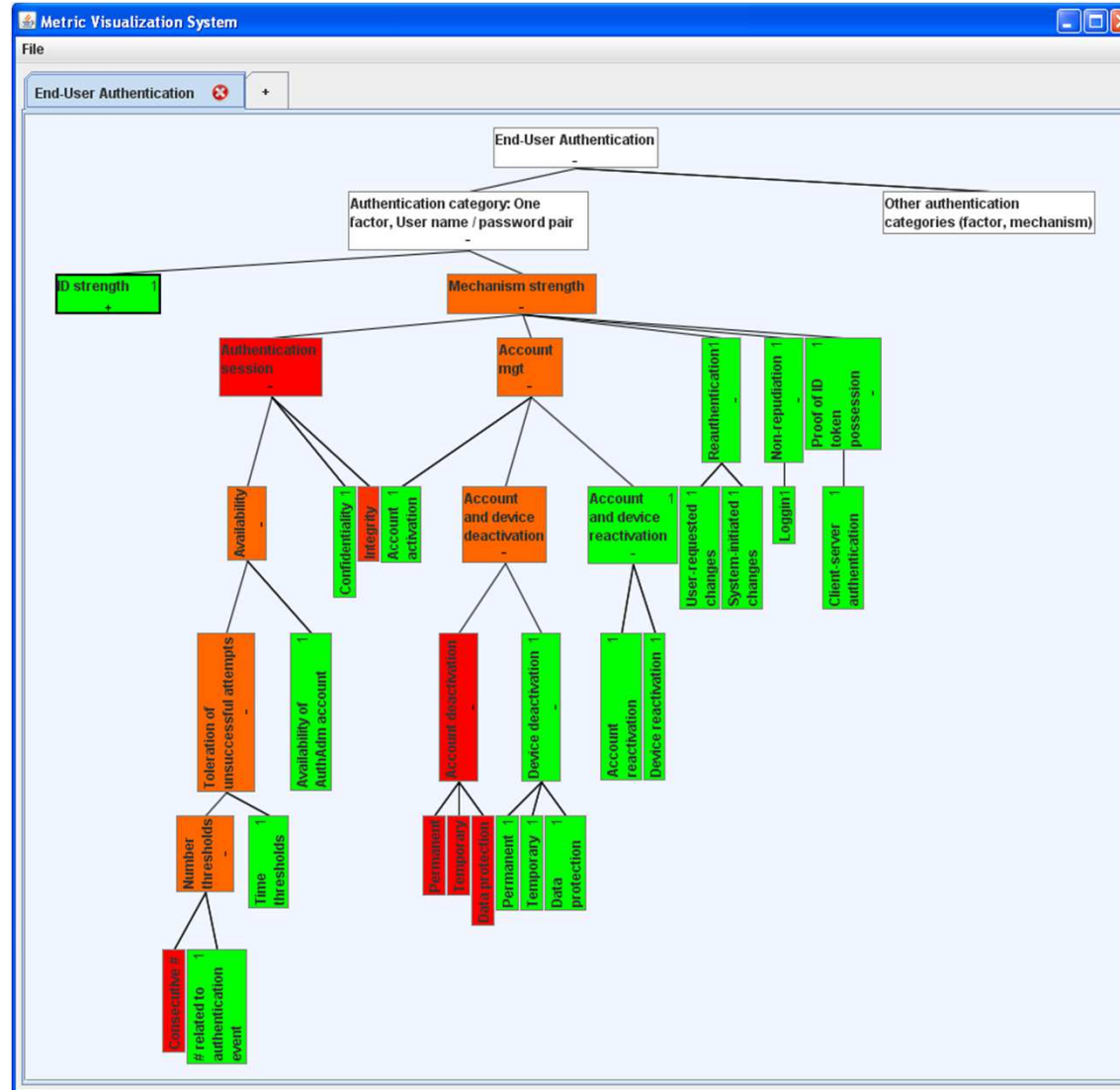
# METRICS VISUALIZATION SYSTEM (MVS)

## Needs for security metrics visualization

- Structured security metrics entities, “building blocks”:
- Meaningful metrics relationship modeling
- Alleviation of the metrics aggregation oversimplification challenges by visualization
- Measurement probe and security-measurability-enhancing mechanism support

**Plain aggregation of sub-metrics over-simplifies security related issues!**

# METRICS VISUALIZATION SYSTEM (MVS)



# METRICS VISUALIZATION SYSTEM (MVS)

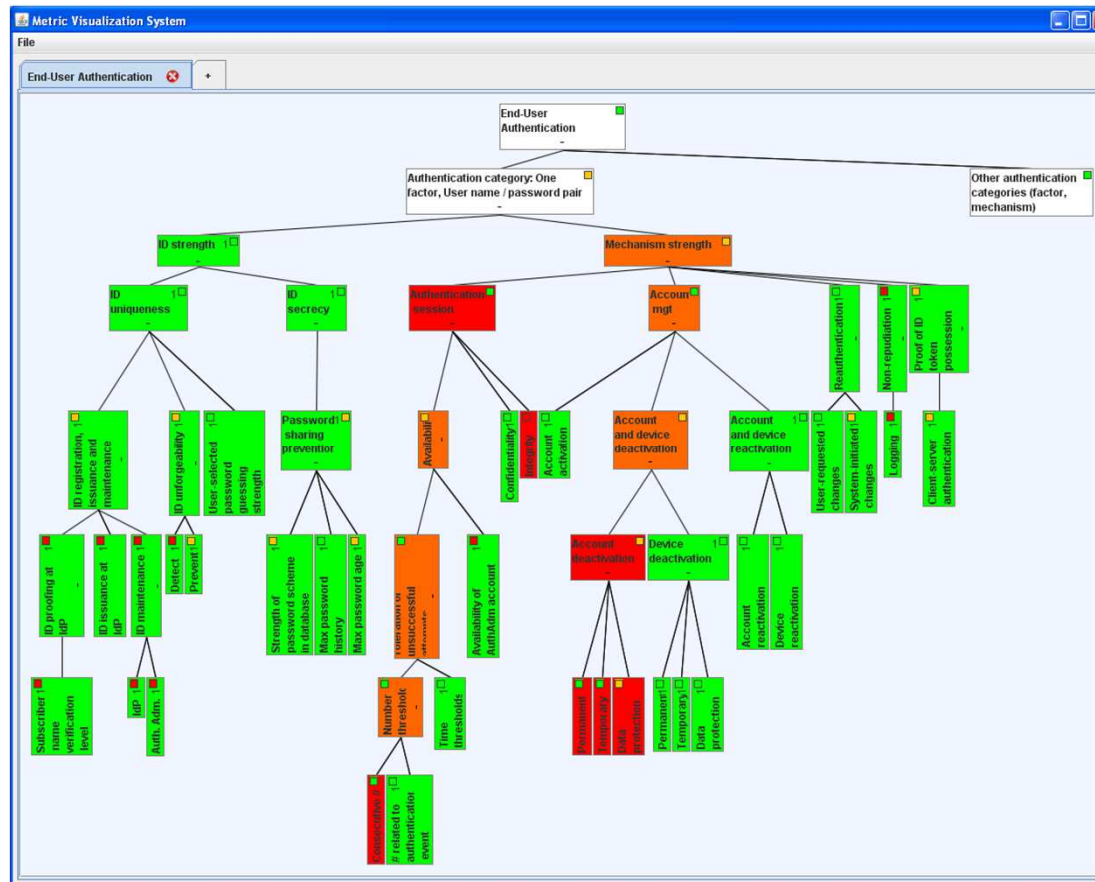
## Security Metrics Node (SMN)

- The MVS model consists of hierarchical presentation of SMNs
- Properties:
  - Distinctive name
  - Confidence value of metric/measurement (range 0...1)
  - Operation specification (logical expression)
  - Threshold criteria and associated visualization
  - Poll frequency field for automated measurements
  - Enable / disable flag for operation value evaluation

# METRICS VISUALIZATION SYSTEM (MVS)

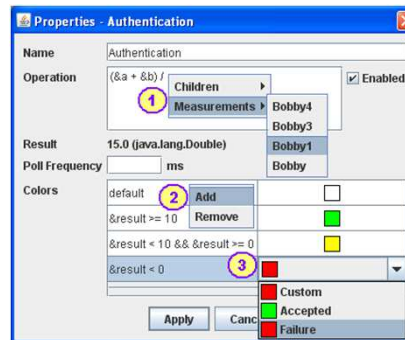
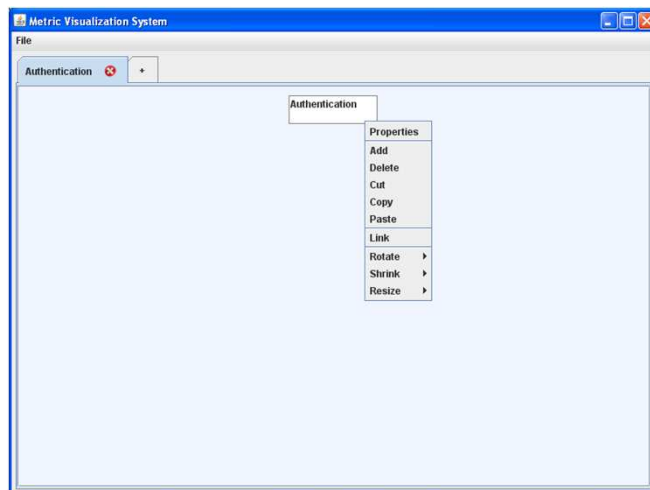
## Coloring of Nodes

- “Traffic lights” coloring makes it possible to track the status of a large number of metrics in the same view
- All SMNs can be colored or left blank



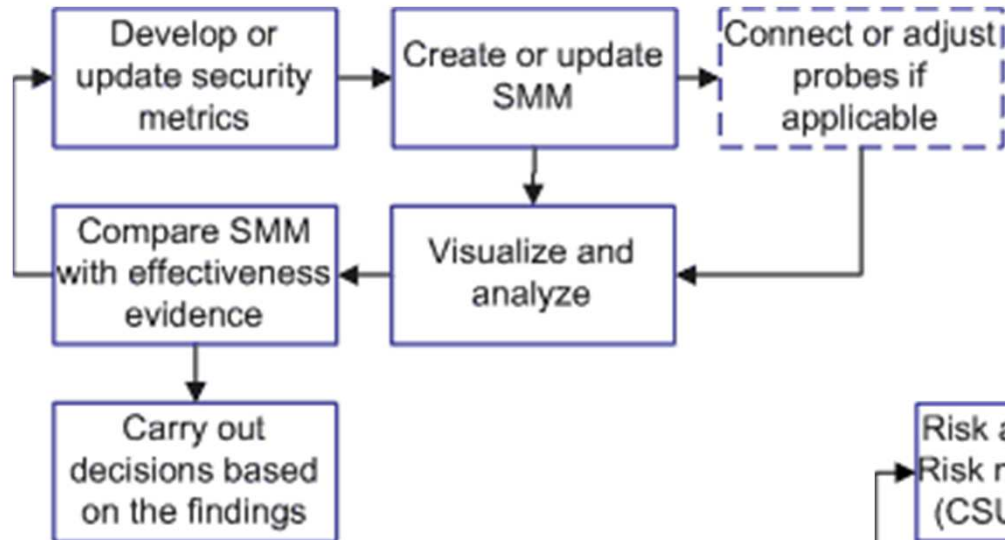
# METRICS VISUALIZATION SYSTEM (MVS) Platform Modules

- Hierarchy modeling engine
- REST (Representational State Transfer) based communication module
- Graphical working environment with pop-up menus
- Security-metrics-enhancing mechanism support:
  - Multi-point monitoring
  - Use of shared metrics, XML file structure
  - Reuse of metrics: easy interconnection of several MVS models

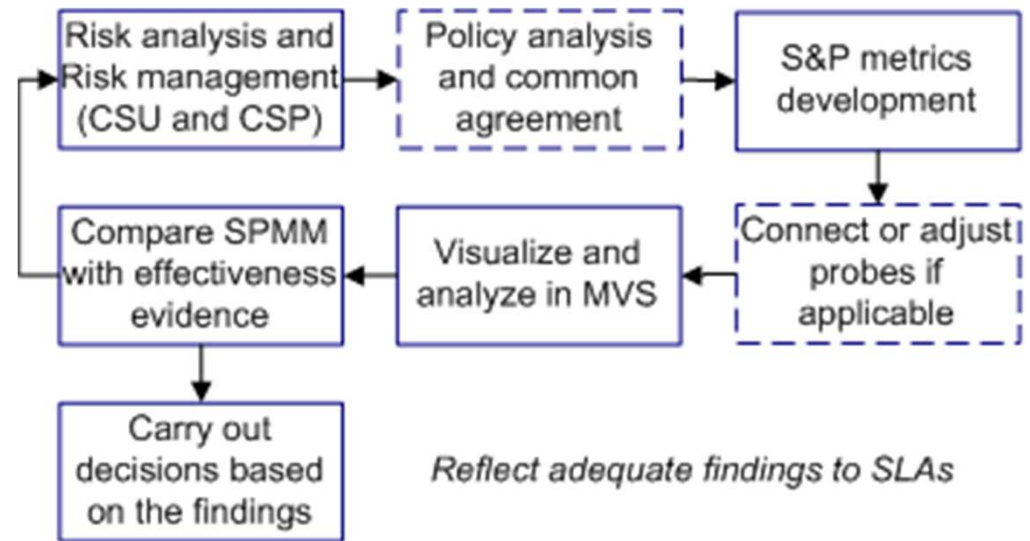


# METRICS VISUALIZATION SYSTEM (MVS)

## Process for security metrics management



E.g., application to cloud services:



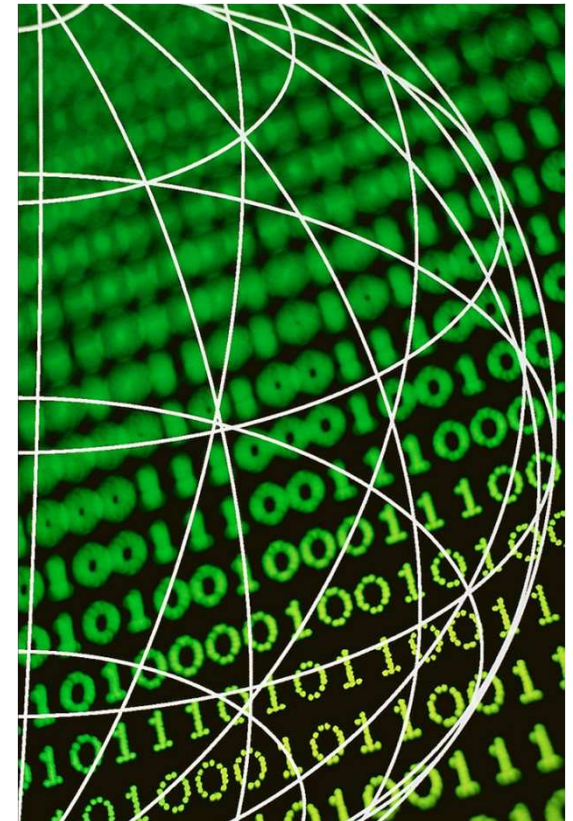
## FUTURE DIRECTIONS

- A widely-accepted “trust, security and privacy metrology” framework is needed:
  - Practical
  - Adaptive: incrementally applicable to different targets
- System intrinsic TSP measurability (utilization of existing measurements, evidence) should be exploited
- TSP-measurability-enhancing mechanisms should be built-in the systems
- Visualization of metrics and measurements is a promising direction
- Investigation of dependencies of different factors affecting security effectiveness
- Realistic cases and data is needed!!!



## CONCLUSIONS

- A research prototype of a security metrics visualization and management tool MVS developed
  - Metrics development by decomposition
  - Metrics management and visualization tool
  - Metrics management process
- It is important to be able to see higher and more detailed abstraction levels at the same time when interpreting security issues.
  - Hierarchical presentation of metrics nodes
  - Coloring schemes
- Future work needed in practical use cases, currently practical use cases are being carried out in telecommunications R&D



---

Thank you!  
Questions?