Measuring Cryptographic Primitives and Systems

Kimmo Halunen
Remember this!

- We do not have actionable metrics for measuring the strength and security of cryptographic systems from theory to practice
- Tools for building new metrics exist
- We will build better metrics in the future
Agenda

• Different levels of cryptography
• Measuring cryptography
• Current measures
• Measures from related fields
• Differences and similarities
• New measures?
Different levels of cryptography

• Theoretical level
  • Proofs, algorithms, protocols and schemes
• Applications
  • Different (software) implementations of the above
• Hardware
  • The devices that run the applications
• Auxiliaries
  • Support to the cryptographic systems e.g. network and radio links, randomness sources
Measuring cryptography

• Traditionally by a security parameter that is translated into bits
• Also by the threat model of the proof
  • Chosen-plaintext, chosen-ciphertext, random oracle etc.
• Tightness of the proof
  • How close to the underlying hard problem the actual cryptographic system is
• Attack metrics
  • Measuring the residual insecurity of the system
Current measures

• NIST and ENISA key length and algorithm recommendations
• National guidelines
• Common Criteria
• Standards
Measures from related fields

- ENISA metrics for privacy enhancing technologies
- Several systems and applications for evaluating these
- Scoring along two-dimensional axis
  - Maturity (idea – outdated) and quality (1 – 5)
- Common Criteria
- Other maturity models
Figure 5. Overview of Possible PET Maturity Level Values.
Define Target of Assessment

Select Board of Experts

Concurrent Assessments
- Gather Measurable Indicators
- Gather Expert Opinions

Elaborate PET Maturity Level and Assessment Report

Documentation and Logging
Differences and similarities

- Mathematical proofs and theorems vs. consensus by experts vs. heuristic evaluations
- One dimension vs. two or more dimensions
- Context free vs. context dependent
New measures?

• Building a new metric with the help of other metrics
• Combining ”best of both worlds”?
  • Measuring the traditional security and also the insecurity of attack metrics
• Actionable metrics at all levels!
Thank you!

Questions?