Performance Evaluation in Wireless Networks and Technologies from 2.5 G, 3G, LTE to 4G and Beyond

ICIW 2008, AICT 2008

Athens, June , 2008

Dr. Reda
Innovation Communication Technologies
Munich / Vienna

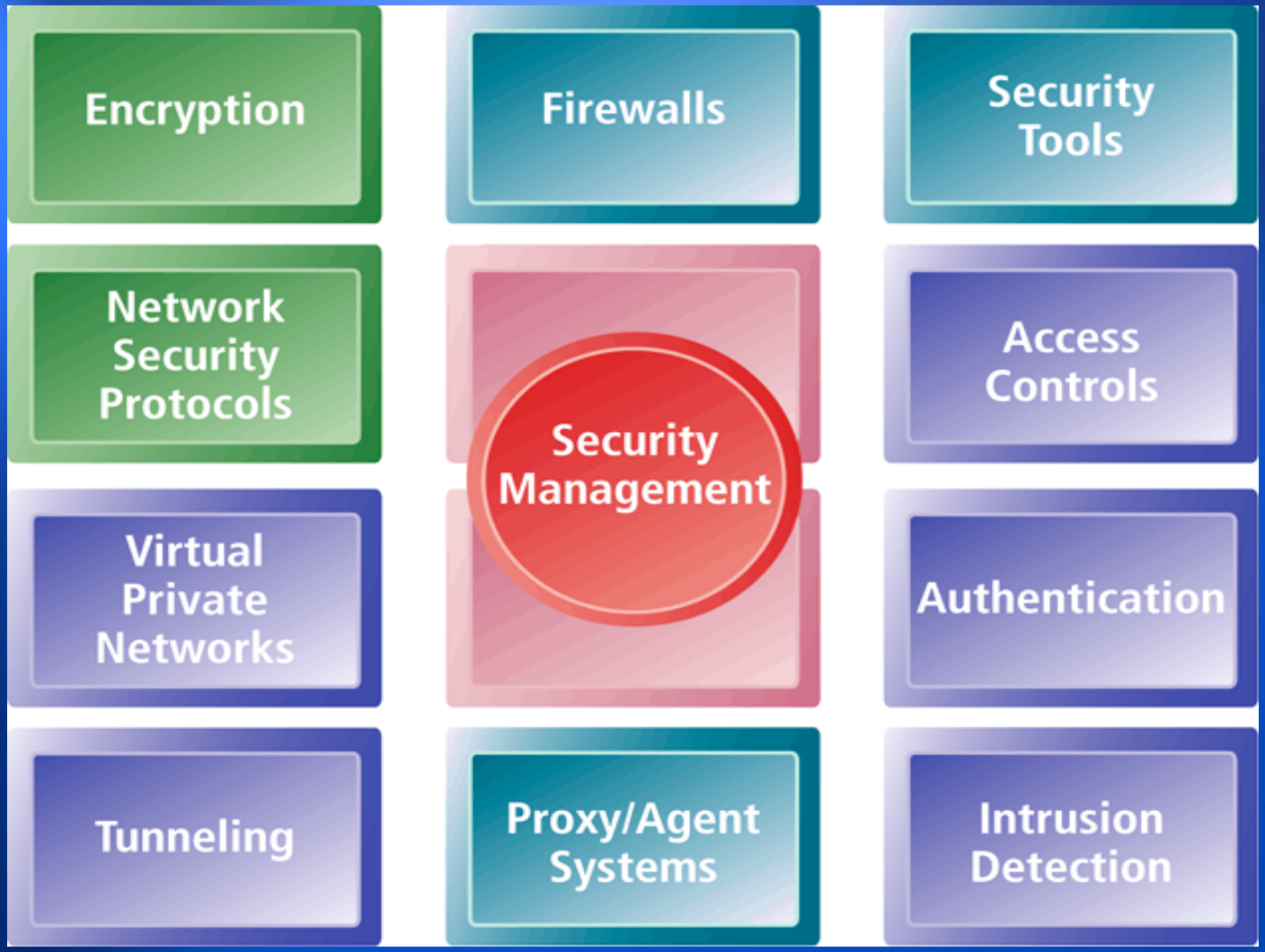
The Dilemma of Security

- The problem that we cannot get away from in computer security is that we can only have good security if everyone understands what security means, and agrees with the need for security.
- Security is a social problem, because it has no meaning until a person defines what it means to them.
- The harsh reality is the following: In practice, many users have little or no understanding of security **BIG PICTURE**. This is our biggest security hole.

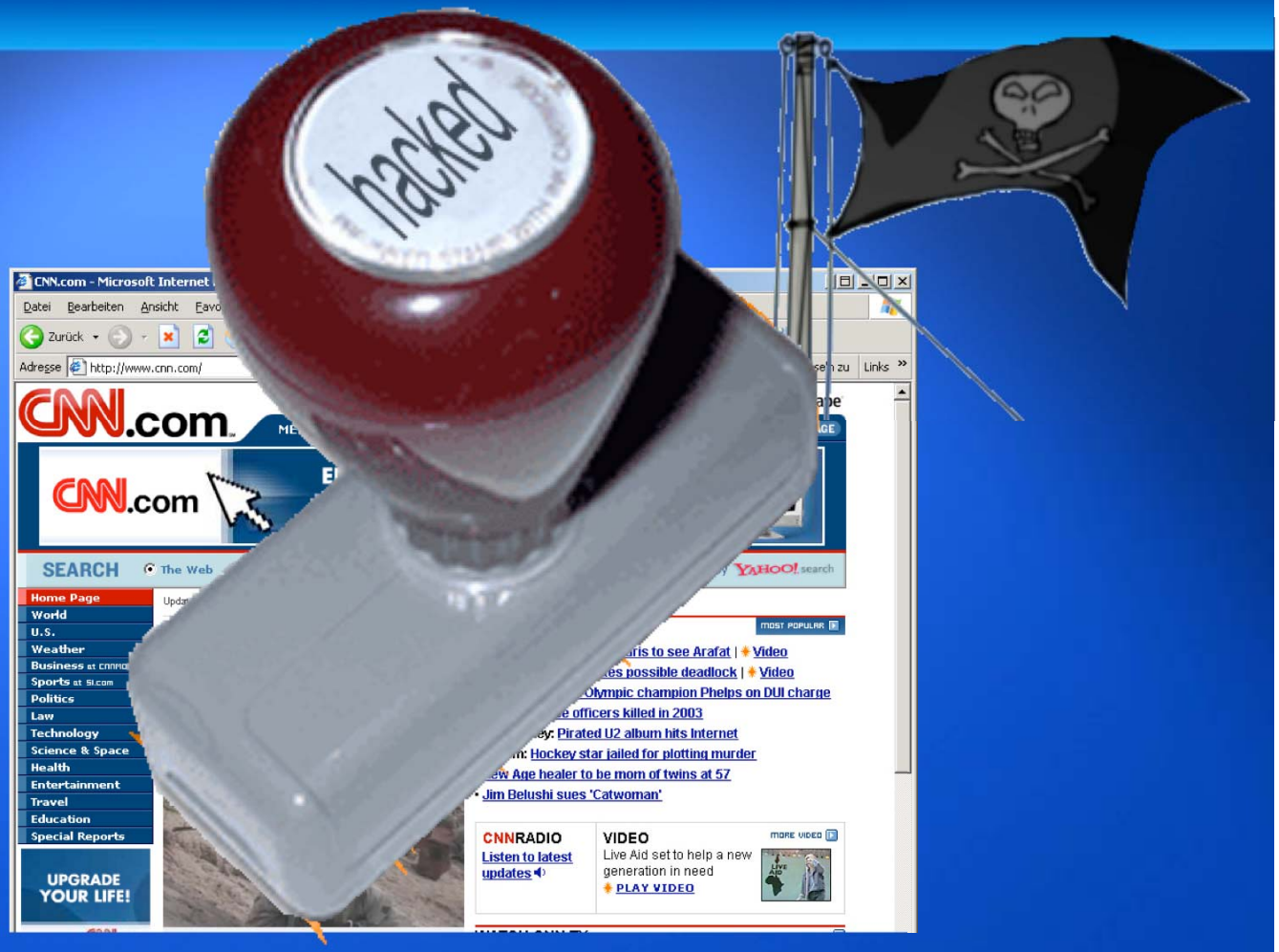
Do we have

SECURITY ?

Tools Available to Achieve Site Security

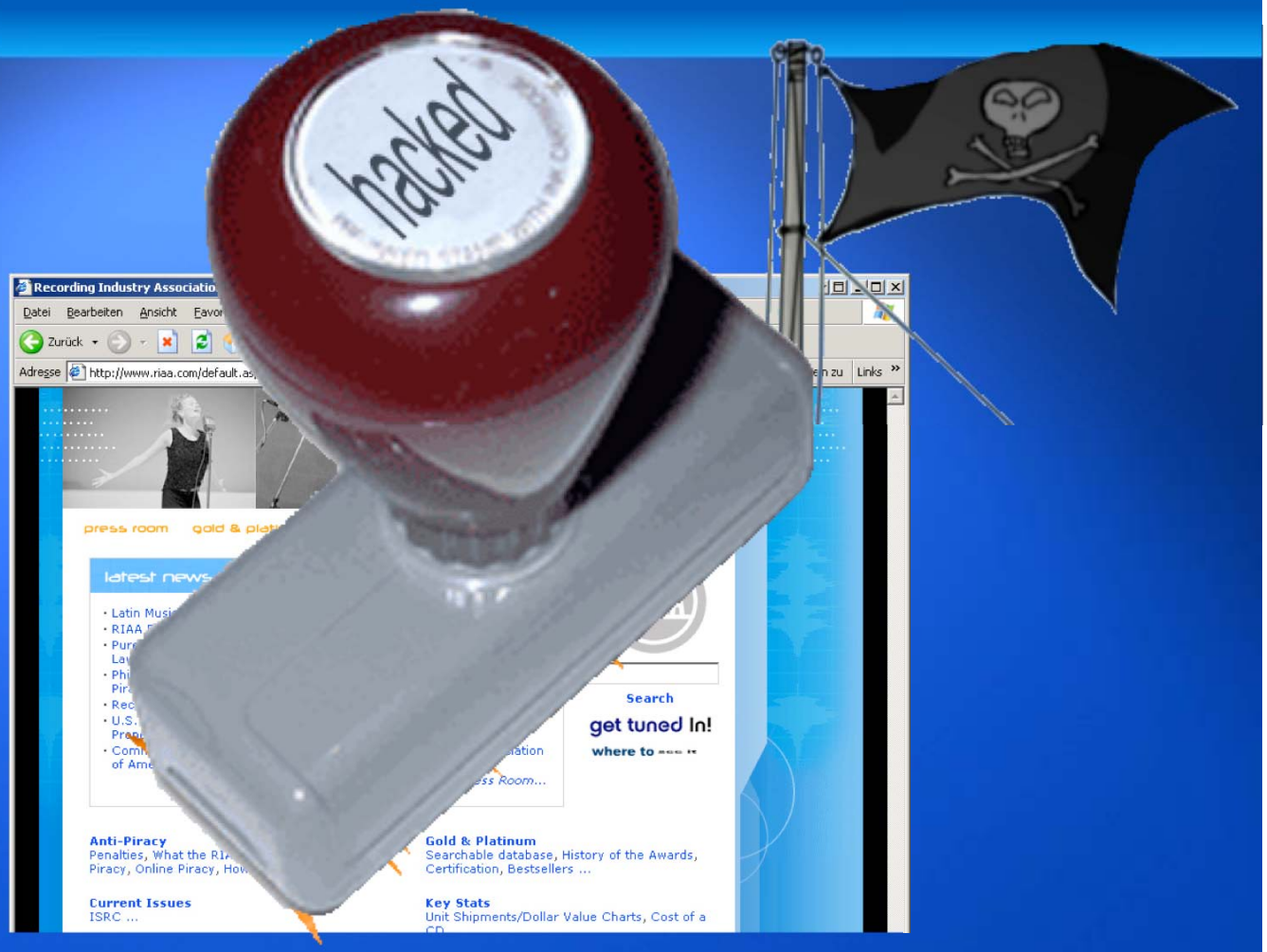


NASA – www.nasa.gov



CNN – www.cnn.com

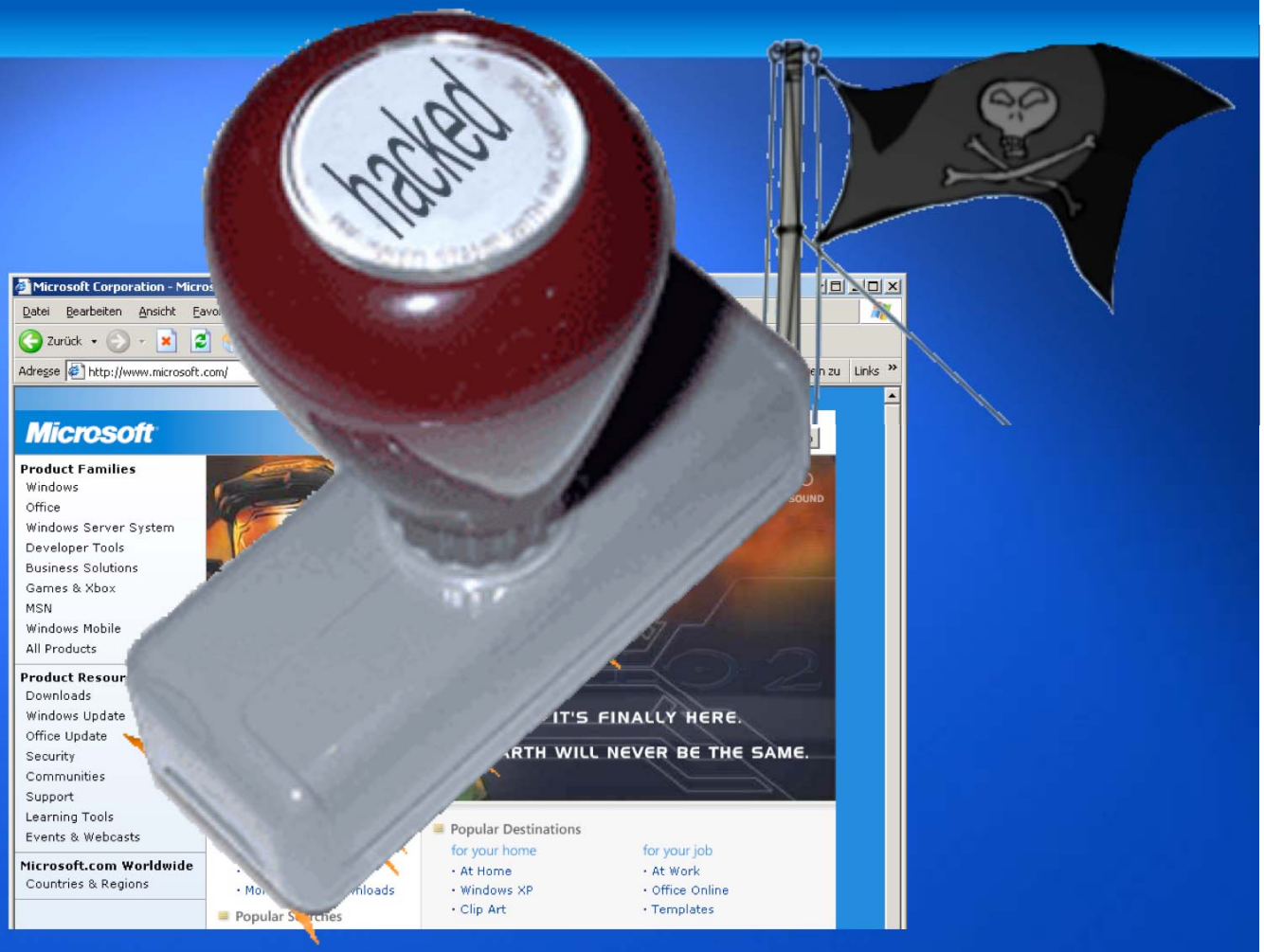
NSA – www.nsa.gov



RIAA – www.riaa.com

NAVY – www.navy.mil

Samsung - www.samsung.com

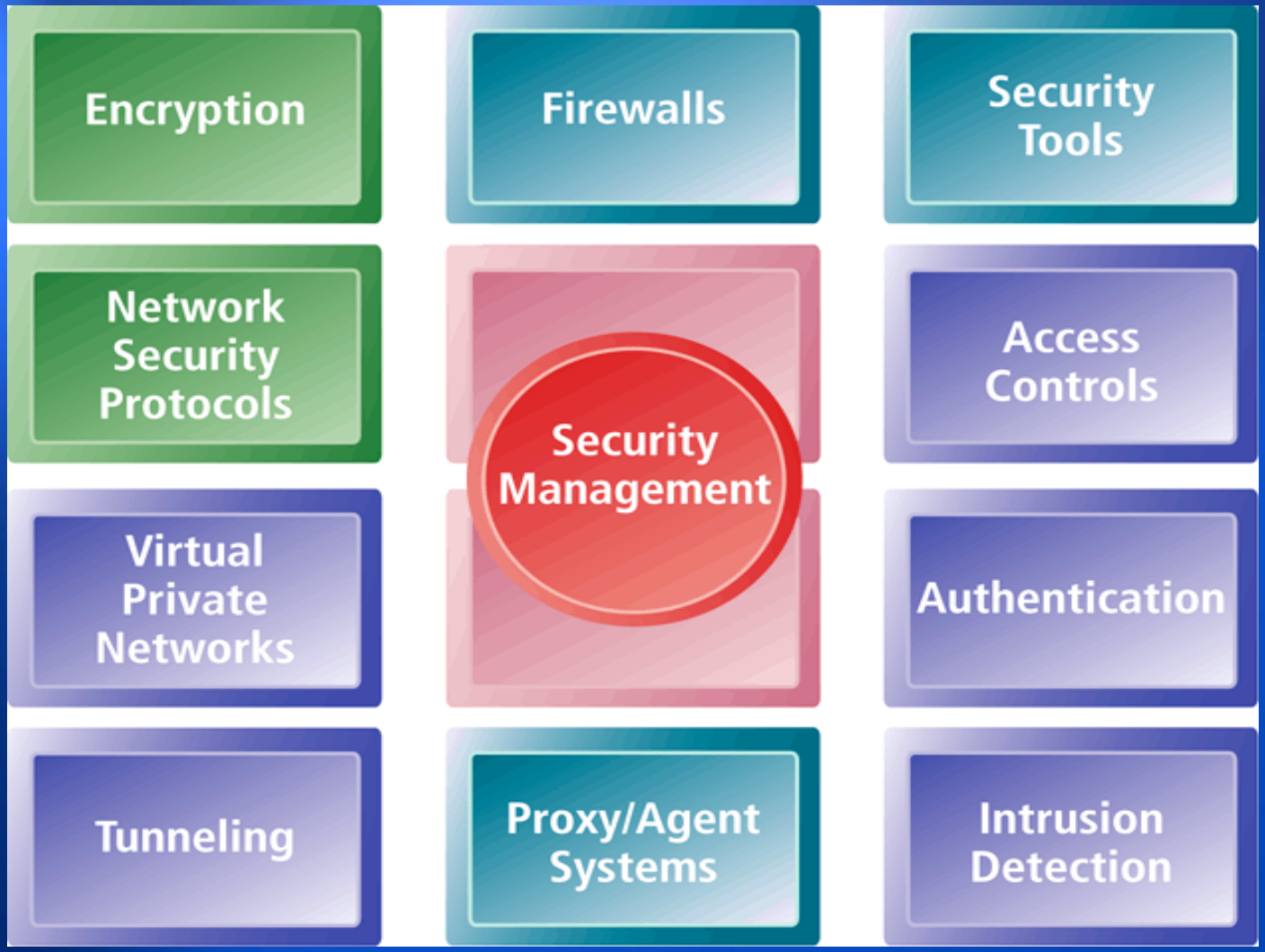


Microsoft - www.microsoft.com

Sony Music www.sonymusic.com

Security Bla Bla ….

Tools Available to Achieve Site Security

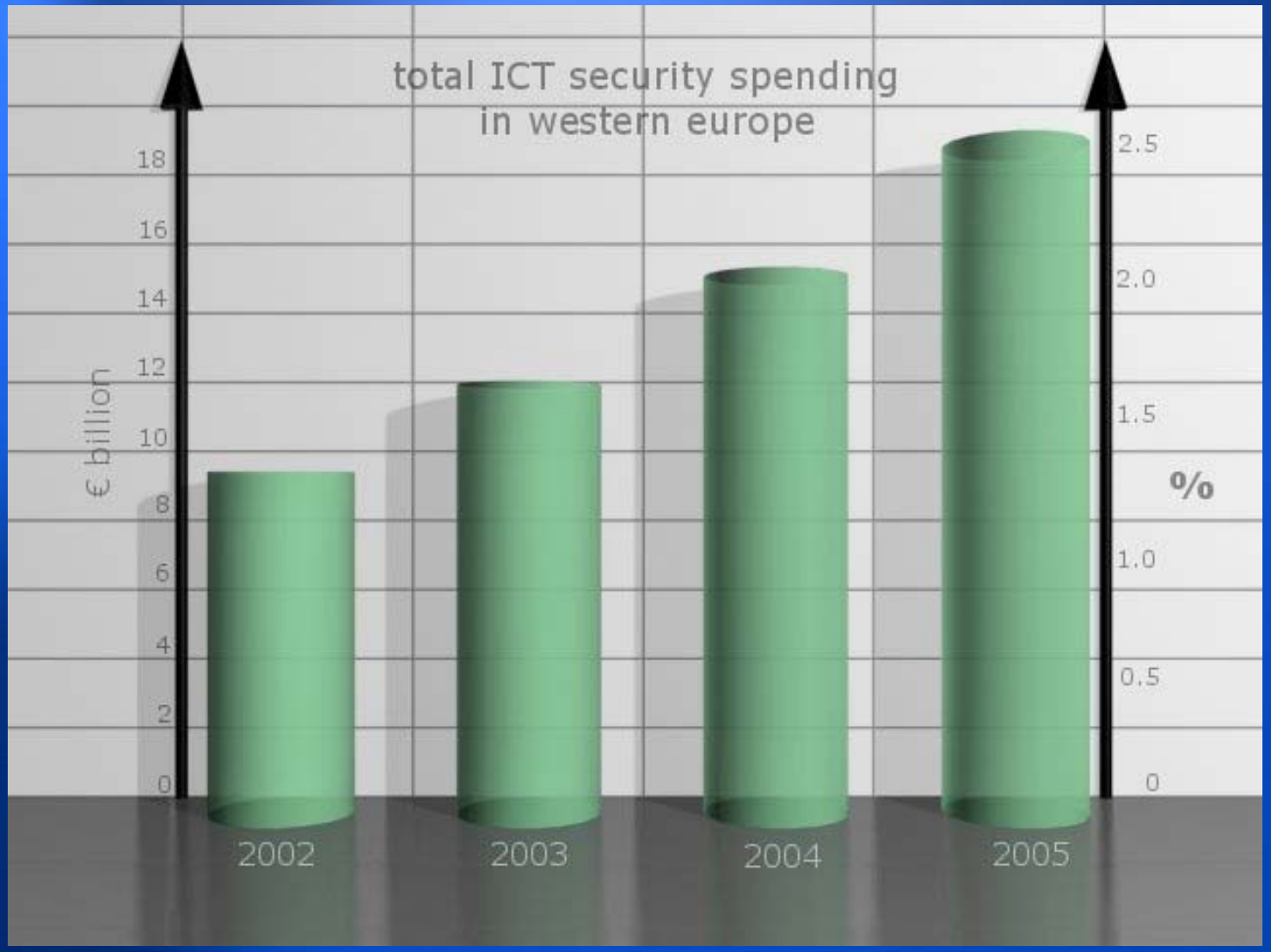


Cyber Security Risks

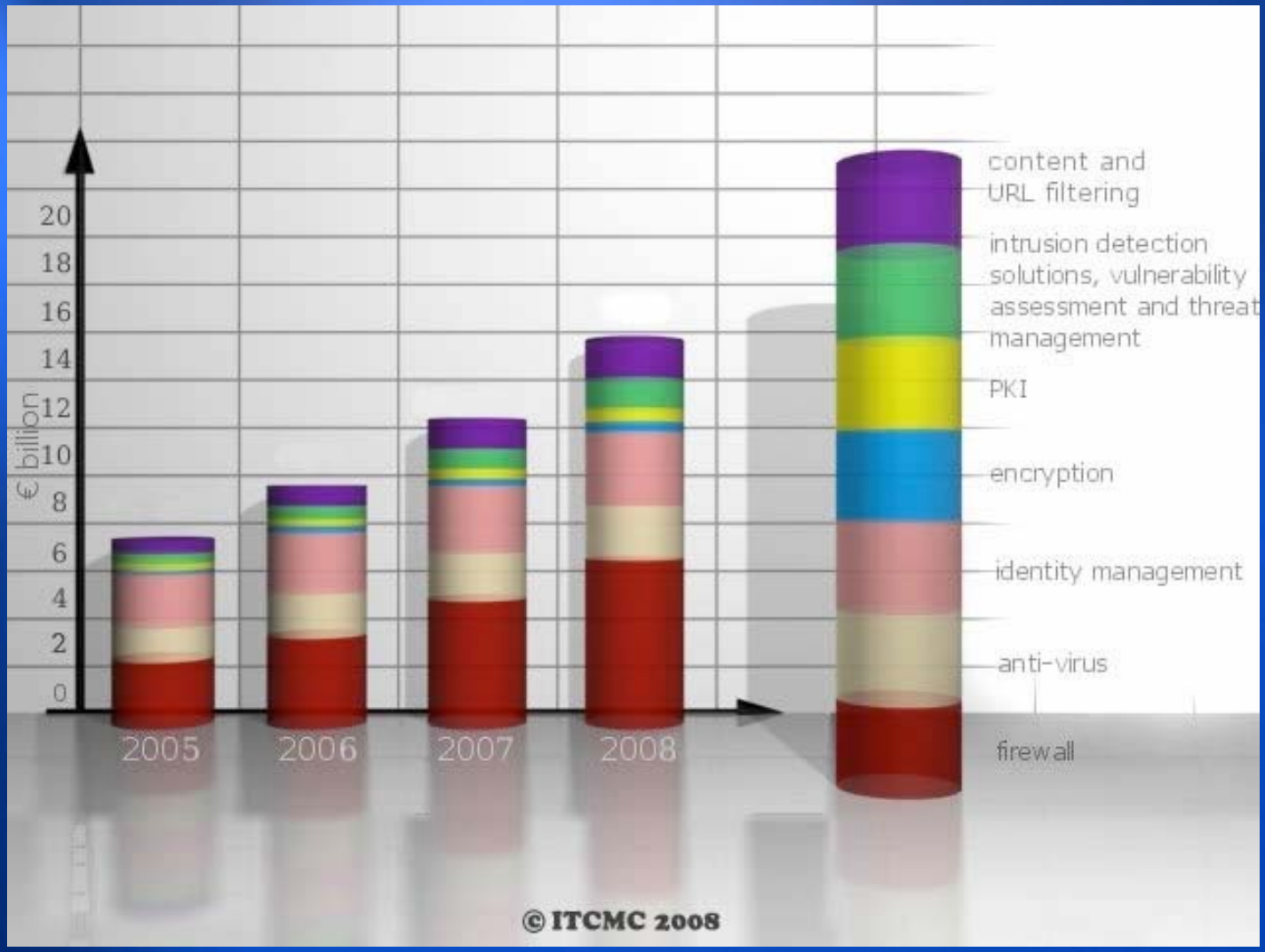
Number of Malicious Hacking Attacks Worldwide
8,000 in 2000
31,000 in 2001
60,000 in 2004
100,000in 2005
240,000 in 2006
450.000 in 2007
??? In 2008

mi2g

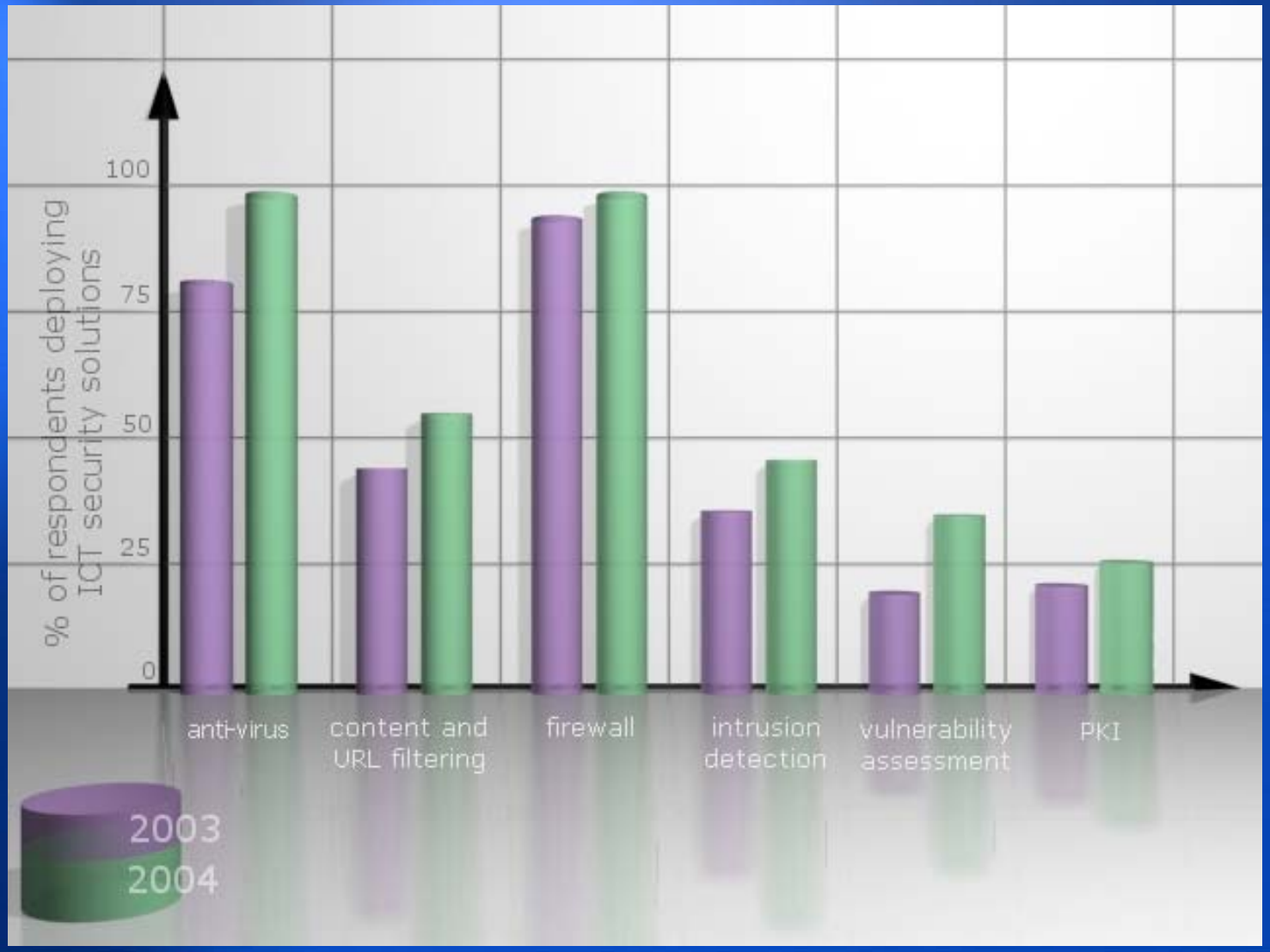
Worldwide ICT Security Market



Split-Out of the ICT Security Market



Percentage of respondents deploying ICT security solutions



Balance: A and C

SECURITY

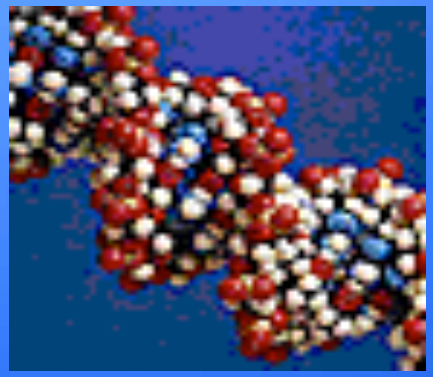
The

R & D Trends

Information may take different physical forms…

… mechanical,

… or electronic,



… or bio-molecular,

… or quantum, etc.

There is no information without a physical carrier, and no computation without a physical process.

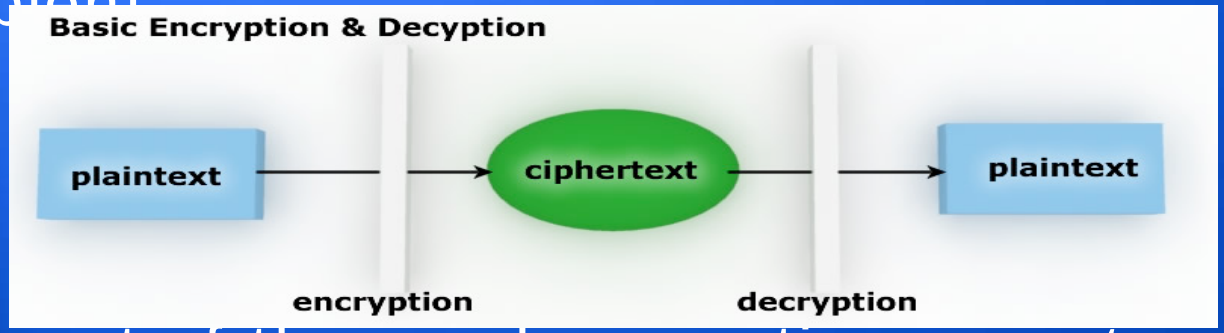
The laws of physics dictate what computations can be

Introduction
Security and **Encryption**

- **Encryption:**
  - The process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- **Purpose:**
  - Secure stored information
  - Secure information transmission
- **Provides:**
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

What is Encryption ?

Encryption is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. As shown in the figure below, Encrypted data must be deciphered, or decrypted, before it can be read by the recipient.



The root of the word encryption—*crypt*—comes from the Greek word *kryptos*, meaning hidden or secret.

Modern Encryption Algorithms

- Private Key Encryption
- Public Key Encryption
- Quantum Cryptography

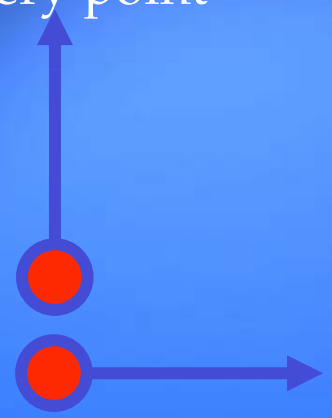
Quantum,
from Physics to Programming

C. Physics	Q. physics
At any given time, a physical system is in one state, and only one state, among a set of possible states of that system.	At any given time, a physical system can be in one state among a set of possible basis states. But, in general, it is in a state which is a superposition of several basis states.
The transformations of the state of a physical system are not, in general, reversible.	The transformations of the state of an unobserved physical system are reversible and deterministic.
The observation of a physical system in state S does not modify S and it is deterministic: it returns the same information for identical systems in state S.	The observation of a physical system in state irreversibly modifies S and it is probabilistic: it may return different information for identical systems in state S.
The state of a physical system A can be copied into another physical system B, if both systems have the same set of possible states.	The state of a physical system A cannot, in general, be copied into another physical system B.
The state of a physical system composed of n sub-systems is reducible to an n-tuple of the states of these sub-systems.	The state of a physical system composed of n sub-systems is not, in general, reducible to an n-tuple of the states of these sub-systems.

Classical Bit

A classical bit is, at every point in time:

- either in state 1:
- or in state 0:



State of a classical bit: $b \in \{0,1\}$

B ist ein element aus dem wertbereich 0 or 1

Quantum Bit

A quantum bit (« qubit ») is, at every point in time:

- either in basis state $|1\rangle$
- or in basis state $|0\rangle$:
- or in a superposition state, i.e. at the same time $|1\rangle$ and $|0\rangle$:

State of a qubit:

$|\psi\rangle \in E$

where E is a 2-dimensional vector space

Quantum Cryptography

- Method of secure key exchange over an insecure channel based on the nature of photons
- Polarized photons are transmitted between sender and receiver to create a random string of numbers, the quantum cryptographic key
- Perfect encryption for the 21st century
- Experimental stages
- Very secure

What Does it Mean- “Security”?

- **Communications security** - concerned with the protection of an organization’s communications media, technology, and content.
- **Network security** is the protection of networking components, connections, and contents.
- **Information Security –** protection of information and its critical elements, including the systems and hardware that use, store, or transmit that information.

Information Security Threats

- **Act of Human Error or Failure** *(accidents, mistakes)*
- **Compromises to Intellectual Property** *(piracy, copyright infringement)*
- **Acts of Espionage or Trespass** *(unauthorized access and/or data collection)*
- **Acts of Information Extortion** *(blackmail of information disclosure)*
- **Acts of Sabotage or Vandalism** *(destruction of systems or information)*
- **Software Attacks** *(viruses, worms, macros, denial of service)*

What Does it Mean- “Security”?

- Communications security
- Network security
- Information Security
- ..
- ...

Society Security

Meaning of Security Lies in Trust

- Every security problem has this question it needs to answer first: **Whom or what do we trust?**
- On our daily lives, we placed some sort of technology between us and the “things” we don’t trust. For example lock the car, set the house alarm, give Credit Card number only to the cashier, etc.
- So we decided to trust somebody/something to have some sort of security (trust the lock, trust the police, trust the cashier).
- We have to have the same scenario for computer & network systems we use today.

State of the Industry

•According to the 2007 Computer Security Institute and FBI annual study on security, 95% of respondents detected computer security breaches in the last 12 months.

•Companies will spend nearly $96 Billion on network security in 2008 and it is expected this amount could triple in the next two years.

Information Security Threats

- **Forces of Nature** *(fire, flood, earthquake, lightning)*
- **Quality of Service Deviations from Service Providers** *(power & WAN service issues)*
- **Technical Hardware Failures or Errors** *(equipment failure)*
- **Technical Software Failures or Errors** *(bugs, code problems, unknown loopholes)*
- **Technological Obsolescence** *(antiquated or outdated technologies)*
- **TERROR**

The CISSP

- What is it ?
- Why is it important to you ?
- How do you prepare ?

CISSP Overview

- Certified Information System Security Professional
- Intended for those who make descisions about information security risks and the protection of that information
- Most common certifications sought by employer looking for Chief Security Officers and Consultants
- 8000+ worldwide

Benefits to vs. costs

It‘s not VoIP, it‘s not QoS, it‘s all about Security

- First competence centre for Information Security and trust (3Q 2008)

Requirements

3 Years
Relevant Experience

Agree to Follow
Code of ethics

Passing Grade on
Comprehensive Exam

Continued Annual Development

Advantages of CISSP

- To the employer and customer
  - Reduced risk
    - In a field that has grown so rapidly, it is difficult to evaluate qualifications
  - Encourages employee growth
- To the professional
  - Exposure to complete body of infosec knowledge
  - Increased employment opportunities
  - More status

Benefits of (ISC)² Certification

- Establishes best practices
- Provides a solutions-orientation, not specialization, particularly with the broader understanding of the IS
- Access to a network of global industry and subject matter/domain experts
- Resource for broad-based security information
- Adds to credibility with the rigor and regimen of the certification examinations
- Provides a business and technology orientation to risk management

The BIG Disadvantage