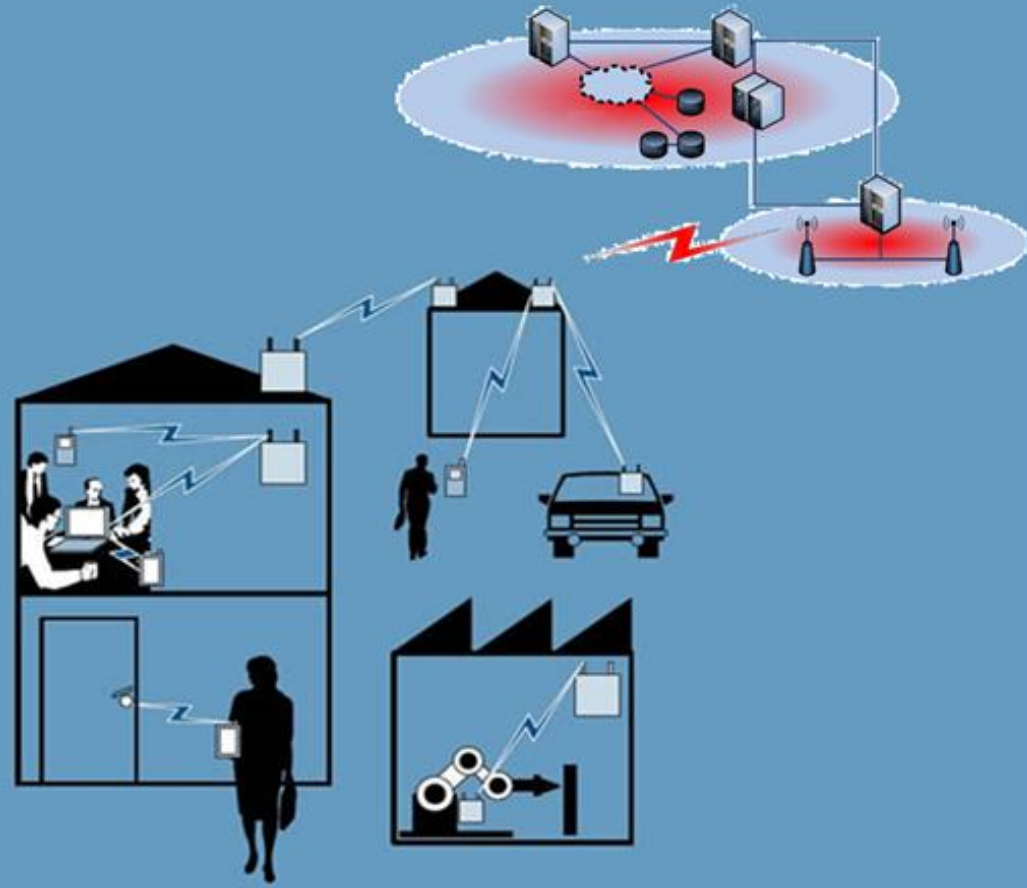


Technology, Security, Privacy On The (Mobile) Internet

Dr. Udo Helmbrecht
Executive Director
European Network and
Information Security Agency

THE ONASSIS FOUNDATION SCIENCE
LECTURE SERIES 2010 IN COMPUTER
SCIENCE

FORTH, Heraklion Crete, Greece,
1 July 2010



Content

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

1. **IT-Security Risks**
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

IT-SECURITY RISKS

Risk Trends

Threats	2007	2009	Forecast
Zero-day exploits	↑	↑	→
Drive-by downloads	—	↑	↑
Trojan horses	↑	↑	↑
Viruses	↓	↓	→
Worms	↓	↓	→
Spyware	↑	↑	→
DDoS attacks	→	↑	↑
Unsolicited e-mail	↑	↑	↑
Bot networks	→	↑	↑
Identity theft	↑	↑	↑

Source: BSI 2009

Risk Potential

Technology / Application	2007	2009	Forecast
Voice over IP	↑	→	→
Mobile data transmission	—	↑	↑
Web 2.0	—	↑	↑
SCADA	→	↑	↑
DNS	—	↑	↑
Multi-function devices	—	↑	→
Interfaces and storage media	—	↑	→
Network coupling elements	—	↑	↑
SOA	—	↑	↑

Source: BSI 2009

Risk Profiles

Technology / Application	2007	2009	Forecast
RFID	→	→	↑
Biometrics and personal ID's	—	↑	↑
IPv6	—	↑	→
Automotive	—	↑	↑
Health ID card	—	↑	→

↑ Risk increasing

→ Risk remaining the same

↓ Risk decreasing

Source: BSI 2009

Economic Dimension

	Spam	Viruses	Spyware	Phishing
	The incidence of heavy spam is as high as last year.	The frequency is the same as in last year's survey.	545,000 households had to replace computers in the past six months.	34,758 attacks in December 2008 alone.
National incidence	1 in 3 had heavy levels of spam.	1 in 7 had serious problems.	1 in 12 had serious problems.	1 in 90 lost money.
Total damage	N/A	\$5.8 billion	\$1.7 billion	\$483 million

Source: Consumer Reports Magazine, June 2009

Costs

	ISBS 2008 - overall	ISBS 2008 - large businesses
Business disruption	£8,000 - £15,000 <i>over 1-2 days</i>	£80,000 - £130,000 <i>over 1-2 days</i>
Time spent responding to incident	£600 - £1,200 <i>2-4 man-days</i>	£2,500 - £5,000 <i>6-13 man-days</i>
Direct cash spent responding to incident	£1,000 - £2,000	£4,000 - £8,000
Direct financial loss (e.g. loss of assets, fines etc.)	£500 - £1,000	£4,000 - £8,000
Damage to reputation	£50 - £200	£2,000 - £15,000
Total cost of worst incident on average	£10,000 - £20,000	£90,000 - £170,000
<i>2006 comparative</i>	<i>£8,000 - £17,000</i>	<i>£65,000 - £130,000</i>

Source: Information Security Breaches Survey, Price Waterhouse Coopers/
UK Department for Business, Enterprise & Regulatory Reform (BERR) 2008

1. IT-Security Risks
2. **Political Awareness in ICT**
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

EUROPE POLITICAL AWARENESS IN ICT

500 Million people in 27 Countries



23 languages

The European anthem:
"Ode an die Freude"
Beethoven's 9th Symphony
composed in 1823

Players

The European Parliament
- voice of the people

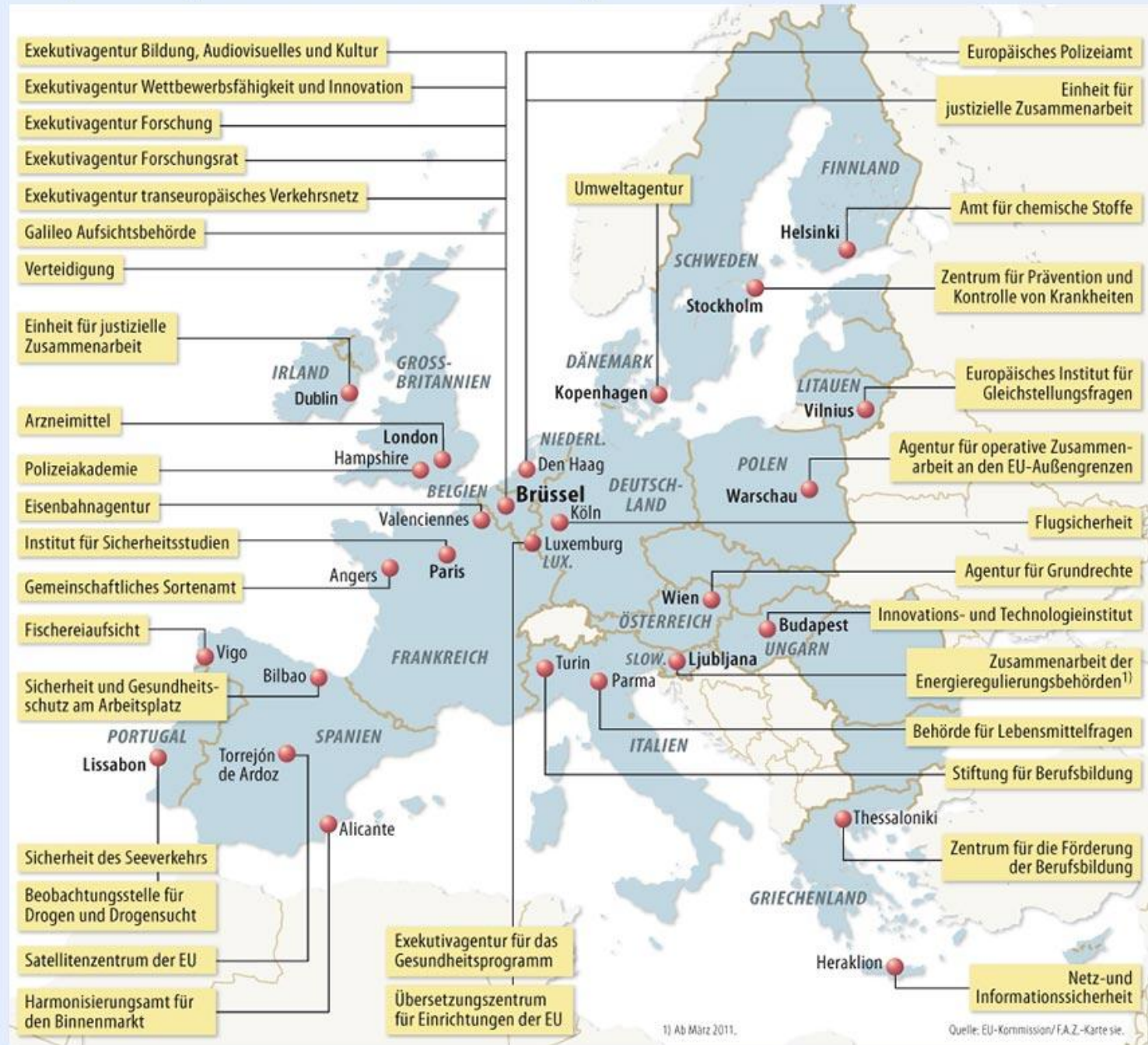
The council of Ministers
- voice of the Member States

The European Commission
- promoting the common interests
José Manuel Barroso, President
of the European Commission



The European Agencies
- a desire for geographical devolution

Europäische Agenturen und andere Einrichtungen



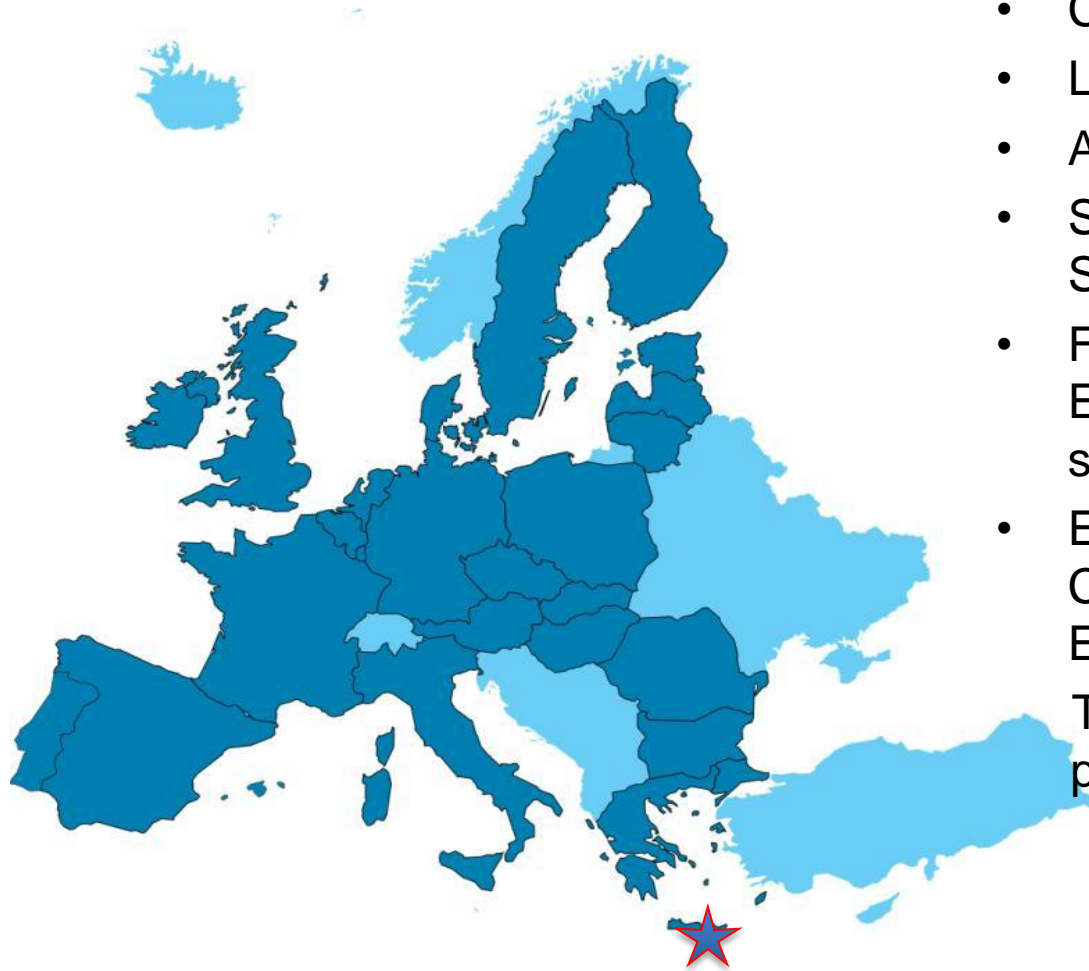
¹⁾ Ab März 2011.

Quelle: EU-Kommission/FAZ-Karte sie.

IT Security on EU level

- In March 2010 the European Commission launched the EU 2020 strategy and
- In May a flagship initiative *A digital agenda for Europe*
COM(2010) 245 of 19th May 2010
- High level goals:
 - Modernise and enhance ENISA
 - Enhance cooperation of CERTs on national & European level
 - Provide CERT services for European institutions
 - Support EU-wide cyber security preparedness exercises
 - Enhance prevention and combating cybercrime

ENISA – overview



- Created in 2004
 - Located in Heraklion / Greece
 - Around 65 Experts
 - Supports EU institutions and Member States
 - Facilitator of information exchange between EU institutions, public sector & private sector
 - ENISA assists Member States and the Commission in global issues that affect the European Community as a whole
- This is an advisory role and the focus is on prevention and preparedness

1. IT-Security Risks
2. Political Awareness in ICT
3. **Technological Areas with an Impact on Resilience**
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

TECHNOLOGICAL AREAS WITH AN IMPACT ON RESILIENCE

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - **Development of Network Technologies**
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

DEVELOPMENT OF NETWORK TECHNOLOGIES

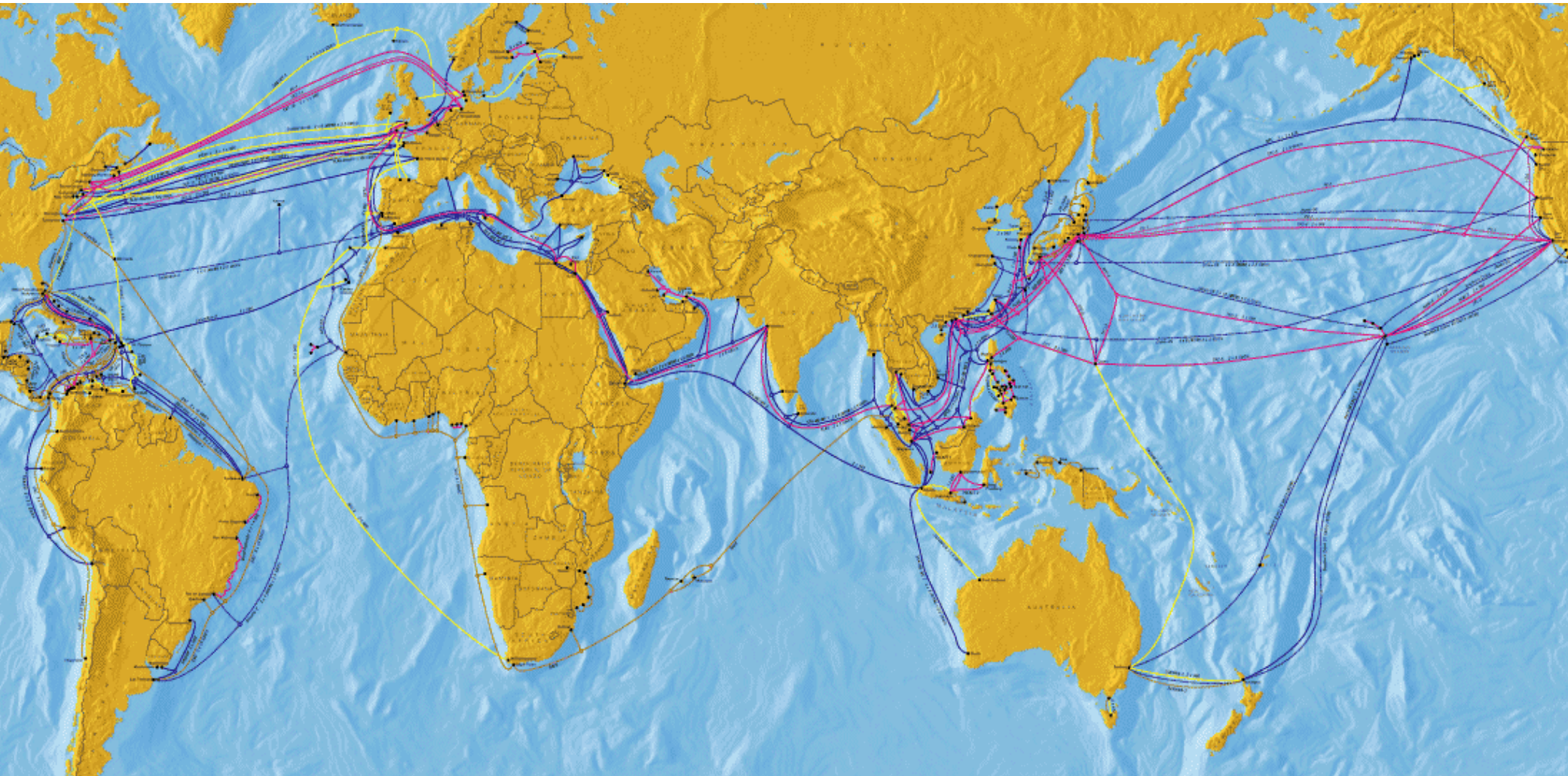
- Public computer networks have become an essential enabler for the communications on which most every-day activities rely
- IT-related risks are generated by excessive automation and the vulnerability of technology:
 - diverse levels of resilience in interconnected networks and devices,
 - increases in attack surface – down to firmware and up to applications,
 - exponential increases in traffic,
 - regulatory disconnections between different geographical areas.

Impact on Resilience

- Cloud computing
- Real time detection and diagnosis systems
- Future wireless networks
- Sensor and actuator networks
- Integrity of supply chain
- Cognition and cooperation in networks –
information on sensors, environment, user preferences, applications history
- Emergency response – readiness regarding information security incidents
- Future ICT threats – ambient intelligence and Internet of Things
preparedness
- Interoperability – gaps between interconnected networks
- ‘Self-x’ networks – self-healing, self-protecting, self-organising

- Machine-to-machine networks – stochastic, rapidly changing properties
- Peer-to-peer networks and resilient routing
- Protocols for authentication and communication
- Residential networks – auto-configuration in consumer devices
- Supervisory control and data acquisition (SCADA)
- Service level agreements
- Smart objects – accessible in the Internet namespace
- Trust models – trusted networks and trusted and assured platforms
- Trust and confidence in the technology
- Modelling of networks – apply of the formal methods
- Network & information theory (Le Boudec, MacKay, Hutchison, Sterbenz)

Cables....



1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - **Cloud Computing**
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

CLOUD COMPUTING

Cloud Computing (CC)

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable

- computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned
- and released with minimal management effort or service provider interaction. This cloud model promotes
- availability and is composed of five essential characteristics, three service models, and four deployment models.

CC – Essential Characteristics

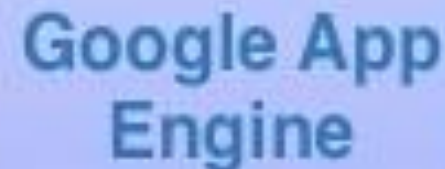
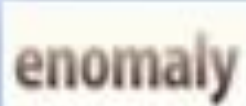
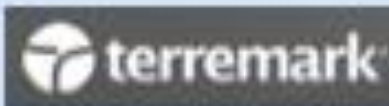
- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

From the Consumer's Perspective...



Everything Is Cloud...

Enterprise-Centric



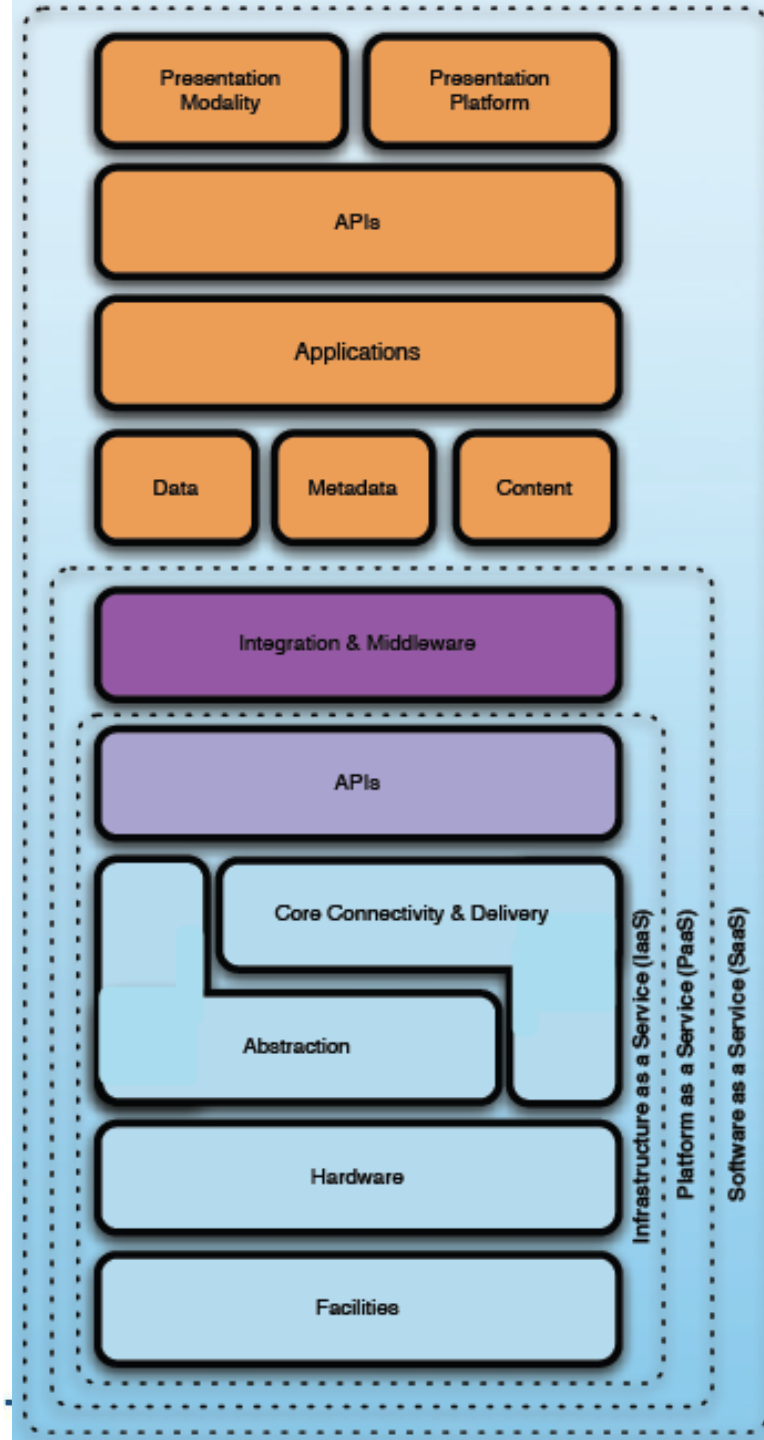
Utility Hosting

Platform-as-a-Service

Web-Centric

CC - Service Models

- SaaS:
Cloud software as a service
- PaaS:
Cloud platform as a service
- IaaS:
Cloud infrastructure as a service

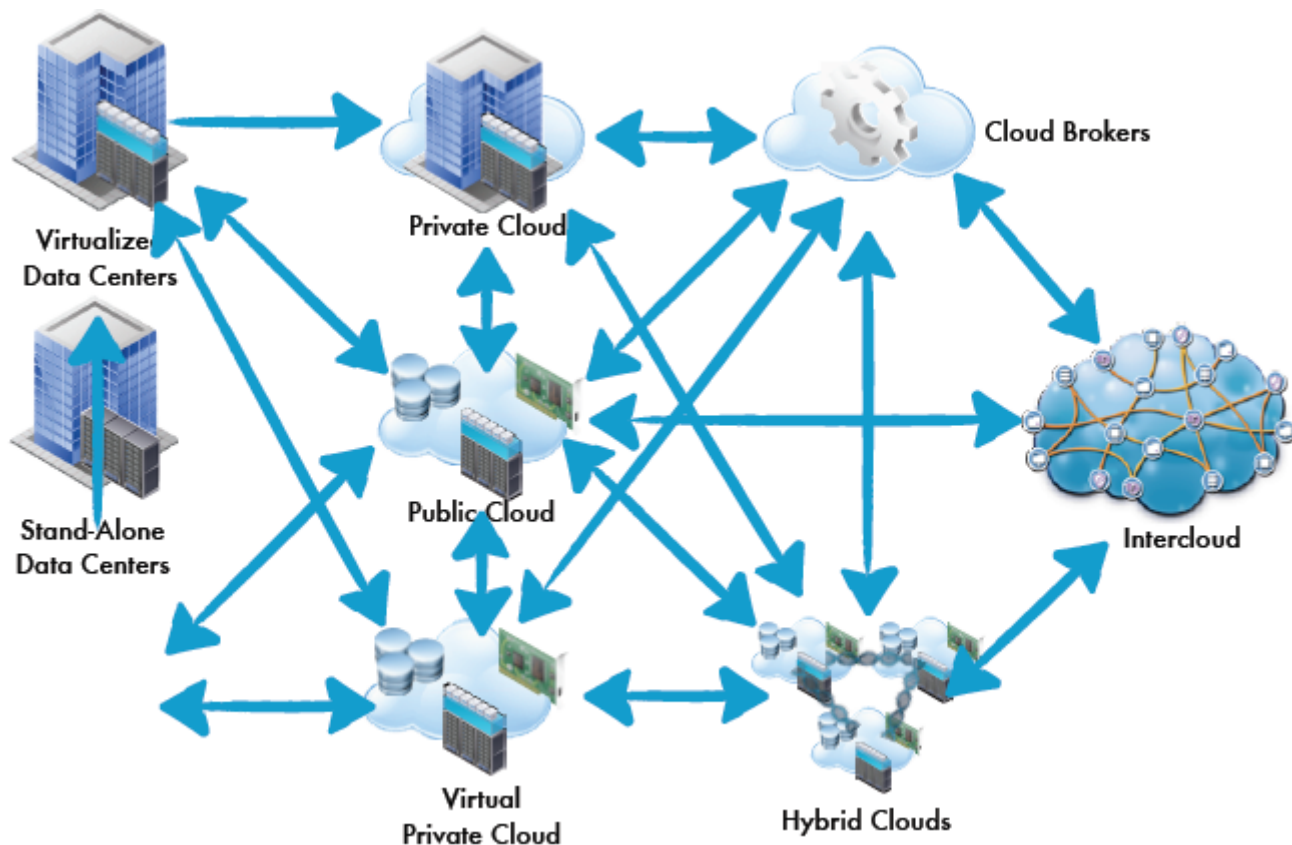


CC - Deployment Models

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

Advantages

- Operational
- Financial
- Productivity



Impact of the Cloud Computing Paradigm on Resilience

- Impacts on service availability
 - All-hazards
 - Support for business continuity
 - Disaster recovery
- Protecting sensitive data is essential
- The cloud computing paradigm changes the threat landscape with respect to both service availability and the protection of sensitive data

- Benefits
 - High degree of redundancy
 - Economies of scale
- Risks
 - Loss of Governance
 - Compliance Challenges
 - Legal and contractual risks
 - Key management
 - Vendor Lock in
 - Impacts on data protection

CC - Research Recommendations

- Trusted cloud computing models
- Data protection in the cloud computing paradigm
- Cloud assurance, security best practices and certification standards
- Standardized data formats and migration
- Service availability in the face of connectivity loss

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - **Data Protection and Legal compliance in Cloud Computing**
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

DATA PROTECTION AND LEGAL COMPLIANCE IN CLOUD COMPUTING

Data Protection Requirements

- In what country is the cloud provider located?
 - Is the cloud provider's infrastructure located in the same country or in different countries?
 - Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
 - Where will the data be physically located?
 - Will jurisdiction over the contract terms and over the data be divided?
 - Will any of the cloud provider's services be subcontracted out?
- ...

- Will any of the cloud provider's services be outsourced?
- How will the data provided by the customer and the customer's customers, be collected, processed and transferred?
- What happens to the data sent to the cloud provider upon termination of the contract?

Data protection benefits

Economies of scale

- A large and reputable (Cloud Service Provider) CSP will usually be able to offer a higher level of security per user, unit of storage, unit of processing power, etc, than a smaller enterprise data centre, particularly:
 - Cloud infrastructure as a service (IaaS) and
 - Cloud software as a service (SaaS)
- protection of the infrastructure
- specific security technologies, like VPN or data encryption

Recommendations

1. Technical data protection measures
2. Data Security
3. Data Transfer
4. Law Enforcement Access
5. Confidentiality and Non-disclosure
6. Intellectual property
7. Risk Allocation and limitation of liability
8. Change of Control

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - **Future Wireless Networks**
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

FUTURE WIRELESS NETWORKS

Future Wireless Networks (FWN)

Resilience has become an important concern in the design and architecture of the security of future wireless networking architectures such as

- mobile ad-hoc networks (MANETs) and
- wireless mesh networks (WMN¹)
- Usually protected by authentication, access control, cryptographic algorithms and protocols
- Challenges
 - peer-to-peer network architecture, shared wireless, medium, stringent resource constraints, highly dynamic network topology

FWN - Resilience requirements

- Ability for mobile users and applications to access information when needed
- Maintenance of end-to-end communication;
- Ability for distributed operation and networking.

- Increasing the robustness of the networking mechanisms
- Intrusion and misbehaviour detection and recovery

Networking mechanisms improving resilience

- **Protecting route discovery**
protection against misbehaving routers or manipulated routing messages
- **Reactive distance vector routing**
routes are defined on-demand by flooding the entire network with route messages.
- **Proactive link-state routing**
e.g. link-state routing protocols OLSR, nodes periodically flood the network with link-state update messages that contain the current link values of all their links
- **Protecting resource reservations**
tracking the reservations on requests of other nodes
- **Design issues in error recovery mechanisms**
handle link breakage

Intrusion detection and recovery

- Automated identification of abnormal activity by collecting audit data, and comparing it with reference data
- Resilience requirements for intrusion detection
- Attack recovery and mitigation
- Misuse detection
- Anomaly detection
- Protocol-based or specification-based detection

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - **Sensor networks**
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

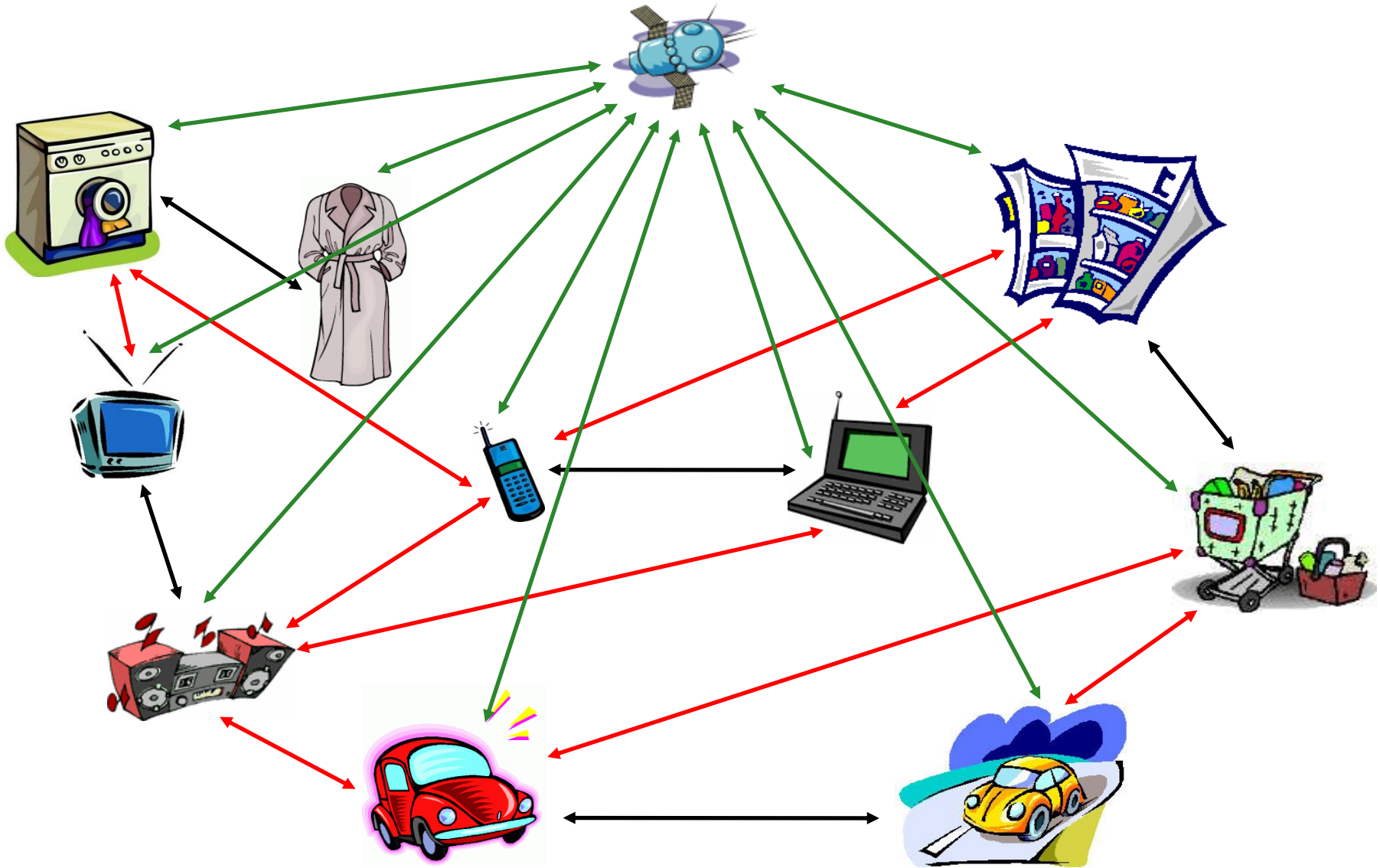
SENSOR NETWORKS

- Sensor networks are widely installed around the world in urban, suburban and rural locations – on the ground and on various airborne platforms, including balloons, high-altitude platforms, unmanned airborne vehicles and satellites.
- At present, few of them have a purpose that involves real-time interaction with human beings. The Internet of Things will change this and make sensors, and actuators, first class devices, fully visible with end-to-end connectivity.

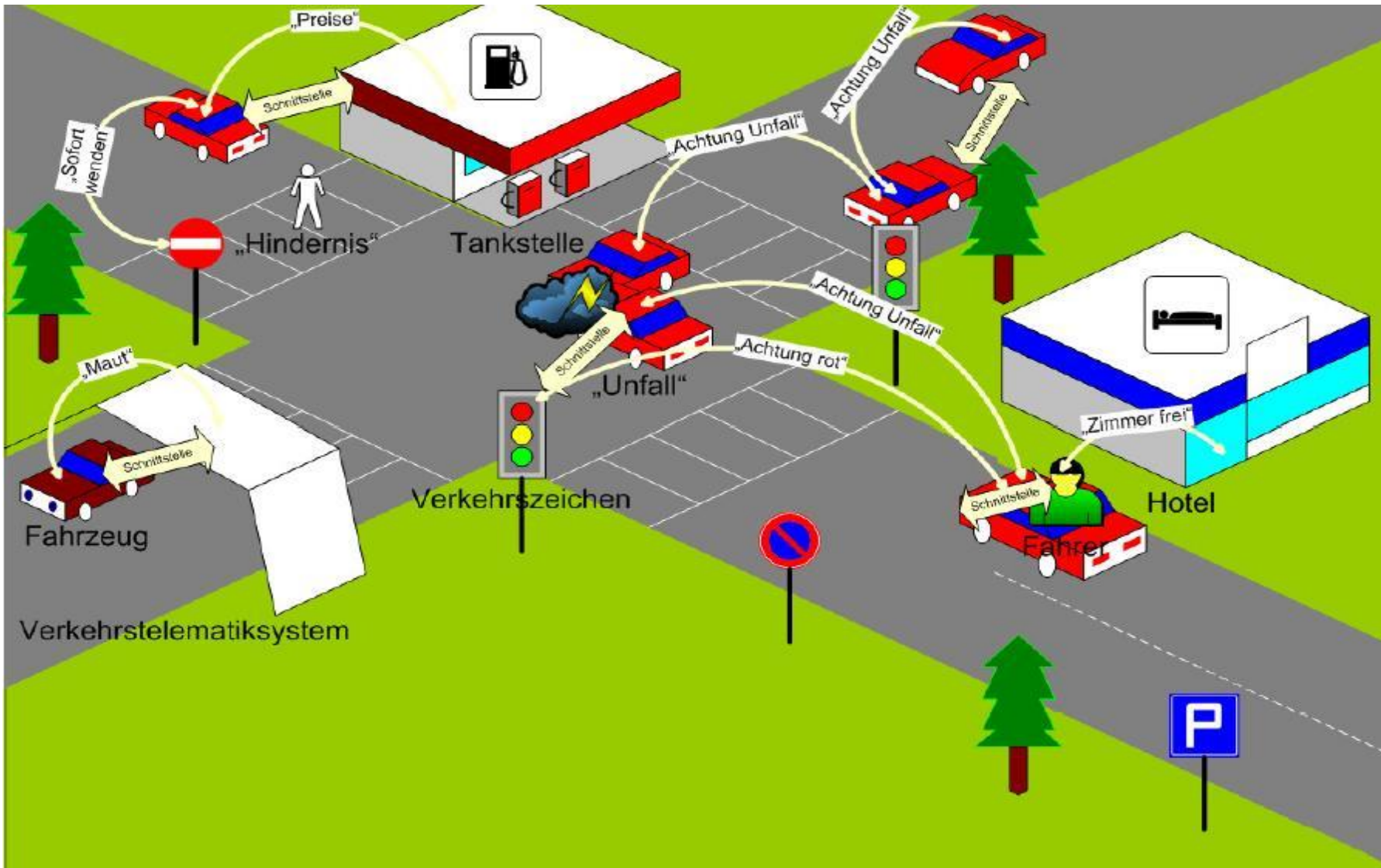
Types of sensor networks

- Electronic commerce – banks and the financial sector
- The police, immigration, homeland security and other security services, and the emergency services
- Transportation, including highways, inshore water, railways, and civil aviation
- Resources, specifically electricity, gas, oil, water and heat
- Environment, including quality of air and water, disaster anticipation, first-response and recovery (from fire, flood, earthquake, storm and attack)
- Health, including related enterprises, eg, the NHS in the UK, tele-care, and e-health
- Military systems

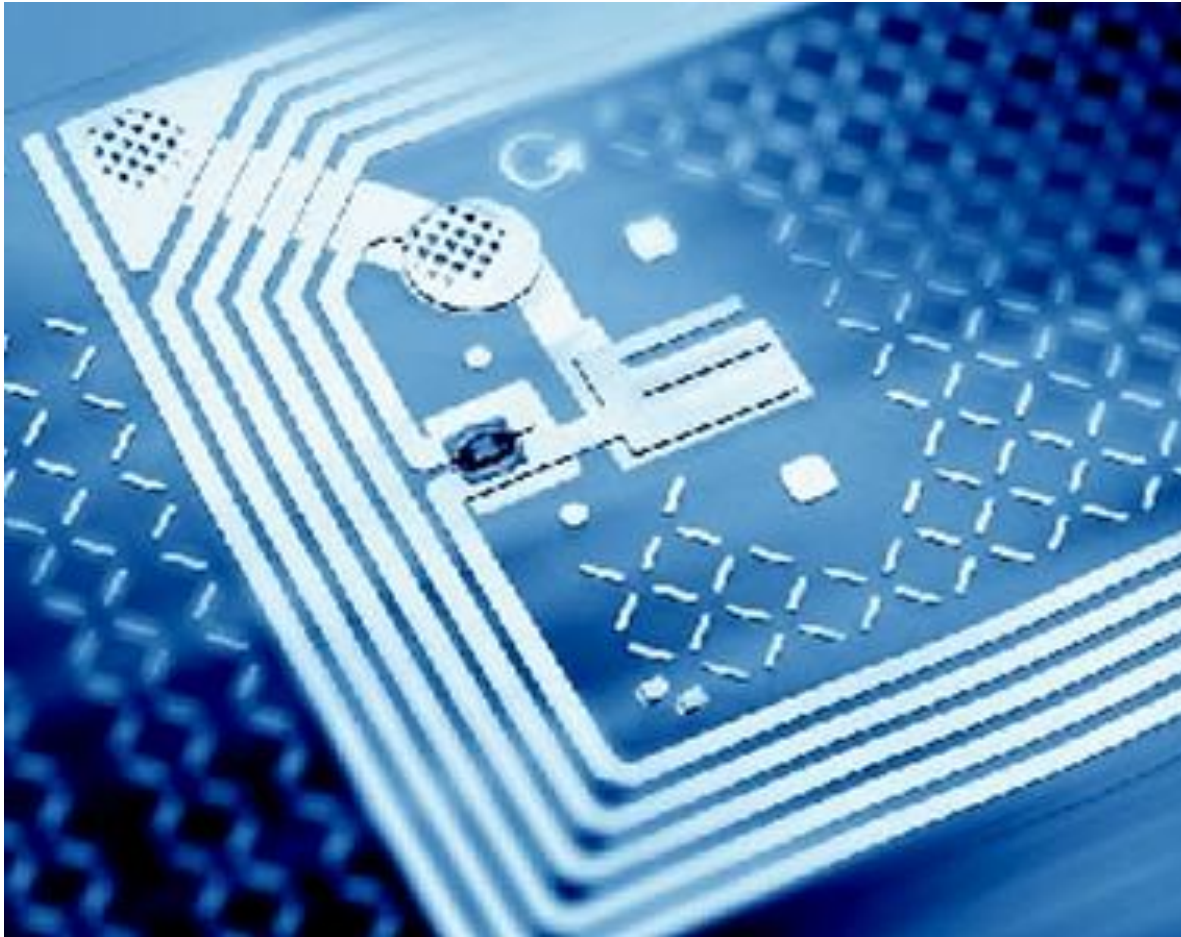
Pervasive Computing - BSI Study, 2006



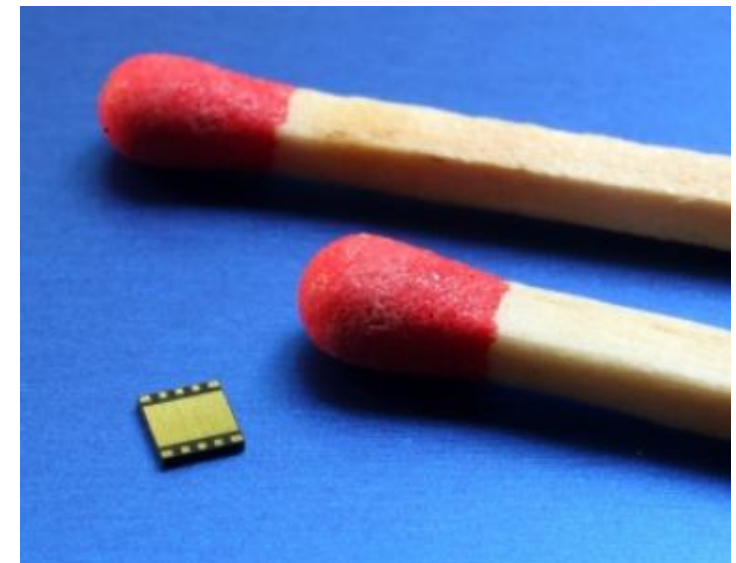
Car to Car Communication



Mobile Kryptographic RFID-Chips



SIEMENS



Objective

Sensor network applications operating over critical infrastructure should be protected effectively:

- resilience in society's key functions;
- improved situational awareness in anticipating and reacting to imminent events;
- better understanding of strengths, weaknesses, new opportunities and threats;
- much more information to be available, so decision support is improved and reactions are of a higher quality;
- systems to be more efficient and cost-effective.

Risks

- dependency on systems that are not fit for purpose
- reduced security – less critical for disconnected systems, but essential when interconnected
- many kinds of attack – intrusion, denial of service, interception, and masquerading
- poor interoperability – devices not working together
- service level agreements not being clear – the communications support may be inadequate or, at the other
- loss of privacy and confidentiality

Guidelines for design choices

- **Fault-tolerance** – handling node failures and unscheduled disruptions
- **Scalability** – dimensions of deployment, number of nodes
- **Topology** – fixed or movable nodes
- **Routing** – routing protocols
- **Fusion** – aggregation and consolidation of data, eliminating duplicates
- **Roles** – sense & transmit and/or receive and execute
- **Scheduling** – when is a node active?
- **Performance** – CPU, memory, peripheral device, access time, power source
- **Environment** – home, travel, global, orbit
- **Security** – e.g. confidentiality, privacy, denial of service, injection of incorrect data

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - **Integrity of supply chain**
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography

INTEGRITY OF SUPPLY CHAIN

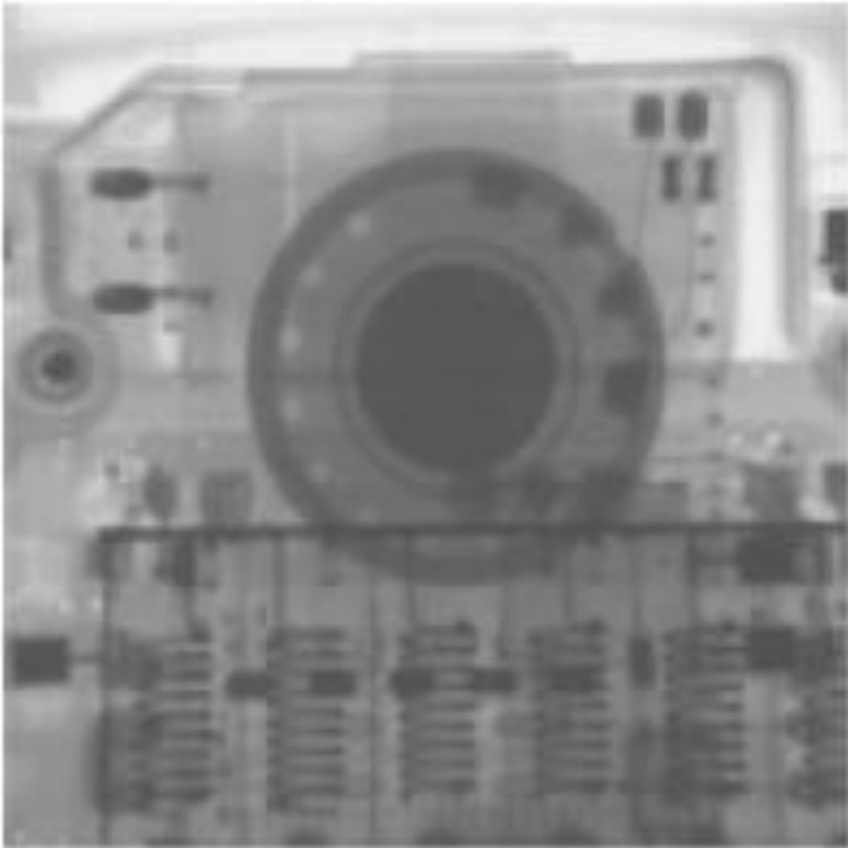
Problems....

- Supply chain integrity in the ICT industry is an important topic that receives attention from both the public and private sectors
(i.e, vendors, infrastructure owners, operators, etc).
- Currently, it is addressed separately in different industries. Important solutions have been developed in various ICT segments in this context.
- Electronic communications networks comprise numerous network elements, many of them consisting of outsourced components supplied by both new and established equipment vendors

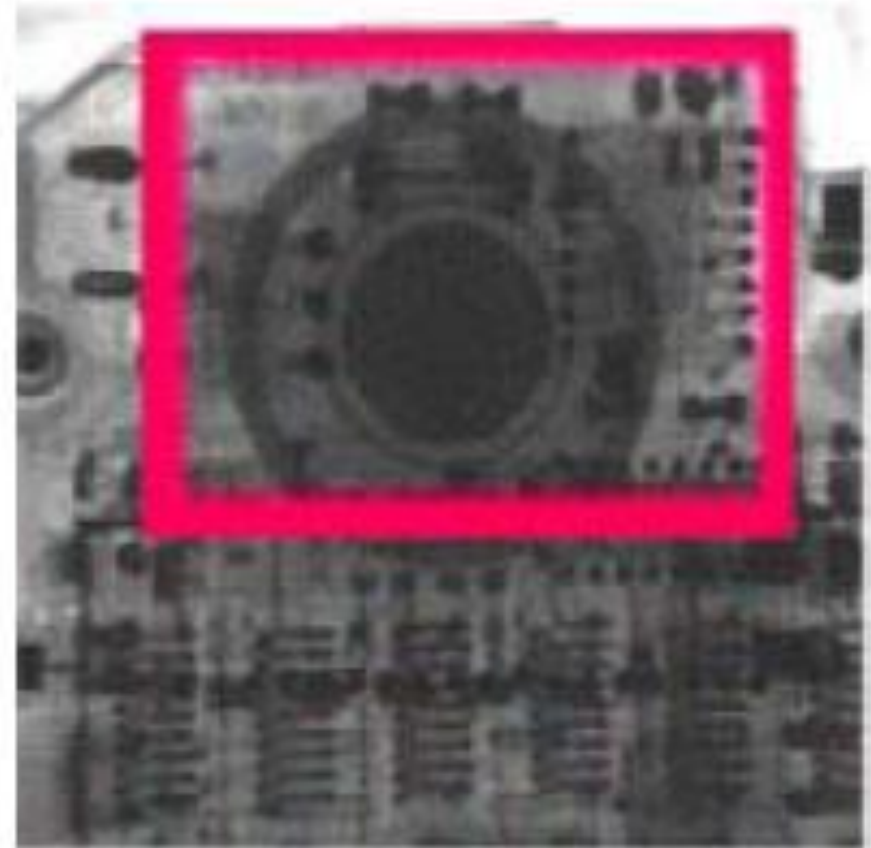
Challenges

- Complex nature of globally distributed supply chains
- Components are manufactured in various countries around the world.
- Lack of common guidelines for ICT supply chain integrity.
- Absence of tools, processes and controls to help measure statistical confidence levels and verify integrity across the IT ecosystem.
- Ineffective methodologies & technologies for end-user verification
- Lack of broadly applicable tools, techniques, and processes to detect or defeat counterfeiting and tampering in systems.
- Lack of coordinated approaches to preserving integrity from production through purchasing into operations and use.
- Absence of common business models that could drive the harmonization of integrity requirements across various ICT segments

Manipulated Mobile Phone



Referenzröntgenbild eines Mobiltelefons
(Teilansicht)



Röntgenbild eines hardware-manipulierten
Mobiltelefons (Teilansicht)

Managing supply chain integrity risks

- Clearly defined product and service requirements consistently carried through the whole supply chain from design, through production, delivery, purchase, installation, and maintenance of installed products and systems.
- Methodologies for evaluation and verification of components for compliance with upstream requirements.
- Ability to evaluate provenance (the confirmed origin) and authenticity of the component parts, for both hardware and software, during assembly and installation of the solution, as well as through appropriate (to be defined) portions of the life of the product.
- Measures to protect and maintain the integrity of systems, their configuration and operating parameters throughout their originally intended usage model.

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. **Mobile Computing Security**
 - Overview
 - Smart Phone Security
5. Elliptic Curve Cryptography

MOBILE COMPUTING SECURITY

1933

Erich Kästner schreibt in seinem Buch „Der 35. Mai“: „Am meisten imponierte ihnen aber folgendes: Ein Herr, der vor ihnen auf dem Trottoir langfuhr, trat plötzlich aufs Pflaster, zog einen Telephonhörer aus der Manteltasche, sprach eine Nummer hinein und rief: ‚Gertraud, hör mal, ich komme heute eine Stunde später zum Mittagessen. Ich will vorher noch ins Laboratorium. Wiedersehen, Schatz!‘ Dann steckte er sein Taschentelephon wieder weg, trat aufs laufende Band, las in einem Buch und fuhr seiner Wege.“

1983

Motorola



Mobile Devices

- The term mobile computing covers a large number of devices:
 - Portable storage devices.
 - Portable computers.
 - Netbooks.
 - Hand-held computers (PDA).
 - Smart Phones.
- These devices have different characteristics and are used in different ways, but many of the key risks are the same.



Mobile devices – security issues

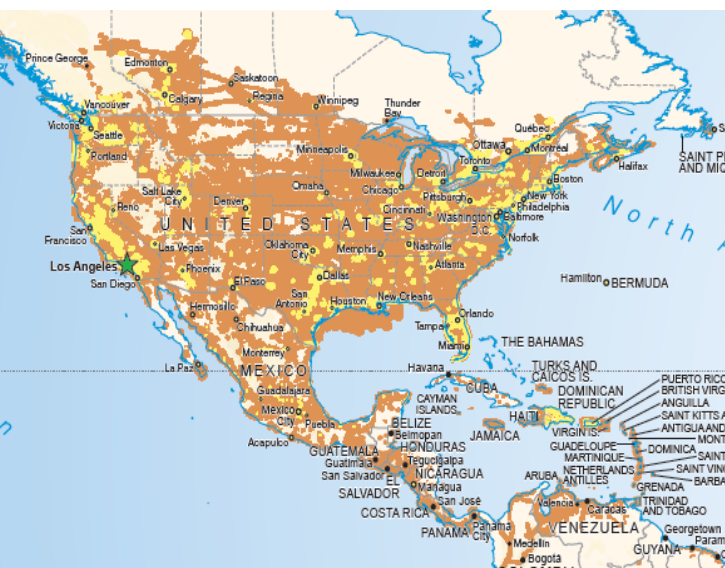
- Theft is easier.
- User interfaces are more primitive due to device constraints.
- Battery life is an issue for encryption etc...
- Changes of context – different networks, devices, different roles etc....
- Wireless protocols – weaker encryption..
- Greater concentration of personal data
- Trend towards cloud-based backup.



1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - **Overview**
 - Smart Phone Security
5. Elliptic Curve Cryptography

OVERVIEW

Global System for Mobile Communications



USA



China/Indien

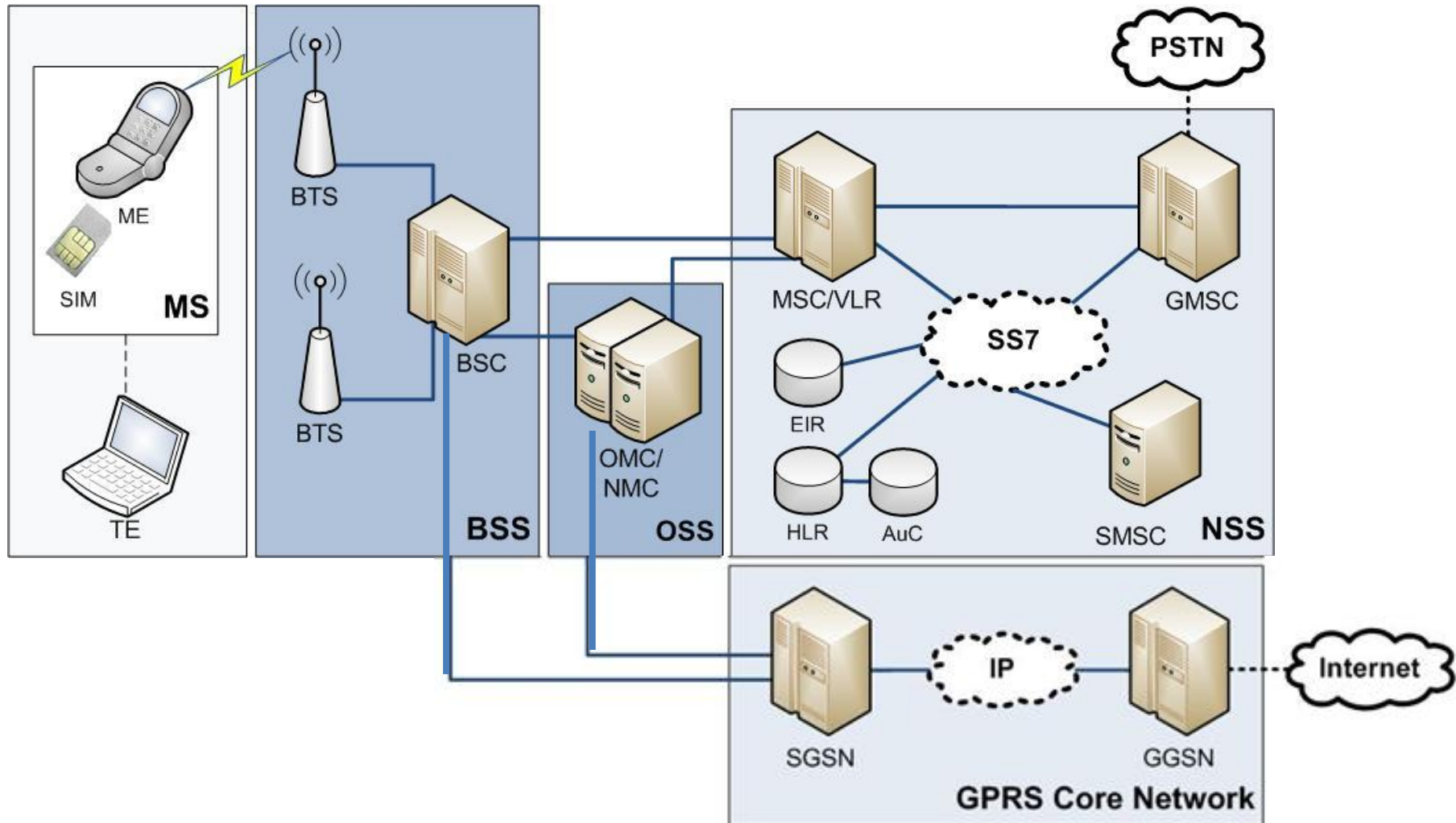


Europa

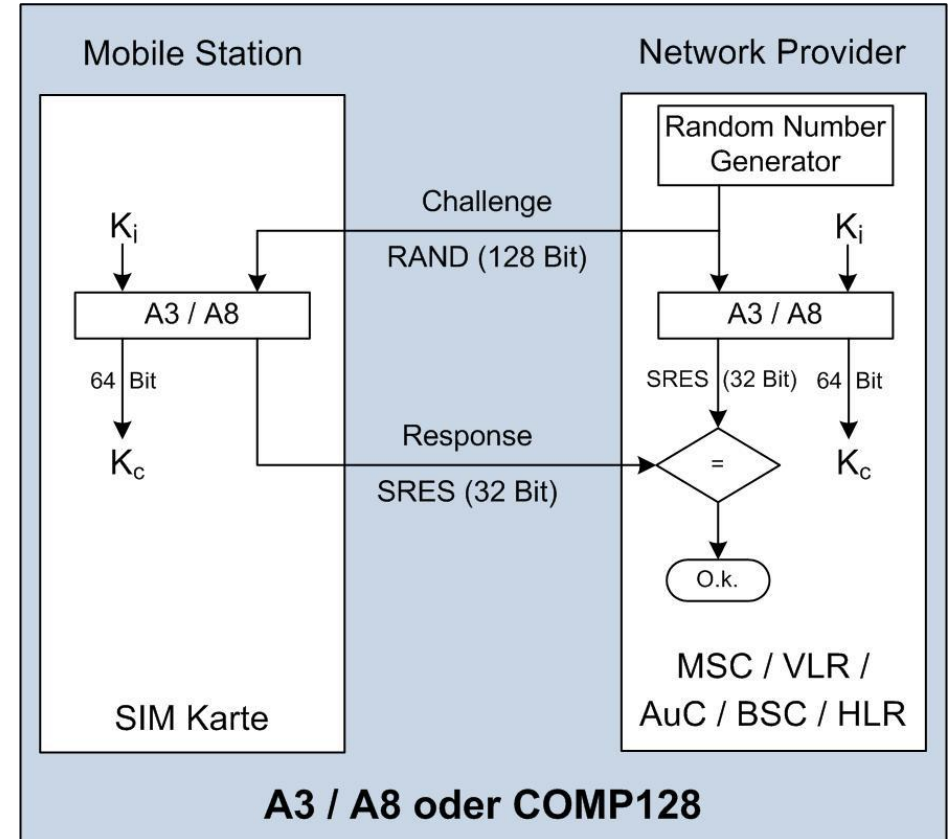
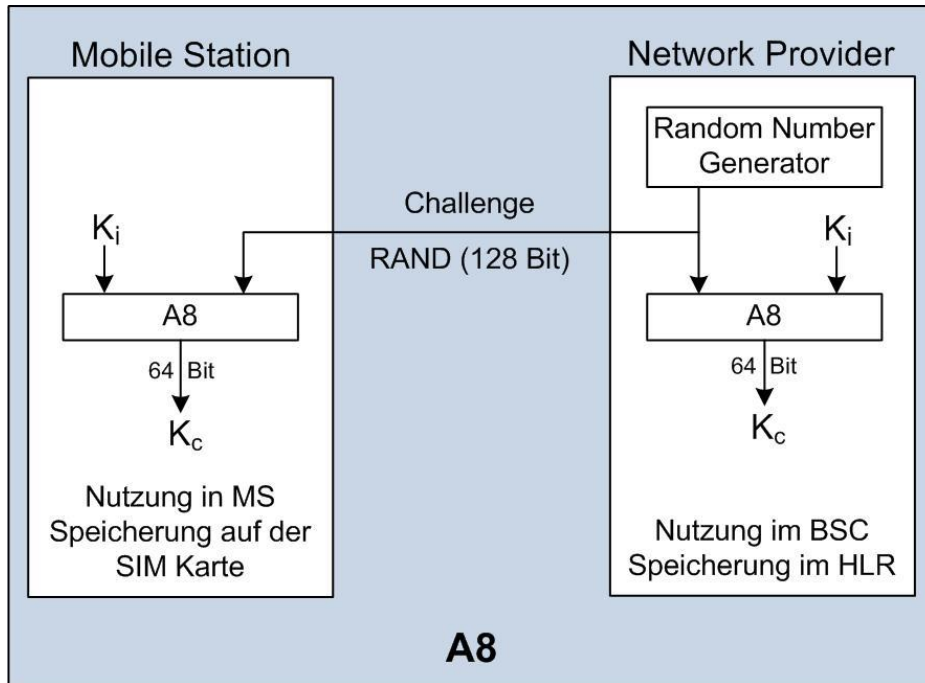
Source: GSM Association



GSM



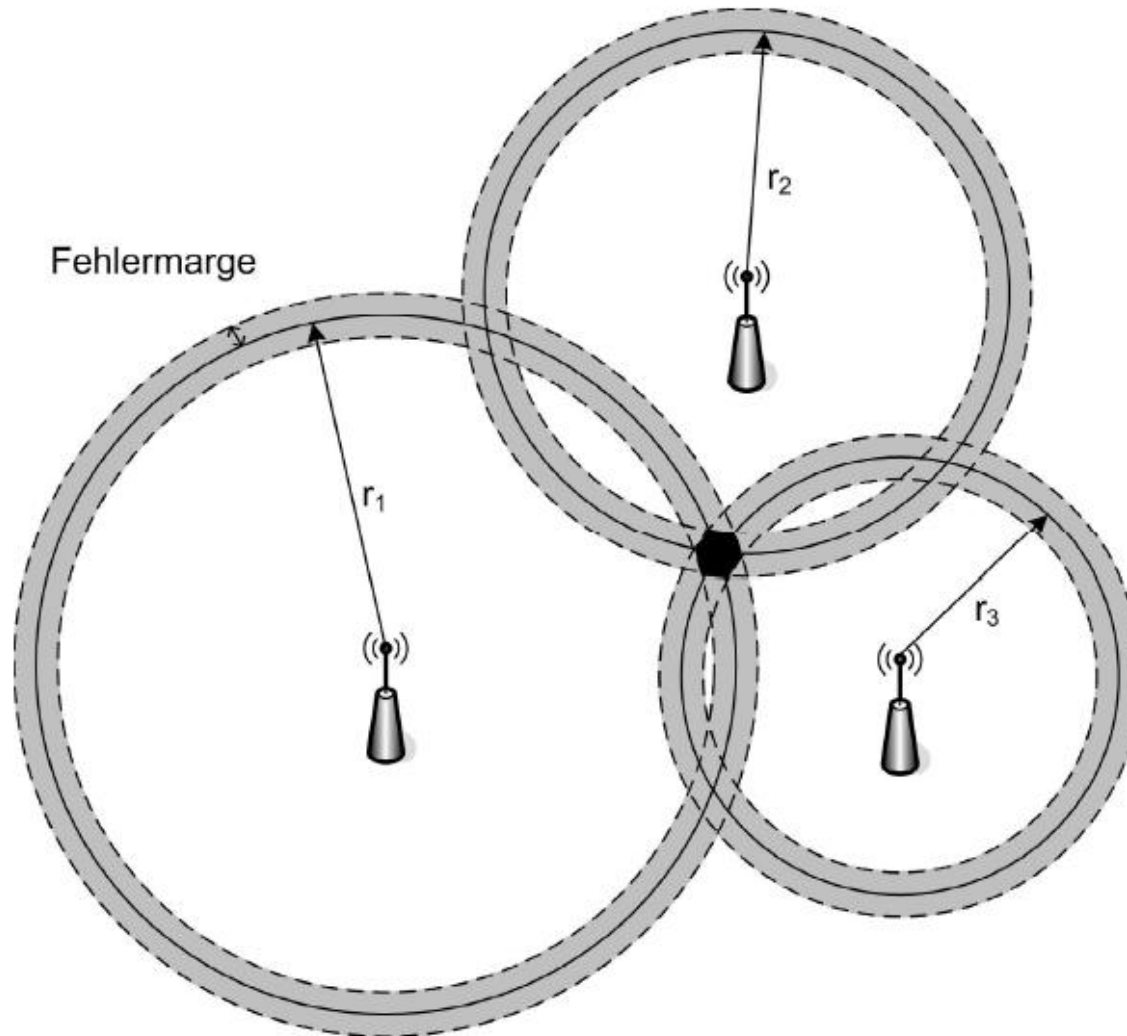
Encryption



A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It was initially kept secret, but became public knowledge through leaks and reverse engineering.

- Mobile Station (MS)
- Mobile Equipment (ME)
- Subscriber Identity Module (SIM)
- Base Station Subsystem (BSS)
- Operations and Support System (OSS)
- Network Subsystem (NSS)
- International Mobile Subscriber Identity (IMSI)
- International Mobile Station Equipment Identity (IMEI)
- Network Subsystem (NSS)
- Mobile Switching Center (MSC)
- Gateway-MSC (GMSC)
- Das Home Location Register (HLR)
- Short Message Service and SMS Center (SMSC)
- General Packet Radio Service (GPRS)

Locating...



Mobile Technology Risks



FLEXISPY

Protect Your Children | Catch Cheating Spouses

[Home](#)[Features](#)[Phones](#)[Demo](#)[Support](#)[Community](#)[Reseller](#)[Affiliates](#)[About Us](#)[Cart](#)

Is Someone Keeping Secrets from You? Reveal All with the Worlds Most Powerful Spyphone

- ≡ Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase.
- ≡ Catch cheating wives or cheating husbands, stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.
- ≡ Learn all about FlexiSPY. Still have questions, try Live Chat who are waiting to help

FlexiSPY America



Blackberry [Start here](#)
Nokia [Start here](#)
Win Mobile [Start here](#)
iPhone [Start here](#)
Android [Start here](#)

FLEXISPY - PRO - X

NEW

FLEXISPY iPhone

FlexiSPY Android Community Edition

HOW CAN FLEXISPY HELP YOU

- ≡ UNCOVER Employee espionage
- ≡ CATCH cheating husbands and cheating wives
- ≡ TRACK THEIR location using GPS
- ≡ PROTECT your children from SMS abuse.
- ≡ ARCHIVE all your own SMS for the future.
- ≡ SAVE your call history.
- ≡ BUG Meeting rooms and CHECK babysitters
- ≡ Ten Day MONEY BACK GUARANTEE



This Could Be You!

I Knew It . . .

Thanks to FlexiSPY I finally figured out my wife was cheating on me with my brother. I had a bad feeling about this for over a year. After the divorce, my life is so much better now.

Thanks FlexiSPY, I'm free again - Divorced

SMS messages, call history & other phone data are uploaded directly from the mobile phone to the FlexiSPY server 4x a day.

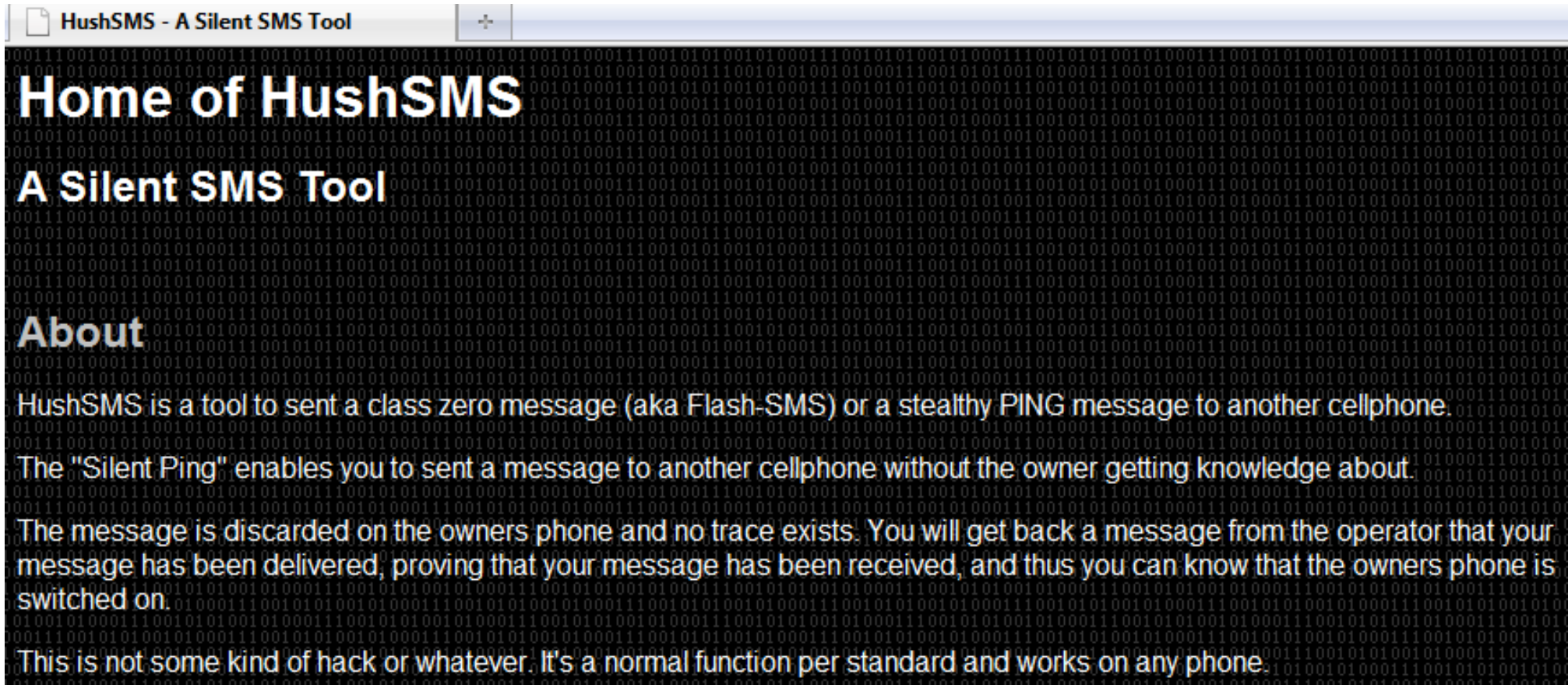


All data received by FlexiSPY can be accessed 24 hours a day, 7 days a week via any computer connected to the internet



Mobile Phone with FlexiSPY installed & activated

Any computer connected to the internet with a web browser.



Home of HushSMS

A Silent SMS Tool

About

HushSMS is a tool to send a class zero message (aka Flash-SMS) or a stealthy PING message to another cellphone.

The "Silent Ping" enables you to send a message to another cellphone without the owner getting knowledge about.

The message is discarded on the owners phone and no trace exists. You will get back a message from the operator that your message has been delivered, proving that your message has been received, and thus you can know that the owners phone is switched on.

This is not some kind of hack or whatever. It's a normal function per standard and works on any phone.

A Silent SMS Denial of Service (DoS) Attack

N.J Croft and M.S Olivier

Information and Computer Security Architectures (ICSA) Research Group

Department of Computer Science

University of Pretoria

Pretoria

South Africa

Abstract— Global System for Mobile communications (GSM) is a popular mobile communications network. Short Message Service (SMS) is an easily adopted person-to-person communications technology for mobile devices. The GSM architecture allows for the insertion of mass application-generated SMS messages directly into the network infrastructure. This is achieved through a SMS Mobile Switching Centre (SMSC) using a variety of request-response protocols, for example Short Message Peer-To-Peer Protocol (SMPP).

Standards



WLAN 802.11



GSM



DECT

Bluetooth



IEEE 802.11i Specification for Enhanced Security			IEEE 802.11w Protected Management Frames			IEEE 802.11e Quality of Service	IEEE 802.11n Enhancements for higher effective Throughput
IEEE 802.11s ESS Mesh Networking							
IEEE 802.11 Medium Access Control (MAC), Wired Equivalent Privacy, Layer Management						IEEE 802.11h Dynamic Frequency Selection & Transmit Power Control	
IEEE 802.11 Frequency Hopping Spread Spectrum (FHSS) 2,4 GHz	IEEE 802.11 Direct Sequence Spread Spectrum (DSSS) 2,4 GHz	IEEE 802.11 Infrarot	IEEE 802.11b High Rate DSSS 2,4 GHz	IEEE 802.11g Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band 2,4 GHz	IEEE 802.11a Orthogonal Frequency Division Multiplexing (OFDM) 5 GHz		

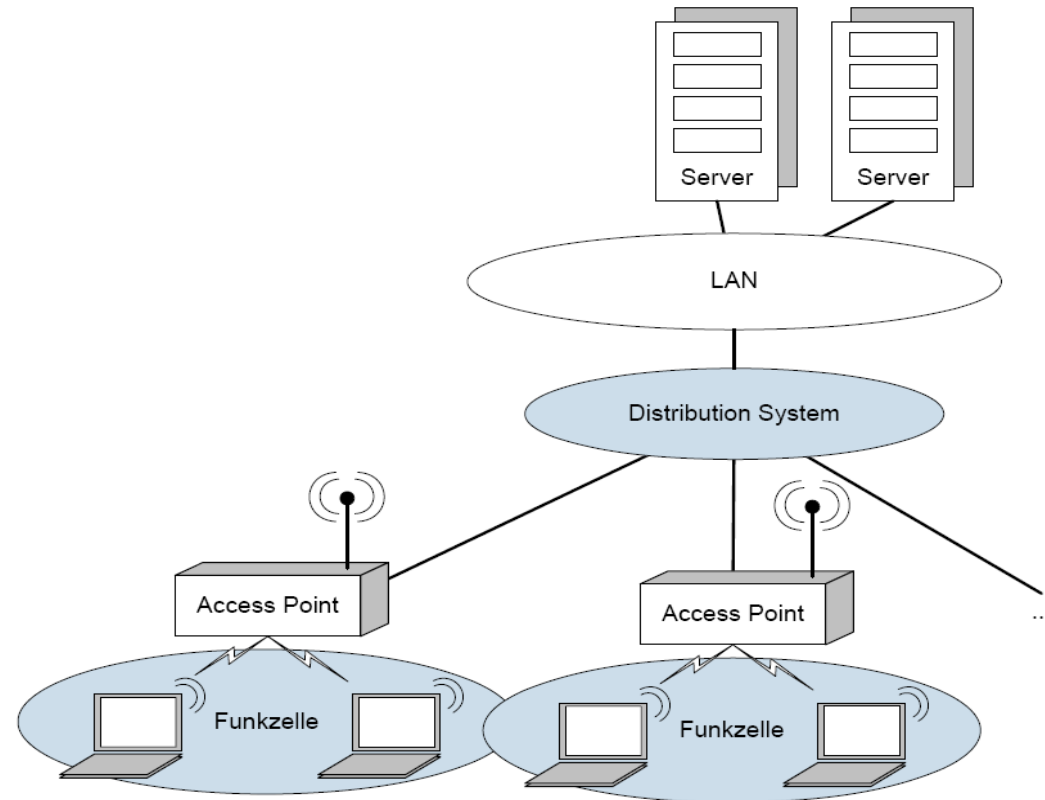
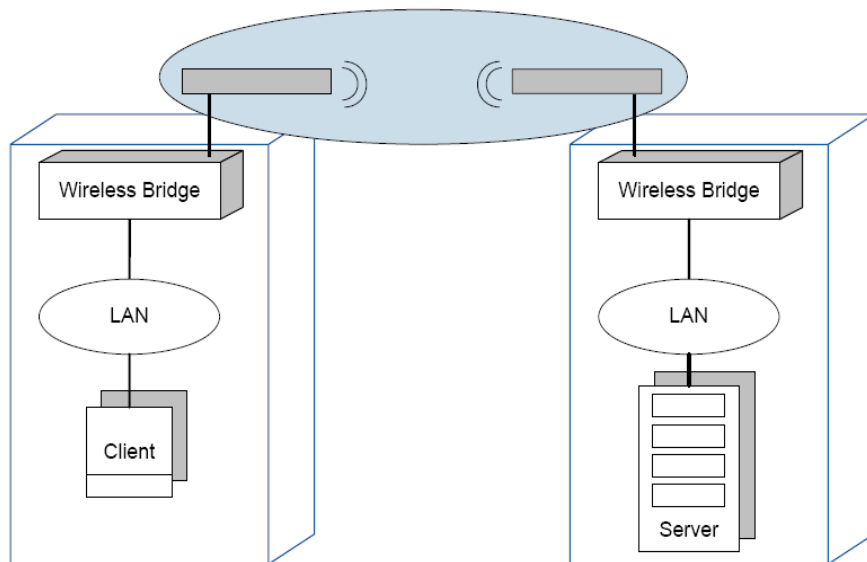
WLAN

Don't broadcast the Service Set Identifier (SSID)

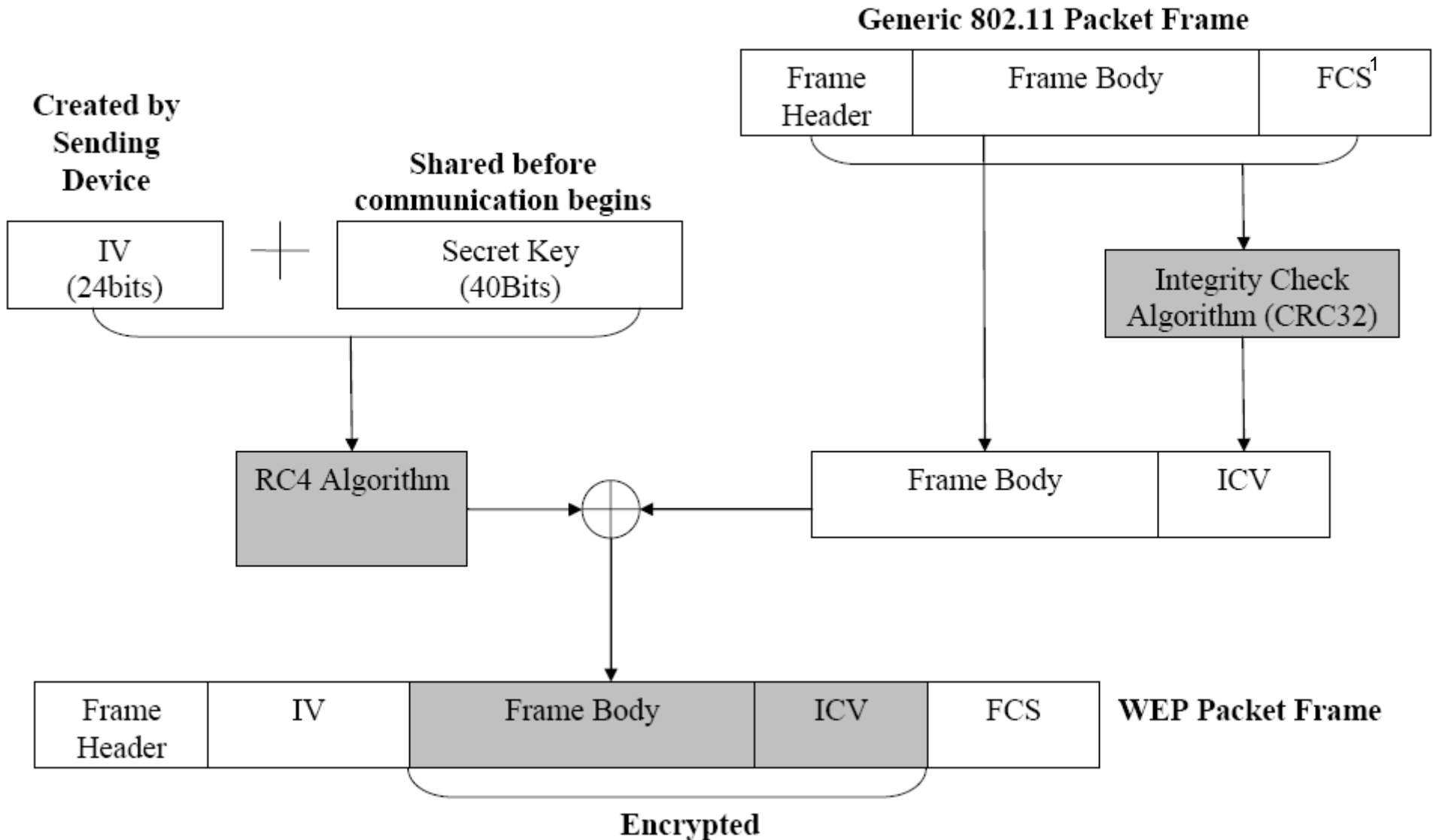
Wired Equivalent Privacy (WEP), **compromised!**

IEEE 802.11i

Wi-Fi Protected Access (WPA)



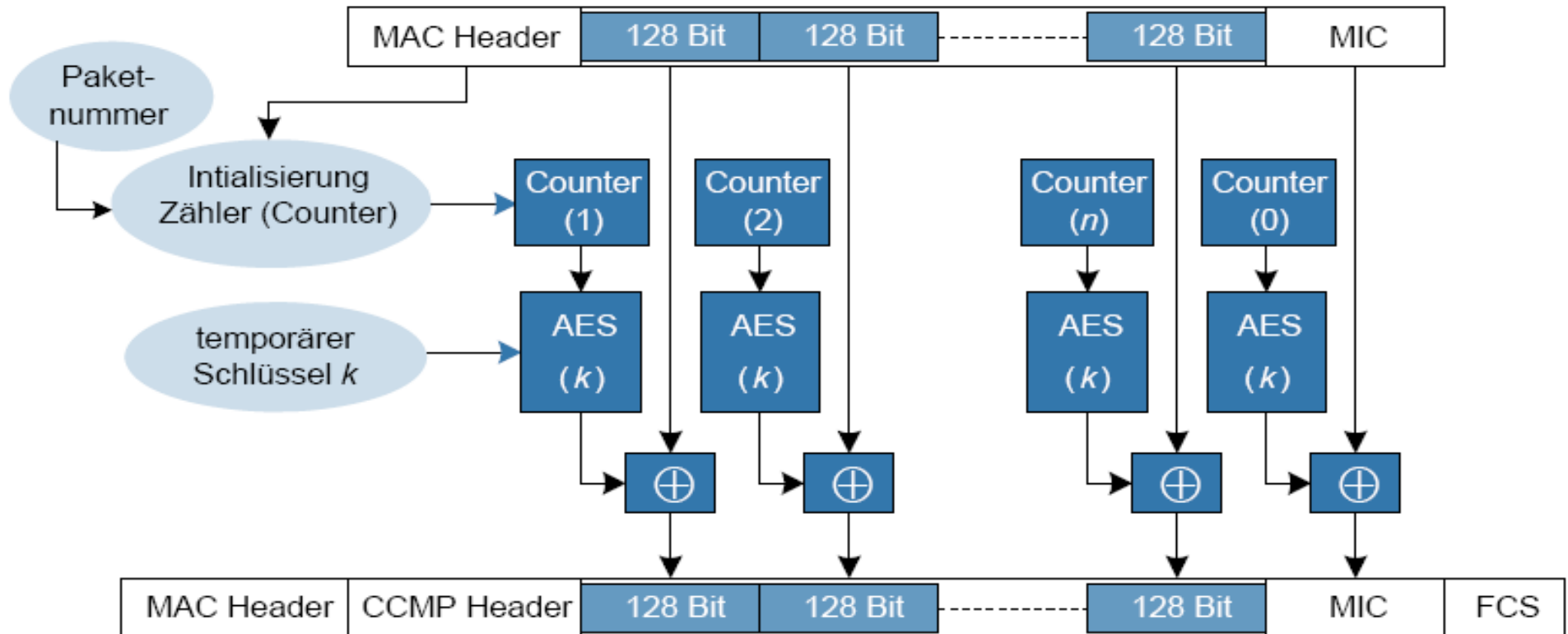
WEP



¹ Frame Check Sequence



AES in IEEE 802.11i



ENISA work

- 2008
Report on Mobile Authentication
<http://www.enisa.europa.eu/act/it/eid/mobile-eid>
- 2009
Report on Mobile Identity Management
<http://www.enisa.europa.eu/act/it/eid/Mobile%20IDM>
- 2010
Report on smartphone application security risks and best practices
Expert working group on smartphone security
- 2011 (planned)
Targeted actions to disseminate best practice in specific areas of smartphone security. Supporting an ongoing promotion of smartphone security best practice through the expert group

Mobile Authentication Paper (1)

Scope

- Token: mobile phones,
PDAs - in conjunction with smart cards.
- Use cases:
 - E-Ticketing using NFC phone
 - Interactive advertising (smart posters)
 - Mobile Voting
 - Electronic signatures (trustworthy viewing)
 - Phone as national ID card
 - Online authentication
- Risk assessment: assets, vulnerabilities, threats

Mobile Authentication Paper

Conclusions

- Consumer's need easy to use solutions.
- Mobile devices can act as a user interface for online applications and become a secure, secondary authentication channel.
- Mobile device as national ID card still a vision in Europe.
- Personalization and registration processes for phones, payment cards and ID cards are different.
- Harmonization is needed:
pan-European interoperability, privacy requirements,
global standards

Mobile Identity Management

- Identity theft:
 - Mobile devices contain a wide range of personal information (including even personal credentials, such as encryption keys or biometric data), making mobile devices a gold mine for identity thieves.
 - Much easier to steal the actual device – remote wipe and reset important
- Bluetooth pairing is not user-friendly and sniffing is possible.
- Traffic data or localized EMEI (International Mobile Equipment Identity) data can be used for unauthorized monitoring or surveillance.

Mobile Identity Management

- Weaknesses in GSM and 802.11x encryption make eavesdropping attacks relatively easy :
[<http://www.engadget.com/2008/02/21/researchers-claim-gsm-calls-can-be-hacked-on-the-cheap/>].
- In GSM, encryption is only applied for the wireless transmissions, that is, the messages are sent in plain text from the base station to the gateways.
- Smartphone applications now offer another layer of encrypted SMS and calls.

Mobile Identity Management

- Many privacy protection mechanisms assume the existence of a trusted third party that can certify the credentials of a service provider.
- This requires connectivity to the trusted third party or reliance on public key infrastructure.
- However, a mobile device may experience frequent disconnections from the Internet and/or an infrastructure
- Biometrics are not effective for remote authentication because you cannot trust the device.

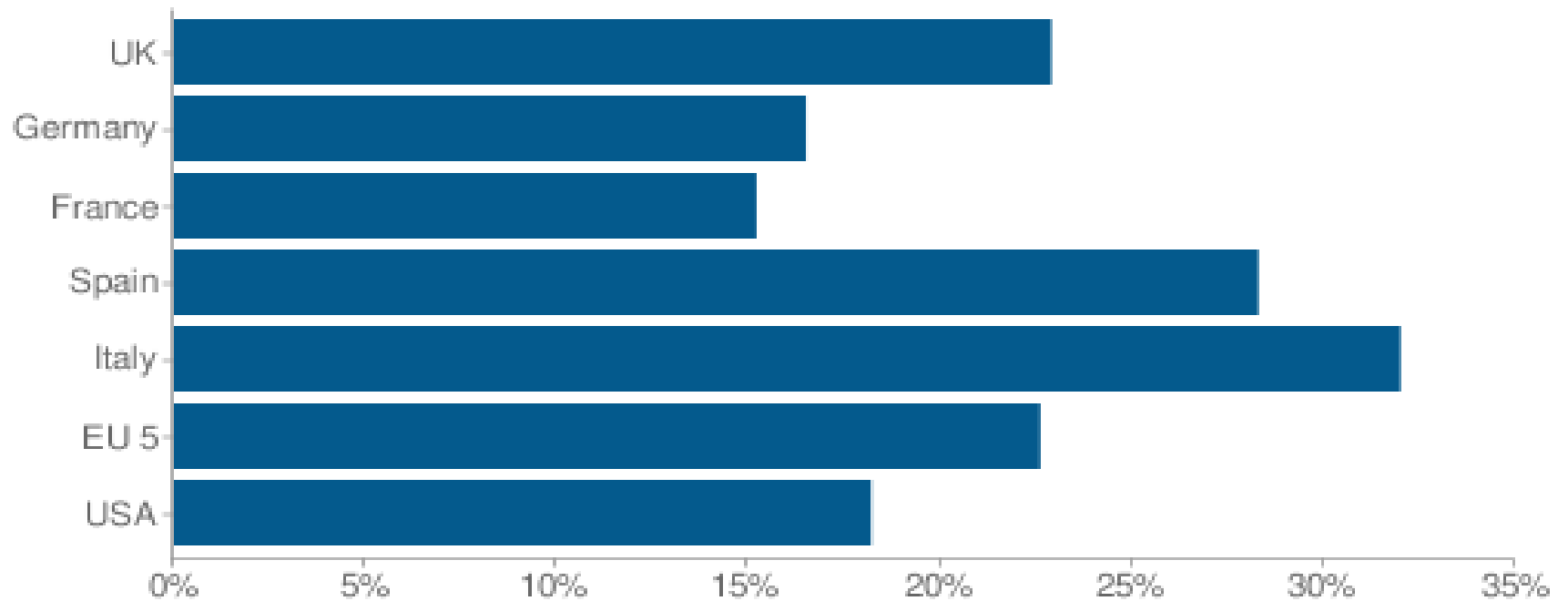


1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Overview
 - **Smart Phone Security**
5. Elliptic Curve Cryptography

SMARTPHONE SECURITY

Smartphone Security

Market penetration (%) of Smartphones



Comscore data for 2009

Smartphone: Capabilities

- Full internet access capabilities.
- Support for storing and making use of private data.
- Support for a wide range of applications, including e.g. Internet banking and location-based social applications.
- Supported applications are becoming more critical.
- Possibility to download third party applications from “marketplaces”.
- Smartphones are often equipped with sensors.
 - Position, Acceleration, Orientation, Temperature, Magnetic field.



Smartphones: Security Issues (I)

- Smartphones are designed to be used **anywhere** – the security model must take account of this.
- This immediately implies that sensible use of the device will be a major concern.
- Security model may not be well understood by most users, but users tend to trust the security model without question.
- Security cues are harder to implement reliably on a small form factor.
- Physical security of the device is a major issue, due to the high probability of loss or theft.



Smartphones: Security Issues (II)

- Standardisation is an issue:
 - Many different devices and development platforms.
 - Different access control and security models.
 - Marketplaces have different policies regarding application security.
- Implementing cryptographic solutions on smartphones is not easy
 - There is a need for lightweight cryptography due to the limitations on size and performance.
 - The size and diversity of the community makes key management problematic.
 - Some currently used solutions are still weak – e.g. Wireless encryption.

Smartphones: Security Issues (III)

- We are not prepared for smartphone security issues, because we are used to phones being diverse, locked down platforms.
- Smartphones used for increasingly critical applications – the device contains a snapshot of a person's life.
 - Address book, photos, social networks, email, etc....
 - One of the first actions after the Polish government plane came down was for the intelligence services to go in and find their blackberries.
 - Interpol has joined our expert group and uses smartphones for non-sensitive data.
 - Risks very different for business and end-users.

Secure Development & Testing

- Many different devices and development platforms.
- Patching and updates are currently VERY primitive:
 - e.g. Android has only a 6 monthly patching cycle and the apps have to be updated manually.
 - This is largely due to difficulty of testing patches on so many devices.
- Battery life and airtime costs are also important considerations.
- Development nightmare similar to internet before the web came along.
- Makes security testing very difficult.



Other key security issues (1)

- Preventing phishing – application identity is very weakly verified. But users tend to equate signatures with trust. Now banks are issuing applications.....
- Some devices do not give enough privileges (for security reasons) to allow for effective anti-virus software.
- The main model for application access control is to ask for permissions at application install time. In reality people never read these consent requests.
- Form factor and battery life is a key limiting factor on e.g. Anti-virus

Other key security issues (2)

- Individual sensors might not give away much information, but mining/combining them might.
- For instance, combining sensor output from Accelerometer and Magnetometer data.
- Actually smartphones have realised the vision of the so-called **Internet of Things**, without anyone realising it.
- They provide a network of interconnected sensors which are attached to people and locations.



Solution for speech encryption (1)



TOPSec GSM



 <http://www.rohde-schwarz.de/>

Solution for speech encryption (2)

 <http://www.secusmart.de/>

seamless secure communication

Welcome to Secusmart.

Secuvoice

Latest News

Security can be so easy!

Secusmart combines top security voice encryption and authentication technology with modern mobile phones.



1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. **Elliptic Curve Cryptography**
 - Motivation
 - Elliptic Curves
 - Cryptography on Elliptic Curves

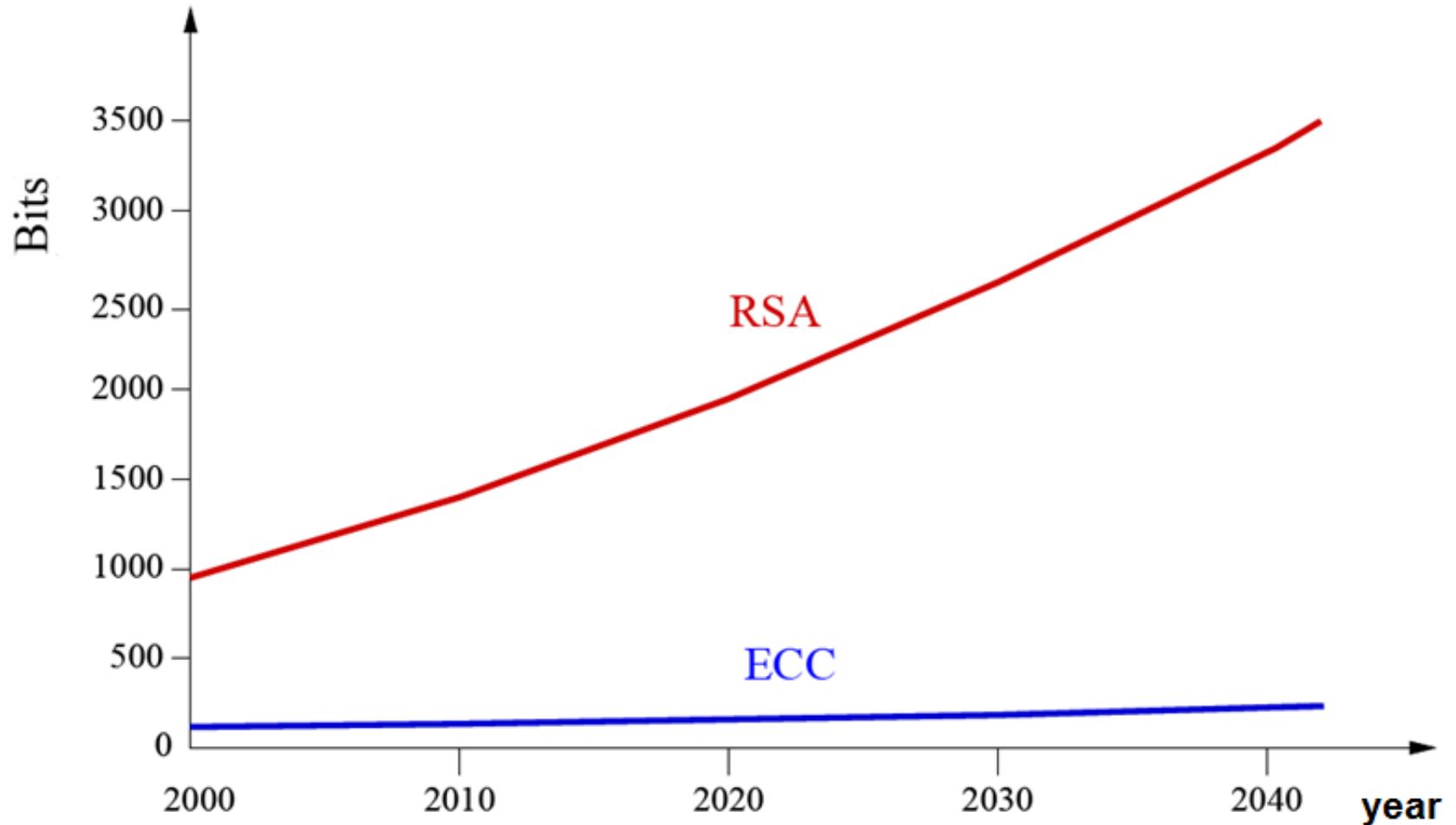
ELLIPTIC CURVE CRYPTOGRAPHY

1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography
 - **Motivation**
 - Elliptic Curves
 - Cryptography on Elliptic Curves

MOTIVATION

Security

Keylength RSA - 1.024 corresponds to Keylength ECC - 160



Examples





Zertifizierungsrichtlinie

eHealth Token CA 02

Version: V 2.0
 Datum: 26.3.2007
 Status: Freigegeben

Bundesministerium für Gesundheit, Familie und Jugend
 Abteilung I/A/15 (organisatorisch)
 Abteilung I/A/2 (technisch)

Radetzkystraße 2
 1030 Wien

Tel.: +43 (0)1 711 00-0
 Fax: +43 (1) 713 44 04 - 2179
 DVR 2109254

Email: ca@ehvd.at
 Web: <https://ca.ehvd.at>

Zertifizierungsrichtlinie

eHealth Token CA 02

dort in Form von Fingerprints oder X.509 Zertifikaten abrufbar – siehe 2.2).

Zusätzlich wird der öffentliche Schlüssel des eHealth Token CA 02 Zertifizierungsdienstes von der RTR als Aufsichtsstelle veröffentlicht.

6.1.5 Schlüssellänge

Die Schlüssellänge in den eHealth Zertifikaten ist folgender Tabelle zu entnehmen:

eHealth Trustcenter 02 Stammzertifikat	eHealth Token CA 02 CA-Zertifikat	eHealth Token CA 02 Anwenderzertifikat
RSA 4096 bit	RSA 4096 bit	RSA 2048 bit ECDSA 192 bit

6.1.6 Parameter der Schlüssel-Generierung

Schlüssel für eHealth CA-Zertifikate sind RSA Schlüssel.

Für eHealth Anwenderzertifikate werden RSA Schlüssel mit 2048 bit und ECDSA Schlüssel nach X9.62 mit 192 bit mit der named curve prime192v1 (1.2.840.10045.3.1.1) unterstützt. Siehe auch 7.1.3.

Für Schlüssel die in der Zertifizierungsstelle erzeugt werden, wird ein Pseudozufallszahlengenerator verwendet.



1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography
 - Motivation
 - **Elliptic Curves**
 - Cryptography on Elliptic Curves

ELLIPTIC CURVES

Mathematics: Groups & Fields

A **group** is a set S together with a binary operation “ x ”

- Closure: For all a, b in S : $a x b$ is in S
- Associativity: For all a, b and c in S : $(a x b) x c = a x (b x c)$
- Identity element: There exists an element e in S , such that for every element a in G , the equation $e x a = a x e = a$ holds.
- Inverse element: For each a in G , there exists an element b in G such that $a x b = b x a = e$, where e is the identity element.

An **Abelian group**: Commutativity of x : $a x b = b x a$

A **Field** is a set S together with binary operations “ $+$ ”, “ \cdot ”:

- Closure: For all a, b in S : $a + b$ is in S and $a \cdot b$ is in S
- Associativity: For all a, b, c in S : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Identity element: *additive identity*: $a + 0 = a$, *multiplicative identity*: $a \cdot 1 = a$
- Inverse element: $-a$: $a + (-a) = 0$, a^{-1} : $a \cdot a^{-1} = 1$
- Distributivity : $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Modulo Operation & Finite Fields

Modulo operation

a, b, n are integer,

a and b is **congruent modulo n** ,

if $(a - b)$ is an integer multiple of n :

$$a = b \pmod{n}$$

Finite field or Galois field (GF in honor of Evariste Galois)

contains a finite number of elements

there is exactly one finite field up to isomorphism of size p^n for each prime p and positive integer n

Example

$$\mathbb{Z}_{10} = \{0, 1, 2, \dots, 9\}$$

$$\begin{aligned} \mathbb{Z}_{10}^* &= \{x \text{ in } \mathbb{Z}_n \mid \gcd(x, 10) = 1\} \\ &= \{1, 3, 7, 9\} \end{aligned}$$

ggT(0, 10) = 10
ggT(1, 10) = 1
ggT(2, 10) = 2
ggT(3, 10) = 1
ggT(4, 10) = 2
ggT(5, 10) = 5
ggT(6, 10) = 2
ggT(7, 10) = 1
ggT(8, 10) = 2
ggT(9, 10) = 1

• (mod 10)	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

\mathbb{Z}_{10}^* is a group !

Example

A **cyclic group** can be generated by a single element “a”.
 G is a group, define

$$\langle a \rangle := \{a^n \text{ for } a \text{ in } G \text{ a subset of } Z\}$$

If $\langle a \rangle = G$ then G is called cyclic group.

$a=2, \text{ mod } 10$:

$$\langle 2 \rangle^+ = \{2, 4, 6, 8, 0\}$$

$$\langle 2 \rangle^* = \{2, 4, 8, 6\}$$

+	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

·	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

Elliptic Curve Groups over Real Numbers

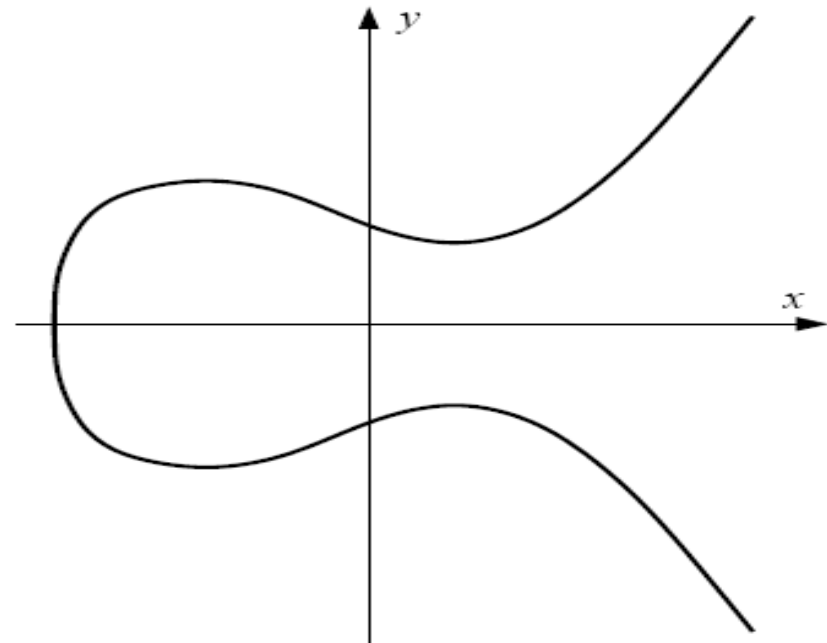
An elliptic curve over a real field K is defined as the set of points (x,y) which satisfy the equation (“Weierstrass-equation”)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with a_i real and (x,y) elements of E :

$$E = \{(x, y) \text{ in } K \times K \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

\mathcal{O} is the point in infinity.



Example with $K = \mathbf{R}$

ECC for Cryptography

For cryptographic applications the following elliptic curves are used:

$$y^2 = x^3 + ax + b \quad \text{with } 4a^3 + 27b^2 \text{ unequal } 0$$

$$y^2 + xy = x^3 + ax^2 + b \quad \text{with } b \text{ unequal } 0$$

on the finite field $GF(2^n)$ resp. $GF(p)$, $p > 3$ prime.

Addition of Points on EC

E is an elliptic curve

$P + \mathcal{O} = \mathcal{O} + P = P$ for all P on E ,

For $P = (x, y)$ and $Q = (x, -y)$: $P + Q = \mathcal{O}$,

For $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ on E with P_i unequal \mathcal{O} and (x_2, y_2) unequal $(x_1, -y_1)$ $P_3 := P_1 + P_2$, $P_3 = (x_3, y_3)$ with

$$x_3 := -x_1 - x_2 + \lambda^2$$

$$y_3 := -y_1 + \lambda (x_1 - x_3)$$

$$\lambda := \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{for } P_1 \neq P_2, \\ \frac{3x_1^2 + a}{2y_1} & \text{for } P_1 = P_2. \end{cases}$$

If $P = (x, y)$ then $-P = (x, -y)$ on E .

$E \cap \mathcal{O}$ is a group.

Adding distinct points P and Q

When $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are not negative of each other,

$P + Q = R$ where

$$s = (y_P - y_Q) / (x_P - x_Q)$$

$$x_R = s^2 - x_P - x_Q \text{ and } y_R = -y_P + s(x_P - x_R)$$

Note that s is the slope of the line through P and Q .

Doubling the point P

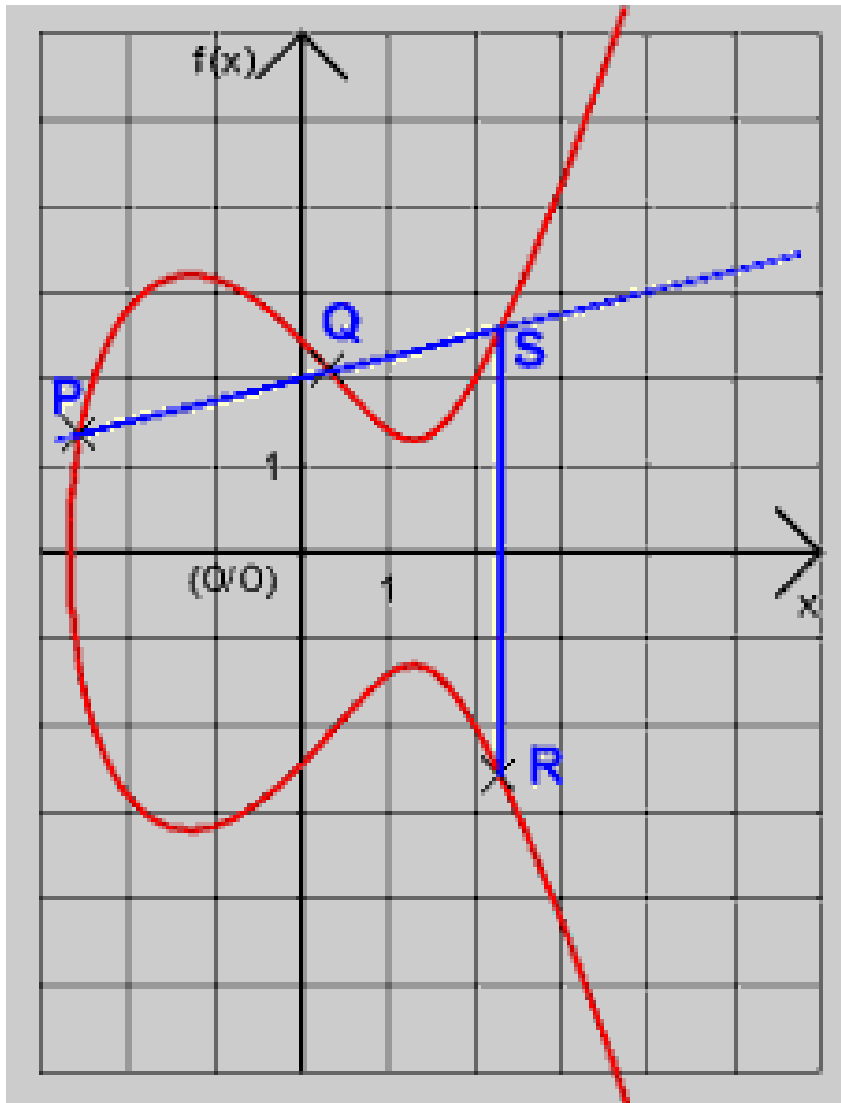
When y_P is not 0,

$2P = R$ where

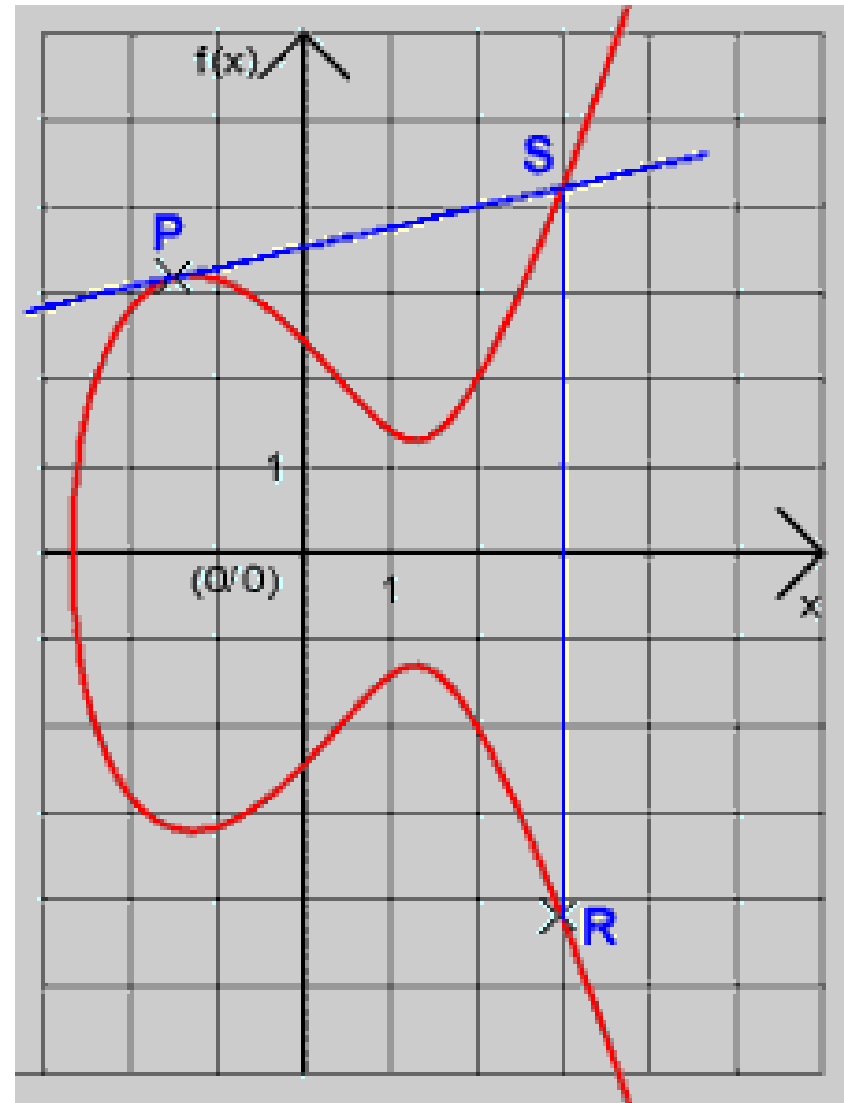
$$s = (3x_P^2 + a) / (2y_P)$$

$$x_R = s^2 - 2x_P \text{ and } y_R = -y_P + s(x_P - x_R)$$

a is one of the parameters chosen with the elliptic curve and that s is the tangent on the point P



$$R = P + Q$$

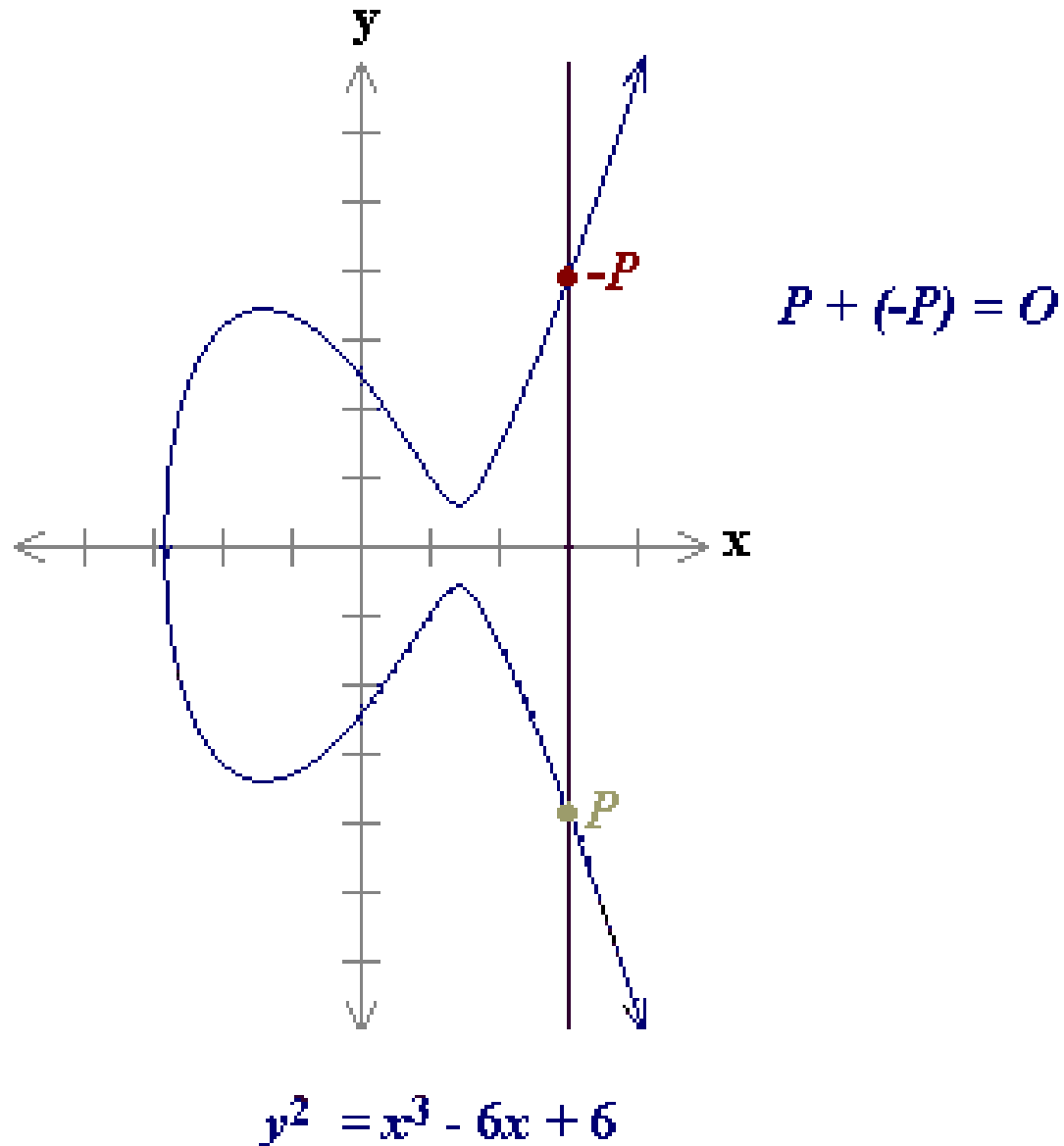


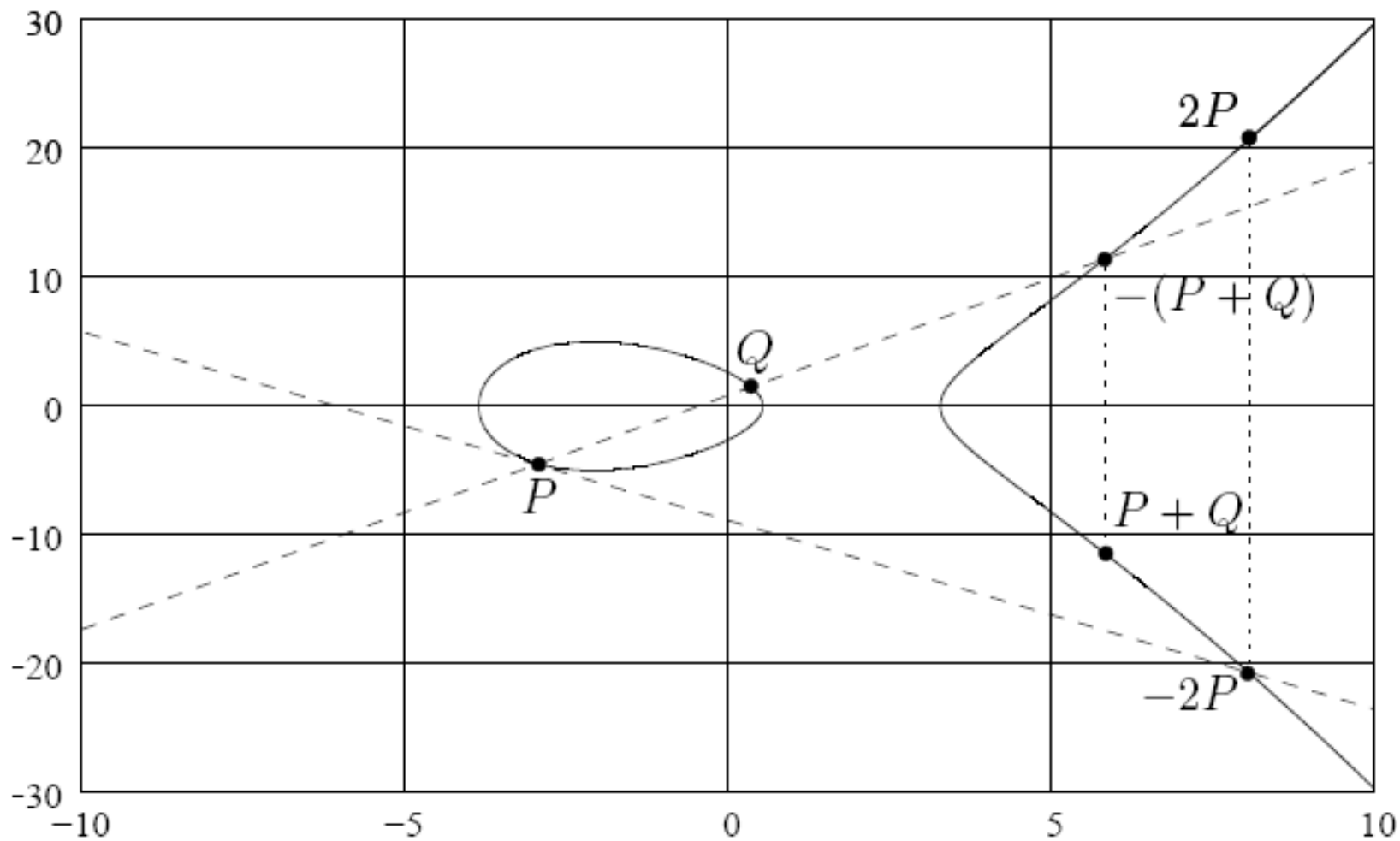
$$R = 2P$$

The line through P and $-P$ is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and $-P$ cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity O .

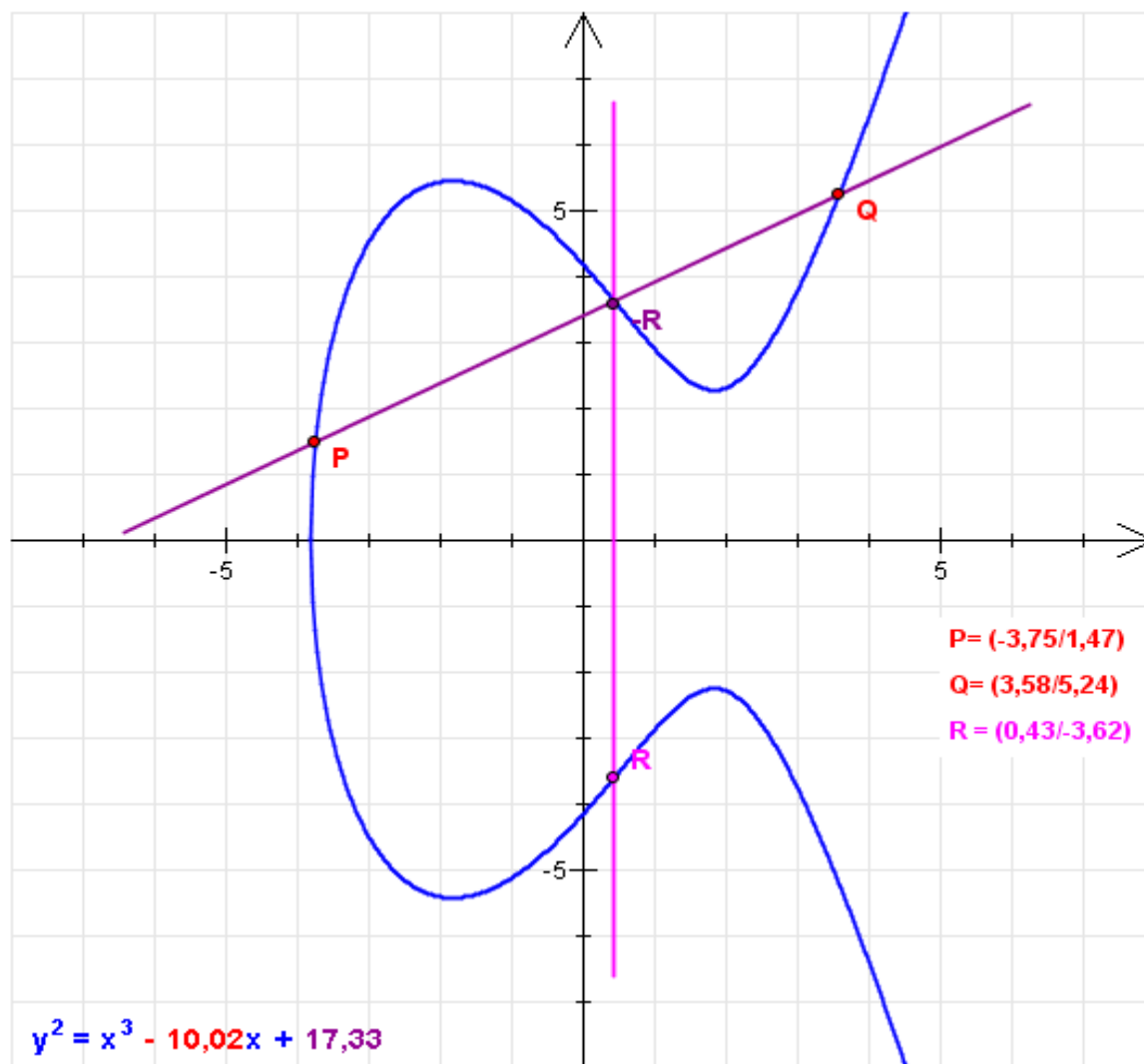
By definition, $P + (-P) = O$.

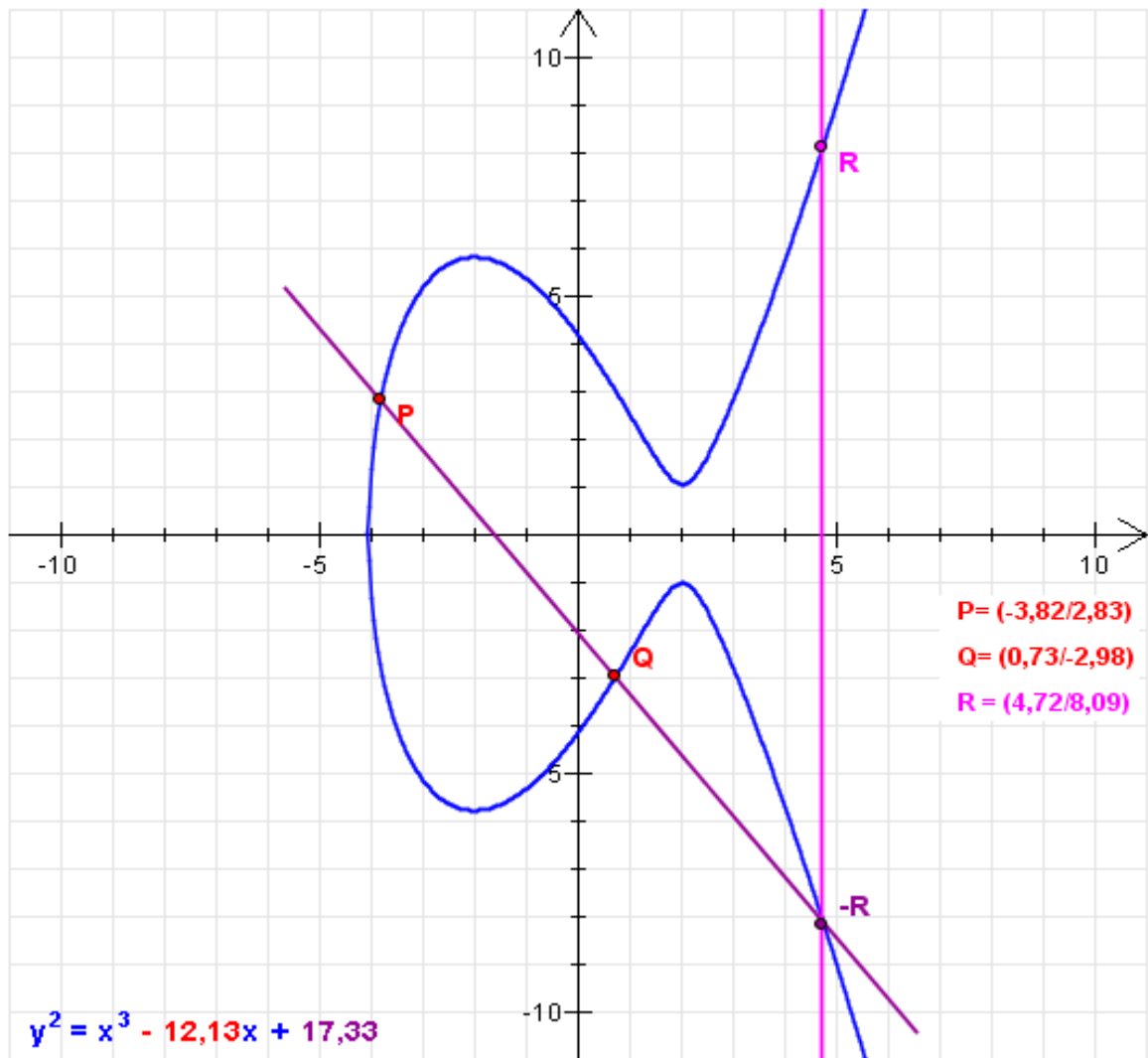
As a result of this equation, $P + O = P$ in the elliptic curve group. O is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity

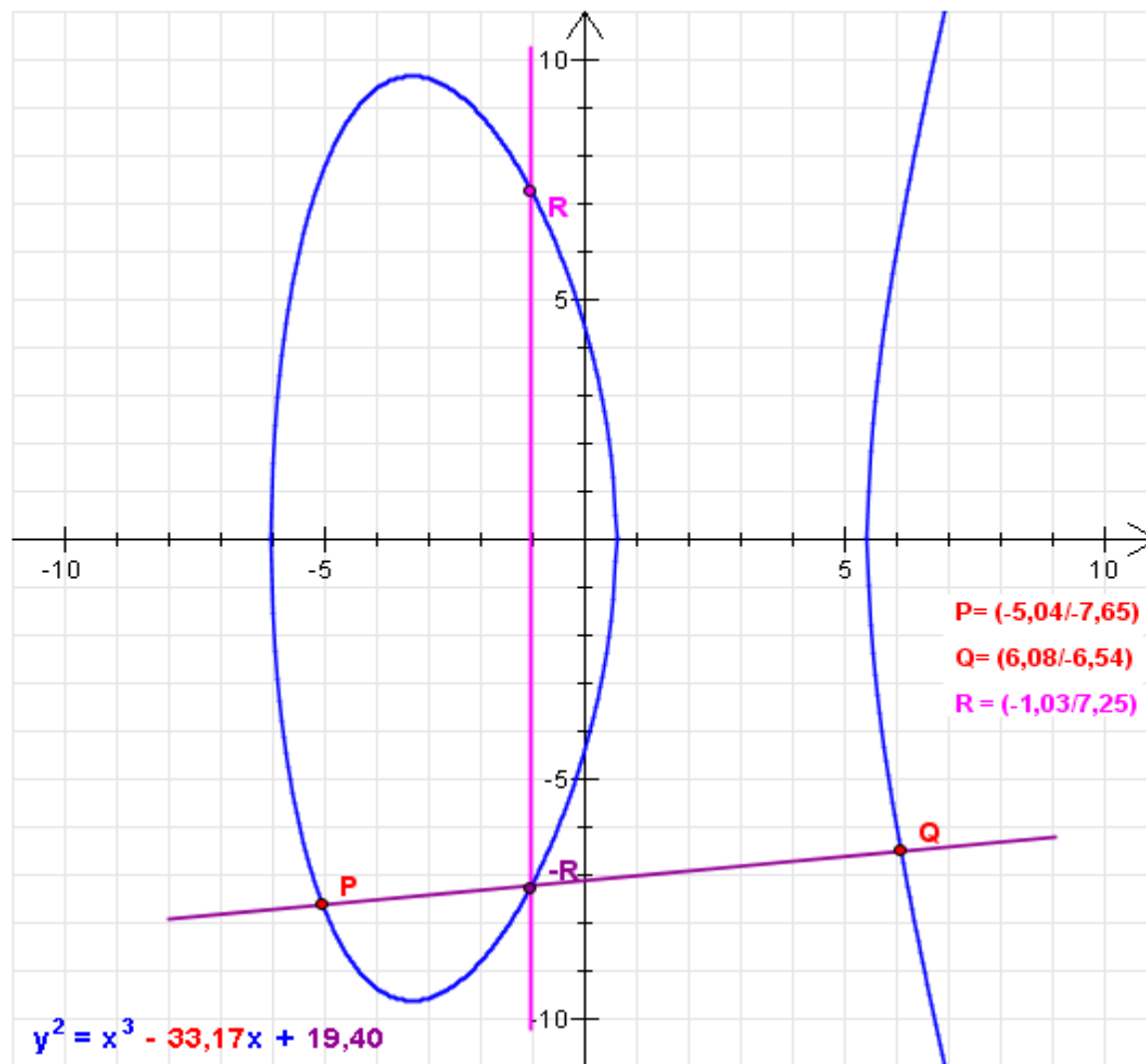


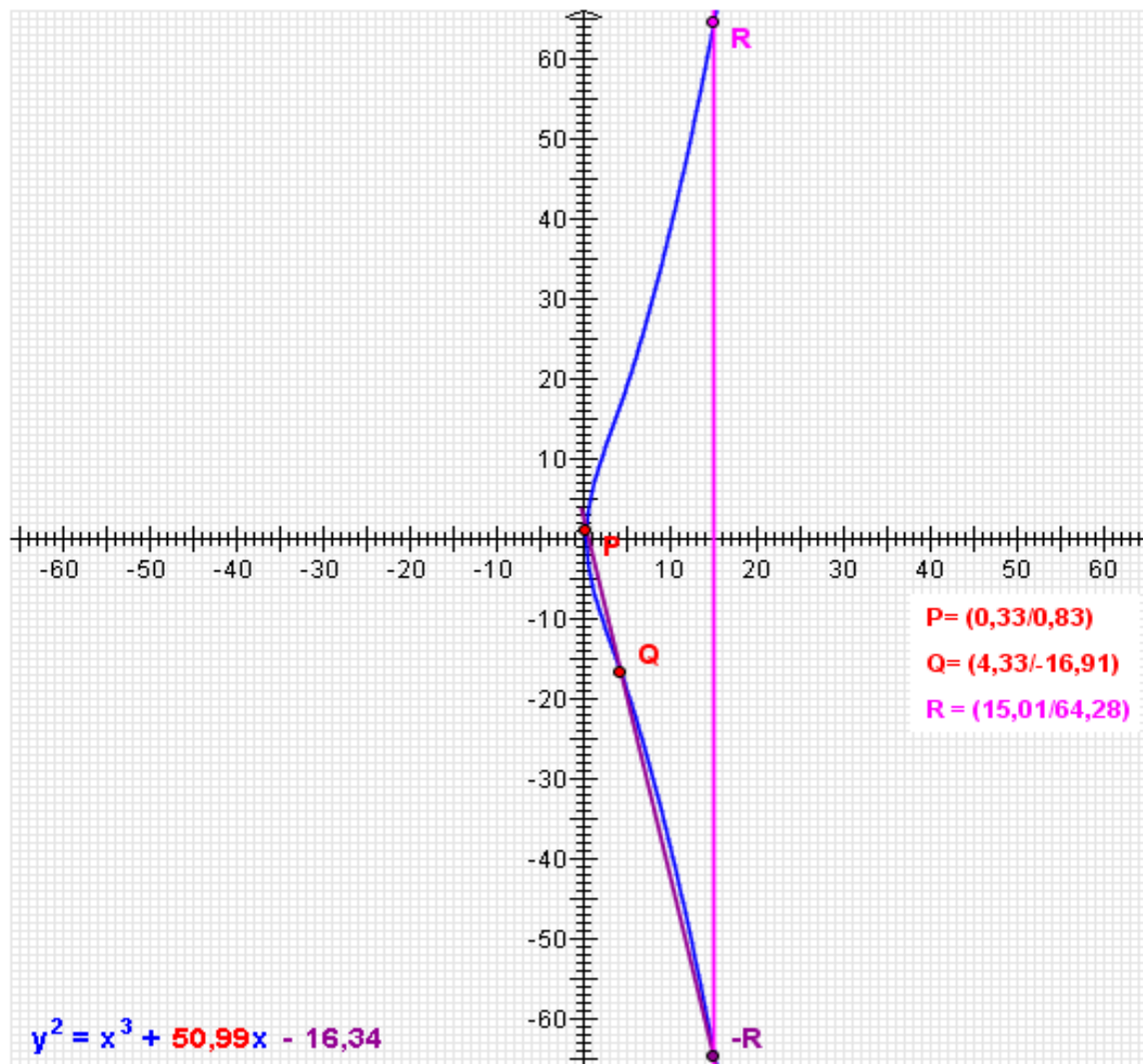


$$y^2 = x^3 - 13x + 7$$









1. IT-Security Risks
2. Political Awareness in ICT
3. Technological Areas with an Impact on Resilience
 - Development of Network Technologies
 - Cloud Computing
 - Data Protection and Legal compliance in Cloud Computing
 - Future Wireless Networks
 - Sensor networks
 - Integrity of supply chain
4. Mobile Computing Security
 - Smart Phone Security
5. Elliptic Curve Cryptography
 - Motivation
 - Elliptic Curves
 - **Cryptography on Elliptic Curves**

CRYPTOGRAPHY ON ELLIPTIC CURVES

Source: <http://www.certicom.com/index.php/ecc>

RSA vs. ECC

RSA-Algorithm

Signing, Encryption, Key-distribution based on “e-th root mod n” problem, hardness is believed to rely on the difficulty of factoring n

$$y := g^k \text{ mod } n \quad n=p \cdot q, \quad p, q \text{ prime}$$

$$\log_g(g^k) = k$$

Elliptic Curve-Cryptography (ECC)

is based on arithmetic of points from an elliptic curve over a finite field, i. e. solutions of the equation

$$E: y^2 = x^3 + a x + b \text{ mod } p$$

“discrete log” problem on elliptic curves

Example

Elliptic curves E on discrete fields $GF(p)$.

Parameters a and b within the field of $GF(p)$.

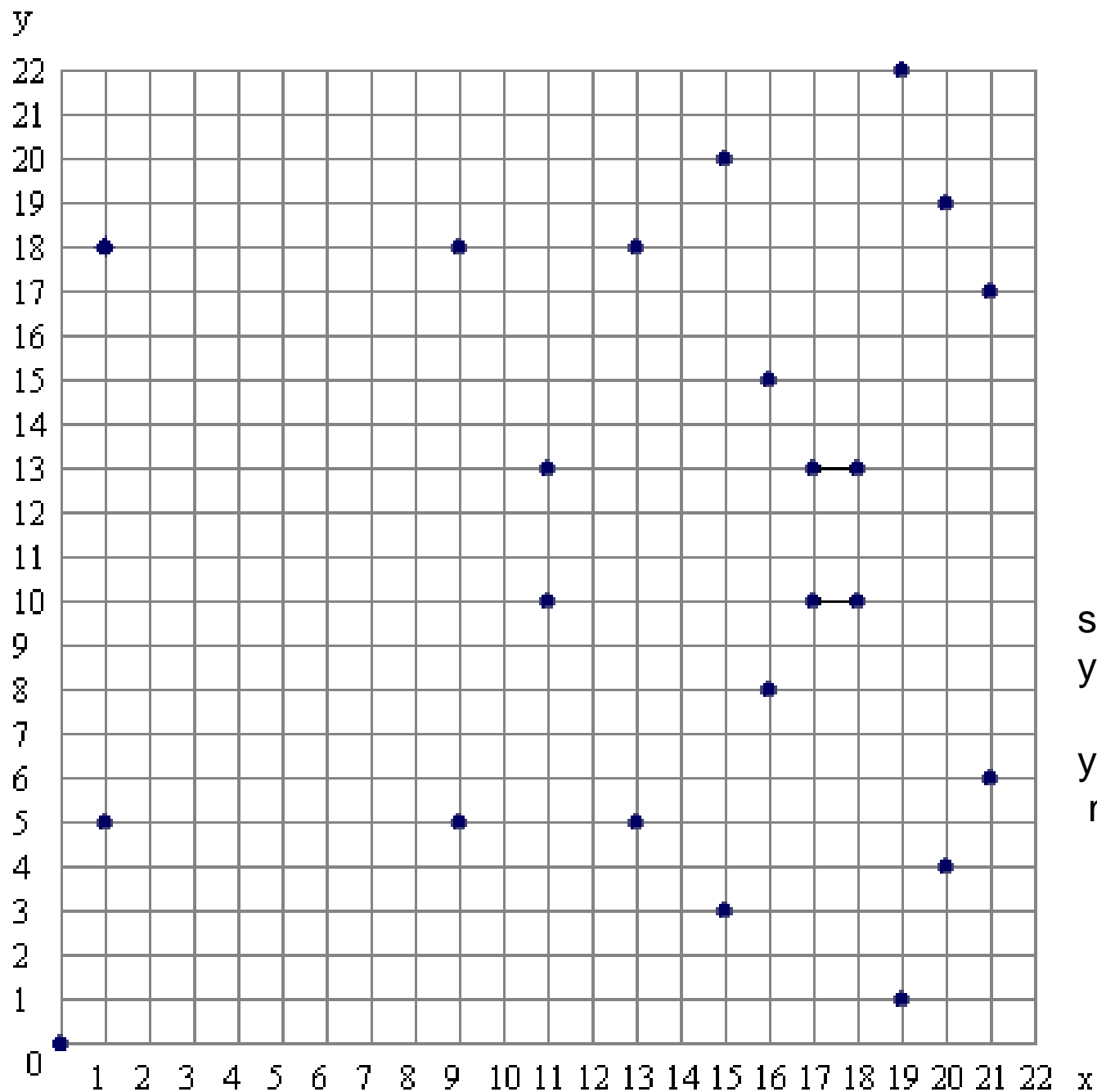
$GF(23)$ the field is composed of integers from 0 to 22.

$a = 1$ and $b = 0$, the elliptic curve equation is $y^2 = x^3 + x$.

The 23 points are:

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5)
(13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13)
(18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6)
(21,17)

e.g. for (9,5):
 $y^2 \bmod p = x^3 + x \bmod p$
 $25 \bmod 23 = 729 + 9 \bmod 23$
 $25 \bmod 23 = 738 \bmod 23$
 $2 = 2$



symmetry about
 $y = 11.5$

y-values are taken
modulo 23

Elliptic Curve Discrete Logarithm Problem

For every m in Z we can calculate $mP := P + P + \dots + P$.

To calculate mP one needs $\log m$ additions!

But

To calculate m for given P and $Q = mP$ one needs m additions!

Until now no efficient algorithm is known to calculate m .

This is called the „ECDLP - Elliptic Curve Discrete Logarithm Problem,,

Challenge: to find „good elliptic curves“

<http://www.certicom.com/index.php/curves-list>

ECC Technical Guideline¹⁾ TR-03111

(1) Elliptic Curve Domain Parameters

- ◆ the finite field \mathbf{F}_p
- ◆ the coefficients a and b of the Weierstraß equation
- ◆ a base point G in the group $E(\mathbf{F}_p)$,
- ◆ its order n in $E(\mathbf{F}_p)$
- ◆ the cofactor $h = \#E(\mathbf{F}_p)/n$
- ◆ the base point G generates a cyclic subgroup of order n in $E(\mathbf{F}_p)$:
 $\langle G \rangle = \{G, [2]G, [3]G, \dots, [n-1]G, [n]G\}$

Parameter	Comment
p	A prime number specifying the underlying field \mathbb{F}_p .
a	The first coefficient of the Weierstraß equation E (cf. Section 2.2.3).
b	The second coefficient of the Weierstraß equation E (cf. Section 2.2.3).
G	A base point on $E(\mathbb{F}_p)$.
n	The order of G in $E(\mathbb{F}_p)$.
h	The cofactor of G in $E(\mathbb{F}_p)$.

(2) elliptic curve discrete logarithm problem (ECDLP)

given (1) and an elliptic curve point P in $\langle G \rangle$

find the unique integer k , $1 \leq k < \underline{n} - 1$ such that $P = [k]G$.

- ◆ An elliptic curve group is called cryptographically strong if the underlying ECDLP is considered to be intractable for the application in use.
- ◆ Cryptographically strong elliptic curve groups for different security levels are published by standardization bodies (e.g. ECC-Brainpool, ANSI, NIST, ISO).

ECDLP is currently considered to be intractable, if at least the following conditions hold:

1. The order n of the base point G MUST be a prime of at least 224 bits.
2. To avoid the elliptic curve to be anomalous the order n MUST be different from p .
3. The ECDLP MUST NOT be reducible to the DLP in a multiplicative group F_{p^r} for a 'small' integer r . Thus, it is REQUIRED that $p^r \not\equiv 1 \pmod{n}$ for all $1 \leq r \leq 10^4$.
4. The class number of the fundamental order of the endomorphism ring of E SHOULD be at least 200. If an elliptic curve is generated at random, this curve respects this requirement with a very high probability

Elliptic Curve Key Pair Generation

- ◆ An elliptic curve key pair consists of a public key P and a private key d . Such a key pair is generated as follows:
- ◆ Input: Cryptographically strong elliptic curve domain parameters
(p, a, b, G, n, h)
- ◆ Output: the key pair (d, P)
- ◆ Actions: The following actions are performed:
 1. $\text{RNG}(\{1, 2, \dots, n - 1\}) \rightarrow d$
where RNG denotes a (pseudo) random number-generator
 2. $[d]G \rightarrow P$
 3. Output (d, P).

Diffie Hellmann over ECC

- ◆ Alice and Bob agree in public on an elliptic curve E defined in $GF(p)$.
- ◆ They select on random r_A, r_B in $\{1, 2, \dots, p-1\}$ and starting point G .
- ◆ Calculate points $R_A = r_A G, R_B = r_B G$ on E .
- ◆ They exchange R_A and R_B .
- ◆ Alice calculates $R = r_A R_B$.
- ◆ Bob calculates $R = r_B R_A$ which equals $r_B r_A G = r_A r_B G$.

Diffie Hellmann over ECC

Select $p = 23$, $a = 1$, $b = 0$, $G = (9,5)$.

Alice selects randomly his private key $r_a = 4$ and Bob $r_b = 5$.

Alice calculates the public key $R_a = r_a G = (18,13)$, Bob $R_b = r_b G = (9,18)$.

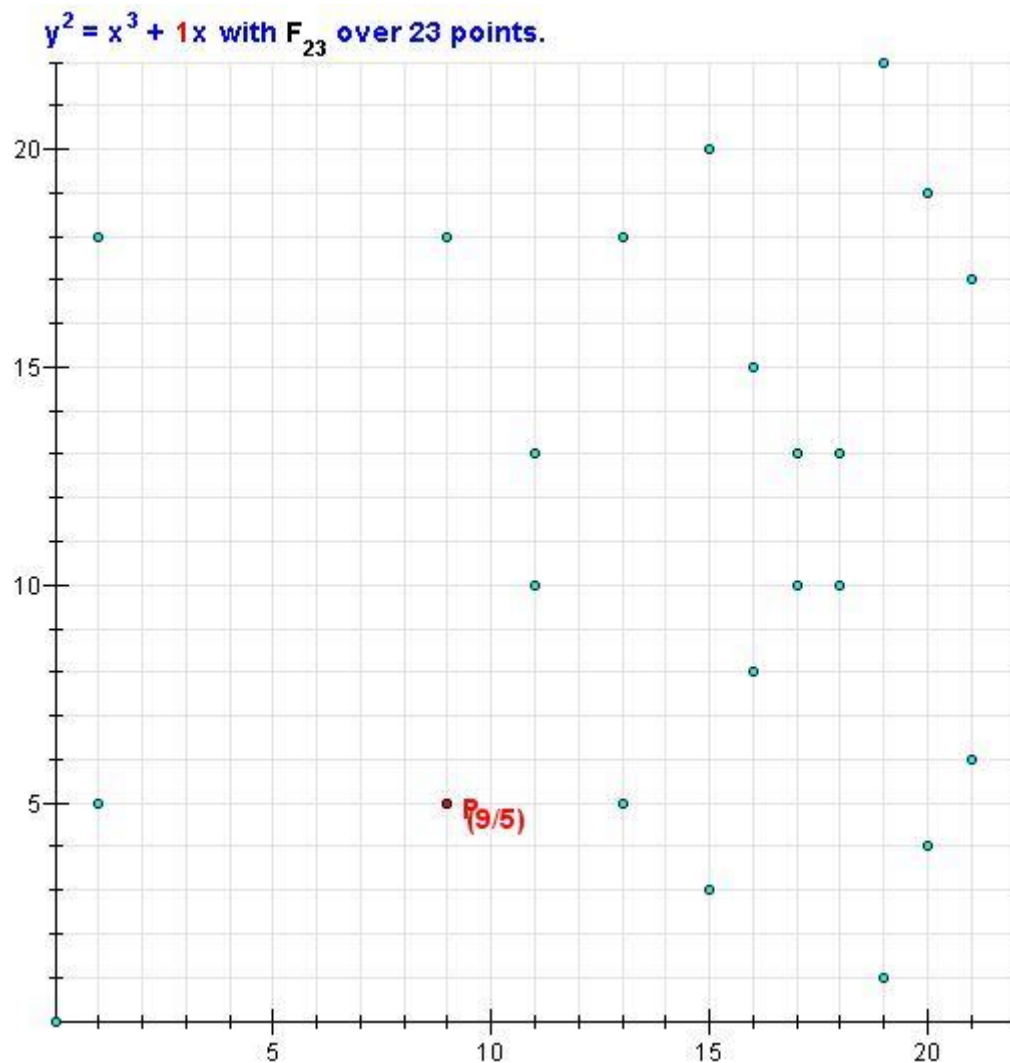
Both exchange R_a and R_b

$$R_{\text{Alice}} = r_a R_b = (0,0)$$

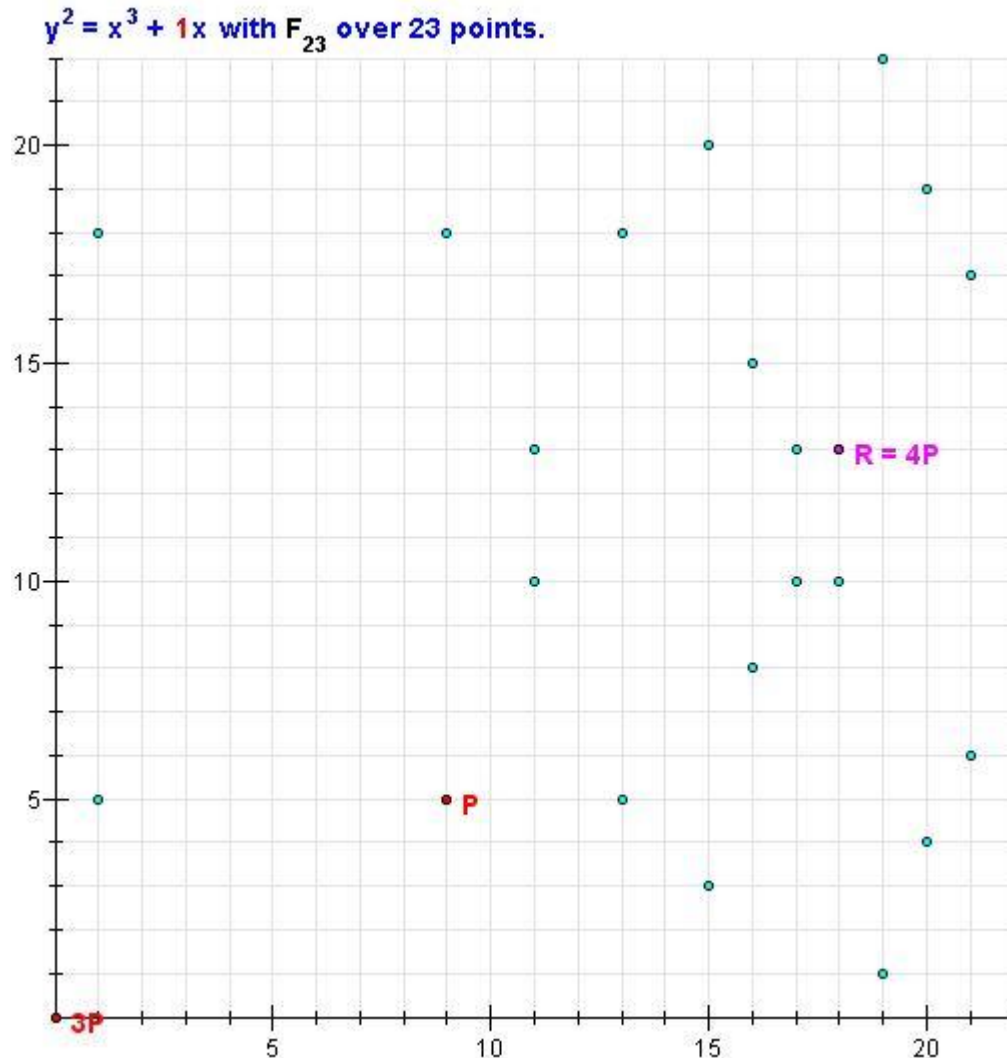
$$R_{\text{Bob}} = r_b R_a = (0,0)$$

$$R_{\text{Alice}} = r_a R_b = r_a (r_b G) = r_b (r_a G) = r_b R_a = R_{\text{Bob}}$$

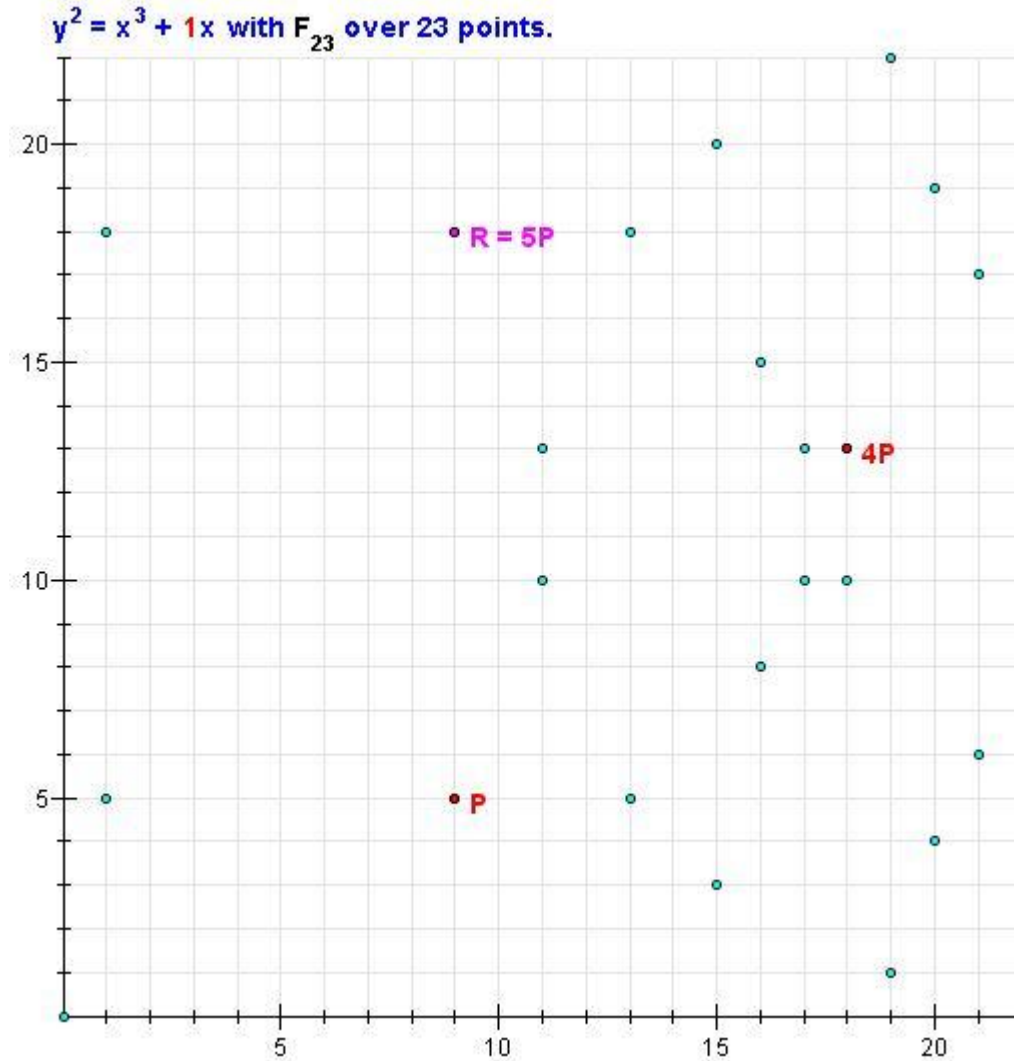
$$G = (9,5)$$



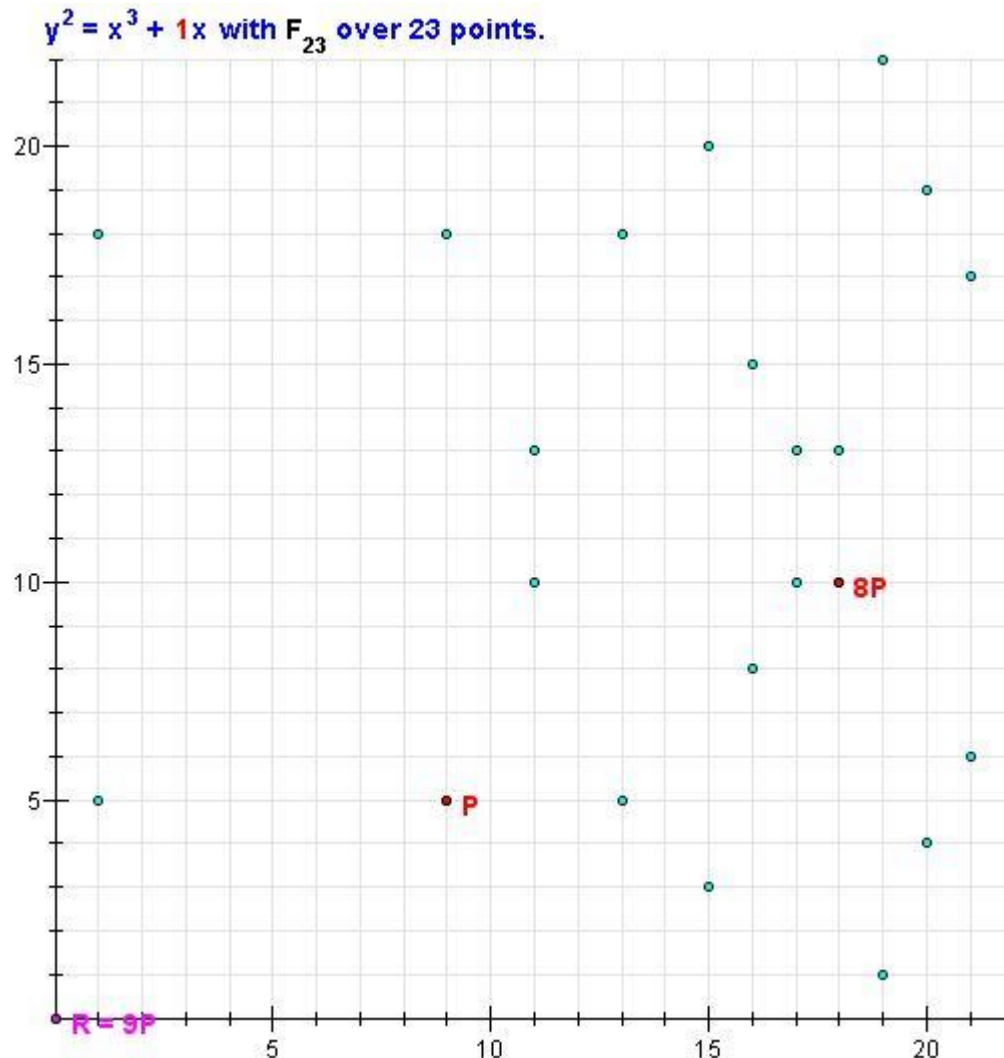
$$R_a = 4 G = (18, 13)$$



$$R_b = 5 \quad G = (9, 18).$$



$$R_{\text{Alice}} = r_a R_b = 9 G = (0,0) = R_{\text{Bob}}$$



ECDLP

Example: $GF(23): y^2 = x^3 + 9x + 17$

Problem: What is the ECDLP of $Q = (4,5)$ and $P = (16,5)$?

Solution: $P = (16,5)$, $2P = (20,20)$, $3P = (14,14)$, $4P = (19,20)$,
 $5P = (13,10)$, $6P = (7,3)$, $7P = (8,7)$, $8P = (12,17)$,
 $9P = (4,5)$

$m=9$ and $Q = 9 P$

REFERENCES



Site Map | Accessibility | Contact | Legal Notice | Search Site

enisa
European Network
and Information
Security Agency

Home About ENISA Our Activities Publications Press & Media Events Public Procurement Recruitment

you are here: home

Awareness Raising
CERT
Identity & Trust
Resilience
Risk Management
Stakeholder Relations

ENISA - Securing Europe's Information Society
Every day we experience the Information Society. Interconnected networks touch our everyday lives, at home and at work. It is therefore vital that computers, mobile phones, banking, and the Internet function, to support Europe's digital economy. That is why ENISA is working with Network and Information Security for the EU and the Member States.
See ENISA's tasks and activities

Future security 'compass course' for Europe; key message at FIRST, Miami
News item 18/06/2010
The Executive Director of ENISA, Dr Udo Helmbrecht, made a keynote presentation at the 22nd annual FIRST conference, taking place in Miami, USA, on 16 June. The key message of Dr Helmbrecht was that, with the Digital Agenda in our backpack, the future 'compass course' and reinforced Internet security tasks for Europe and ENISA are getting clearer every day. See [full story](#).

Security Summit: Cross border cooperation - a key point for security

press releases
 @ Key security actors, strategies, & good practices in Europe mapped
May 12, 2010
 @ Future EU Research: IT Security Priorities Identified - Always Online Availability in Focus
Apr 29, 2010
 @ Flying 2.0? Study of Internet of Things/RFID in air travel launched
Apr 13, 2010

NEWS
 @ Future security 'compass course' for Europe: key message at FIRST, Miami

upcoming events
 MeSSa 2010, 1st International Workshop on Measurability of Security in Software

ENISA

<http://www.enisa.europa.eu/>



Legal notice | About

Europa
Gateway to the European Union

EUROPA

About the EU

- Basic information
- Institutions and bodies
- 27 member countries
- History
- Work for the EU
- More about the EU

Your life in the EU

- Work and business
- Studying
- Healthcare
- Consumer rights
- Your EU rights
- More about life in the EU

Publications and documents

- Official documents
- Legislation and treaties
- Order or download a publication
- Statistics and opinion polls
- Tools and manuals
- More documentation

Policies and activities

- Policy areas
- Funding and grants
- Tenders and contracts
- More policies & activities

Take part!

- Have your say on policies
- Blogs
- Video - EU on YouTube
- Visit the EU institutions
- Prizes & Competitions
- More about taking part

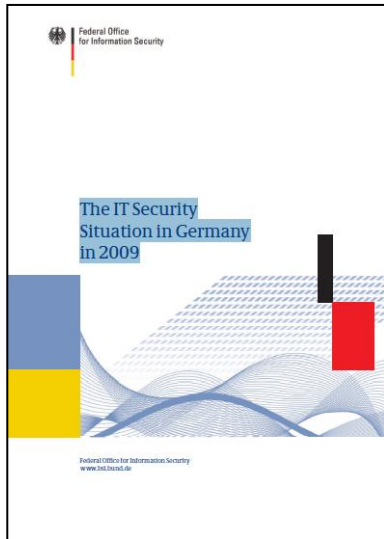
Media centre

- Press services
- Videos and photos
- Events
- RSS feeds and podcasts
- More media services

European Union

http://europa.eu/index_en.htm

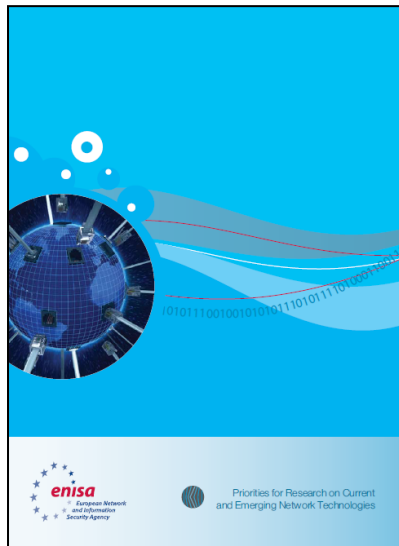




The IT Security Situation in Germany in 2009

BSI 2009

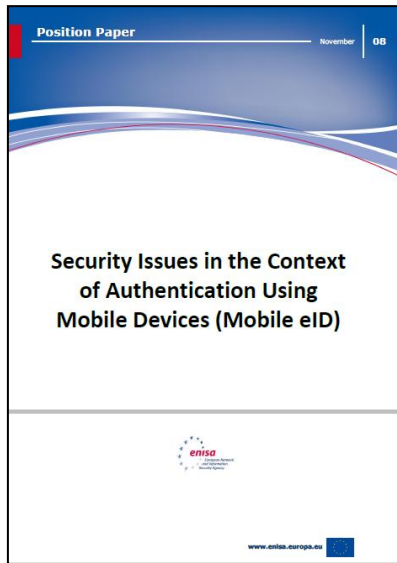
https://www.bsi.bund.de/cae/servlet/contentblob/517474/publicationFile/28002/bsi_lagebericht09_pdf.pdf



Priorities for Research on Current and Emerging Network Trends

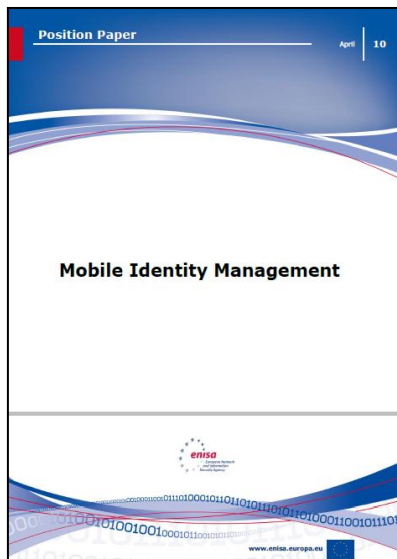
ENISA, 2010

<http://www.enisa.europa.eu/act/it/library/deliverables/procent>



Report on Mobile Authentication ENISA, 2008

<http://www.enisa.europa.eu/act/it/eid/mobile-eid>



Report on Mobile Identity Management ENISA, 2009

<http://www.enisa.europa.eu/act/it/eid/Mobile%20IDM>

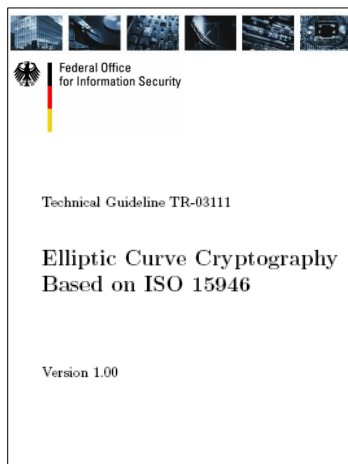


ECC Tutorial

Certicom, 2010

<http://www.certicom.com>

<http://www.certicom.com/index.php/10-introduction>



Baier, Kügler, Margraf

Technical Guideline ECC Based on ISO 15946TR-03111
BSI, Bonn, 2007

<http://www.bsi.de/literat/tr/tr03111/index.htm>

Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)

P.O. Box 1309

71001 Heraklion - Crete – Greece

<http://www.enisa.europa.eu>

