Trust and Security Challenges in Cyberspace

Defining an RTD Agenda for Europe

Report of the workshop held in Brussels on 7-8 December 2000

Final version February 2001

1 Introduction

On 7-8 December 2000, the European Commission (EC), Directorate General Information Society with support from the Joint Research Centre (JRC), held a workshop on the theme: "Trust and security challenges in Cyberspace".

The workshop aimed at stimulating an open and visionary discussion in order to:

- Explore emerging issues and challenges in the areas of cyberspace trust, security technologies and security processes;
- Formulate recommendations to provide input for the preparation of the 6th Framework Programme ("FP6").

Fourteen experts invited from industry and research organisations attended the workshop.

The workshop was structured around:

- A plenary session with presentations from the invited experts and subsequent discussions, and
- 3 parallel sessions aimed at refining issues pertaining respectively to the areas of *m-commerce*, *new types of networks* and *trust in virtual communities*.

This report provides a summary of the presentations and discussions in the plenary session and the three parallel sessions. The workshop agenda is attached as Annex 1. The list of workshop participants is attached as Annex 2.

2 Summary of the discussions

2.1 Issues raised in presentations

Information Society Technologies are becoming more and more pervasive in a wide range of socio-economic activities. We increasingly depend on complex information infrastructures that are becoming more open, are interdependent, and increasingly offer "intelligent" services on a personalised basis. An open Information Society creates new opportunities for value creation and knowledge sharing, thereby leading to possible conflicts with the traditional principles of privacy. It also opens up new vulnerabilities for its users in terms of malfunction, contentious activities and privacy invasion. Mobile technologies and m-commerce in particular will have far reaching implications for trust and security. These technologies involve the mobility of users of information and communications services (e.g. mobile phones, PDA's), the mobility of applications for personalised and location based services (e.g. downloadable code and content) and the mobility of the components in the communications networks (e.g. transport vehicles or even humans becoming themselves network nodes). Against that background, the human perception of "trust and security" is changing and user requirements need to embrace the new environment created by "networked" organisations transcending the traditional boundaries of nations, culture and jurisdictions and the traditional static concepts of structure and topology.

As noted above, there emerged from the presentations a widespread concern about the implications of new technological developments on privacy and confidentiality; while there was not agreement on what level of protection for privacy and confidentiality were appropriate, it was felt that technological

development risked pre-empting a collective judgement on this point by rendering certain options technically impossible.

2.2 Emerging research issues

The workshop discussions identified important trust and security challenges that would be pertinent for structuring research issues relevant for a publicly funded R&D programme.

The following structure for organising potential scenarios for R&D was proposed:

The security of the personal info-sphere, which covers the notion of securing personal info-assets and credentials and relates to the deployment of personal area networks composed of personal devices, including devices implanted in the human body. These devices can all be interconnected and individually or jointly may store and manage considerable amounts of information. Privacy aspects related to anonymity, pseudonymity, linkability and observability must be considered in the design phase of such networks.

The security of the virtual community, which covers aspects related to establishing and managing trust relations in virtual communities, concerning social as well as business relations. Within this context there is a need for flexible and configurable security policies that also cover different levels of authentication and authorisation of the actors in transactions whilst safeguarding anonymity requirements for certain categories of actors. Trusted infrastructures are needed to implement these policies. This challenge is getting even harder because of the growing intelligence, functionality and responsiveness being placed in the infrastructure, which itself is increasingly becoming dynamic.

The Security of the Infrastructure, which covers the notion of securing the essential IT infrastructure that underpins the economy and society of the European Union. Technological developments and the needs of law enforcement provide increased opportunities for surveillance in cyberspace. Better managing and strengthening our infrastructure would make it more efficient and resilient without the need for unnecessary surveillance. A societal debate that strikes an acceptable balance between surveillance and the rights of the individual should underpin that issue.

The above structure was instrumental in helping the workshop to identify a set of common research topics. In particular, the participants shared the view that any future developments would have to address the following areas:

Privacy is by far the most important security concern that should be considered in any R&D activity aiming to sustain and promote the development of large-scale networks and information infrastructures. The level of concern is growing because of:

- Weaknesses in research and technology developments in privacy so far, apparently mainly for socio-economic reasons. Despite the presence of privacy protection policies and laws, there is a lack of business drivers for technology and systems providers to invest in privacy;
- The extensive and unrestrained deployment of invasive and data producing/gathering/storing/processing technologies for personalisation of services, identity checking in transactions, traffic monitoring, location

observability which, not always lawfully and transparently, bring opportunities for profiling and tracking;

- The disappearing of traditional fixed terminals which are being replaced by ensembles of networked and communicating personal objects/devices (cellular, PDA, etc.);
- The increasing distribution of active functionality and intelligence capability to network components which become increasingly autonomous and powerful.

In this context, new **privacy preserving schemes** are required, possibly based on pseudonyms and capable of empowering the user to control anonymity and observability. Awareness-raising exercises should close the gap between stakeholders and policies.

While not wishing to pre-empt the societal debate mentioned above over the level of surveillance which is appropriate, research and development work is needed to ensure that the technology can deliver whatever level of privacy protection society agrees to be appropriate. It seems likely that this will involve significant elements of user choice, and in this context it is important to ensure the **usability and functionality** of the choice mechanisms concerned.

Privacy requirements on one side and the need for strong authentication on the other require new **authorisation schemes** adapted to different kinds of applications. Such schemes would be based on limited disclosure authentication models and be sufficiently flexible to cope with multiple authorisation requirements for components in different transaction scenarios.

To support user confidence and security, **trustworthy ("trusted") components** should become more easily available to users. Users should be given the possibility to choose (as appropriate) components which they trust and which they would use to store personal information and credentials so as to build trust relations with other entities and objects. However, the overall security model is changing rapidly and profoundly, and this means that the notion of "trusted component" is changing as well: from monolithic systems the drive is towards distributed systems and networked components.

Information **infrastructures** are critical for the functioning of society. They are vulnerable because of new types of threats and of complex interdependencies, both of which need to be better understood. Appropriate constituencies (e.g. CERTs or similar) should promote co-operation between stakeholders on incident handling and ensure its effectiveness towards end users and service providers.

Another aspect of confidence and trust is linked to the capability to **evaluate and assess** the security levels/features of components, systems, services, etc. Since the security of a system depends on the interworking and interoperability of different systems and processes, schemes for evaluation and assessment should support the same dynamics (in time and space) and lifecycle as the technologies they are assessing.

There is also a need for fundamental research, to improve techniques for assessing and verifying security properties, and to ensure that alternative approaches are available in the event of unexpected successes, for example in breaking factoring-based cryptography or in developing quantum computing.

3 Parallel sessions discussions

3.1 M-commerce

3.1.1 Context

The discussion group emphasised that there were differences between wired e-commerce and m-commerce, so that concepts, whether technological or legal, which are appropriate for wired commerce could not in all cases be taken over directly. Indeed it was not clear a priori what were the security, liability, and privacy issues involved in ensuring trust, still less how to answer them. For that reason it was felt to be important to study the requirements in this area. These requirements might vary according to the type of devices and technologies in use, although there would probably be a common core.

Questions of liability should be thought of as distinct from those of trust.

The essential concept needed for m-commerce is that of a valid transaction, rather than that of strong authentication of the person involved. Indeed, a role-based model is probably needed, involving different layers of authorisation.

It was agreed that, while commercial operators would doubtless spend substantial efforts in making e-commerce useable, it was not so clear that market forces could be trusted to ensure the usability of the mechanisms required to ensure trust. This suggested a role for public funding, both in developing that usability and ensuring its integration with the overall User Interface.

3.1.2 Challenges

The group identified the following areas to be considered for public R&D funding:

- Specification of requirements for security and privacy specific to mobility
- A "trusted component" (which could be a credentials device): -
  - How to develop and verify it
  - User Interface and usability of functionalities for security and privacy choices
  - Location awareness, and user empowerment to enable such a feature
  - Biometrics and privacy implications
- New types of evaluation profiles for mobile devices
- Development of new applications on trusted devices, e.g. use of credentials
- A rich delegation/authorisation infrastructure that would support several levels of certificates and support the management of different roles, credentials and privileges.

Of these, the last item was seen as a long term research item, while all the others were appropriate for work in both the short and the long term.

Another area considered by the group was the development of new technical approaches to protecting or securing IPR, but they came to no firm conclusion on this.

3.2 New types of networks

3.2.1 Context

There is an increasing interest in both security and trust at application level and, more generally, in the user perspective on security. This interest is not surprising given the high media visibility of these issues. However, it should not be forgotten that networks and communication/information infrastructures are necessary to provide adequate and provable levels of security to Information Society systems and services. Most of the "network security" interests are in the communications and applications and very little attention is normally paid to security issues of the architecture.

For applications, security challenges are thus getting much attention, but it is important also to consider the future evolution of the communication infrastructure. Furthermore we must not forget that the "personal sphere" is becoming more and more part of the infrastructure.

The communication infrastructure is becoming more and more "dynamic" and "mobile" with increasing levels of flexibility, self-configurability, intelligence, autonomy, etc. Of course, all these dynamic aspects of the infrastructure introduce new types of vulnerabilities, and securing dynamic and reactive networks is a major challenge.

A closely related challenge is that of realising secure and seamless interoperability among all these diverse and new networks.

New types of networks

The technical and business trend in communication networks is to integrate more "intelligence", "autonomy" and "functionality" into networks that become more and more responsive/active. These new networks can differ in physical extension and scale (local, personal, domestic, etc.), timeliness, configurability etc. In particular, connectivity and communications are more and more being realised by integrating an increasing number of diverse and heterogeneous networks and/or components of networks which give birth to new categories of networks, namely:

- Spontaneous/Self-Organising Networks**,** which are at the service level (or service related) – such as enabling people in a room to establish communication. These embrace the "plug and play" concept and generalise the "JINI" model.
- Ad Hoc Networks normally formed by an ensemble of network nodes without fixed and predefined infrastructures (topology). These are routing related and, normally, embrace the notion of communicating objects, piconets, Bluetooth, etc.
- Programmable Networks, which can be differentiated into
  - Open signalisation (where the issue is to define the API and provide service)
  - Active
    - Integrated (where the services are downloaded with the data)
    - Discrete (where the download is in the router and packets are executed there)
- Ambient Networks - which are context aware in the sense of "personalisation", localisation (in space and time) and contextualisation.

Bluetooth and other domestic ("domotic", i.e. for use in an automated home environment) protocols would bring computers everywhere as communicating objects. This will drive demand for security models deployable through space and time. In this respect, new patterns/behaviours of communications would emerge, including multi-party communications and virtual associations of any kinds (devices, components, entities, domains, hybrid, etc.) This in turn will require novel paradigms to manage and share secrets, such as new cryptography protocols to enable more parties to contribute to the same discussion (multilateral discussion)

Lastly, it is envisaged that all these developments would tend to resolve the current complexity by clearly distinguishing between the application layer and the transport layer.

Interoperability Issues

The emergence of new networks and services would bring about the problem of how to secure the interoperability of all these networks. The situation would also be made more complex by the fact that networks would themselves be the "access device/gateway" to wider "scope" networks, such as:

- Ad hoc/self-organising vs. Wide Area Networks. How to secure any trespassing between the 2 domains?
- different types of Wide Area Networks/Corporate Networks (Mobile telecomm nets, mobile Internet, fixed networks)
- different types of access networks

The secure interoperability issues would not only stem from the "structural" diversity of the networks but, even more importantly, from the evolutionary aspects related to the capability of dynamically re-configuring networks and service components.

On top of the huge difficulties in realising secure physical and logical interoperability between networks, the challenge will be made even harder by the ever increasing number of network service providers involved in the provision of network services (active nets, segmented value chain, etc.).

3.2.2 Challenges

The working group identified the following research topics for coping with new types of networks. They have been grouped under the titles "network security architecture definition" and "security challenges related to interoperability" (between heterogeneous networks).

Network security architecture definition

- Innovative network security models, including
  - ✓ new cryptographic paradigms and novel multi-party cryptographic protocols that can be easily adapted to different security policies and that can enhance the configuration of policies.
  - ✓ new approaches to defining security policies not necessarily based on access control, which may not be a viable solution in a mobile environment.
- New protocols (in particular for multicasting) for identification and authentication of nodes, services, routes, active code, etc. as well as for distribution of credentials

- Coping with new attack models such as distributed denial of service attacks
- Multi-party security association management
- Issues related to management of sources of trust and accountability in dynamic environments.
- Survivability of infrastructures, including assurance of unbounded and novel network types (e.g. "mobile" networks).
- Mechanisms for credentials management and privacy management in spontaneous nets. New certificate formats are needed that are more flexible and transcend the X509 certificate type of formats.

Security challenges related to interoperability

- Common security framework for both wireless and wireline architectures
  - ✓ Providing uniform access to security functions from a user's perspective.
  - ✓ Rethinking the access control function to subdomains, when dealing with increasing number of domains and increased heterogeneity and to the user (personal) sphere.
- The importance of security standards was underlined in order to avoid proliferation of interworking procedures.

3.3 Trust in virtual communities

3.3.1 Context

In an electronic environment of virtual communities, the human perception of trust relations is changing, concerning social as well as business relations. This environment is characterised by dynamic and networked organisations transcending the traditional boundaries of nations, culture and jurisdictions. Within this context, the following issues were discussed in this working group.

Authentication, privacy and anonymity

The different actors involved in a business transaction (e.g. customer, bank, merchant) or in a social transaction (e.g. person-to-person, person-to-group) will have different requirements for authentication. For instance strong authentication of the merchant may be needed during the contract negotiation, and strong authentication of the customer during payment. Also, one single actor (e.g. Citizen) can potentially be involved in different types of transactions depending on the circumstances.

Advances in electronic tracking techniques applied to transactions and to physical positions (e.g. cellular phones), combined with data mining techniques for profiling, put privacy at risk. While anonymity is considered a right, it is also acknowledged that absolute anonymity in all circumstances would be impractical. The real issue is to limit observability to the minimum and to empower the citizen to control the leakage and exploitation of personal data.

Therefore configurable authentication schemes will be needed that strike the right balance between managing risk in e-business relations on one side and anonymity/ controlled identity disclosure on the other.

Trusted platforms

The future personalised application environment will be characterised by massive software downloads. In open environments, servers will be moved

outside protected environments. As a result, the concept of security protection will change towards more responsibility lying with the end users of platforms and devices to configure their security requirements. Therefore trusted platforms with customisable security policies are needed, including means for trust enabling evaluations. An important issue for such a platform would be the secure operating system.

Protecting content, securing IPR

There was a divided view within the discussion group and in the subsequent plenary discussions on the appropriateness for public funding of this topic. Industry interests at stake are huge, industry will invest on its own and therefore one view is that it should not be the subject of a public EU research programme. The other view is that the EU lags behind US/Asia in protecting its content and therefore concerted action is needed. In particular, can the EU afford passiveness, considering its huge cultural heritage?

Critical infrastructures

The issue of critical infrastructures was considered important but only briefly discussed because of time constraints. It requires thorough further investigation, including issues and concepts within the policy domain. Information infrastructures increasingly underpin the correct functioning of critical infrastructures of society. Their availability and integrity must be preserved; they must be protected from attacks; and they should be given greater protection against being used as vehicles for cybercrime. Work is needed to study new types of vulnerabilities, and the dependability of information infrastructures against new threats, including the possibility of high-impact attacks such as large scale identity theft. This work should also take account of the complexities involved in protecting against certain types of threat.

3.3.2 Challenges

Within the above context, the working group identified the following research topics:

Authentication, privacy and anonymity

- Generic architectures for Privacy Enhancing Technologies
- Limited disclosure authentication models
  - Pseudonymity and identity management
  - Metrics on authentication and anonymity
- Independent assurance of "authentication"
- Flexibility of authentication
  - Multiple requirements for components in different transaction scenarios
  - Versatile authentication schemes which allow for various granularity of the authentication of subjects and objects in virtual communities

Customising trusted platforms

- Research on secure pervasive platforms including:
  - ✓ Virtual machines, domain separation, memory protection, trusted operating systems encompassing the principle of least privilege access control.

- ✓ Integrated automatic intrusion detection and intrusion response
- ✓ Suitability of these mechanisms for mobile systems (cellular, PDA, handhelds, etc.) as well as for server platforms.

- The usability of the security mechanisms for the end users must be addressed for transparency and acceptability reasons. Personal decision support capabilities focusing on guidelines for secure usage might enhance usability.

Trust and security assessment

- New approaches to trust assessment
  - ✓ Independent evaluation, the role of open source in evaluations.
  - ✓ How to overcome Common Criteria limitations in particular for systems and infrastructures increasingly becoming dynamic?
  - ✓ Schemes for private sector evaluation and best practice dissemination, including system security requirements modelling able to cope with complexity.
  - ✓ Public certification schemes and metrics for evaluation/auditing of trusted third parties.
  - ✓ Privacy auditing, including appropriate metrics for auditing
- Research on Fundamentals
  - ✓ New cryptography methods as alternatives to those based on factoring approaches (e.g. RSA) in order to limit dependence on one assumption

Infrastructure Dependability

- Methods for modelling existing and new vulnerabilities and threats, such as cybercrime and cyberterrorism.
- Incident handling/response: promoting co-operation and effectiveness towards end-users.

4 Annex 1: Agenda

Brussels, 7th-8th December 2000, European Commission - DG Information Society, Av. de Beaulieu 24, Room 0/22.

7 December 2000

10.30	Welcome - Thierry Van der Pyl, Head of Unit C4, DG Information Society
10.45	Overview of Workshop and Objectives – Rapporteur
11.30	Position Statements and Discussion – All
13.00	Lunch Break
14.00	Position Statements and Discussion – All
15.00	Open Discussion – All
16.00	Parallel Panels – All
	Panel 1: m-commerce
	Panel 2: new types of networks
	Panel 3: trust in virtual communities
18.30	Panels' Presentation and Discussion – Panel Convenors
19.00	Summary of the day – Chair
19.15	End of the first day

Agenda 8 December 2000

09.00	Opening
09.05	Panels' Presentation and Discussion – Continued
10.30	Summary - Chair and Rapporteur
11.00	Refinement of issues by the three panels – parallel panels
13.00	Lunch Break
14.00	Consolidation of requirements and challenges – All
15.00	Conclusions and Next Steps – All
15.30	Close meeting

5 Annex 2: Participants

D. Chadwick	Univ. Salford	D.W.Chadwick@iti.salford.ac.uk
Y. Deswarte	LAAS-CNRS	yves.deswarte@laas.fr
G. Horn	Siemens	Guenther.Horn@mchp.siemens.de
H. Leitold	TU Graz	Herbert.Leitold@iaik.at
V. Niemi	Nokia	Valtteri.niemi@nokia.com
T. Ostwald	CERT Pol-34	Tomasz.ostwald@man.poznan.pl
A. Pfitzmann	Univ. Dresden	pfitza@inf.tu-dresden.de
B. Preneel	Univ. Leuven	bart.preneel@esat.kuleuven.ac.be
M. Riguidel	Thomson-CSF	Michel.Riguidel@tcc.thomson-csf.com
M. Sievers	SmartTrust	marc.sievers@smarttrust.com
R. Temple	BT	robert.d.temple@BT.com
P. Van Dijken	Shell	Piet.P.vanDijken@IS.Shell.com
M. Waidner	IBM Corp.	wmi@zurich.ibm.com
R. Winsborrow	DERA	r.winsborrow@eris.dera.gov.uk
Thierry Van der Pyl	EC DG Information Society	Thierry.Vanderpyl@cec.eu.int
Andrea Servida	EC DG Information Society	Andrea.Servida@cec.eu.int
Roman Tirler	EC DG Information Society	Roman.Tirler@cec.eu.int
Marc Wilikens	EC Joint Research Centre	Marc.Wilikens@jrc.it
Neil Mitchison	EC Joint Research Centre	Neil.Mitchison@jrc.it

6 Annex 3: Position papers

6.1 David Chadwick, University of Salford

10-15 Year Vision Statement

In order for electronic commerce over the Internet to flourish, a relying party (RP) has to have confidence that the remote party is

a) who they say they are (i.e. authentication) and

b) they have permission to execute the given task (i.e. authorisation)

c) and are likely to follow through with the transaction (i.e. are trustworthy)

Note that physical transactions do not have these problems to the same extent, as the two people are together at the same time, and the goods and payment can be exchanged simultaneously.

I would expect the RP software to be fully automated and be able to receive a digitally signed message from anyone; be able to automatically retrieve the permissions for the person and validate the trustworthiness of their electronic credentials on a global basis. Furthermore the seller RP needs to either validate that the buyer has sufficient funds to pay for the transaction or is creditworthy, and finally gain assurance that the buyer will actually pay for the goods i.e. is trustworthy and does not have a history of receiving goods and never paying for them or revoking the transaction at a later date. Similarly the buyer RP needs to validate that the seller actually has the goods on offer and is able to deliver them before he parts with his money.

What is needed?

i) Global mechanisms for authentication and validating the trustworthiness of remote (unknown) trusted third parties (TTPs). The number of TTPs today is large and growing. Therefore unless consolidation occurs, RPs will need some mechanism for assessing the trustworthiness of remote (previously unknown) TTPs.

ii) Global mechanisms for authorisation and privilege management, that enable any RP to obtain the credentials of any sender. Privileges will have to be globally recognised and understood. Very little research has been done in this area to date.

iii) Global mechanisms for allocating "trustworthiness" metrics to buyers and sellers. I don't believe this last aspect has received much attention yet. The quality is rather elusive, but is a measure of the reliability of a person, based on his previous patterns of behaviour. Online auction houses have started to address this issue so that buyers and sellers gain a more trusted status the more successful transactions they participate in. This is perhaps the most difficult aspect to quantify, as personal privacy issues can be involved.

Assessing the Trustworthiness of Authentication

The current mechanism in browsers, is that they come pre-configured with 20 or more root CAs, that the user is told he trusts. This mechanism is completely flawed and open to abuse. Research needs to focus on better ways of doing this.

There are no easy to use or automated mechanisms available for trusted authentication at the moment, except in closed user groups. The closest we have is to inspect the published Certificate Policies (CPs) and Certification Practice Statements (CPSs) of TTPs. Public CAs such as Verisign and Viacode publish these on the Web. But it is beyond the scope of all except a few

security experts to understand the implications of these. Research should focus on ways of automating the process of calculating the trust in a remote CA, using its published CPS, so that a RP can easily assess whether a remote user is who they say they are. (Note. At Salford we have already built a pilot expert system that can do this, but significantly more work is needed in this area.)

However, even this may prove to be too difficult for many users to perform. Therefore we need standard mechanisms for the auditing of public CAs, and the publishing of the results. We already have standard ways of financially auditing companies, and publishing their annual financial results. We need a similar mechanism for CAs. Research should focus on defining standard auditing metrics, standard electronic ways of publishing this information on the Internet, and software tools that are easy enough for the average user or application developer to use, so that he/she/it can understand the results of the audit sufficiently enough for him/her/it to make their authentication trust decision. (Note. At Salford, we have already defined a provisional Audit Certificate – which is an X.509 standard attribute certificate, signed by the auditor – that is available for download from an LDAP directory. But this is just the tip of the iceberg. Not only does its contents need to be standardised, but also the way the elements are ranked in order to give a consistent trust score or trust quotient.)

Assessing the Trustworthiness of Authorisation

Large Internet e-commerce organisations may set up their own mechanisms for this. We already have examples of this in e-banking e.g. Scotiabank. In these cases the organisation will most likely be responsible for both the authentication and authorisation of their customers, and so trust issues will be handled by existing mechanisms. The organisation can therefore use its own internal databases to find out whether a remote user is trusted to perform a task or not. Only users within its own internal databases will be allowed access. This is not an area that should be considered for RTD projects, as it is essentially a closed user group.

Other e-commerce sites may delegate the role of authorisation to external trusted entities such as Visa or MasterCard. It is therefore essential to have standard protocols and data structures that allow a RP to contact any authorisation authority to determine if the remote user is authorised to perform a transaction or not. X.509 (2001) has made a start on this by defining attribute certificates and Privilege Management Infrastructures. The IETF PKIX group is further extending these standards. However, we have no real practical experience of using these at the moment. In truth, this subject area is about 5 years behind PKI research. Thus a major focus in the coming years should be in the development and use of PMIs. There is a lot of work to be done here, in defining standard data structures for PMI information, standard protocols to be used between the various entities, and standard APIs that will allow applications to be built from component parts. For example, when constructing secure e-commerce applications, we need a standard API so that an application can present digital tokens to the API, and get back the set of privileges that the remote user is entitled to. Standard data structures for privileges that can be used by different e-commerce applications are needed.

Assessing the Trustworthiness of the End Entities

We have all seen the cartoon "On the Internet no-one knows you're a dog". To counteract this, electronic strangers need some way of assessing the past performance of the remote entity and validating their trustworthiness. Are they likely to complete the transaction in the way promised? (On a more worrying note, we have already had incidences of paedophiles attracting young girls in

chat rooms and then arranging to meet them in person.) Very little research seems to have been done in this area, but we need to be able to allocate trust metrics to end entities, that are dynamically updated as a result of their past and current behaviour. The trust metrics will be context dependent, so that entities may have a whole raft of them, one for each type of transaction they participate in. Once a RP knows that the remote user is authentic, authorised and trustworthy, we have a solid basis on which e-commerce can flourish.

(Footnote. I am strongly against anonymous E-commerce as this is an open door for criminals and money launderers to spend their ill-gotten gains. I do not propose that we should make this easier on the Internet.)

6.2 Yves Deswarte, LAAS-CNRS

Facing good security, we need better privacy

The security of large network infrastructures has recently improved significantly and will improve in the next few years:

- European directive and national laws on digital signatures -> PKI
- IP-Sec -> Ipv6
- Deployment of Intrusion Detection Systems

… while in parallel the threats are also growing:

- DDOS (distributed denial of service)
- e-commerce fraud
- transnational e-criminality

… thus fuelling the need for more security:

- e.g., ingress traffic filtering by ISPs

… and all these security measures are undermining the citizens' privacy:

- it is more and more practical and easy to collect more and more information on innocent network users
- the European directive and the national laws on the protection of personal data are inefficient (they are founded on a voluntary basis, nearly impossible to enforce technically)

Research in the area of privacy is very weak:

- there is no economic pressure for privacy (but there is a strong pressure
- AGAINST privacy)
- historically, research in security has been funded by defence agencies, who are very interested in secrecy, but not in privacy; more recently, research has been funded by financial organisations (banks, e-commerce) who are more interested in identifying securely their clients than in protecting their privacy (except from their competitors).

So, research should be funded to improve privacy:

- e.g., promoting pseudonym certificates, anonymity relays, etc.
- developing transaction schemes which do not disclose more information than needed:

For example, a merchant does not need to know the real identity of a customer, he needs only to be sure that the money order is valid; the customer's bank does not need to know the identity of the merchant (and of course, the nature

of the purchased goods), only some reference of the merchant's bank account, etc.

Of course, such privacy-preserving schemes should be able to reveal to a judge the real identities in case of dispute, or on request by judicial authorities (to prevent money laundering, for instance).

6.3 Stefan Engel-Flechsig, Radicchio

SECURITY IN MOBILE COMMUNICATIONS – A POWERFUL CHANNEL FOR NEW SERVICES AND SECURITY

Great excitement surrounds the future of wireless communications – a market that, in a few short years, has evolved from a voice-centric industry to one that allows us to communicate in just about any way imaginable. Mobile communications is no longer only about voice, but a means to exchange text and data, access the Internet, conduct business and a whole lot more – all while on the move!

Already wireless e-commerce, or m-commerce, is threatening to overtake traditional e-commerce in Western Europe, with financial services the key commercial driver for the market.

Add into the equation the soaring mobile phone penetration figures across Europe – the Nordic region currently nudging the 70 per cent mark and UK, Germany, France and Spain not far behind – and you have a market ripe for an m-commerce explosion.

This continued strong growth bodes extremely well for the rapid development of a dense wide-based consumer market for mobile telephony and revenue-generating value-added services. The route to these services will be Internet-enabled mobile phones.

The emergence of mobile phones that link to the Internet will not only allow users to communicate and interact with billions of people around the world, but also give access to the wealth of information on the Internet – all using a device small enough to fit in a jacket pocket. But it won't end with simple communications – individuals and companies will soon demand more from their handsets and expect to conduct their business on the move.

However, the true commercial potential of m-commerce will not be realised until a standard security framework is agreed within the marketplace. The need for high-end security in mobile financial services is being met by PKI-based security systems that support mobile transactions, such as solutions for generating a digital signature in the SIM card of a mobile phone. They take advantage of an infrastructure that is already present: hundreds of millions of GSM phones - mobile smart cards plus mobile card reading devices - in use throughout Europe which can be used for m-commerce.

Mobile commerce in the financial area will require secure, legally binding transactions that use a mobile wireless communication device. In a nutshell, the industry has to exploit technological and regulatory opportunities to provide a necessary trigger for wireless e-commerce growth.

One organisation which is absolutely committed to making the most of the opportunity for mobile communications is Radicchio, a global body of more than 50 leading companies, handset-manufacturers, mobile operators, CA-software vendors, chipcard manufacturers, chip-producers and leading global financial service providers - committed to the development of secure electronic commerce, information access and information exchange using mobile and wireless communication based on Public Key Infrastructure.

Radicchio aims to promote the use of Public Key Infrastructure on wireless devices and networks, providing a showcase for the members to display their technology and expertise.

A PKI is a combination of hardware and software products, policies and procedures, which offers the security that is required to carry out e-commerce activity in order that users -- who may not know one another, or may be scattered over a wide geographical area, or both -- can communicate securely through a chain of trust. The basis of PKI are digital identifications known as digital certificates. These act like an electronic passport and bind the user's digital signature to his or her public key.

Radicchio will not be issuing specifications and standards, but will instead fuel the emerging wireless commerce market by acting as a focus group which provides education, training and marketing support. Radicchio is setting about achieving its mission of enabling a dynamic global market for secure wireless e-commerce through a combination of processes that include regulatory discussions at a high level, technical collaboration and strategic discussions with members:

- Raise industry and consumer awareness in PKI and secure transactions for wireless devices.
- Develop wireless PKI for secure transactions on wireless devices
- Drive and develop the wireless e-commerce market globally
- Lobby the regulatory and standards bodies to ensure laws and technology support the growth of the emerging market
- Provide a forum and showcase for PKI-based wireless e-commerce solutions.

Radicchio's overriding objective is to create an environment where wireless e-commerce can truly flourish. This will be achieved by maintaining a high profile across the industry, initiating collaboration and dialogue across all levels to promote new technologies and practical, workable strategies. A major component of the Radicchio initiative will be a fully integrated marketing communications campaign, collectively funded by Radicchio member subscriptions.

Radicchio is totally committed to the principle that the future of mobile communications lies in wireless e-commerce.

6.4 Alain Filée, Bull

Trust & Security: 2001-2006 major focus

1. Citizen privacy protection

- Identify risks and develop methods, technology and best practices to insure, for the day to day life, a level of anonymity equivalent as the one we may have today (when NOT using e-commerce, GSM, PC & Internet, e-voting,...);... balance this with the requirement of law enforcement activities against cybercriminality...
- Educate citizen on the risks of the e-society. Balance it with the benefits

2. Critical European Union infrastructure protection

- technological independence: develop security software and cryptographic hardware that are under the full (= R&D and sales) control of EU companies. Areas:
  - cryptographic resources
  - automated intrusion test & detection tools
  - high availability and automated resources reconfiguration/reallocation tools
  - e-disaster recovery methods, plan & facilities
  - end user (= peer to peer) security tools for encryption & signature
  - virus detection / protection
  - WYSIWYS: 'what you see is what you sign': trusted resources for electronic signature of an electronic document
- encourage these EU companies to develop products that are freely cross exchangeable (i.e. on a PC client: replace the smart card of supplier 1 by the smartcard of supplier 2 to be used with the security software of supplier 3 and on the server side: use the crypto hardware of supplier 4 as a replacement of the one of supplier 3.
- promote critical infrastructure protection trials using these trusted technologies
- educate deciders, politician,... on the risks of electronic intelligence. Promote best practice

3. Study and harmonisation of legal rules, laws, trust & security compliance requirements,....

6.5 Günther Horn, Corporate Technology, Siemens AG

This short position statement presents a personal view on discernible trends in future communications technologies and resulting security challenges. It does not make an attempt to be comprehensive or well balanced. The author admits to a bias towards mobile communications.

Much attention has been paid recently to the security for applications, in particular security for electronic commerce and mobile commerce. While these remain important areas of work with many open problems, the communications infrastructure and terminals will also undergo important changes creating new security challenges. This position statement will mainly dwell on the latter, and only briefly address the former.

Some major trends with security relevance relating to the communications infrastructure and terminals, which can already be seen today and are expected to influence the development in this field over the next ten years are:

– At the technical level:
– increasing heterogeneity;
– increasing mobility;
– seamless service provision across system boundaries;
– increased importance of real-time services in IP-based networks;
– proliferation of networked devices;
– spontaneity of networking;

– changing nature of the terminal.

At the commercial level:

– increasing segmentation of the value chain;
– increasing diversity of and interaction among service providers.

In the following, I try to explain these related trends and their security implications.

Increasing heterogeneity: to predict the convergence of telecommunications networks and the Internet has become commonplace. However, it has been slow to materialise. Current developments include the introduction of an IP-based multimedia domain in UMTS and the activities relating to micromobility concepts for the Internet, to a large extent driven by requirements originating from mobile telecommunications networks. Also, techniques designed for media distribution networks, such as DVB, may be used in a telecommunications or Internet environment. The future is expected to give users access to network services over a multitude of access networks, both fixed and mobile, IP-based or not. These access networks may be connected to an IP-based core network, or to various types of legacy networks. Many of these networks have their own security mechanisms already defined. The security challenge consists in providing the user with a uniform means to access these diverse networks and to ensure smooth interoperation and security association provisioning for the diverse subnets. Diverse types of terminals, ranging from PCs to Laptops, PDAs, and mobile phones or even smaller embedded devices with diverse capabilities to support security techniques will have to be taken into account. The types of network to be considered may range from the smart home to private or enterprise networks to public networks. Partial results in this area may be obtained within the next couple of years, but the security challenges are expected to persist for the envisaged time-frame.

Increasing Mobility: in several countries, the number of mobile phone users already exceeds that of both fixed phone users and Internet users. Users will increasingly expect to be able to access services independent of their location and while in movement. This means increased demand for the Internet going mobile, and for cellular networks supporting the provision of Internet services. A security architecture for the Mobile Internet ensuring global access and its security interworking with existing and emerging cellular systems is far from complete and will continue to remain an issue for the coming years.

Seamless service provision across system boundaries: a user will require seamless continuity of service provision while moving e.g. from a Wireless Corporate LAN to a cellular network. This results in requirements on the security interworking between systems, in addition to those resulting from heterogeneity. It is not clear today what types of systems would allow such security interworking, and how it should be accomplished.

Increased importance of real-time services in IP-based networks: it may not be obvious why the introduction of real-time services would present new security challenges. This may become clear from the above requirement of seamless service provision: real-time services pose severe performance constraints e.g. in cases of handover and therefore rule out certain security solutions which may be workable for non-real-time services. In addition, real-

time services in lossy environments, such as mobile, may require different security mechanism, e.g. for integrity provision.

Proliferation of networked devices: it is expected that systems embedded in appliances capable of communicating with each other and with the world at large will see a tremendous increase in numbers. Many of the applications of such networked devices will require security. The management of the required security parameters and algorithms will require new approaches.

Spontaneity of networking: this issue is related, but not identical to the previous one. The advent of short-range wireless techniques and ad-hoc networks will allow people and devices to form spontaneous, dynamically changing networks. These networks will require the ad-hoc set-up of security associations. In general, it may not be assumed that the entities forming these ad-hoc networks will be able to rely on a common security infrastructure, such as a global public key infrastructure, be it because it is not available to all parties involved or because the devices are not powerful enough to support the required technology. The management of these security associations presents a challenge whose proposed solutions are in its infancy.

Changing nature of the terminal: while the mobile terminal is, by many, considered a trustworthy personal device today, this may change due to the increased configurability of the terminal of the future unless appropriate precautions are taken. On the one hand, the download of software, both application SW and "native" code, e.g. to configure the radio properties of a SW defined radio, will significantly increase the vulnerability of the terminal to attacks such as Trojan horses or viruses. On the other hand, the trend from a monolithic piece of hardware on which the terminal is implemented towards a distributed terminal platform with dynamically changing components communicating using wireless techniques (e.g. personal or body networks) makes it increasingly difficult to tie terminal security to an identity representing a physical entity. These problems are expected to remain with us for the considered time frame even if partial results may be seen in the next few years.

Increasing segmentation of the value chain: A network operator today typically controls the access network as well as the core network, provides many network services implemented in switches and often also controls the provision of value added services in some form. It is expected that, in the future, the value chain will be increasingly decomposed in independent segments, with open interfaces between them. In each segment, there will be several players, which may interact in a dynamically changing way. This raises obvious questions of trust and mutual guarantees, as all parties involved require reasonable assurance regarding the protection of their resources.

Increasing diversity of and interaction among service providers: as a consequence of the previous item, the number of service providers interacting in dynamically changing relationships will increase. These relationships require the dynamical set-up of trust relationships and the establishment of mutual guarantees. Support from a public key infrastructure will be helpful, but striking the right balance between technical security measures and non-technical, e.g. legal arrangements, will be crucial in finding commercially acceptable solutions. Privacy aspects merit particular consideration in such a context as it may be increasingly difficult to control the flow of user related data.

Brief remarks on M-commerce: it is expected that mobile specific constraints will be eased, but will not go away. The establishment of a global PKI which is also workable for small mobile devices is crucial. Whether there will be one standard or several (PKIX, SPKI, X9.68, WAP) is not decided at present. A trustworthy device is essential for the user to securely conduct M-commerce

(but cf. what was said above). This device is likely to require hardware-based security tokens, which may be used with different types of communication terminals. Mobile agents offer a great potential in the context of E- and M-commerce, but open up additional security risks.

6.6 Valtteri Niemi, Nokia

The number of mobile phone subscribers world-wide is expected to reach 1 billion by 2002. A significant share of these users will be equipped with Mobile Internet-enabled terminals. This means that by 2003 Mobile Internet users will outnumber fixed-line Internet users. Several industry analyses predict that mobile e-commerce will constitute a multi-billion dollar business by 2005. With the mobile phone in pocket and constantly online via GPRS and 3G technologies, instant shopping, further enabled by payment services from the mobile phone, will be a full reality.

Mobile e-commerce is one of the key applications of the mobile information society simply because it offers excellent opportunities for all stakeholders, including consumers, operators, finance industry and service or content providers.

The market today is typical of an emergent one, encumbered with an abundance of approaches and concepts that may not interoperate. The lack of a coherent roadmap for the future may lead to market fragmentation and delay of the growth phase, as it is usually difficult to offer truly user-friendly, easy-to-use services in a fragmented environment. Consistence of user experience is a key element in fostering market takeoff.

The mobile phone is rapidly evolving into much more than a wireless telephone. It is transforming into a personal trusted device, with the ability to handle a wide variety of new services and applications such as banking, payments, ticketing and secure access -based operations.

The consistent user experience in mobile e-commerce comprises of the following parts:

- flexible service selection
- awareness of used service/brand
- awareness of security environment
- user verification
- awareness of digital signing
- access to digitally signed contracts
- access to delivered objects (receipts/tickets)

There are three environments for mobile e-commerce. The remote environment is defined as the virtual/mobile Internet world, characterised by typical WAP services over any PLMN, such as the GSM and TDMA networks. The local environment is defined as the physical world, where the end user can use the phone to access payment services in a store, ID services at work, etc., possibly using Bluetooth wireless technology as bearer. The personal environment is defined as one in which the end user can access fixed-line Internet content using the personal trusted device for identification, authentication and authorisation of transaction services, again using Bluetooth as bearer.

6.7 Tomasz Ostwald, MAN, Poznan, Poland

As our civilisation becomes more and more dependent on digitally processed information, the meaning of security significantly increases. With continual development of information technologies new possible applications are being created. Unfortunately, it also refers to exploiting new potential vulnerabilities. Obviously new security concepts and their practical implementations are also systematically introduced. Yet, at present it seems that research of practical protection methodologies is still a step behind the development of the new attack techniques.

Generally, the forthcoming challenges referring to issues of trust and security can be classified in reference to a general model of activity assuming incident prevention, actual protection methodologies and incident handling (if required).

Incidents prevention

The incident prevention has a critical meaning and is nearly connected with issues of trust and general security awareness. Both these elements are especially important in the context of e-commerce. A trust should be considered as mutual relation built on prior individual experiences or publicly known ones. Thus, it is a hard task to build a stable trust relation and this effort can be easily wasted for example through reputation damaging. As the trust relation refers not only to specific entities but also to definite technologies or even general concepts, the consequences of multiple incidents may be very harmful.

Actual protection

As it should be assumed that no information system can be considered completely secure, a need of security mechanisms of new kind becomes critical. At present, most of practical solutions offer only passive protection, which is connected with the requirement of establishing a settlement between security level of the system and its practical usefulness. The most important technological challenge for the security domain will be to develop active protection systems, self managing and self learning, capable not only of detecting an attempt of intrusion but also of preventing it from being successful and eventually undertake adequate countermeasure. It seems that such systems might be built for example upon a general concept of host-based Intrusion Detection Systems, obviously with the application of adequate distributed architecture and adaptation to open network environments. Such systems should also integrate both approaches to an analysis process i.e. misuse detection (of known attacks) and anomaly detection (of deviation from state defined/learned as normal). Achieving such a goal obviously requires significant research in the domain of machine learning, knowledge discovery and general artificial intelligence.

Incidents handling

The general activity of incidents handling requires solutions to some problems of both organisational and technological kind. There is still a need for unambiguous definition of constituencies, establishing adequate authorities and developing standardised operating procedures (including co-operation with other entities). Purely technological attacks aimed at the systems' integrity, confidentiality or availability will obviously evolve (escalation of the distributed attack methodologies and methods for various phases of attack metastasis is highly expected), however, quite new forms of attack to deal with should also be expected. They may for example be aimed against the entities' reputation, what can result in damaging the existing trust relations.

Security has become an essential part of every engineering process in the domain of IT. However, issues related to security are often referred to as additional components and not as a basis, as they should be. If the information system is to be effective, practically useful and secure at the same time, critical components of its structure must be distinguished and heavily protected. Some more methodological approaches to the continuous process of securing the information system with special emphasis on modelling information flow and creating acceptable security policy should also be applied. If a system is to be secured, it has to be effectively managed in the first place.

6.8 Andreas Pfitzmann, Matthias Schunter, TU Dresden

In this position paper, we outline the major technical obstacles for security. They are divided into short-term goals and activities (i.e., within the next 5 years) and long-term ones. We do not consider legal problems even though we are aware that legal liability and harmonisation of cross-bolder commerce are far from being solved.

Short term goals and activities within 5 years

The most challenging short-term goal is to bring existing security and privacy solutions into the large-scale mass market. Research results and prototypes for most technologies leading to a substantial increase of end-user security and privacy already exist. Since they are barely exploited by offering products, the major short-term goal is to increase the market demand for security and privacy-enhancing technologies. This will lead to an increased supply and, as a consequence, to increased security and privacy for the end user.

Possibilities to increase the market demand are:

- Increase user-awareness. This enables companies to advertise a security advantage of their products and services.
- Promote evaluation and rating of security and privacy enhancing technologies used by existing businesses.
- Develop user-interface tools for inexperienced users that enable the specification of their security and privacy goals and mechanisms in an intuitive and straightforward way while illustrating security problems resulting from the chosen set of goals and mechanisms.

The most important building block that does not exist as a prototype is a solution for managing pseudonyms and the authorisations associated with them. The goal of pseudonym management (called identity management in the literature) is to go one step beyond public-key infrastructures (PKI) by allowing the following additional features:

- The participants in a transaction are enabled to stay anonymous by using pseudonyms.
- The participants are nevertheless able to show certain authorisations. Examples for such authorisations are memberships, age, or the fact that a court of law can determine who is the holder of this pseudonym.

Besides this activity, one is required to prevent bad things from happening. In particular the widely held misbelief that tamper-proof technology exists and that technologies such as tamper-resistant smartcards are the solution to most problems. In fact, the opposite is true, cf. Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules; Computer 30/2 (1997) 61-68. Since such technology can hardly be evaluated by end-users or their trusted experts, it opens the door for Trojan horses that can easily be used for privacy invasions and industrial

espionage. This is even more so since most hardware is manufactured outside the EU.

Long term goals and activities within 10-15 years

In the long run, the major challenge is the privacy-protecting integration of the various security and privacy enhancing technologies. We call this pervasive security and privacy. This can be subdivided into three major research areas that again need to be broken down into short-term objectives and research activities.

Secure Computing Platform

Current computer systems are inherently insecure. This includes secure hardware as well as secures operating systems research and development.

Pervasive Unobservability

In the long run, pseudonymity alone as described above is not sufficient. The reason is that long-term use of pseudonyms again enables profiling and thus enables de-anonymisation. Therefore, the level of unobservability needs to be improved considerably.

Technical means to achieve this are communication networks without user observability (e.g., MIXes), untraceable payment systems, as well as corresponding unlinkable authorisation schemes (e.g., generalised cryptographic credentials).

Multilateral Security Services

If two players do not trust each other while a certain amount of trust is required to achieve the desired goals, it is sometimes useful to introduce additional so-called trusted third parties.

These parties act as a trusted intermediary that is partially trusted by both players and provides services such as notarisation of transactions, fair exchange, or general secure atomic transactions.

6.9 Reinhard Posch, Applied Information Processing, Graz University of Technology, Austria

Introduction

Neither e-Commerce nor e-Government applications can be reliably build upon existing systems of trust. This is best shown by the various studies both by the Commission and by commercial companies like VISA. As a consequence, initiatives towards trust enabling technologies have been established such as the information security aspects of eEurope, expected to even be enhanced by the Council by advanced information society security (ISS) aspects.

The basic issue is that trust and security is still not a deciding factor for success of a hardware or software vendor. Unless this situation changes dramatically, COTS products will not be secure enough to form an environment for the new economy. As shown in Annex I in a simple example, manufacturers just do not afford security because it does not pay yet. This is basically because the lack of awareness at the users.

The situation becomes even more complicate when situations are exploited where users get strongly pushed into the use of electronic communications media, as they tend to be much more suspicious in this case.

The general lack of trust basically results from two facts:

- Security is not visible and only becomes evident as there is a security problem. It is therefore quite complicated to build consciousness at the

users and also very complicated to build business cases for end user products.

- Security and trust is focussing single elements rather than general systems. Internet and download of software is just one very evident example. There is no holistic view in the general case as Internet and communications technology are often viewed more or less like a toy by the broad public.

It seems obvious that measures have to be taken in the area of trust and security that primarily focus on the end user and its awareness. This is the basis that can be used to build securer systems.

As studies show, security enhancement and a higher level of trust is important to cope with the growth of online applications. This position paper expresses a train of thought to point out issues that strive for being addressed on Community level in a co-ordinated manner. In particular, aspects are raised that ask for priority treatment in the ISS research community in order to achieve leverage effects in its combination with e-Commerce and e-Government initiatives.

Trust needs a co-ordinated effort

I. The dilemma with products

At present there seem to be three different approaches to software-based systems.

A) The usage of software available as COTS products.

B) The exploitation of open source.

C) Special purpose software designed for specific applications.

While C) is not a valid approach for broad applications it should preferably not even be deployed by public administration: Such strategy has proven to be very expensive in the past.

As for research and development there results the need of:

A) Building awareness so that security becomes a commercial issue for COTS products and that manufacturers adopt.

B) Conduct research as how evaluation of COTS products to security standards could work.

C) Focus on the security of handhelds, mobile phones and other non-PC devices.

These items have turned crucial in the area of home PCs at the moment, but will soon also concern handhelds and mobile phones. It has to be assumed that these devices—as they have already been made openly programmable—will suffer from security issues. This is expected to happen to a much greater extent than for PCs at the moment, as the time to market is limiting possible security efforts and since the basic operating systems in question are much less structured and the hardware is in many cases not able to deliver adequate protection of applications.

II. IT security is not in the product development cycle

Research is needed to find ways to integrate IT security and responsibility on IT security into the various product development cycles without causing a delay that will impair the competitiveness. Similarly, efforts are needed that allows building trust which is based on evaluation that is independent from manufacturers. This shall break up the vicious cycle where to compete in

minimum security and maximum marketing of security, as long as all effort and quality is invisible to the laymen.

III. Trust bases are needed

Research would be needed to establish trust bases where trust and security can be achieved without the user being technically educated. Such trust bases have to be developed in a way to be available to the open public on a non-regulatory basis. One field where such trust base is more than urgently needed is the download of executables and the security configurations.

Systems are delivered in a way that insecure download is almost inevitable to run those systems. It is an especially big danger that even organised crime will abuse this situation. Such trust bases will have to be included into the usage cycles of various products. It is not only the feasibility of such trust bases which should be part of the research conducted but the methods that allow wide coverage. This should include product and policies of usage that should be deployed as a result of such activity.

IV. Special mechanisms needed in the broadcast/multicast oriented areas

Broadcast data and information as well as data communication that is using broadcast media is especially endangered by fraud and abuse. Whereas methods and mechanisms are well in place in the field of point-to-point communication where communicating partners are mutually identified, research is still needed in the area where information is communicated in a more open system and still needs various aspects of security to be ready for commercial use.

V. Completing application security

At present security is readily available at some elements. However, there are very few applications where security is a general design principle. Standard tools and APIs are needed that integrate security into applications. We have to move towards provable functionality and security. This needs research in altering and completing the various design tools. Design principles have to be developed that allow trust as they induce inherent security.

VI. Security awareness

Security awareness programs are needed at many places. One very crucial example is the use of third party software that is delivered via the Internet. In this context infrastructures are needed for trusted executables. Such infrastructure must allow trustworthy systems to be installed and configured by the average end user at a level of comfort seen with present insecure systems. Such trusted base must be independent from the manufacturer of the software itself and must exhibit the level of trust.

VII. Proactive precaution and responsive elements

Awareness creating elements are to be complemented by trust bases that enable rapid spreading of ISS achievements or recognition of upcoming threats to the end users. Research is needed of how to co-ordinate proactive precaution and responsive organisational elements such as critical infrastructure protection centres or emergency response teams with the end user elements which are public administrations, companies or citizens increasingly being dependent on IT. An example where recognition of serious

threats by well established organisational elements could not prevent the threat to cause damage a few months later is given in the Annex.

VIII. Security policies and security education

With e-Commerce and e-Government it is inevitable that appropriate policies be followed even with private use. This not only calls for the development of such policies and the monitoring of their acceptance by the user but also needs such effort to close the language gap. In this context formalisation of policies could be one element that is researched.

Annex I: Microsoft OUTLOOK exhibits negligent treatment of signed mails

At least since Outlook 98 and still with the present version and the service release 1 Microsoft OUTLOOK shows corrupt mails as properly signed and displays no warning. In the preview pane this product even shows the icon of a correctly signed mail as seen below in the screen shot.

This malfunctioning is despite of the situation that Microsoft was properly informed of that fact. There is no security patch or any other method available to face this problem, if this product is deployed with electronic signatures.

Such behaviour shows drastically that industry is not prepared to take security and trust on board in a way that businesses and governments can build their applications safely upon.

Emergency response and infrastructure protection need proactive response

Organisational initiatives such as computer emergency response teams or infrastructure protection centres, although important, require additional efforts to enable rapid spreading of results, preferably as automatic proactive models instead of responsive models. The crucial period between issue recognition and efficient response needs to be reduced.

As one prominent example where spreading of information seems to have not been sufficiently efficient are the warnings issued by the US national infrastructure protection center end of 1999 (raised at an ACSAC critical infrastructure protection in December 1999, issued as a warning on 30th December 1999) that distributed denial of service (DDoS) attacks tools being increasingly installed throughout the Internet. The recognition of the threat did not prevent a serious DDoS hit against various sites two months later in February 2000.

6.10 Bart Preneel, Katholieke Universiteit Leuven, Belgium

During the last two decades, substantial progress has been made in the development of security technology. We know how to evaluate systems, how to design security protocols, how to design cryptographic algorithms and how to implement them in a secure way. Nevertheless, it is fair to say that the security of many systems leaves much to be desired. The situation is probably the best in the financial sector, where this technology has been implemented first, and where techniques for risk analysis are well understood; the main problem in this environment is probably the existence of many legacy systems and the difficulty to keep pace with the fast developments. In the telecommunications sector, the GSM and UMTS networks are good examples as well, as these networks have at least been designed with security in mind. For the Internet technology, the situation is much worse, and in spite of recent progress, we seem to be still quite far from a global deployment of a secure network (IPSEC, Secure DNS,…).

The main source of concern is still the insecurity of the end systems, and more specifically the PCs. This is in part because they were not designed with security in mind, and in part because of their complexity and their fast evolution. As a consequence, even security experts have great difficulties in setting up a secure configuration with the most popular operating systems and browsers, and keeping up to date with the security developments is very time-consuming. We even accept for a fact that we exchange documents in a format that is prone to macro-viruses; and while security experts do understand the limitations of file scanning, they keep sending each other (accidentally) old and new viruses in this way.

The solution for this problem, as we all recognise, is to include a subsystem that is smaller, simpler and more stable, and to provide the security based on this subsystem. Current examples include smart cards and the trusted module proposed by the TCPA (http://www.trustedpc.org). The problems which we do not yet fully understand include:

- which functionality needs to be build into this subsystem; and
- how to perform a secure integration between the subsystem and the insecure larger system (e.g., how do we know that what is displayed on the screen is indeed that what is signed in this module).

Another solution might be to split systems by functionality.

The second problem, I want to bring forward has received quite some attention. However, as Information & Communication Technologies become more and more pervasive, the problem of protection of our privacy becomes more and more difficult. I strongly believe that it is not possible to achieve such privacy through legislation only: new technologies need to be developed that are transparent and user friendly. It is also clear that the cost model is a substantial problem in this area: on the one hand, the user is not willing to pay for his privacy, or to perform too much extra effort for it (see for example Zero Knowledge Systems, http://www.zks.net/), and on the other hand the service providers have too large an interest in collecting personal data (this data is important to provide intelligent services, it is valuable, and this data typically makes it easier to secure the system).

Finally I believe that substantial effort should go to basic research in the area of information security (that is, research which has market potential, but for the next 5-10 years rather than for the next 3 years), and to training of young researchers. One of the fundamental problems in this area is lack of expertise available, both in industry and in academia.

6.11 Michel Riguidel, Thomson-CSF Communications

Creating a new security for tomorrow's communication networks and information systems.

Abstract: (from Thomson-CSF Communications, Annales des Télécommunications)

In this article, the author covers his contribution to security in the security paper forming part of the report prepared by the "Internet of the Future" group, and his conference presentations at the RNRT Workshop on February 4, 2000, at Brest (France) and at the OFTA seminar on Mai 9, 2000 in Paris. A French version [13] of these presentations was published in Mai 2000 by the Observatoire Français des Techniques Avancées (OFTA, 5, rue Descartes - 75 005 Paris, ofta@wanadoo.fr), Arago Volume 23 - Logiciel et Réseaux de communication, led by Michel Diaz, Directeur de Recherche at CNRS, Laas-CNRS.

The article provides a global overview of modern security issues in the future communication networks. It presents a prospective viewpoint of Internet and mobile security, and gives many starting points to research on. The author describes the limitations of current communication security in the rising multimedia communication age, the need for more complex/subtle security mechanisms and policies. This article starts with a review of the new threats and vulnerabilities created by the emergence of digital technology, multimedia, mobility, heterogeneity and the characteristic, openness and interconnectability of systems. Emphasis is made on the distinction between the content of the users' information and the content of the systems (container), meaning the basic network hardware and software infrastructure. With the trend toward configurable, mobile infrastructures, threats arising from this dynamism are emerging. The solution to these vulnerabilities lies in designing new intermediation services to manage the interfaces between telecom operators, users and service providers, offering security protocols yet to be invented. Finally, the author gives an overview of possible future developments and research areas that need to be explored to provide security in the future communication networks. This includes (i) Specification of policies compatible with the Content and the Container, (ii) Set up of a context-oriented, plural, configurable policy, (iii) Design of new encryption protocols, (iv) Placing cryptology and steganography in perspective and (v) Introducing security in an open world.

Full article available from the author: michel.riguidel@tcc.thomson-csf.com

6.12 Robert Temple, BT Technology, UK

Future Trust and Security Research Topics for EU Funding

Secure Storage of Private Keys

2 factor authentication is fine provided the "something you have" doesn't rely on the user to remove it for part of the security – are there new techniques using biometrics to get round this? How do we measure their effectiveness in a commonly understood way?

Inter-operability

This continues to be an issue. Within the m-commerce field you have a multiplicity of protocols (e.g. Proprietary Sonera, WAP, ETSI, and Raddicchio). Would further research help?

Psychology

We know users are worried about security – we also know that users choose poor passwords. Some industry sectors are convinced security is important –

others are less so. Research could help to understand the user mentalities across a number of scenarios.

Developing consistent definitions of vulnerabilities and threats

In order to define and compare any aspect of dependability there is a requirement for a consistent language and methodology. Despite some work, more is needed in order to help establish a common framework for such definitions.

Assessment Methodologies

We have failed to translate ITSEC/CC into the mainstream. Nevertheless trust and confidence in products and systems has never been more important. http://www.s2ml.org/ is an example of vendor-led research in this area. Research could validate this or point out extensions such that it is appropriate for the assessment of consumer products. For networks, dependability assessment is a research area where the Rainbow books are past their sell by date! What comes next?

Doing it for Real

The EU has done a great deal to move forwards research in this area – however, large parts of the Commission still work on a paper and fax mentality … some money should be allocated to further trial projects which actually use PKI to securely automate more of the Commission's work.

Not Just Europe!

We need to establish a common research agenda with North America and Asia Pacific.

6.13 Piet van Dijken, Shell Group, The Netherlands

Introduction

Information security concerns - also coined as "cyber threats" - continue to climb our agenda under the label "critical infrastructure assurance". The Y2K experience plus a few recent high profile incidents (e.g. I LOVE YOU virus) taught us lessons on the vulnerability of societies for new classes of risk, related to IT infrastructure. Low probability – high impact threat scenario's ("information warfare") have set the stage for numerous shared initiatives, addressing these risks. Partnerships between governments and "critical" sectors like energy, telecommunications, financial services and transportation are in different stages of delivery of measures, ranging from improved alert and warning to shared sponsorship of R&D.

Steps taken so far

Over the past two years substantial progress has been made in Shell Group of companies in addressing the security risks associated with the supply of IT services, by the introduction Trust Domain (BS 7799 based) scheme. The scheme mandates minimum-security standards for the Group infrastructure, and introduced an internal certification scheme as the basis of the compliance management process.

An independent (KPMG) assessment rated the scheme as state of the art in security management practices. It stated that it was advanced but achievable and that the scheme offers the required flexibility in usage of IT, while maintaining 'control'. In a brief industry comparison it noted that financial institutions and some government agencies aim higher and Shell was not best in class on technical security, but overall better managed and at a consistent

minimum level throughout the organisation. It concluded that the implementation of the Trust Domain standards has resulted in an impressive, worldwide focus on security issues.

Group Risk and Internal Control Policy

The Group Risk Framework is now being used to build on our success with the Trust Domain by tackling the other various components building up from infrastructure, in particular applications, and e-business security. A program of work (as detailed below) has been identified in response to the current framework assessment. Additionally, a process is being established to manage the framework.

It is considered important that the risk framework should, be kept simple with thin management, build on or link to existing initiatives e.g. Trust Domain/e-architecture and use existing standards and guidelines. It needs to be flexible to cater for all risk responses i.e. from a very light touch to a certification scheme. It has to cater for the setting of targets and assurance levels for global responses while allowing individual Operating Units to assess local risk when appropriate.

The framework will address opportunities as well as protecting existing IT services. "Business Base Rules" will be established to allow the IT Steering Group (Group CIO chairing) to set direction and define the environment in which risks are assessed. OU's will be provided with a clear definition of objectives, requirements, implementation targets and the emphasis to be placed on assurance mechanisms.

Risks are not static and a central process must be established for identifying and assessing their impact. This requires monitoring trends, continuous liaison with governments, close monitoring of the response by societies and industry. The relevance to Group IT strategies and objectives will be assessed and the benchmarking of responses to those of comparable industries will be provided.

OU's will be provided with "Key Questions" to ask themselves. These will be supported by detailed self-assessment questionnaires for each area of risk and will point to relevant standards and guidelines. The level of assurance required from OU's will vary depending upon the severity of the risk and will range from self–assessment, audit/formal security review and certification.

An appraisal process will be implemented to ensure that the framework is functioning. This will include a Group "Health Check" and regular penetration tests.

Programme for 2001

A comprehensive programme of work is being established for 2001 based on the current risk and response assessment:

- Implementing a management process for the Risk Response framework.
- Progressing a plan of action to meet the requirements of the European directive on privacy.
- Implementation of a study into the latest anti virus protection procedures.
- The development of an "Application Controls Framework"
- The development of a "security framework for e-business"
- The implementation of an enhancement programme for the Trust Domain scheme. This will include developing a process for on-boarding new businesses, reviewing technical standards, introducing secure cells to protect sensitive systems, and developing recommendations for compliance monitoring tools and intrusion detection.

7 Annex 4: Presentations

Facing good security, we need better privacy

Yves Deswarte

LAAS-CNRS, France

SRI International

Network security is improving

- Laws on digital signatures -> PKIs
- IP-Sec -> IPv6
- Deployment of Intrusion Detection Systems

… but threats are growing

- DDoS (distributed denial of services)
- e-commerce fraud
- Transnational e-criminality

…thus the need for more security

- e.g., ingress traffic filtering by ISPs
- more audits, more records, …

… which undermines privacy

- It is more and more practical and easy to collect private information
- Laws on the protection of personal data are inefficient

In privacy area, research is weak

- There is no economic pressure for privacy
- Historically,research on security has been funded by defence agencies, and later by financial organisations

Research should be funded

- Pseudonym certificates, anonymity relays, …
- Development of privacy-preserving schemes

Example

- A merchant does not need to know the real identity of a customer, only the validity of the money order
- The customer 's bank does not need to know the identity of the merchant, only the reference of his bank account
- Etc.

… of course

- Real identities would be disclosed to a judge in case of dispute, or on request by judicial authorities (to prevent money laundering, for instance)

Workshop Brussels, 7-8 December 2000
„Trust and Security Challenges in Cyberspace“

Position Paper - Overview

Herbert Leitold
Reinhard Posch

IAIK, Graz University of Technology

A-SIT, Secure Information Technology Center - Austria

Workshop Brussels, 7-8 December 2000
„Trust and Security Challenges in Cyberspace“

Contents

Basic Issues

IT security is not visible in many cases

- *Only becomes evident as there is a security problem*

Current focus is on single elements

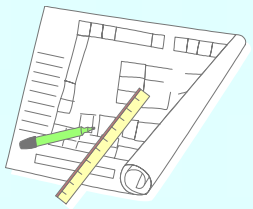
- *Global communication is omnipresent*
- *Holistic view is required rather than targeting single elements*

trust and security challenges in cyberspace

@iaik.at, @a-sit.at

Workshop Brussels, 7-8 December 2000
„Trust and Security Challenges in Cyberspace“

Specific Challenges



- Train of thought
  - products dilemma
  - development cycle
  - trust bases
  - broadcast/multicast
  - application security
  - security awareness
  - responsiveness
  - policies

I products dilemma

Research need for

- *awareness creation that security becomes a commercial issue for COTS products*
- *how evaluation of COTS products to security standards may work*
- *specific focus on handhelds (cell phones, PDAs, etc.)*

trust and security challenges in cyberspace

@iaik.at, @a-sit.at

II development cycle

Ways to include IT security into the various product development cycles

- *manufacturer independent evaluation*
- *not impairing competitiveness by causing additional delays*
- *break up vicious cycle of minimal introduction and maximum marketing of security that is invisible to the layman*

trust and security challenges in cyberspace

@iaik.at, @a-sit.at

III trust bases

Achieving trust without need of the user being technically educated

- *e.g. systems in many cases inevitably require insecure downloads in order to run the system*
- *research on feasibility of trust bases that allow a wide coverage*

IV broadcasts/multicasts

Mechanisms for point-to-point communication are well in place

- *e.g. mutually identified users*

Broadcast and multicast scenarios still require research, as especially endangered by fraud and abuse

V application security

Security is readily available at some elements

- *still security is not yet a general design principle*
- *requires standard tools and APIs*
- *provable functionality and security*
- *design principles that induce inherent security need to be developed*

VI security awareness

Security awareness programs needed at many places

- *e.g. Internet downloads*
- *Infrastructure to enable trustworthy downloads as convenient to the user as current insecure executables*
- *requires appropriate trust bases*

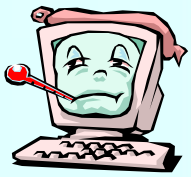
VII responsiveness

IT security is a dynamic field

- *vulnerabilities and exploits arise*

CERTS and NIPCs do a good job, but

- *research towards trust and proactive responsiveness seems appropriate*



VIII policies & education

With e-commerce and e-government definition of appropriate policies seem inevitable

- *formalisation of policies*
- *monitoring of acceptance*
- *accompanying user education and awareness creation*

Conclusions

Lots to be done ...

... let's start

trust and security challenges in cyberspace

IAIK

@iaik.at, @a-sit.at

Trust and Challenges in Cyberspace: a Few Observations

Prof. Bart Preneel
Katholieke Universiteit Leuven, Belgium

Bart.Preneel@esat.kuleuven.ac.be
www.esat.kuleuven.ac.be/~preneel
bart@abtcrypto.com,
www.abtcrypto.com

Security: what we have created

- Cryptographic algorithms
  - DES, AES, RSA, EC-DSA, SHA-1, RIPEMD-160
- Cryptographic protocols
  - GSM, 3GPP
  - EMV, CEPS
  - SSL/TLS, IPSEC, S/MIME, SET
- Evaluation criteria
- Electronic signature directive

But…

- do we use electronic signatures?
- do we use (qualified) electronic signatures?
- do I really trust my browser and the certificates in it?
- would it make a (substantial) difference if the browser was evaluated?

But…

- GSM phones can be eavesdropped
- my credit card has no smartcard yet
- how can I remember 2 dozen passwords?

- is RSA secure?
- is RSA with PKCS#1 secure?
- is RSA with PKCS#1 v2.0 secure?

And the end systems

- Do I know what I sign on my PC?
- Can I control and understand the software that runs on my PC?
- Am I better off with an O/S which has Kerberos & SSO, PKI, ….?
- Viruses: do we suffer less from them than 10 years ago?
- Back Orifice, mobile code,…
- Will my WAP++ phone be more secure?

End systems

- security engineering is difficult
- complexity and security don't really match

- two complementary approaches
  - detect security breaches, and react
  - trusted submodule

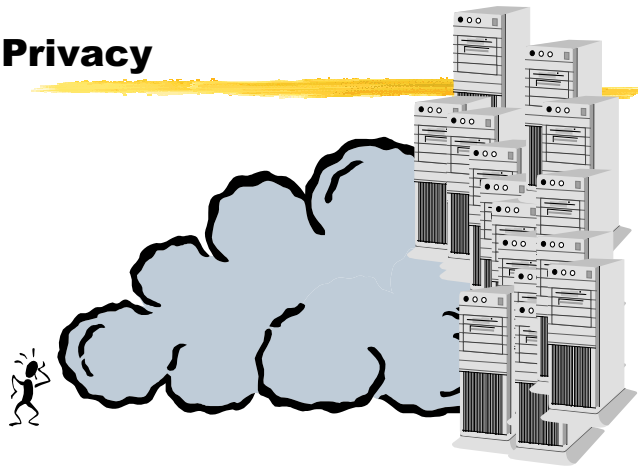
- both can bring risks for privacy

Trusted subsystem

- smart card
- TCPA module (www.trustedpc.org)

- how to securely build such systems?
- how to integrate them?
- how to update them?
- how to prevent that they give away our privacy?

Privacy



Privacy

- hard to achieve from network: multiple layers
- hard to manage for user
- often economically uninteresting
- differs between cultures
- risk of biometrics, intrusion detection
- when is it too late?
- can we build a secure voting scheme over the Internet using the current technology?

RSA: security (1)

- based on the fact that it is hard to factor the product of 2 large primes
- more precisely, the assumption behind RSA is that it is hard to extract random modular roots
  - there is an indication that breaking low-exponent RSA is **NOT** equivalent to factoring

RSA: security (2)

- several attacks on RSA encryption or RSA signatures are not based on factoring
  - low exponent, repeated message
  - attack on PKCS #1 v1.0
  - attack on ISO 9796-1 (withdrawn) and ISO 9796-2
  - even OAEP may have problems [Shoup00]

Is factoring hard?

YES !

- try to factor 2419
- Gauss could not factor 12-digit numbers
- R. Guy (1976): "I shall be surprised if anyone regularly factors numbers of size 10^{80} without special form during the present century"
- R.L. Rivest (1977): "factoring a 126-digit number would require at least 40 quadrillion years using the best factoring algorithm known,..." ($40 \cdot 10^{15}$ years)

How hard is factoring?

- making predictions beyond 1024 bits or beyond 15 years is very difficult
  - *"We do not believe that any public key size specified today should be used to protect something whose lifetime is more than 20 years" R.D. Silverman, RSA Laboratories*
- manage risk: approach should be application dependent

Is factoring really hard?

- what about a new algorithm that can factor 4000-bit numbers in 1 day?
- what about quantum computers?
- it better be hard, because soon our digital economy will rely for a large part on it

Other problems

- discrete log in Z_p: same difficulty
- discrete log in finite field over an elliptic curve: this may be harder
- need for new public-key systems
  - based on multivariate polynomial equations: FLASH, SFLASH, QUARTZ
  - based on ……..

Need for

- fundamental research in information security (research network?)
- training of young researchers (Summer Schools, grants)
- some impact on computer science curricula (?)
- privacy impact report?

RADICCHIO: Unleashing the potential of wireless e-commerce

Marc Sievers, SmartTrust
Head of the Radicchio Legal and Regulatory Working Group
EU - ISTP Workshop
Brussels 7./8.12.2000

RADICCHIO'S MISSION...

- To be the industry voice on the opportunities in secure wireless e-commerce
- To promote trusted Public-Key-Infrastructure (PKI) with personal handheld devices and wireless networks

RADICCHIO'S VISION

- Over 6.4 billion USD e-commerce sales in 2001*
- Over 337 million mobile phones in 2001**
- Over 600 million (75%) wireless terminals with the ability to use digital signatures on PKI in 2004**
- PKI triggers wireless e-commerce growth giving the ability to perform secure electronic transactions any time, in any location

Source: * Forrester Research; ** Industry estimates

SECURITY & MOBILE DEVICES

Infineon Technologies

- Smartcard architecture in PKI
  - secure storage, PKI security devices, card architectures, client identification...
- Applications for PKI
  - models, showcases for PKI, e-to-e, WIM/SWIM, PETs.....
- Phone and Smartcard
  - interfaces, dual slots, USB.....

LEGAL & REGULATORY

Focus on newly developing issues from a legal point of view

- differences wireless/ wireline
- mobility as such
- privacy enhanced PKI (blinded credentials,...)

MEMBERS.....

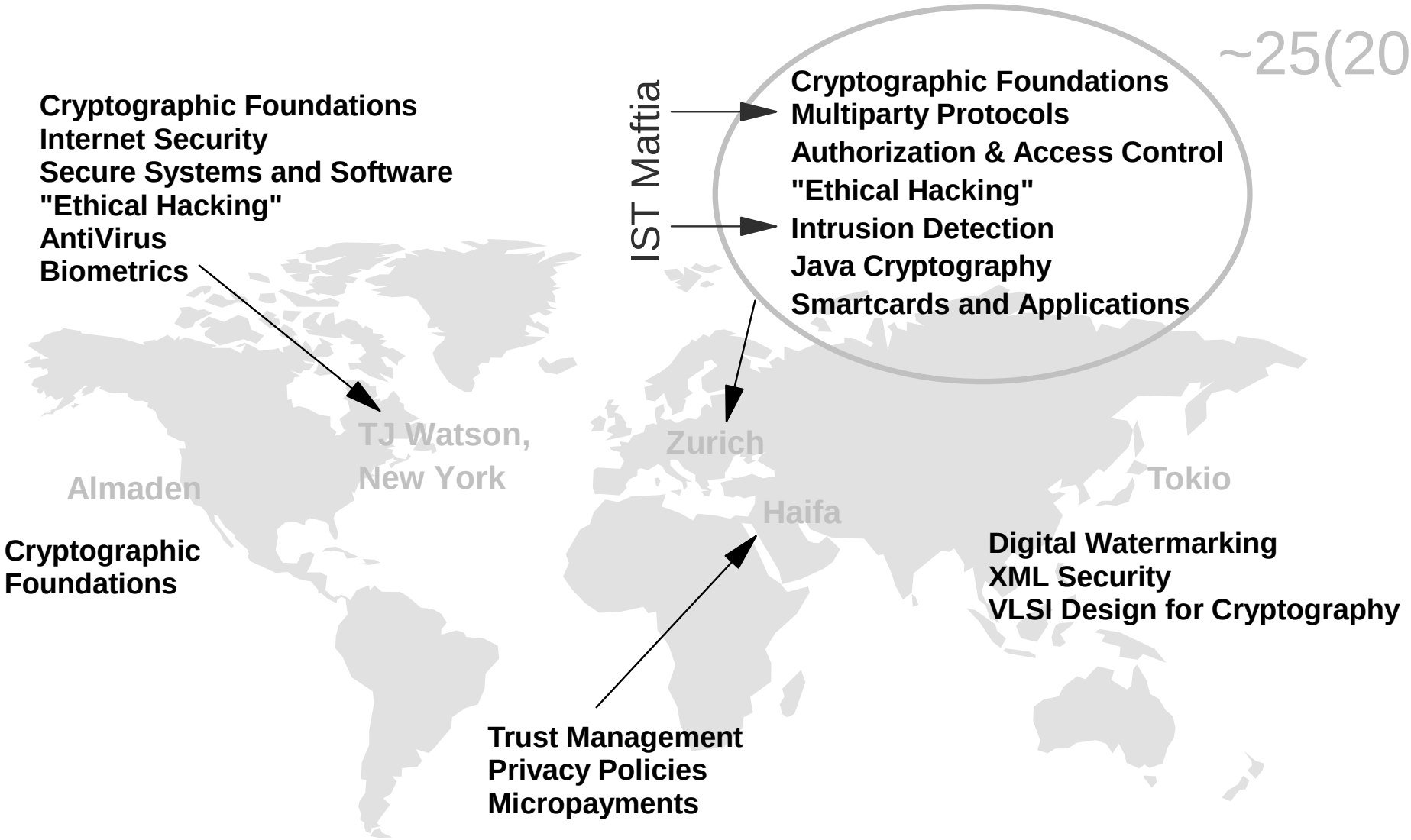

Radicchio
www.radicchio.org
e-mail: enquiries@radicchio.org
THANK YOU !
A global initiative to unleash the potential of wireless e-commerce

Michael Waidner
wmi@zurich.ibm.com
IBM Zurich Research Laboratory
Rüschlikon, Switzerland

Trust and Security Challenges

Trust and security challenges in Cyberspace: Defining an RTD Agenda for Europe
Brussels, December 8-9, 2000

Security and IBM Research



http://www.zurich.ibm.com/Technology/Security

Some technology trends (1/3)

- Internet as the society's IT backbone
  - **dependability in general? availability in particular?**
  - **COTS & mono culture of routers and OS's = not dependable?**
- The transparent society vs. Big Brother
  - security through public control
  - infinite storage capacity, everything can be joined and analysed
  - policy $\rightarrow$ **enforcement/PETs** $\rightarrow$ **audit/detection**
  - **pervasive anonymity, user-friendly pseudonym management**
- Wireless Internet
  - always connected everywhere anytime
  - pervasive infrastructure (ambient network, etc.), m-commerce
  - personalized, location-aware services: **privacy, security management**

Some technology trends (2/3)

- Person-to-person electronic transactions
  - direct interactions without central control
  - person = their PC
  - **trustworthy computing base, user-friendly security management, (PKI), (IPR protection)**
- Dynamic e-business
  - all the usual PKI stuff: (maintaining trust & confidence)
- Delegation of services
  - ASPs, outsourcing: **growing number of insiders**

Some technology trends (3/3)

- Number theory, quantum computing
  - might kill modern cryptography in x years
  - **what are the alternatives?**
- Verification of security
  - current public-key cryptography is >5 years behind state of the art
  - formal methods community has made substantial progress, but is not much used in practice

Summary: Challenges

- **Ensure privacy in (mobile) Cyberspace**
  - privacy despite personalized, location aware services
  - closing the gaps between policies, enforcement, audit/evaluation
- **Realize a secure computing platform**
  - secure, usable desktop (and server) OS
  - user-friendly security management, P2P-authentication
- **Strengthen the foundations**
  - formal methods in information security
  - cryptography in the age of "the next Gauss" and quantum computers
- **Dependability of the infrastructure**
  - e-democracy ... vulnerability of the power grid ... httpd in each light bulb
  - mono-culture effects, increasing number of insiders
  - poor awareness, poor education in security