



**Università degli Studi di
Trento**

MASTER 
Managing and Auditing
Security and Trust for sERvices

Future Internet The End of Trust as We Knew It

Fabio Massacci

**University of Trento
www.massacci.org**

(NOT TORINO!)

3/9/2010



Where is Trento?



- **1962**
Autonomous Research Institute

- **1972**
Recognized as private University

- **1982**
Become Statal, public University

2007 Ranking of Italian mid-sized Universities

- Arts 1st
- Economics 2nd
- Engineering 2nd
- Law 1st
- Sciences (including CS) 1st
- Sociology 1st

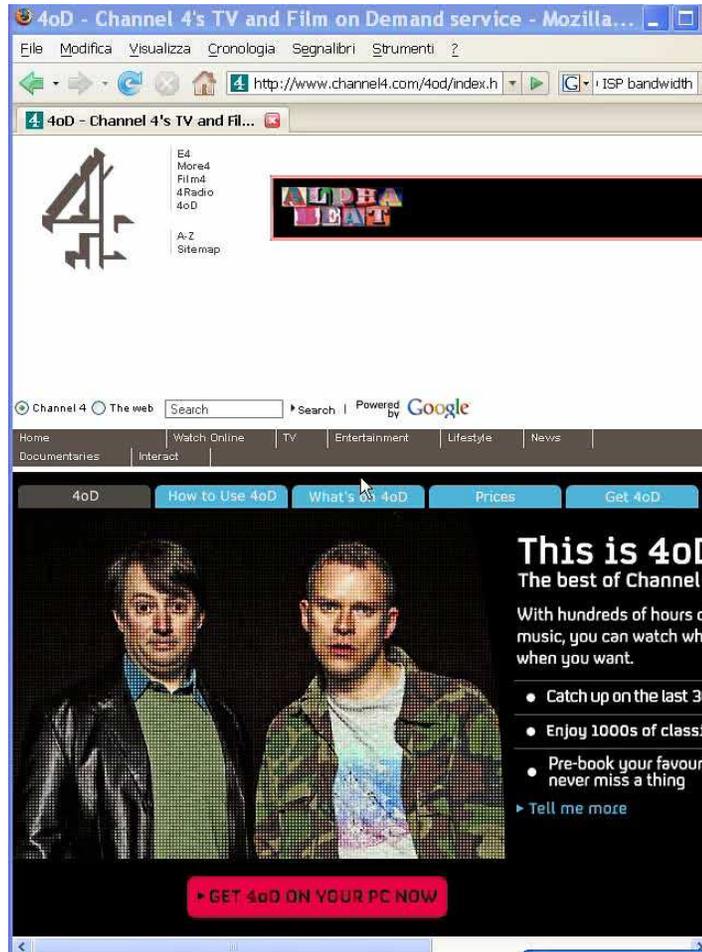


Two things I'll tell

- **What is the Future of Internet?**
 - **The End of Trust as we Know it...**
 - The demise of WS-Trust, WS-* and all that
 - The end of everywhere services...
 - **The rise of Security-&-Privacy-by-contract**
 - **Macro-Security is born...**
 - As in Micro and Macro Economics
 - Security as an Experimental Discipline
- **Remember these two things and**
 - **now can check your email...**



A Picture is worth a 1000 words...



Videotape from
UK Channel 4
9 June 2008



Tu quoque Brute, fili mi...

- **Do you know 4oD?**
 - **A software to view, stream, save and own TV movies**
 - **You download it from the Internet**
 - **But it installs on your PC a stealthy P2P servent...**
 - which serves movies elsewhere in the world...
- **But it's not shady software from rbnexploit.com**
 - **It is from UK's Channel 4! A reputable broadcaster...**
 - **But servent isn't in the FAQ, isn't in the readme....**
 - Hidden in the license agreement after 5 pages of legalese
 - **But your ISP will tell, oh man, it will tell you....**
- **That's the end of (digital) Trust as we know**



- **Do you know Google for University?**
 - Free emails for students
 - Access to Google Scholars etc. etc
 - A business model where services can be anywhere and accessible from anywhere
- **In Italy**
 - University of Ferrara first to sign agreement with Google
 - Offered to UniTN as well
- **A little question: WHERE is our data?**
 - Google agreed to sign that data is in Italy, outside the reach of US subpoena
 - The death of the idea of services can be anywhere and accessible from everywhere...



The end of (digital) trust....

- **The Demise of WS-Trust, WS-Policy, WS-Federation**
 - **From digital signatures to webs of trust for services...**
 - **But nothing is attached to a signature...**
 - What security relevant action you do...
 - Where you are...
 - What obligations you pose...
 - How compliant you are with policies, legislations...
- **So you cannot bootstrap trust from nothing**
 - **(Digital) Trust was killed the day 4oD went on the internet...**
 - And ironically in the very country that invented the habeas corpus...
 - **Everywhere Services were killed when Google named a physical place**
 - And ironically in the very Company that invented them



- **Are you a service?**
 - **Tell me what you do it (and where are you)**
 - Design software with security claims
 - **Let me check it**
 - Compliance of services Contracts with user's Policies
 - **Show me your evidence or**
 - Check that the service actual fulfills its claims
 - **Let me keep an eye on you or**
 - run-time monitor the services.
 - **Let me vaccinate you**
 - Inoculate Security Policy into software
 - **Assess globally how things are going**
 - Indicators for security & assurance



- Easier done than thought
- Security by Contract for the Mobile Phones
 - **S3MS project with DoCoMo-EuroLabs --- www.s3ms.org**
 - Applications come with acontract
 - Matching Application's contracts with Phone's Policy
 - Inoculation of policies for "bad" applications
 - .NET and Java
 - Project successfully concluded – see the video
 - At first Gaming application hacks access to the SIM card
 - Then same application with S3MS technology cannot do
- Compliance for services
 - **MASTER project --- www.master-project.eu**
 - Design software with security claims
 - Compliance of services Contracts with user's Policies
 - run-time monitor for services in outsourcing
 - Indicators for security & assurance
 - Just started





Macro-Security is born...

- **Do you remember Micro-vs-Macro Economics?**
 - **The Gas Law vs molecular cinematics**
- **So far we all worked on Micro-Security**
 - **Properties of security components (Crypto, SW, TPMs, etc.)**
 - **Security design, verification, integration of components**
- **But now will have a by-product of S&P-by-Contract**
 - **“Users” have their security & privacy policies**
 - **“Services” have their security & privacy contracts**
 - **A “Market” is born...**
- **Macro-Security as experimental discipline of Future Internet**
 - **Can we study the Macro-security of users and services?**
 - **... without looking at individual components?**
 - **Can we discover global security laws? Which is the Gas Law?**



Something to take home

□ What is the Future Internet?

□ The End of Trust as we Know it...

- The demise of WS-Trust, WS-* and all that

□ The rise of Security-&-Privacy-by-contract

- Application & Services should tell what they do
- We should check, vaccinate, monitor & assess them

□ Macro-Security will be born...

- As in Micro and Macro Economics
- Security as an Experimental Discipline