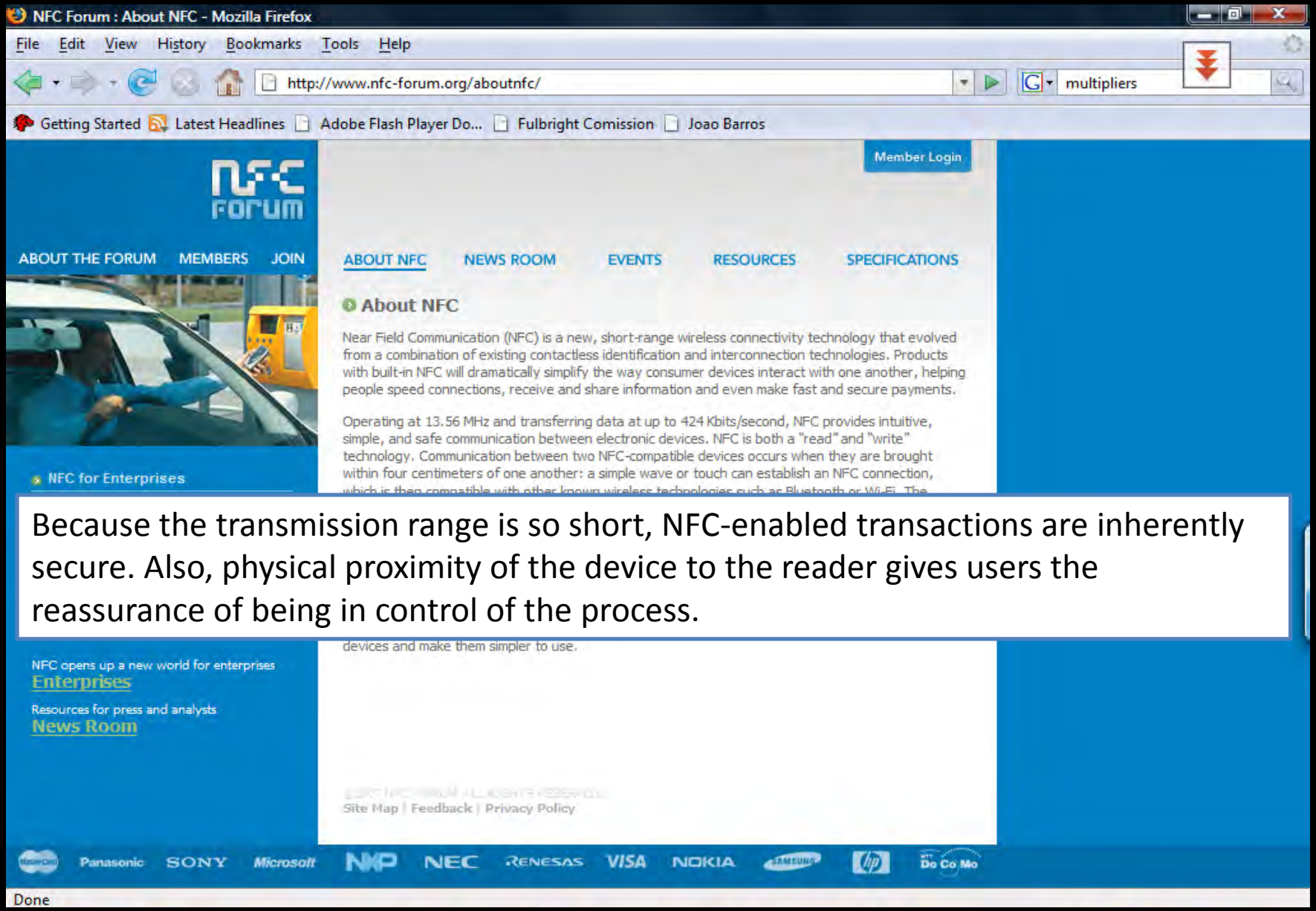
Cyber-Attacks are real

- Case studies:
  - 2000 Australia: sewage treatment plant
  - 2007 Estonia: attacks on government, banks, media
  - 2008 Poland: signaling for trams in Lodz
  - 2010 Stuxnet: first computer worm that targets industrial control systems (Iranian centrifugues)
  - 2011 Sony Playstation: leakage of personal data (24.6M costumers)



Because the transmission range is so short, NFC-enabled transactions are inherently secure. Also, physical proximity of the device to the reader gives users the reassurance of being in control of the process.

Many Open Issues

- How can we keep up with emerging cyber-risks (it is much like an arms race)?
- How can we promote advanced education in cyber-security?
- How can we measure system trustworthiness?
- What are the right policies to ensure security-by-design?
- How can we involve end user communities in matters related to risk?
- How can we engage the private sector?

More Open Issues

- Should we separate cyber-security, cyber-crime and cyber-defense?
- How can we ensure universal access to the Internet while ensuring information security and critical infrastructure protection?
- What are the basic principles of security economics?
- How can we speed up the legislative process and international regulation to match the speed of Internet growth and evolution?
- How can we raise risk awareness and promote global risk governance in matters related to cyber-security and critical infrastructure protection?

And many more…

Some Institutional Developments

- European Network and Information Security Agency (ENISA):
  - exchange of information, best practices and knowledge
- EU-US Working Group on Cyber-Security and Cyber-Crime:
  - Industrial control systems, smart grids, awareness raising, PPP, Botnets
- EP3R Public-Private Partnership for Resilience
  - Continuous and secure provision of electronic communication, cooperation towards emergency readiness
- EFMS European Forum of Member States

  (a) the definition of criteria to identify European critical infrastructures;

  (b) the identification of European priorities, principles and guidelines for Internet resilience and stability;

  (c) the exchange of good policy practices, in particular on cyber exercises.
- European Security Research Advisory Board (ESRAB)
- European Security Research and Innovation Forum (ESRIF)
- European Defence Agency

THE LONDON CONFERENCE ON CYBERSPACE

1 - 2 NOVEMBER 2011

The aims of the conference

The London Conference will launch a focused and inclusive dialogue to help guide the behaviour of all in cyberspace.


“when governments do discuss this subject we are at risk of adopting wrong or dangerous conclusions, or of being out of touch and out of date the minute we sit down. It is vital that we understand our limitations in this area.”
William Hague