Future Threats to Future Trust

Sotiris Ioannidis
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece

Goals

- The future is hard to predict…
  - Worms
- … but we have had success stories
  - RFID
- The FORWARD Project is a coordinated action
  - Bring together academics, industry, and policy makers who are interested in emerging threats in ICT
  - Discuss future threats
  - Develop realistic scenarios

Consortium

http://www.ics.forth.gr/dcs

TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

FORTH

Roadmap

- Motivation
  - Why is this work important?
- What drives future threats in trust?
  - Technical Dimensions
  - New Applications
  - Market Trends
- What are the Risks?
  - Current, Emerging, and Future
- Conclusions

Roadmap

- Motivation
  - Why is this work important?
- What drives future threats in trust?
  - Technical Dimensions
  - New Applications
  - Market Trends
- What are the Risks?
  - Current, Emerging, and Future
- Conclusions

Motivation

- Prepare for the future
- Anticipate the emerging risks
  - you can prepare better
  - you can inform beneficiaries
  - you may be one step ahead in the security “arms race”

So…

- We need to collect information for
  - Current,
  - Emerging, and
  - Future threats and vulnerabilities in
  - Network and information systems security
- Current threats: 2008
- Emerging threats: 2008-2010
- Future threats: 2010-2013

Roadmap

- Motivation
  - Why is this work important?
- What drives future threats in trust?
  - Technical Dimensions
  - New Applications
  - Market Trends
- What are the Risks?
  - Current, Emerging, and Future
- Conclusions

What drives emerging threats in trust?

- Technical Dimensions
  - What will be the technologies of the future?
- Application Dimensions
  - What will be the applications of the future?
- Future Market Trends and Dimensions
  - What are the trends in the market?

Drivers: Technical Dimensions

- Which technical dimensions drive future threats?
  - Scale
    - Long chains of trust
      - Chains of trusted devices
    - Lots of things to verify
      - Large, complex software
    - What happens if we cannot verify something?
      - Rollback may not be an option
      - Users don't like that
    - Not every device has a TPM
      - Cost

Drivers: Technical Dimensions

- Which technical dimensions drive future threats?
  - What is the network? Can you trust it?
    - Physical infrastructure, wired, wireless
  - Which network do you trust?
    - Internet, cellular, bluetooth, etc.
  - Do you trust the routing infrastructure?
    - Hijacking, attacks on routers, can we practically secure BGP?

Drivers: Technical Dimensions

- Which technical dimensions drive future threats?
  - Wireless Networks, so you trust them?
    - Wireless networks could potential be eavesdropped
    - Wireless devices may become more transparent
      - Less visible – more integrated with other appliances
  - Proliferation of Broadband Networks
    - i.e. **compromised computers have more firepower today.**
    - e.g. a 1 Mbps DSL computer can send
      - 10 Gbytes of information per day
      - One million (1,000,000) SPAM email messages
      - 10 million attack packets
    - 10 years ago a computer on a 28.8Kbps modem
      - Had two-three orders of magnitude less firepower

Drivers: Technical Dimensions

- Which technical dimensions drive future threats?
  - Device miniaturization
    - Devices will not remind us of a traditional computer
    - They will be integrated into other devices (doors, stoves, etc.)
    - They may not run (properly configured) protection software (e.g. Antivirus, firewalls)
    - They may not run secure operating systems
  - Digital identities (e.g. RFID)
    - More products will have a digital ID
    - People will frequently carry (or wear) products with digital IDs
    - Digital ID readers will proliferate (in public buildings, etc.)

Drivers: Applications

- Smart Mobile Phones
  - Eavesdropping, loss of privacy, stalking
- E-banking, e-commerce, e-everything
  - Financial loss, attacks to banking system, attacks to the stock market, etc.
- Smart Home – AmI
  - Lots of wireless potentially vulnerable devices
- Smart Vehicles
  - What if the computer that controls the brakes is compromised?
  - Do you trust your car?

Drivers: Applications

- E-health
  - What if the computer which controls a medical device gets compromised?
  - What if our medical record is stored in a compromised computer?
- E-government
  - More and more of our personal information will be stored on-line
- Blogs/Social Networks
  - Blogs encourage people, including minors, to publish their information on the web
  - This may be used for stalking today
  - It may be used to invade their privacy, etc.
  - Build up trust, then exploit it

Drivers: Future Market Trends and Dimensions

- **On-line services will become more common**
  - Online services: commerce, entertainment, news, etc.
  - Even a “second-life” is possible on-line
- **Mobile phone use will prevail**
  - People are “on the go” – mobile phones are needed to support our mobile world
- **Service-oriented information society**
  - European Economy moves away from “traditional products” and steps into new forms of “services”
  - The Internet enables these services to be composed to create even *“fancier”* ones
    - E.g. find a doctor who has an opening at a date a time compatible with your schedule and your mother’s schedule and who is located nearby

Roadmap

- Motivation
  - Why is this work important?
- Which are the drivers of the emerging threats?
  - Technical Dimensions
  - New Applications
  - Market Trends
- What are the Risks?
  - Current, Emerging, and Future
- Conclusions

Current Risks

- Spam
  - to email addresses, phones, etc.
- Botnets
  - “zombie” computers
- Phishing
  - Using more means (phones, SMS)
  - More targeted
    - (“Hey Pal. We met at the IST conf. Let me tell you about…”)
- Identity theft
  - Login/password
- Route hijacking
  - Divert/Intercept traffic from the Internet
- Instant Messaging
  - Chat, etc. SMS, etc.

Current Risks

- Peer-to-peer systems
  - File sharing systems
    - Download malware
- Malware on Cell Phones
  - Through SMS, MMS, (free) games
- Hackers in Stock Market
  - Through compromised bank accounts
- Software Vulnerabilities
  - Software is getting larger and more complex
- No protection (e.g. antivirus) in some devices
  - Mobile phones
  - Printers, game consoles (protection for all the wrong reasons)
  - Refrigerators, air-conditioners, stoves, etc.

Emerging Risks

- SCADA
  - Supervisory Control And Data Acquisition
- Increased home automation
  - A hacker may penetrate the computer which controls the front door
- Massive collections of personal data
- Invisible data collection in public places
- Invisible data collection in private premises
- Security is more an art than a science

Emerging Risks

- DoS attack to the home telephone
  - Imagine hackers/spammers continuously calling someone's telephone
- Hacking home heat and/or air-conditioning system
  - Turn on/off the stove while the owner is away…
- Internet users are younger, less experienced, and more prone to subtle attacks
- Internet users may not have strong motives to clean up their compromised computers
- Malware over multiple networks (GSM, GPRS, Internet, Bluetooth)

Future Risks

- **Manageability**
  - Currently we manage a few digital devices:
    - Computer, PDA, mobile phone, laptop
  - In the future we will have 10's if not 100's of such devices most of which will be hidden
- **Over-use of ICT**
  - People use ICT even when not needed
    - They send email/IM instead of talking to people
    - They use e-voting systems when traditional "raise your hand" votes work just fine
      - Such approaches open the road to cyber attackers
- **Use home appliances to attack infrastructures**
  - Use thousands of compromised phones to overload the telephone network
  - Use thousands of compromised air-conditioning units to overload the electric power grid

Roadmap

- Motivation
  - Why is this work important?
- Which are the drivers of the emerging threats?
  - Technical Dimensions
  - New Applications
  - Market Trends
- What are the Risks?
  - Current, Emerging, and Future
- Conclusions

European Initiative

- FORWARD Project
  - FP7 funded, Six European partners
    - Vienna Technical University, Institut Eurecom, Vrije Universiteit, Chalmers University, IPP-BAS, FORTH
  - Working groups on
    - Malware and Fraud, Critical Infrastructures, Smart Environments
  - www.ict-forward.eu

In closing…

- The factors that drive emerging risks in security, privacy and trust are:
  - New technology
    - Wireless networks, residential broadband networks, device miniaturization, TPMs, etc.
  - New applications
    - Mobile phones, e-banking, e-government, etc.
  - Social Engineering
    - Phishing, etc.
- We need to
  - Understand the dimensions of the problem
  - Work towards addressing current, emerging and future risks