Privacy of Mobile Computer Users

Janne Lindqvist
Dept. of Computer Science and Engineering
Helsinki University of Technology (TKK)

AFSecurity Seminar, UNIK, Kjeller, Nov. 13, 2008

Outline

- Privacy Enhancing Technologies Research
- Mobile Internet users and anonymity
  - Anonymity towards casual observers at the access link
- Network chatter
  - Examples, analysis tools, details of some leaks
- Reducing network chatter
  - Outline of a solution based on network location awareness (NLA)

Privacy?

- Information flow control
  - “the claim of individuals, groups, or institutions to determine themselves when, how, and to what extent information about them is communicated to others”, Alan F. Westin, “Privacy and Freedom”,1967
- The right to be left alone
  - “…modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”, Warren and Brandeis, Harward Law Review, 1890.

Our Work on Privacy Enhancing Technologies 1/2

- "Privacy Management for Secure Mobility"
  - We showed how a mobility management protocol with IPsec can be used to protect privacy [Lindqvist & Takkinen, WPES'06]
- "IPv6 Stateless Address Autoconfiguration Considered Harmful"
  - We showed how PETs can be *harmful* for privacy, [Lindqvist, MILCOM'06]
- "Cure for Spam over Internet Telephony"
  - CAPTCHAs over SIP [Lindqvist & Komu, CCNC'07]

Our Work on Privacy Enhancing Technologies 2/2

- "Chattering Laptops"
  - Bulk of this talk [Aura, Lindqvist, Roe, Mohammed, PETS'08]
- "Protecting Privacy with Protocol Stack Virtualization"
  - Mitigating privacy leaks with traffic isolation [Lindqvist & Tapio, WPES'08]
- "Privacy-Preserving 802.11 Access-Point Discovery"
  - Enhancing WiFi client privacy in AP discovery, [Lindqvist, Aura, Danezis, Koponen, Myllyniemi, Mäki, Roe, *under submission*]

Mobile Internet users and anonymity

Anonymity in public places

- We are used to relative anonymity in public places: e.g., streets, shops, trains, cafes, airports
  - It is easier to relax when nameless and “off duty”
  - Name or affiliation could draw unwanted attention
  - Usually not a strong requirement: it is normal to be spotted occasionally
- Do you remove your conference name tag in the evening?
- Summary of this talk: using a wireless computer is like wearing a name tag

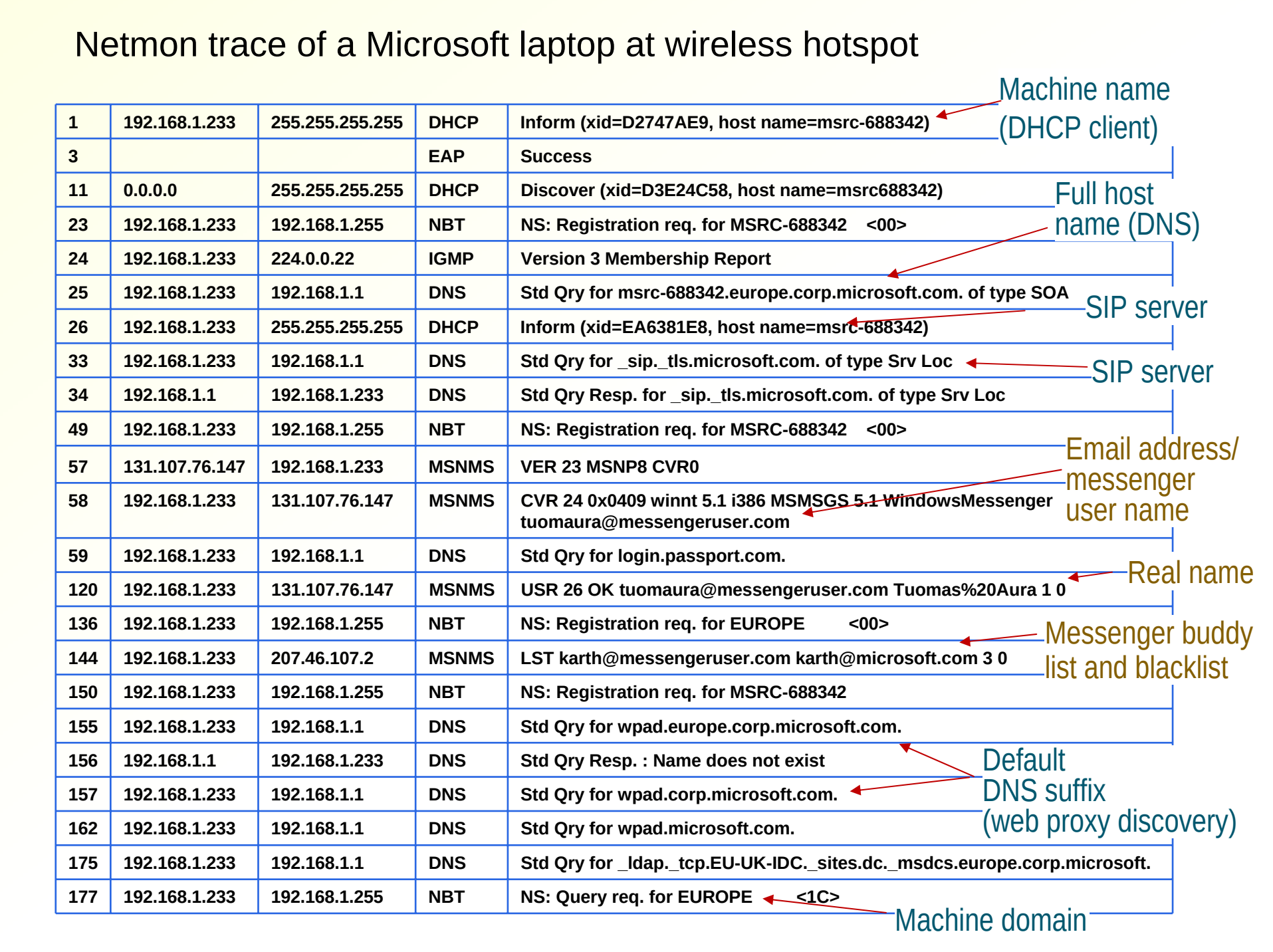
Anonymity and location privacy on the Internet

- Discussion on anonymity is usually about:
  - Anonymity towards servers across the Internet
  - Location privacy towards peers across the Internet, central location-tracking databases
  - Global observers, “total information awareness”
- Proposed solutions: anonymous routing, privacy laws and policies
- What about *casual observers* such as the lone person with a laptop two tables away? What can they find out about me?

Network chatter

Netmon trace of a Microsoft laptop at wireless hotspot

1	192.168.1.233	255.255.255.255	DHCP	Inform (xid=D2747AE9, host name=msrc-688342)
3			EAP	Success
11	0.0.0.0	255.255.255.255	DHCP	Discover (xid=D3E24C58, host name=msrc688342)
23	192.168.1.233	192.168.1.255	NBT	NS: Registration req. for MSRC-688342 <00>
24	192.168.1.233	224.0.0.22	IGMP	Version 3 Membership Report
25	192.168.1.233	192.168.1.1	DNS	Std Qry for msrc-688342.europe.corp.microsoft.com. of type SOA
26	192.168.1.233	255.255.255.255	DHCP	Inform (xid=EA6381E8, host name=msrc-688342)
33	192.168.1.233	192.168.1.1	DNS	Std Qry for _sip._tls.microsoft.com. of type Srv Loc
34	192.168.1.1	192.168.1.233	DNS	Std Qry Resp. for _sip._tls.microsoft.com. of type Srv Loc
49	192.168.1.233	192.168.1.255	NBT	NS: Registration req. for MSRC-688342 <00>
57	131.107.76.147	192.168.1.233	MSNMS	VER 23 MSNP8 CVR0
58	192.168.1.233	131.107.76.147	MSNMS	CVR 24 0x0409 winnt 5.1 i386 MSMSGS 5.1 WindowsMessenger tuomaura@messengeruser.com
59	192.168.1.233	192.168.1.1	DNS	Std Qry for login.passport.com.
120	192.168.1.233	131.107.76.147	MSNMS	USR 26 OK tuomaura@messengeruser.com Tuomas%20Aura 1 0
136	192.168.1.233	192.168.1.255	NBT	NS: Registration req. for EUROPE <00>
144	192.168.1.233	207.46.107.2	MSNMS	LST karth@messengeruser.com karth@microsoft.com 3 0
150	192.168.1.233	192.168.1.255	NBT	NS: Registration req. for MSRC-688342
155	192.168.1.233	192.168.1.1	DNS	Std Qry for wpad.europe.corp.microsoft.com.
156	192.168.1.1	192.168.1.233	DNS	Std Qry Resp. : Name does not exist
157	192.168.1.233	192.168.1.1	DNS	Std Qry for wpad.corp.microsoft.com.
162	192.168.1.233	192.168.1.1	DNS	Std Qry for wpad.microsoft.com.
175	192.168.1.233	192.168.1.1	DNS	Std Qry for _ldap._tcp.EU-UK-IDC._sites.dc._msdcs.europe.corp.microsoft.
177	192.168.1.233	192.168.1.255	NBT	NS: Query req. for EUROPE <1C>



182	192.168.1.233	192.168.1.1	DNS	Std Qry for _ldap._tcp.EU-UK-IDC._sites.gc._msdcs.corp.microsoft.com. of type Srv Loc
187	192.168.1.233	65.53.212.30	ISAKMP	Major Version: 1 Minor Version: 0 GSS-identity: msrc-688342.europe.corp.microsoft.com
193	192.168.1.233	65.53.212.30	HTTP	CCM_POST Request from Client MSRC-688342
249	192.168.1.233	192.168.1.1	DNS	Std Qry for msrc-688342.europe.corp.microsoft.com. of type SOA
271	192.168.1.233	192.168.1.1	DNS	Std Qry for research.microsoft.com.
283	192.168.1.233	131.107.65.14	HTTP	GET /users/tuomaura/ HTTP/1.0
516	192.168.1.233	255.255.255.255	DHCP	Inform (xid=20CCCAE8, host name=msrc688342)
522	192.168.1.233	192.168.1.1	DNS	0x82A0:Std Qry for itgweb.europe.corp.microsoft.com.
525	192.168.1.233	192.168.1.255	NBT	NS: Query req. for ITGWEB <00>
569	192.168.1.233	192.168.1.1	DNS	0x37BD:Std Qry for mail.microsoft.com.
675	192.168.1.233	192.168.1.1	DNS	0xDCBB:Std Qry for red-lcsdr-02.europe.corp.microsoft.com.
684	192.168.1.233	192.168.1.255	NBT	NS: Query req. for RED-LCSDR-02 <00>
706	192.168.1.233	192.168.1.1	DNS	0xECB9:Std Qry for euro-dc-10.europe.corp.microsoft.com.
716	192.168.1.233	192.168.1.1	DNS	0xF5B7:Std Qry for prn-corp1.redmond.corp.microsoft.com.
717	192.168.1.233	192.168.1.255	NBT	NS: Query req. for camitgs01
718	192.168.1.233	192.168.1.255	NBT	NS: Query req. for POMO.KOTI.LOCAL
726	192.168.1.233	192.168.1.1	DNS	0x59B7:Std Qry for pomo.koti.local.
735	192.168.1.233	192.168.1.1	DNS	0x96B6:Std Qry for camitgs01.europe.corp.microsoft.com.
744	192.168.1.233	192.168.1.255	NBT	NS: Query req. for KOTI <1C>
748	192.168.1.233	192.168.1.255	NBT	NS: Query req. for camitgs01 <00>
754	192.168.1.233	192.168.1.1	DNS	0x76B6:Std Qry for sha-fp-01.fareast.corp.microsoft.com.
884	192.168.1.233	192.168.1.1	DNS	0x4FB5:Std Qry for cam-01-srv.europe.corp.microsoft.com.
930	192.168.1.233	192.168.1.255	NBT	NS: Query req. for CAM-01-UNX

Host name (IKE initiator id)

IE home page

OWA / Exchange

Domain controller

Print servers

File server (Z: drive)

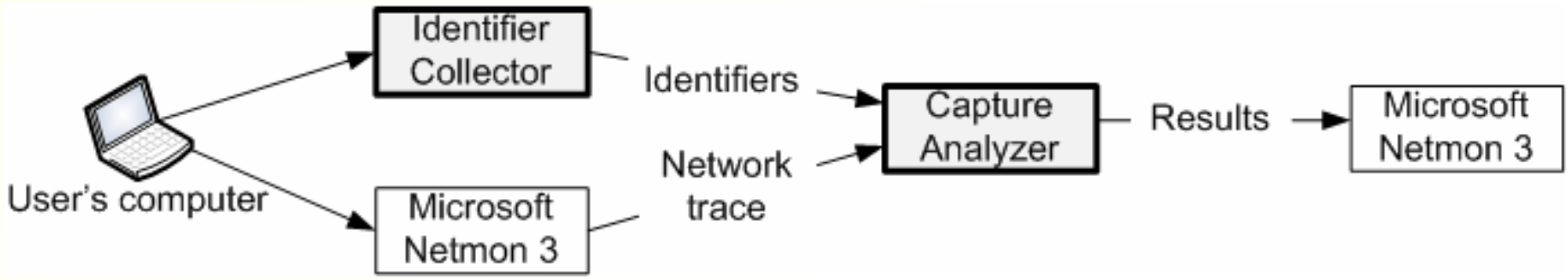
File server (shortcuts)

Network chatter

- Modern computers perform many tasks automatically, without asking the user
  - Configuring the network interface (e.g. DHCP)
  - Service discovery for local services (e.g. printers, WiFi)
  - Access to intranet and Internet services (e.g. DC, email)
- These protocols reveal information about
  - Mobile computer identity
  - User identity (sometimes)
  - Affiliation with services and organizations
  - History of service usage
- Many unnecessary, failed connection attempts, to services that are currently not available

Tools for analyzing information leaks

Analyzing network captures



- Defensive tools for detecting information leaks from my own computer
  - Collect various identifiers of the user, computer and organization from the computer and intranet
  - Record network traces while roaming
  - Search for the known identifiers in various encodings
- Research prototype implemented for domain-joined Windows XP and Vista

Challenges in trace analysis

- Need to know which identifiers to look for
  → only detects leaks from one's own computer
- Many string and binary encodings
  - Character variations (lower and upper case, accents)
  - Escape sequences
  - ASCII, Unicode encodings
  - Multiple (recursive) encoding layers

  We try to detect as many encodings as possible
- Cannot detect intentionally obfuscated data, only unintended leaks
- Currently cannot decode encrypted, compressed or base64 data

Lessons from the analysis: leak details

DHCP

Source	Destination	Protocol	Info
0.0.0.0	255.255.255.255	DHCP	DISCOVER, hostname=msrc-688342
192.168.1.5	255.255.255.255	DHCP	OFFER (offered IP address)
0.0.0.0	255.255.255.255	DHCP	REQUEST, fqdn=msrc-688342.europe.corp.microsoft.com
192.168.1.5	255.255.255.255	DHCP	ACK

Host name

Host name and DNS suffix

- Client sends the hostname and FQDN
  - To obtain host-specific IP address and other parameters, and for (reverse) DNS registration
  - May also request previous IP address
- DHCP is often the first protocol executed
  - Link broadcast, so visible on switched LANs
  - Client does not yet know which network it is on

→ How would you prevent these leaks?

DNS queries

- Many connection attempts and service-discovery protocols start with DNS queries
- Some DNS queries from traces:
  - DC discovery: _ldap._tcp.EU-UK-IDC._sites.dc._msdcs.europe.corp.microsoft.
  - Print server: camitgs01.europe.corp.microsoft.com
  - Web proxy: camproxy.europe.corp.microsoft.com
  - Exchange: euro-msg-43.europe.corp.microsoft.com
  - Exchange over HTTPS: mail.microsoft.com
- Private DNS zones used on intranets
  - *.private.contoso.com or *.contoso.local
- Default DNS suffix appended
  - To resolve www.tkk.fi, query first for www.tkk.fi.europe.corp.microsoft.com,

IKE and Kerberos

Source	Destination	Protocol	Info
172.19.5.12	157.58.41.12	IKE	IKE: version = 1.0, Identity Protected Mode, Main Mode, SA Payload: GSS-API using Kerberos, GSS Identity Name = MSRC-688342.EUROPE.CORP.MICROSOFT.COM

Host name and DNS suffix

- Identity protection was one of the main design goals for the Internet Key Exchange (IKE)
- Kerberos authentication for IKE (GSS-API)
  - Reveals client name in the SA payload in initial message
  - Intended only for intranets where Kerberos is available
- But… after moving away from the intranet, the computer may still send data to cached intranet IP addresses → IKE initiated → identity leaked
- Kerberos ticket requests also sometimes seen outside the intranet

TLS and WLAN security

- TLS handshake has no identity protection: certificates sent in clear

  → TLS VPN will reveal client certificate
- The EAP-TLS method in wireless network authentication (WPA(2), 802.11i) similarly leaks certificates
  - Passive observer can identify clients at a WLAN
  - Recent RFC 5216 adds client identity protection to EAP-TLS

Application metadata 1/2

- Application data can usually be encrypted end-to-end
  - Free services like instant messengers do not always encrypt *data* to save data-center costs
  - Some services provide end-to-end encryption for e.g. email data

    However, the devil is in the details!

Application metadata 2/2

- No easy solution when the goal is to discover new peers
  - Apple iTunes discovers other users nearby to enable sharing; Bonjour protocol broadcasts user and computer names to the local link
    - (janne@Janne Lindqvist's computer)

Solutions based on network location awareness (NLA)

Solutions?

- What does not work well:
  - Avoiding network access
  - Disabling all automatic service discovery
  - Manual configuration for each network
  - Tunneling everything via VPN
  - Expensive or complex strong anonymity solutions
  - Outbound firewall to filter known identifiers
- The user experience depends on the computer doing things automatically for us
  - Maybe: privacy-preserving protocols for service discovery (e.g. WLAN SSID)
- Recall our observation: most leaks are caused by failed connection attempts at the wrong network

Network location awareness (NLA)

- Computer identifies access networks and stores settings for each network location
- New feature in Windows Vista
- How NLA works:
  - Network fingerprint includes various data, e.g. router MAC address, depending on network type
  - NLA computes a network identifier as a hash of the network fingerprint
  - OS and applications use the network identifier to store and access per-network settings
- Main purpose of NLA is to recognize previously visited networks

Using NLA

- We propose a new privacy policy:
  Automatically connect to a service only in networks where the service is know to exists
- Implementation:
  - Store known network identifiers for each service; require manual configuration for each new network
  - E.g. file shares and printers are specific to a network
  - Disable NetBIOS by default
  - Filter DNS requests for private zones when not in intranet
  - Use the default DNS suffix only in intranet
  - Access AD and Kerberos only in intranet
  - Enable GSS-API authentication in IKE only in intranet
  - Design similar network-location awareness to all new protocols
- Requires a culture change in the way network-enabled software is written
  - Could filter legacy protocols and applications at firewall (not trivial)

Further Information

- The publications are online
  - http://www.tml.tkk.fi/~jklindqv/publications.html

- *Tuomas Aura, Janne Lindqvist, Michael Roe, Anish Mohammed*, "Chattering Laptops", in the 8th Privacy Enhancing Technologies Symposium (PETS), Leuven, Belgium, July 23-25, 2008.
  - http://www.tml.tkk.fi/~jklindqv/pets2008web.pdf

Summary

- Using a laptop is like wearing a name tag: everyone can see your name and affiliation
- The real problem is that so many protocols and applications leak the same information; that makes the leaks difficult to stop
- Long-term solution: attempt connecting to services only when in the right network
- Requires network location awareness
- Need to address this problem first before deploying more advanced anonymity mechanisms such as MAC-address randomization