

Timo Kiravuo

Topic 1

Implementing the Orwellian society

Pervasive monitoring and data collection technologies existing and being developed today provide very interesting possibilities for collecting freely available information. For example now that mobile phones have usually the Bluetooth on, it is easy to identify individual phones from their unique MAC addresses and to keep track of a telephone's owner. This could enable us to implement the Orwellian society, where the Big Brother monitors people constantly for their wellbeing.

This topic suits a student who is imaginative and willing to combine data from several areas of technology (or even several branches of science). Since the topic is not straight forward, this is a challenging topic, but hopefully also a rewarding one.

Some sources to start with:

Title: An XML-based model for monitoring pervasive environments
Authors: Mostefaoui-SK; Dustdar-S Source: Proceedings, IEEE, Piscataway, NJ, USA

Title: A protocol for tracking mobile targets using sensor networks
Authors: Yang-H; Sikdar-B; Cayirci-E; Znati-T; Ekici-E
Source: Proceedings-of-the-First-IEEE-International-Workshop-on-Sensor-Network-Protocols-and-Applications-Cat, IEEE, Piscataway, NJ, USA

Title: Acceptance of electronic monitoring and its consequences in different cultural contexts: A conceptual model
Authors: Panina,D.; Aiello,J.R. Source: Journal of International Management, 2005

Title: An Innovative System that Runs on a PDA for a Continuous Monitoring of People
Authors: Bagues,M.I.; Bermudez,J.; Burgos,A.; Goni,A.; Illarramendi,A.; Rodriguez,J.; Tablado,A. Source: 2006.CBMS 2006.19th IEEE International Symposium on Computer-Based Medical Systems, 2006, 151

Title: Sensor network for supporting elderly care home
Authors: Hori,T.; Nishida,Y.; Aizawa,H.; Murakami,S.; Mizoguchi,H. Source: 2004.Proceedings of IEEE Sensors, 2004, 575

And of course: Geroge Orwell: 1984

Topic 2

NAT/Firewall traversal

Currently NAT and firewall control is done through a number of different proprietary mechanisms. As devices and their capabilities become even more diverse, there is a need to define to common mechanism to open holes and set up NAT-bindings on the network edges. The IETF NSIS working group is defining such an international standard.

This topic is not too demanding, but it requires you to familiarize yourself with a new protocol suite and its features and also to get more familiar with some details of firewall and NAT operations.

References:

<http://www.ietf.org/html.charters/nsis-charter.html>

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html

Title: Characterization and Measurement of TCP Traversal through NATs and Firewalls Authors: Guha,Saikat; Francis,Paul Source: 2005, Usenix

Topic 3

Better-than-nothing security

The current mode of the IP security architecture (IPsec) provides an all-or-nothing service, where security is provided only if nodes can be authenticated. In many cases security between peers would be useful even the parties are not authenticated through certificates, as this would protect the session integrity and against eavesdropping.

This is a relatively simple technology review and analysis. Some thought should be applied to the questions "what is the protection offered, what is protected, what is unprotected, where would this be useful?"

References:

<http://www.ietf.org/html.charters/btns-charter.html>