Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 08: Conclusion
Module 01: Conclusion and Outlook

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Looking Back

Source: sxc.hu

Learning Objectives

As taken from the module guide (Modulhandbuch)

- “Students attending the lecture are acquiring knowledge in the domain of communication network security with *emphasis on Internet security*. Students are able to apply and transfer the most important fundamentals from IT security and cryptography to the field of communication networks.”
- “Students … have a thorough understanding of *security mechanisms on the different network layers* (application layer, transport layer, network layer, link layer, physical layer). As a result, they are able to thoroughly discuss the *characteristics* and *principles* in the area of network security and exhibit detailed theoretical and practical knowledge in this field. Additionally, students are able to describe *recent developments* in the area of network security (e.g. peer-to-peer security, mobile network security, etc.).”
- “The exercise deepens the theoretical foundations by means of exercises, which consist of literature, calculation as well as practical implementation/application examples.”

Network Security

VS.

[Source: stumbled upon on some tumblr.com blog]

Contents of the Lecture

(00) Organization and introduction

(01) Fundamentals: security threats, attacks, services, and mechanisms

(02) Crypto pitfalls and applicability of crypto

(03) Application layer security

(04) Transport layer security

(05) Network layer security

(06) Link layer & physical layer security

(07) Operational security & selected topics: firewalls, intrusion detection systems

More Network Security

We did not (or only barely) cover

- Cybercrime, DRM, …
- Copyright, legal implications, ethical issues

We mostly considered the "traditional" network models

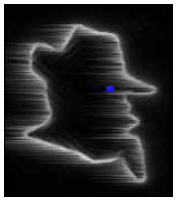
- Networks or servers are operated by trusted parties

But, in future wireless networks the trust model will be much more complex

- entities play multiple roles (users can become service providers)
- number of service providers will dramatically increase
- user – service provider relationships will become transient in many instances and permanent for dominating services (walled gardens)
- how to build up trust in such a volatile and dynamic environment?

Who is Malicious?
Who is Selfish?

Harm everyone: viruses,…

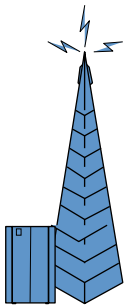


Big brother

Selective harm: DoS,…

Spammer

Cyber-gangster:
phishing attacks,
trojan horses,…



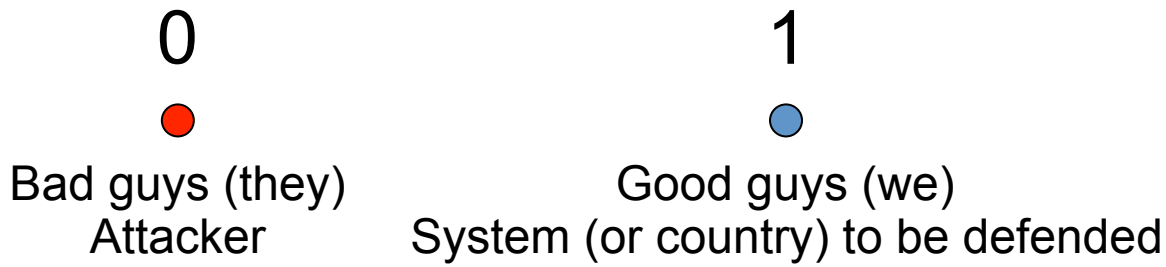
Greedy operator

Selfish
mobile station

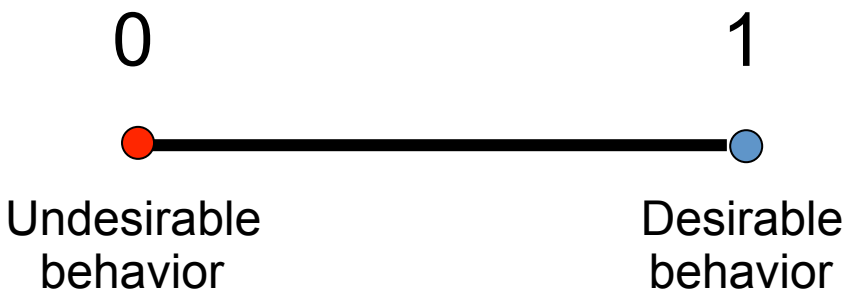
There is no watertight boundary between malice and selfishness
➔ Security does not solve all issues

From Discrete to Continuous

Warfare-inspired Manichaeism*



The more subtle case of commercial applications:



- Security often needs incentives
- Incentives usually must be secured

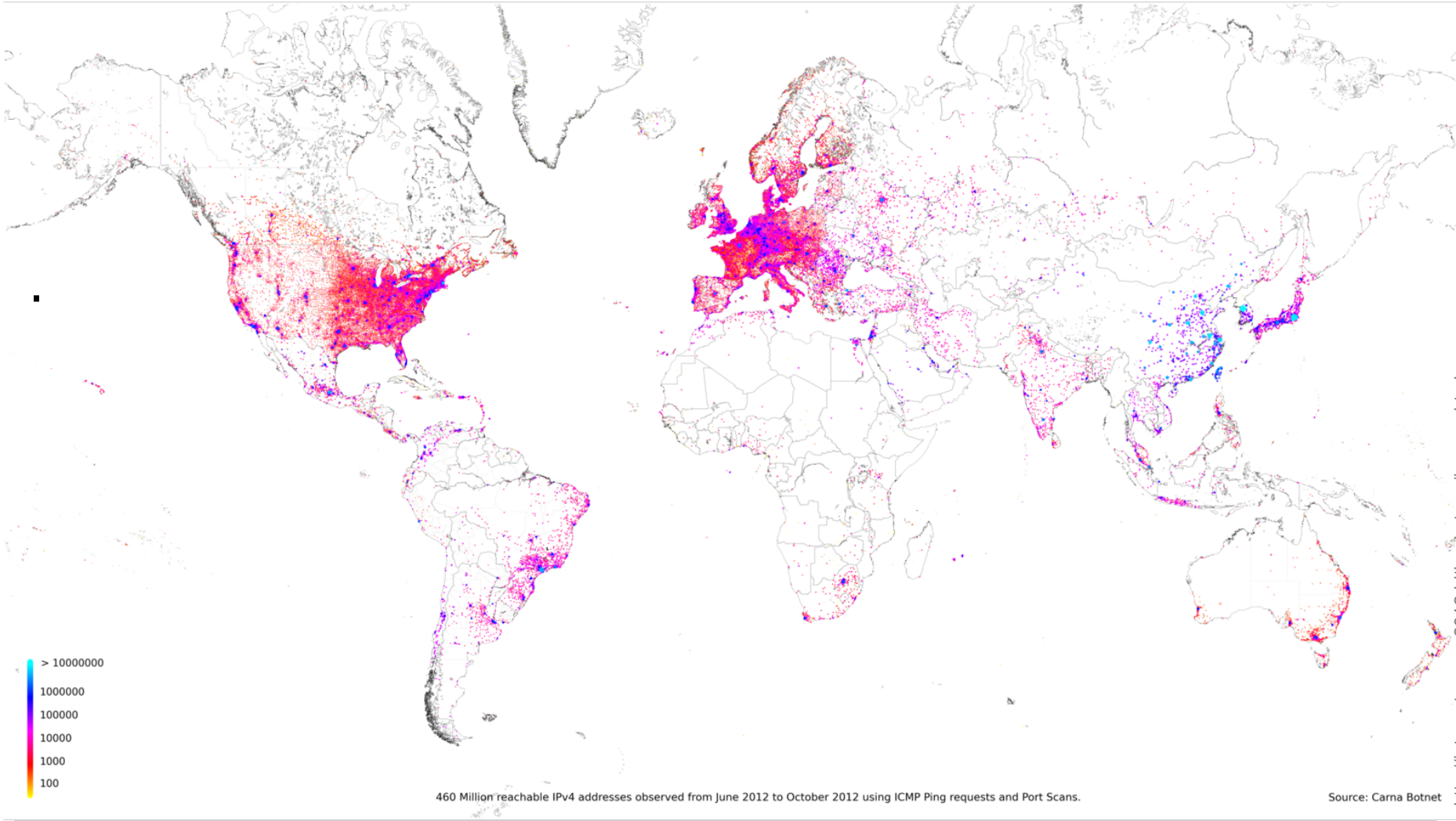
From Wikipedia: "… Manichaeism taught an elaborate cosmology describing the struggle between a good, spiritual world of light, and an evil, material world of darkness. …"

Grand Research Challenges: Towards Secure and Resilient Infrastructures

SECURE MOBILE NETWORKING

http://www.sxc.hu/photo/1874, http://www.sxc.hu/photo/6067,http://www.sxc.hu/photo/842709, http://www.sxc.hu/photo/909829, en.wikipedia.org, http://www.sxc.hu/photo/859795, Matthias Hollick,

Grand Research Challenges: Towards Secure and Resilient Infrastructures



General Questions

Observations (pessimistic? realistic?)

- "Traditional" infrastructures in dire need of renovation
- Our telecommunication networks are not secure
- Our software is not secure

What will be the consequence of not "owning" our cyber-infrastructures?

Grand Challenge: Secure Cyberinfrastructures

US President John Fitzgerald Kennedy on May 25, 1961, announcing the goal of sending an American safely to the Moon before the end on the decade

http://www.voanews.com/content/man-on-the-moon-challenge-50-years-on-122543039/149870.html

How do we address this challenge

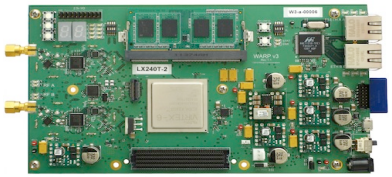
- Which capabilities do we have to develop?
- Who can contribute to this quest?
- What are the key research questions we should work on?

Selected Topics at SEEMOO

SECURE MOBILE NETWORKING

Security and privacy for wireless and mobile systems

Security on all layers



Hacking the wireless world ... to make it more secure

Cars hacked through wireless tire sensors

Researchers have shown that the tire pressure monitoring sensors found in new …

by **Peter Bright** - Aug 10 2010, 10:20pm CEST

65

Privacy

Anonymity

Resilience against censorship

Cyberphysical systems

Security for Software-defined Networks

OpenFlow

Infrastructureless networks, hybrid networks

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Some slides courtesy of J.-P. Hubaux, EPFL

Recommended reading

- The reading that helps you to get ready for the exam

Contact


SECURE MOBILE NETWORKING
TECHNISCHE UNIVERSITÄT DARMSTADT
Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science
SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de
Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de

Copyright Notice