TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Resilient Networking

Thorsten Strufe

Disclaimer: this course has been created with very valuable input from Günter Schäfer, Mathias Fischer, and the members of the Chair.

Dresden, SS 15

Lecture Outline

Who are we?

Organizational matters (Preliminaries)

Course outline

A brief introduction

Who is Who

Professur „Datenschutz und Datensicherheit“

For this lecture:

- Thorsten Strufe (Lectures)
  - INF 3070 / +49 351 463 38247
  - thorsten.strufe [at] tu-dresden.de

Teaching assistants

- This lecture doesn‘t have one.
- Stefanie Roos for some math/darknet parts

Consultation:

- Send me an Email (repeatedly…)

https://dud.inf.tu-dresden.de

What We're Interested In

- Can we prevent surveillance and retain our privacy?
- How can networks be made robust and secure?
- How can you socialize with confidentiality?
- Can we provide competitive (useful and performant) services without snooping on the users?
  - *Social Networking?*
  - *Recommendation Systems?*
  - *Data Mining on confidential data (biomedical!)?*
- How can we analyse this context and develop sustainable solutions (scientifically)?
- With everything getting digital: how can we avoid the next big data-loss desaster? [1] [2] [3] [4]

The fields we're working on

Surveillance Prevention
- Anonymous Communication
- Darknets
- Social network privacy

Cloud Security
- Distributed Clouds
- Secure Computation
- Oblivious Recommenders

Network Security
- Network resilience
- Secure Network Coding
- DoS-resistant streaming

System Security
- Protocol/Service partitioning
- Intel SGX

Data Collection & Analysis
- Crawling and Monitoring
- User behavior understanding
- Dynamic complex graphs
- Inference prevention

What we offer you

FS	Wintersemester	FS	Sommersemester
1		2	Informations- und Kodierungstheorie
3	Betriebssysteme & Sicherheit	4	*Forschungslinie*
5	**BAS-4** *SaC-1* / Kanalkodierung	6	**BAS-4** *SaC-2/Crypto*
7		8	**Vert-4,** ANW/AFT, Beleg *SaC-2/Crypto/Resilient Networking*
9	**Vert-4**, ANW/AFT *FB-Mining*/Kanalkodierung	10	Diplomarbeit

BAS-4:

- **S**ecurity **& C**rypto 1
- **S&C** 2 (PETs)
- Crypto
- Kanalkodierung

Vert-4:

- S&C 1&2
- Crypto
- Resilient Networking
- Mining Facebook
- Kanalkodierung

B-510/B-520:

- **S**ecurity **& C**rypto 1
- **S&C 2** (PETs)
- Kanalkodierung
- Seminare/Praktika

FS	Wintersemester	FS	Sommersemester
B1		B2	Informations- und Kodierungstheorie
B3		B4	
B5	**B-510** Betriebssysteme & Sicherheit	B6	**B-520** Bachelor-Thesis
M1	**BAS-4**	M2	**BAS-4, VERT-4, ANW**
M3	**Vert-4, FPA**	M4	Master-Thesis

Some Words Regarding this Course

Main topic of the course is the *security of deployed, crucial networks, networking functions, and network protocols.*

Considering the Internet: *networking is an essential service, hence the networking infrastructure is/may be the main target of attacks!*

Now what!?

Preliminary Course Overview

1. Introduction
2. Graphs and graph theory
3. Crypto basics (Symmetric/Asymmetric/MACs)
4. Link-Layer Security
5. IPsec
6. Resilient Routing (Attacks on BGP, SBGP)
7. TLS
8. DNS Security
9. DDoS and Countermeasures
10. Resilient Overlay Networks / Darknets
11. Intrusion Detection and Response

Organizational Matters

There will be some ex-cathedra parts, but please ask and discuss as much as possible!

Course Language

- Slides are in English, presentation as you prefer
- => What‘s your language of preference?

Slide history

- Based on several former courses given at TU Ilmenau, Uni Mannheim, and TU Darmstadt
- Heavily derived from „Network Security“ and „Protection of Communication Infrastructures“ of/with Prof. Schäfer in Ilmenau

Organizational matters

Courses
- Mo 14:50 – 15:20
- E010

Exercises
- Wed 9:20 – 10:50
- E009 (starts now, first meeting in CW 18: May 4, prepare *now*)

Exams
- Oral exams, make appointments
- Procedure:
  - Questions available in German (and English upon request)
  - Answers given in German (and English upon request)
- No written material allowed (books, slides, notes)
  - *Except* language dictionaries for non-native speakers (German/English), ***without*** any personal add-ons, handwritten comments, supplements, etc.
  - If needed, we will provide a list of important equations

All necessary information (will be) on the Web site

The Reading Group (Exercises)

Exercise course will be organized as a reading group

- Papers (links) available on the webpage (soon)
- Read papers early…
- One paper with relation to lecture topics will be presented (by a random ***one*** of ***you***!) and discussed (by ***you***!) each week (please take note of the emphasize on ***YOU :-)***)

The Reading Group

Intention of the reading group is to learn

- from good (and bad) scientific papers
- that what others do is mostly no rocket science
- how to read a paper properly
  (for sure not in the order from beginning to the end!)

Different kinds of papers

Papers: the classic form of scientific content spreading, a single contribution

- *Workshops*: Early ideas, WiP, Challenges/discussions ("*Recurring issues with spark-plug electrodes*")
- *Conferences*: concise studies ("*On the electrode shapes in spark-plug design*")

Journal papers: self-contained ("*On spark-plug design*")

Surveys: summarizing a field or research area

The Reading Group – Reviewing Papers

Paper idea

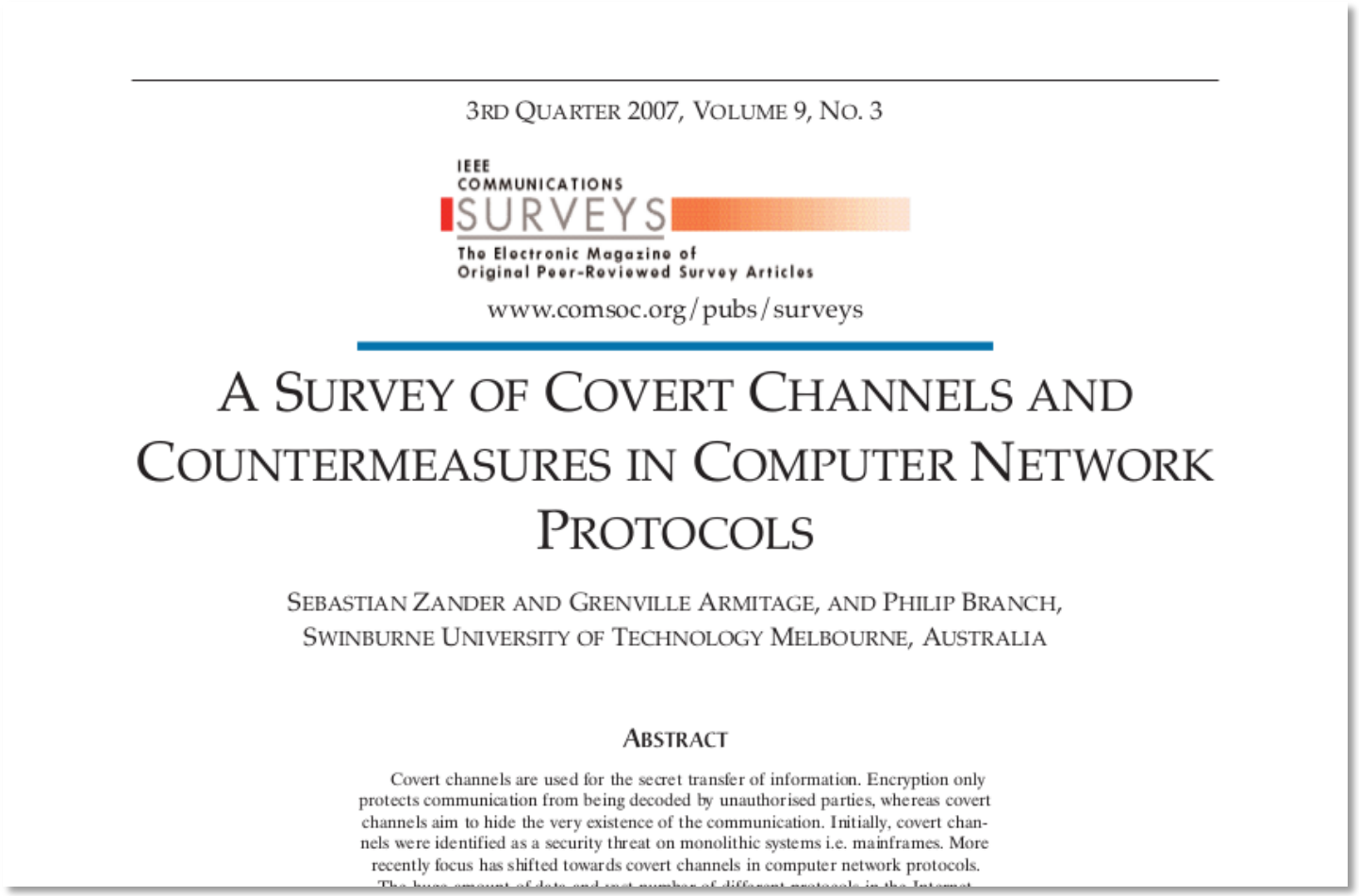
- What is the field of research? What is the motivation of the paper?
- What is the problem the paper tries to solve?
- What is the research question?
- How relevant is this research?
- What is the paper hypothesis?

Paper content

- What are the assumptions of the paper?
- Which definitions are contained?
- What is the idea for solving the problem?
- Which implications does it entail?
- How is the evaluation carried out? What about the results?

Critical acclaim: Merits & Shortcomings

The Reading Group – Reviewing Surveys (1)



3RD QUARTER 2007, VOLUME 9, NO. 3

IEEE COMMUNICATIONS SURVEYS

The Electronic Magazine of Original Peer-Reviewed Survey Articles

www.comsoc.org/pubs/surveys

A SURVEY OF COVERT CHANNELS AND COUNTERMEASURES IN COMPUTER NETWORK PROTOCOLS

SEBASTIAN ZANDER AND GRENVILLE ARMITAGE, AND PHILIP BRANCH,
SWINBURNE UNIVERSITY OF TECHNOLOGY MELBOURNE, AUSTRALIA

ABSTRACT

Covert channels are used for the secret transfer of information. Encryption only protects communication from being decoded by unauthorised parties, whereas covert channels aim to hide the very existence of the communication. Initially, covert channels were identified as a security threat on monolithic systems i.e. mainframes. More recently focus has shifted towards covert channels in computer network protocols.

The Reading Group – Reviewing Surveys (2)

What is the field of research? What is the exact problem domain?

Survey content

- What are the assumptions in the survey? Which definitions are used?
- Aspects, requirements, concepts, properties?
- Which *classification* is used?
- Which implications does each class entail?

Papers are on the web page, start reading ***NOW*** ☺

Critical acclaim

- How convincing are classification and implications?
- Completeness of the survey
- Merits & shortcomings

Material

Slides/recordings will be on the web site

Literature/References

- Schäfer, Roßberg: Network Security
- For crypto: Dan Boneh‘s coursera course

- David Kahn: The Codebreakers
- Simon Singh: The Code Book

Questions?