Privacy-Enhancing Technologies

Lecture series Summer Term 2022 -- The Reading Group

Patricia Guerra-Balboa, Thorsten Strufe

25.04.2022 – KIT/TUD

KASTEL Security Research Labs

The Reading Group (Exercise Course)

- Exercise course will be organized as a reading group
  - Papers (links) available on the webpage (soon, depending on |participants|)
  - 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

- how science works, and how to stay up to date and inform yourselves at the source
- from good (and bad) scientific papers
- that what others do is mostly no rocket science
- how to read a paper properly
  (probably not in the order from beginning to the end!)

How does science work, after all?

- Scientific process of
  - Hypothesize, establish theory, verify (empirically, by proof)
  - Quality control (peer review, replication)

Different kinds of papers

- Papers: the classic form of scientific content dissemination, 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 articles: self-contained ("*On spark-plug design*")

- Surveys: summarizing a field or research area

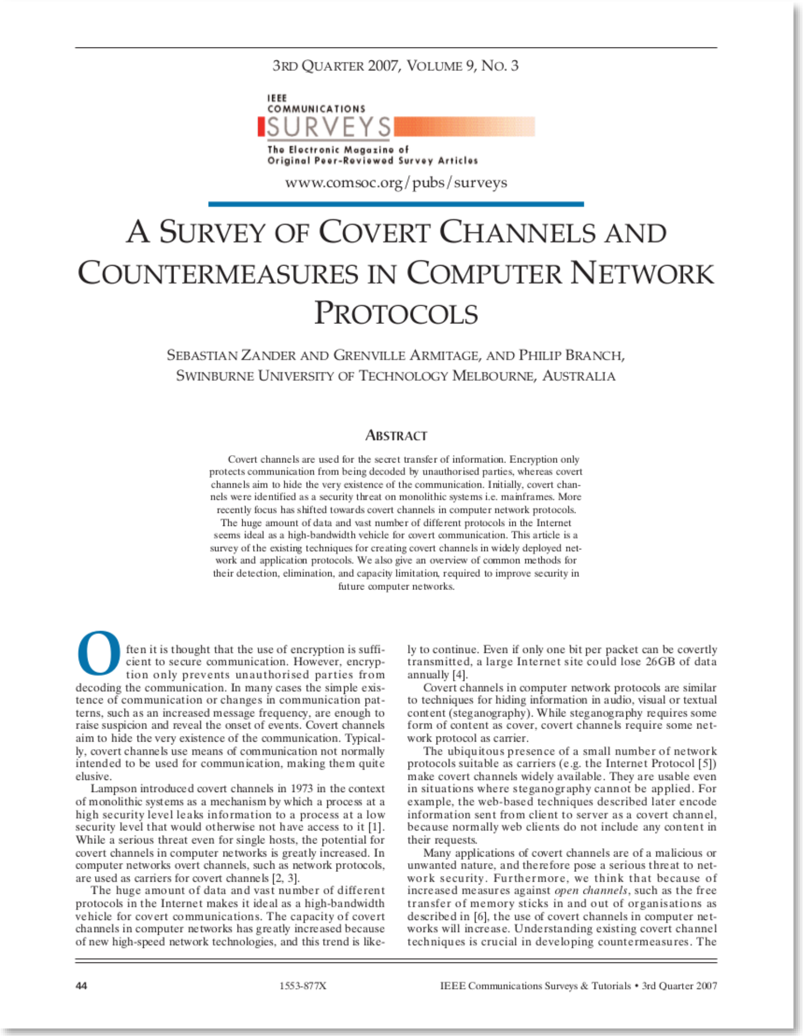
The Reading Group – Reviewing Papers

- Paper idea
  - What is the field of research?
  - What is the motivation of the paper?
  - What is the problem the paper tries to solve/it's innovation?
  - What is the exact research question?
  - What is (are) the paper's hypothes(i|e)s?
  - How relevant is this research?

- Paper content
  - What is the ***claim***, what are the ***assumptions*** of the paper?
  - Which definitions are contained?
  - What is the idea for solving the problem/investigating the phenomenon?
  - Which implications does it entail?
  - How is the evaluation carried out? Does it suffice to demonstrate/substantiate the claims? 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 huge amount of data and vast number of different protocols in the Internet seems ideal as a high-bandwidth vehicle for covert communication. This article is a survey of the existing techniques for creating covert channels in widely deployed network and application protocols. We also give an overview of common methods for their detection, elimination, and capacity limitation, required to improve security in future computer networks.

Often it is thought that the use of encryption is sufficient to secure communication. However, encryption only prevents unauthorised parties from decoding the communication. In many cases the simple existence of communication or changes in communication patterns, such as an increased message frequency, are enough to raise suspicion and reveal the onset of events. Covert channels aim to hide the very existence of the communication. Typically, covert channels use means of communication not normally intended to be used for communication, making them quite elusive.

Lampson introduced covert channels in 1973 in the context of monolithic systems as a mechanism by which a process at a high security level leaks information to a process at a low security level that would otherwise not have access to it [1]. While a serious threat even for single hosts, the potential for covert channels in computer networks is greatly increased. In computer networks overt channels, such as network protocols, are used as carriers for covert channels [2, 3].

The huge amount of data and vast number of different protocols in the Internet makes it ideal as a high-bandwidth vehicle for covert communications. The capacity of covert channels in computer networks has greatly increased because of new high-speed network technologies, and this trend is likely to continue. Even if only one bit per packet can be covertly transmitted, a large Internet site could lose 26GB of data annually [4].

Covert channels in computer network protocols are similar to techniques for hiding information in audio, visual or textual content (steganography). While steganography requires some form of content as cover, covert channels require some network protocol as carrier.

The ubiquitous presence of a small number of network protocols suitable as carriers (e.g. the Internet Protocol [5]) make covert channels widely available. They are usable even in situations where steganography cannot be applied. For example, the web-based techniques described later encode information sent from client to server as a covert channel, because normally web clients do not include any content in their requests.

Many applications of covert channels are of a malicious or unwanted nature, and therefore pose a serious threat to network security. Furthermore, we think that because of increased measures against *open channels*, such as the free transfer of memory sticks in and out of organisations as described in [6], the use of covert channels in computer networks will increase. Understanding existing covert channel techniques is crucial in developing countermeasures. The

The Reading Group – Reviewing Surveys (2)

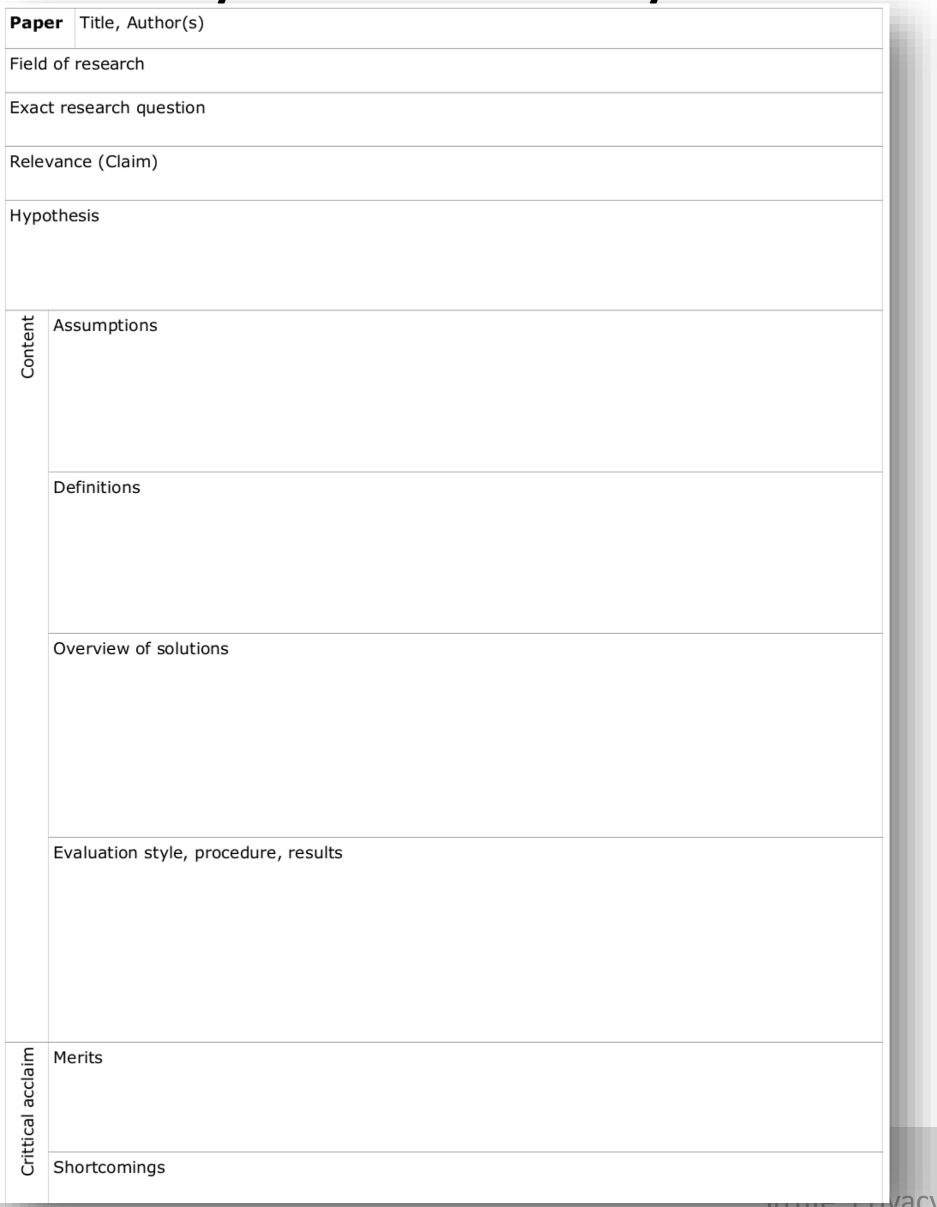
- What is the field of research? What is the exact problem domain?

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

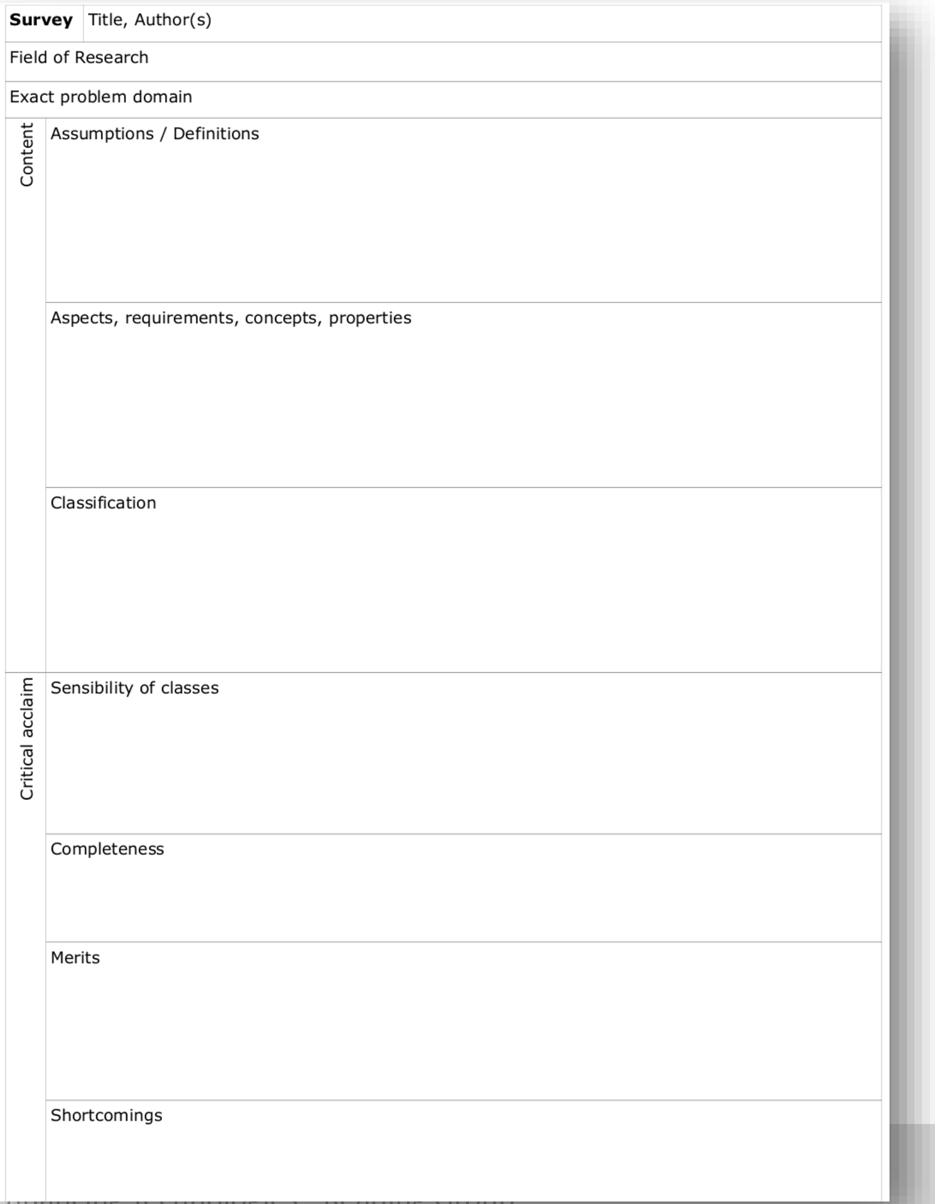
- Critical acclaim
  - How convincing are classification and implications?
  - Completeness of the survey
  - Merits & shortcomings

Also “standardization of knowledge” (SoK)

From your anonymous benefactor…



Paper	Title, Author(s)
	Field of research
	Exact research question
	Relevance (Claim)
	Hypothesis
Content	Assumptions
	Definitions
	Overview of solutions
	Evaluation style, procedure, results
Critical acclaim	Merits
	Shortcomings



Survey	Title, Author(s)
	Field of Research
	Exact problem domain
Content	Assumptions / Definitions
	Aspects, requirements, concepts, properties
	Classification
Critical acclaim	Sensibility of classes
	Completeness
	Merits
	Shortcomings

find this template on the web page…

Organization

- Please help us with the organization:
  - One reading group can host students with up to 16 papers
  - Tuesday/Thursday 14:00h are the scheduled slots

- Alternatives:
  - Tue 2PM hybrid, starting May 10th
  - Not everybody presents a paper
  - Two reading groups (Tue/Thu 2PM, offline/online?)

- Please email us if you would like to participate until Tue, 3.5. 18:00h !
  - thorsten.strufe[at]kit.edu

Questions?