Project Info

CSIE 7190 Cryptography and Network Security, Spring 2019

https://ceiba.ntu.edu.tw/1072csie_cns

cns@csie.ntu.edu.tw

Hsu-Chun Hsiao

National Taiwan University

Timeline

Deadline	Task
4/09	分組名單 (4-5人一組) 1-2個有興趣的主題
5/07	Project title & proposal
6/11, 6/18	Final project presentation
6/25	Final project report

Course projects logistics

Aim high, but be realistic about 3-month work

Encourage to explore any **security-related** topics (including those not taught in class)

Highly encourage to bring security thoughts to your current research or in familiar contexts

Don't try to learn new non-security fields

Grade based on novelty, depth, correctness, clarity

Project Ideas

Project ideas: 3 broad directions

1. Attack and analyze (**Attack your own devices only! or attack them “mentally”)
2. Design and build
3. Measure and/or survey

以往年的期末報告為例

Attack and analyze

NTU Vote: Attack and Defense

Attacks on the Judge System

Studying on VPN – NTU SSLVPN

電子發票的安全性議題

A Practical Attack on EasyCard using Android Device

I Want Your Password

Juice Jacking Implementation using Embedded Device

Hacking Android Apps!

Flash Crowd Mimicking Attacks with Implementation and Analysis in Heterogeneous Network

Internationalized Domain Names (IDN) phishing

Don’t: run existing tools only
Better: find new attack vectors, analyze new systems, …

Evil-Twin Attack

Bash vulnerability – Shellshock

NFC: Potential Threats and Attacks

WooTalk 安全性分析

台大校園網站安全檢測

Website Security against Brute Force Attack

Survey of Antivirus

Clickjacking

以往年的期末報告為例

Design and build

Privacy-preserving data mining
Secure I-Voting System
I-voting System Implementation
Location Anonymity
Bitcoin Address Management
Cyber Hunting System
Sound Pay: A Better Choice for Mobile Payment
The Study of Batch Verification for Vehicular Communications
Defending Against Browser-Based DDoS
End to End Secured Realtime Chat Room
AdvertiXmentsert: The Extreme Ad Terminator
Learning to Defend -- From ML to Security
Learning to Detect - From ML to Malware Family

Don’t: invent your own crypto
Better: design and build secure systems with better performance, usability, functionality, etc.

以往年的期末報告為例

Measure and/or survey

Shortened URLs

Security Issues of Short URLs

Deep web and darknet survey

When Ransomware Becomes Service

An Examination of Ways Against Ransomware

Risk Analysis and Hack in Android Apps

Android Malware Survey and Design

電子貨幣初探及相關資訊安全議題

A Survey on DoS: Attack and Defence

Don’t: write an encyclopedia
Better: build tools for large-scale measurement, provide new findings, systematical reviews and evaluation, …

Investigation and Study on Browser Hijacking

WarWalking NTU: A Survey of NTU WiFi

Survey and Experiments on Wi-Fi Vulnerabilities

Common WiFi vulnerability investigation

Malicious Mining Program in Browser Survey

Mirai analysis and IoT Mitigation

以我們lab為例

DDoS/SDN security

Privacy-preserving cloud-based DDoS defense

Defending against browser-based DDoS attack

Large flow detection & flow monitoring algorithms

Securing SDN data plane

Mitigating flash crowds

Pulsating DDoS attack and defense

Bandwidth allocation for DDoS defense

Mitigating denial of service using proof of stake

Estimating whether a website is protected by DDoS protection services and what's the strength of protection

以我們lab為例

IoT security

IFTTT-related security issues

Using VLC for IoT security

USB security

OAuth issues

Smart grid security

Efficient key management for dynamic IoT

Virtual IoT patching using SDN

Detecting bitcoin mining bots

Investigating AR security issues

以我們lab為例

Software & Web Security

Lightweight instrumentation for fuzzing

Solver selection for symbolic execution

Handling path explosion in symbolic execution

Heap exploitation

Analyzing bitcoin wallets

Analyzing cryptocurrencies and smart contracts

Ticket scalping bot detection and forensics

Security oriented API crawler

HTTPS adoption measurement

Proposal

Your proposal should contain…

Problem description: What is the problem that you are trying to solve? Clearly state your attacker model and security properties.

Related work: How is it done today, and what are the limits of current practice?

Plan

- What is your initial approach? What is your plan for evaluation?
- Timeline
- Deliverables (e.g., a software prototype, a case study, a formal proof, …)

Length: 2 pages

Proposal grading rubrics

Problem description (30%)

- What is the problem that you are trying to solve?
- Clearly state your attacker model and security properties.

Related work (30%)

- How is it done today (請提供reference)
- What are the limitations of current practice?

針對上述想解決的問題，
現今的解法有什麼不足，
希望在此project有所突破？

Plan (20%)

- What would be your approach?
- What is your plan for evaluation?(佐證你們的方法比前人好)

Timeline (10%)

Deliverables (e.g., a software prototype, a case study, a formal proof, ...) (10%)

Final Presentation

Final presentation format

台上的講者要做什麼?

- 每組15分鐘presentation + 5分鐘 Q&A
- 預先準備可以討論的點 (如果台下沒太多問題，也可以用這個時間和大家聊聊甘苦談，或是有什麼問題可以問大家)

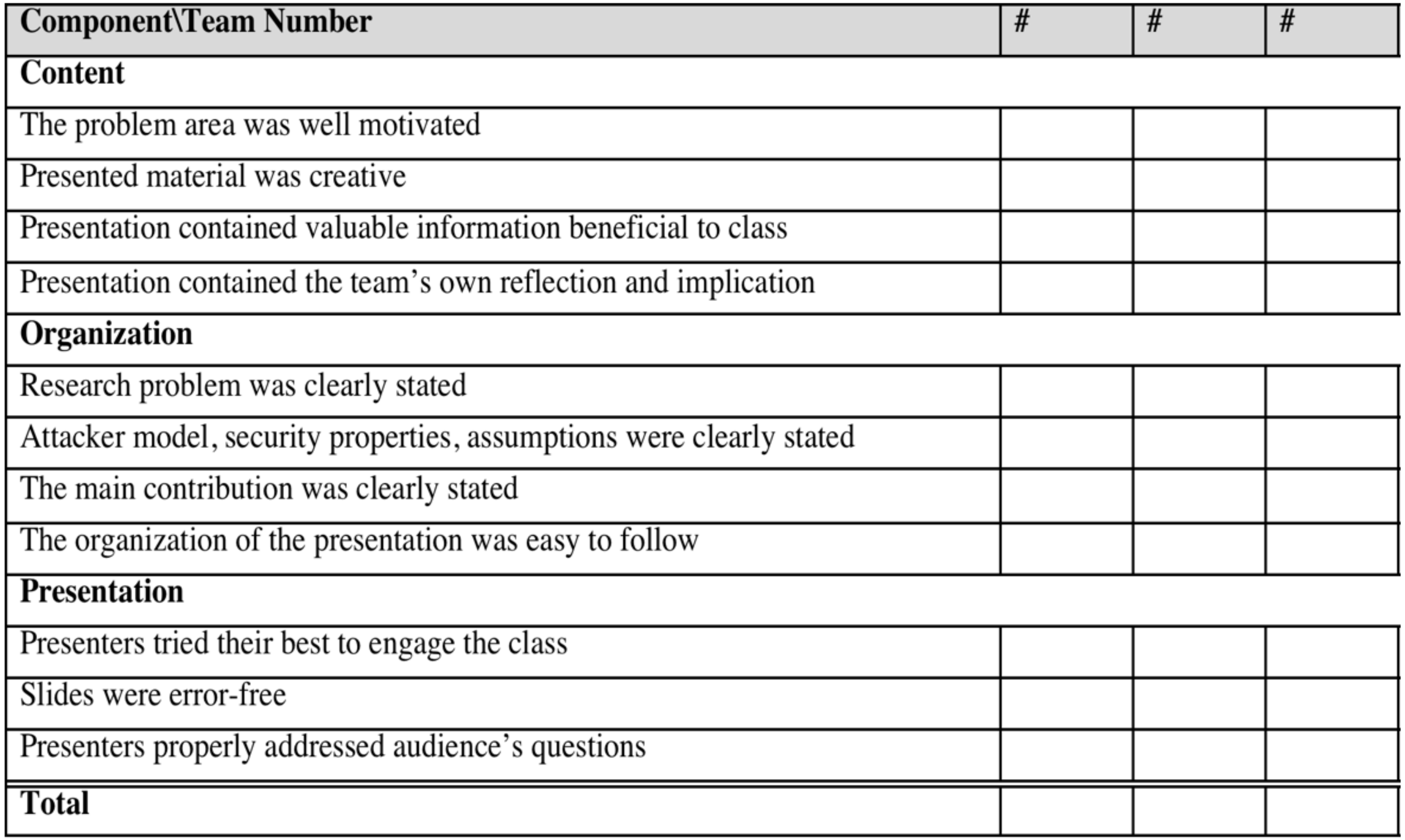
在台下的同學也不能閒著

- 問問題、提出建議
- 以組別為單位填寫報告評量表 (Presentation Evaluation Form)

報告評量表 Presentation Evaluation Form

組別互評 (50%) + TAs & instructor (50%)

1 = Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree



Component\Team Number	#	#	#
Content			
The problem area was well motivated			
Presented material was creative			
Presentation contained valuable information beneficial to class			
Presentation contained the team's own reflection and implication			
Organization			
Research problem was clearly stated			
Attacker model, security properties, assumptions were clearly stated			
The main contribution was clearly stated			
The organization of the presentation was easy to follow			
Presentation			
Presenters tried their best to engage the class			
Slides were error-free			
Presenters properly addressed audience's questions			
Total			

Confidential form only accessible by TA & me.

Final report format

4-6 pages in two-column ACM style

- https://www.acm.org/sigs/publications/proceedings-templates

中英文皆可

根據口頭報告時的Q&A和建議做調整

繳交期限: 6/25 23:59 (no late submission!)

同時要個別繳交個人互評表 (Peer & Self Evaluation Form)

These sections are required in your report:

1. Title
2. Abstract
3. Introduction
4. Problem definition
5. **Results**
   - Depending on the nature of your topic, you might have section(s) like “System Design”, “Results”, “Evaluation”...
6. Related work
7. Conclusion and future work
8. References

Final report rubrics

The grade will depend on the *originality, correctness, clarity, depth*

I’ll have a higher standard for larger groups

Point distribution (忘記寫的話整個都沒分)

- Abstract (5%)
- Introduction (15%)
- Problem definition(10%)
- Results (50%)
- Related work (10%)
- Conclusion and future work (5%)
- References (5%)

Final report rubrics: 踩點建議

Abstract (5%)

Introduction (15%)

- **Motivation**: Why does the problem area matter?
- **Research problem**: What is the specific problem the paper addressed?
- **Approach**: What is the approach used to solve the problem?
- **Comparison**: How is your work different from others?
- **Contribution**: What are the main contributions of your paper?

Problem definition (10%): 1) formally define your problem, 2) describe your attacker model and assumptions.

Results (50%)

Related work (10%): review ≥ 6 scholarly resources

Conclusion and future work (5%)

- How would you improve or extend the work if you had more time?
- What are the broader impacts of this proposed technology?

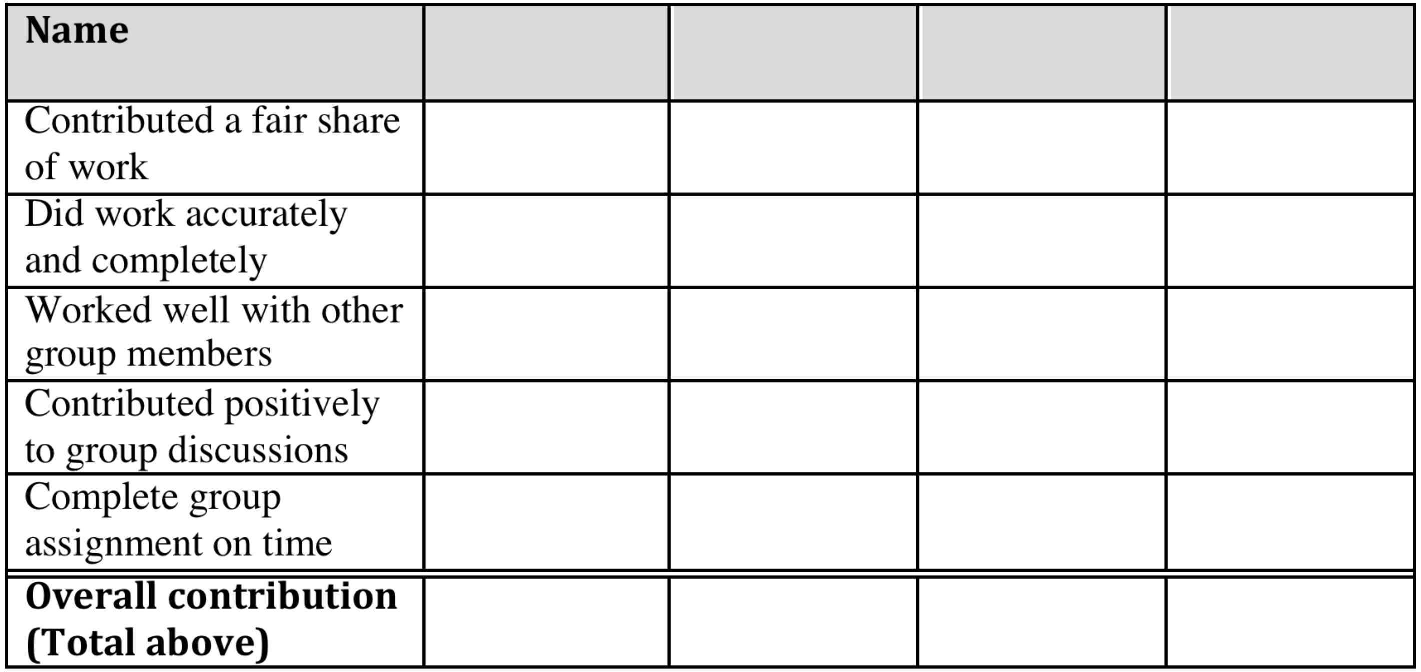
References (5%)

個人互評表 Peer & Self Evaluation Form

Confidential form only accessible by me

Evaluate the quality of each group member’s work

1 = Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree

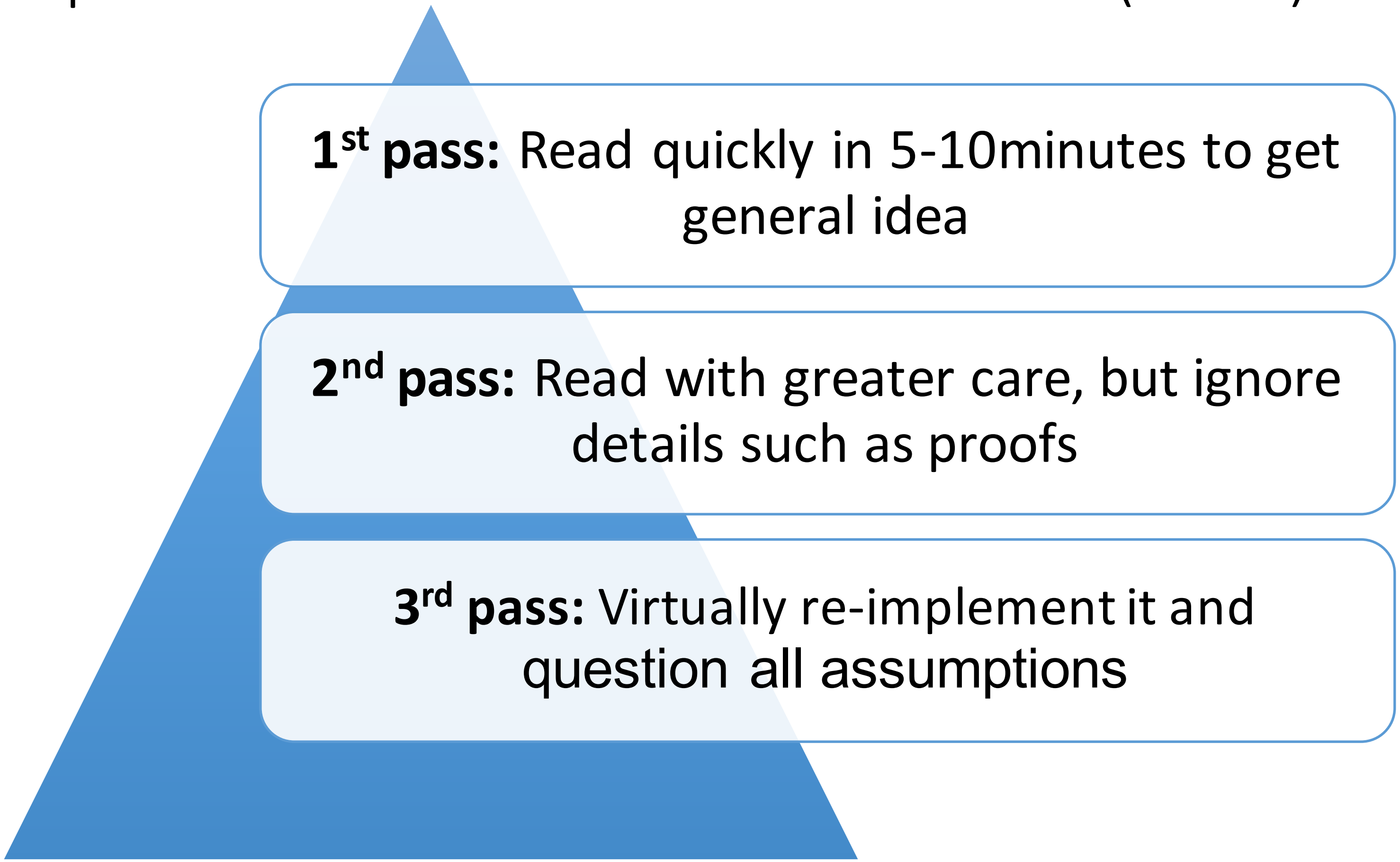


Name				
Contributed a fair share of work				
Did work accurately and completely				
Worked well with other group members				
Contributed positively to group discussions				
Complete group assignment on time				
Overall contribution (Total above)				

Resources

How to read a paper: A three-pass approach

Keshav, S. "How to read a paper." ACM SIGCOMM Computer Communication Review 37.3 (2007): 83-84.



1st pass: Read quickly in 5-10minutes to get general idea

2nd pass: Read with greater care, but ignore details such as proofs

3rd pass: Virtually re-implement it and question all assumptions

1st pass: bird's eye view in 5-10 minutes

Quick scan of the paper

- Title, abstract, introduction
- Section and subsection headings
- Conclusions
- Glance over references

Answer the five C's

- **Category**: What type of paper is it?
- **Context**: Where does it fit in?
- **Correctness**: Do assumptions make sense?
- **Contributions**: What are the main ones?
- **Clarity**: Is it well-written?

2nd pass: read in greater care

Spend ~1 hour to read in greater care, but ignore details

Write key points and make comments

Figures, diagrams, illustrations, graphs

Mark relevant unread references

After this pass, you should be able to summarize main story and identify main supporting evidence

3rd pass: virtually re-implement the paper

Can take one or more hours

Virtually re-implement the paper

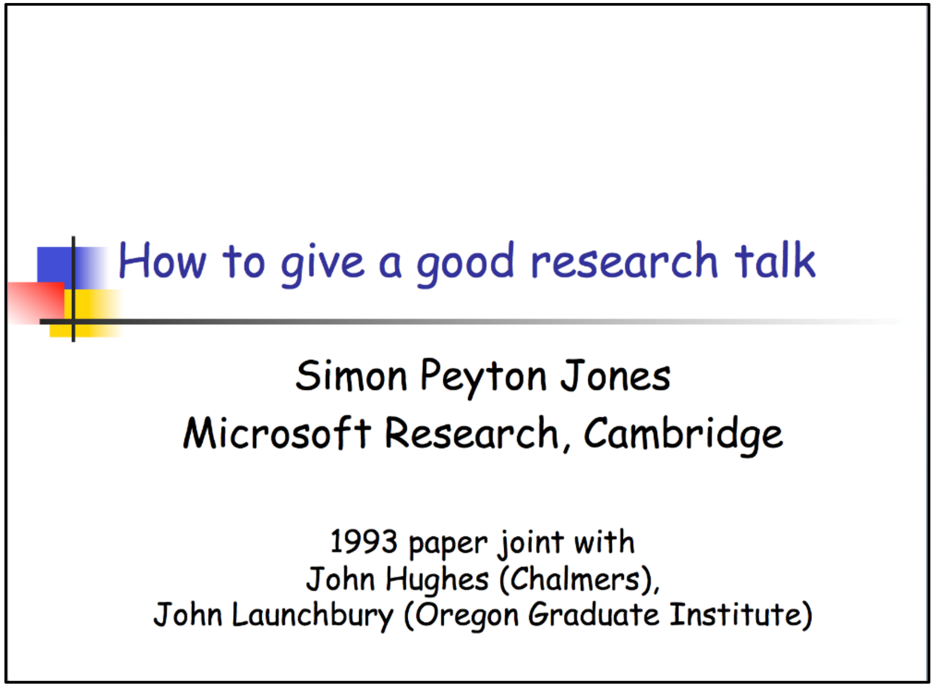
Identify and challenge assumptions

Write down ideas for future work

After this pass, you should be able to

- Reconstruct entire structure of paper from memory
- Identify strong and weak points
- Pinpoint implicit assumptions, missing citations to related work, issues with experimental or analytical techniques

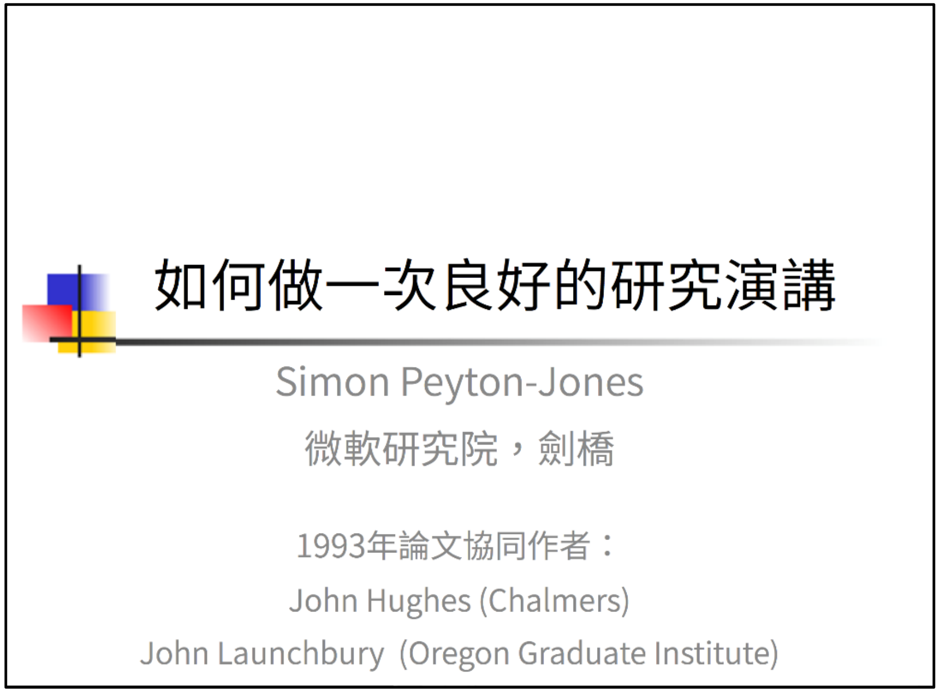
How to give a good research talk



How to give a good research talk

Simon Peyton Jones
Microsoft Research, Cambridge

1993 paper joint with
John Hughes (Chalmers),
John Launchbury (Oregon Graduate Institute)



如何做一次良好的研究演講

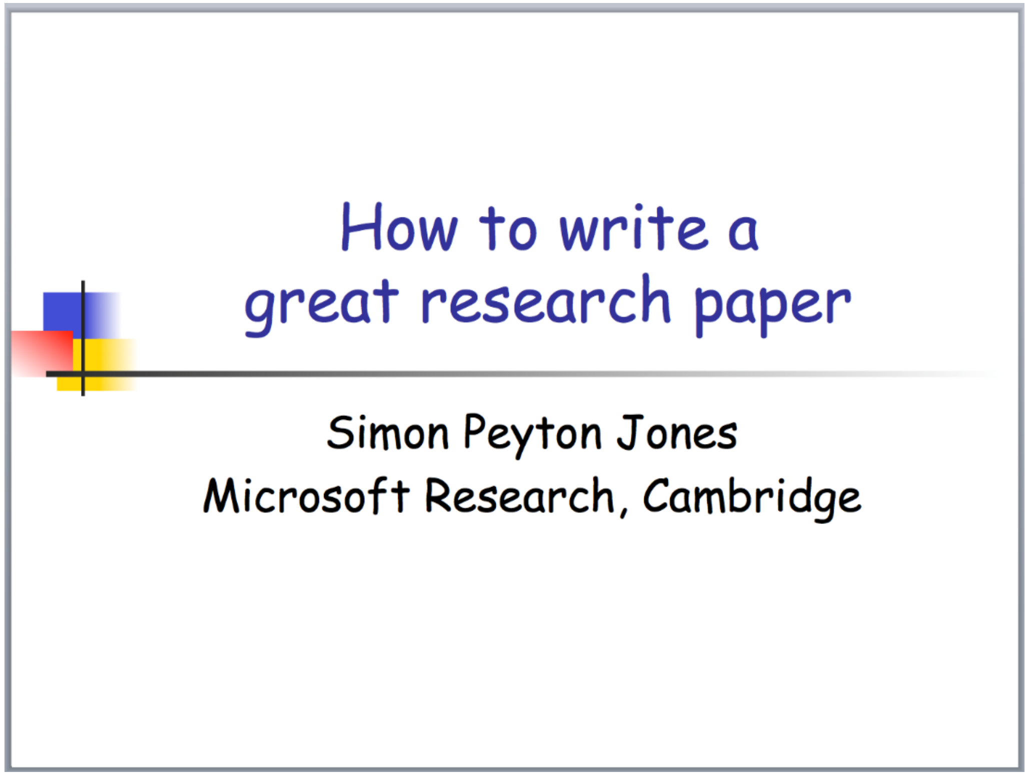
Simon Peyton-Jones
微軟研究院，劍橋

1993年論文協同作者：
John Hughes (Chalmers)
John Launchbury (Oregon Graduate Institute)

Watch the video, highly recommended!
http://research.microsoft.com/en-us/um/people/simonpj/Papers/giving-a-talk/giving-a-talk.htm

Translated by 唐鳳
https://speakerdeck.com/audreyt/ru-he-zuo-ci-liang-hao-de-yan-jiu-yan-jiang

How to write a good research paper



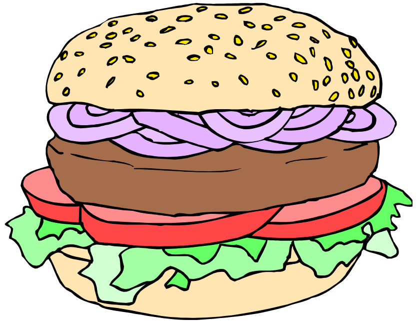
How to write a great research paper

Simon Peyton Jones
Microsoft Research, Cambridge

Watch the video, highly recommended!
http://research.microsoft.com/en-us/um/people/simonpj/Papers/giving-a-talk/giving-a-talk.htm

What your talk is for

Your paper = **The beef**



Your talk = **The beef advertisement**

Do not confuse the two

By Simon Peyton-Jones