

How to write top conference papers in security?

Yongdae Kim

Security Top Conferences

□ Security

- ISOC Network and Distributed System Security (NDSS)
- IEEE Symposium on Security & Privacy (S&P, Oakland)
- Usenix Security
- ACM Computer and Communication Security (CCS)

□ Crypto

- IACR International Cryptology Conference (Crypto)
- IACR European Cryptology Conference (EuroCrypt)

Other Related Top Conferences

- ❑ Computer architecture: ASPLOS, ISCA, MICRO
- ❑ AI, Machine Learning: AAAI, ICML, KDD, NIPS, WWW
- ❑ Computer networks: SIGCOMM, NSDI
- ❑ Mobile computing: MobiCom, MobiSys
- ❑ Measurement: IMC
- ❑ Operating systems: OSDI, SOSP
- ❑ Programming languages: PLDI, POPL
- ❑ Human-computer interaction: CHI

Acceptance Rate

	NDSS	S&P	Usenix Sec	ACM CCS
2021	15.2% (573)	12.1% (952)	18.7% (1316)	22.3% (879)
2020	17.4%	12.4%	16.1%	16.9%
2019	17%	12%	15.5%	16%
2018	21.5%	11.5%	19.1%	16.6%
2017	16%	13%	16.3%	17.9%
2016	15.4%(60/389)	13.3%(55/413)	15.6%(72/463)	16.5%(137/831)
2015	16.9%(51/302)	13.5%(55/407)	15.7%(67/426)	19.8%(128/646)
2014	18.6%(55/295)	13%(44/334)	19%(67/350)	19.5%(114/585)
2013	18.8%(47/250)	12%(38/315)	15.9%(44/277)	19.8%(105/530)

Topic Selection: Red Ocean

- Many Red-Ocean-Area
 - Ex: Android, Software Security, System Security
 - Excelt a few long term open problems, fast moving area
 - 100 related works
 - Hall way discussion during academic conferences
 - Program committee members
 - The most important thing: Up to date information, ...

Topic Selection: Blue Ocean

- ❑ “volte security cellular”, “3d printer security”, “medical device security”, “drone security”, ...
- ❑ What I have but no one in the world has?
 - Data, Network, Equipment, Infra, New Area, ...
- ❑ Less competitive area, less attention
- ❑ New area or tech paper is easier
 - 2nd paper, 3rd paper?
- ❑ Making new area is difficult.

Topic: Blue Ocean in Red Ocean

- ❑ Hard to find, but
- ❑ Once you find one, you may get best paper award + many citations follow
- ❑ Ex) Bring research from other areas to security
 - PL+Sec, Compiler+Sec, Machine learning+Sec...
 - Sensor hacking, Low level Arch ... (Blue ocean)
 - Hard part is how to convince security researchers

How to do Blue Ocean Research

- ❑ Most security people don't know such area.
- ❑ Sensor, Complex Network Analysis, Low Level HW,
- ❑ Background section is important
- ❑ Encourage people to read the paper after understanding terms
- ❑ Easy to understand evaluation
 - Rocking drone
 - Row hammer to get root permission
 - Bitcoin attacks earn money

Attack vs Defense paper

□ Attack Paper

- Target: Security as well as top conference in other areas too
- In service, many users, novel attacks, ...
- Intro, Background, Attack Overview, Attack Design, Experiment, ...
- New attack paper = Finding new problem in science
 - » High citation

□ Defense paper

- Defense against attack paper in security conferences
- Fast, low overhead, not incurring new attacks, easy to use, novel, ...
- In depth literature reviews
- Writing defense paper in Red Ocean area is difficult

Problem first or solution first?

- ❑ Properly motivated papers are easy to write
- ❑ However, sometimes 1) your solution does not solve the original problem or 2) finding problem after finding solution
 - 1) Be careful with a tunnel view
 - 2) Sometimes, you need to find a new, good problem
 - » Be creative
 - » You might need new evaluation

Hunting Ideas

- ❑ All of the above +
 - Follow news
 - Check titles of papers in other areas
 - Presentation from Hacking conferences such as Blackhat, Defcon
- ❑ Need detailed analysis after pick your target
- ❑ Check every attack vectors
 - Drone: GPS, Sensor, Telematics, Software, Firmware update, OS, Fail Safe
- ❑ What is new?
 - Related Work, Methodologies, results, performance...

Organization

- ❑ Pick a paper most similar to what you want to write
- ❑ Think about storyline
 - Top to bottom
 - paragraphs
- ❑ Intro – Background - Overview and Target System – Attack model – Vulnerabilities and Exploits – Evaluation – Discussion – Related Work* - Conclusion

Title, Abstract

- ❑ Sexy title.
 - Frying PAN: Dissecting Customized Protocol for Personal Area Network
 - Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE
 - Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane
 - Fuzzle: Making a Puzzle for Fuzzers
 - Platform-Independent Programs
- ❑ Title is deeply related with the reviewer assignment: Most PCs bid with title (and sometimes abstract)
- ❑ Abstract
 - Title => Abstract => Intro => Background
- ❑ All terms must be defined before being used

Intro

- ❑ Background, definition, history, problem, solution, evaluation, lessons learned, organization
- ❑ As if it contains a whole paper
- ❑ Abstract => 1 min elevator pitch, Intro => 5 min pitch
- ❑ May be better to write after writing other parts
 - May write it first to decide the tone of the whole paper (and revise it after you are done)

Background

- ❑ Not my contributions
- ❑ Necessary to understand the paper
- ❑ Existing theory, target area, target system, ...
- ❑ Boring if too long

Attack Model

- ❑ What attacker
- ❑ Good attack papers assume weak adversary
- ❑ System assumptions are added

Overview

- ❑ Based on attack model and system assumptions
- ❑ Overview of the overall attacks or systems
- ❑ Needed only if it is complicated

Vulnerabilities and Exploits

- ❑ Introduce analysis methods based on background
- ❑ Individual vulnerabilities
 - How you find them
- ❑ How these vulnerabilities can be exploited to a serious attack
 - Causes and results
 - Better to be serious

Evaluation

- ❑ Very important
- ❑ Theoretical evaluation, Experimental results, Empirical results, Numerical results, ...
- ❑ Include everything readers might be interested
- ❑ People suspect with missing evaluation
- ❑ Comprehensive and precise

Discussion

- ❑ Every paper has limitation
- ❑ Criticize yourself before reviewers do
- ❑ Be frank
 - Argue that the limitation is not serious
- ❑ Don't skip if you feel uncomfortable
 - Tell you advisor

Related Work and Bibliography

- ❑ Very very important
- ❑ Why we are new
- ❑ Academic papers, Presentations from hacking conferences, news, ...
- ❑ Some organizations
- ❑ Papers from PC members ;-)

Concluding Remarks and Future Work

- ❑ Summary
- ❑ Lessons learned
- ❑ Future direction

Responsible Disclosure and Open Source

- ❑ Korea: KISA, US: CERT
 - Avoid law suit, follow ups
- ❑ Be ethical
 - And be legal
- ❑ Open Source Release

After submitting paper

- ❑ Don't just wait
- ❑ Try to improve it
- ❑ Write much and cut later

Questions?

□ Yongdae Kim

- email: yongdaek@kaist.ac.kr
- Home: <http://syssec.kaist.ac.kr/~yongdaek>
- Facebook: <https://www.facebook.com/y0ngdaek>
- Twitter: <https://twitter.com/yongdaek>
- Google “Yongdae Kim”