Quick Overview of Recently Released Papers at Top Cybersecurity Venues

ANALYZING PLOTS AND DETERMINING NEXT STEPS IN RESEARCH

Sergio Esposito

Goals

- Categorizing papers to get a grasp of trending topics at top cybersecurity venues;

- Determining what others researchers are currently working on;

- Understanding how different topics evolved throughout the years, to distinguish promising topics from saturated ones;

- Carefully selecting a research topic to develop further.

Taxonomy

The first step towards all listed goals was understanding how many major topics can be identified, looking at papers discussed within a single conference.

We therefore identified **11** different categories.

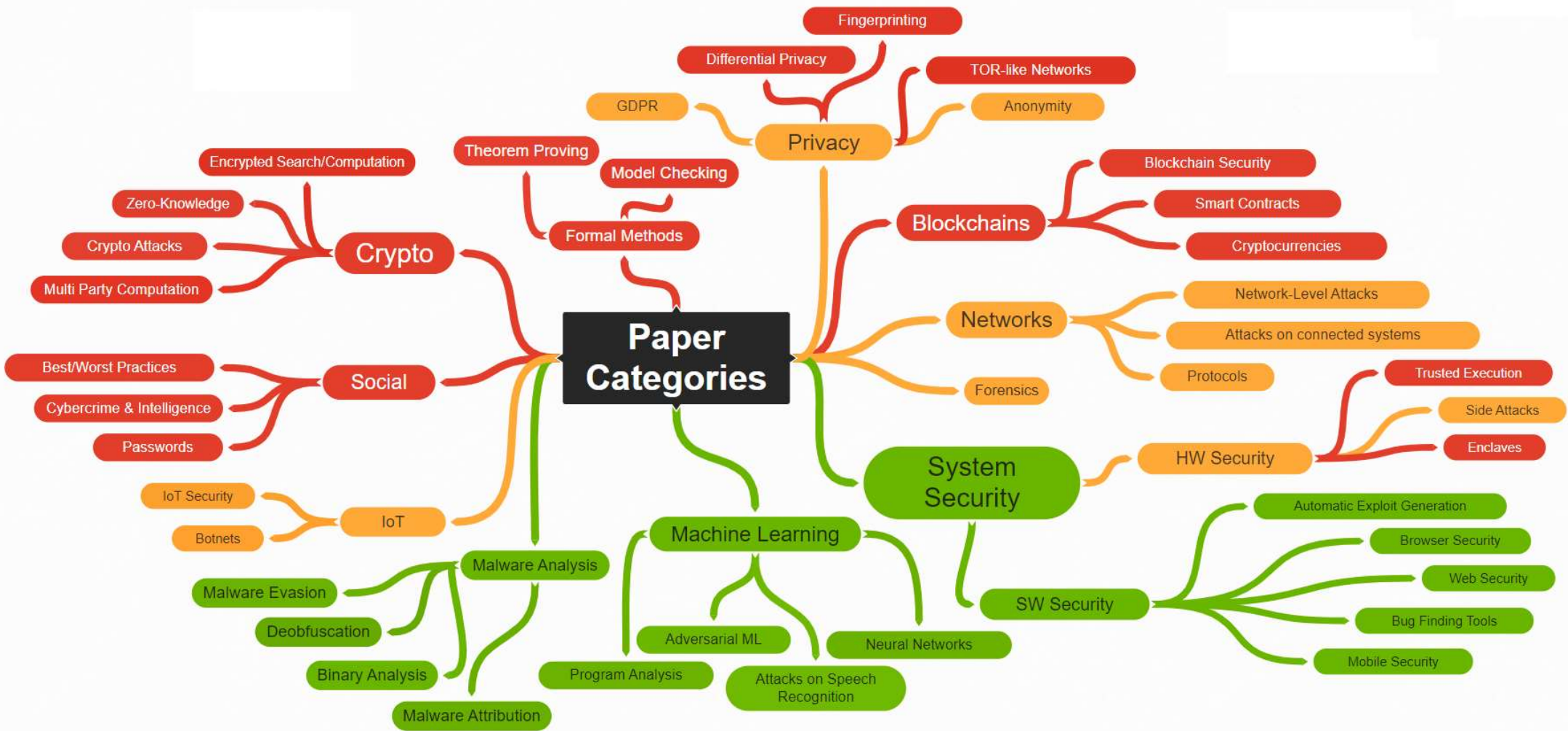|		
Cryptography		**Machine Learning**
	Networks	
Formal Methods		**IoT**
	Forensics	
Privacy		**Social**
	System Security	
Blockchains		**Malware Analysis**

Taxonomy - 2

Every paper belongs at least to one category, with the most «complex» paper being assigned to **four** categories. Of all the **1018** analyzed papers, only **3** did not find place in any of the mentioned categories: being those papers **< 0.003%** of the total set, they have been left uncategorized.

For **10** categories out of the **11** listed, we were able to identify some subcategories.

These subcategories are by no means exhaustive, and are just one of the possible classifications for the analyzed papers.

Paper Categories

- **Privacy**
  - Fingerprinting
  - Differential Privacy
  - GDPR
  - TOR-like Networks
  - Anonymity
- **Crypto**
  - Encrypted Search/Computation
  - Zero-Knowledge
  - Crypto Attacks
  - Multi Party Computation
- **Formal Methods**
  - Theorem Proving
  - Model Checking
- **Blockchains**
  - Blockchain Security
  - Smart Contracts
  - Cryptocurrencies
- **Networks**
  - Network-Level Attacks
  - Attacks on connected systems
  - Protocols
  - Forensics
- **HW Security**
  - Trusted Execution
  - Side Attacks
  - Enclaves
- **Social**
  - Best/Worst Practices
  - Cybercrime & Intelligence
  - Passwords
- **IoT**
  - IoT Security
  - Botnets
- **Malware Analysis**
  - Malware Evasion
  - Deobfuscation
  - Binary Analysis
  - Malware Attribution
- **Machine Learning**
  - Adversarial ML
  - Program Analysis
  - Attacks on Speech Recognition
  - Neural Networks
- **System Security**
- **SW Security**
  - Automatic Exploit Generation
  - Browser Security
  - Web Security
  - Bug Finding Tools
  - Mobile Security

Taxonomy Mind-map

For categories, a greater box corresponds to more papers related to that subject. This does not hold true for subcategories.
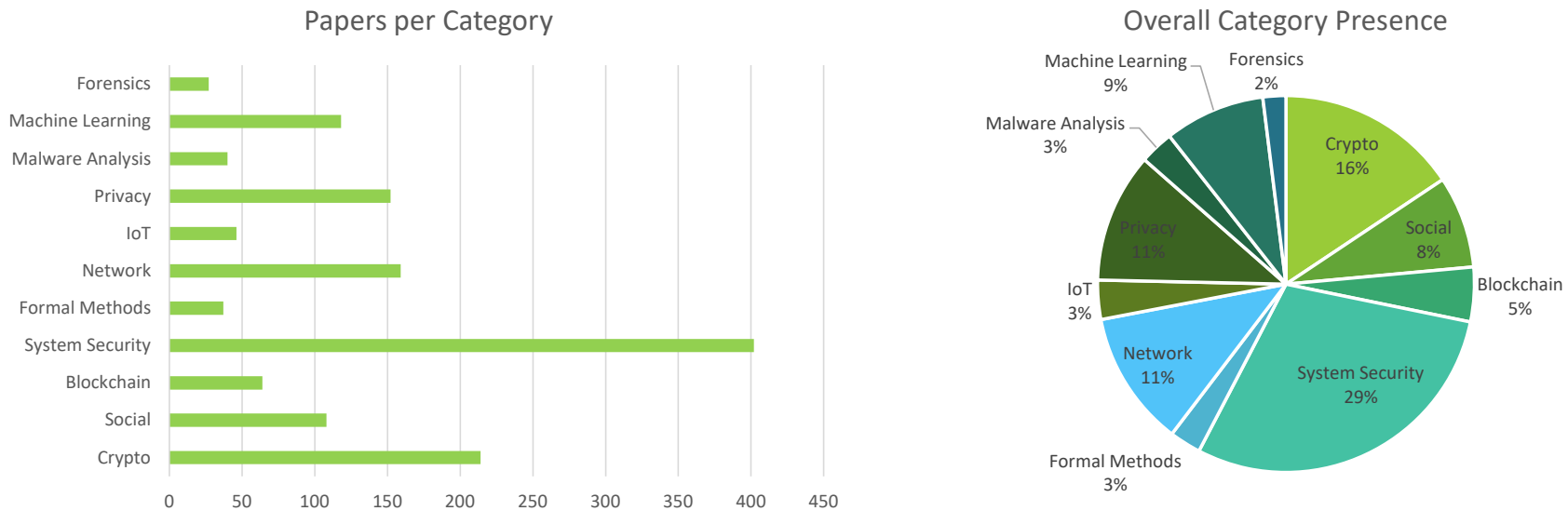
Colours are related to the personal interest in that research field.

Red: not interested;
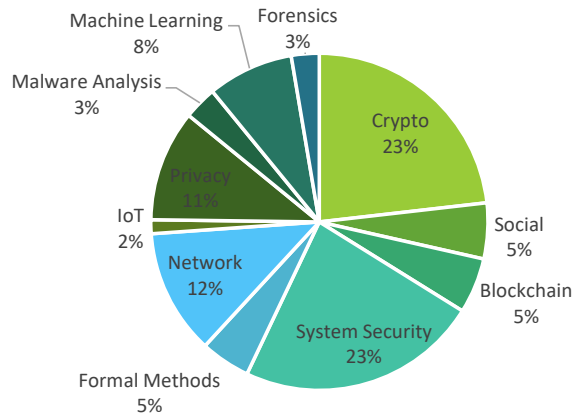
Orange: rather interested;

Green: very interested.

Category Presence through all venues

Papers per Category
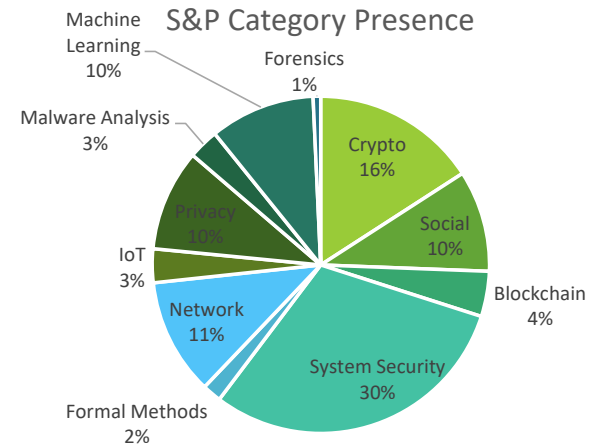

Overall Category Presence

Plots hint at System Security being the most active category. It may indicate saturation of the research field and/or vastness of research opportunities in that field. Crypto is leading after SSec. ML, Privacy, Networks and Social are in the middle tier. Forensics, Malware Analysis, IoT, Formal Methods and Blockchain are in the bottom tier for presence. This may indicate lack of interest from such venues or, most likely, less researchers working on those topics.
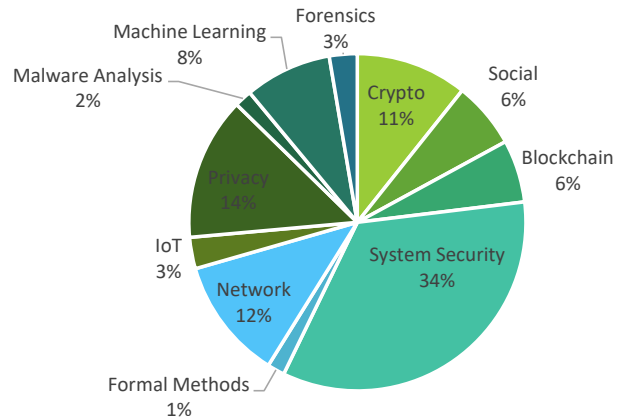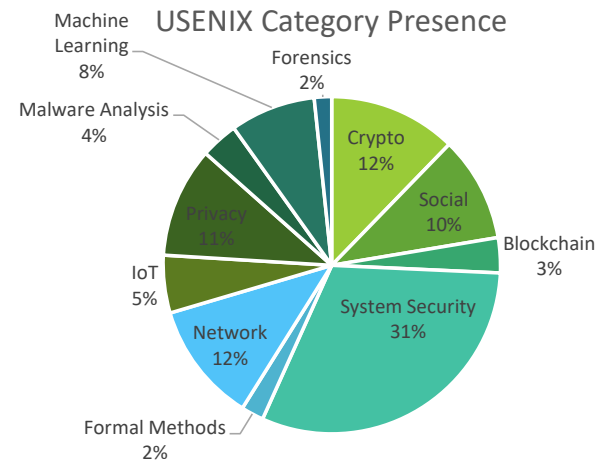
Category Presence per venue

CCS Category Presence

Forensics 3%
Machine Learning 8%
Malware Analysis 3%
Privacy 11%
IoT 2%
Network 12%
Formal Methods 5%
System Security 23%
Blockchain 5%
Social 5%
Crypto 23%

S&P Category Presence

Machine Learning 10%
Forensics 1%
Malware Analysis 3%
Privacy 10%
IoT 3%
Network 11%
Formal Methods 2%
System Security 30%
Blockchain 4%
Social 10%
Crypto 16%

NDSS Category Presence

Forensics 3%
Machine Learning 8%
Malware Analysis 2%
Privacy 14%
IoT 3%
Network 12%
Formal Methods 1%
System Security 34%
Blockchain 6%
Social 6%
Crypto 11%

USENIX Category Presence

Machine Learning 8%
Forensics 2%
Malware Analysis 4%
Privacy 11%
IoT 5%
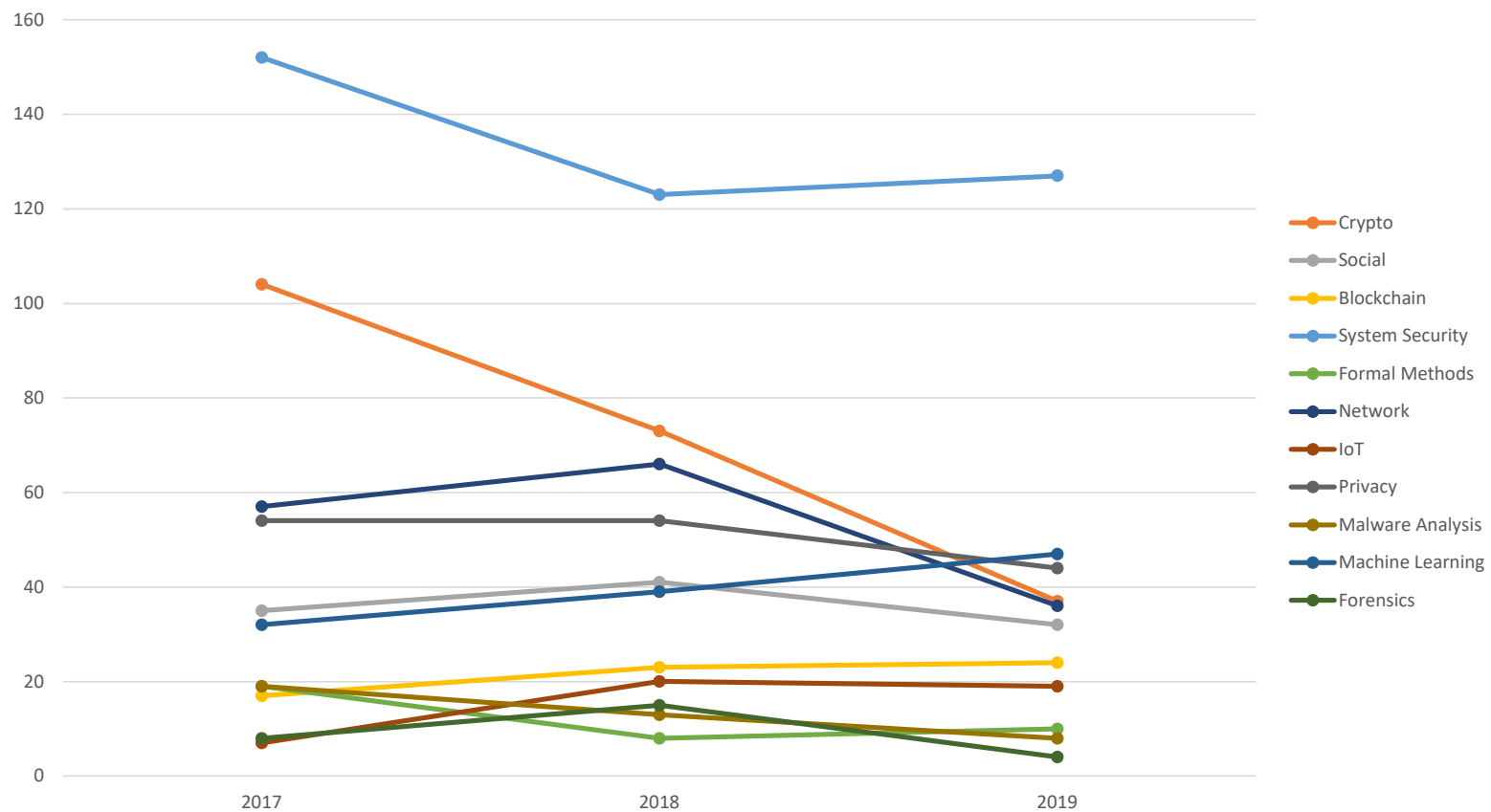Network 12%
Formal Methods 2%
System Security 31%
Blockchain 3%
Social 10%
Crypto 12%

Papers per Category, per Year

Crypto papers dramatically decreased in number over two years. Network-related papers seem to go the same way. IoT and Machine Learning are slowly gaining interest: this might indicate that more researchers are approaching the field or that they are achieving more milestones, or also that venues are now more interested in these topics than they were before. Other fluctuations are rather negligible.

Future improvements

- **Parametrizing the worksheet to automate compilation of fields:** this work was mostly done manually and it was rather time-consuming.

- **Including citation count and related plots:** they could be used not only to rank papers, but also to measure how useful was past work in the different fields, how many researchers are following those topics or doing research on them and how much awareness has been developed in the various categories.

- **Getting more plots done:** more lines, cakes and heatmap could help in determining which fields are more active or effective than others, also observing changes in time.

- **Comparison with similar works**, f.e. *«A Data-Driven Reflection on 36 Years of Security and Privacy Research»*.