Anna Sperotto

a.sperotto@utwente.nl
http://annasperotto.org

Relevant Experience

University of Twente, The Netherlands **April 2015 -**
Assistant Professor
Design and Analysis of Communication Systems Group
Topics: Network Security, Network Monitoring and Measurements, Traffic Modeling

University of Twente, The Netherlands **Nov. 2010 - April 2015**
Post Doctoral researcher
Design and Analysis of Communication Systems Group
Topics: Network Security, Network Monitoring and Measurements, Traffic Modeling

University of California, San Diego, USA **January - March 2013**
Visiting Researcher
The Cooperative Association for Internet Data Analysis – CAIDA (Prof. kc claffy)
Topics: Network Security, Botnet characterization, Network measurements

Technical University Berlin, Berlin, Germany **March 2012**
Visiting Researcher
Internet Architectures Group (Prof. A. Feldmann)
Topics: Network Security, Network measurements

Education

University of Twente, The Netherlands – PhD in Computer Science **2006 - 2010**
Thesis: *Flow-based Intrusion Detection*
Promotor: Prof. dr. ir. B.R.H.M. Haverkort
Assistant promotor: dr.ir. A. Pras
Topics: Network Security, Network Monitoring, Traffic Modeling.

University of Manchester, United Kingdom – Erasmus Project **February 2006 - June 2006**
Topics: Computer Vision, Data Clustering.

Ca' Foscari University, Venice, Italy – MSc in Computer Science **2004 - 2006**
Thesis title:*Szemerédi's Regularity Lemma and its applications to Pairwise Clustering and Segmentation*
Proposer: Prof. M. Pelillo
Grade: 110/110 cum laude
Topics: Computer Vision, Data Clustering

Ca' Foscari University, Venice, Italy – BSc in Computer Science **2001 - 2004**
Thesis title: *Raggruppamento Percettivo e Insiemi Dominanti (Dominant Set and Perceptual Grouping)*
Proposer Prof. M. Pelillo
Grade: 110/110 cum laude
Topics: Computer Vision, Data Clustering

Selected publications

- van Rijswijk-Deij, R., Jonker, M., Sperotto, A. and Pras, A. *The Internet of Names: A DNS Big Dataset - Actively Measuring 50% of the Entire DNS Name Space, Every Day*, Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication (SIGCOMM 2015)
  Summary: The Domain Name System (DNS) is part of the core infrastructure of the Internet. Tracking changes in the DNS over time provides valuable information about the evolution of the Internets infrastructure. Until now, only one large-scale approach to perform these kinds of measurements existed, passive DNS (pDNS). While pDNS is useful for applications like tracing security incidents, it does not provide sufficient information to reliably track DNS changes over time. We use a complementary approach based on active measurements, which provides a unique, comprehensive dataset on the evolution of DNS over time. Our high-performance infrastructure performs Internet-scale active measurements, currently querying over 50% of the DNS name space on a daily basis. Our infrastructure is designed from the ground up to enable big data analysis approaches on, e.g., a Hadoop cluster. With this novel approach we aim for a quantum leap in DNS-based measurement and analysis of the Internet.

- van Rijswijk-Deij, R., Sperotto, A. and Pras, A. *DNSSEC and its potential for DDoS attacks a comprehensive measurement study*, ACM Internet Measurements Conference 2014 (IMC 2014) (acceptance rate 22.9%, awarded with the **ACM IMC Community Contribution Award** and with an **IRTF Applied Networking Research Prize 2015**)
  Summary: Over the past five years we have witnessed the introduction of DNSSEC, a security extension to the DNS that relies on digital signatures. DNSSEC strengthens DNS by preventing attacks such as cache poisoning. However, a common argument against the deployment of DNSSEC is its potential for abuse in Distributed Denial of Service (DDoS) attacks. The paper establishes ground truth around the open question of DNSSEC and its potential for DDoS attacks, based on large-scale measurement encompassing 70% of all the signed DNSSEC domains worldwide.
- van den Broek, G., van Rijswijk-Deij, R., Sperotto, A. and Pras, A. *DNSSEC meets real world: dealing with unreachability caused by fragmentation*, IEEE Communication Magazine, April 2014
  Summary: The Domain Name System is a critical system that represent one of the fundamental pillars of nowadays Internet architecture. Traditional DNS does not provide guarantees about authenticity and origin integrity. DNSSEC, an extension to DNS, improves this by using cryptographic signatures, at the expense of larger response messages. However, packet fragmentation can hinder the functionality of DNSSEC. This paper investigates how packet fragmentation can affect DNSSEC deployment and proposed and evaluate solutions to the fragmentation problem. This research has been conducted in collaboration with the Dutch Education and Research Network SURFnet.
- Sperotto, A., Schaffrath, G.,Sadre, R., Morariu, C., Pras, A., Stiller, B. *An Overview of IP Flow-based Intrusion Detection* IEEE Communications Surveys & Tutorials, 12 (3). pp. 343-356, 2010. (169 citations, ISI Impact 4,82)
  Summary: This paper is a survey of current research in the area of flow-based intrusion detection. The paper introduces the concept of network flows and the relevant related standards; it provides a classification of attacks and defense techniques and shows how these techniques have been applied to the field of flow-based intrusion detection. The paper is intended to fulfill the requirements of students and researchers approaching the field for the first time.
- Hofstede, R., Drago, I., Sadre, R., Sperotto, A., and Pras, A. *Measurement artifacts in Netflow/IPFIX data*, Proceedings of the Passive and Active Measurement conference (PAM 2013), 18-20 May 2013, Hong Kong, China (Acceptance rate: 32.4% - **Best Paper Award**)
  Summary: For deployment and scalability issues, we are nowadays focusing more and more on the use of flow-based measurement in various application areas of networking, such as accounting and security. However, it has been noticed that flow equipment can introduce artifacts in the measurement data. This paper investigates the qualitiy of flow-based data with respect to a set of artifacts introduced in the measurements by different implementation decision in a wide spectrum of devices. These results provide researchers and operators with important insights for developing robust analysis applications.
- Drago, I., Mellia, M., Munafò, M.M, Sperotto, A., Sadre, R. and Pras, A. Inside Dropbox: Understanding Personal Cloud Storage Services. In: ACM SIGCOMM Internet Measurement Conference, IMC 2012, 14-16 Nov 2012, Boston, USA (136 citations, Acceptance rate: 24% - **Awarded with the IRTF Applied Research Network Prize 2013**)
  Summary: This paper presents a characterization of on-line personal storage systems and it details the working mechanism and the performance of the most prominent of those, namely Dropbox. The paper characterizes the workload users in different environments generate to the system, highlighting how this reflects on network traffic. It also shows possible performance bottlenecks caused by both the current system architecture and the storage protocol.

Projects

- D^3 Distributed Denial-of-Service Defense: protecting schools and other public organizations (NWO Cyber Security Program, 2014 - 2018) – **Project coordinator**
- FLAMINGO – Management of the Future Internet (FP7 - Network of Excellence, 2012-2016) – **WP leader**
- CAD – Cyber Attack Detector (Founded by AgentschapNL, research conducted in partnership with TNO, KLPD, Fox-IT and UvA) – **UT coordinator**
- SURFnet GigaPort 3 – Next Generation Infrastructures and SURFnet Research on Networking (Yearly founded by SURFnet, contributed in 2010, 2011, 2012, 2013, 2014)

Awards and honors

IRTF Applied Networking Research Prize 2015 **2015**
For the paper *DNSSEC and its potential for DDoS attacks - a comprehensive measurement study* (R. van Rijswijk-Deij, A. Sperotto and A. Pras – ACM IMC 2014)

IRTF Applied Networking Research Prize 2013 **2013**
For the paper *Inside Dropbox: Understanding Personal Cloud Storage Services* (Drago, I. and Mellia, M. and

Munafò, M. M. and Sperotto, A. and Sadre, R. and Pras, A. – ACM IMC 2012)

Community Contribution Award at ACM IMC 2014 **2014**

For the paper *DNSSEC and its potential for DDoS attacks - a comprehensive measurement study* (R. van Rijswijk-Deij, A. Sperotto and A. Pras – ACM IMC 2014)

Best paper award **2015**

For the paper *How asymmetric is the Internet? A Study to Support the use of Traceroute* (de Vries, W., Santanna, J.J., Sperotto, A., Pras. A. – AIMS 2015)

Best paper award **2013**

For the paper *Measurement artifacts in Netflow/IPFIX data* (Hofstede, R., Drago, I., Sadre, R., Sperotto, A., and Pras, A. – PAM 2013)

Best paper award **2012**

For the paper *SSHCure: A Flow-Based SSH Intrusion Detection System* (Hellemons, L., Hendriks, L., Hofstede, R., Sperotto, A., Sadre, R., Pras, A. – AIMS 2012)

Best paper award **2009**

For the paper *Hidden Markov Model modeling of SSH brute-force attacks* (Sperotto, A., Sadre, R., de Boer, P.T. and Pras, A. – DSOM 2009)

UT stimuleringsfund grant for performing a series of academic visit abroad **2014**

UT stimuleringsfund grant for performing an extended academic visit abroad **2012**

Kivi Niria Telecommunication prize, candidate for UTwente, second classified **2012**

Anita Borg Finalist, Google **2009**

CTIT annual symposium on CreativeIT, University of Twente, second classified **2008**

PhD supervision

Daily supervision:

- Wouter de Vries (PhD candidate, 2015-2019) *Security and Stability of DNS*
- Mattijs Jonker (PhD candidate, 2014-2018) *Distributed Denial-of-Service Defense*
- Roland van Rijswijk-Deij (PhD candidate, 2014-2018) *DNS security*
- Christian Dietz (PhD candidate, in collaboration with Universität der Bundeswehr München 2014-2018) *Botnet detection*
- Jessica Steinberger (PhD candidate, in collaboration with the Center for Advanced Security Research Darmstadt (CASED), Hochschule Darmstadt, 2014-2018) *A collaborative approach to DDoS defense*
- Rick Hofstede (PhD candidate, 2011-2015) *Real-time and Resilient Intrusion Detection: a Flow-based Approach*

Additional support:

- Luuk Hendriks (PhD candidate, 2014-2018) *Security in Software Defined Networking*
- Morteza Karimzadeh (PhD candidate, 2013-2017) *Software Defined Networking to Improve Mobility Management Performance*
- José Jair C. Santanna (PhD candidate, 2013-2017) *Detection and Mitigation of Distributed Denial of Service Attacks*
- Ricardo de Oliveira Schmidt (PhD November 2014) *Estimating Required Bandwidth using Flow-based measurements*
- Idilio Drago (PhD December 2013) *Monitoring Cloud Systems*
- Giovane C. M. Moura (PhD March 2013) *Internet Bad Neighborhoods*

PhD defense Committee

- Ricardo de Oliveira Schmidt *Estimating Required Bandwidth using Flow-based measurements*, University of Twente, November 2014
- Philip Leroux, *Optimization and Distribution of Interactive Personalized Services*, Ghent University, 27 September 2012

Teaching experience

University of Twente, The Netherlands

Lecturer

Course: CreaTe Module “Data: From the source to the senses”, Internet Technology **2015 -**

Course: Cloud Networking **2014 -**

Course: Network Security **2011 -**

Project supervisor

Course: Design Project **2014 -**

Course: Cybercrime & Cybersecurity **2015 -**

Teaching assistant **2008 - 2014**
Course: Network Security course: complementary laboratory for students enrolled in the Kerckhoffs program (Computer Security)

Teaching assistant **2013 -**
Course: Bachelor Referaat

Ca' Foscari University, Venice, Italy
Teaching assistant **2003 - 2006**
Course: Algorithms, Data Structures and Complexity

Teaching assistant **2004, 2005**
Course: Coding Laboratory

MSc/BSc supervision

- Kaspar Hageman *The Performance of ECC Algorithms in DNSSEC: A Model-based Approach*, October 2015
- Justyna Chromik *Booter (black)list* , February 2015
- Erwin Middelesch (Kerckhoffs Institute and TNO) *Anonymous and hidden communication channels*, February 2015
- Terence Slot (Kerckhoffs Institute) *APT malware by comparing external and internal network traffic*, Jan 2015
- Wouter de Vries (Kerckhoffs Institute) *How asymmetric is the Internet? - A study to support DDoS Mitigation Approaches*, November 2014 (presented at RIPE 69, submitted to TMA 2015)
- Daniel van der Steeg *Flow-based DDoS attack detection in Cisco IOS*, August 2014 (accepted for publication at IM 2015)
- Mattijs Jonker (Kerckhoffs Institute) *Flow-based SSH Dictionary Attack Detection: the Effects of Aggregation*, August 2014 (accepted for publication at IM 2015)
- Mark Wierbosch (Kerckhoffs Institute) *It is raining packets*, July 2014
- Luuk Hendriks (MSc) *SSH Compromise Detection using NetFlow and IPFIX*, March 2014
- Dirk Maan (BSc) *Can we trust the Internet Census 2012?*, Feb 2014
- Jarmo van Lenthe (Kerckhoffs Institute) *Combining Multiple Malware Detection Approaches for Achieving Higher Accuracy*, January 2014
- Gijs van den Broek (Msc) *Improving Response Delivarability in DNSSEC*, July 2012
- Ivo Beckers (BSc) *The Distribution of Data Traffic using Flow Data*, January 2012
- Rick Hofstede (Msc) *IPFIX Export for the Ethernet-Layer*, July 2011
- Rick Hofstede (BSc) *Investigation of information sources for network monitoring*, July 2009
- Gert Vliek (MSc) *Detecting spam machines, a Netflow-data based approach*, February 2009
- Stephan Roolvink (MSc) *Detecting DDoS attacks involving DNS servers, a Netflow-data based approach*, December 2008
- Daan van der Sanden (MSc) *Detecting UDP attacks in high speed networks using packet symmetry with only flow data*, August 2008
- Joris Kinable (BSc) *Detection of network scan attacks using flow data*, June 2008

Journal Editor

- Guest Editor for the Special Issue of the International Journal on Network Management (IJNM): *Measure, Detect and Mitigate - Challenges and Trends in Network Security* (G. Dreo Rodosek, A. Sperotto, C. Schmitt, R. Hofstede and A. Dainotti) - scheduled for publication in September 2015
- Guest Editor for the Special Issue of the International Journal on Network Management (IJNM): *Flow-based Approaches in Network Management: Recent Advances and Future Trends* (R. Sadre, A.Sperotto, R.Hofstede and N.Brownlee) - published July 2014

Events organization

- Technical Programme Committee for the 7th International Workshop on Traffic Monitoring and Analysis (TMA 2015), April 23-24, 2015, Barcelona
- Co-chair for the 8th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2014), June 30 - July 3 2014, Brno, Czech Republic
- Co-chair for the Ph.D Workshop of the 7th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2013), June 25-28, 2013, Barcelona, Spain
- Technical Programme Committee of the IEEE/IFIP Network Operations and Management Symposium (NOMS 2014)

- Technical Programme Committee for the IFIP/IEEE International Symposium on Integrated Network Management (IM 2013, IM 2015)
- Technical Programme Committee of the Asia-Pacific Network Operations and Management Symposium (APNOMS 2012, APNOMS 2013, APNOMS 2014)
- Technical Programme Committee of the 6th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2012), June 4-8, 2012, University of Luxembourg, Luxembourg
- Technical Programme Committee for the Ph.D Workshop of the 5th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2011), June 13-17, 2011, Nancy, France
- Technical Programme Committee of the 3rd Workshop on the Pervasive Application of Wireless Technologies, September 27, 2011, Enschede, The Netherlands.
- Local organization of 5th International Week on Management of Network and Services, (MANWEEK 09) TelecomItalia Future Centre, Venice, Italy, October 26-30, 2009.
- Local organization of 3rd International Conference on Autonomous Infrastructure, Management and Security (AIMS 09), University of Twente, The Netherlands, June 30 July 2, 2009.

Reviewer

- IEEE/ACM Transaction on Networking
- Elsevier Computer Networks
- IEEE Communications Magazine
- IEEE Transactions on Network and Service Management
- Journal of Network and Systems Management
- Journal of Internet Services and Applications
- International Workshop on Traffic Monitoring and Analysis (TMA)
- IFIP Networking
- International Conference on Network and Service Management (CNSM)
- IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON)
- IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services (MMNS)
- IEEE/IFIP Network Operations and Management Symposium (NOMS)
- IFIP/IEEE International Symposium on Integrated Network Management (IM)
- ACM/IEEE International Workshop on Quality of Service (IWQoS)
- COST Traffic Monitoring and Analysis Workshop (TMA)
- Performance and Dependability Symposium (DSN-PDS)