Yarochkin Fyodor

fygrave@o0o.nu
mobile: +886920811510
Address: XiZhi Qu, Huqian Str, lane 110, alley 97, no 3-5, 10th floor
114, XinBei City, Taipei County, Taiwan. R.O.C.

Education

- **National Taiwan University**, Taipei, Taiwan.
  2006 - present: Ph.D. in Computer Science, expected graduation: January 2018.
  Thesis title(draft):*Large-scale Network Risk Assessment with Big Data.*

- **Kyrgyz-Russian Slavic University**, Kyrgyzstan.
  1995 - 2000: Diploma [M.Sc.] in Computer Science.
  Thesis title: *SnortNet - A Distributed Intrusion Detection System.*

- **Bishkek Technical College**, Kyrgyzstan.
  1991 - 1995: Diploma with honors in "Inventory Control Devices and Applied Robotics".

Research interests

- Network and Computer Security, Intrusion Detection and Threat Analytics. Malicious Software Analysis.
- Network Forensics and Covert Channel Detection.
- Distributed and Cloud Computing, Machine Learning. Data Mining.
- Applications of artificial intelligence and natural language processing algorithms to infomation security.

Research projects

- Honeynet: use of honeypots as an investigative practice in targeted attacks (APT).
- Current research in distributed and parallel data processing. Distributed event analysis and data correlation. Advisor: Dr. Kuo, Sy-Yen
  Distributed event data processing and clusterization.
- Current research distributed Internet information mining and intelligence analysis. Automated natural language processing. Advisor: Dr. Kuo, Sy-Yen
  Intelligence analysis: studying underground economies of eastern blocks.
- Research Project: Xprobe-NG: Building efficient network discovery tools. Advisor: Dr. Huang, Yen-Nun
- Research Project: Adaptive Covert Channels. Advisor: Dr. Huang, Yen-Nun
- Team Research Project: Automated analysis of malicious software.

Publications

- Investigating DNS traffic anomalies for malicious activities. Fyodor Yarochkin, Vladimir Kropotov, Yennun Huang, Guo-Kai Ni, Sy-Yen Kuo, Ing-Yi Chen, 2013/6/24, Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference
- Holography: a behavior-based profiler for malware analysis, Shih-Yao Dai, Yarochkin Fyodor, Ming-Wei Wu, Yennun Huang, Sy-Yen Kuo, 2012/9/1, Software: Practice and Experience

- F.V. Yarochkin, S.Y. Dai, Y.Huang, and S.Y. Kuo, "Building Biologically Inspired Defenses Against Malicious Software", Proceedings of the 41th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2011), Hong Kong, Jun. 2011
- Fyodor Yarochkin, Distributed Security Event Analysis in Cloud. Proceedings of the 41th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2011), Hong Kong, Jun. 2011
- Shih-Yao Dai, Fyodor Yarochkin, Sy-Yen Kuo, Ming-Wei Wu, Yennun Huang: Malware Profiler Based on Innovative Behavior-Awareness Technique. PRDC 2011: 314-319
- Fyodor V. Yarochkin, Ofir Arkin, Meder Kydyraliev, Shih-Yao Dai, Yennun Huang, Sy-Yen Kuo: Xprobe2++: Low volume remote network information gathering tool. DSN 2009: 205-210
- Shih-Yao Dai, Fyodor Yarochkin, Jain-Shing Wu, Chih-Hung Lin, Yennun Huang, Sy-Yen Kuo: Holography: A Hardware Virtualization Tool for Malware Analysis. PRDC 2009: 263-268
- Fyodor V. Yarochkin, Shih-Yao Dai, Chih-Hung Lin, Yennun Huang, Sy-Yen Kuo: Towards Adaptive Covert Communication System. PRDC 2008: 153-159
- Fyodor Yarochkin, Ofir Arkin. "A remote active OS fingerprinting tool using ICMP", published in USENIX "Login" magazine, April, 2002, and Phrack 57.
- Fyodor Yarochkin, Ofir Arkin. "Xprobe v2.0-A Fuzzy Approach to Remote Active Operating System Fingerprinting." Las Vegas, NV, USA, BlackHat 2002.
- Fyodor Yarochkin, Yu-Ming Chang, Chieh-Chu Lin, Huang-Yu Wang. ""Non-Common Architectures Buffer Overflows." BlackHat 2001, Singapore, BlackHat 2001, HongKong, 2002 .
- Linux-admin FAQ (http://www.tigerteam.net/linuxgroup/linux-admin-FAQ/)
- Fyodor Yarochkin. "SnortNet-A Distributed Intrusion Detection System." Final Diploma, Kyrgyz-Russian Slavic University , 2000.

  http://www.netsys.com/cgi-bin/display_article.cgi?1150

Selected Conference Presentations

- Fyodor Yarochkin, Grugq. "From Russia with Love.exe": an insight on underground economies of eastern blocks. HITB 2009, Kuala Lumpur.
- Fyodor Yarochkin, MikaSoft. "Artificial Intelligence for a Lazy Hacker." Ruxcon, Sydney, Australia, 2003.
- Fyodor Yarochkin, Meder Kydyraliev. "Security Tools Integration Framework (STIF)." HITB, Kuala Lumpur, Malaysia, 2004.
- Fyodor Yarochkin, Meder Kydyraliev. "Security Tools Integration Framework: Automating Distributed Hacking" Syscan, Bangkok, Thailand, 2005.
- Fyodor Yarochkin. "Advanced IDS normalization and correlation." Bellua Security Conference, Jakarta, Indonesia, 2005.
- Fyodor Yarochkin, Meder Kydyraliev. "STIF-ware evolution." HITB, Kuala Lumpur, Malaysia, 2005.

Career Summary

- **FTR Researcher**, Trend Micro/Taiwan (January 2017 – present)
  Responsibilities:
  - ◇ Foreward Looking Threat Landscape Research

- ◇ Timely response to onging network threats including malware outbreaks, vulnerability exploitation campaigns.
- ◇ Collaboration with other ops teams

- **Threat Researcher**, vArmour, Inc (April 2014 – December 2016)
  Responsibilities:
  - ◇ Threat Research: monitoring for malware outbreaks, evaluating vulnerabilities, prototyping network detection mechanisms.
  - ◇ Design and Evaluation of a Scalable Threat and Security Analytics System.
  - ◇ Maintenance of Threat Analytics Backend Platform.
  - ◇ Prototyping and Development of Stream Event Processing Security Engine.
  - ◇ Handling of Incident Response and Forensic Analysis cases.
- **Network and Security Operations**, Plurk (December 2012 – April 2014)
- **Research Assistant**, Academia Sinica (December 2012 – April 2014)
  Responsibilities: Primarily resposible for Research and Development of Information Security Portal, including development malicious software analysis platform, threat assessment platform, automation for vulnerability assessment platform.
  - ◇ Developed a scalable platform for risk assessment of large network infrastructures.
  - ◇ Developed an evaluation platform for malicious software analysis using sandboxing technology.
- **Senior Security Analyst and Software Architect**, Armorize Technologies (January 2007 – December 2011)
  Responsibilities: Develop and support components of Automated Vulnerability Assessment Platform, support Malware Analysis Team (building and evaluating automated malicious software components), Support Penetration Testing team (building automated tools for penetration testing and results processing), Support Static Source Code Analysis Team (security policies review, customer support, manual source code audits)
  - ◇ Developed components for automated scalable Vulnerability Assessment Platform (python/C/custom scripting languages/Java/Erlang).
  - ◇ Built automated javascript deobfuscation components (python/C).
  - ◇ Developed ICAP integration with Anti-Virus scanning platforms (python/C).
  - ◇ Built various protocol integration components (SOAP, SMTP) (python).
  - ◇ Buiilt and maintain Information Security Assessment Data Management System (ruby on rails/HTML/AJAX/Javascript).
  - ◇ Conducted several information security training courses (Code Auditing and Code Security, Disk Forensics, Network Forensics, Information Security for a pen-tester, Wireless Security, RFID and Bluetooth Security, Telecom Security)
- **Senior Security Analyst**, Guard-Info (Juanuary 2003 - January 2007)
  Asia-Pacific regional responsibility, performing Information Security consulting for large Banking and Finance Institutions, Insurance, Telecoms, Education, Military and Government organizations across the region with primary focus on supporting Taiwan based clients.
  - ◇ Network Architecture and Application Architecture Security reviews
  - ◇ Digital Forensics Services
  - ◇ Remote Network Security Assessments
  - ◇ System Security Assessments and Hardening
  - ◇ Vulnerability Research and exploit development
  - ◇ Application Security Assessments

- ◇ Reverse Engineering
- ◇ Wireless and Mobile Security Assessments
- ◇ Information Security and Web Application Security Training Courses (Instructor)
- ◇ Prototyping Security Event Management System

- **Information Security Analyst**, Trusecure Corporation (2001 - 2003)
  Asia-Pacific regional responsibility, performing Information Security consulting for large Banking and Finance Institutions, Insurance, Telecoms, Education, Military and Government organizations across the region.

  - ◇ Conducting network and host security assessments
  - ◇ Conducting firewall, IDS, and network equipment security reviews
  - ◇ Vulnerability mitigation and risk assessment
  - ◇ Handling incident response for customers
  - ◇ Remote Network Security Assessments
  - ◇ System Security Assessments and Hardening
  - ◇ Vulnerability Research and exploit development
  - ◇ Application Security Assessments
  - ◇ Reverse Engineering
  - ◇ Wireless and Mobile Security Assessments
  - ◇ Information Security Training Courses (Instructor)

- **Security Analyst**, RelayGroup (June 2000 - June 2001) The company was aquired by Trusecure.
  Conducted remote intrusion tests and provided security consulting services for Finance, Banking and Communication Institutions.

  - ◇ Conducting network and host security assessments
  - ◇ Conducting firewall, IDS, and network equipment security reviews
  - ◇ Threat analysis and vulnerability research
  - ◇ Research and development of internal-use security tools, innovative defensive and offensive security techniques and methodologies
  - ◇ Research and development of internal-use intrusion tests automation system

- **Network Engineer/System Administrator**, Soros Foundation (1998 - 2000) - part time employment

  - ◇ Design and installation of Cisco routers based WANs
  - ◇ Deployment and configuration of various routing protocols in Cisco hardware-based networks
  - ◇ Maintenance of Solaris2.X/BSD/Linux based networks
  - ◇ Installation and security auditing of Solaris2.X/BSD/Linux systems
  - ◇ Configuration/maintenance of DNS servers
  - ◇ Installation/configuration of mail delivery system based on deeply customized sendmail daemons
  - ◇ Installation, configuration and maintenance of news servers, web servers and transparent caching proxy servers
  - ◇ Development of custom CGI scripts and various custom network daemons

- **System Administrator**, Kyrgyz-Russian Slavic University (1996 - 1998) - part time employment

  - ◇ Local Network design, maintenance and service
  - ◇ Maintenance of NIS domains

- ◇ Maintenance of X-Window systems
- ◇ Administration of Unix systems, providing email and online Internet access for CTC staff
- ◇ Design and implementation of Web pages for CTC (including CGI/forms and Java applets development)
- ◇ Administration of Novell NetWare systems

Skills

- ◇ Building Parallel Data Processing Systems using distributed and cloud computing technology (Hadoop, JPPF, Erlang)
- ◇ Intrusion testing, internal security audits, authentication and access control, firewalls, intrusion detection systems, secure programming, secure payment systems.
- ◇ Excellent research and development skills on vulnerability research and exposure (including development of proof-of-concept vulnerability exposure code).
- ◇ Excellent experience with UNIX security on a variety of flavors (SunOS. Solaris, HP-UX, Digital UNIX, AIX, BSD flavors, Linux). Excellent experience with Windows NT/2000 security. Advanced knowledge of Cisco equipment, network protocols and technologies. Excellent experience with various clones of Firewall and IDS systems (CheckPoint, Cisco PIX, Raptor, RealSecure, Dragon IDS, NFR)
- ◇ Limited experience with AS/400 and OS/390 mainframe systems.
- ◇ Limited experience with Oracle and Informix database systems.
- ◇ Programmed various security tools (scanners, exploits, IDS utilities).

Specialized Skills

- Programming: C, C++, Java, Javascript, Python, Ruby, Perl, Pascal, Intel x86 and Sparc Assembler, Forth, Lisp, Erlang, Node.js;
- Distributed data processing: Hadoop/MapReduce, JPPF, RDBMS;
- Reverse Engineering, Vulnerability Research, Natural Language Processing.
- Fluent spoken/written English, Russian and Chinese(Mandarin);

Reference

- Available on request.