Fotios (Fotis) Chantzis

Website	sock-raw.org	**Email**	fotis.hantzis@gmail.com
Linkedin	profile	**Twitter**	@ithilgore

Personal Profile

I am a computer programmer and researcher with a strong background in Information Security and a focus on network exploitation techniques (Phrack publication, Nmap/Ncrack developer, Cyber Defense Directorate). Lately, I have been focusing on medical device security research.

Experience

Nov 2016 - Present Mayo Clinic
Principal Information Security Engineer

- Managing and conducting vulnerability assessments on medical devices and clinical support systems for Clinical Information Security - Resiliency. Participating in Red Team operations and running penetration tests on the hospital network and consulting on threat intelligence,

Oct 2015 - Present Nmap/Ncrack
Nmap/Ncrack Maintainer / Network Security Researcher

- Main developer and maintainer of Ncrack, the network authentication cracking tool of Nmap. Mentor for Google Summer of Code 2016 and 2017.

Sep 2016 - Nov 2016 Packt Publishing
Mastering Nmap author

- Authored and published a video course on Mastering Nmap. Focused on showing network administrators and information security professionals ways to to effectively utilize Nmap, NSE and Ncrack to conduct extensive and refined scans, including how to deal with very large networks.

Nov 2015 - Oct 2016 CENSUS SA
IT Security Engineer / Computer Security Researcher

- Conducted vulnerability assessments on infrastructure and devices for clients around the world using a variety of techniques including code inspection, reverse engineering, black box testing and fuzzing. Researched and developed tools for exploitation of special-purpose network protocols.

Mar 2015 - Dec 2015 Cyber Defense Directorate, Hellenic National Defense General Staff
Information Security Engineer

- Researched and developed a variety of network security projects (mainly C/C++). Conducted malware analysis and performed penetration tests on mission critical infrastructure. Consulted on threat intelligence.

Aug 2012 - Mar 2015 PrimaVista
Co-founder / Cloud Engineer / Software Engineer

- Designed and implemented the back-end cloud infrastructure based on Amazon Web Services (EC2, S3). Built an internal REST API on Tornado Web Server and crafted a custom queuing mechanism for load balancing worker tasks using RabbitMQ and Redis.
- Developed a synchronization algorithm tailored for sheet music files and metadata, offering functionality similar to Dropbox/Evernote and ensured data integrity in every possible error case by designing a robust recovery mechanism as part of the synchronization software.
- Designed and developed the Android application from scratch, supporting both mobile phones and tablets for all versions above 2.3. Optimized the user experience by integrating an internal PDF reader for faster image loading. Ensured asynchronous network communication with the back-end server by building the corresponding REST API client library and supporting push notifications through Google Cloud Messaging. Built custom library to support a third party service (MuseScore) through their REST API.

  Was also responsible for securing and hardening various components of the back end.

Aug 2012 - Dec 2012 Lesspaper
Co-founder / Cloud Engineer / Software Engineer

- Developed the Android application demo for snapping pictures out of a printed page or book, sending them to the back-end server for image processing (Optical Character Recognition) and returning the text back to the user.
- Implemented minimal back-end service by leveraging Parse (parse.com) and Amazon Web Services in addition to building on Tornado Web Server and RabbitMQ.

  Demo was accepted in first round of YCombinator.

Apr 2010 - Sep 2010 Ncrack
Nmap/Ncrack Author / Network Security Researcher

Continued development of Ncrack, the network authentication cracking tool of the Nmap project.

- Wrote the first working RDP cracker for all modern Windows editions by thoroughly inspecting captured network data and reverse engineering part of the protocol.

  Funding was provided by Google, as a student participant in Google Summer of Code.

Apr 2009 - Sep 2009 Ncrack
Nmap/Ncrack Author / Network Security Researcher

Developed Ncrack, the network authentication cracking tool of the Nmap project. Ncrack was built in C/C++ using a modular architecture and asynchronous network programming (based on Nmap's Nsock library) for massive parallelism using one thread. Researched the internals and implemented module support for many network protocols including SSH, RDP, FTP, Telnet, HTTP(s), SMB, VNC and POP3(s).

- Built all-encompassing SSH support by hacking the actual OpenSSH client code and converting part of it into a library tailored for Ncrack's non-blocking architecture.
- Improved overall network speed and authentication accuracy by programming a dynamic, optimized timing engine and using reconnaissance probes to collect metrics.

  Funding was provided by Google, as a student participant in Google Summer of Code.

Oct 2005 - Nov 2011 Computer Engineering & Informatics Department, University of Patras
Computer Center Administrator / IT Security Engineer

- Administered a large variety of computer servers used as the infrastructure of the Computer Engineering and Informatics Department. Conducted penetration tests on mission critical servers and worked with the principal engineers to harden the systems.
- Regulated the distribution of updates and hotfixes in the Computer Center by managing Windows Server Update Services and Active Directory in Windows Server editions. Automated deployment of client systems by leveraging Symantec Ghost and programming scripts. Coordinated the computer administration group and conducted seminars about a variety of technical subjects, focusing on network security.

Education

2018-now PhD candidate - Medical Device Security
University of Piraeus

2005-2012 Master of Engineering (MEng) -
Computer Engineering and Informatics Department, University of Patras, Greece
Grade: 8.46/10

2002-2005 High School - 19.6/20

Research

Exploiting TCP and the Persist Timer Infiniteness
Phrack

Discovered an inherent vulnerability in Transmission Control Protocol (TCP) by exploiting the TCP Persist Timer mechanism. Developed a Proof of Concept tool to demonstrate the attack by using a variety of network techniques: statelessness, client SYN cookies and TCP Timestamp time-keeping.

Abusing Network Protocols
AthCon security conference

Invented a new stealthy port-scanning attack by abusing the popular XMPP.

Hacking the OpenSSH library for Ncrack
Nmap

Analysis of the process of building the OpenSSH-based library for Ncrack's SSH module.

SOCK_RAW Demystified

Thorough analysis of the raw socket mechanism on the Linux 2.6 and FreeBSD 7.0 network stacks. Inspection of behind the scenes process of creating, delivering and receiving raw socket datagrams by delving into network internals of both contemporary kernels.

Conferences

- **Defcon (2018)**

  Organized and led the medical device security section of the biohacking village and CTF.
- **Defcon China (2018)**

  Designed and led a 4-hour workshop on advanced techniques of Nmap and Ncrack
- **Medical Device Security 101 conference (2018)**

  Presented about common vulnerabilities on medical devices and Mayo Clinic's assessment methodology for assessing them
- **Athcon security conference (2012)**

  Presented advanced techniques of network authentication cracking by leveraging Ncrack of the Nmap project.
- **Athcon security conference (2011)**

  Presented a new technique I invented for exploiting the popular XMPP network protocol.

Projects

- **Logo recognition system**

  Implemented a full-fledged logo recognition system for my diploma thesis, using OpenCV and Android.
- **Other projects**

  - Proof-of-concept Intrusion Detection System for detecting distributed SSH attacks.
  - Implemented an auto-defragmentation strategy for the Minix3 filesystem
  - Hardware keylogger using microprocessor PIC16F84A
- **National Cyberdefense Exercise PANOPTIS 2011**

  Participated as one of the representatives from the University of Patras led by Aristeidis Ilias. Coordinated the attacks of the red team and set up hacking challenges for the blue team.
- **Wargames at Fosscomm 2011, Patras**

  Organized the wargames session for Fosscomm 2011, designing and implementing the three main network hacking challenges.

Software Engineering Skills

- **Programming Languages**

  C/C++ - most experienced with ANSI C
  Python - scripting language of choice
  Java & Android - done a lot of development
  Javascript, PHP, Perl - working knowledge
- **Technologies**

  Reverse Engineering - IDA, Binary Ninja, Immunity Debugger, BinDiff, gdb, OllyDbg, adb
  Infrastructure - Amazon EC2/S3, MySQL, RabbitMQ, Tornado, Apache, Redis/memcached
  Network debugging - Nmap, tcpdump/wireshark, socat, hping, nc
  Operating Systems - GNU/Linux, MacOS, FreeBSD/OpenBSD (net stacks), Windows

Certifications

- **OSCE** - Offensive Security Certified Expert - License: OS-CTP-17601
- **OSCP** - Offensive Security Certified Professional - License: OS-101-034495
- **CISSP** - Certified Information Systems Security Professional - License: 635441

Distinctions

- **Highest score in school** - Two scholarships for graduating with the highest overall grade in high school.
- **3rd highest score in University** - Scholarship for having entered with the 3rd highest score in the Computer Engineering and Informatics Department, University of Patras.

Languages

- **English** - Full professional proficiency (Cambridge/Michigan Proficiency)
- **German** - Limited working proficiency (Mittelstufe)
- **Japanese** - Elementary proficiency (Level 4 Japanese Language Proficiency Test)
- **Greek** - Native

Interests

Ninjutsu, Guitar, pen-and-paper RPGs, biohacking, cognitive science