G0 - Security

G-SEC-xxx

Call For Papers

Show me what you got!

1.11

Call For Papers

binary name:	Freely name your paper (.pdf)
repository name:	SEC_CFP_$ACADEMICYEAR
repository rights:	ramassage-tek

It has been a while now that you are in the coding business, and you must be tired of the C/C++ inhuman syntax and cannot stand reading one more Unix manpage. After all that time, your programs still crash during code reviews, and you wake up sweating in the middle of the night after awful nightmares about your last failed unit tests.

Looks like it's time to stop programming to hack other people's work and attend awesome security talks for a change!

> *Sharing knowledge is the most fundamental act of friendship. Because it is a way you can give something without loosing something.*
>
> *Richard Stallman*

The field of computer science, and moreover its security aspect, is based on sharing knowledge. This knowledge can be a debugging technique, a little exploit you wrote, it can also be the knowledge of some protocols, of some vulnerabilities or of some cryptography primitives. All you learn in this field will be useful, to you, or someone else. Here comes the importance of sharing your knowledge. By doing so, you will encourage other developers to draw their attention to the impact of a poorly-written code, leaving huge breaches for malicious users to exploit. Remember all of what you have learnt about security till date. Was it by learning protocols by heart, by reading a project's documentation, or was it by fiddling with some pieces of code, reading tips given by some unknown user on a weird forum, or even hearing a trick that a mate found inadvertently? Keep in mind, what you know is different from what others know, keep on sharing knowledge.

If you think you have good knowledge or valuable insight to share in/on/about the field of computer and network security, crawl out of your basement and put on your best attire. Short talk or a workshop, submit your papers and be among this year's security chosen beings!

Papers should include the title of the talk/workshop along with a brief description of it (5-10 lines).

If you do not have any material to present, go fill up those information tanks at the back of your brains with new notions like how the outside world is full of poorly programmed pieces of software or how evil hackers steal your mom's identity, break into your connected toaster and ransom you for lodicoins.

Topics are NOT limited to one theme and may include (among others):

- reverse engineering
- vulnerability analysis
- cryptography
- privacy
- usage of common or new security tools
- anything that made the headlines in IT security news

If your paper ends up being selected, you will animate the short talk or the workshop during the corresponding security project. These events will be open to all students, streamed live and may take place in any Epitech site.

Talks must preferably be short (15-20m + questions).
Workshops can be any length, but not more than 4 hours, and should require minimal hardware (preferably virtual environments).