1100 - Hacking Smart Contracts

Friday at 11:00 in Track 3
45 minutes | Demo
Konstantinos Karagiannis*Chief Technology Officer, Security Consulting, BT Americas*

It can be argued that the DAO hack of June 2016 was the moment smart contracts entered mainstream awareness in the InfoSec community. Was the hope of taking blockchain from mere cryptocurrency platform to one that can perform amazing Turing-complete functions doomed? We've learned quite a lot from that attack against contract code, and Ethereum marches on. Smart contracts are a key part of the applications being created by the Enterprise Ethereum Alliance, Quorum, and smaller projects in financial and other companies. Ethical hacking of smart contracts is a critical new service that is needed. And as is the case with coders of Solidity (the language of Ethereum smart contracts), hackers able to find security flaws in the code are in high demand.

Join Konstantinos for an introduction to a methodology that can be applied to Solidity code review ... and potentially adapted to other smart contract projects. We'll examine the few tools that are needed, as well as the six most common types of flaws, illustrated using either public or sanitized real world" vulnerabilities.
Konstantinos Karagiannis
Konstantinos Karagiannis is the Chief Technology Officer for Security Consulting at BT Americas. In addition to guiding the technical direction of ethical hacking and security engagements, Konstantinos specializes in hacking financial applications, including smart contracts and other blockchain implementations. He has spoken at dozens of technical conferences around the world, including Black Hat Europe, RSA, and ISF World Security Congress.

@konstanthacker

#defcon25/by_track/track3/friday #defcon25/By_Day/_Friday