Cloud Computing 2020

Securing the Internet of Things from the Bottom Up Using an Immutable Blockchain-Based Secure Forensic Trail

Dr Bob Duncan

Dr Bob Duncan

30 years in industry as a corporate accountant

5 years as a lecturer at University of Aberdeen

Research area cloud security and corporate compliance

UNIVERSITY OF ABERDEEN

IARIA

Presentation Outline

- Introduction/Background
- Why should companies care about compliance?
- Cloud forensic problem – and why it is so hard
- Is is possible to achieve compliance without solving the cloud forensic problem?
- How can we address securing corporate systems?
- How can distributed ledger technology help?
- Limitations and discussion
- Conclusion and future work

Introduction/Background

- IoT started with great promise
- However, most IoT components were cheaply made with minimal resources and no security
- This would offer an easy route in to both corporate systems and SCADA systems once IoT systems were added
- Solve by developing secure IoT systems?
- Not much use if corporate and SCADA systems are not also upgraded
- The only proper solution is to find a robust means of securing corporate and SCADA systems

Why should companies care about compliance?

- Criminals who attack corporate systems are too difficult to catch
- This means governments and regulators will come after corporates
- There will be penalties for those who fail to comply
- Shareholders might not be happy
- There could be business disruption from the attack, the clean up and the regulatory investigation
- All of this could adversely affect the share price

Cloud forensic problem – and why is it so hard?

- Attackers seek to cover their tracks
- They do this by deleting all records of their visit from the forensic records
- This is usually very easy for them to do, as there is often little security on the forensic records
- Companies rarely use immutable database systems
- If you do not have a full forensic trail, you cannot tell who got in, what they looked at and what they modified, deleted or stole

Is compliance possible without solving the cloud forensic problem?

- The short answer is no
- If your forensic trail is incomplete, then you may not be able to tell when a breach occurs
- If you are unable to report the breach to the regulator within the appropriate time scale, then you would be non-compliant
- Of course, criminals are happy boast about their success, meaning the matter could come to the attention of the regulator
- If that happens after the reporting deadline, you would be non-compliant

How can we address securing corporate systems?

- First, we need to ensure the integrity of the system
- This means we need to retain a complete forensic trail
- This should be very hard to access, meaning stored away from the main system
- We could the turn to the financial world to use something robust and secure
- Cryptocurrencies spring to mind
- They use Blockchain to achieve this, with cryptographic protcols, immutable database and off-site storage

How can distributed ledger technology help?

- You have all heard that it is unwise to put all your eggs in one basket – drop the basket and your eggs are mush
- If you put each egg in a different basket, you will probably only drop one or two baskets, so the majority of the eggs survive
- This is the principal of distributed ledger technology
- If everything is in one place, once attacked, there is no more integrity
- But if you spread everything across different areas, then you can check for consensus across them all to find those that have been attacked, which can then be ignored from the consensus, then updated by the good ones that agree, so they all end up the same

Limitations and discussion

- There have been plenty of high value cryptocurrency attacks
- In all cases, the Blockchain could not be broken
- So by splitting cryptocurrency off the Blockchain, we can limit the risk
- By going to a private ledger instead of a public ledger, we can reduce latency caused by the sheer volume of ‘miners’ who have to be used, and paid, to achieve consensus
- Blockchain provides ‘security by design’ and with sufficient tightening down, can deliver a highly robust system

Conclusions and future work

- This approach could be a simple way for corporates to secure all their systems
- There is no need for a major software overhaul or re-write
- It does not take long to implement, minimising disruption
- This can help ensure a hoigh level of compliance can be achieved, leading to aconsiderable reduction in costs
- We are planning to run tests on comparable systems to demonstrate just how secure this system will be to protect a standard corporate system

Questions?

UNIVERSITY OF ABERDEEN

IARIA