12th International Cloud Computing Conference

Incorporating Permanent Audit Trails for Corporates

Bob Duncan, Magnus Westerlund and John Wickström

UNIVERSITY OF ABERDEEN

IARIA

ARCADA

Incorporating Permanent Audit Trails for Corporates

Introduction

- The introduction of the Internet of Things (IoT) brought one of the most serious challenges to the security of corporate systems
- The threat from cyber attack is constantly increasing year on year, and last year in the UK alone, 75% of large corporates suffered breaches
- Vulnerabilities are many and often well understood, but one key area where most corporates fall down, is with their inability to retain the audit trail of key transactions processed in their systems

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Introduction (Cont.)

- This is not a new problem, and has been around for at least the past four decades
- Traditional highly centralised corporate systems used a tight firewall around all corporate IT assets and still attackers were able to get in
- With todays ever more complex systems and the trend to the use of more distributed systems, often due to multiple site locations across both countries and continents, the challenge has only intensified

Incorporating Permanent Audit Trails for Corporates

Introduction (Cont.)

- Once the attacker penetrates the system, they usually seek out the audit trail in order to cover their tracks. Every time they enter the system, the remove their tracks, meaning they can remain undetected
- This can have implications for corporate security compliance, and in the event of a cyber breach this can lead to increased fines
- The continuing evolution and expansion of corporate systems will only cause this problem to increase, which is why we have chosen to do something about it

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Background

- This problem is well known, with a great many solutions proposed
- Unfortunately, attackers are still getting in, often with impunity
- The key here is to secure the audit trail
- With conventional databases, it is difficult to stop attackers compromising the records in the database
- Westerlund, Neovius and Pulkkis (2018) started development of a blockchain based solution for companies deploying IoT systems

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Background (Cont.)

- Securing the audit trail is the primary requirement to ensure ALL forensic records are retained
- This can provide evidence to authorities of who was responsible, thus it is vital that these records be maintained intact
- Corporates have a high motivation to do this properly
- Dealing with an intrusion can be very time consuming and seriously costly, through recovery time, penalties from regulators and possible adverse impact on share value, as well as reputational damage

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Practical Requirements

- To find a secure IoT solution, we have developed an approach for distributed security where all entities, both actors and devices, authenticate themselves through smart contracts running on the Ethereum blockchain
- Nodes can be hardened and also made invisible to the network
- External access is denied, making it extremely difficult to carry out an attack remotely
- This will be extremely effective for securing distributed networks

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Practical Requirements (Cont.)

- To be able to hold records in a trustworthy manner offering good redundancy. Thus, records require to be immutable, in that new records can be added, but can never be modified or deleted – a task that conventional database management systems cannot do
- There were early developments of immutable databases, but they suffered from management issues that made them impractical
- There are more modern developments, but since we plan to adopt the NSA Zero Trust approach, these will also not be suitable for our needs

Incorporating Permanent Audit Trails for Corporates

Why we opted for blockchain

- We have seen how Ethereum and blockchain technology provide an extremely robust level of redundancy and security
- The bar for corporate compliance for security is set very high these days, and the consequences of getting it wrong are so serious that we need to provide the strongest approach possible, and smart contracts running on the Ethereum blockchain
- It also offers us the opportunity to include new or existing systems one at a time to minimize implementation disruption

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Why we opted for blockchain (Cont.)

- This is because existing large corporate systems may already have inherent weaknesses, and adding new systems which are highly secure will not be a good solution
- Thus, adding a high security IoT system will not solve our problem, but if we then implement our solution to the main corporate system, then we get a high security solution, which is what we are dealing with here
- Then, as further additions take place, everything will be high security without the need for any disruption

Incorporating Permanent Audit Trails for Corporates

How we structured our approach

- Having determined that securing the main corporate system would be our task for this paper, we also wanted to consider how we would move forward
- We could see that the evolution of edge computing, machine learning operations and artificial intelligence would all be something to consider for the future, although they are not considered in this paper
- We also felt the NSA Zero Trust approach would be something that large corporates would be keen to adopt

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

How this can align with the NSA Zero Trust Approach

- The NSA approach assumes that in all corporate systems, you trust nothing. Computers, software, assorted devices, and even (and especially), people
- This ensures there will be no nasty surprises due to poor assumptions
- Every part of the work we have developed so far is geared for Zero Trust, which means once we are ready to implement the approach, we are good to go

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Conclusion and Future Development

- We have developed a high security audit trail system that can theoretically be applied to any system, or any part of a system, to protect all the forensic information generated
- This means that once an attack takes place, we will know how the attacker got in, what the did while they were there, and specifically which data the viewed, copied, exfiltrated or deleted
- This will make dealing with the regulatory authorities much more efficient, and should lead to a reduction in the level of any fine

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Conclusion and Future Development (Cont.)

- We will also have a great deal of evidence to present to the authorities, which will more readily be able to pursue the attackers
- The addition of Zero Trust will further tighten systems, which will be a good thing
- We may also be able to develop automated analysis of the forensic data to detect live intrusions in progress, and to bring an end to them

UNIVERSITY OF ABERDEEN

ARCADA

Incorporating Permanent Audit Trails for Corporates

Thank you for your attention

We are happy to answer any questions

UNIVERSITY OF ABERDEEN

ARCADA