All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

50 Ways to defeat your blockchain / distributed ledger / cryptocurrency system

Before you go off all flustered, know that I strongly support, as I have for many years, the use of cryptographic checksums[1] in a redundant distributed backward chaining system[2] to provide transaction integrity[3]. That is not the issue. The issue is that:

1. Like all systems, current and anticipated systems of this sort are vulnerable,
2. Current systems are being used and trusted to levels far exceeding their capacity to mitigate the associated attack consequences,
3. Many of these systems can be substantially improved by the use of long-known reasonable and prudent practices.

Why not write an academic paper on this?

In the late 1990s I wrote a “National InfoSec Baseline Study” on issues with intrusion detection systems. The net effect was that it was largely ignored by the relevant communities. So some time later, I wrote a little paper for a rag titled “50 ways to defeat your intrusion detection systems”[4] and this became the subject of lots of commentary in the research community followed by lots of crap coming my way, largely saying things like [only 20 of them worked against our defenses].

I have found that in your face slightly humorous expressions of large numbers and some substantial classes of attacks against systems at a hypothetical level is more effective in getting the message cross. I did this several other times since then, but it has been a while, so I am out of practice. Still, I will be timing myself in coming up with these methods, and will report how long it took at the end.

Starting at the end user platform to steal money / cause false transaction:

1. Trojan in the end-user wallet software
    - *The wallets are the interface between the user and the system. So if they don’t do and show what they indicate to you they are doing, you lose – and they can do anything on your behalf that you could do through them.*
2. Trojan in the platform supporting the wallet
    - *The platform supporting the wallet (e.g., your smart phone) can cause the wallet to do or not do anything the wallet could do on its own.*

---

1 F. Cohen, "A Cryptographic Checksum for Integrity Protection", IFIP-TC11 "Computers and Security", V6#6 (Dec. 1987), pp 505-810.

2 A non-distributed version of this method was used in the 1999 release of “ForensiX” A digital forensics ToolKit for Linux and Unix that tracked user activity using overlapping crypto-checksums, and it is similar to cypher feedback mode in the DES cryptosystem from the 1980s.

3 Cryptographic checksums for transaction integrity have been widely used since at least the 1960s in financial transactions and similar check codes were used before that in many cryptographic systems.

4 December, 1997 - 50 Ways to Defeat Your Intrusion Detection System - http://all.net/Analyst/index.html

3. False interface to the wallet
    - *By interfering with the user interface, even without altering a wallet, a system can appear to do things it is not and not do things it does. "We control the horizontal, we control the vertical, ..."*[5]
4. False wallet download to the end user platform by forged Web site
    - *If the Web site / app store you download the wallet from has one that is untrusted and you download it, you are getting the wrong one. Trojans have been put in software ion the Apple and Android stores in the past.*
5. False update to the wallet by attacking update process
    - *Even a legitimate piece of software can be updates to contain malicious or simple erroneous code. If the code was perfect as delivered there wouldn't be a need for updates.*
6. Altered instructions on the Web site where you get the wallet to release the keys
    - *Altered instructions can cause users to do the wrong things. And "legitimate" instructions can as well...Convincing users to do the wrong things is commonplace and easily done.*
7. Virus to infect many wallets and grant lots of access
    - *Anything you can do with a program can be reproduced, spread, and done by a virus carrying similar program code. So whatever vulnerability it is, can be reproduced across many systems. Stealing little bits of money from many places has been done before, and of course you can also steal a lot from a lot of people...*
8. Convince the user to use the wallet in the wrong way (e.g., false help desk)
    - *There are lots of ways to influence user behavior. All of those communications path to the user are potential points of perception management attack.*
9. Get the user to authorize transactions that are not legitimate (desired)
    - *Again, perception management can cause users to fall pray to frauds, including that extra charge to upgrade your wallet from CryptoWalletUpgrade.com*[6]
10. Cause the user to use a too complex password and forget/lose it
    - *Of course lots of users do this and some have lost lots of crypto money this way – which brings us to a business opportunity – crackyourwalletpassword.com ...*[7]

Now to the supply chain

11. Disrupt transactions (lots of ways to do this) to slow the system to unusability
    - *Some such systems are already slowing because of the high transaction overhead of having lots of nodes required to validate a transaction (50%+1 nodes have to*

5 Introduction to "The Outer Limits"
6 I didn't check if there is such a site – so if there is a legitimate one – sorry… OK I checked and it didn't exist as of the time of writing.
7 See the previous footnote.

agree to validate a transaction in some systems, and when you get to 100,000 nodes, that's a lot of checking and network bandwidth.

12. Plant a Trojan in the library routines used by wallet / crypto software (already done)
    - *When I say already done – I don't mean a specific case in a specific wallet library. Just that it has been done many times for other things. Of course it may have been done in a wallet, but then I wouldn't know until after this was made public.*
13. Plant a Trojan in the operating systems using the software (already done)
    - *This is widespread and commonplace. According to various leaks, it is done by governments (including the US government) and has been a methodology in use for many years.*
14. Plant a Trojan in the wallet software
    - *Wallet software is (presumably but maybe not really) checked more closely than the libraries it depends on. But do you really trust these programmers from wherever working for whoever to write software that protects your money?*
15. Plant a Trojan in the node processing software
    - *Same thing at a volume discount to the attacker. Do you think there is more scrutiny here? Don't bet on it. Ah – but if you are using crypto-currency you are.*
16. Exploit a previously unknown vulnerability in the node software (done all the time)
    - *Here's one I know has been done, since I exploited such a vulnerability in such a software component while working for the US government some time ago. This was not classified, but I won't be detailing it to you here… It was not something that (as far as I am aware) is present in the current wallet software – but I suspect similar things are present.*
17. Introduce a Trojan in the update to the previously unknown vulnerability
    - *According to various studies, updates produce vulnerabilities to the point where you can never really eliminate all the vulnerabilities through updates. You just get to a steady state of the number of vulnerabilities present.*[8] *Of course there is a cost to the process and producers commonly optimize that cost rather than trying to be perfect. After all, it's not their money you will be losing… And errors are not the same as intentional Trojans that look just like errors.*
18. Alter the compilers/interpreter used to produce the software distributed to the nodes
    - *Reflections on Trusting Trust – a Turing Award lecture by Ken Thompson in 1984 identified this path to Trojan horses.*[9]
19. Alter the infrastructure to change DNS entries and take over transactions (done)

8 I apologize for not citing lots of them here – I am being a bit loose in this presentation.

9 Ken Thomson, "Reflections on Trusting Trust", CACM V27#8, Aug 1984. Note that this was after the first publications on Computer Viruses (1983 and earlier in 1984) even though Thompson did not cite the earlier works.

- *I am too late on this one. Someone did this in the last few weeks and stole a bunch of bitcoin value. But we know that it's feasible now – as are the rest of the things here.*

20. Alter the infrastructure to reroute transactions through your nodes to slow processing
    - *This has been done lots of times, including through DNS systems, lower level autonomous system (AS) controls, and there are lots of other ways. Slowing down systems is just pone of the things that can be done of course...*

Now on to the systems controlling the overall operation

21. Attack the processing nodes to slow the overall system to a halt
    - *What can be done at the infrastructure level can be done to the endpoints.*
22. Disrupt the network connections to processing nodes to slow the system to a halt
    - *Or with other parts of the infrastructure.*
23. Introduce hardware Trojans into the supply chain for the nodes to gain control
    - *Of course WikiLeaks showed examples of the US government doing this. Only people with US government clearances are unaware of the details because they are not allowed to see what the rest of the public sees in this regard.*
24. Introduce software Trojans into the operating systems / libraries used by the nodes
    - *OK – Trojans can be put all over the place. And they are – lots of them – all the time – by lots of different people for different reasons. But if there is enough value at risk, it becomes worthwhile to actually do it directed at a specific target set.*
25. Exploit previously unidentified vulnerabilities in the nodes to gain control
    - *The crypto-currency folks complain that this will have no effect. The system as a whole will keep working just fine. But of course put the exploit in a virus and you can get lots of the nodes all at once.*
26. Alter the virtual machine used to interpret the node code at run time
    - *Many folks fail to appreciate that much of the software running on systems like cell hones is actually running in a virtual machine environment. The VM can of course be attacked just as the physical machine and the operating system and the libraries, etc. You really are trusting a lot of stuff with your transactions here.*
27. Alter the registration process for nodes to control who registers nodes
    - *By controlling who registers nodes, you can control who controls the infrastructure, and of course this can be used to ultimately take over the system as a whole and introduce an alternative reality.*
28. Alter the node formation process so that nodes get automatically created with Trojans
    - *The whole node creation process is problematic in current systems. Since the nodes validate the transactions and keep the authoritative records, altering those records in enough of the nodes – or simple denying services from them, can defeat, alter, or otherwise disrupt the entire system.*

29. Identify a problem in the cryptographic protocol and exploit it
    - *It turns out that the cryptographic protocols used in these systems have not been proven to meet specifications, which means that there are almost certainly vulnerabilities at the protocol level. Find one and exploit it and you might take over the entire system and all of the various versions of it.*
30. Alter the database(s) providing details on the nodes used to process transactions
    - *So when you go to process a transaction, there is a list of nodes you have to go to / through to get the transaction validated in the system. The registration process is only one place you might be able to control or alter this list. Do so elsewhere and the system becomes dynamic in terms of its trust model. Do so in large volume and the system collapses.*

Just thought I would break this list up a bit here...

31. Deny services to the databases used to find nodes to process transactions
    - *Of course if I cannot find the nodes to execute transactions the system will grind to a halt.*
32. Add nodes to the system in large numbers to force increased processing delays
    - *And if I add enough nodes to the system that are slow or don't act properly over time, the system will slow down under the increased load.*
33. Create large numbers of "forks" in systems to make the whole thing confusing
    - *OK – that's already being done. There are lots of Etherium systems out there running different "forks", each with their own rules about how things work. Build all you want and sew confusion and distrust. And by the way, do all of them have the same quality controls?*
34. Create fake domain names similar to the real ones to get users into fake systems
    - *This was identified in the early 50 ways article about defeating Web systems about 20 years ago, and it still works today.*
35. Create man in the middle attacks using the fake systems so users are using real systems but not actually in a secure way
    - *Technically this is an exploit that can be used with the previous method or others. In effect, you crate a fake registration process, fake wallet, etc. and act as an intermediary with the rest of the system, altering and observing everything passing back and forth. All of the endpoint protection mechanisms fall away under this sort of attack if well performed.*
36. Create man in the middle attacks on the node creation process to take over new nodes
    - *Something about the goose and gander applies here. You can do the same thing to the nodes as the endpoints with the wallets. Has it been done already? Nobody probably actually knows for blockchain systems, but it has for lots of other kinds.*
37. Create large numbers of very small transactions to slow the system as a whole down

- *In many of these systems the transaction times are getting slower and slower. This attack just increases the rate of decline of the systems for the duration of the attack. Note that if the time gets long enough, lots of other bad things can happen...*

38. Create a “too large” transaction to cause errors in the accounting systems and different balances at different nodes
    - *Do you think the current systems are all using “bignum” applications for all of their processing? If there is a different word size or overflow point in different implementations, this might wreck havoc across an entire infrastructure of such systems as different systems agree the transaction was valid but have different end results for the balances.*
39. Take a lot of fiat currency out of the system at one time to crash the value (no market watch or regulation here)
    - *The lack of market controls by an independent entity make these system ripe for all sorts of frauds and other exploitations. Pump and dump is already widespread as a fraud technique and when you don’t have all the normal controls of a fiat currency or regulated market, things tend to go bad fast.*
40. Slowly take down more and more nodes to reduce the number of active nodes, thus slowing transactions
    - *What can be done quickly can also be done slowly in many cases. In this case, the full lifecycle of nodes has not been adequately taken into account. As time goes on, more and more of these conditions will arise and we will see what happens.*
41. Take down 50%+1 of the nodes and cause the system to be unable to process further
    - *Distributed Denial of Service (DDoS) attack seems logical here.*

Now to the weight of money in the system

42. Exploit “random number generation” to produce more crackable keys
    - *The so-called random number generators at the heart of much of the cryptographic technology today are based on a theory rarely realized in reality. Exploits of pseudo-random number generators and other related technologies have happened for decades and are likely to occur again in this context as the value increases to the level worthy of the exploit.*
43. Exploit stolen computer time to generate value using stolen resources (widespread)
    - *This is commonly done today by running code in Web browsers downloaded as part of normal use. The thieves take your computer time to generate their crypto-money. It consumes power as well, so it harms the environment, you pay the power bill, they get the money.*
44. Convince governments that they need to control the currency and not allow such private money systems to exist
    - *This is always a threat until the mechanisms get normalized into the legal system. People in China wishing to get money to the US but crypto-currency there and sell it here. It’s illegal in many cases, and verges on smuggling.*

45. Cause legislation to be introduced requiring the same sorts of controls as over fiat currency, thus driving up transaction costs
    - *One of the reasons for those charges you have to pay to move money around the world using the currency of nation states (fiat currency) is because they require controls over the movement of money. When you trade outside of the system the system will not protect you from bad actors or other system failures, and you rely on the controls put in place by the owners of the systems to protect your transactions and their value. If nation states start supporting and allowing this, they will require similar controls to the controls over other transactions in the financial systems, and you will be paying the banks using a different mechanism. Driving up the cost makes small transactions more expensive and no longer worth the transaction costs, etc.*
46. Take down major processing centers causing widespread outages (already done)
    - *Every once in a while one of these systems get taken over or brought down. As a result, people cannot access funds or transactions or process transactions for a while. This is the same as the rest of the financial systems of the world except that the people running the systems are not as well prepared or regulated to meet the needs of the mechanisms that may end up using them.*
47. Use transactions to covertly support terrorist activity forcing increased overhead required by governments countering terrorism
    - *Tracking transactions in such a system will come under government regulation if only to stop illegal payments from being made. Taxation, criminal activity, terrorism, etc. are all reasons regulation has to take hold or these systems will be stopped. Of course much of the world is already doing this...*
48. Manipulate transaction timing to buy and sell before markets move up and down (already done)
    - *This is being done in financial markets today and has been done for a long time. No reason to believe it will not be done in the blockchain transaction world, and you can bet it is already being done with no legal recourse today.*
49. Create lots of ICOs turning them into fiat currency at high prices and reducing the value of the system
    - *Yep – sell high in large volume taking the money out of the system and leaving those at the end of the bubble busted is the way of such things. Get out now while you can? Or try to ride it higher still?*

Last but not least

50. Buy enough nodes to own more than 50% of the nodes and then change reality to meet your desires
    - *You think it will cost too much? Don't bet on it. It costs less than $100 to get into something like Etherium as a node. But even if it costs $1,000 each node and there are 100,000 nodes today, buying 100,000 more nodes will only cost $100M. For a system with many billions of dollars of equivalent cash value, a large enterprise*

> *could do so without much impact, and of course any substantial government could take over such a system at will. Have they done it yet? You don't know and neither do I. And once you own that many of the nodes, you can make arbitrary changes and win the disputes over them. And of course it will wreck havoc on the system along the way...*

OK – for timing purposes, writing this without pre-thinking it all or copying from anyone took 34 minutes – that's about 40 seconds each, including typing them in and correcting spelling. In fairness, #50 was one I thought of time time ago and decided to use this time. I also had discussions surrounding this area with other folks over time. The commentary under each item was added later. How long would it take to generate another 50? Maybe an hour if you didn't want them to be too close to any of these.

Counterarguments

Of course you will hear various folks tell you that this one or that one wouldn't work in their system. And some will tell you that they haven't been done yet so they aren't a real "risk". But I suspect if you look at it deeply with a real expert, every one of these ways will work in some or many systems, many of them will work in most, and some will work in all such systems today. I have sat and listened to folks call me names, and try to claim that their cell phone is invulnerable to such things, or tell me that they aren't worried because they trust the unknown people who created the system they now have $100,000 of value in, etc. And of course I am not perfect – perhaps some of these won't work against one system or another or even most systems.

But that's not the point

The point is that cyber-security is not solved by using a blockchain, or deep learning AI, or the cloud, or any other technology, and certainly not on their own. Systems have weaknesses and those weaknesses can be exploited. If you or I put too much weight on a system, it will ultimately collapse under that weight. There is a lot of surrounding stuff to get right.

The question not being asked and answered about modern cryptocurrency systems and blockchain-based distributed ledger systems is how much weight they can support and how to disaggregate risk to make them sufficiently worthy of the trust being placed in them.

Conclusion(s)

Don't put too much weight on these systems because they are not yet at a level of maturity required to be relatively safe from any number of attacks, including these and many others.

Don't believe the hyperbole about these systems being "secure" - they are not. Cyber-security is a complicated thing that requires building systems that, as a whole, function as desired to a level of certainty that can be understood. Crypto-currency today is managing far more value than it can sustainably protect. It's time to get systematic about protecting the value.

Such systems that run independent of nation states or others entities that back them with the "full faith and credit" of the entity, can only be trusted to that level of faith and credit. If you think Etherium or BitCoin will give you your money back as/if they are destroyed, you may be in for an unpleasant surprise. Think tulips.[10]

10 Charles Mackay, "Extraordinary Popular Delusions and the Madness of Crowds", 1841

