

Declaration of Stephen Spoonamore  
740 Quinby Ave.  
Wooster OH 44691

1. During the evening and early morning on the 2004 General Election in Ohio, on my own computer was watching the results of incoming counties and precincts. I believed there was a more than likely chance County Tabulators had been programmed to manipulate votes. I had a simple Microsoft Excel program running to help with the analysis. As early results showed Kerry ahead, at about 11PM, I noticed a trend in a very few counties (I believe I noted 8 counties on election night) that at about 11PM suddenly began reporting radically different ratios of Kerry to Bush votes. All in favor of Mr. Bush. This sudden rate of change allowing a tuning of the system resembled a fraud technique called an Intelligent Man In the Middle, or KingPin Attack. This type of attack requires a computer to be inserted into the communications flow of an IT system. The computer placed in the KingPin position has the ability to change information at both ends of an IT system.

2. This Kingpin position in which a central computer sees both ends of a system would explain the wide divergence in results reported from the limited group of counties now referred to as the "Connally Anomaly". It is extremely powerful situation, I suggested at the time the incoming information flow to the Secretary of State's offices were diverted to a KingPin computer, or the Sec. of State in fact had allowed the data to be sent to a KingPin. I was dismissed at the time.

3. My second analysis, found that my suspected 8 counties, were part of larger group of 12-14 "Connally Anomaly" counties where the results of a down ballot judicial race indicated wildly different voter preferences than the Presidential Race. In the "Connally Anomaly" Counties, tens of thousands of voters are recorded as having voted for an extremely liberal, minority judge who had done no campaigning in the county, but cast no vote for Kerry.

4. Other experts in voting and statistics have conducted analysis of this event and deemed it "impossible" or "beyond 1 in a Billion" likelihood an election could have had such an outcome. However, all the experts conclusions in the weeks following the election further confirm the only likely explanation of the county level tabulators had been either preprogrammed to flip a certain percentage of votes or, again most likely, a KingPin had changed results during the night of the election. Other experts found additional data indicated Bush's increase in votes from these counties, and Kerry's decrease in votes from these counties had grown by larger numbers after apx 10:45PM on Election Night. This

variable rate of change, which I had seen in results in 8 counties on election night, and detected in 12-14 counties by additional analysis in the following weeks, again indicates a KingPin computer had been "tuning" the election results to a desired outcome.

5. At the time of the analysis above, I, nor do I believe any parties knew of Sec. of State Blackwell's SmartTech insertion. At the time I stated Triad Systems, as the programmers of the suspect tabulators was fully capable of either a Pre-Programmed Hack or the setting up of KingPin.

6. When information about the SmartTech IT routing switch became public, and recalling that staff of Triad were reported to have removed hard drives from County Tabulators in advance of the recount, I again stated that we now have confirmation a KingPin, or Intelligent Man in the Middle position had been created. And it appears an effort is underway to destroy the evidence of the KingPin communicating with the County Tabulators. The SmartTech system was set up precisely as a KingPin computer used in criminal acts against banking or credit card processes and had the needed level of access to both county tabulators and Secretary of States computers to allow whoever was running SmartTech's computers to decide the output of the county tabulators under it's control.

7. After reviewing the system architectures provided last week, I again state that analysis is correct, and the architecture further confirms how this election was stolen. The computer system at SmartTech had the correct placement, connectivity, and computer experts necessary to change the election in any manner desired by the controllers of the SmartTech computers.

8. It has been asserted by some that local County Elections officials had been instructed to Fax final results to confirm them, but this action would not have mattered if the local elections boards computers were already under the control of the KingPin. The results Faxed from the County to the Secretary of State would be results inserted by the SmartTech KingPin into the County Tabulator. The Faxed output is in fact a smokescreen to mask the already hacked results and provide an illusion the tabulators were not reporting results over the internet.

9. The final tabulation results to the Secretary of State's offices. Any tabulator with a known IP address connected to the Internet at the county level could be addressed by the SmartTech computer. The SmartTech computer would as the results of the evening proceeded be able to know how many votes Bush needed to steal from Kerry, and flip enough votes on the desired county tabulators to reverse the outcome of the election.

10. The facts now established of creating SmartTech as a KingPin, also further confirms the process of theft I believed had gone on during election night, and further confirms and is fully consistent with and factually explains the "Connally Anomaly." Where the votes appear to have been switched from Kerry to Bush in twelve SW Ohio counties, to change the outcome of the contest for Ohio's electoral college votes.

11. The only way this could have been detected on election night would be complete monitoring and address logs kept at the county level of any firewalls of other routing or logging operations at or in the tabulator or by conducting a forensic analysis of the complete county tabulator computer, especially the hard drives of these computers. These hard drives were apparently removed by Triad employees before the Green Party Recount, in what appears to be a concerted effort to destroy evidence.

12. Overall, my analysis of the two Architectures provided is the following: They are very simple systems. They are designed for ease of use during the one of two times a year they are needed for an election. They are not designed with any security or monitoring systems for negative actions including MIM or KingPin attacks. These systems as designed would not be sufficient for any banking function, credit card function, or even for many corporate email systems needing a high degree of confidence. They are systems which will work easily, but are based on the a belief all users and the system itself will be trusted not to be hacked. There are obviously many parties willing, with motivation, and able to hack an election for a desired outcome.

13. To minimize the chances of this happening again, I recommend in the strongest of terms, that each county completely disconnect all tabulators from any connectivity before, during and after the voting. The Tabulators should not be touched or accessed by any one or any electronic system. They should have no wireless, IR, BlueTooth or other connectivity. As the incoming precinct are tabulated, the running totals of results should be printed out at regular intervals during the tabulations and the final totals be printed out and copies of the final county totals, in print form handed to local party officials and public sources as the final results are faxed, phoned or emailed into the Secretary of States office from a computer other than the tabulator. The tabulator upon completion of the final precinct tabulation and printed output, should be turned off, disconnected and placed under lock-up by authorities. It should be handled by no one until the election is certified. If any dispute arises from the election, any county tabulator on this system which has had any connectivity during the election is suspect and needs forensic analysis. Further, even a county tabulator disconnected from connectivity during the election night can be subject to preprogrammed hacks or sophisticated attacks by introduced channels on election night. Again in the event of a questioned outcome, forensic analysis by qualified parties can reveal of manipulation has occurred.

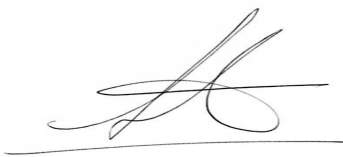
14. I believed on election night 2004, due to my long expertise and work in computer attacks on Banking, Government and Communication systems reversed the outcome of the 2004 Ohio Presidential Race was subjected to a KingPin attack reversing Kerry votes and making them Bush Votes. All information that has come forth since then has further confirmed this belief, and the actions of some parties, notably Triad in removing Hard Drives which would have shown these actions and the refusal of Mr. Connell to testify about what he knows about the SmartTech KingPin set up, further confirm my professional opinion.

15. A final note, Mr. Connell has represented his interest in protecting trade secrets from me as one reason to not appear. This is absurd. We work in extremely different areas of

IT. I am a network Architect principally in fraud detection and infrastructure protection systems. Mr. Connell develops interfaces with databases and front end experiences. If we both built houses instead of IT, this would be like a siding contractor claiming he competes with the electrical contractor. We are two contractors who both need the other's skills do our work. Mr. Connell and I have never to my knowledge competed for the same contracts. I am not aware of any work Mr. Connell does that I, or my firms would be interested in working on. In fact we have referred business leads to each other, and mutually contributed out skills to proposals for projects in International Freedom Initiatives.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 26th day of October 2008.

A handwritten signature in black ink, appearing to be 'S. Spoonamore', written over a horizontal line.

Stephen Spoonamore