Opening Remarks
How did we get here?

Previously in our discussions we have talked about this subject and in particular about the Stuxnet virus. We will come back to that subject again today, but we will be treating the problem of Cybersecurity in a somewhat broader sense.

FirstI I will comment about the origin of the modern computer. This is useful for our discussion, because relates to the question of whether or not a computer can be made safe from a hacker attack and it lays the groundwork for further discussion. Then we will watch the DVD on Cybersecurity. Finally, we will have an open discussion concerning the issues raised by the DVD and in particular, the role of government in the solution.

By the way, when studying into the origin of the computer one discovers that there is dispute and uncertainty as to who did what and when. But this is my best understanding of the process, even though I am leaving a lot of history out of the story.

***

Alan Turing was born in England 100 years ago on June 23, 1912. At that time, the word *computer* was used to describe persons, most of whom were women, who did repetitive calculations for hours on end.

Alan was a brilliant mathematician. As a student at Kings College, he approached a difficult mathematical problem It was the Hilbert problem, which asked the question: “Can mathematics be reduced to a small number of axioms?”

In a 1936 paper, at age 24, Turing described an imaginary machine to test the concept. His machine used a piece of a special tape. His machine could make marks on the tape and erase them. It could move the tape back and forth by reading what the marks were. The machine could be used to count, and add numbers and perform other calculations. In fact, using a handful of instructions, it could do everything that could be done with a calculator. At the same time he showed that there was no way to know if the machine would always come to a final answer.

Although his machine failed to provide a final answer to the Hilbert question, in his search for the answer he conceived the first programmable computer. I say conceived rather than invented because his machine was only a thought experiment. Today we call it a Turing Machine. It did not create much of a stir at the time, because there were only a few people on earth who could appreciate what he had done.

In the forties Alan was recruited into the war effort. He made major contributions by helping to design a machine that could break the German Diplomatic code. This gave Winston Churchill secret information concerning German capabilities and intentions This machine was a single purpose machine, and so it was not a full computer. However, it paved the way because it showed how relays could be used to perform logic. Vacuum tubes later replaced the relays because they were much faster.

After the war, Turing worked on other projects, including the design of a general purpose computer. However, with the war over and lacking financial support, the project proceeded slowly.

Alan spent some time going back and forth between England and Princeton University where he met with Jon von Neumann,

another highly regarded mathematician. We do not know what they talked about, but it is clear that von Neumann ended up with some of Turing's idea.

It is a sad fact that Turing, a homosexual when homosexuality was considered a crime, was ultimately hounded by the same government that he had served, and later committed suicide.

In the middle forties, in the United States, the Army was looking for better ways to compute firing tables for long range guns. When a large gun fires a projectile several miles away, many factors --temperature, humidity, curvature and even the rotation of the earth -- can affect its accuracy. This makes the aiming of long-range guns on land or sea a difficult mathematical problem.

At the University Pennsylvania Moore School of Engineering, two engineers named Eckert and Mauchly, who were unaware of Turing's work, were working an electronic machines to solve these problems. One was called ENIAC* and another called EDVAC*. Both used vacuum tubes, now replacing relays, to do mathematical calculations. Jon von Neumann, from Princeton, was invited to participate and offer suggestions.

He wrote a report called "The First Draft of a Report on the EDVAC dated June 30, 1945.

Two important observations may be drawn from the report

(1) It contains ideas that Alan Turing wrote about in 1936 and later.

(2) Alan Turing is not mentioned anywhere in the report.

We do not know for sure if von Neumann stole Turing's ideas, or whether he only recreated them, Because his report was widely circulated it is a reference point in modern computer history. Von Neumann's description of a working machine was more complete than anything previously published. Today, general purpose binary programmable digital computers, the ones we all use, are often called von Neumann machines.

My purpose in taking you through this is that an important concept, attributed to von Neuman, but originating with Turing, makes the general purpose computer possible. But at the same time, it makes it vulnerable. In fact, no von Neumann machine can be made to be totally secure. Perhaps this is a theory and not a fact, but so far no one has been able to disprove it. Partly as a result of this, mathematicians are working on Non-von-Neumann designs but no one has designed one that is as powerful as the one we have today. The only true competitor in that field today is the human brain.

What is this vulnerability?

A computer operates with two sources of data. One source contains the data being worked on. The other contains the instructions for operating on that data. That is called a program, or an algorithm. A computer operates with two cycles. One cycle goes into its memory to fetch an instruction. The second executes the instruction. And it does this over and over.

What is an example of an instruction?

One instruction might to to fetch a number, from a particular location in memory and put it into the Arithmetic and Logical Unit, the ALU. That is where the work is done. Another instruction might be to fetch a

number and add it to the number that is already in the ALU. A third instruction might be to take the number that is in the ALU and put it somewhere back in memory.

There, I have just written a computer program. Three instructions

fetch
fetch and add
store.

Very simple.

Where does the computer find these instructions? Earlier they would be found on a plug board or on a bank of switches or some other physical device. It was von Neumann's suggestion, based on the Turing machine concept, that those instructions could be stored in the same place as the data. In short, a computer program was just another kind of data. It matters not where it is stored. It matters only how it is used.

Because the program can also be treated as data, it can be changed by another computer program. In fact, a computer program can change itself.

This is a very powerful idea. It is so important that this single concept distinguishes a general purpose computer from a calculator. This concept permits the computer to perform repetitive operations involving different pieces of data. To consider the path of a projectile from a gun to its target, for example, the computer can perform repetitive computations on its trajectory every second, replacing the old position and velocity with the new, over and over, until the projectile reaches its target. In this way the computer can simulate the entire flight path of the projectile

But by using the same concept, this same computer to scan an article looking for a key word or phrase. This is used in data search, like Google.

Using this concept, It can compress an image into the jpeg format.

The concept permits a computer to pause one task, and start another in case it needs to perform some calculations on the side. Or it can work on two entirely different problems at the same time by overlapping the tasks.

The concept permits a computer to solve problems by successive trial and error.

And much more.

But, here's the rub.

The same concept permits a rogue program to be placed in its memory, a program which can interfere with the flow of work and start on a task not intended by the owner of the machine.

It permits a rogue program to seek out a user's program and change it so that it does something that the user did not intend.

It permits a rogue program to copy itself and then send the copy to another computer over a communication line. These are called viruses and worms

It permits a rogue computer program to scan a computer's memory to find personal information, such as Social Security Numbers, bank balances and email addresses.

And the list goes on.

How can this happen?

For a computer to work, it has be able to find the next program instruction. The location of the next instruction is held in a special place of memory. When an instruction is fetched, the location of the next instruction is updated to be the next one in sequence. However, this may be altered on the fly, so to speak. A program can contain a technique the purpose of which is to change the recorded location of the next instruction. This is necessary for the computer to be able to branch from one part of a program to another. It is this technique gives the computer its power.

A rogue program only needs to find a way change the contents of that location in memory so that it leads to the first instruction of the rogue program. This is how the rogue program gains control of the computer.

Computer designers try to prevent this from happening, but he evil hacker tries to find ways to trick the computer. He will look to find vulnerabilities that will bypass the barriers. Computer designers and users constantly look for and eliminate these vulnerabilities, but for several reasons they can not be totally eliminated. Vulnerabilities can be reduced or hidden. Instead of hiding the spare key in the mail box, you put it in the drain pipe because nobody would think of liking for it there

So let us summarize:

General Purpose computers today employ the von Neumann architecture.

A von Neumann machine can be hacked. This may be easy or difficult depending on computer design and the knowledge and skill of the evil hacker. By the way, I here use the term “hacker” in its pejorative sense. There are good hackers as well as bad hackers.

We do not have a successful concept for a working non-von Neumann machine although engineers and scientists are working on it.

I must add, there is a bit of irony to this story. As ingenious as the von Neumann concept for the EDVAC was, the act of publishing and distributing the report caused a huge backlash--a grand kerfuffle if you will--in the technical community. This is partly because some of what he said, whether he knew it or not, revealed other people’s work. He was quickly excluded from the project, and the final machine was built by another team. Ironically, he was not the final designer yet the ideas he presented have prevailed and his name appears on the nameplate.

*EDVAC: Electronic Discrete Variable Automatic Calculator. ENIAC: Electronic Numerical Integrator and Computer

March 20, 2012
Richard Ten Dyke
Bedford, New York

Introduction to the DVD

Several Issues are raised in the DVD. Which of these, in your opinion, are most in need of some kind of action? What action would that be?

a. Personal Security vs. Convenience
b. Corporate Espionage and Theft of Intellectual Property
c. Freedom of Speech and Political Activism in Authoritarian Countries
d. Military Offense and Defense
e. Protecting our Nation's Infrastructure.
f. Stuxnet, a case study
g. The Danger of Anonymity
h. Other _____

For each of the above we will discuss three basic elements of the situation.

a. Description of the Problem, who are the perpetrators and who are the victims?
b. How do we match the response to the threat?
c. What should the Government do vs. what should be left to the private sector?

Post DVD Comments

What are the policy implications in what we are dealing with?

a. How does this affect our relations with Israel, China, India, etc.
b. Should the United States use cyberspace to support of political activism
c. Should governments take a more active role in managing cyberspace?
d. What would constitute an act of war?
e. Should congress act? How?

What is the role of Government: Laws as well as action.

Do we need a Central Authority, a Czar in the federal government?

a. NSA
b. CIA
c. Dept. of Defense
d. Homeland Security
e. FBI

Should the Government take responsibility for personal security?

Responsibilities of service providers vs. users

How can users become better educated concerning risks and actions?

Level of Attack	Recommended Action
It Starts with the User/Victim Sharing of personal data Phishing Scams Financial Scams Viruses and other Malware	Use firewall and virus prevention software Do not respond to requests for personal information Do not respond to requests for money Do not install pirated programs or data Report lost or stolen credit cards Use strong passwords (ten characters) when needed Be alert and aware Track down and imprison the perpetrators
Data & Identity Theft Hackers invade business files and download user passwords, credit card information, social security numbers and other personal information, and steal money	Organizations that own data should use monitoring methods and encryption to detect and prevent intrusion. When it does occur, they must inform users and provide remedies. Individuals should monitor their financial accounts and may use credit monitoring services. Individuals should be cautious when using social networks. Do not share social security numbers or personal information
Industrial espionage & security Theft of trade secrets, marketing and financial data. Denial of service attacks	Know that your data is of interest to outsiders and take the threat seriously. Install and use strong detection programs and employ competent people to monitor. Use encryption. Use internal secure networks or remove of some operations from the internet. Use personal identification in addition to passwords. Develop or hire internal espionage facility to see how it is done. Backup and log all modifications.
Government and Military Intelligence & counterintelligence (monitoring transmissions, code breaking, content scanning and evaluation.) Disabling of military/industrial capability Destroying Infrastructure	Works both for and against our interests. Requires fundamental knowledge of computer design, communications, and programming systems. “Hacking at the highest and deepest level.” Use large and fast computers, sophisticated algorithms (pattern recognition and artificial intelligence). Use supplemental (human) intelligence to focus efforts. Disconnect von Neumann machines from the process
Overall	No system based on a von Neumann architecture can be made totally secure. There are, however, degrees of security, designed to match the degree of capability by the possible intruder.