

Information Security's Changing Threatscape

A Conversation with William P. Crowell, Former NSA Deputy Director

I recently had a conversation with William P. Crowell, former Deputy Director of the National Security Agency (NSA), about the changing threatscape of information security. I've known him for a number of years and because of his extensive professional background, his perspectives are always extremely insightful.

Crowell's involvement in security started in 1962 while working for the NSA. There, he held a series of senior positions over several decades within operations, strategic planning, research and development, and finance. In early 1994, he was appointed as the Deputy Director of NSA and served in that post until his retirement in late 1997. Few individuals have had such an extensive exposure to information security. As if several decades with the NSA weren't enough, he continues to be involved in information security in numerous roles in the private sector.

Today, he is an independent consultant specializing in information technology, security and intelligence systems.

BC: How did you get involved in information security at the NSA?

WC: While working as an intelligence officer for the NSA performing intelligence on information systems, I began to learn a lot about information security. There was a particular project that acted as a turning point for me and that set me on the information security path. I was asked to put some very sensitive information into a new computer system and I began asking questions about how well protected the system was. This was during the 1970s, and I was assured

that the information would be protected as well as any information possibly could because the system used very strong passwords.

I wasn't very convinced by that, so I asked for permission to test the system and that night I was able to gain access by simple password guessing. Then I found a file containing the passwords for all the other systems. From that point on, I always looked at problems from the perspective of both an attacker and a defender.

BC: It's interesting how passwords were a fundamental flaw in security then and many would argue that passwords are still one of the weakest links in information security today?

WC: It has not changed very much. Nothing is ever really a "new" problem.

BC: Obviously there are many stories that you won't be able to share, but is there one that really exemplifies the importance of strong information security?

WC: Back at the NSA in the 1970s, I ran a program that has since been declassified. The program was codenamed VENONA and it involved successful attempts by the United States to exploit the Soviet's KGB and GRU encrypted communications between 1943 and 1948. The exploitation went on for a very long time with the last message being read in 1980.

What was unique about the Soviet communication encryption was that it was double-encrypted material. It had been encoded with a two-part code and then encrypted with a one-time pad. One-time pads of course are essentially random numbers that are generated

once and used once, and if they are used properly it is impossible to read them irrespective of computing power.

BC: It sounds like the Soviets used their encryption correctly. Where was the breakdown?

WC: What we presume happened was that the bureau that produced the pads, under pressure during WWII, had decided to reuse the pads for another user besides the KGB and GRU. They used it for the Soviet Trade Organization. But, they were clever. They reversed the numbers on some pages and reversed the order of other pages to try and disguise the fact that they reused the keys.

Because of the reuse, the analysts were not only able to break through the enormous mathematical difficulties of the one-time pad, but one linguistic genius on the team, was able to substitute in his head all of the code values that had been used across all of the messages that had been broken before and figured out the codebook.

BC: That's amazing; so what was the net of this program?

WC: In the end 2,900 messages were read. The first message read, "Ethel age 32, two children, is the wife of Antenna." Antenna was the cover name for Julius Rosenberg.

BC: Julius and Ethel Rosenberg — the Americans executed for working for the KGB and giving the Soviets nuclear weapons secrets?

WC: Yes, and the entire situation was known from the very first message read,

and that's why there was so much controversy because some of the information that proved their guilt was not releasable because it was still classified.

BC: *What is the most fundamental change in security you've seen since circa 1960?*

WC: The principal change is that we've gone from communication security — protecting information in transit, to information security in a networked world where accessing information isn't just through a radio communication path, but through the network itself. Thus, we've created more avenues for attackers to get to even more information.

BC: *Let's talk a bit more about the attackers. We've all heard about organized crime, extortionists, exploit writers for hire, and identity thieves. But what's your perspective on threats from those groups that have government funding, militaries and intelligence agencies backing them: nation-states threats?*

WC: I think that the number of nation-states that can carry out credible cyber attacks has considerably increased, and that's a major change. There was a time which in order to be successful at attacking information systems, you had to: have a lot of money, be able to fly aircraft or spacecraft, be able to get close to borders, build expensive facilities to intercept communications, and have armies of people. Today, information system attacks are cheap and more nation-states are involved.

BC: *It sounds like if it is cheaper and easier for nation-states to launch attacks against information systems, then the same should apply across the board from script kiddies to terrorists?*

WC: Today, we have tens of thousands of attacks perpetrated by script kiddies.

Back in the days of communication security, you might have had some amateur radio operators that intercepted some Morse code, but nothing nearing the numbers of today's script kiddies. Also, information system attacks perpetrated by organized crime, drug cartels and terror networks are here today, but they are hard to separate from each other without detailed investigations.

Think of this as a Venn diagram where each group is independent yet at some point they overlap each other. This is why it is hard to definitively claim that an attack was motivated by a terror organization or an organized crime group. All these groups need to raise money to finance their agendas, and cyber crime is certainly an attractive alternative, partly because it requires so little in terms of resources. It has reduced risk and is relatively anonymous when compared to more traditional crimes like robbing a bank.

BC: *We've talked a bit now about threats from the outside, what are your thoughts on threats perpetrated by insiders such as trusted employees with legitimate access to information?*

WC: Malicious insiders have always been a problem; they are not new. What is new is that we've given them more keys to the kingdom. Insiders have greater access because businesses are network-based and broad access to critical assets is desired to make the business more efficient and effective. Businesses simply don't provide the same level of security for information assets that they do for their physical assets. For example, a business doesn't leave money sitting around; they put it in a safe. But most organizations leave information assets more vulnerable.

BC: *Speaking of physical security, what do you think about convergence — physi-*



cal and logical security coming together? Is it really just a matter of time before these two disciplines have some level of integration?

WC: Convergence can be driven by a number of different variables. Before the Internet as we know it today, there were mainframe networks that I worked on that were simple, direct connections to IBM mainframes and other large computers of the day using terminal protocols. Networks today use Ethernet and TCP/IP and allow us to connect very large numbers of PCs, servers and mainframes and don't require the expensive interconnection technology like those in the past. The Internet has allowed us to develop low cost network elements — routers, switches, wireless, and so on. This is creating a revolution in how we access information.

Now consider video surveillance. Until five years ago, all video cameras were connected via some type of analog connection. Now IP-based cameras are \$200 instead of \$2000 and the encoding is MPEG4 which uses about 1/3 the bandwidth needed before. So now we have a much more flexible, inexpensive solution that also allows for digital processing. We

We have moved toward a global economy in which the world's economies are interlinked and we become as vulnerable as any organization that we allow to connect into our critical information systems and networks.

can have a worldwide video surveillance system over IP that is less expensive than wiring a video surveillance system for a building in the analog world of a few years ago. And the newer, cheaper systems have a lot more capabilities like video analytics so you don't need 5,000 security guards to monitor 5,000 cameras.

Information assets and physical assets are both vulnerable. The safeguards for addressing these threats are either IP-enabled or quickly becoming so. Addressing information assets and physical assets in tandem through a centralized solution is practical and will eventually become the norm.

BC: *What are the key steps defenders must take to protect their organizations from attackers?*

WC: The attacker will always have the advantage – he only has to find one successful method for attack while the defender must know them all. To compound the problem, the defender is often limited by resources, politics and other constraints as to the steps they can take to defend the information assets. For example, if you decide Windows OS is a source of a lot of vulnerabilities, it isn't likely that it will be feasible to tell everybody to switch to a new OS once the organization is committed to Windows.

The defense has to outrun the offense, be more agile and adapt more quickly. This means being able to stop zero-day attacks, respond more efficiently to malware, have better managed key distri-

bution, use PKI based identity management and encryption systems, and spend more time putting layered security in place. Defenders need to protect and monitor these layers for malicious activity so they can stop an attack that gets through the first layer with certainty before it gets through the second layer.

BC: *What worries you most about the future of information security?*

WC: I have two primary worries. The first is that with our increasing dependence on networks to fight wars, our ability to defend ourselves could be jeopardized by simple and inexpensive attacks, and the second has to do with vulnerabilities in our business systems and therefore our economy. In both cases, we are moving towards information-based business and information-based warfare, so prudence dictates that we start paying more attention to information security than we have in the past.

In terms of defending ourselves consider the first Iraqi war. It was a physical war augmented by a considerable leap in information system capabilities to deliver intelligence. The second Iraqi war was much more of an information war. There were entire military groups in Iraq that didn't fight. It wasn't that they didn't fight because they were afraid, they didn't fight because of some very significant changes that occurred in the ways that the allies fought. Information was king, knowing where people were and putting them under threat early and making them

know that they were going to lose was a powerful resource in the war. We essentially invaded Iraq and took Bagdad and the rest of the country with less than 150 casualties during the initial campaign.

Everything about warfare is becoming network-centric. The Department of Defense has declared Network Centric Warfare as the policy for future force development. Operation of logistics, intelligence, and even small fighting units will all be dependent on information systems and networks. Enemies that can mount information attacks can put this network-centric system in a very dangerous state.

From an economic standpoint, more individuals and businesses alike are putting a greater amount of sensitive information into network based systems. Thus, this information quickly becomes more accessible from insiders and outsiders alike. We have moved toward a global economy in which the world's economies are interlinked and we become as vulnerable as any organization that we allow to connect into our critical information systems and networks.

BC: *What are you most optimistic about?*

WC: I'm beginning to believe that people are developing a balanced attitude about the role of technology, policy, process and people. To me, information security is a balance of all four of these. And there is no technology that will be successful if the other areas are not adequately addressed. Organizations are beginning to understand that throwing technology on top of bad policy, business processes or poorly trained people isn't the answer. With balanced measures in place an effective, dynamic and layered defense can be mounted. **ITD**

Brian T. Contos, CISSP, is the Chief Security Officer of ArcSight.



ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs. For more information, visit www.arcsight.com.