Week 5: Explore the Crypto Museum

No unread replies.No replies.

An extensive history of cryptography is presented at [http://www.cryptomuseum.com/ (Links to an external site.)](http://www.cryptomuseum.com/).  
Choose some specific method, machine, or technique profiled there and present a brief description of it, including your appraisal of how applicable it is to modern Information Security Management.

I chose the **Enigma Machine**, which I also gave a presentation on in WPI's cryptography course because of the importance it played in the history of cryptography, it’s role in WW2, and computer science in general. The enigma machine is responsible for the entire field of cryptography, and all the research that has gone into it since then. During the 1940’s there were no digital computers, and the enigma machine had a 214 or roughly 150 trillion different possible states in which it could be configured to produce a cipher text. It's no wonder why the Germans thought their code unbreakable at the time. However, what they didn’t account for was a critical design flaw.

Since the enigma was essentially an analog, electrical machine, all inputs were sent through wires from the keys to the wires embedded in the rotors. For the signal to make its way back to the user and show the encrypted letter on the lamp board, it had to use something called a reflector plate. This plate sent a signal **NEVER** back through the same path it came, which meant you could never encrypt C as C. Once the allies discovered this flaw, they were able to begin to remove the number of factors needed to decipher the possible rotor positions of the enigma. This was the key breakthrough that allowed Alan turnings machine to solve the enigma rotor positions which ultimately led to breaking the code every morning in 20 minutes after the initial weather report.

The importance of the enigma machine cannot be understated because it led to an entire field of computer science. Almost all our digital traffic is encrypted, and many things in our lives use some type of encryption to protect our assets or information. Today we use cryptography to have something like Bitcoin enable peer-to-peer global payments, which is truly a testament to all the work and research that came after WW2 to get us to this point. I can only imagine what the next 10 years holds for us with the continued development of quantum computers and quantum cryptography.

**Describe a situation in which "Company X" would benefit from SIEM**

A situation that “Company X” could benefit from if using an SIEM would be if an attacker attempted to modify an endpoint inside a company system. In my scenario “Company X” is a college that deals with thousands of emails per day, and one where staff are frequently opening attachments from students, faculty, and those outside the organization. An attacker could attempt to send a malware payload through email attachments, and if “Company X” were to have a SIEM like VMware’s Carbon Black Cloud in place, they could monitor affected endpoints and correlate the data with security logs, and previous network traffic to identify attackers. Carbon Black Cloud also allows organizations to see which endpoints or assets have been affected and allows organizations to quarantine them from the rest of the system to protect against privilege escalation. One of the most rampant forms of cyber-attacks today is ransomware, which is normally delivered through email attachments or software downloads. With “Company X” using Carbon Black Cloud, their system would remain online instead of having to pay an attacker in hopes of cooperation.