SANS Institute
InfoSec Reading Room

The Weakest Link: The Human Factor Lessons Learned from the German WWII Enigma Cryptosystem

This paper highlights the need for security professionals and management to not overlook the weakest link in security systems - that being the human factor. It is easy to become overly confident solely in the use of advanced algorithms and technology. History shows reliance on an advanced technology is doomed if the people operating the system are not fully trained and managed.

The Weakest Link: The Human Factor
Lessons Learned from the German WWII Enigma Cryptosystem

Prelude

With quadrillions of possible encryptions for each message, the German Enigma machine was, at its time, quite possibly the most advanced cryptosystem in the world. "If 1000 operators with captured machines tested four keys a minute 24 hours a day, it would take them 900 million years to try them all! The Germans were convinced that their codes were quite unbreakable." [1]

Objective

This paper highlights the need for security professionals and management to not overlook the weakest link in security systems – that being the human factor. It is easy to become overly confident solely in the use of advanced algorithms and technology. History shows reliance on an advanced technology is doomed if the people operating the system are not fully trained and managed.

Description of the German Enigma Cryptosystem

For roughly 20 years (1926-1945), the Germans employed a cryptosystem, called Enigma.

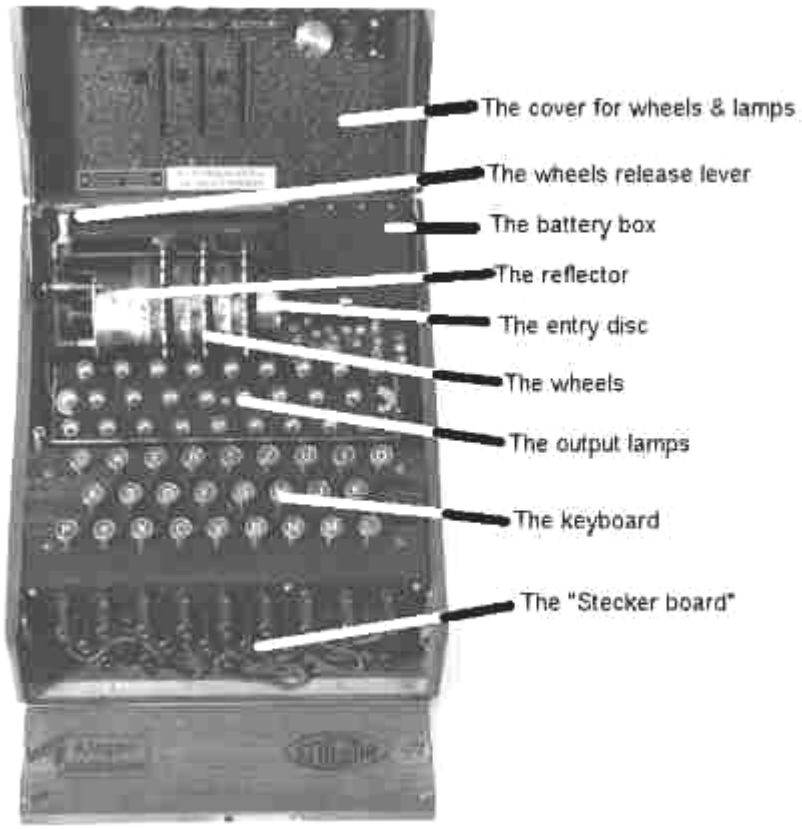


Figure 1: Photo of Enigma Machine, with cover open [2]

The cipher was an electro-mechanical portable device, which looked similar to a typewriter. (See Figure 1). An operator would press a character key on the keyboard, and an output lamp would illuminate the encoded substitution - a letter for letter serial cipher.

Electrical current would flow through a scrambling unit, made up of rotors. Each rotor was hardwired to make a substitution, from the 26 electrical contacts on one side to the 26 on the other. A rotor's internal wiring was not able to be modified. The rotors were placed side by side; one rotor's electrical output was the input of the next rotor.

The interesting feature of this device was the turning motion of the rotors. As one or more rotors moved, different electrical circuits would connect throughout the scrambling unit. This resulted

in identical initial input letters to have different substitutions, from the Enigma machine. For example, G typed three times might produce UAZ, instead of UUU.

A cipher with each letter correspondingly always having the same substitution would be considered a simple cipher. Below is an example of a simple cipher using a mono-alphabetic substitution. The bottom row comprises the substitutes for the corresponding top row plain text alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	S	E	X	D	R	C	F	T	V	G	Y	B	W	H	U	N	J	I	M	K	O	L	Q	A	P

Using the above as the cipher key, a message such as, "Panzers need fuel", would be encrypted as "UZWPD JIWDD XRKDY", (grouped in blocks of five). Simple ciphers can be broken using the fact certain letters of the alphabet are more often used than others. For instance, notice the number of times the letter 'e' was used in the previous sentence. With a large message, encrypted from a mono-alphabetic cipher, one can initially deduce the plain text by counting the occurrences of letters. The German Enigma system was not susceptible to this simple method of cracking because it was a poly-alphabetic system. Each time a key was pressed, one or more of the rotors would turn, resulting in essentially a different encoding alphabet, for each input letter.

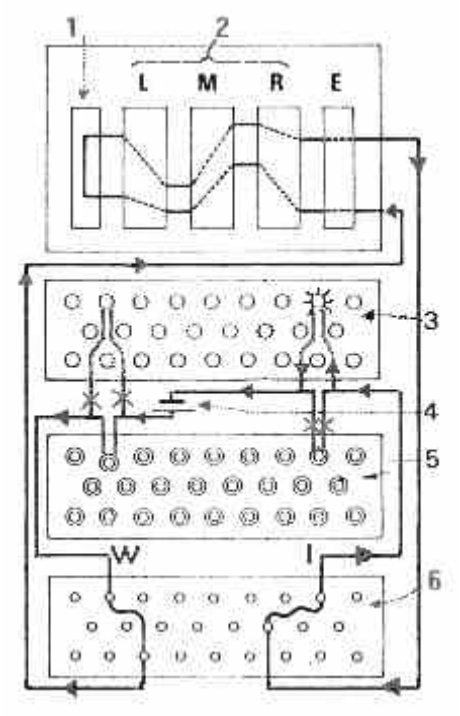
The rotors could be removed and inserted in a different sequence. The Germans had at least eight different rotors from which three were placed into the Enigma machine. One day the sequence might be VIII, III, VI, the next day the sequence might be III, V, I.

An adjustable ring on each rotor determined when its neighboring rotor to the left would rotate. The right-most rotor always turned $1/26^{th}$ of a full rotation, as each key was pressed. With enough turns (or key presses), the right-most rotor would come to the specified ring position causing the neighboring rotor to its left to turn $1/26^{th}$ of a rotation. This turning of the rotors can be likened to an odometer, with the 'turn-over' point adjustable on the rotors.

The German military added another layer of substitution, to the Enigma machine, not implemented on the early commercial version. A plugboard ("Stecker board") with patchcords was on the front of the Enigma machine. In this way, predetermined keyboard letters were substituted with another letter before being sent to the rotors. At first 6 patchcords were employed, but later this number was upped to 10.

One can see, the Enigma machine had several initial settings - the rotor sequence, the rings on the rotors, and the patchcords on the front. These start settings were called the "key".

A 'reflecting' mechanism, left of the rotors, sent the electrical signal back into the rotors in the opposite direction, through different contacts. This made the Enigma machine reciprocal. For example, if pressing T results in X lighting up, then pressing X (with the same settings) would result in T. Thus the 'reflecting' mechanism simplified the operational procedures of the Enigma cryptosystem, by allowing encoding and decoding using the same key settings.



(See Figure 2). "In this illustration, when key W is pressed on the keyboard (5) current from the battery (4) flows to the plugboard panel socket W, but socket W has been plugged to socket X so current flows up to the entry disc (E) at point X. The current then flows through the internal wiring in the rotors (2) to the reflector (1). Here it is turned round and flows back through the rotors in the reverse direction emerging from the entry disc at terminal H. Terminal H on the Entry disc is connected to socket H on the plugboard (6) but this socket is plugged to socket I so finally the current flows to lamp I which lights up. Thus in this instance, the letter W is enciphered to I." [4]

The keyboard was laid out as follows:

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

Figure 2: Circuit Diagram of Enigma [3]

Operation of the German Enigma Cryptosystem

Steps taken by both Sender and Receiver, (as prearranged for time and date):

1. set the rotor sequence (e.g. V, II, III).

2. set the rings (e.g. 14, 22, 04).

3. set the patchcords (e.g. D - E, T - F, C - Q, G - B, L - P, K - S).

Steps taken by the Sender:

1. turn the rotors to a "random" starting position, of his choosing (e.g. FRE), called the "indicator-setting".

2. type a "random" sequence code twice (e.g. YASYAS), called the "message-setting", which produced an output called the "indicator" (e.g. VIMWQZ).

3. again set the rotors, but this time to the "message-setting" (e.g. YAS), from the previous step.

4. key in the message into the Enigma machine, obtaining the encoded message.

5. using another device*, transmit to the receiver.
    * note: The Enigma machine was only an encoding/decoding device. It did not transmit or receive (or even print, for that matter).

The transmitted message had the following form:

1. in clear text, a preamble indicating call signs, time, length of message, and the "indicator-setting" (e.g. FRE – see Sender step #1).

2. in clear text, other various information about the message.

3. in clear text, the "indicator" (e.g. VIMWQZ – see Sender step #2).

4. the encrypted message.

Steps taken by the Receiver:

1. move the rotors to the "indicator-setting" (e.g. FRE)

2. key in the "indicator" (e.g. VIMWQZ), which would produce the "message-setting" (e.g. YASYAS).

3. move the rotors again, this time to the "message-setting" (e.g. YAS)

4. key in the encrypted message, for deciphering.

The Importance of Enigma

German forces swept most of Europe, with their "blitzkrieg", of Stuka dive-bombers, panzers and mechanized infantry. Poland was invaded in 1939, with incredible speed. France (which at the time, was considered superior in manpower, material and defensive positioning) was quickly dominated in 1940. U-boats of the German navy were crippling Great Britain. The island nation had a critical reliance to supply itself using merchant ships. Vital raw material was ever increasingly being sunk by U-boat 'wolf packs'. The Germans accomplished this through an efficient command and control. Generals and admirals most often kept in contact with field commanders through the use of radio communications. They knew the enemy could easily listen in on radio waves, so the Germans relied heavily upon the Enigma cryptosystem to keep messages secret.

The Enigma cryptosystem was designed to be secure, even if one or more Enigma machines fell into enemy hands. The 'keys' (initial settings) were changed daily (most often), and were issued to units by courier, on a monthly basis. The enormous combination of settings for the rotor sequence, rings and patchcords made the task of breaking the Enigma code a virtual impossibility. But the Allies did crack the code, due in large part to the human factor – the

combination of blundering and laziness of the operators, along with the German conviction that their cryptosystem would not be broken.

How Enigma was cracked

Three individuals from the Polish Cipher Bureau who stand out as pioneers in cracking the Enigma code are Marian Rejewski, Jerzy Rózycki and Henryk Zygalski. Through determination and perseverance they accomplished the many extraordinary steps needed to crack the Enigma cryptosystem. These pioneers purchased a commercial version of an Enigma machine, in the1920's, when the machines were still available. The French Intelligence service offered the Poles a booklet, obtained by a German traitor, describing the Enigma setup procedures. (The French and English, at the time, thought the information was impractical). The German traitor was later convinced to provide old (and what he thought, seemingly useless) messages in plaintext and coded format, along with the starting keys! Rejewski brilliantly set up mathematical permutation equations and was finally able to deduce the wiring of the rotors used.

At this point the Poles, remarkably, had a working model of the German's Enigma. But to decipher messages, the initial setting (or daily key) was needed. As it turns out, clues of the initial settings were frequently deduced because of procedural flaws and the lack of training of the German operators. The dangers of the human factor, were overlooked by the Germans, and continually compromised their most trusted cryptosystem.

One such example, of a procedural flaw and lack of training, was the Enigma operators were picking easy to guess "message-settings". Every Enigma machine was set to the 'daily key', but the sender was allowed to pick a so-called random "message-setting". Operators many times used keyboard 'shortcuts', such as diagonals (e.g. QAY *), repetitions (e.g. AAA), or girlfriends' initials. Many radio operators were identified by their 'fists' (their unique way in which they operated the radio transmitting device). By identifying the German operator, and knowing his tendency to use certain keyboard shortcuts, the Allies were sometimes able to group several messages together with guessed "message-settings", and painstakingly work out the daily key.

* note: see Standard German Keyboard Layout, By Phillip, Tim (January 1999)
URL: http://carbon.cudenver.edu/~tphillip/GermanKeyboardLayout.html

Also by identifying the operator, many times the military unit would be known. The Germans predictably sent messages with "to" and "from" the units involved. Knowing parts of the message beforehand, gives a foothold into cracking the code. One German operator faithfully transmitted "nothing to report" (if such was the case), everyday using the daily key.

Some careless Enigma operators, who did not set the machine to the new daily key settings, would resend the identical message again with the correct key. The Allies were able to find many clues by comparing the identical messages.

The blame should not be entirely on the Enigma operators. First, the German leaders initially did not properly train the operators. Secondly the doubly enciphered "message-setting" was a serious mistake. "This was a primitive form of error-correcting code, ensuring that this vital message key arrived correctly, despite possibly bad radio connections. But it meant transmitting

redundant information, and this mistake gave the Polish analysts their great success in the period just before the outbreak of war." [5]

Lastly and most importantly, the German leaders would simply not accept that their Enigma cryptosystem was being cracked. This was remarkable since German weather ships were being captured in 1941, giving the British the printed key sheets for an entire month, each time. The German leaders must have assumed all Enigma material and documentation would be properly destroyed by the crew. The arrogant German leaders failed to take the precaution of changing the monthly sheet of daily keys.

The Germans made improvements in the Enigma cryptosystem, as time progressed. In November 1937, the rotors were rewired. In December 1938, additional rotors to choose from were made. But this was all too late, because the Poles had developed a methodology into cracking the Enigma code.

The Poles met secretly with their British allies, and handed over the entire cracking operation, in July 1939, just weeks before Germany invaded Poland. At the time, the British were dumbfounded, as they were previously considering giving up on ever being able to crack the Enigma code. During the war, the British took over the Enigma cracking operations, which they codenamed Ultra, and centered it on an estate 40 miles from London, called Bletchley Park.

The Germans continued to improve upon Enigma – most importantly by tightening their procedural flaws. The practice of double enciphering the "message-setting" was dropped in May 1940. Operators were no longer allowed to randomly pick the "message-setting". Sheets were printed supplying operators with "message-settings".

Once the Americans were in the war, they facilitated Ultra. As the Germans improved Enigma, the Allies had to devote more and more resources to cracking the Enigma cryptosystem. By the end of the war 10,000 people and (newly-invented) computers were all working on Ultra – quite a change from three Polish mathematicians from years earlier.

Summary

"Enigma codes could have been unbreakable, at least with the methods available at the time, had the machine been used properly. The biggest mistake the Germans made was their blind belief in the invincibility of Enigma. Procedural errors in using the machine, combined with occasional operator laziness, allowed the Poles and, subsequently the British, to crack the "unbreakable" codes." [6]

The cracking of the Enigma cryptosystem can be thought of as, no less than, the most important secret operation of World War II. The Allies had countless advantages of knowledge over the Germans. Rommel's forces in Africa were defeated, in a large part, due to his supplies being destroyed crossing the Mediterranean. Ultra informed the Allies of the German supply schedules and routes. U-boats were reporting their positions to Admiral Dönitz, who directed the 'wolf pack' attacks. Once the naval version of Enigma was cracked, U-boats had the highest fatality rate of all the German services. The U-boat "happy times" were over.

The importance of breaking the German Enigma code cannot be underestimated. "Information from the decrypted messages was used by the Allies time after time to outmaneuver German armies. Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it." [7]

Simply put, the Germany's weakest link was the human factor.

Lessons learned

Today's managers and computer professionals face the ever-daunting tasks concerning IT security. These professionals must not fall victim to the weakest link – the human factor. Implementing the latest most advanced equipment and security safeguards are to no avail if all the users are not properly trained to be part of the security plan.

> There are numerous controls IT professionals can implement to safeguard electronic information from unauthorized users. But it's the authorized end users that possess the IDs and passwords to access that data giving them the ability to print it, share it, alter it or delete it. If they are careless with or choose weak passwords, casually discard confidential printed reports in the trash, prop open doors to secured areas, fail to scan new files for viruses, or leave back-ups of data unsecured, then that information remains at risk.
>
> A Security Awareness program is probably the most important weapon in the Information Security professional's arsenal. A company can have every security product known to the industry, but these products will be worthless in the face of the one user who disregards or is not even aware of the proper security procedures. This includes something as simple as keeping their password secret. [8]

Questions that must be addressed in any effective security plan are:
Have users properly been informed of their responsibilities? Do users understand and have access to the security policy? Are users able to pick easy to crack passwords? Do users have passwords written and near their work area, for instance posted on their monitors? Do users know not to re-use their business password(s) with any other username/password accounts? Do users have unauthorized software, such as PCanywhere or a web server, running on their desktop? Do users have unauthorized modems?

The above is not intended to be a complete and comprehensive checklist, but is given only as a start of a process of not overlooking the human factor. No security plan is effective without fully considering and integrating all end users (or operators). Every security plan ultimately rests upon the end users – a lesson learned from history.

References

Ludwig, Katherine. "Security Awareness: Preventing a Lack in Security Consciousness." (25 May 2001)
URL: http://www.sans.org/infosecFAQ/aware/lack.htm (20 August 2001)

Momsen, Bill. “Codebreaking and Secret Weapons in World War II.” (1996)
URL: http://home.earthlink.net/~nbrass1/1enigma.htm (23 August 2001)

Phillips, Tim. “Standard German Keyboard Layout.” (January 1999)
URL: http://carbon.cudenver.edu/~tphillip/GermanKeyboardLayout.html (25 August 2001)

Sale, Tony. “The components of the Enigma machine.” The Enigma cipher machine.
URL: http://www.codesandciphers.org.uk/enigma/enigma2.htm (22 August 2001)

Sale, Tony. “Military Use of the Enigma.” The Enigma cipher machine.
URL: http://www.codesandciphers.org.uk/enigma/enigma3.htm (22 August 2001)

The National Security Agency. “The Enigma.” National Cryptologic Museum.
URL: http://www.nsa.gov/museum/enigma.html (24 August 2001)

[1] Momsen, Chapter I.

[2] Sale, Components of the Enigma Machine.

[3] Sale, Components of the Enigma Machine.

[4] Sale, Components of the Enigma Machine.

[5] Sale, Military Use of the Enigma.

[6] Momsen, Chapter I.

[7] National Security Agency, The Enigma.

[8] Ludwig, Security Awareness.

Last Updated: May 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced