Mechanical Backdoors in Cold War Encryption Machines

Marcus H. Sachs
Chief Security Officer
Pattern Computer, Inc.
@MarcusSachs
Outline

- VERY Brief History Of Mechanical Encryption Machines
- Boris Hagelin And His Encryption Devices
- The William Friedman Papers
- A Gentlemen’s Agreement
- What We Know About NSA’s Initiative
- The Rest Of The Story
Very Brief History of Mechanical Encryption Machines

- First mechanical devices were leather strips wound around sticks
- Later devices used wood, ceramic, or metal
How They Worked

- Most encryption algorithms work on two principles:
  - Substitution (each letter retains its position but changes its identity)
  - Transposition (each letter retains its identity but changes its position)
- Early mechanical devices typically used the *substitution* principle
  - Caesar cipher shifts each letter three places down the alphabet
  - ROT-13 shifts each letter 13 places, making it a symmetric cipher
Simple Mechanical Cipher Machines

• Until the invention of the radio in the very late 19th Century, speed and strength of encryption was not an issue
  – Messages took minutes or hours to deliver, even over a telegraph
  – Number of “eyes” that could intercept the message was limited
  – Code-breaking was a manual process, and could take days or weeks

• Battlefield encryption used substitution ciphers
Businesses Needed Encryption, Too

- Commercial messages via telegram were vulnerable to eavesdropping
- Code books and mechanical substitution devices were in common use by the turn of the century
Rotor-based Cipher Machines

- Proliferation of radio in WWI created a need for faster encryption tools
- Typewriters and teletype machines were readily available in the 1910’s and served as models for a new approach
The Infamous Enigma Machine

- Invented in 1918
- Major advance in ease of use and cryptographic strength
- Originally designed for commercial and business customers
- Adopted by German military in late 1920s and early 1930s
- Used into the 1960s
Boris Hagelin And His Encryption Devices

- 1921 - first cipher machine developed while working for Arvid Gerhad Damm in Sweden
- 1935 – first mechanical machine under Hagelin’s brand name of A. B. Ingeniörsfirman Teknik (later changed to A. B. Cryptoteknik)
- After WWII, company moved to Switzerland as Crypto AG*
- Model numbers often reflect year of development
  - C-35 was developed in 1935
  - C-52 was developed in 1952

*AG is the abbreviation of Aktiengesellschaft
Hagelin vs Enigma

B-21 by Hagelin (1925)

Enigma by Heimsoeth und Rinke (1937)
Inside the B-21

- Keyboard and lamp panel are similar to the Enigma
- Enigma used alphabet substitution; B-21 used coding wheels to scramble a 5x5 matrix
Pin-and-Lug System versus Enigma-style Rotors-and-Bulbs

- **Pin and Lug**
  - Five or more wheels with pins, all relatively prime
  - 25-bar “drum” with lugs
  - Lugs interact with pins to create a pseudo-random stream of enciphered letters
  - No electric power – mechanical hand operation

- **Rotors and Bulbs**
  - Three or more rotors with 26 or more contacts
  - Rotation of rotors similar to a vehicle’s odometer
  - Pressing a key closes an electrical circuit
  - Battery or external power illuminates bulbs

https://www.youtube.com/watch?v=mcX7iO_XCFA
Various Hagelin Pin-And-Lug Devices

C-35
C-36
C-38
M-209
C-52 and CX-52
CD-57
Crypto AG in the 1950s

- T-52 1951–1952
- TMX-53 (Prototype) 1954
- TC-52 1954–1955
- T-55 1955–1956
- C-36
- C(X)-52 1951–1952
- B(C)-52 1956
- CD-55 1955–1956
- CD-57 1956–1957
- RTE-5 (WUMA) 1959–1960
- RT/C4 1954–1956
William Friedman (September 24, 1891 – November 12, 1969)

- US Army cryptographer who ran the research division of the Army's Signal Intelligence Service (SIS) in the 1930s, and parts of its follow-on services at the National Security Agency (NSA) into the 1950s
- Married to Elizebeth Friedman, also a cryptographer
- Initiated a secret agreement with Crypto AG in 1954
- William and Elizebeth’s personal papers were donated to the George C. Marshall Foundation in 1969
  - Contained documents mentioning a “Gentleman’s Agreement”
William Friedman Papers

- NSA requested that the papers be “sequestered” in 1976
  - Library complied, but reopened files from 1979-1983
  - Bamford found references to the “Boris project”
  - Papers were again closed by the NSA in 1983
- In 2015, over 52,000 pages of this collection were redacted and released to the public
  - Papers are available online via the US National Archives
Redaction Errors

- Process of reviewing and declassifying over 52,000 pages of material took NSA over two years
- Even though papers were over 50 years old, some information needed to remain secret to protect sources and methods
- Several cleared government officials were involved in the redaction process
  - Some papers had multiple copies
  - Those copies were not always reviewed and redacted by the same person
1. In accordance with letter dated 27 January 1955, as notified by L.O. 272 A dated 6 February 1955, I left Washington via N.Y.L. at 1000 hours on 28 February, arriving at Hong Kong, China, on 16 March. On 10 March, I arrived in Singapore, and on 12 March, I arrived in Bangkok, Thailand. On 14 March, I arrived in Tokyo, Japan, and on 15 March, I arrived in Seoul, Korea. On 16 March, I arrived in Shanghai, China, and on 17 March, I arrived in Hong Kong, China. On 18 March, I arrived in Tokyo, Japan, and on 19 March, I arrived in Shanghai, China. On 20 March, I arrived in Hong Kong, China, and on 21 March, I arrived in Tokyo, Japan. On 22 March, I arrived in Shanghai, China, and on 23 March, I arrived in Hong Kong, China. On 24 March, I arrived in Tokyo, Japan, and on 25 March, I arrived in Shanghai, China. On 26 March, I arrived in Hong Kong, China, and on 27 March, I arrived in Tokyo, Japan. On 28 March, I arrived in Shanghai, China, and on 29 March, I arrived in Hong Kong, China. On 30 March, I arrived in Tokyo, Japan, and on 31 March, I arrived in Shanghai, China. On 1 April, I arrived in Hong Kong, China, and on 2 April, I arrived in Tokyo, Japan. On 3 April, I arrived in Shanghai, China, and on 4 April, I arrived in Hong Kong, China. On 5 April, I arrived in Tokyo, Japan, and on 6 April, I arrived in Shanghai, China. On 7 April, I arrived in Hong Kong, China, and on 8 April, I arrived in Tokyo, Japan. On 9 April, I arrived in Shanghai, China, and on 10 April, I arrived in Hong Kong, China. On 11 April, I arrived in Tokyo, Japan, and on 12 April, I arrived in Shanghai, China. On 13 April, I arrived in Hong Kong, China, and on 14 April, I arrived in Tokyo, Japan. On 15 April, I arrived in Shanghai, China, and on 16 April, I arrived in Hong Kong, China. On 17 April, I arrived in Tokyo, Japan, and on 18 April, I arrived in Shanghai, China. On 19 April, I arrived in Hong Kong, China, and on 20 April, I arrived in Tokyo, Japan. On 21 April, I arrived in Shanghai, China, and on 22 April, I arrived in Hong Kong, China. On 23 April, I arrived in Tokyo, Japan, and on 24 April, I arrived in Shanghai, China. On 25 April, I arrived in Hong Kong, China, and on 26 April, I arrived in Tokyo, Japan. On 27 April, I arrived in Shanghai, China, and on 28 April, I arrived in Hong Kong, China. On 29 April, I arrived in Tokyo, Japan, and on 30 April, I arrived in Shanghai, China. On 1 May, I arrived in Hong Kong, China, and on 2 May, I arrived in Tokyo, Japan. On 3 May, I arrived in Shanghai, China, and on 4 May, I arrived in Hong Kong, China. On 5 May, I arrived in Tokyo, Japan, and on 6 May, I arrived in Shanghai, China. On 7 May, I arrived in Hong Kong, China, and on 8 May, I arrived in Tokyo, Japan. On 9 May, I arrived in Shanghai, China, and on 10 May, I arrived in Hong Kong, China. On 11 May, I arrived in Tokyo, Japan, and on 12 May, I arrived in Shanghai, China. On 13 May, I arrived in Hong Kong, China, and on 14 May, I arrived in Tokyo, Japan. On 15 May, I arrived in Shanghai, China, and on 16 May, I arrived in Hong Kong, China. On 17 May, I arrived in Tokyo, Japan, and on 18 May, I arrived in Shanghai, China. On 19 May, I arrived in Hong Kong, China, and on 20 May, I arrived in Tokyo, Japan. On 21 May, I arrived in Shanghai, China, and on 22 May, I arrived in Hong Kong, China. On 23 May, I arrived in Tokyo, Japan, and on 24 May, I arrived in Shanghai, China. On 25 May, I arrived in Hong Kong, China, and on 26 May, I arrived in Tokyo, Japan. On 27 May, I arrived in Shanghai, China, and on 28 May, I arrived in Hong Kong, China. On 29 May, I arrived in Tokyo, Japan, and on 30 May, I arrived in Shanghai, China. On 31 May, I arrived in Hong Kong, China.

Redactor 1

Redactor 2

Redactor 3
(Example of fully un-redacted text)

Ref: AJ436259

Redactor 1

Redactor 2

Redactor 3
(Example of partially un-redacted text)
Redacted Documents – Report of February, 1955 Visit (First mention of a “gentlemen’s understanding”)

Ref: A2436259

Ref: USCIB = United States Communications Intelligence Board

Redactor 1

Redactor 2

Redactor 3
BBC Story On Friedman And Hagelin

- Papers declassified and put online in April, 2015
- BBC story in July 2015 highlighted redaction mistakes
- Rejuvenated an old rumor that NSA and GCHQ had secretly worked with Crypto AG to develop “weaker” devices for non-NATO countries
Friedman and Hagelin’s “Gentleman’s Understanding”

- New Hagelin machines, in particular the CX-52 and the forthcoming TC-55 (teletype encryption) were of serious concern to the NSA, due to “insolvability”

- Friedman communicated with Hagelin using private stationary and his home address about the situation to avoid the delivery of NSA letters to a small town

- Friedman and Hagelin agreed to a “gentleman’s understanding” that Crypto AG would not sell the new devices until NSA could develop new guidance
Old vs New Crypto AG Machines – Six Month Agreement

M-209/C-38
**OK to sell to non-NATO**

C-446
**OK to sell to non-NATO**

CX-52
**Not OK to sell to non-NATO**
A Gentleman’s Understanding Becomes A Formal Arrangement - 1955

- Original understanding was for a six-month delay of sales (January to July, 1954) but was still in effect in February 1955

- New proposal was for NSA to develop instructions for NATO countries that would be different from instructions for non-NATO countries for the new machines
  - NATO instructions would ensure that very strong encryption was used
  - Non-NATO instructions would result in the devices producing weakened encryption
  - Crypto AG would not have access to the NATO instructions
  - Crypto AG could sell devices to any country, NSA would provide separate operating instructions to NATO users
Agreement Summary

- Crypto AG continues to sell C-446 and C-52 to countries Hagelin felt should have their messages intercepted and read
  - Crypto AG would inform NSA and GCHQ about technical specs of the machines and which versions were sold to which countries

- Crypto AG sells CX-52, TC-55, etc. to “friendly” countries
  - All customers receive Crypto AG instructions that, if followed, result in a weaker system
  - NATO countries provided with classified instructions (“brochures”) for much stronger encryption using the same machines

- Hagelin allowed to sell his machines in the US with no import/export restrictions

- Hagelin’s son-in-law had his active duty status in the US Air Force retained and a cousin of Hagelin's wife was employed by the NSA
Revelation Of “Backdoor” To Israel And Iran

- Secret deal disclosed to Israel by spy Jonathan Pollard in 1983
- Israel passed Hagelin information to Russia in exchange for increase in Soviet Jewish refugees
- Soviets already knew about the arrangement from spies Aldrich Ames and Robert Hanssen, and likely told Iran about the backdoor
- Former Iranian Prime Minister Shahpour Baktiar assassinated in 1991
- The day of the assassination, but before his body was found, US decoded a message to Iranian embassies, "Is Bakhtiar dead?"
In 1992, Iran kidnapped Crypto salesman Hans Buehler, accused of spying for US/Germany.

Buehler interrogated five hours per day for nine months but had no knowledge of the weaker Crypto AG devices.

Crypto AG and Siemens paid the million dollar ransom.

Buehler wrote a book about his ordeal and discoveries—Available online as a free PDF.

Boris Hagelin admits existence of special arrangement to Hagelin engineer, but Crypto AG denies it.

2015 release of Friedman papers confirmed the rumors.
The Rest Of The Story

- Accusation of the NSA deal by Iran caused Crypto AG sales and stock value to plummet
- Faced with bankruptcy, Crypto AG was saved by angel investor Marc Rich
- Rich was a resident of Zug and a fugitive billionaire with ties to Israel’s Mossad
- Speculated he used the agreement information for financial gain and to aid Israeli intelligence
- Clinton pardoned Rich in his last hours in the White House, January 2001
  - Rich’s attorney was Scooter Libby, later Cheney’s Chief of Staff, who outted CIA agent Valerie Plame and was later convicted of four felonies (Libby was pardoned by Trump in April 2018)

Marc Rich
(1934-2013)
Apply What You Have Learned Today

- Next week you should:
  - Review information you have made public that might be sensitive
- In the first three months following this presentation you should:
  - Verify the source and trustworthiness of your technology providers
  - Define appropriate controls for future purchases
- Within six months you should:
  - Verify that any dependencies you have on encryption use publicly recognized algorithms, and not privately developed ones
  - Read a book on security history and apply what you learned
Credits and References

Many thanks to the following websites for images, diagrams, and historical information:

- archives.gov
- bbc.co.uk
- cryptomuseum.com
- ciphermachines.com
- nf6x.net
- nsa.gov
- users.telenet.be