How To Rob A Bank

The SWIFT and easy way to grow your online savings
DISCLAIMER
The views expressed here are solely my own and do NOT reflect those of my employer.
A TALE OF TWO SERVERS
Once Upon a Time
There was a bank
Telex: How SWIFT messages used to move. (Source: Arnold Reinhold/CC.)
It needed ... Magic!
What Is SWIFT

• The Society for Worldwide Interbank Financial Telecommunications (if that doesn’t sound like something from a James Bond movie …)
• A secured and trusted exchange for financial messages
• Banks use it to send back end payment instructions to each other
• Brussels-based banking consortium
• Does NOT hold funds or manage accounts for customers
SWIFT Transactions for Dummies

- Each financial org gets a unique code of 8 or 11 characters. This is the BIC or Bank Identifier code or SWIFT ID or ISO 9363 code.

- The first 4 characters are the institute; next 2 are Country; next 2 or location/city; last 3 are branch codes and optional. Eg DEUTDEFF Deutche bank, Germany, Frankfurt.

- You can send a message through a SWIFT member bank if you have the recipients corresponding SWIFT code and account id.

- Other message services are Fedwire, CHIPS, Ripple but SWIFT is the biggest and best at doing this.
SWIFT By NUMBERS

Currently:

- 200 countries
- 10,800 users
- $9 trillion transferred daily
- Started 40 years ago
- 99.99 % availability (thank you mainframes)
“The global backbone of the financial industry”
TRUST ME
A Zero-Risk Approach to Failure

- Confidentiality
- Efficiency
- Reliability
- Security
- Resilient topology
- Robust software designs
Just How Does *This* Add Up to Security?

“Our record *availability* levels are a direct result, and proof of, our *security* commitment”
“We relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks, and eliminate operational inefficiencies”

What’s missing here?
Before any transaction can take place, the two banks create an agreement. This agreement, called the Relationship Management Application (RMA), defines the code and procedure for their unique messaging.

- Users enter the SWIFT system through an assigned computer connected to the SWIFT system via the Internet.
- After accessing SWIFTNet Link (SNL), the functions of SWIFT begin. The SNL has three consecutive gateways, where three authorised personnel at the bank play three key roles – Creator, Verifier and Authoriser.
- If the codes and other messaging procedures match with the scheduled procedure, the message is forwarded to VPN.
- From there it is forwarded to a router through which it enters SWIFTNet’s IP Secure Network (SIPN). It is then sent to the receiver portion of the partner network.
- Then the message is verified at every stage of the receiver’s network and sent to a VPN. If the message matches with the scheduled system, it is sent to the SNL of the receiver and if the assigned computer of the receiver body activated SNL activities, it is printed automatically.

The system verified Link level encryption (LLE) in SNL, SWIFTNet PKI and IP Security works on both sides of the network. If it does not match the previous encryption it stops the order and returns it to the sender.
Dangerous Assumptions

- Air-gapped is absolute. It isn’t
- Private networks ensure safety. They don’t
- Special systems operating in their own secure enclaves, with their own proprietary setups will remain impenetrable. They won’t
- Inherent Protections. Are not.
No Virginia, there is no Inherent Security
TRUST ISSUES

What do we know about TRUST people?

Complete the sentences

1. Trust ...

2. Trust ...
Who's afraid of the big, bad wolf?
Then one day

the Magic

stopped working
Allways chek for speling erors
### The SWIFT message

- This is one of the simpler messages
- It's easy to parse into strings but there are complex rules about how the fields relate to one another
- Constructing the message might also seem simple but get it wrong and SWIFT will fine you big-time!

---

**Example SWIFT Message:**

```
DATE OF ISSUE: XX
INSTANCETYPE AND TRANSMISSION: XX
20 NOTIFICATION (TRANSMISSION) OF ORIGIN SENT TO SWIFT (UK)
NETWORK DELIVERY STATUS: NETWORK LINK
PRIORITY/DUE DELIVERY: NORMAL
MESSAGE INPUT REFERENCE: XX

54/BANK SCREEN CODE: MT45222X/XX/
SWIFT: MT45222FMT452 FORMAT MESSAGE

SENDER BANK:

BANK ADDRESS:

BANK SWIFT CODE:

ACCOUNT NAME:

ACCOUNT NUMBER:

BANK OFFICER:

PHONE/FAX NUMBER:

TOD:

BANK NAME:

ADDRESS:

ACCOUNT NAME:

ACCOUNT NUMBER:

SWIFT CODE:

BANK OFFICER:

BANK OFFICER PHONE:

BANK OFFICER FAX:

BANK OFFICER EMAIL:

SWIFT MESSAGE TEXT:

20 TRANSACTION REF CODE:

22

34: PLACE OF ISSUE:

31C: DATE OF ISSUE:

31D: DATE OF EXPIRY:

33B: CURRENCY:

77C: NARRATIVE: TRANSACTION OF XX AS FOLLOWS:

We, ______, with head offices at ______, hereby confirm, certificate and recognize, with full bank responsibility, that M/S ________, is the legitimate beneficiary of the aforementioned ________ valued in the amount of ________ MUSEUM ISSUED on ________ 2013.

We further confirm as per instruction of M/S ________, that we have irrevocably blocked reserved and assigned the aforementioned ________ in favor of ________ for a period of one year and one month from ________ to ________ 2014 for ________.

This is clear, clean, free of any lien, liens or encumbrances and the rule of full disclosure has been established that such was legally obtained from non-criminal business activities.
```

---

**Relevance:**

Understanding SWIFT messages is crucial in the banking sector as they are used for international transactions. The message is structured with specific fields that need to be filled accurately to ensure successful transmission. The message text is typically embedded with critical information such as account details, transaction references, and confirmation of funds.
Banker’s Hours
Hello?
Bangladesh Bank heist

In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL

**Transaction date**

<table>
<thead>
<tr>
<th>Date Range</th>
<th>Location</th>
<th>Amount</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb. 4-5, 2016</td>
<td>Via New York Fed</td>
<td>$101 million</td>
<td>Via RCBC</td>
</tr>
<tr>
<td>Feb. 5-13</td>
<td>Via Philrem</td>
<td>$31 million</td>
<td>Weikang Xu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$29 million</td>
<td>Solaire*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$21 million</td>
<td>Eastern Hawai* Leisure Co.</td>
</tr>
</tbody>
</table>

**Money Trail Details**

- **$951 million**
  - 35 orders
  - Via SWIFT global bank messaging system

- **$101 million**
  - 5 orders
  - Via New York Fed

- **$81 million**
  - Four U.S. dollar accounts
  - Via RCBC

- **$850 million**
  - 30 orders
  - Via New York Fed

- **$20 million**
  - Shalika Foundation
  - Via Pan Asia Banking Corp.

- **$21 million**
  - Hackers misspelled name of the NGO

Sources: Philippines Court of Appeals documents; Reuters

* A casino resort owned and operated by Bloomberry Resorts

W. Foo, 31/03/2016
Hackers accessed SWIFT to Steal $81 Million & Erase Evidence

1. Attackers gain access and install malware
2. Malware decrypts config file containing search terms to scan within SWIFT messages
3. Malware identifies and exploits host’s SWIFT application to bypass validity check within Oracle DLL
4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016
5. SWIFT messages sent to printer are tampered with in real time
6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction
7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts
8. Checks the ‘Login/Logout’ status of the Journal table every hour and sends result to attacker domain over HTTP
Responsible for:
- Starting the database
- Backup and restore functions
- Reading database paths from registry

liboradb.dll

1. Malware infects server running SWIFT Alliance software
2. Malware lists all running processes on server
3. Malware checks to see if any processes have ‘liboradb.dll’ module loaded
4. If found, it overwrites 2 bytes at a specific offset with ‘do nothing’ (0x90 NOP) instructions
5. Overwritten bytes forces the host application to always pass the validity check
6. The malware is now able to execute database transactions
For example, the original code could look like:

```
85 C0  test eax, eax ; some important check
75 04  jnz failed ; if failed, jump to 'failed' label below
33 C0  xor eax, eax ; otherwise, set result to 0 (success)
  eb 17  jmp exit ; and then exit
failed:
B8 01 00 00 00  mov eax, 1 ; set result to 1 (failure)
```

Once it’s patched, it would look like:

```
85 C0  test eax, eax ; some important check
90    nop ; 'do nothing' in place of 0x75
90    nop ; 'do nothing' in place of 0x04
33 C0  xor eax, eax ; always set result to 0 (success)
  eb 17  jmp exit ; and then exit
failed:
B8 01 00 00 00  mov eax, 1 ; never reached: set result to 1 (fail)
```
2.1 Optional number of passes specified, filling with varying data depending on pass number

1. Original file is passed to function for secure deletion

Filename.log

DFB02
9815A
0AD69F6E8A
7B69F0DC73
1285564A27
19D5AFCC02
F62BC52A2E

2. File is filled with random data, occupying all associated disk sectors

Filename.log

DFB02
9815A
0AD69F6E8A
7B69F0DC73
1285564A27
19D5AFCC02
F62BC52A2E

dbgnaeypwtk

3. File name is renamed using random characters from lowercase a-z

4. File is deleted from disk
The Telltale Printer: "HP LaserJet 400 M401"
The Telltale Printer: "HP LaserJet 400 M401"

SILENCED
And another question

“Extensive integrity controls built into SWIFT apps to protect against unauthorized changes to messages and to detect corruption of messages”

SWIFT website

So how exactly did that Oracle db thing get by you?
“It was the bank's systems or controls that were compromised, not the software. The SWIFT software behaved as it was intended to, but was not operated by the intended person or process. This is a bank problem, not a SWIFT problem.“

William Murray, independent payments security consultant
## Heist by Numbers

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>BANK</th>
<th>AMOUNT</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangladesh</td>
<td>Bangladesh Bank</td>
<td>$81 Mil</td>
<td>Feb 2016</td>
</tr>
<tr>
<td>Philippines</td>
<td>Unnamed</td>
<td></td>
<td>2015</td>
</tr>
<tr>
<td>Ecuador</td>
<td>Banco Del Austro</td>
<td>$12 Mil</td>
<td>June</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Tien Phong Bank</td>
<td>Failed</td>
<td>June</td>
</tr>
<tr>
<td>Ukraine</td>
<td>Unnamed</td>
<td>$10 Mil</td>
<td>April</td>
</tr>
</tbody>
</table>
About that $10 switch ...
The FED vs SWIFT
“SWIFT is ... as flaky as ICS or SSL... you can’t separate workstations from SWIFT and remove them from the network.”

Risky Business Podcast
Now with MORE Security!
A SWIFT Response

- The new Customer Security Programme CSP
- 5 Steps to better security: 5 strategic initiatives
- Daily Validation Reports. Out of band access.
- “customer systems or operational staff that have been compromised and locally stored records that have been obfuscated”

While SWIFT’s network, software and services have not been compromised, each of these incidents took place after a customer suffered security breaches within its locally managed infrastructure.
## SWIFT New Core Security Standards

<table>
<thead>
<tr>
<th>3 Objectives</th>
<th>8 Principles</th>
<th>27 Controls</th>
</tr>
</thead>
</table>
| Secure Your Environment | 1. Restrict Internet access  
2. Segregate critical systems from general IT environment  
3. Reduce attack surface and vulnerabilities  
4. Physically secure the environment | • Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure  
• Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002 |
| Know and Limit Access | 5. Prevent compromise of credentials  
6. Manage identities and segregate privileges | • Some controls are mandatory, some are advisory  
• Documentation and collateral will be available by end of October |
| Detect and Respond | 7. Detect anomalous activity to system or transaction records  
8. Plan for incident response and information sharing | |
“The Swift payment system is only as strong as the operational controls built and enforced around it ... and a lack of strong policies and procedures for increased vulnerabilities.”

Mark Williams, lecturer at Boston University
“The Vietnam case shows that the global banking system is vulnerable to cyber attacks, and we should make a global effort to prevent these attacks”

Bangladesh Bank spokesman Subhankar Saha said Monday.
Who Dunnit?
It was the Lazarus Group,
It was the Lazarus Group, in North Korea,
It was the Lazarus Group, in North Korea, with a wrench
The targets of the Lazarus Group

The most affected regions and countries by the Lazarus group malware

Lazarus Group is a highly malicious entity responsible for data destruction as well as conventional cyber-espionage campaigns targeting financial institutions, media stations, and manufacturing companies, among others, since at least 2009.
A Common Thread
Typos are common in cyberattacks, as criminals rush through tasks to stay ahead of network defenders

<table>
<thead>
<tr>
<th>Event</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sony attack, 2014</td>
<td>“Mozillar” instead of “Mozilla”</td>
</tr>
<tr>
<td></td>
<td>“Fandation” instead of “foundation”</td>
</tr>
</tbody>
</table>

Source: BAE Systems
The Sony Hack

"How to Rob a Bank" by @3ncr1pt3d
Meanwhile, back on the ranch ...
“If we haven’t seen them in the US it’s because nobody’s bothered ... Most Western Banks have not had to deal with these attacks”

Brian Krebs on Risky Business podcast
“Banks are fighting a war on every conceivable front. It’s a losing battle. There’s no way to share enough information among enough people.”

Anonymous source
Who’s afraid of the big, bad wolf?
How the Carbanak cybergang stole $1bn
A targeted attack on a bank

1. Infection
   - Carbanak backdoor sent as an attachment
   - Bank employee
   - 100s of machines infected in search of the admin PC
   - Emails with exploits
   - Credentials stolen

2. Harvesting Intelligence
   - Intercepting the clerks’ screens

3. Mimicking the staff
   - How the money was stolen
     - Online-banking
       - Money was transferred to fraudsters’ accounts
     - E-payment systems
       - Money was transferred to banks in China and the US
     - Inflating account balances
       - The extra funds were pocketed via a fraudulent transaction
     - Controlling ATMs
       - Orders to disperse cash at a pre-determined time
Which brings us to ... Odinaff

- Discovered January 2016 attacking banks, securities, trading, payroll globally
- Mounted attacks on SWIFT users, malware hiding fraudulent transactions
- Lightweight backdoor Trojan
- Makes use of common hacking and legitimate software tools like mimikatz, PSEexec, Netscan, Powershell, Runas
- Malware designed to compromise specific computers. Requires a lot of manual intervention
- Linked to Carbanak through shared infrastructure, 3 C+C IP addresses, backdoor Batel
But what if I told you there was a fire-breathing dragon
Bigendian POC
Hospital ransomware + JBOSS

Here’s the plan:
We hold the hospital ransom for...

40 BITCOINS
What Would You Do Better?
The Moral of the Story

• Trust No One/Trust but Verify
• Go looking for the big bad wolf before you get eaten
• For God’s sake do the basics right
• Don’t Assume Anything. It makes an ass out of U and Me
Thank You!!

- @bigendiansmalls
- @mainframed767
- SecTor
- DefensiveSec, Brakeing Down Security and Risky Bus Podcasts
- Numerous members of the InfoSec community