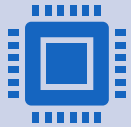
The "Illusion" of Privacy

SWAN Expo 2022

Who Are We?



Rudy Host – SWAN Systems Engineer

13 Years in Library Technology, 6 with SWAN

Secure System Design, Custom App Development

Ian Nosek – SWAN Systems Administrator

17 Years in Library Technology, 7 with SWAN

ILS and System Administration, Third-Party Integrations

Magic Time

What is SIP2?

- SIP2 is the industry standard for library authentication and self-service applications
  - Self-checks
  - Computer reservation systems
  - Material handling systems
  - Electronic Resources
  - Research Databases
- SIP (Standard Interchange Protocol) was developed by 3M to transmit user data between self-check systems and an ILS (Integrated Library System)
- Developed by 3M and released in 1993, with Version 2 of the SIP standard published in 2006

```
2022-07-26 14:06:38,084, 13408, INFO , IlsConnector, requestPatronInformation, Requesting user
information for 21140003533188
2022-07-26 14:06:38,085, 13408, INFO , IlsConnector, processSipRequest, Sending message on socket
2022-07-26 14:06:38,085, 13408, INFO , IlsConnector, processSipRequest, Sent message on socket
2022-07-26 14:06:38,085, 13408, INFO , IlsConnector, processSipRequest, Creating empty SipResponse
2022-07-26 14:06:38,086, 13408, INFO , IlsConnector, processSipRequest, Created empty SipResponse,
checking if connected
2022-07-26 14:06:38,086, 13408, INFO , IlsConnector, processSipRequest, Checked if connected,
getting reply from socket
```

What data does SIP2 carry?

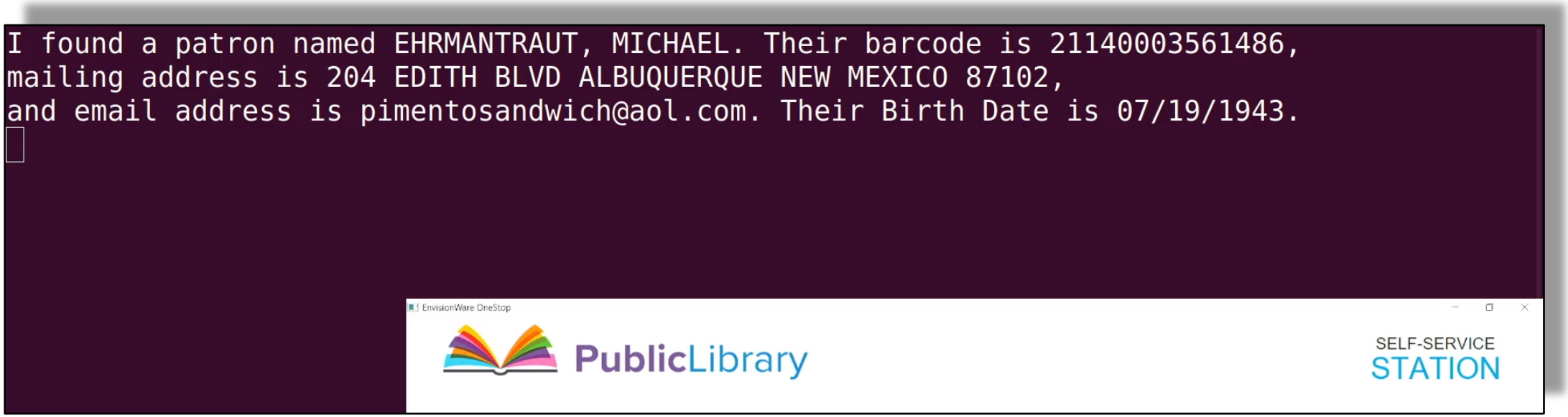
- Transactional data between client and server
- Patron authentication returns most of the personally identifiable information (PII) saved in the patron's record, including:
  - Name
  - Home Address
  - Email Address
  - Birthdate
  - Gender
  - Barcode
  - PIN

```
2022-07-26 14:06:38,158, 13408, INFO , SyncSocketDevice, readData, Received: 64      00020220726
140638000000000020001000000000
AOWMS|AA21140003533188|AENOSEK,IAN|AQSWS|BZ0075|CA0000|CB0200|BLY| BV15.00|BD800 QUAIL RIDGE DR
WESTMONT IL 60559-6149|BEian@swanlibraries.net|BHUSD|PD19830618|PCSWS_STAFF|PEMALE|PFADULT|PG
```

Ubiquitous but Flawed

- The SIP2 standard does not offer any native encryption
  - Encryption is a way to conceal information by altering it so that it appears to be random data.

- All data passed via SIP2 is delivered in plain-text



What is SWAN doing?

- SWAN is no longer configuring any external SIP2 connections unless they explicitly support TLS encryption
- Existing vendors will eventually be required to use an encrypted port
- We are currently working with Overdrive on TLS implementation, and anticipate having Overdrive secured later this year
- SIP2 is ubiquitous, but there are other authentication methods available
  - OpenAthens Proxy – Supports basic barcode authentication and is used for the majority of research databases
  - Web Services – A proprietary SirsiDynix API which serves as the connection method for Aspen, Communico, BLUEcloud, and others

Securing SIP2 Traffic

- While SIP2 traffic is unencrypted, SWAN is actively working to increase the security of all transmitted PII
- All SIP2 connections internal to the library (reservation systems, self-checks, etc.) are encrypted by way of the VPN tunnel that connects each library to SWAN
- Most external vendors (Overdrive, Hoopla, etc.) are not currently encrypted, but options are available to secure these connections
  - TLS-SIP2 encrypts transmitted data via Transport Layer Security (TLS) SirsiDynix supports TLS-SIP2 natively in our current version
  - Stunnel is an open-source application that is capable of securing connections that have no native encryption

What can you do?

- Consult with SWAN prior to selecting new vendors
  - Each vendor integration requires a unique configuration on our server
  - The sooner we're involved, the faster we can identify any challenges
- Ask potential vendors what authentication types they support
  - While most vendors will simply request a SIP2 connection, there may be other authentication methods that satisfy a vendor's requirements
- Principle of Least Access
  - *Only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary (remember to relinquish privileges). Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. Therefore, careful delegation of access rights can limit attackers from damaging a system.*

Magic revealed

```
payload_data = ByteStringToString(packet.tcp.payload)

barcode = re.search("\|AA(.+?)\|", payload_data)[1]
name = re.search("\|AE(.+?)\|", payload_data)[1]
address = re.search("\|BD(.+?)\|", payload_data)[1]
email = re.search("\|BE(.+?)\|", payload_data)[1]
birthdate = re.search("\|PD(.*?)\|", payload_data)[1]
formatted_birthdate = f'{birthdate[4:6]}/{birthdate[6:8]
os.system('clear')
print(f'I found a patron named {name}. Their barcode is
```

Raspberry Pi	• Small computer running Linux OS
VPN software	• Connection back to SWAN servers
Very small Python script	• Intercepting and interpreting SIP2 traffic

Repeat Demo

Questions?