SANGOMA

STIR/SHAKEN

Ben Ford
Software Engineer
Sangoma Technologies

About Me

SANGOMA

Moving On to STIR/SHAKEN

© Copyright 2020 Sangoma Technologies

What Is STIR/SHAKEN?

- Secure Telephony Industry Revisited (STIR)
- Signature-based Handling of Asserted Information using toKENs (SHAKEN)

© Copyright 2020 Sangoma Technologies

Cool, But What Does It Do?

- A method to combat call spoofing on public telephone networks
- Calls may appear like they are coming from a place you know, but are they really?

SANGOMA © Copyright 2020 Sangoma Technologies

STIR

- Add digital certificates to SIP headers to help secure calls
- Used to verify the source of a call
- Relies on private and public keys
- What level of trust is it?

© Copyright 2020 Sangoma Technologies

SHAKEN

- Responsible for tokens
- Identify missing STIR information
- SIP not present in original telephony network

© Copyright 2020 Sangoma Technologies

How It’s Useful

Stating the Obvious

- Helps prevent fraudulent calls
- You’re much more likely to answer a call if you recognise the…
  - Number
  - Caller ID
  - Area code

© Copyright 2020 Sangoma Technologies

“Harmless” Cases

- A call from an unknown number
- Suspected spam callers
- Telemarketers

© Copyright 2020 Sangoma Technologies

Dangerous Cases

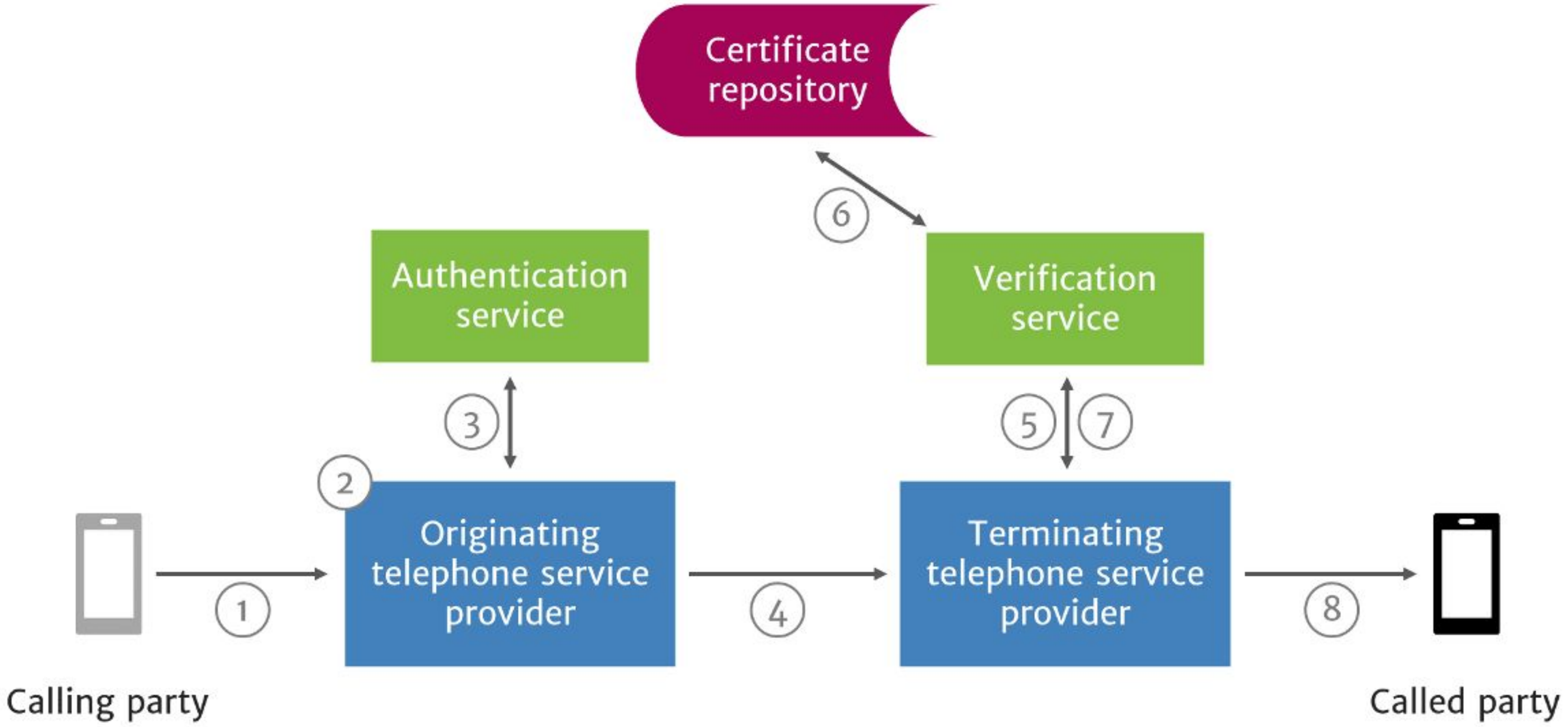
- You get a call from the bank
- “We have reason to believe someone has stolen your credit card information…”
- You may recognise the source, but you wouldn’t know the person on the other end of the phone
- Other popular scenarios include but are not limited to:
  - IRS, delivery charge not paid, a warrant for your arrest

© Copyright 2020 Sangoma Technologies

How Does It Work?

SANGOMA

https://transnexus.com/whitepapers/understanding-stir-shaken/



© Copyright 2020 Sangoma Technologies

Attestation

- Done when an INVITE is received by the provider
- Three different levels
  - **Full Attestation (A)**: the provider authenticated the calling party and they are authorized to use the number
  - **Partial Attestation (B)**: the provider authenticated the call origination, but cannot verify if they are authorized to use the number
  - **Gateway Attestation (C)**: the provider authenticated where the call was received, but cannot authenticate the source

SIP Identity Header

- Contains STIR/SHAKEN information
  - Calling number
  - Called number(s)
  - Timestamp
  - Attestation
  - Origination identifier
  - Other standard STIR/SHAKEN required fields

© Copyright 2020 Sangoma Technologies

SIP Identity Header

https://transnexus.com/whitepapers/understanding-stir-shaken/

```
INVITE sip:18001234567@example.com:5060 SIP/2.0

Via: SIP/2.0/UDP example.com:5060

From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789

To: "Bob" <sip:18001234567@1.2.3.4:5060>

Call-ID: 1-12345@5.6.7.8

CSeq: 1 INVITE

Max-Forwards: 70

Identity:
eyJhbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogImh0dHBzOi8vY2VydGlmaWNhdGVzLmNsZWFyaXAuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVkMTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQifQ.eyJhdHRlc3QiOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2NjA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgwMDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhNDdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtk89P6a6ru0ncDfSrdb1GyK_mJj-10hsLW-dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.clearip.com/b15d7cc9-0f26-46c2-83ea-a3e63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>alg=ES256;ppt=shaken
```

© Copyright 2020 Sangoma Technologies

Verification

- Identity header is used to verify the source
- The header and payload are BASE64 decoded
- The public certificate is obtained from a repository and used to verify the signature
- The chain of trust is then verified

© Copyright 2020 Sangoma Technologies

How Does It Work In Asterisk?

New Configuration

- stir_shaken.conf
- 3 different sections
  - general
  - certificate
  - store

New Configuration - general

- **ca_file**: path to the certificate authority certificate
- **ca_path**: path to the chain of trust
- **cache_max_size**: the maximum size to use for caching public keys
    - Puts a limit on how many downloaded public keys we store

© Copyright 2020 Sangoma Technologies

New Configuration - general

- **curl_timeout**: the maximum amount of time (in seconds) to wait before timing out a cURL request
  - Allows flexibility based on network
- **signature_timeout**: the amount of time (in seconds) a signature will be considered valid
  - Uses the timestamp provided in the STIR/SHAKEN header

© Copyright 2020 Sangoma Technologies

New Configuration - certificate

- **path**: the path to the certificate
- **public_key_url**: the public key URL where the public key can be retrieved
- **caller_id_number**: the caller ID number to match on
  - Subject to change in the future
- **attestation**: the level of trust for this certificate
  - A, B, or C

© Copyright 2020 Sangoma Technologies

New Configuration - store

- Future work

© Copyright 2020 Sangoma Technologies

New Configuration - stir_shaken.conf.sample

```
[general]
ca_file=/etc/asterisk/stir/ca.crt
ca_path=/etc/asterisk/stir/ca
cache_max_size=1000
curl_timeout=2
signature_timeout=15

[certificates]
type=store
path=/etc/asterisk/stir
public_key_url=http://mycompany.com/${CERTIFICATE}.pub
```

```
[alice]
type=certificate
path=/etc/asterisk/stir/alice.crt
public_key_url=http://mycompany.com/alice.pub
caller_id_number=1234567
attestation=B
origid=MyAsterisk
```

© Copyright 2020 Sangoma Technologies

New Configuration - pjsip

- To make use of the stuff we just covered…
- STIR/SHAKEN support needs to be enabled
- Support is enabled **per endpoint**
- Applies to inbound and outbound
- In pjsip.conf…

  -
    ```
    [my_endpoint]
    stir_shaken=yes
    ```

© Copyright 2020 Sangoma Technologies

Outbound INVITE

Outbound INVITE

- Much simpler than inbound INVITEs
- We have an endpoint (1234)
- Before anything else, enable STIR/SHAKEN support!

© Copyright 2020 Sangoma Technologies

Outbound INVITE

- stir_shaken.conf needs some information to let Asterisk know what to do

```
[my_cert]
type=certificate
path=/path/to/my_cert.crt
public_key_url=http://example.com/my_pub_cert.crt
caller_id_number=1234
attestation=B
origid=MyAsterisk
```

© Copyright 2020 Sangoma Technologies

Outbound INVITE

- If you want to generate some certificates for testing…
  - https://github.com/asipto/secsipidx/
  - openssl ecparam -name prime256v1 -genkey -noout -out ec256-private.pem
  - openssl ec -in ec256-private.pem -pubout -out ec256-public.pem

© Copyright 2020 Sangoma Technologies

Outbound INVITE

- With STIR/SHAKEN support enabled and the mappings in place, Asterisk handles the rest
- On outbound calls from 1234, an Identity header is added to the SIP message

© Copyright 2020 Sangoma Technologies

Inbound INVITE

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- More involved than outbound INVITEs
- Outbound INVITEs just add Identity header
- Asterisk actually needs to do verification

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- We MUST have an Identity header
- Contains all the information we need to verify a call

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- Identity header contains a JSON web token
  - header.payload.signature
- Full format is…

<encoded header>.<encoded payload>.<signature>;info=<public key URL>alg=ES256;ppt=shaken

© Copyright 2020 Sangoma Technologies

Inbound INVITE - header

https://transnexus.com/whitepapers/understanding-stir-shaken/

INVITE sip:18001234567@example.com:5060 SIP/2.0

Via: SIP/2.0/UDP example.com:5060

From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789

To: "Bob" <sip:18001234567@1.2.3.4:5060>

Call-ID: 1-12345@5.6.7.8

CSeq: 1 INVITE

Max-Forwards: 70

Identity:
eyJhbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogImh0dHBzOi8vY2VydGlmaWNhdGVzLmNsZWFyaXAuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVkMTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQifQ.eyJhdHRlc3QiOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2NjA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgwMDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhNDdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtk89P6a6ru0ncDfSrdb1GyK_mJj-10hsLW-dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.clearip.com/b15d7cc9-0f26-46c2-83ea-a3e63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>alg=ES256;ppt=shaken

© Copyright 2020 Sangoma Technologies

Inbound INVITE - header

- Header is BASE64 encoded
- Contains 4 fields we care about
  - **alg**: the encryption algorithm (must be **ES256**)
  - **ppt**: the extension (must be **shaken**)
  - **typ**: the token type (must be **passport**)
  - **x5u**: the location of the certificate used to sign the token

© Copyright 2020 Sangoma Technologies

Inbound INVITE - payload

https://transnexus.com/whitepapers/understanding-stir-shaken/

```
INVITE sip:18001234567@example.com:5060 SIP/2.0

Via: SIP/2.0/UDP example.com:5060

From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789

To: "Bob" <sip:18001234567@1.2.3.4:5060>

Call-ID: 1-12345@5.6.7.8

CSeq: 1 INVITE

Max-Forwards: 70

Identity:
eyJhbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogImh0dHBzOi8vY2VydGlmaWNhdGVzLmNsZWFyaX
AuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVkMTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQi
fQ.eyJhdHRlc3QiOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2NjA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgw
MDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhNDdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtk89P6a6ru0ncDfSrd
b1GyK_mJj-10hsLW-dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.clearip.com/b15d7cc9-0f26-46c2-83ea-a3e
63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>alg=ES256;ppt=shaken
```

Inbound INVITE - payload

- Payload is BASE64 encoded
- Contains 3 fields we care about
    - **attest**: the attestation level (must be **A**, **B**, or **C**)
    - **iat**: the timestamp from when the token was created
    - **orig**: the calling number or identifier
        - **tn**: the transaction number

© Copyright 2020 Sangoma Technologies

Inbound INVITE - signature

https://transnexus.com/whitepapers/understanding-stir-shaken/

```
INVITE sip:18001234567@example.com:5060 SIP/2.0

Via: SIP/2.0/UDP example.com:5060

From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789

To: "Bob" <sip:18001234567@1.2.3.4:5060>

Call-ID: 1-12345@5.6.7.8

CSeq: 1 INVITE

Max-Forwards: 70

Identity:
eyJhbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogImh0dHBzOi8vY2VydGlmaWNhdGVzLmNsZWFyaX
AuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVkMTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQi
fQ.eyJhdHRlc3QiOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2NjA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgw
MDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhNDdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtk89P6a6ru0ncDfSrd
b1GyK_mJj-10hsLW-dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.clearip.com/b15d7cc9-0f26-46c2-83ea-a3e
63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>alg=ES256;ppt=shaken
```

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- If everything is present, Asterisk can determine if call was spoofed
- STIR/SHAKEN support must be enabled on endpoint

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- Reasons verification can fail
  - No STIR/SHAKEN information is available
  - A field does not have the required value
  - The token is expired
  - The signature does not work with provided key
  - Caller ID mismatch

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- The verification result can be queried in dialplan
- New dialplan function: STIR_SHAKEN()
- Has two different variations

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- STIR_SHAKEN(count)
  - Returns the number of STIR/SHAKEN results for the channel
  - Useful for the other variation

```
exten => example,NoOp(Number of STIR/SHAKEN identities: ${STIR_SHAKEN(count)})
```

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- STIR_SHAKEN(index, field)
  - Returns information about a specific result
  - Index based (0 being the first entry)
  - Three possible values for field
    - **identity**: the STIR/SHAKEN identity
    - **attestation**: the attestation level (**A**, **B**, or **C**)
    - **verification_result**: the verification result

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- verification_result can be used to determine what to do with a channel after verification has been performed
- Possible results
  - **Verification not present**
  - **Signature failed**
  - **Verification mismatch**
  - **Verification passed**

© Copyright 2020 Sangoma Technologies

Inbound INVITE

- Easy to pass a call through
- Flexible call handling
- Full control over dialplan call flow

© Copyright 2020 Sangoma Technologies

Inbound INVITE

```
same => n,NoOp(Identity ${STIR_SHAKEN(0, identity)} has attestation level ${STIR_SHAKEN(0, attestation)})
same => n,NoOp(Verification result - ${STIR_SHAKEN(0, verification_result)})
```

© Copyright 2020 Sangoma Technologies

Future Work

SANGOMA

Certificate Stores

- Configuration is set up for a “store” of certificates
- Reads in a directory and processes each certificate in the directory

© Copyright 2020 Sangoma Technologies

Caller ID Ranges and Lists

- Allow for more than one caller ID per certificate via a range or list mechanism

© Copyright 2020 Sangoma Technologies

Caller ID On Certificate

- As a follow up to caller ID ranges
- Caller ID numbers should be fetched from the certificate itself
- No need to specify caller ID number via configuration

© Copyright 2020 Sangoma Technologies

Thank You!

bford@sangoma.com

SANGOMA