SO YOU'VE DECIDED TO HACK SHAKEN STIR
Hacking SHAKEN/STIR

White-Hat Vulnerability Analysis
ECG.

Staff Augmentation & Consulting.


US / Canada / Europe Service Providers & Enterprise Federal / State / Municipal

Mark R Lindsey mark@ecg.co @markrlindsey
Don’t bother hacking fundamental math & protocols of SHAKEN/STIR.

So the real weaknesses will be in real networks...
1. Steal Service Provider Private Key

- Corporate data stolen from enterprises regularly
- Theft of Private Certificate Keys would potentially let others sign with your SPID
Legitimate Network

"Caller Verified" Indication

Signed PASSporT

SHAKEN via HTTPS

Path of Phone Call

SBC - Session Border Controller

(Access) P-CSCF

Core Trusted

Caller Alice

SBC - Session Border Controller

 Caller Call Control Servers

Core Trusted

Untrusted Access Network

SIP Intermediate Providers

STI-AS Authentication Service

Untrusted Peering Network

SBC - Session Border Controller

(SIP Interconnection) IBCF

Core Trusted

Untrusted Peering Network

SBC - Session Border Controller

(SIP Interconnection) IBCF

Core Trusted

Untrusted Access Network

SBC - Session Border Controller

(Access) P-CSCF

Core Trusted

Callee Call Control Servers

Callee Bob

Certificates

STI-VS Verification Service

Call Direction
Compromised Private Keys
Compromised Private Keys

- Compromised Private Keys

- STI-AS Authentication Service

- SIP Intermediate Providers

- Calls

- Call Control Servers

- SBC - Session Border Controller

- Core Trusted

- SBC - Session Border Controller

- (Access) P-CSCF

- Caller Call Control Servers

- Core Trusted

- Untrusted Peering Network

- SBC - Session Border Controller

- (SIP Interconnection) IBCF

- Core Trusted

- Untrusted Peering Network

- SBC - Session Border Controller

- (SIP Interconnection) IBCF

- Core Trusted

- Untrusted Access Network

- SBC - Session Border Controller

- (Access) P-CSCF

- Core Trusted

- Callee Call Control Servers

- Core Trusted

- Certificates

- STI-VS Verification Service

- SHAKEN via HTTPS

- "Caller Verified" Indication

- Signed PASSporT

- Path of Phone Call

- Caller Alice

- Callee Bob
Compromised Private Keys

"Caller Verified" Indication

SHAKEN via HTTPS

Path of Phone Call

Signed PASSporT

"Caller Verified" Indication

Untrusted Access Network

Core Trusted

SBC - Session Border Controller

P-CSCF

Core Trusted

STI-AS Authentication Service

Untrusted PoP Network

Path of Phone Call

SIP Intermediate Providers

Core Trusted

Untrusted Access Network

STI-VS Verification Service

Core Trusted

Untrusted Peering Network

SBC - Session Border Controller

P-CSCF

Core Trusted

Callee

Bob

SBC - Session Border Controller

(Access)

P-CSCF

Core Trusted

Callee

Alice

Callee

Attacker

"Caller Verified" Indication

Untrusted Access Network

Core Trusted

SBC - Session Border Controller

P-CSCF

Core Trusted

STI-AS Authentication Service

Untrusted PoP Network

Path of Phone Call

SIP Intermediate Providers

Core Trusted

Untrusted Access Network

STI-VS Verification Service

Core Trusted

Untrusted Peering Network

SBC - Session Border Controller

P-CSCF

Core Trusted

Callee

Bob

SBC - Session Border Controller

(Access)

P-CSCF

Core Trusted

"Caller Verified!"
How to hack a whole service provider

- Steal Private keys from the Service Provider using tnAuthList with SPID only
- Use legitimate SHAKEN protocol to create certificates for fraudulent calls
- Send calls with fraudulent PASSporT
### Hack Service Provider Private Keys
Can my network be attacked like this?

<table>
<thead>
<tr>
<th>Caller Voice Network Technology</th>
<th>Factors affecting attack source</th>
<th>Risk of sourcing attack</th>
<th>Risk of receiving attack -- fraudulent “Caller Verified”</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCaaS &amp; Hosted PBX</td>
<td>Malware &amp; Social Engineering.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>SIP Trunking</td>
<td>Malware &amp; Social Engineering.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>IMS / Mobile</td>
<td>Malware &amp; Social Engineering. Likely to have <em>many</em> certificates – only one needed to attack</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
What makes this hack harder?

Train staff to handle SHAKEN keys carefully – better than is standard for HTTPS SSL certs!

OS and Application Patching to minimize malware.

Use SHAKEN Certificates with Telephone Numbers in tnAuthList, not just SPID
2. Hack registering SIP devices

- Callee has to authenticate the calling party -- so trick it into believing you’re authentic.

- If you can steal a user's registration, launch calls from that user with full SHAKEN attestation.
Legitimate Network

"Caller Verified" Indication

Signed PASSporT

Path of Phone Call

SHAKEN via HTTPS

Call Direction
Compromised Network

“Caller Verified” Indication

SHAKEN via HTTPS

Certificates

STI-AS Authentication Service

SIP Intermediate Providers

P-CSCF

Core Trusted

Call Control Servers

SBC - Session Border Controller

(Untrusted Access Network)

(Interconnection)

IBCF

Untrusted Peering Network

Untrusted Access Network

Attacker

Path of Phone Call

Signed PASSporT

Signed PASSporT

"Caller Verified" Indication

SHAKEN via HTTPS

Call Direction

Call Verified!
How to hack registering SIP device

- Discover / Steal SIP credentials
- Scan, or Hack Device Management at the Service Provider
- Disclosed Device Configurations used to discover SIP credentials.
- Penetrate the Customer’s SIP device itself
- Hacked Provisioning platforms
**Hack registering SIP devices**
Can my network be attacked like this?

<table>
<thead>
<tr>
<th>Caller Voice Network Technology</th>
<th>Factors affecting attack source</th>
<th>Risk of sourcing attack</th>
<th>Risk of receiving attack -- fraudulent “Caller Verified”</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCaaS &amp; Hosted PBX</td>
<td>SIP Authentication. Device Config discovery. Open to Internet.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>SIP Trunking</td>
<td>No Device config accessible. Often limited IP range.</td>
<td>MODERATE</td>
<td>HIGH</td>
</tr>
<tr>
<td>IMS / Mobile</td>
<td>Private networks.</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
What makes this hack harder?

- Modern/Secure Device Management, e.g., Mutual TLS
- Strong SIP passwords
  Automatically-enforcement
- SBC Scanning prevention
  Blacklisting password scanners
3. Hack SIP Trunking & Peering

- Trick the callee’s system into believing you’re authentic
- Easiest: Exploit enterprise security. Compromise the SIP trunk customer’s network
Compromised Network

- **Customer SIP PBX**
  - SIP Trunk
  - SBC - Session Border Controller (Access) P-CSCF
  - Caller Call Control Servers
  - Core Trusted

- **Untrusted Access Network**
  - SBC - Session Border Controller (Access) P-CSCF
- **Untrusted Peering Network**
  - SBC - Session Border Controller (SIP Interconnection) IBCF
  - Core Trusted

- **SIP Intermediate Providers**
- **Untrusted Peering Network**
  - SBC - Session Border Controller (SIP Interconnection) IBCF
  - Core Trusted

- **Callee Call Control Servers**
  - Core Trusted

- **Untrusted Access Network**
  - SBC - Session Border Controller (Access) P-CSCF

- **Callee Bob**

- **Certificates**
  - **STI-AS Authentication Service**
  - **STI-VS Verification Service**
  - Signed PASSporT
  - "Caller Verified" Indication
  - SHAKEN via HTTPS
  - Path of Phone Call

- **Attacker**

**Call Direction**
Compromised Network

CALLER VERIFIED Indication

SIGNED PASSPORT

Path of Phone Call

STI-AS Authentication Service

SIP Intermediate Providers

Callee Call Control Servers

SBC - Session Border Controller (Access) P-CSCF

Core Trusted

Call Trunk

Customer SIP PBX

Untrusted A Network

Untrusted Peering Network

SBC - Session Border Controller

SIP Interconnection IBCF

Called Call Control Servers

SBC - Session Border Controller (Access) P-CSCF

Untrusted Peering Network

Untrusted Access Network

Attacker

Customer SIP PBX

Call Direction

SIP Trunk

SHAKEN via HTTPS

Certificates

STI-VS Verification Service

Secrets

"Caller Verified" Indication

CALLER VERIFIED

Verified!

Call Direction
How to Hack Enterprise SIP trunks

• Hack the enterprise network
• Use malware via email to first access the corporate network
• Use a Command and Control system to blast out calling campaigns
• Compromise vulnerabilities in the Enterprise PBX
How to Compromise Corporate PBX

1. Target staff with phishing emails to get them to click links.
2. Links lead to sites that trigger installation of malware.
3. Malware installs on internal system and connects outbound to Command & Control (C&C).
4. Botnet probes network to find Corp PBX Voice platform.
5. Specific attacks against unpatched Corp PBX loaded to local Malware.
6. Calling campaigns loaded & scheduled on compromised enterprise PCs.
### Hack Enterprise SIP Trunking
Can my network be attacked like this?

<table>
<thead>
<tr>
<th>Caller Voice Network Technology</th>
<th>Factors affecting attack source</th>
<th>Risk of sourcing attack</th>
<th>Risk of receiving attack -- fraudulent “Caller Verified”</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCaaS &amp; Hosted PBX</td>
<td>Voice platform on the Internet. Compromising the enterprise network brings no special access to the voice platform.</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
<tr>
<td>SIP Trunking</td>
<td>Service Providers forced to trust security at enterprise networks.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>IMS / Mobile</td>
<td>Private networks.</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
What makes this hack harder?

- **Patching:** Enterprise PBXs must be regularly updated with latest security patches. *Help them!*
- **Strong admin login security** on Enterprise PBXs
- **Isolated PC & Voice networks** – preventing cross-network attack
- **SIP Authentication** on SIP trunks
4. Hack internal Trust Model at Service Providers

- Peering SBCs will add Attestation to all calls received from trusted networks
- Peering SBCs will be setup to trust internal network infrastructure.
- Many SPs have a hard-shell-squishy-center model
Compromised Network

- STI-AS Authentication Service
- SIP Intermediate Providers
- STI-VS Verification Service
- SBC - Session Border Controller
  (SIP Interconnection) IBCF
- Core Trusted
- Untrusted Peering Network
- IBCF

Attacker

- Call Direction
- Callee Bob

Certificates

- Core Trusted
- Callee Call Control Servers
- SBC - Session Border Controller
  (Access) P-CSCF
- Core Trusted
- Untrusted Access Network
- Untrusted Peering Network

Callee

- Bob
Compromised Network

- STI-AS Authentication Service
- SIP Intermediate Providers
- Untrusted Peering Network
  - SBC - Session Border Controller
    - (SIP Interconnection) IBCF
  - Core Trusted

- Untrusted Peering Network
  - SBC - Session Border Controller
    - (SIP Interconnection) IBCF
  - Core Trusted

- SIP Intermediate Providers
  - Core Trusted

- Untrusted Access Network
  - SBC - Session Border Controller
    - (Access) P-CSCF
  - Core Trusted

- Call Direction
- Callee Bob

Certificates
- STI-VS Verification Service

Attacker
Compromised Network

Certified Network

SIP
Intermediate Providers

Untrusted Peering Network
SBC - Session Border Controller

(SIP Interconnection) IBCF
Core Trusted

Core Trusted
Untrusted Peering Network
SBC - Session Border Controller

Ice Breaker Core Trusted
Untrusted Peering Network

Callee

Bob

Call Direction

Attacker

STI-AS Authentication Service

STI-VS Verification Service

Certificates

Caller Verified!
How to Hack Internal SBC

- Many expect to do attestation in the SBC
- In these designs, the SBC will trust all calls originating from certain IP addresses internally
- Launch the attack from the trusted IP range permitted by the SBC
How to Compromise Peering SBC

1. Load botnet on Internal Network via Linux malware
2. Probe with SIP to determine which IP’s route calls to the PSTN
3. Manage calling campaigns with C&C servers
4. Automate to deploy rapidly across multiple botnets
# Hack Internal Service Provider Networks

Can my network be attacked like this?

<table>
<thead>
<tr>
<th>Caller Voice Network Technology</th>
<th>Factors affecting attack source</th>
<th>Risk of sourcing attack</th>
<th>Risk of receiving attack -- fraudulent “Caller Verified”</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCaaS &amp; Hosted PBX</td>
<td>Windows PCs and Linux servers common. Dependence on SHAKEN in SBC.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>SIP Trunking</td>
<td>Windows PCs and Linux servers common. Dependence on SHAKEN in SBC.</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>IMS / Mobile</td>
<td>Highly-targeted providers; higher malware defense competency.</td>
<td>MODERATE</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
What makes this hack harder?

Operating System Patching:
- Routinely Update Servers, PCs, SBCs

Minimize the IP addresses considered trusted

Move SHAKEN Attestation to the servers that actually authenticate the callers

Migrate toward Zero-Trust networking: Authenticate each step, e.g. mTLS to core SBC
SHAKEN/STIR could be undermined by network designs & operational insecurity.

- Steal the SHAKEN cert private key.
- Attack SIP Device interface to customers.
- Attack SIP Trunking & Peering from customers.
- Attack SP Internal Trust Model.
SHAKEN/STIR could be undermined by network designs & operational insecurity.

Steal the SHAKEN cert private key.

Attack SIP Device interface to customers.

Attack SIP Trunking & Peering from customers.

Attack SP Internal Trust Model.

[Checkmarks labeled 'Caller Verified!']
ECG.
Your voice matters.

Let’s talk.
@markrlindsey
mark@ecg.co