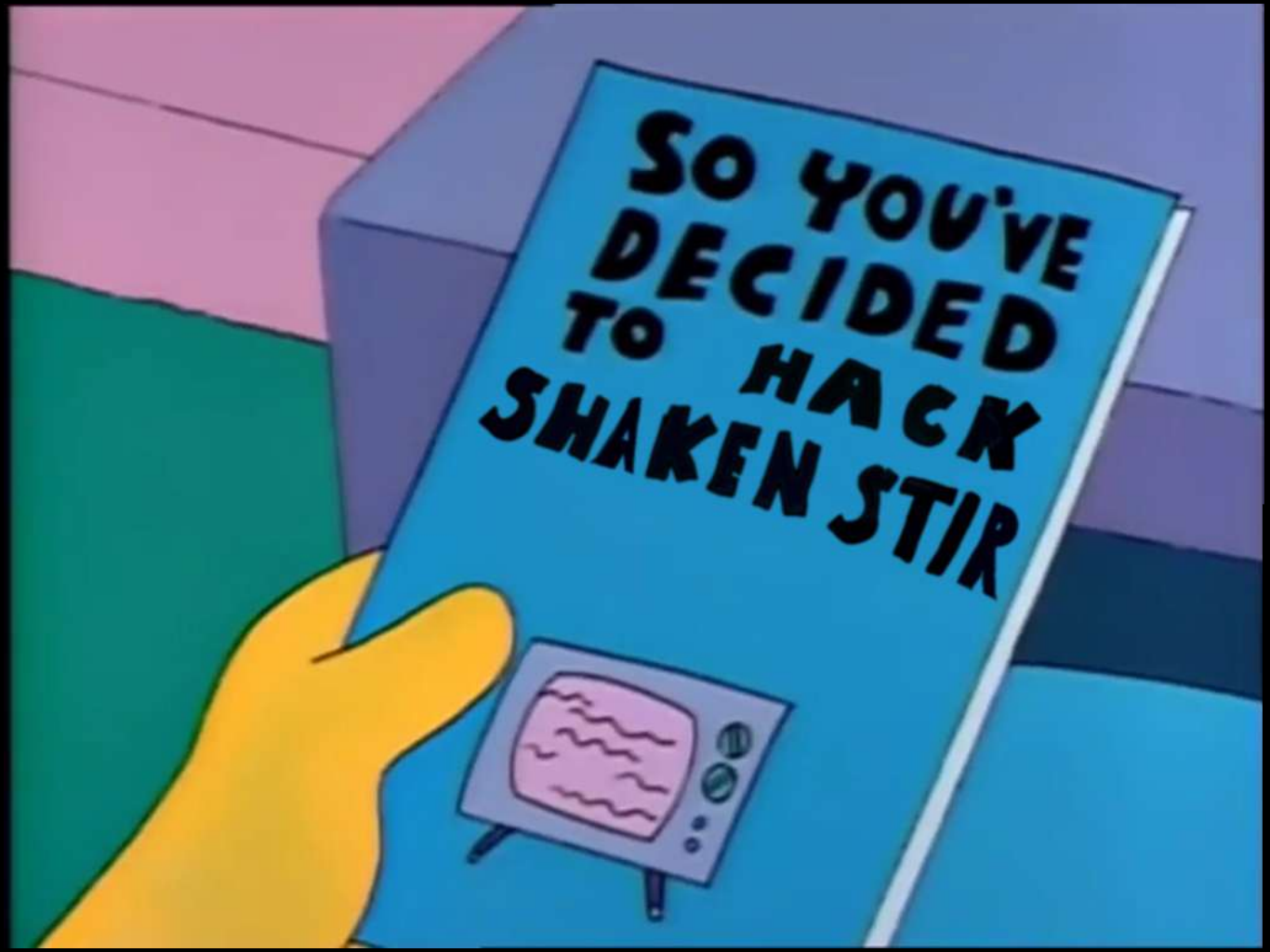

SO YOU'VE
DECIDED
TO HACK
SHAKEN STIR

Hacking SHAKEN/STIR

White-Hat Vulnerability Analysis

ECG.

Staff Augmentation &
Consulting.

Voice Network
Configuration.
Troubleshooting.
Security.

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

Mark R Lindsey
mark@ecg.co
@markrlindsey

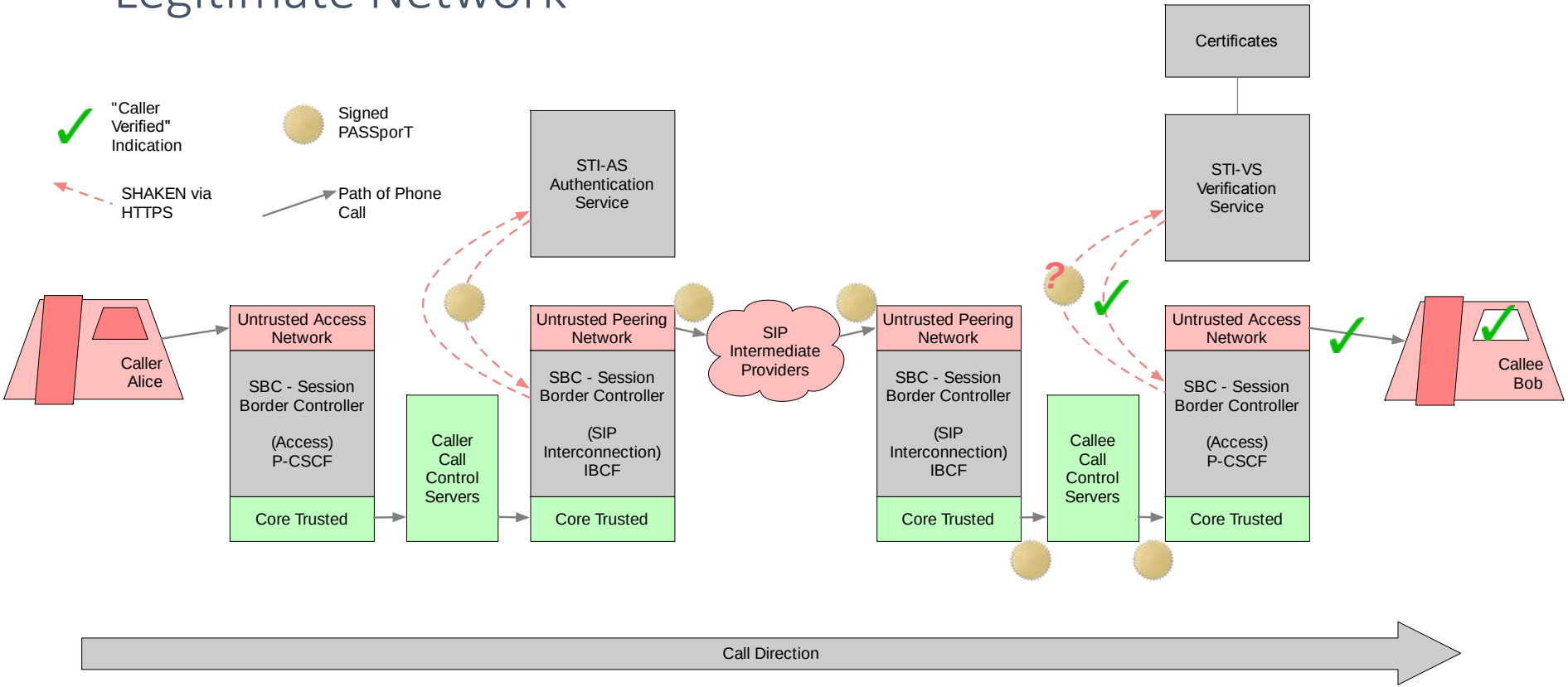
Don’t bother hacking fundamental math & protocols of SHAKEN/STIR.

So the real weaknesses will be in real networks…

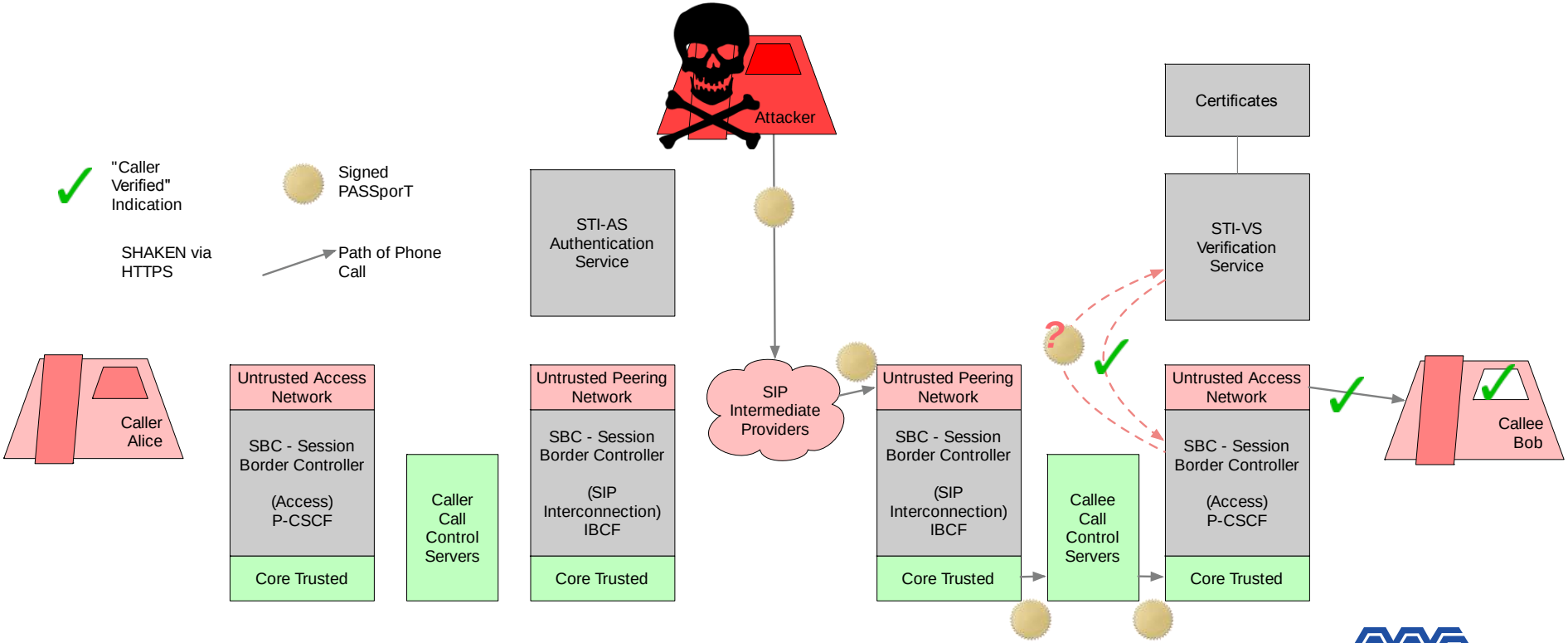
1. Steal Service Provider Private Key

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

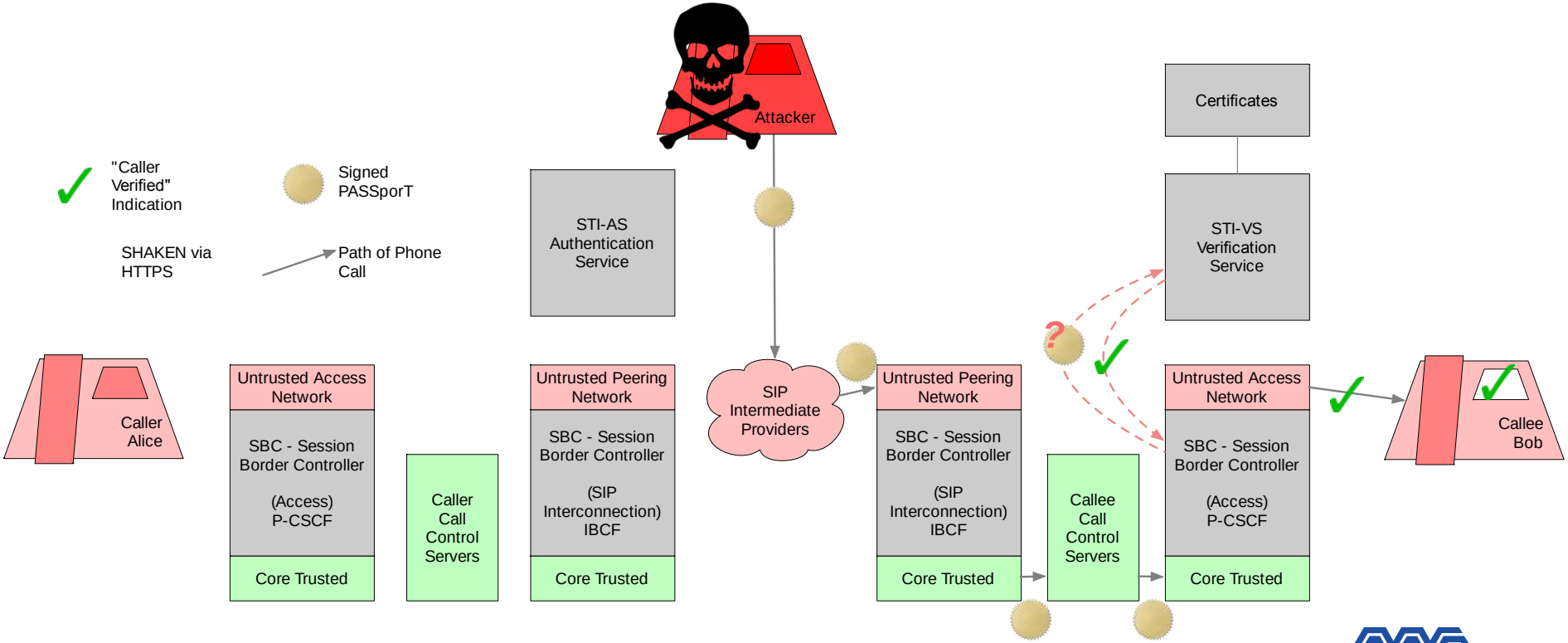
Legitimate Network



Compromised Private Keys



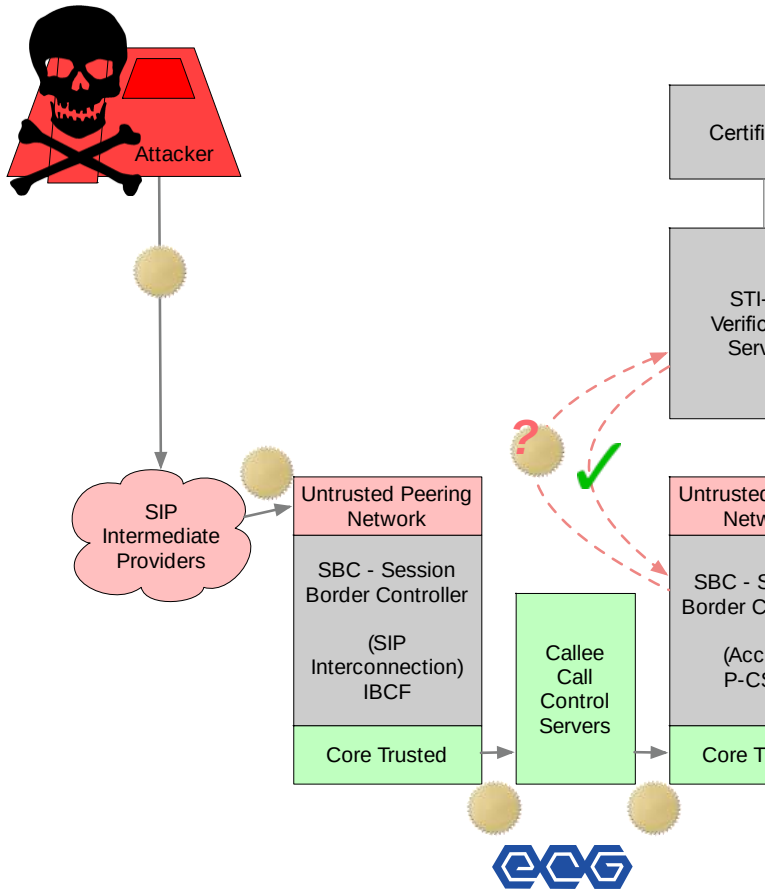
Compromised Private Keys



Compromised Private Keys

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?

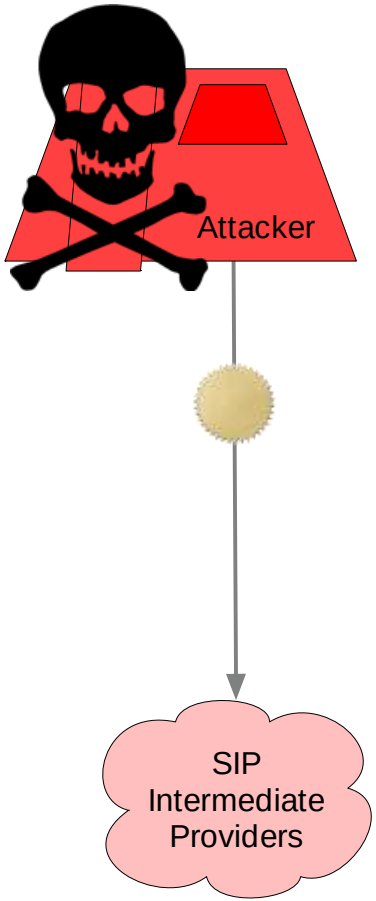
Caller Voice Network Technology	Factors affecting attack source	Risk of sourcing attack	Risk of receiving attack -- fraudulent "Caller Verified"
UCaaS & Hosted PBX	Malware & Social Engineering.	HIGH	HIGH
SIP Trunking	Malware & Social Engineering.	HIGH	HIGH
IMS / Mobile	Malware & Social Engineering. Likely to have *many* certificates – only one needed to attack	HIGH	HIGH

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.

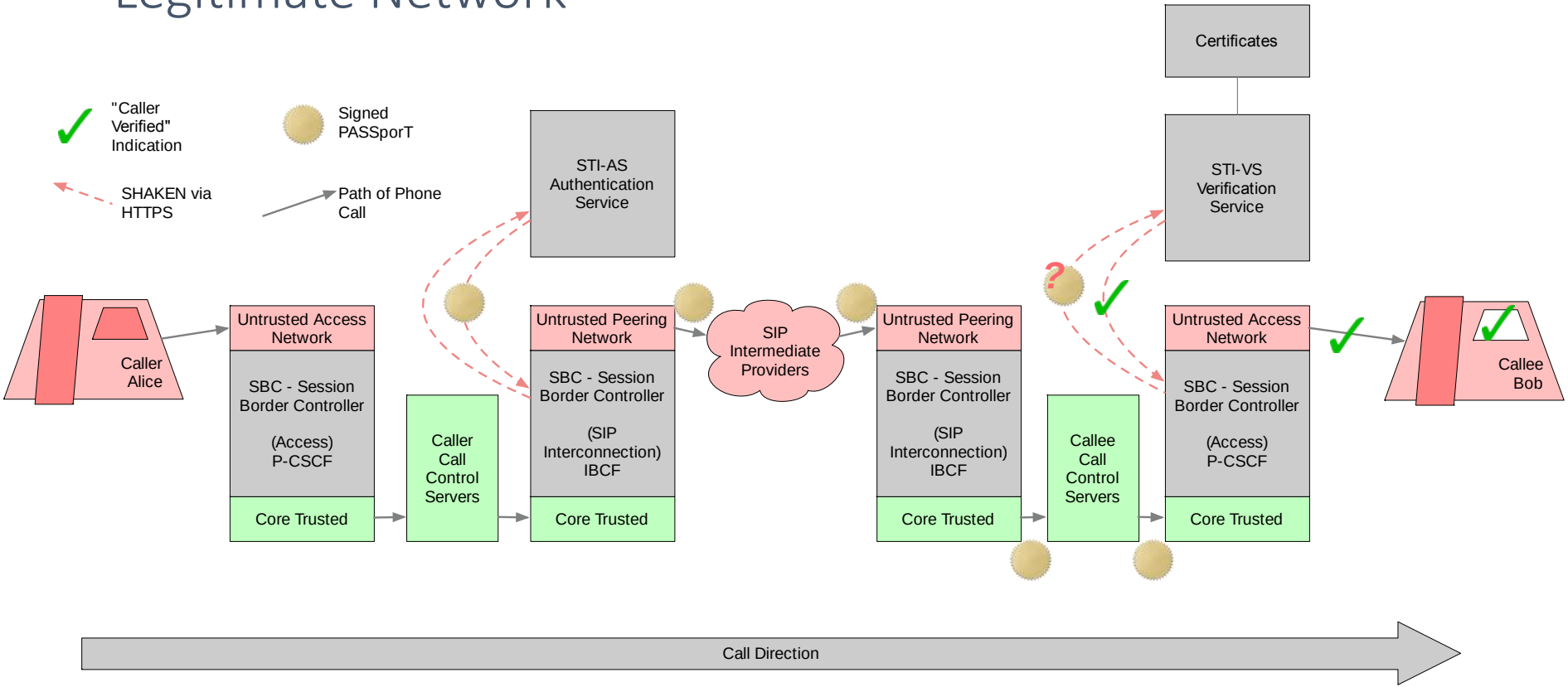
Use SHAKEN Certificates with Telephone Numbers in tnAuthList, not just SPID



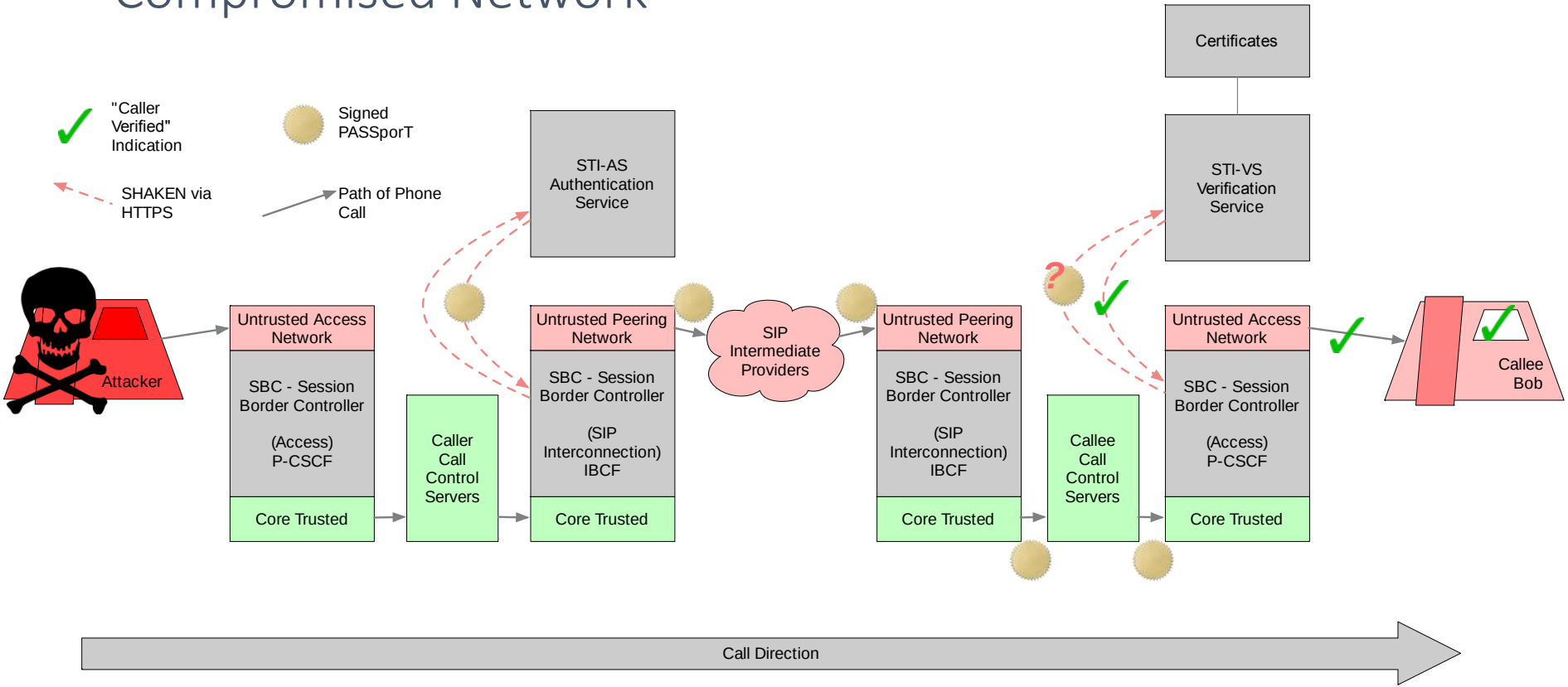
2. Hack registering SIP devices

- 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.

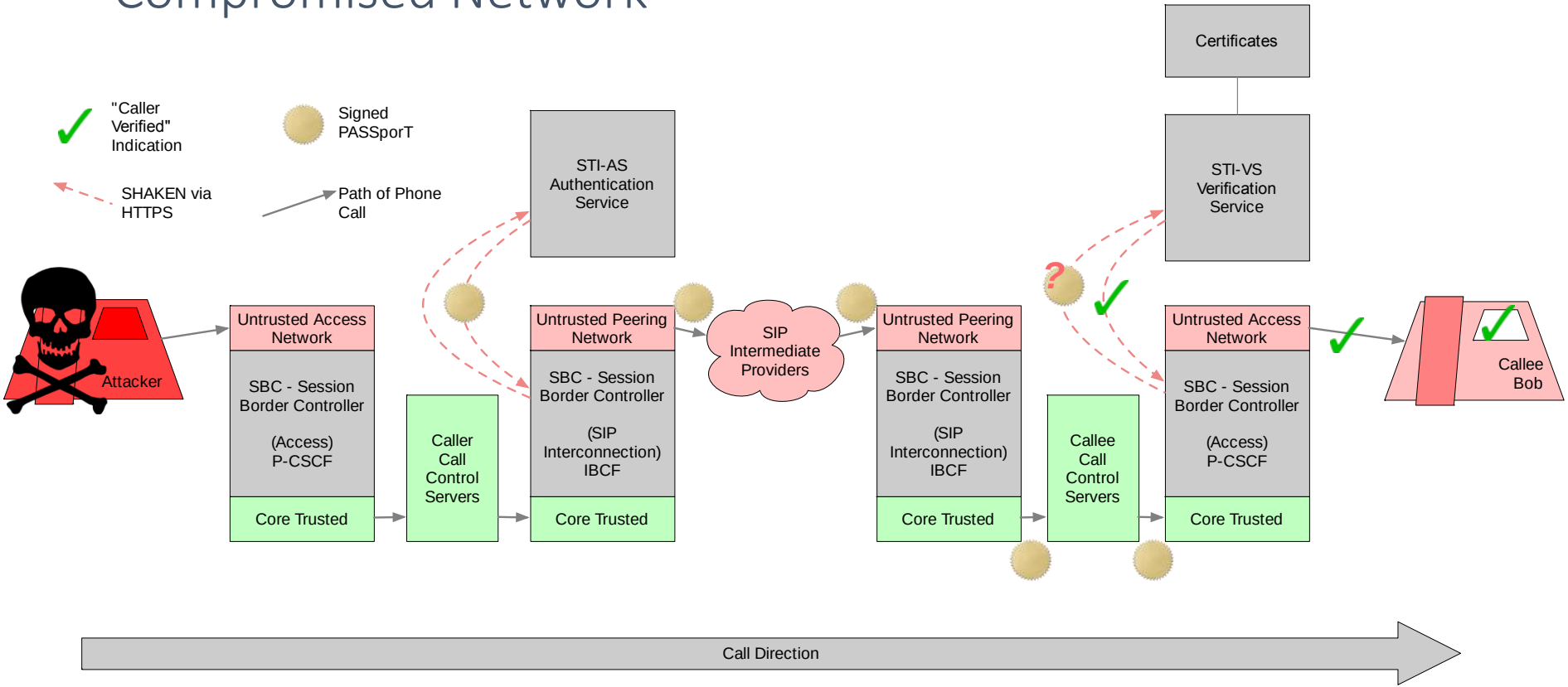
Legitimate Network



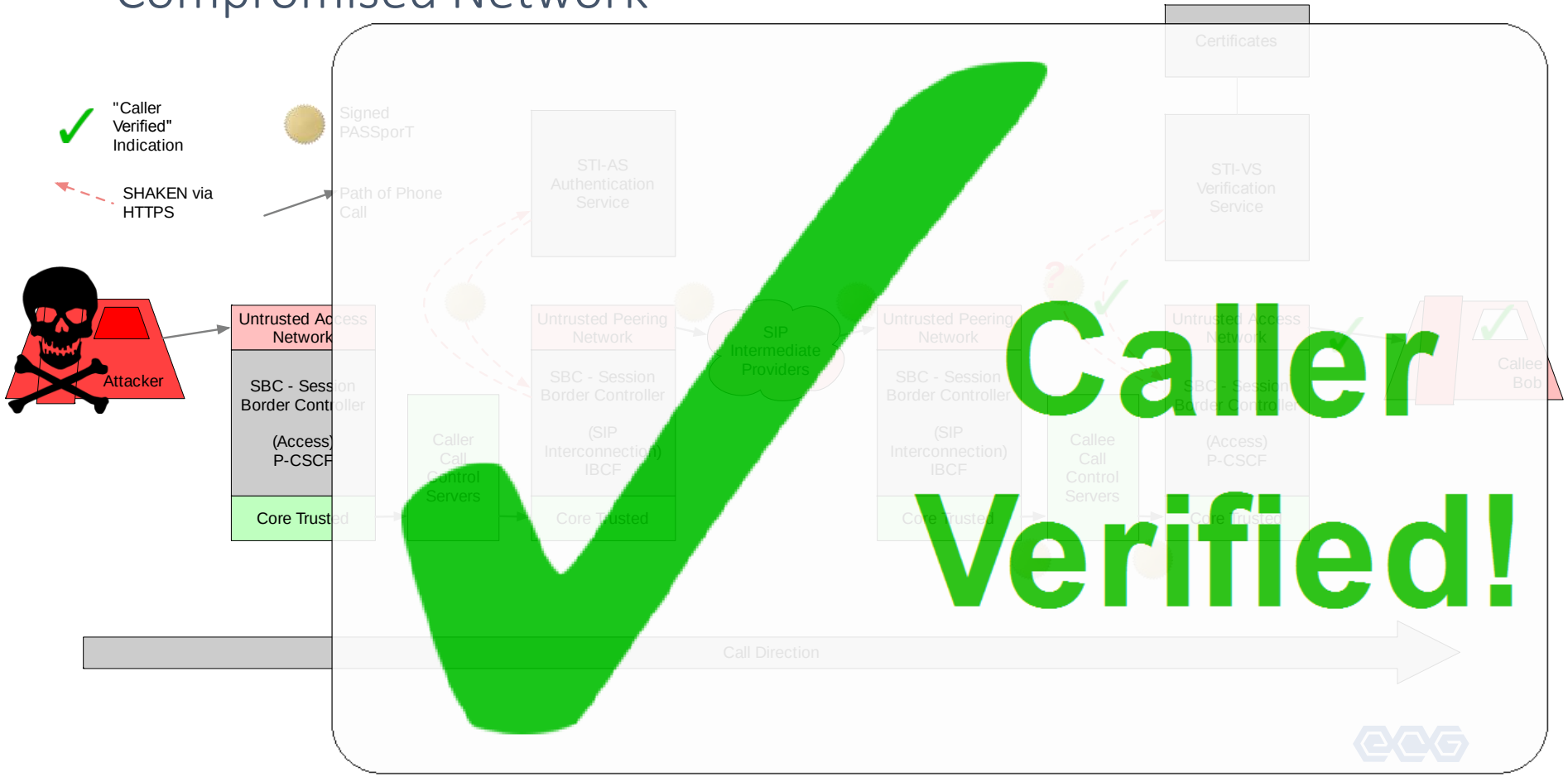
Compromised Network



Compromised Network

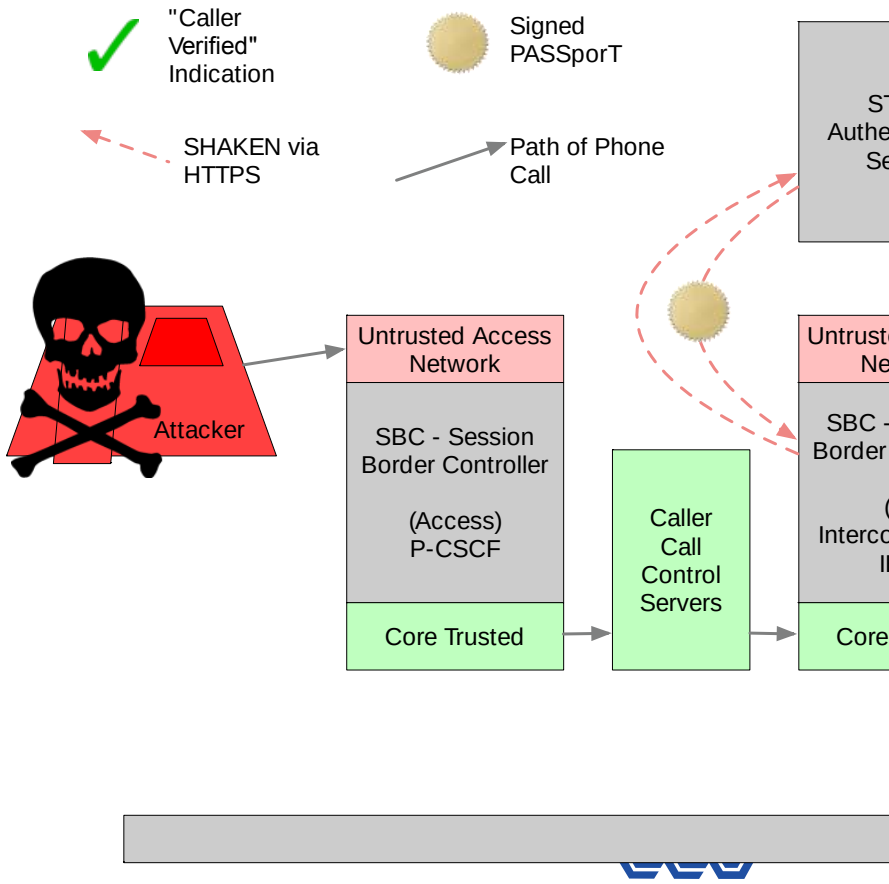


Compromised Network



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?

Caller Voice Network Technology	Factors affecting attack source	Risk of sourcing attack	Risk of receiving attack -- fraudulent "Caller Verified"
UCaaS & Hosted PBX	SIP Authentication. Device Config discovery. Open to Internet.	HIGH	HIGH
SIP Trunking	No Device config accessible. Often limited IP range.	MODERATE	HIGH
IMS / Mobile	Private networks.	LOW	HIGH

What makes this hack harder?

Modern/Secure Device Management, e.g., Mutual TLS

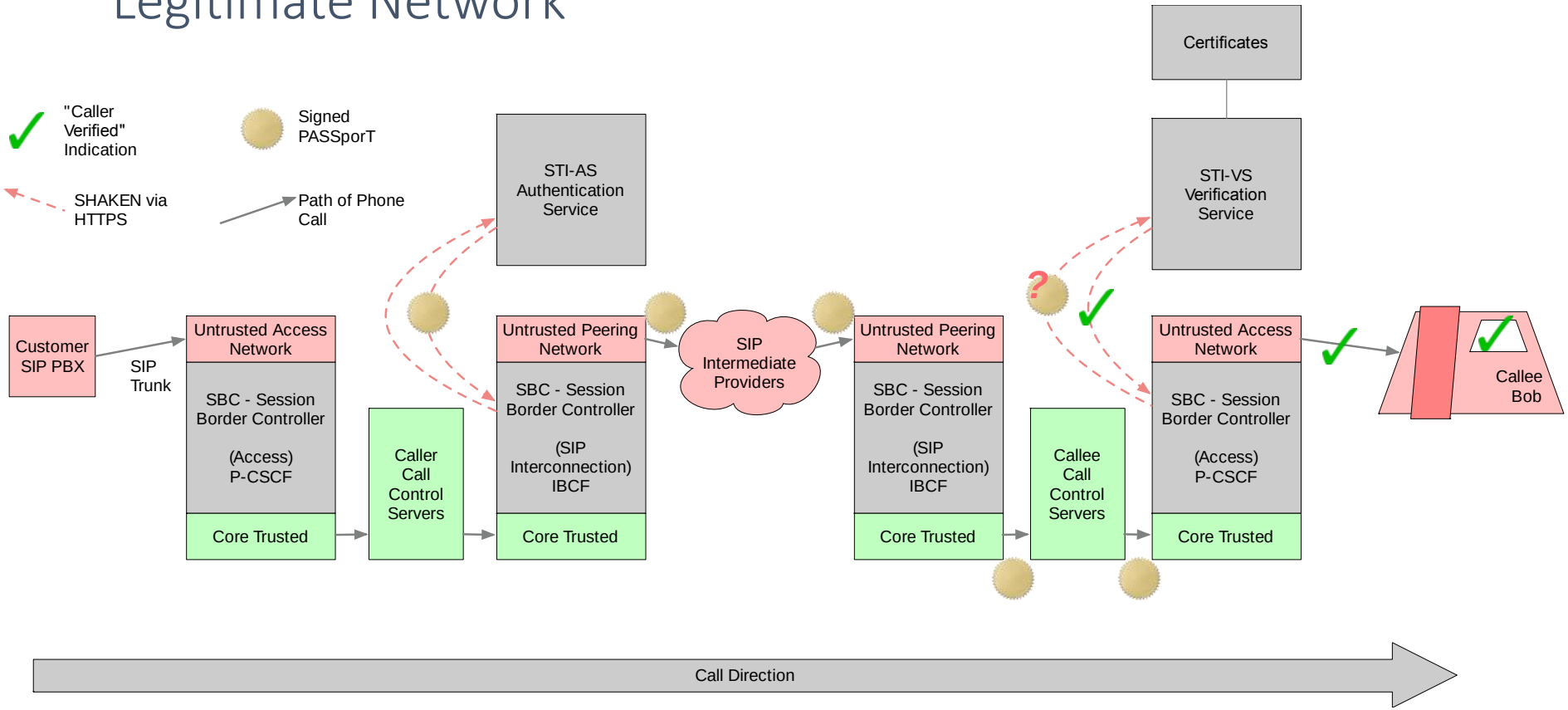
Strong SIP passwords Automatically-enforcement

SBC Scanning prevention Blacklisting password scanners

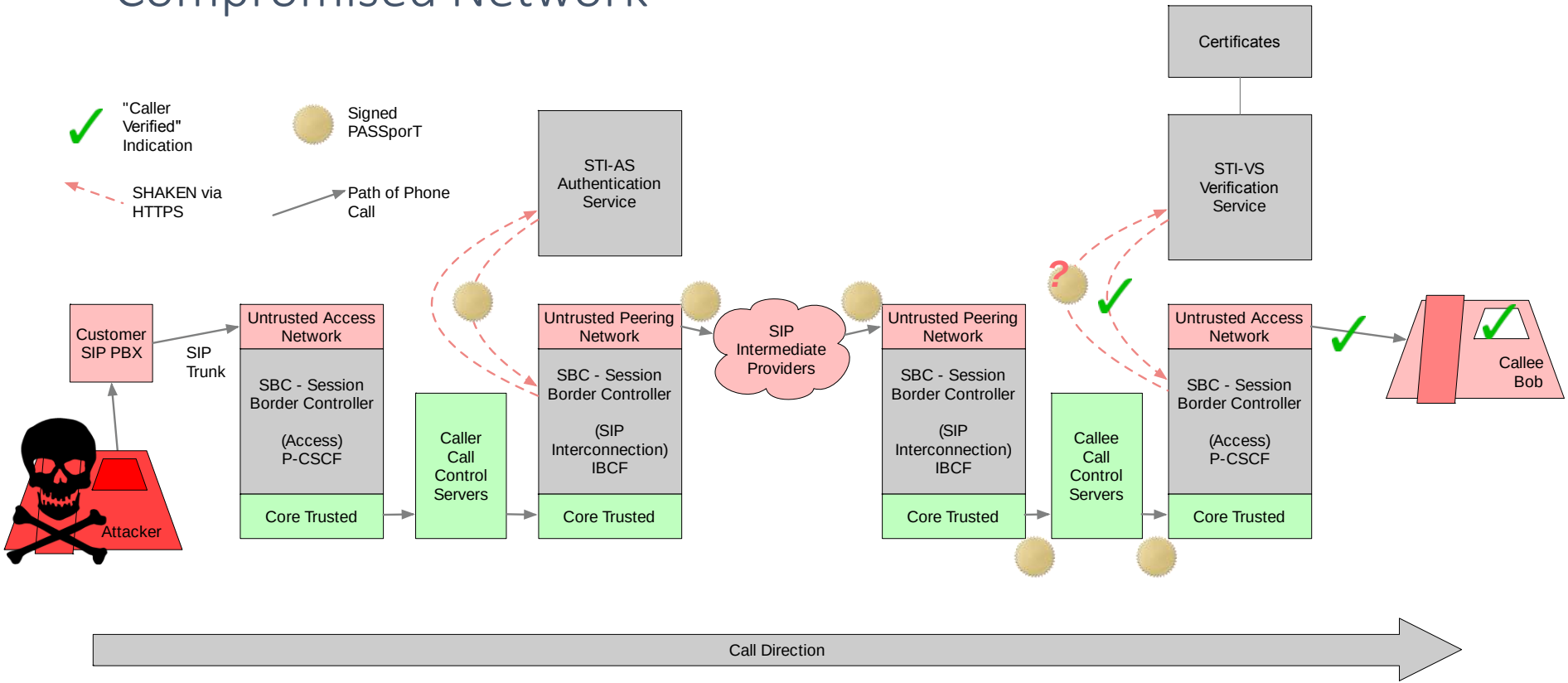
3. Hack SIP Trunking & Peering

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

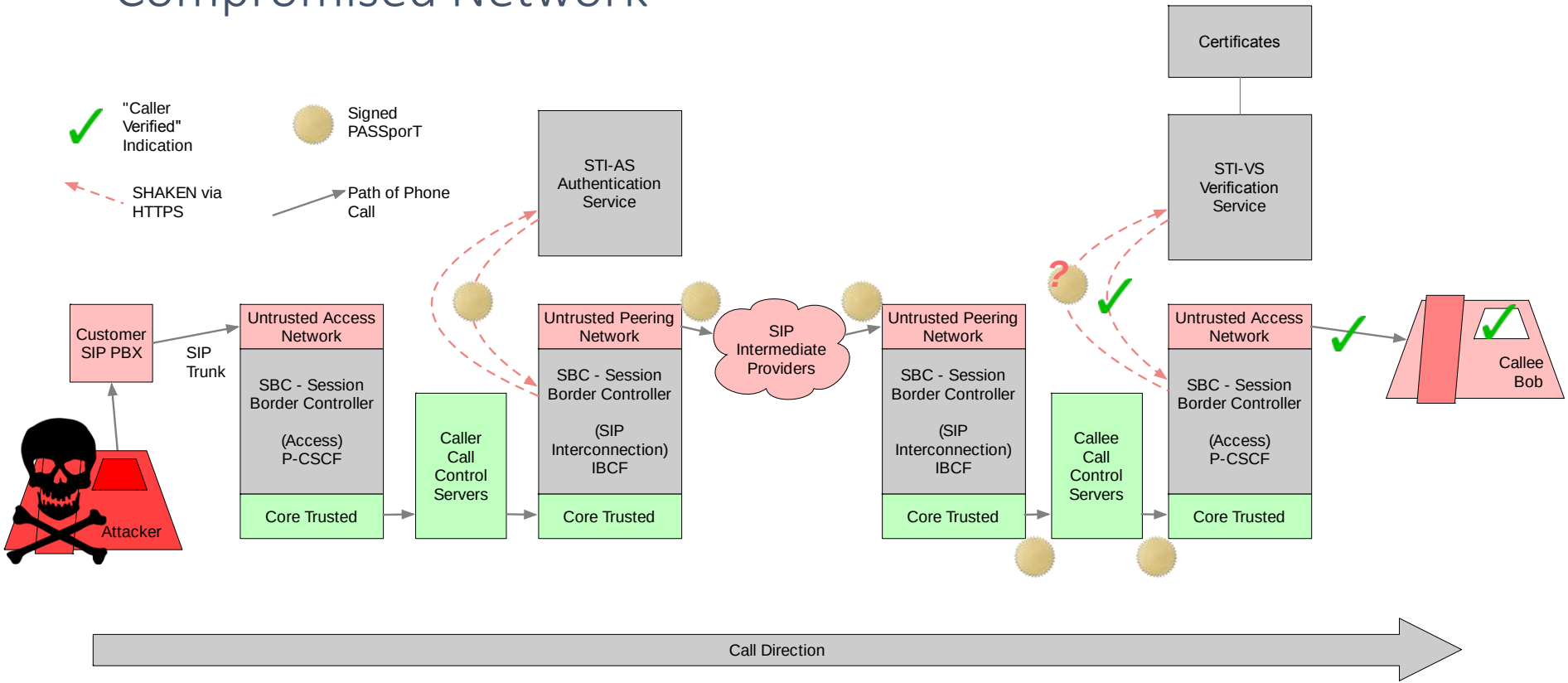
Legitimate Network



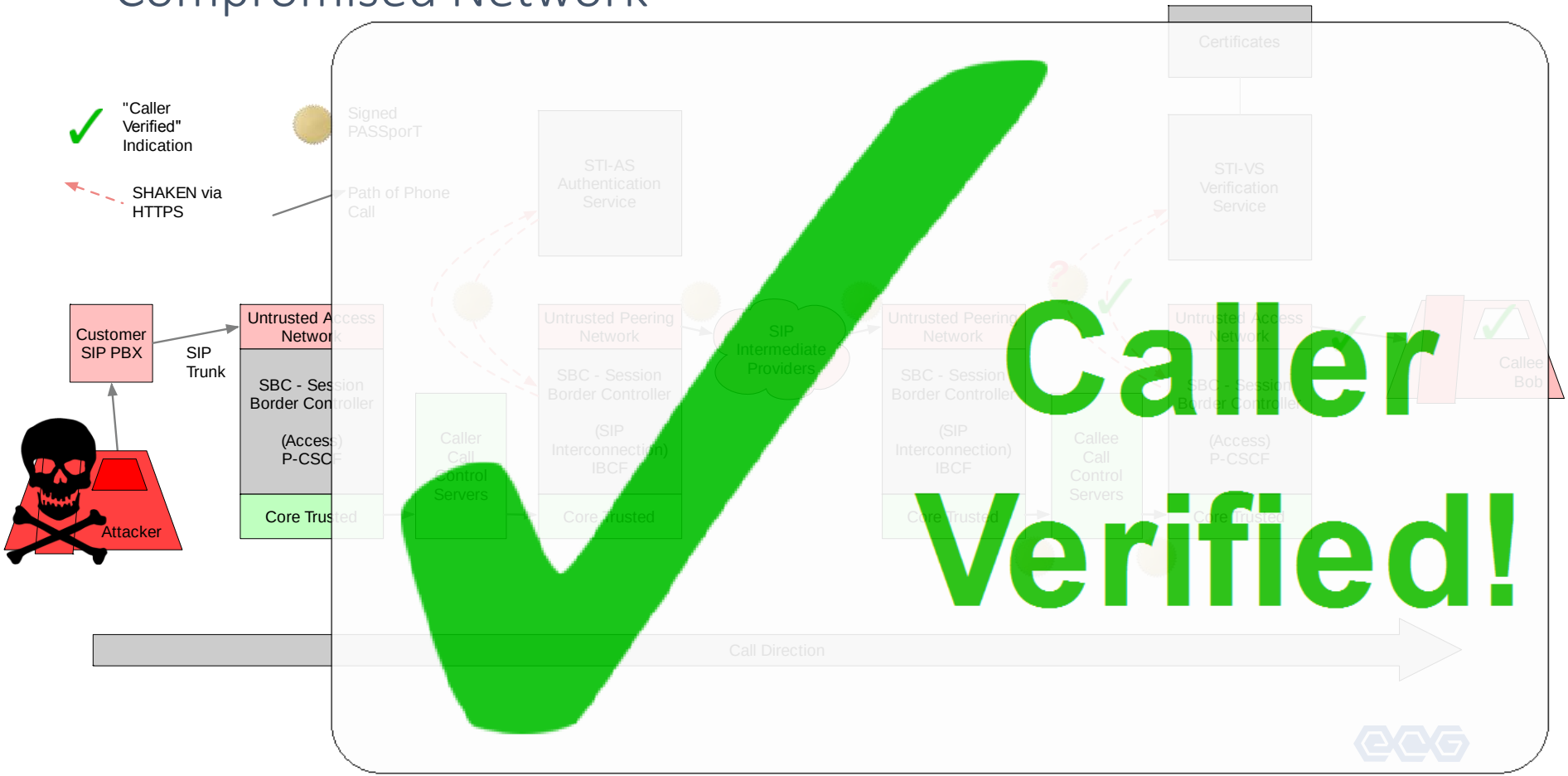
Compromised Network



Compromised Network

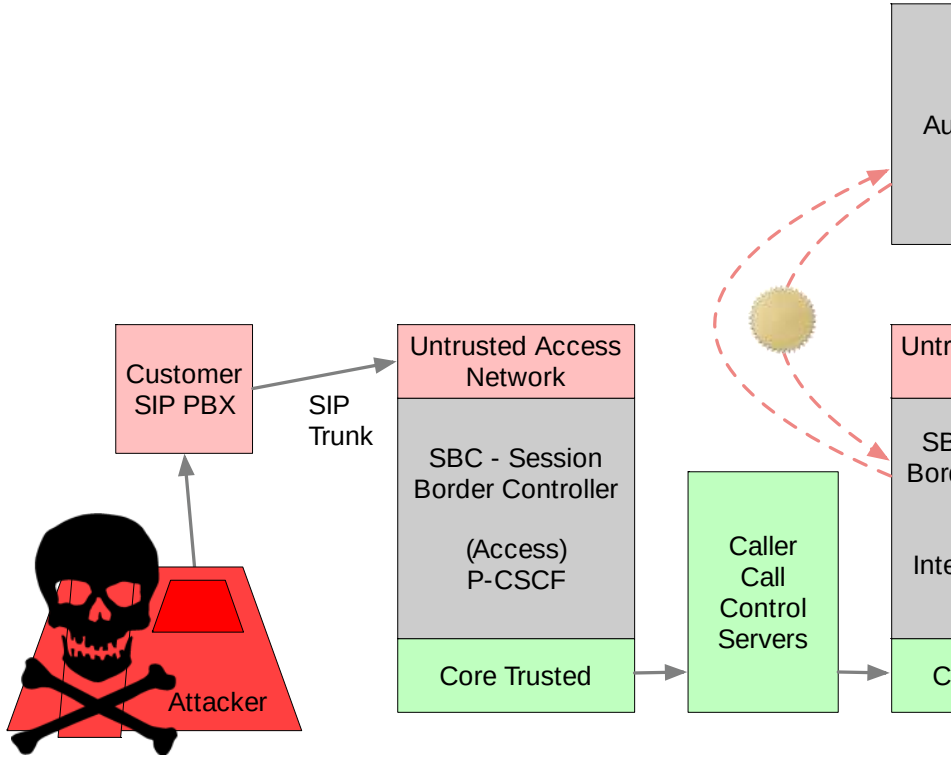


Compromised Network

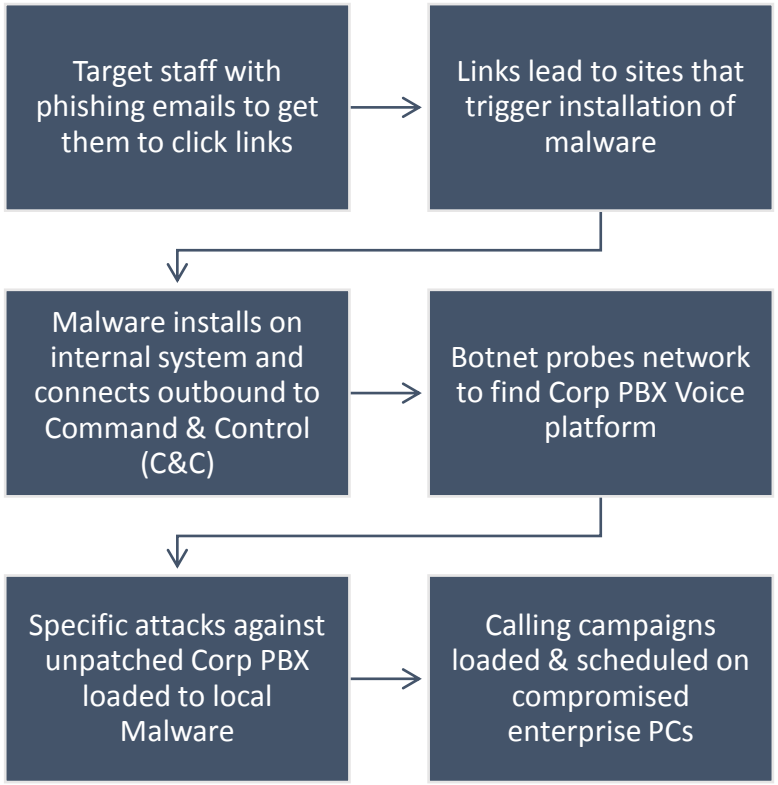


How to Hack Enteprise SIP trunks

- 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



Hack Enterprise SIP Trunking
Can my network be attacked like this?

Caller Voice Network Technology	Factors affecting attack source	Risk of sourcing attack	Risk of receiving attack -- fraudulent "Caller Verified"
UCaaS & Hosted PBX	Voice platform on the Internet. Compromising the enterprise network brings no special access to thee voice platform.	LOW	HIGH
SIP Trunking	Service Providers forced to trust security at enterprise networks.	HIGH	HIGH
IMS / Mobile	Private networks.	LOW	HIGH

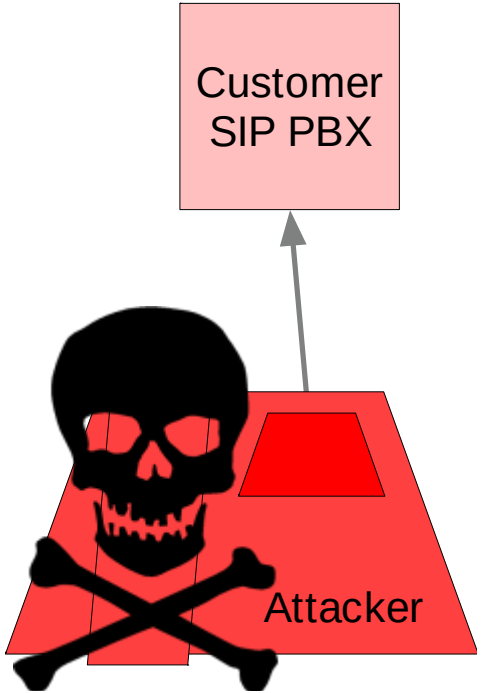
What makes this hack harder?

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

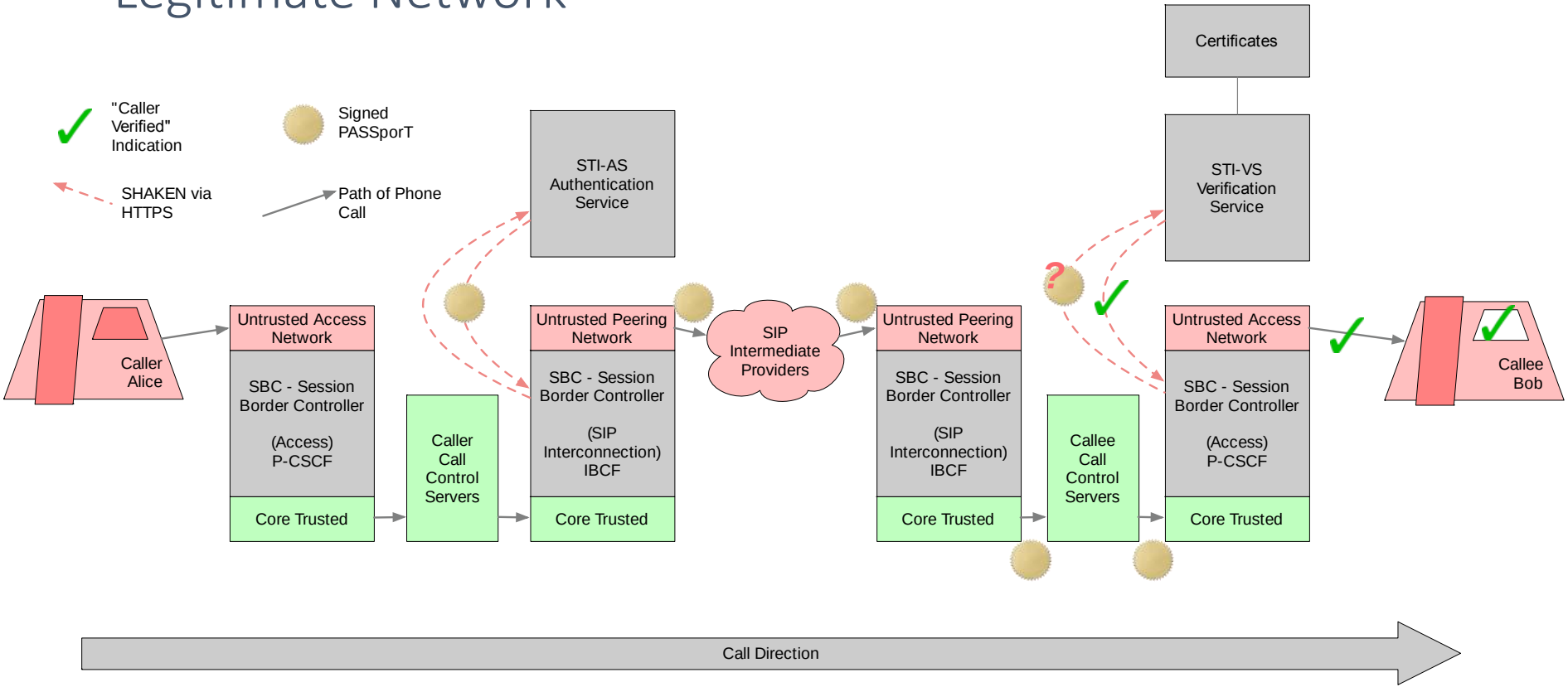
SIP Authentication on SIP trunks



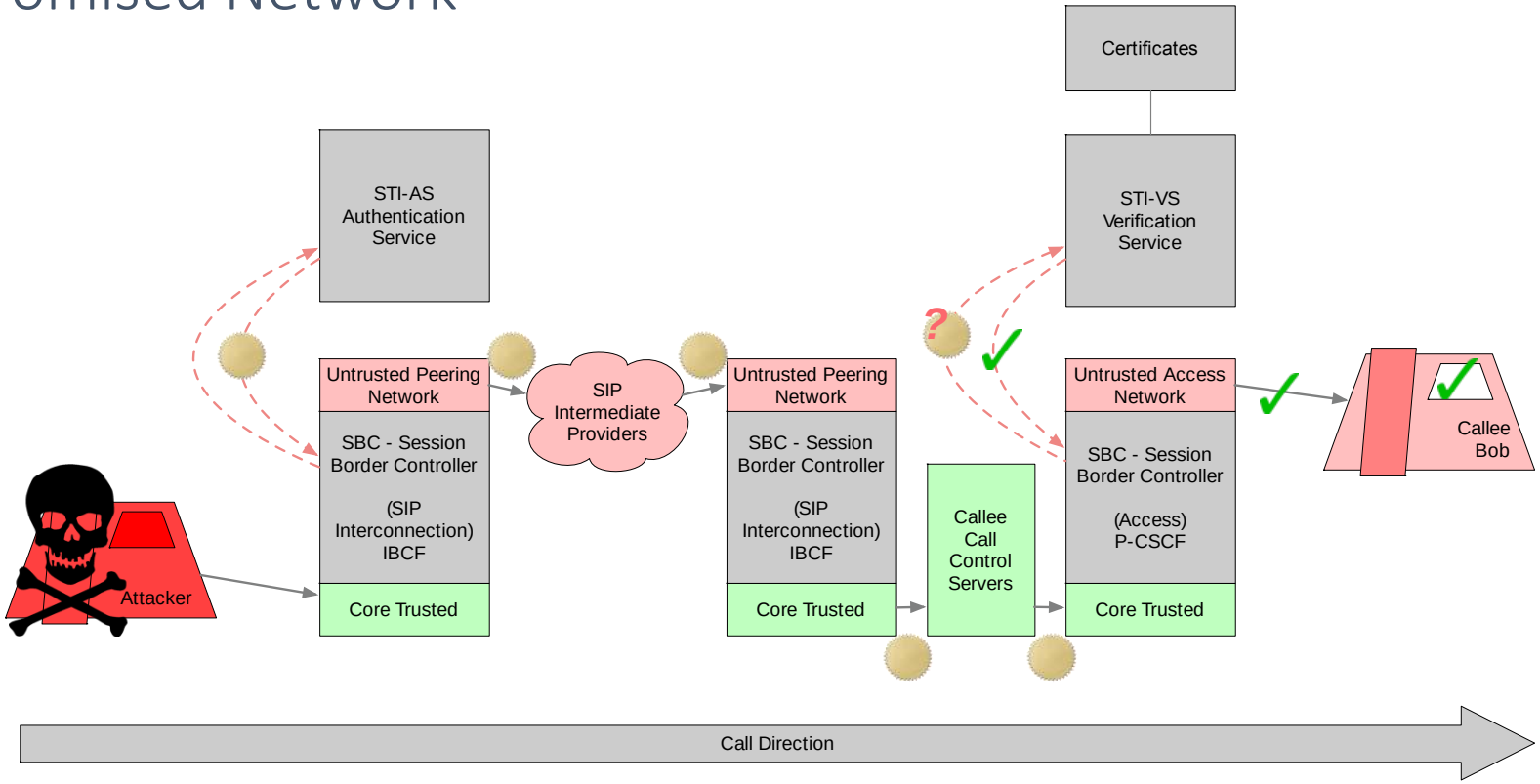
4. Hack internal Trust Model at Service Providers

- 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

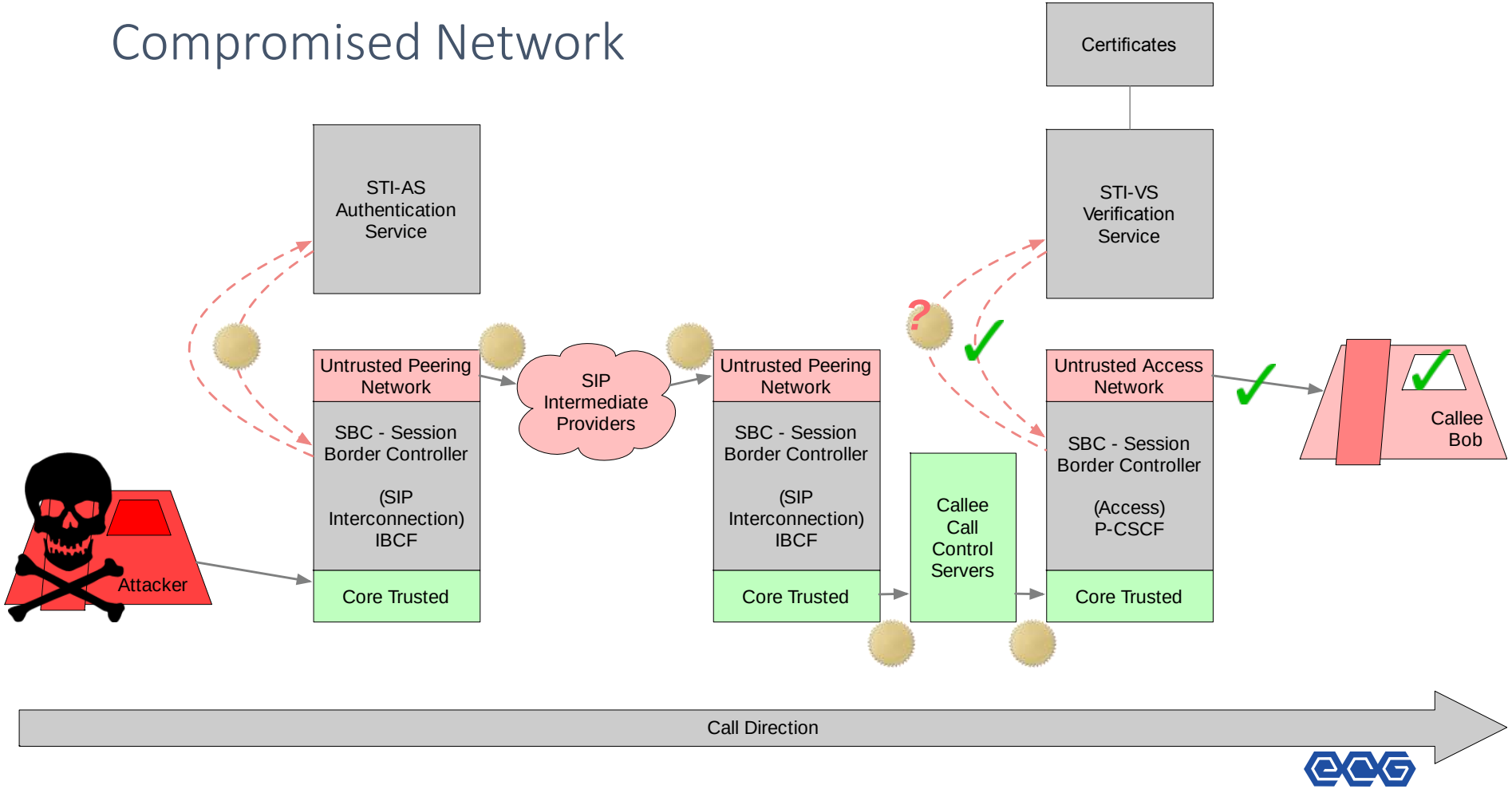
Legitimate Network



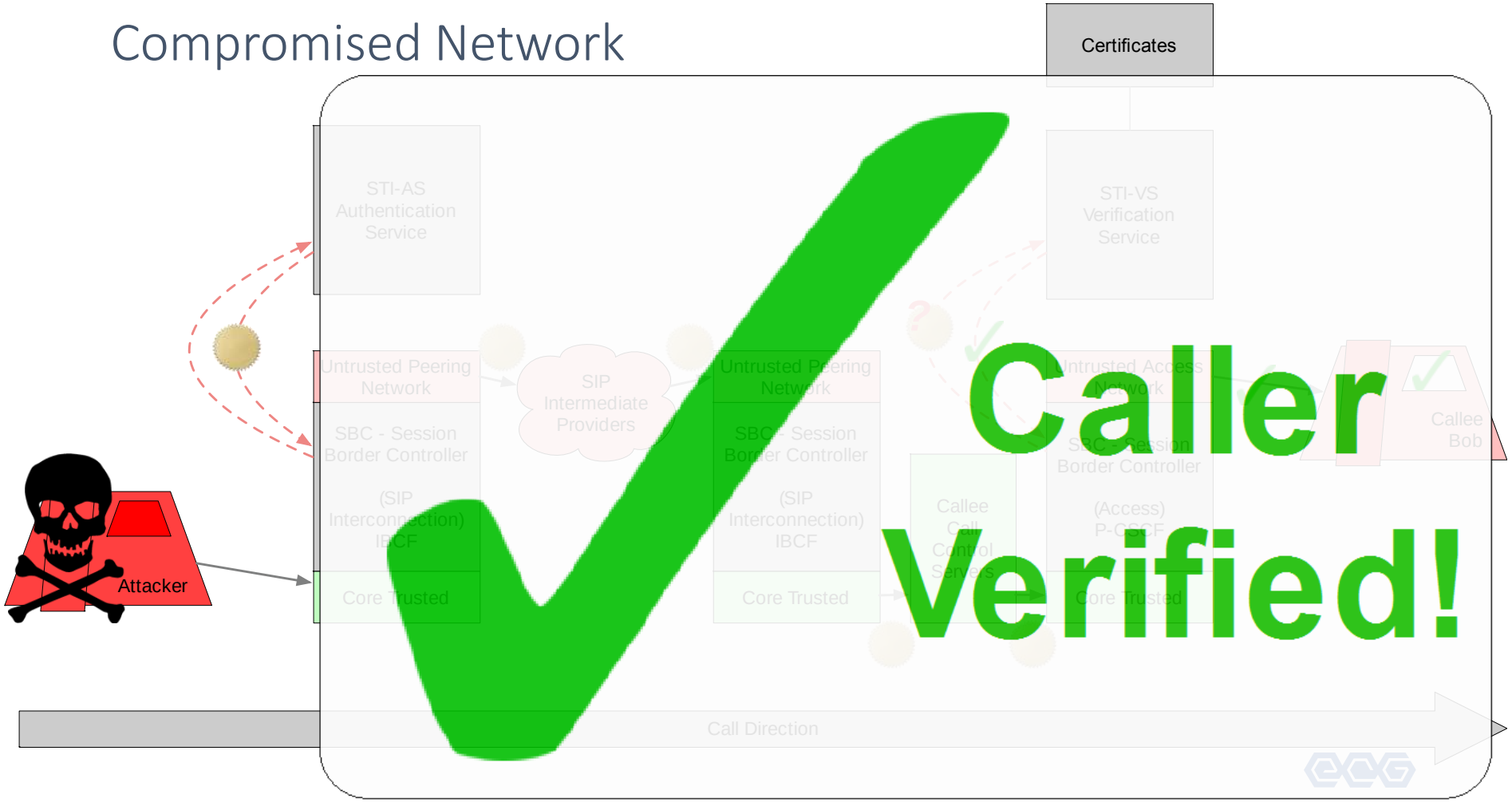
Compromised Network



Compromised Network

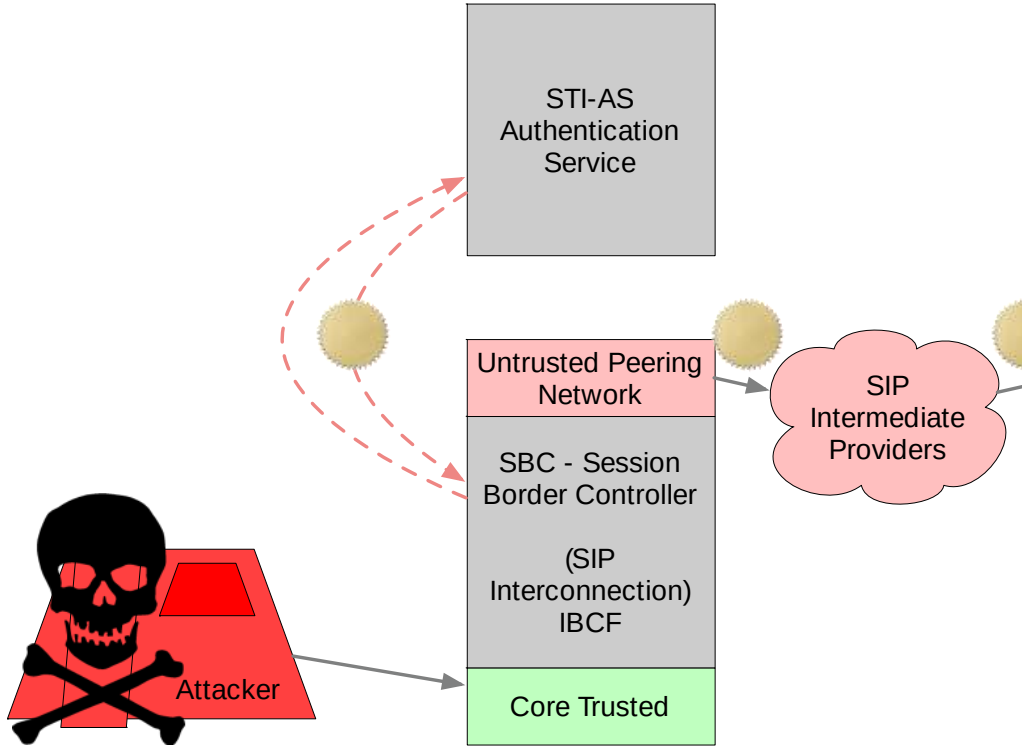


Compromised Network

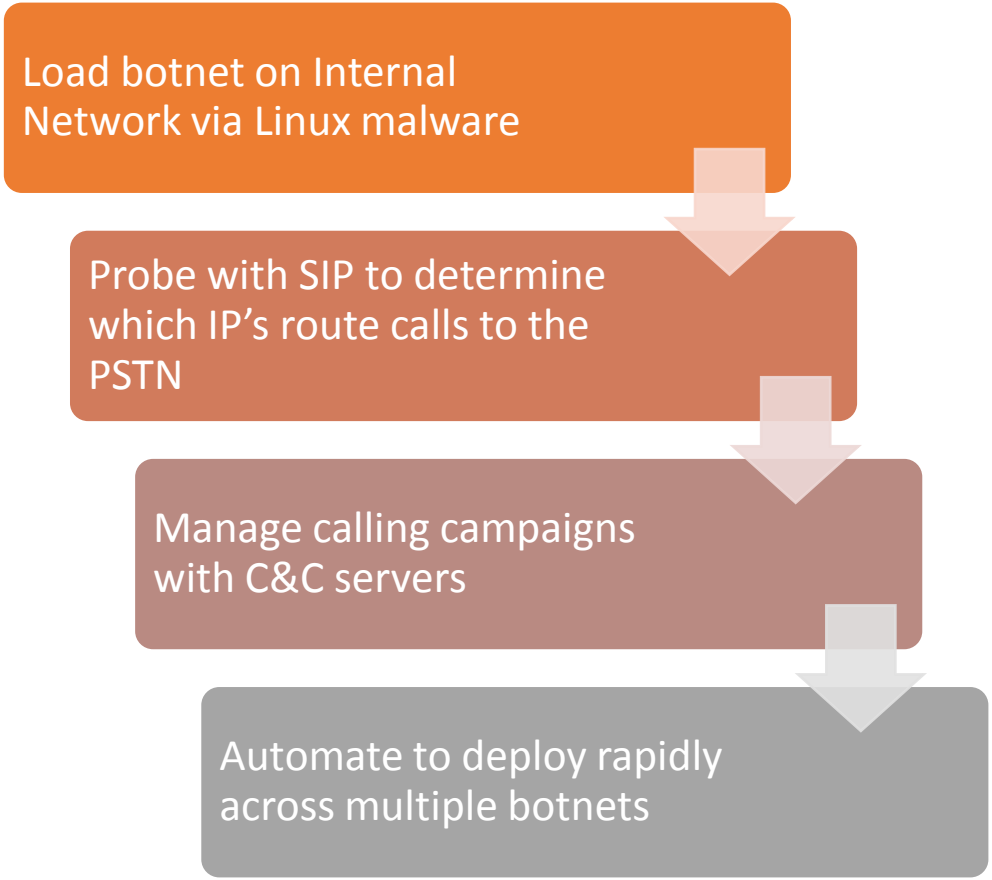


How to Hack Internal SBC

- 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



Hack Internal Service Provider Networks
Can my network be attacked like this?

Caller Voice Network Technology	Factors affecting attack source	Risk of sourcing attack	Risk of receiving attack -- fraudulent "Caller Verified"
UCaaS & Hosted PBX	Windows PCs and Linux servers common. Dependence on SHAKEN in SBC.	HIGH	HIGH
SIP Trunking	Windows PCs and Linux servers common. Dependence on SHAKEN in SBC.	HIGH	HIGH
IMS / Mobile	Highly-targeted providers; higher malware defense competency.	MODERATE	HIGH

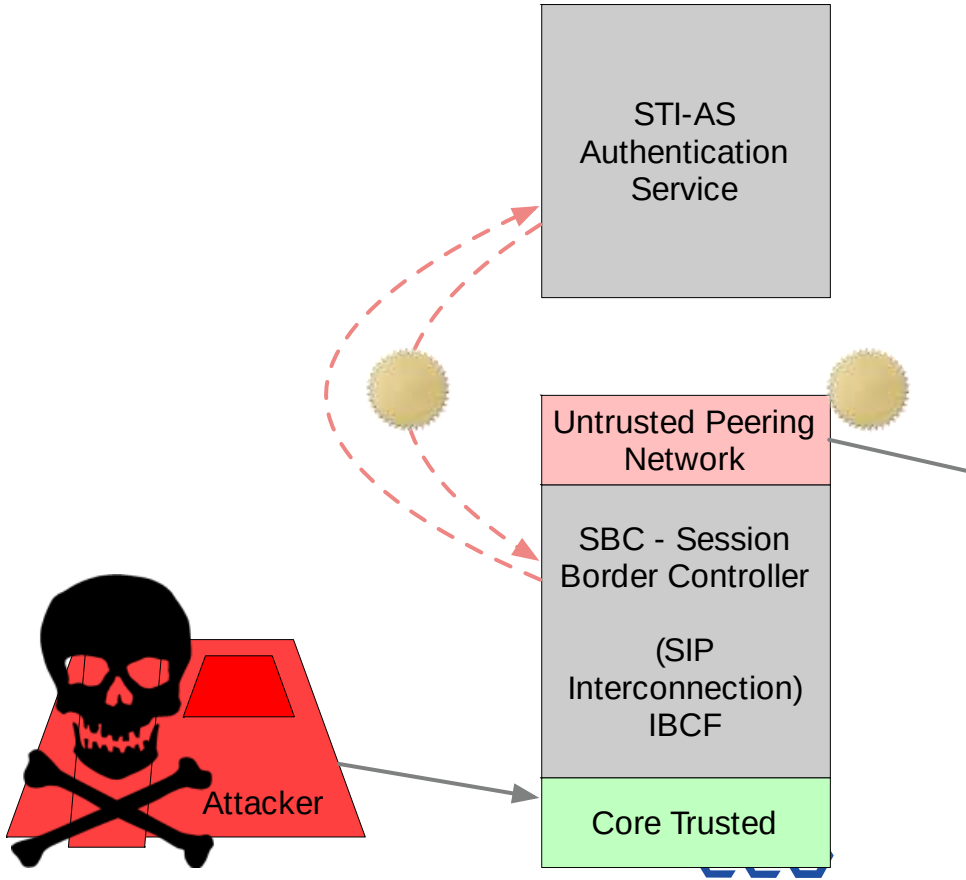
What makes this hack harder?

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.

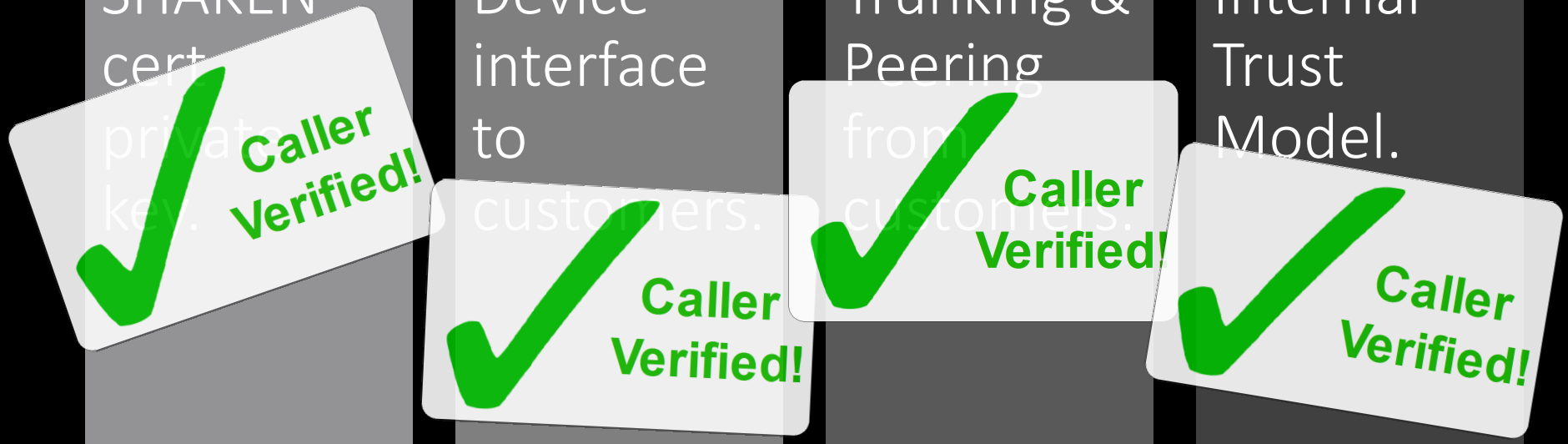
SHAKEN/STIR could be undermined by network designs & operational insecurity.

Steal the SHAKEN cert private key.

Attack SIP Device interface to customers.

Attack SIP Trunking & Peering from customers.

Attack SP Internal Trust Model.



ECG.
Your voice matters.

Let’s talk.
@markrlindsey
mark@ecg.co