To pin or not to pin

SWIFT USER GROUP VERSION 0X3: SECURITY

JEROEN WILLEMSEN

About me

Jeroen Willemsen
@commjoenie
jwillemsen@xebia.com

“Security architect”
“Full-stack developer”
"Mobile security”

Xebia

Agenda

- MASVS & MSTG
- Should you pin?
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- Basic verification
- Anti-anti pinning techniques
- Recap

OWASP MASVS & MSTG

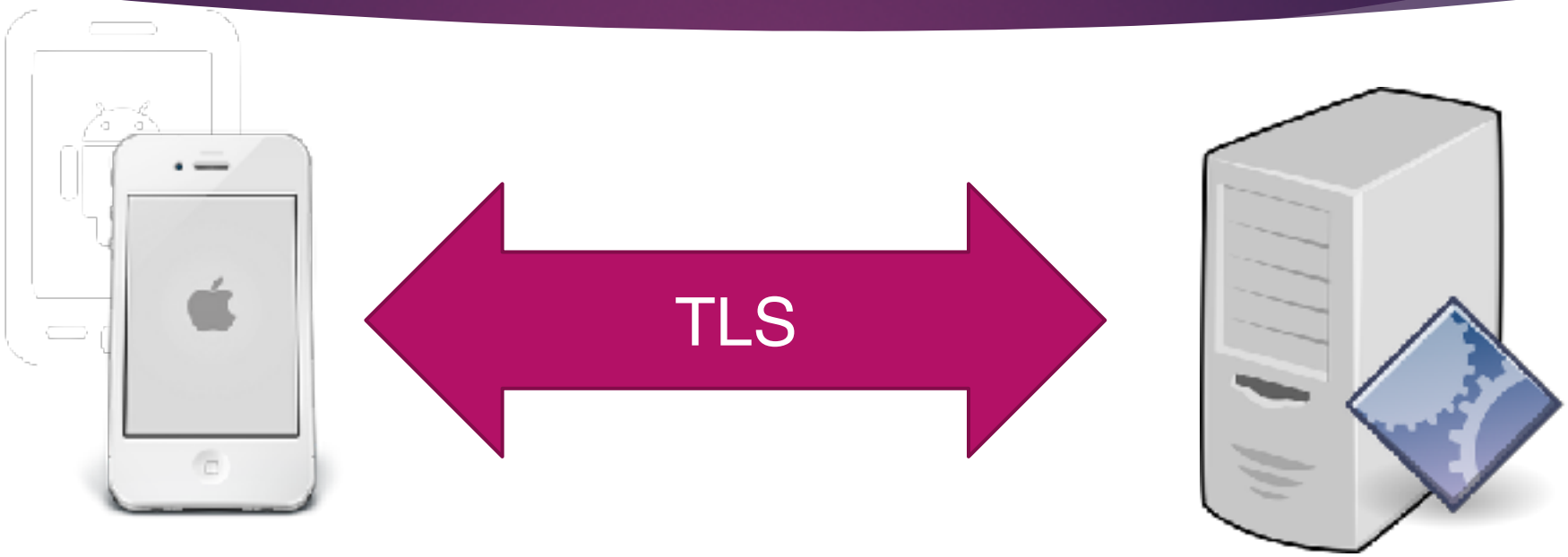
- Mobile Application Security Verification Standard (MASVS)
- https://github.com/OWASP/owasp-masvs

- Mobile Security Testing Guide (MSTG)
- https://github.com/OWASP/owasp-mstg

Agenda

- MASVS & MSTG
- **Should you pin?**
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- Basic verification
- Anti-anti pinning techniques
- Recap

Basics first: TLS



TLS is based on PKIX

TLS

Leaf cert

Intermediate

Root CA

Should you pin?

Is your organisation mature enough?

It takes proper certificate lifecycle management to pin!

The in app implementation is **just the next step!**

How about protecting the private key?

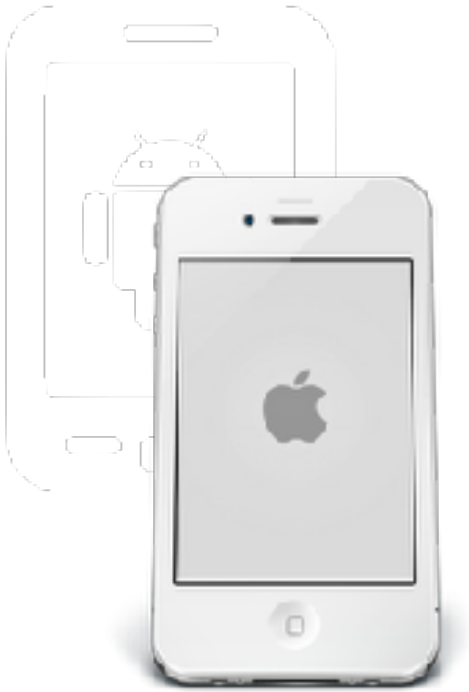
Should you pin?

Pin when you have something valuable to protect
and when you don't trust PKIX

Should you pin?

Pinning does ***NOT protect*** against local attacks

That's where other controls come into play



Agenda

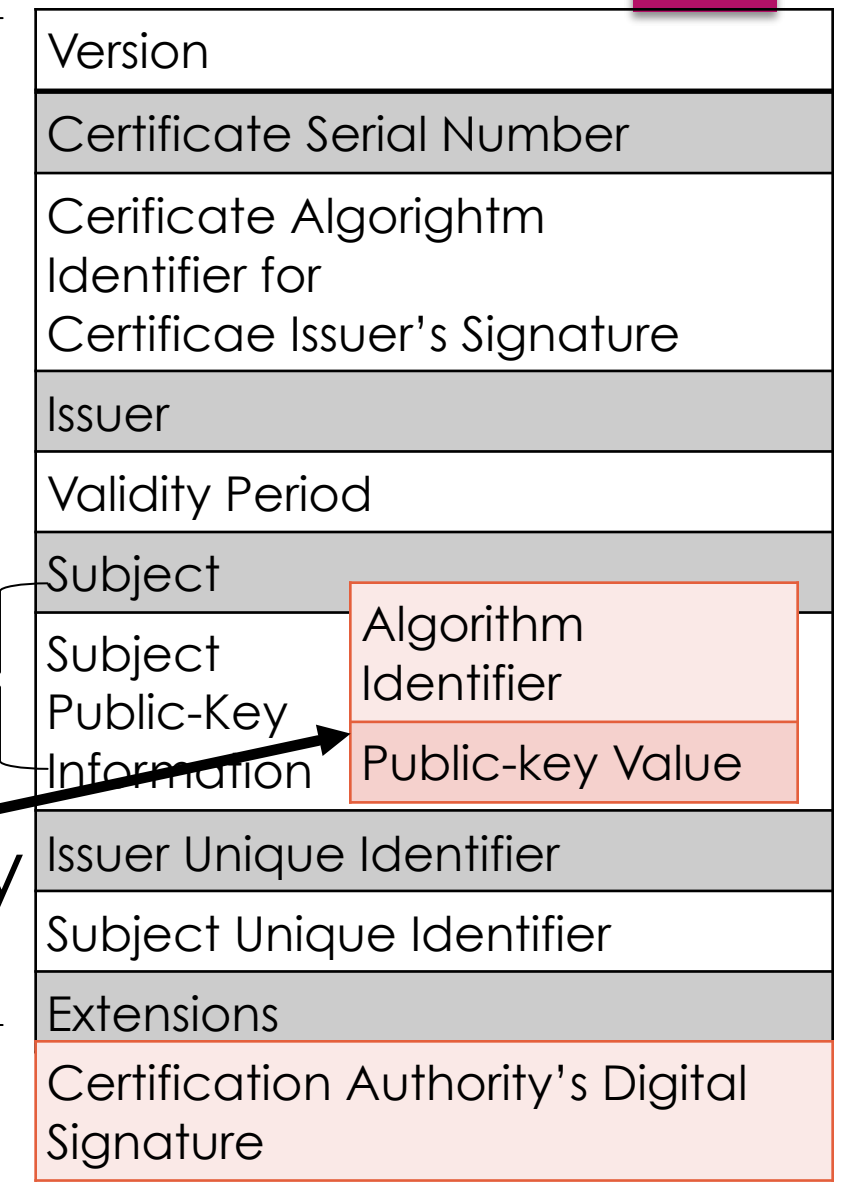
- MASVS & MSTG
- Should you pin?
- **Where to pin to?**
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- Basic verification
- Anti-anti pinning techniques
- Recap

Where to pin to?

Certificate pinning

SPKI fingerprint

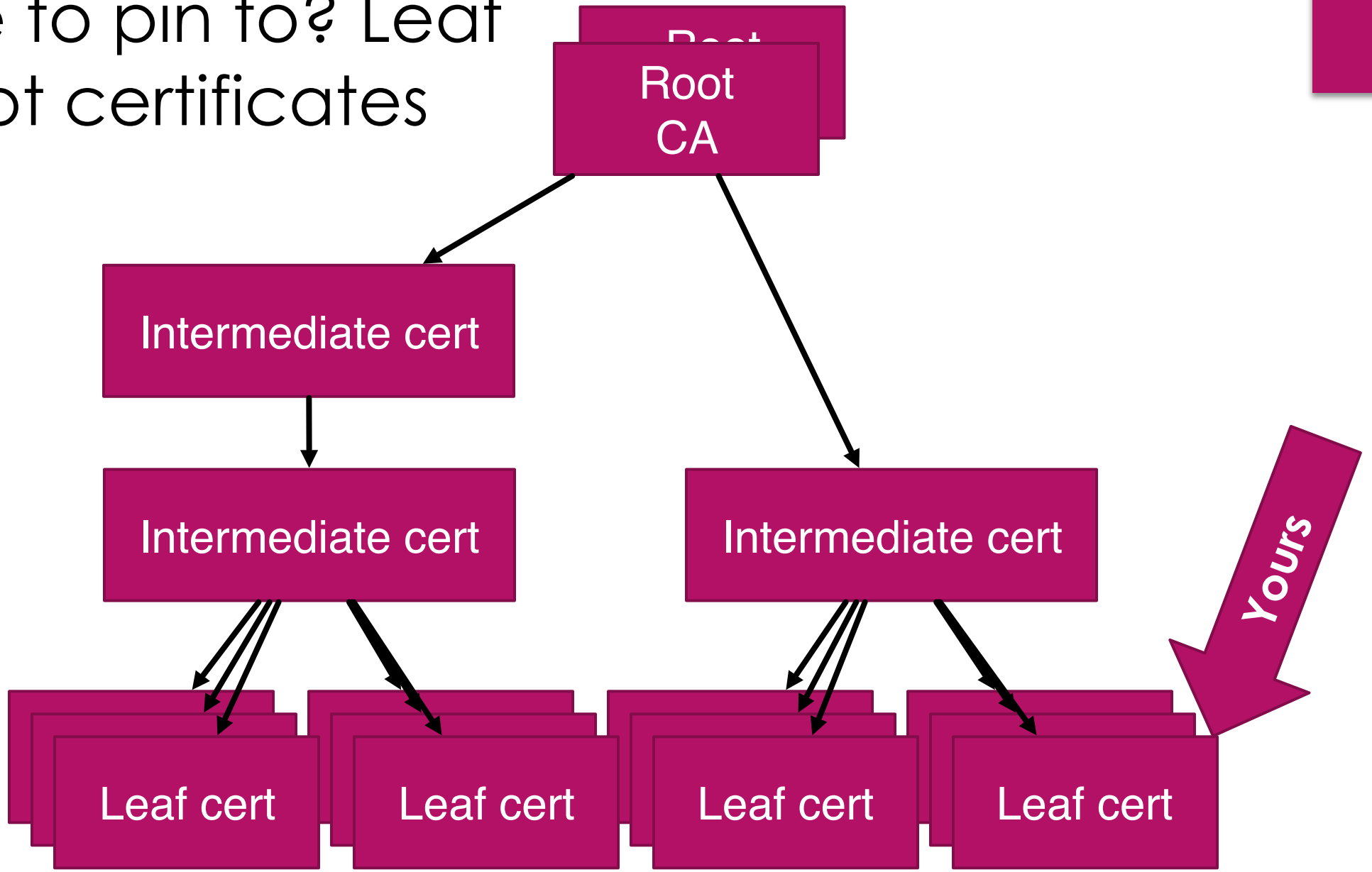
Public key



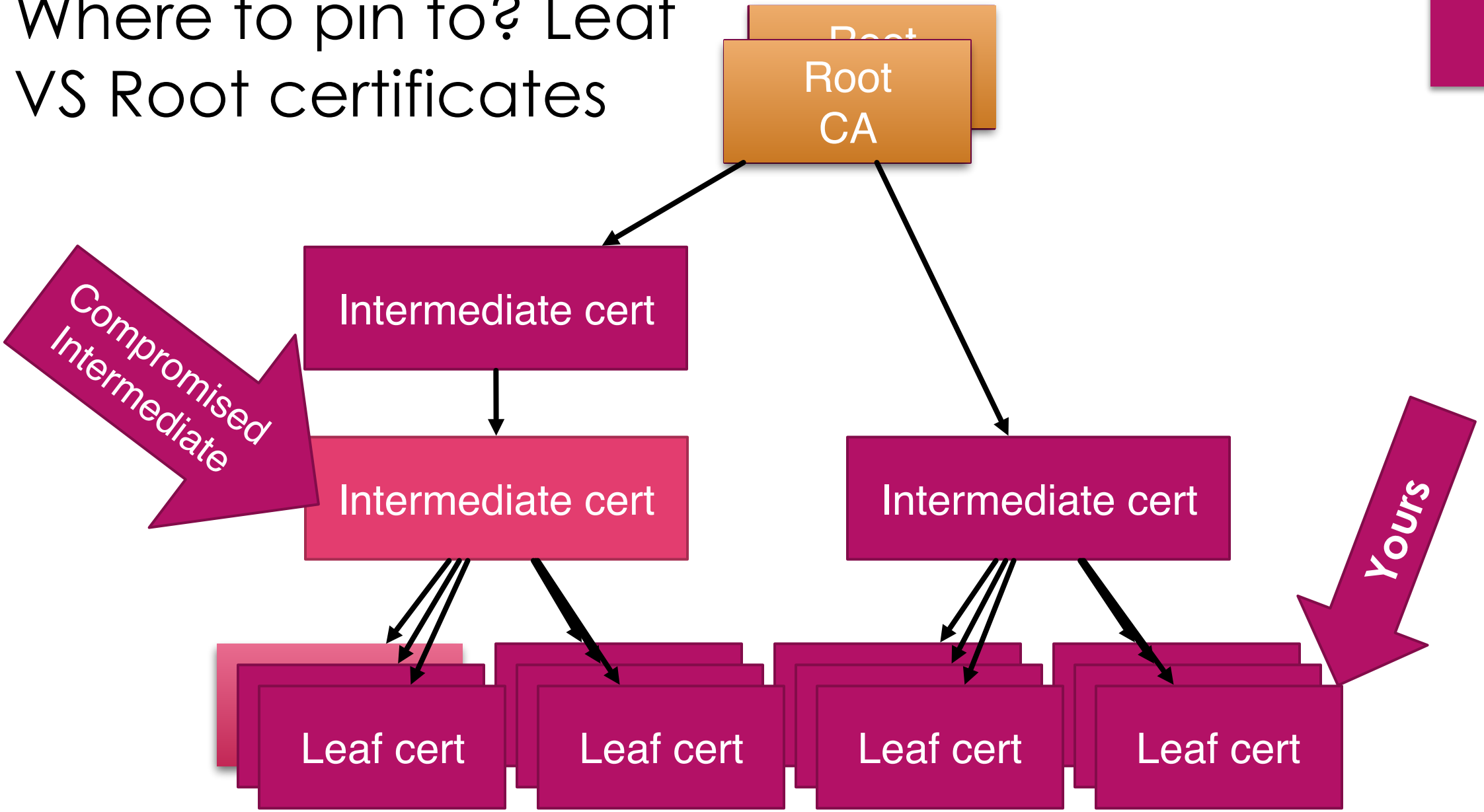
Where to pin to?

What	Certificate	SPKI/public key
Ease of Installation	Just use cert: easiest	Getting easier recently
Expiry	When cert expires	When you stop using the public key
Challenges	- CA's might have multiple certs - Has to be updated more often	- How long can you use that same public key? - Using a self-signed CA? … Still needs a trust-store..

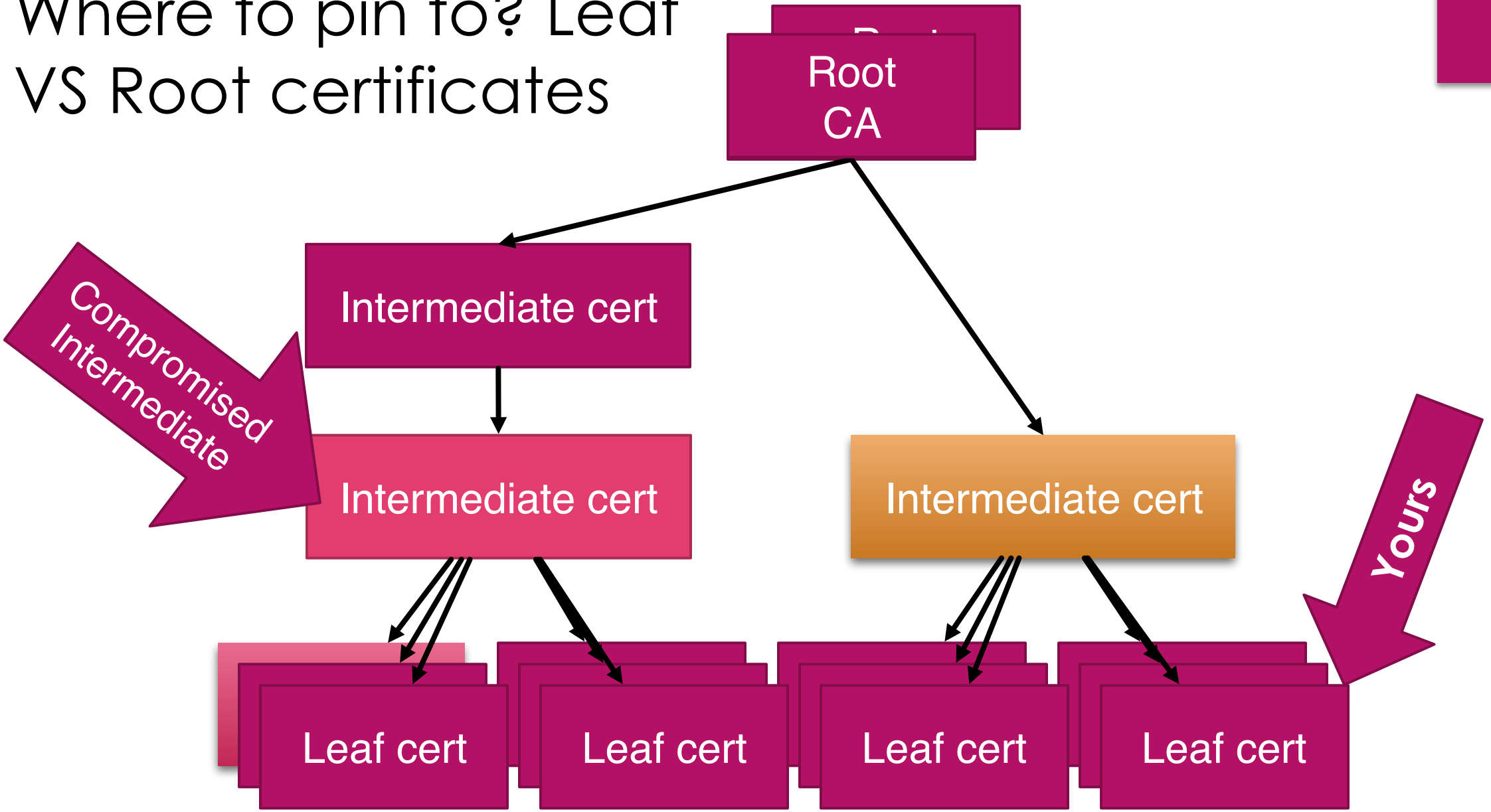
Where to pin to? Leaf VS Root certificates



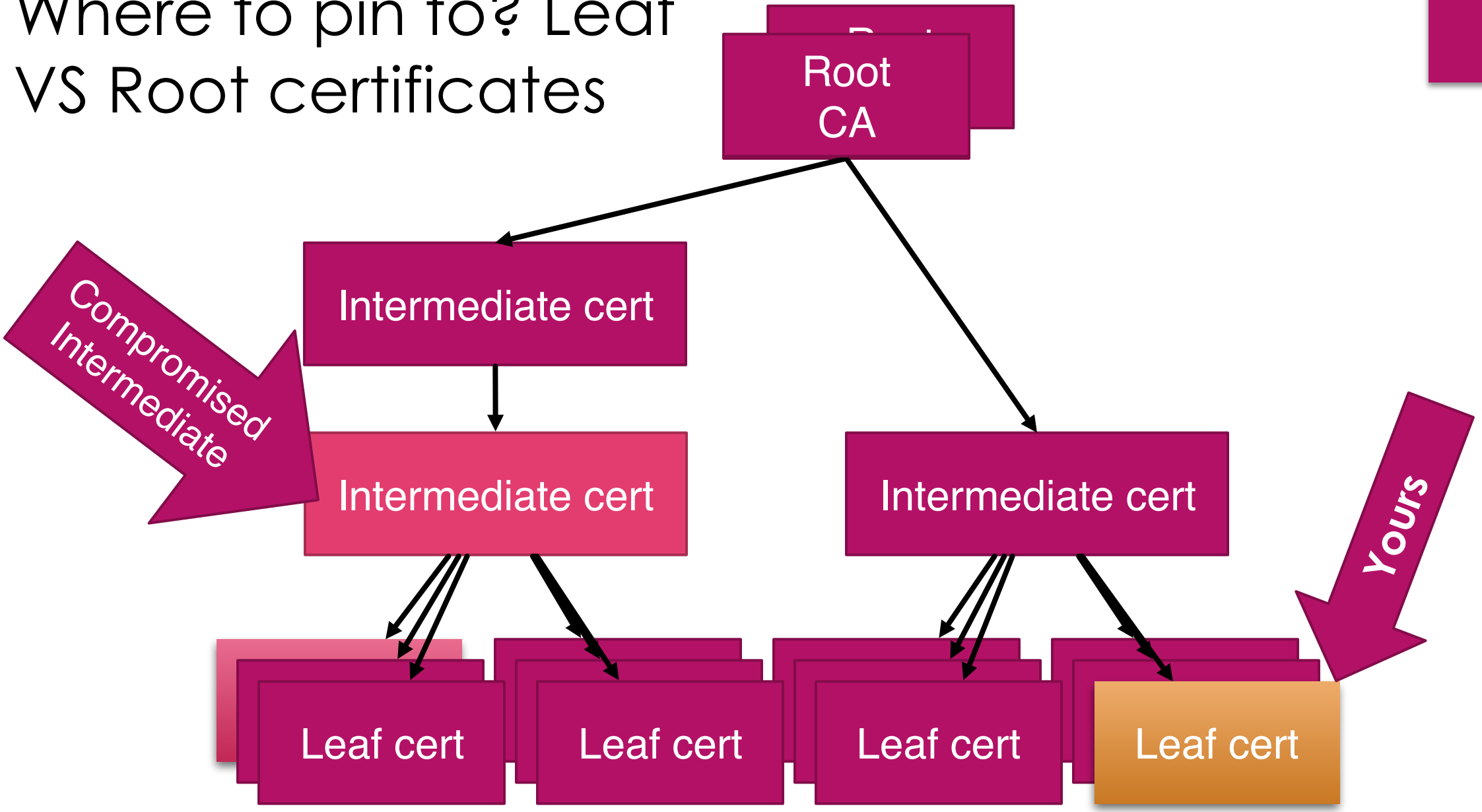
Where to pin to? Leaf VS Root certificates



Where to pin to? Leaf VS Root certificates



Where to pin to? Leaf VS Root certificates



Agenda

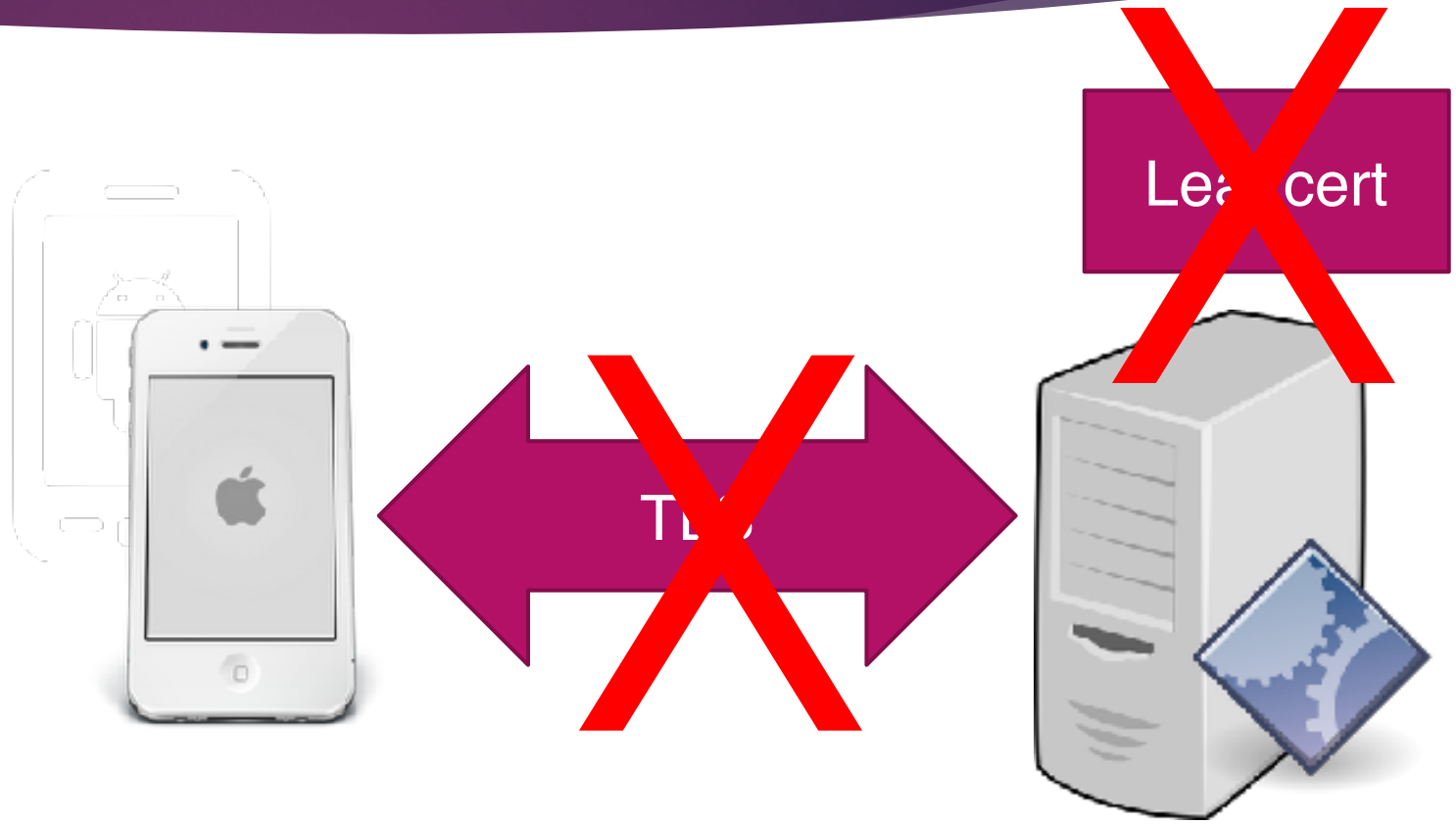
- MASVS & MSTG
- Should you pin?
- Where to pin to?
- **Hardcode VS HTTP Public Key Pinning**
- Pinning in iOS
- Basic verification
- Anti-anti pinning techniques
- Recap

Hardcode it or use HTTP Public Key Pinning

Hardcode:
Programmatically define
to which cert/key you pin.

Stops if key/cert is
no longer there.

Add future public key?



Hardcode it or use HTTP Public Key Pinning

Public-Key-Pins-Report-Only:
max-age=2592000;
pin-sha256="E9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g=";
pin-sha256="LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ=";
report-uri="https://other.example.net/pkp-report"

HTTP Public Key Pinning
RFC 7469
Trust On First Use ← → Vulnerable On First Use
Requires backup pin

Agenda

- MASVS & MSTG
- Should you pin?
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- **Pinning in iOS**
- Basic verification
- Anti-anti pinning techniques
- Recap

Get the materials to pin

- Certificate: download & save
  - *openssl s_client -showcerts -connect your.sub.domain:443*
- Public key:
  - Use your app program-code to extract it programmatically from your cert.
  - *openssl s_client -connect www.google.com:443 -CAfile rootcert.pem | openssl x509 -pubkey -noout | openssl rsa -pubin -outform der | openssl enc -base64 -d > publickey.der*

Get the materials to pin

- Hash over SPKI
  - *openssl s_client -connect www.github.com:443 -CAfile rootcert.pem | openssl x509 -pubkey -noout | openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64*

Pinning in iOS

- Using NSURLConnection
  - canAuthenticateAgainstProtectionSpace: & didReceiveAuthenticationChallenge: → DEPRECATED
  - *optional func connection(_ connection: NSURLConnection, willSendRequestFor challenge: URLAuthenticationChallenge)*

Pinning in iOS

- Using NSURLConnection: connection(_ connection: NSURLConnection, willSendRequestFor challenge: URLAuthenticationChallenge)
  1. Load the certificate in .DER format
  2. Get the remote certificate you want to pin to using *SecTrustGetCertificateAtIndex*
  3. Evaluate the server trust
  4. Verify that the loaded certificate (its public key) is the same as the selected remote certificate

Pinning in iOS

- Using Alamofire:
  1. Setup ServerTrustPolicy with the certificates (or keys)

```
let serverTrustPolicy = ServerTrustPolicy.PinCertificates(
    certificates: ServerTrustPolicy.certificatesInBundle(),
validateCertificateChain: true,
    validateHost: true
) //or keys: pinPublicKeys
```

  2. Initialze the *serverTrustPolicyManager* with the policy

```
let sessionManager = SessionManager( serverTrustPolicyManager:
ServerTrustPolicyManager(policies: serverTrustPolicies) )
```

Pinning in iOS

- Alternative: Trustkit
  1. Get the pins you want to pin to
  2. Enter them in your *Info.plist* file or programmatically initiate the *TrustKit* with a configuration that specify the pins
  3. In your URLSession completionhandler use

*TSKPinningValidator *pinVallididator= [[TrustKit sharedInstance] pinningValidator];*

and evaluate

[pinningValidator handleChallenge:challenge completionHandler:completionHandler]

Agenda

- MASVS & MSTG
- Should you pin?
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- **Basic verification**
- Anti-anti pinning techniques
- Recap

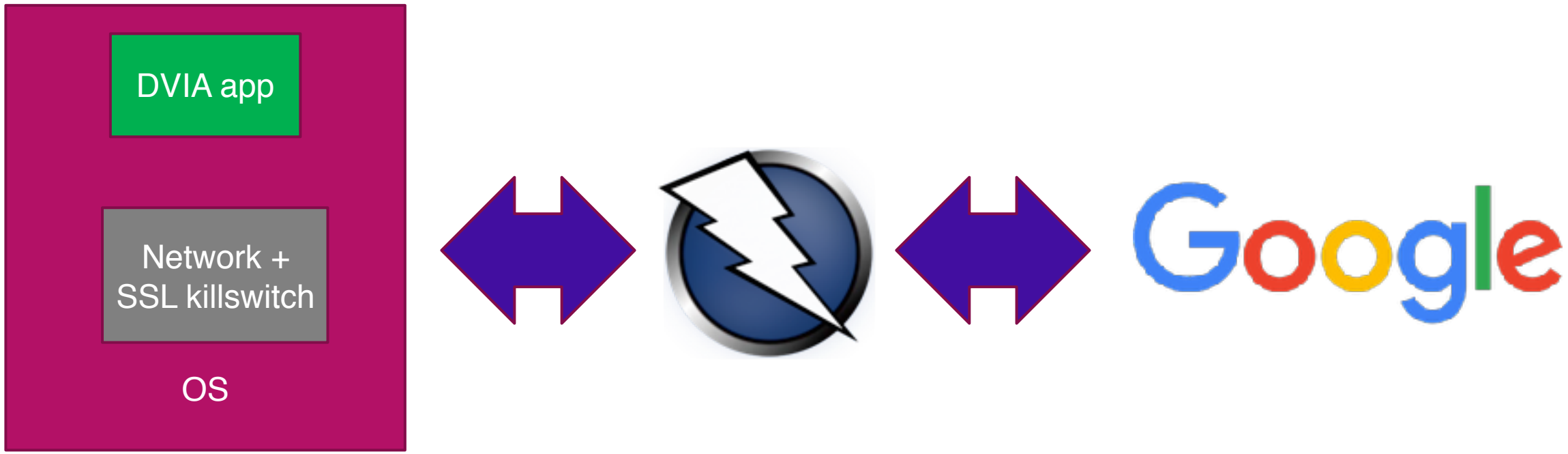
Basic verification

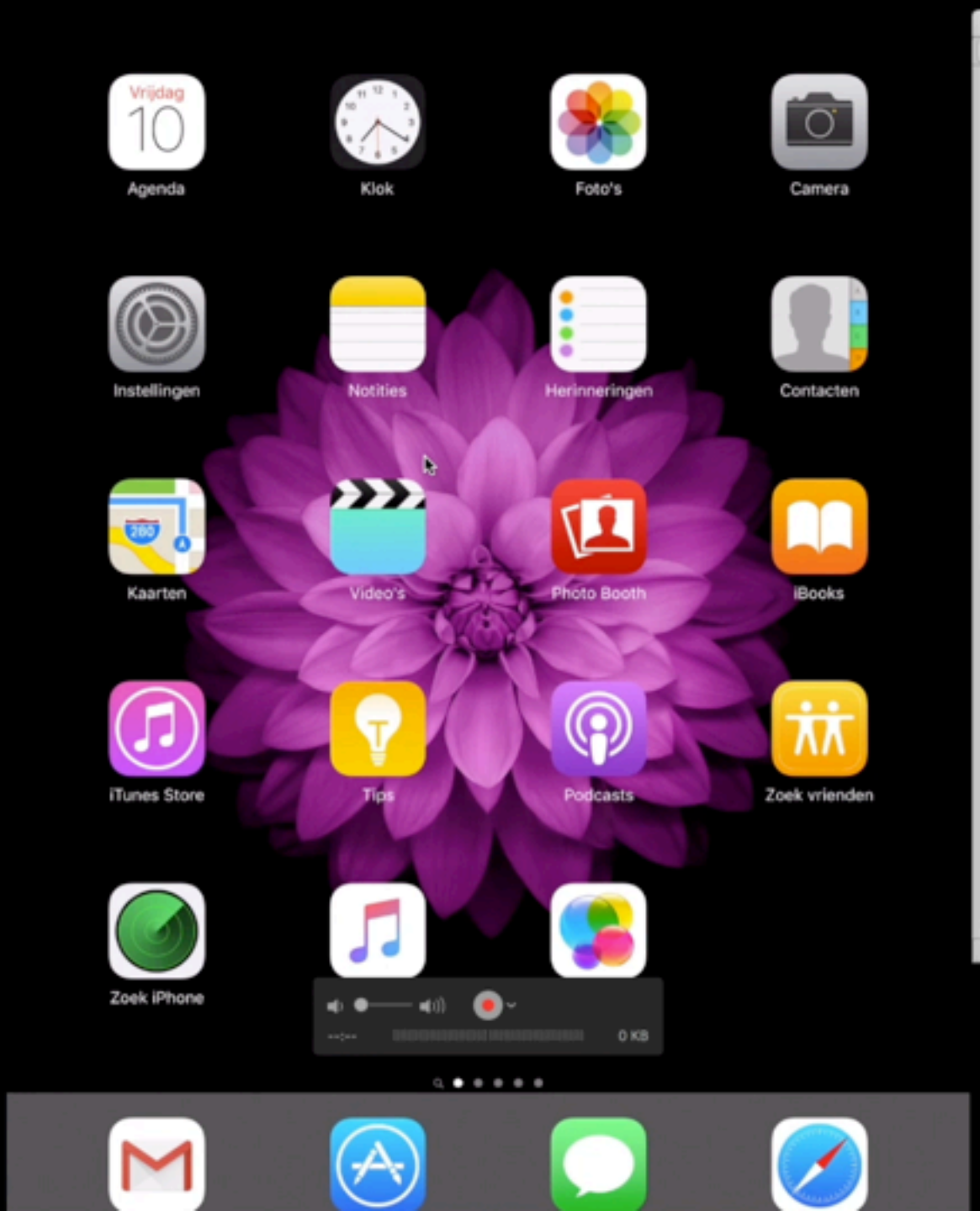
1. Setup Burp
2. Generate a certificate for the given domain and install it on your device
3. Proxy your device through Burp
4. Try to connect with your app to the designated domain.
   - You can? Then you pinned wrongly
     - Repeat same process, now with wrong hostname in step 2.
   - You cannot? BASIC verification completed

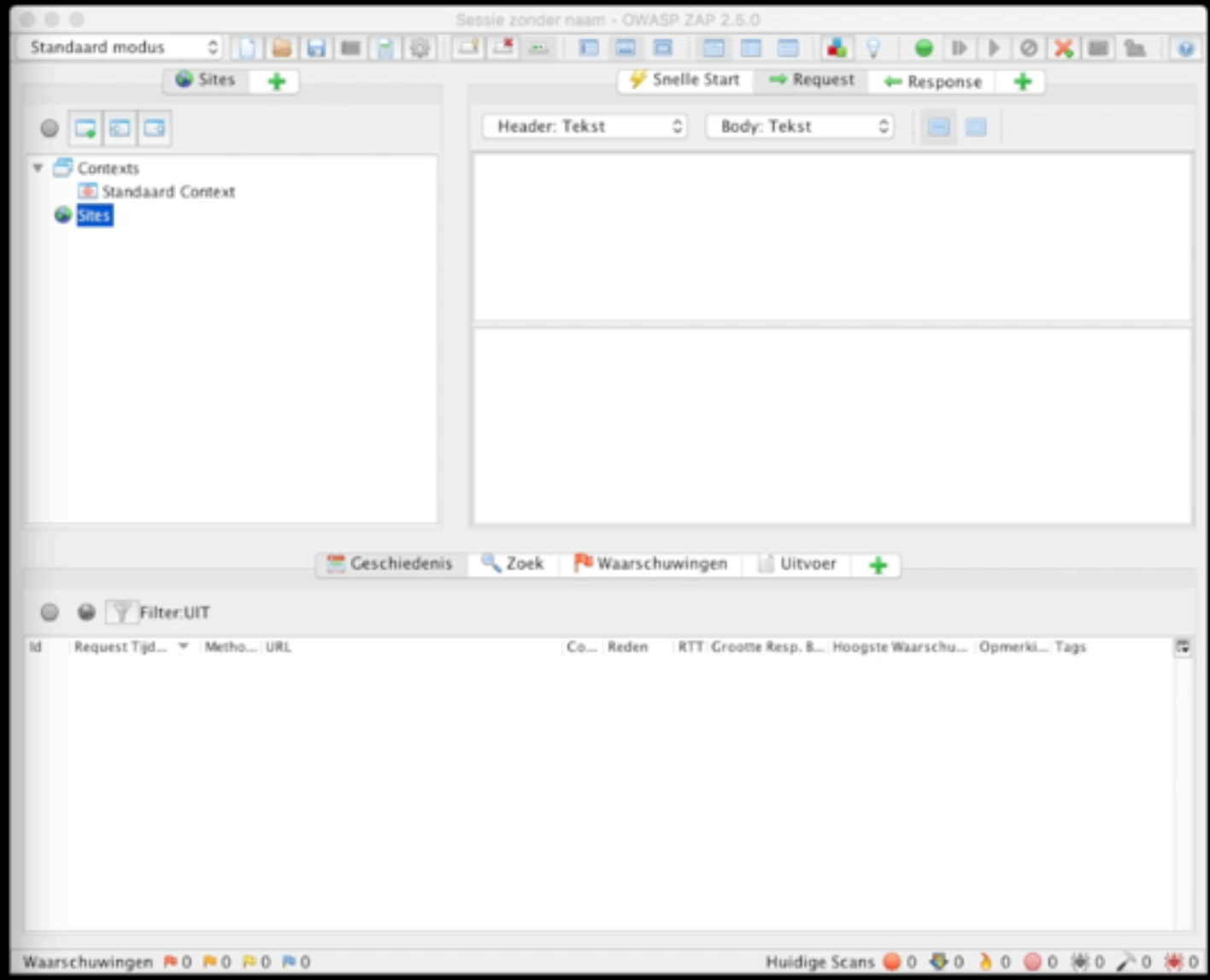
Your secure connection

Demo time!

Basic verification with ZAP and DVIA




Vrijdag
10
Agenda
Klok
Foto's
Camera
Instellingen
Notities
Herinneringen
Contacten
Kaarten
Video's
Photo Booth
iBooks
iTunes Store
Tips
Podcasts
Zoek vrienden
Zoek iPhone
0 KB


Sessie zonder naam - OWASP ZAP 2.5.0
Standaard modus
Sites
Snelle Start
Request
Response
Header: Tekst
Body: Tekst
Contexts
Standaard Context
Sites
Geschiedenis
Zoek
Waarschuwingen
Uitvoer
Filter:UIT
Id
Request Tijd...
Metho...
URL
Co...
Reden
RTT
Grootte Resp. B...
Hoogste Waarschu...
Opmerki...
Tags
Waarschuwingen
Huidige Scans

Agenda

- MASVS & MSTG
- Should you pin?
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- Basic verification
- **Anti-anti pinning techniques**
- recap

Anti anti pinning techniques

- Payload encryption:
  - Using asymmetric crypto
  - Using Secure Remote Password protocol
  - Using other Password Agreement Key Exchange (PAKE) protocols
- Slow down the attacker:
  - Anti-reverse engineering controls (obfuscation)
  - Tamper detection

Agenda

- MASVS & MSTG
- Should you pin?
- Where to pin to?
- Hardcode VS HTTP Public Key Pinning
- Pinning in iOS
- Basic verification
- Anti-anti pinning techniques
- **recap**

Recap

- Pin only if you have to
- Choose your pinning strategy wisely
- Make sure you only pin when your organization is ready
- Validate your pinning implementation

Questions?

Thank you!