nccgroup
freedom from doubt

SSL/TLS SMACK:
State Machine AttaCKs
SKIP-TLS & FREAK

NCC Group Cyber Defence Operations

NCC Group Technical Security Consulting

NCC Group Managed Services

Headlines

- Disclosed late March 3rd (EU time) - https://www.smacktls.com/
- Two attacks
  - SKIP-TLS: spoofing and encryption removal
  - FREAK: downgrading of encryption
- Requires Man-in-the-Middle capabilities

Impact

- SKIP-TLS
  - Spoof any SSL/TLS certificate
  - Downgrade the connection to clear-text

- FREAK
  - Downgrade RSA negotiated connections to export cipher strength

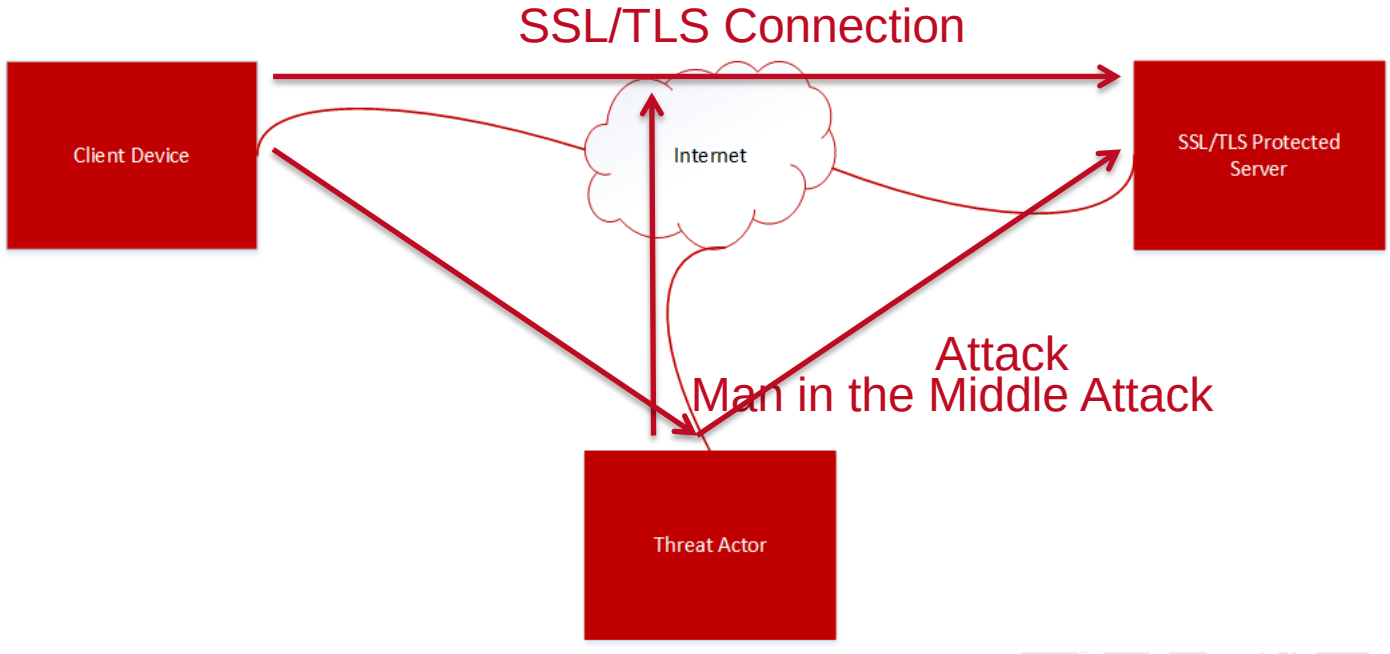
nccgroup
freedom from doubt

What is impacted?

- SKIP-TLS
  - Java's JSSE
  - CyaSSL – embedded system SSL/TLS library

- FREAK
  - OpenSSL / LibreSSL libraries*
  - Safari / BlackBerry (OpenSSL)
  - Android / WebView etc (OpenSSL)

How would exploitation work?



nccgroup
freedom from doubt

What is required for Man-in-the-Middle

- Local network attack (ala Wi-Fi hotspot)
- Remote data path attack (rouge carrier / nation state / other)
- Other means such as DNS

nccgroup
freedom from doubt

Detecting and mitigating vulnerability

- Servers:
  - scan for export cipher support for all SSL/TLS server
  - disable to mitigate FREAK against your clients
- Clients:
  - use software inventory management and/or other analysis techniques
  - not possible to mitigate without upgrade

Real world risk…

- Exploitation likelihood: less than Heartbleed

- Impact – SKIP-TLS:
  - complete loss of identification authentication of server
  - complete loss of integrity and encryption

- Impact: FREAK
  - downgrade of encryption leading to complete loss

Summary and conclusions

- Very serious but..
- … less mass scale exploitable than Heartbleed
- FREAK can be mitigated for your clients/customers at the sever
- FREAK/SKIP-TLS hard to mitigate at device level

Ongoing activities

NCC Group Cyber Defence Operations are looking at possible signatures for vulnerability as well as active attack.

Updates will be provided via the blog:

https://www.nccgroup.com/en/blog/2015/03/smack-skip-tls-and-freak-ssltls-vulnerabilities/

Thanks! Questions?

nccgroup
freedom from doubt

North America

Atlanta
Austin
Chicago
Mountain View
New York
San Francisco
Seattle

Europe

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Milton Keynes
Amsterdam
Copenhagen
Munich
Zurich

Australia

Sydney

Blog:
https://www.nccgroup.com/en/blog

Twitter:
@NCCGroupInfoSec

Cyber Incident Response Team
cirt@nccgroup.com

Cyber Security Services

nccgroup
freedom from doubt

Risk Management & Governance	Technical Security Consulting	Managed Services	Cyber Incident Response & Cyber Defence Operations
PCI DSS , ISO 27001	App & Infra Assessments	PCI ASV Scanning	Cyber Readiness
CAS(T), CLAS, PSN	CBEST,CHECK,CTAS,CPA	Web App Scanning	CIR Training
SANS/CPNI Top 20	Mobile Security	SQA Web App Scanning	Intrusion Discovery
Virtual CISO or ISM	Code Reviews	Internal & External Scanning	Incident Response
Cyber Security Strategy	Product Evaluations	Daily Delta Scanning	Digital Forensics
Risk Transformation	M&A Due Diligence	DDoS Simulation	Malware Analysis
Data Protection	Red Teaming / Phishing	SAST & DAST	Protective Monitoring
Security Architecture	Cyber Essentials		Light Weight Threat Intel
Innovation and Research			