密级：外部公开

31C3会议的热门议题

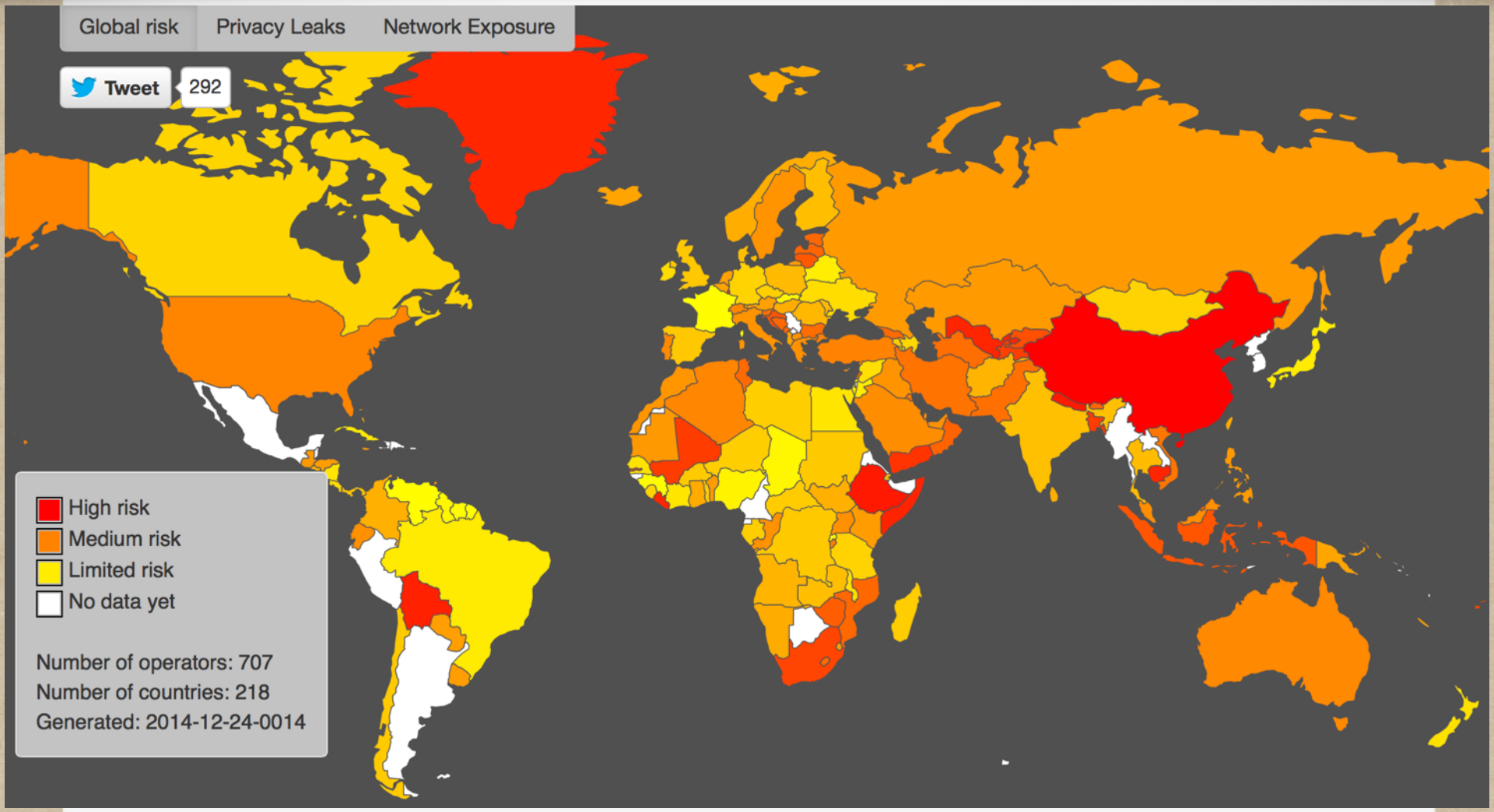
(ISC)² 北京分会

2015年1月15日

Agenda

1. SS7 七号信令安全问题
   - SS7: Locate. Track. Manipulate.
   - Mobile self-defense
   - SS7map : mapping vulnerability of the international mobile roaming infrastructure
2. EMV 银行卡PIN拦截和欺诈检测
   - Practical EMV PIN interception and fraud detection
3. NSA 的新爆料(声明:纯转发不代表分会观点)
   - Reconstructing narratives

1. SS7安全问题 - SS7map



1. SS7安全问题 - 风险点

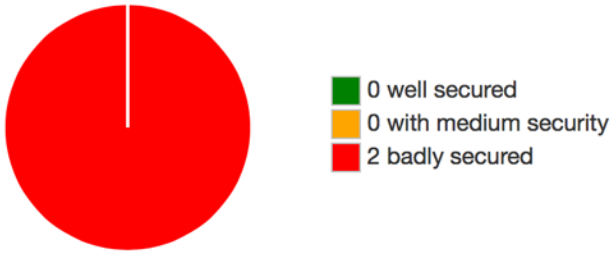
- Privacy Leaks
  - Operators are leaking out subscriber privacy data such as location of their subscribers or IMSI to anyone on the SS7 network.
- Network Exposure
  - Network Elements exposed and security mechanism implemented by operators. It shows the attack surface of the Telecom Network of a country from the SS7 perspective.

1. SS7安全问题 - 中国现状

Privacy Risk level	**164 / 218** 2986.8
SS7 messages disclosing subscriber city location	8
SS7 messages disclosing subscriber street location	4
SS7 messages disclosing private informations	8
Leak of subscriber keys	2
Leak of prepaid/postpaid status	2
Leak subscriber location through Home Routing bypass	?
Network Exposure level	**164 / 218** 2644.9
SCCP discovery attack surface	567
Network Elements fingerprint	567
Potential change of prepaid/postpaid status (fraud)	2
Home Routing*	0
Leak of internal topology through Home Routing bypass	?

SS7 Security of China

Operators tested



2 surveyed operator / 3 operators

2. EMV 银行卡PIN拦截和欺诈检测

由于时间关系，请自行观看最后一页链接的演讲视频:P

3. NSA的新爆料

Prying Eyes: Inside the NSA's War on Internet Security

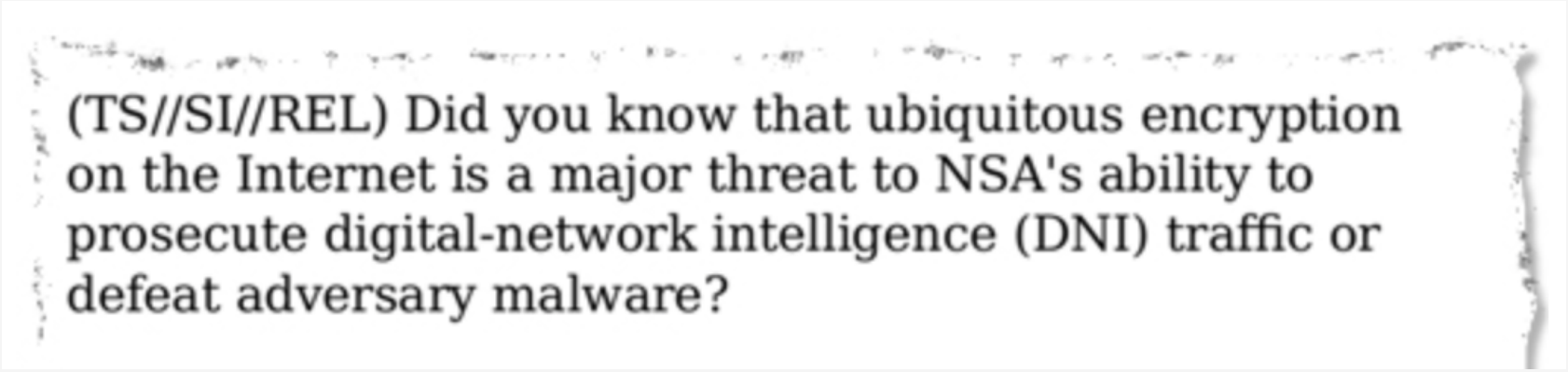
By SPIEGEL Staff

AP/dpa

US and British intelligence agencies undertake every effort imaginable to crack all types of encrypted Internet communication. The cloud, it seems, is full of holes. The good news: New Snowden documents show that some forms of encryption still cause problems for the NSA.

Different Threat?

- For the NSA, encrypted communication -- or what all other Internet users would call secure communication -- is "a threat".


(TS//SI//REL) Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?

$$$$$

- In 2013, the NSA had a budget of more than $10 billion.
- According to the US intelligence budget for 2013, the money allocated for the NSA department called Cryptanalysis and Exploitation Services (CES) alone was $34.3 million.

Skype

- “Sustained Skype collection began in Feb 2011”

VPN

- NSA operates a large-scale VPN exploitation project to crack large numbers of connections, allowing it to intercept the data exchanged inside the VPN — including
  - the Greek government's use of VPNs
  - SecurityKiss, a VPN service in Ireland

VPN…cont.

- by the end of 2011, the NSA … simultaneously surveilling 20,000 supposedly secure VPN communications per hour.
- PPTP
  - a project called FOURSCORE that stores information including decrypted PPTP VPN metadata.
- IPSec
  - attack routers involved in the communication process to get to the keys to unlock the encryption rather than trying to break it

SSL/TLS

- NSA intended to crack 10 million intercepted https connections a day by late 2012
- collects information about encryption using the TLS and SSL protocols … in a database called "FLYING PIG."
  - weekly trends report to catalog services
  - Sites like Facebook, Twitter, Hotmail, Yahoo and Apple's iCloud service top the charts

SSH

- SSH
  - The NSA also has a program with which it claims it can sometimes decrypt the Secure Shell protocol (SSH)

Weakening Cryptographic Standards

- NSA agents travel to the meetings of the Internet Engineering Task Force (IETF)
  - ...to influence the discussions there

Weakening Cryptographic Standards…cont.

- using supercomputers
  - The NSA maintains a system called Longhaul, an "end-to-end attack orchestration and key recovery service for Data Network Cipher and Data Network Session Cipher traffic."

Weakening Cryptographic Standards…cont.

- to steal cryptographic keys from the configuration files found on Internet routers.
  - A repository called Discoroute contains "router configuration data from passive and active collection”

Weakening Cryptographic Standards…cont.

- gathering of vast amounts of data
  - For example, they collect so-called SSL handshakes

Weakening Cryptographic Standards…cont.

- If all else fails, the NSA and its allies resort to brute force
  - They hack their target's computers or Internet routers

Blind to NSA

- Truecrypt
  - Developers stopped their work…last May
- OTR (off-the-record)
  - "No decrypt available for this OTR message.”
- PGP
  - it remains too robust for the NSA spies to crack
  - Five Eyes intelligence services sometimes use PGP themselves

Blind to NSA…cont.

- Tor+CSpace+ZRTP
  - "near-total loss/lack of insight to target communications, presence”

1. Tor: Anonymization service
2. CSpace: Instant messaging system
3. ZRTP: Internet telephony (voice over IP)

A Grave Threat to Security

- For the NSA, the breaking of encryption methods represents a constant conflict of interest.
- NSA is also tasked with providing the US National Institute of Standards and Technology (NIST) with "technical guidelines in trusted technology"
- One NSA document shows that the agency is actively looking for ways to break the very standard it recommends. e.g. AES

The End


The Colbert Report
March 14, 2014 ·
Like Page
"Remember NSA employees: surveillance is designed to out treason, so it shouldn't bother you if you aren't hiding anything. Since nothing can be hidden from the NSA, nothing is bothering you." http://on.cc.com/1fucu7d
Like · Comment · Share
815 people like this.
Top Comments

结束语


Google
Sign in
Translate
English
Spanish
French
English - detected
Chinese (Simplified)
English
Spanish
Translate
surveillance is designed to out treason, so it shouldn't bother you if you aren't hiding anything. Since nothing can be hidden from the NSA, nothing is bothering you.
监督的目的是叛国罪，所以它不应该打扰你，如果你不隐瞒任何东西。因为没有什么可以隐藏的国家安全局，没有什么在困扰你。

Links

1. http://media.ccc.de/browse/congress/2014/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel.html#video
2. http://media.ccc.de/browse/congress/2014/31c3_-_6122_-_en_-_saal_1_-_201412271830_-_mobile_self-defense_-_karsten_nohl.html#video
3. http://media.ccc.de/browse/congress/2014/31c3_-_6531_-_en_-_saal_6_-_201412272300_-_ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira.html#video
4. http://media.ccc.de/browse/congress/2014/31c3_-_6120_-_en_-_saal_1_-_201412271600_-_practical_emv_pin_interception_and_fraud_detection_-_andrea_barisani.html#video
5. http://media.ccc.de/browse/congress/2014/31c3_-_6258_-_en_-_saal_1_-_201412282030_-_reconstructing_narratives_-_jacob_-_laura_poitras.html#video
6. http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

关于(ISC)²北京分会

- (ISC)²是推出信息安全领域金牌认证CISSP的美国非盈利教育组织，在中国的(ISC)²北京分会成立于2014年11月1日，专注信息安全，旨在建立北京及周边地区的一个安全技术交流的网络，促进分会会员之间的信息分享、经验交流、技术讨论和个人职业发展
- (ISC)²北京分会微信公众号：ISC2BJ
- 联系邮件：info@isc2chapter-beijing.org