THEY

Hear See Don't Speak

The Impact of Pervasive Monitoring on Corporate InfoSec

Enno Rey, erey@ernw.de

ERNW
providing security.

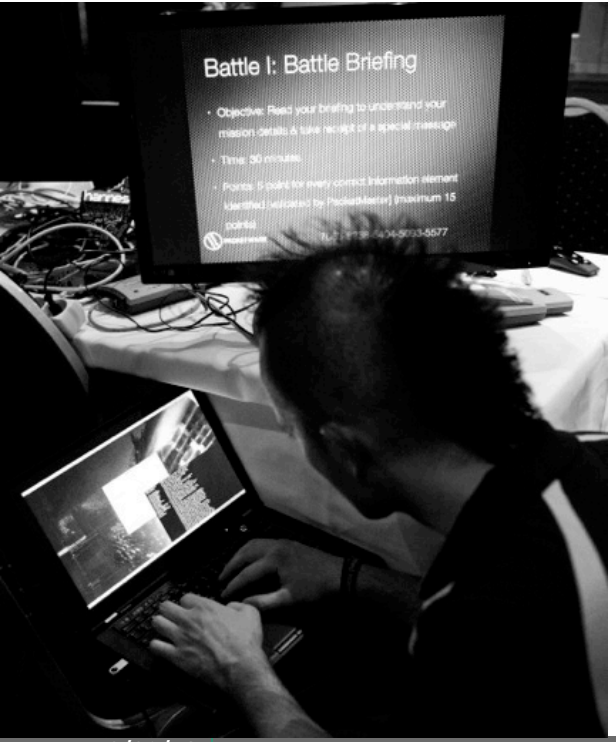
On the speaker

- Founder (2001) and managing director of highly specialized security consulting and assessment services company ERNW.
- Works as "right hand" and trusted business advisor of several CISOs of very large enterprises.
- Host of security conference *TROOPERS.*
- Regularly blogs on www.insinuator.net.

Main Question of this Presentation

- Do the recent revelations about large-scale surveillance activities by the NSA (and other intelligence agencies) change the way we perform corporate information security (management)?

Agenda



- Surveillance Approaches
- Consequences for CorpInfoSec
- Conclusions

Some Definition

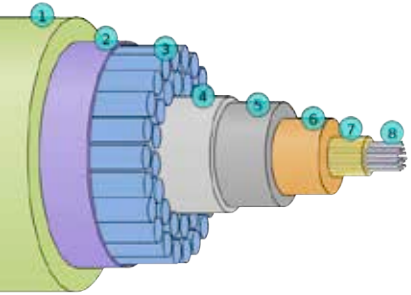
RFC 6973 *Privacy Considerations for Internet Protocols*

Surveillance is the observation or monitoring of an individual's communications or activities.

The effects of surveillance on the individual can range from anxiety and discomfort to behavioral changes such as inhibition and self-censorship, and even to the perpetration of violence against the individual.

Taxonomy

Access data



in transit

at rest

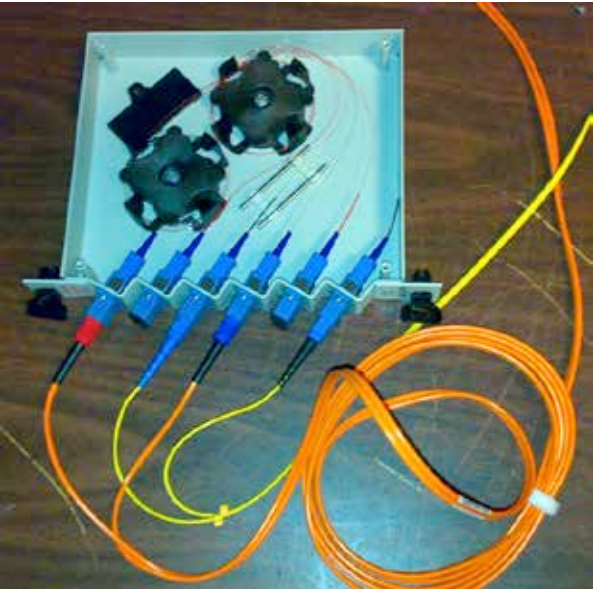
at 3rd parties

Of course, Several Approaches Can Be Combined

- Think Dropbox
  - In transit
  - At rest (locally & remote)
  - 3rd party

- Well, it's encrypted.
  - But they have the keys...
  - Who's *they* anyway?

In Transit



Fibre optic tab

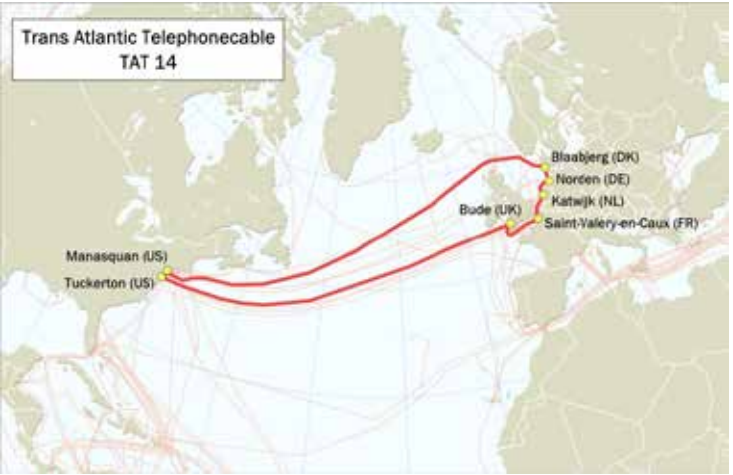
- Get hold of it (redirect, if needed)
- Store & analyze
- Decrypt
- Correlate

Get Hold of It

The infamous *Room 641A*

- Redirect
- Sniff at centralized points
  - MPLS backbones
  - *Transatlantic Telecommunications Cables*

TAT-14



Copyright: Alexrk2

- This And That
- Take All Transactions
- Trust American Thieves

Spot the difference ;-)

Belgacom Attack – EU Calling… and NSA Listening?

ERNW providing security.

http://www.standaard.be/cnt/dmf20130915_00743233

Belgacom Attack – EU Calling… and NSA Listening?

ERNW
providing security.

http://www.standaard.be/cnt/dmf20130915_00743233

The Fake Internet Café

& FREE WIFI FOR EVERBODY ;-)

http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

Store & Analyze

Correlate

Find the Needle in A Haystack

aka: Identify an Individual's Actions

- The need (and, btw, capability) to correlate might be one of the main differences to a *targeted attack*.
- This is where XKeyscore et.al. come in

The effects of surveillance on the individual can range from anxiety and discomfort to behavioral changes such as inhibition and self-censorship, and even to the perpetration of violence against the individual.

- Keep in mind that all collected data is stored anyway.

#NSAPickUpLines

ERNW
providing security.

N. Pitaphoros
@engineofentropy
Follow

"No gurl, I wasn't *stalking* you, I was just mining your metadata. There's totally a difference" #nsapickuplines

2:13 PM - 6 Jun 2013

61 RETWEETS 33 FAVORITES

Jude Morrissey
@Steampunk_Gypsy
Follow

I know EXACTLY what will make you happy. No, seriously, I've been looking into that for a while now. #NSAPickUpLines

2:18 AM - 25 Aug 2013

134 RETWEETS 66 FAVORITES

Jay Rosen
@jayrosen_nyu
Follow

You're free Friday. Would you like to have dinner? #NSAPickUpLines

6:08 AM - 25 Aug 2013

268 RETWEETS 112 FAVORITES

NSA pick up lines
@NSApickuplines
Follow

#NSAPickUpLines my love for you is unconstitutional

7:54 AM - 25 Aug 2013

39 RETWEETS 10 FAVORITES

Sec of explaining
@SecOfExplaining
Follow

Where have you been all my life? Just kidding, I know. #NSAPickUpLines

8:06 AM - 26 Aug 2013

5 RETWEETS 5 FAVORITES

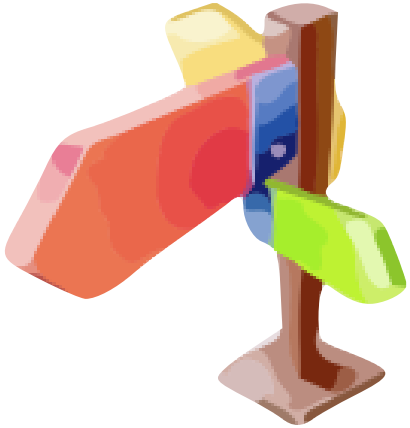
Decrypt

Main Approaches

- Get access to key material
- Break it / Cryptanalysis

Access to Key Material

Some Approaches



- (Friendly) Ask CAs to hand it over
  - Or hack them. DigiNotar?
- (Friendly) Ask Vendors to cooperate
  - I can't help myself of thinking of RSA…

TROOPERS11 Keynote

- Compromise end points

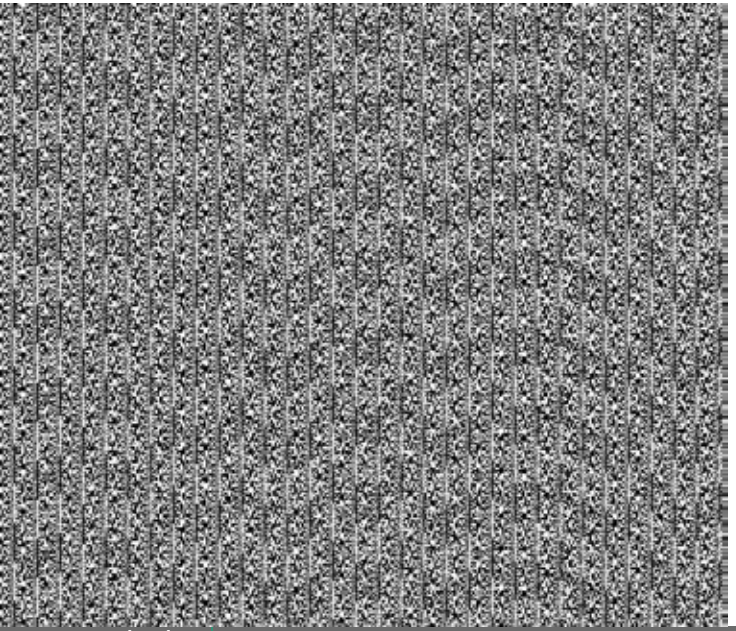
Cryptanalysis

Again, some Approaches

- Advanced cryptanalysis capabilities for supposedly "secure" ciphers?
  - RC4
  - ECC crypto?
  - Others, e.g. AES?
    - Schneier et.al: "probably not".
- Deliberate Weakening
  - Implementation level
    - → Vendor discussion
  - PRNGs

PRNGs

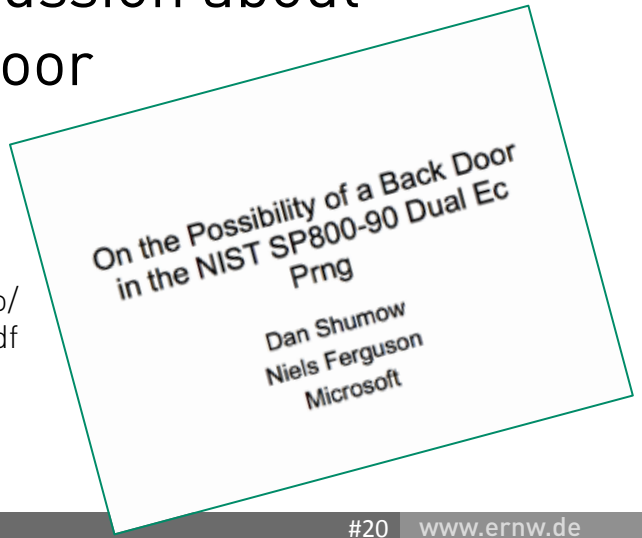
The Discussion about Dual_EC_DRBG



Pseudo randomness visualized by Bo Allen

- Standardized 2006 in NIST *Special Publication 800-90*
- Since 2007 discussion about potential backdoor

http://rump2007.cr.yp.to/15-shumow.pdf



On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow
Niels Ferguson
Microsoft

Dual_EC_DRBG

DRBG Validation List

Last Update: 8/17/2013

401	**Cisco Systems, Inc.** 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	**IOS Algorithms** Version 1.0 (Firmware)	Cavium CN5200; Freescale MPC8343A; Intel 82576; Freescale P1021; Freescale MPC8358E	8/30/2013

CTR_DRBG: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256) (AES Val#2620)]

"IOS Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions."

Dual_EC_DBRG

Where It *Might* Be Used

DRBG Validation List

Last Update: 9/17/2013

Overview

The page provides technical information about implementations that have been validated as conforming to the Deterministic Random Bit Generator (DRBG) Algorithm, as specified in Special Publication 800-90, Recommendation for Random Number Generators Using Deterministic Random Bit Generators.

The list below describes implementations which have been validated as correctly implementing the DRBG algorithm, using the tests found in The DRBG Validation Suite (DRBGVS). This testing is performed by NVLAP accredited Cryptographic And Security Testing (CST) Laboratories.

The implementations below consist of software, firmware, hardware, and any combination thereof. The National Institute of Standards and Technology (NIST) has made every attempt to provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, NIST cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list.

This list is ordered in reverse numerical order, by validation number. Thus, the more recent validations are located closer to the top of the list. The column after the Validation Date column contains information indicating what modes and features for these modes has been successfully tested.

Validation No.	Vendor	Implementation	Operational Environment	Val. Date	Description/Notes
403	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team	IOS Common Cryptographic Module (IC2M) within CatsK Version Rel 1 (1.0.0) (Firmware)	Freescale MPC8572E	9/11/2013	CTR_DRBG [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df (AES-256) (AES Val#2624)] "IOS Common Cryptographic Module within catsk"
402	Box, Inc. 4440 El Camino Real Los Altos, CA 94022 USA -Crispen Maung TEL: (650) 329-1210	Box Upload/Download Cryptographic Module Version 1	Intel(R) Xeon(R) CPU w/ Scientific Linux 6.4	9/11/2013	CTR_DRBG [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df (AES-256) (AES Val#2622)] BlockCipher_No_df (, AES-256) (AES Val#2622)] "Box"s cryptographic module is a C language-based implementation of cryptographic functions built using an OpenSSL FIPS Object Module. Box provides assurance that content encrypted by the product utilizes a FIPS 140-2 solution."
			Cavium CN5200, Freescale MPC8310A, Intel E2576, Freescale P1021, Freescale MPC8555E	8/30/2013	CTR_DRBG [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df (AES-256) (AES Val#2620)] "IOS Firmware cryptographic implementations used within Cisco devices to provide cryptographic functions."
			Motorola Freescale MPC8280 (PPC12)	8/30/2013	Hash_Based DRBG [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS Val#2199)] "The SslC Cryptographic Library provides cryptographic algorithms for the SslC family of products. Based on OpenSSL, the SslC Cryptographic Library requires an Application Programming Interface (API) to support software based security relevant services within SafeNet"s SslC product line."
					Hash_Based DRBG [Prediction Resistance Tested: Not Enabled (SHA-256) (SHS

ERNW
providing security.

Re: [Cryptography] Opening Discussion: Speculation on "BULLRUN"

John Gilmore | Fri, 06 Sep 2013 17:49:35 -0700

Speaking as someone who followed the IPSEC IETF standards committee pretty closely, while leading a group that tried to implement it and make so usable that it would be used by default throughout the Internet, I noticed some things:

* NSA employees participted throughout, and occupied leadership roles in the committee and among the editors of the documents

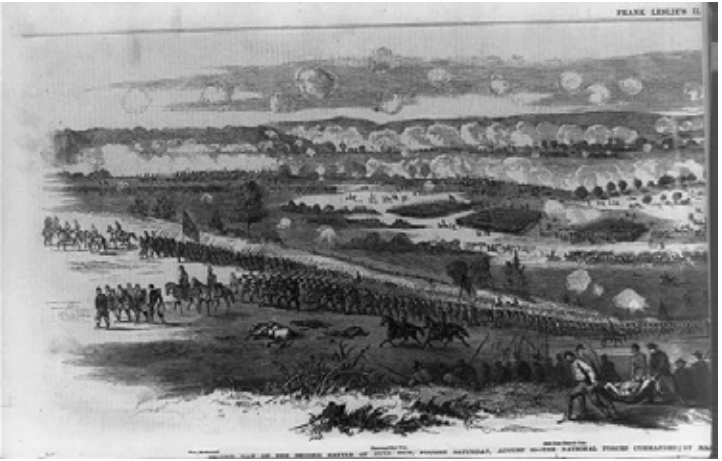
* Every once in a while, someone not an NSA employee, but who had longstanding ties to NSA, would make a suggestion that reduced privacy or security, but which seemed to make sense when viewed by people who didn't know much about crypto. For example, using the same IV (initialization vector) throughout a session, rather than making a new one for each packet. Or, retaining a way to for this encryption protocol to specify that no encryption is to be applied.

Speculation on "BULLRUN"

http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html

Bullrun

http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html



Twitter List: Reporters and Editors

Readers' Comments

Readers shared their thoughts on this article.

Read All Comments (1466) »

At Microsoft, as The Guardian has reported, the N.S.A. worked with company officials to get pre-encryption access to Microsoft's most popular services, including Outlook e-mail, Skype Internet phone calls and chats, and SkyDrive, the company's cloud storage service.

Microsoft asserted that it had merely complied with "lawful demands" of the government, and in some cases, the collaboration was clearly coerced. Some companies have been asked to hand the government the encryption keys to all customer communications, according to people familiar with the government's requests.

Cryptographers have long suspected that the agency planted vulnerabilities in a standard adopted in 2006 by the National Institute of Standards and Technology and later by the International Organization for Standardization, which has 163 countries as members.

Classified N.S.A. memos appear to confirm that the fatal weakness, discovered by two Microsoft cryptographers in 2007, was engineered by the agency. The N.S.A. wrote the standard and aggressively pushed it on the international group, privately calling the effort "a challenge in finesse."

"Eventually, N.S.A. became the sole editor," the memo says.

Bruce Schneier

in Applied Cryptography Second Edition (1995)

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files."

Access (Data) At Rest

- Traditional exploitation of COTS OSs
  - Reportedly NSA sits on many 0-days.
  - Did they discover & write them?
  - Why should they (take the effort)?
    - There's *TippingPoint's* ZDI.
    - HP is headquartered in Palo Alto, CA. USA
- Attacks against smart phones
  - Anybody trusted Apple before? ;-)
  - Btw... did you already submit your fingerprints?

- Traditional exploitation of COTS OSs
  - Reportedly NSA sits on many 0-days.
  - Did they discover & write them?
  - Why should they (take the effort)?
    - There's *TippingPoint's* ZDI.
    - HP is headquartered in Palo Alto, CA. USA
- Attacks against smart phones
  - Anybody trusted Apple before? ;-)
  - Btw... did you already submit your fingerprints?

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop

RSS | Mobile | Newsletter

Sign In | Register

SPIEGEL ONLINE INTERNATIONAL

Front Page | World | Europe | Germany | Business | Zeitgeist | Newsletter

English Site > World > NSA Spying Scandal > Privacy Scandal: NSA Can Spy on Smart Phone Data

Privacy Scandal: NSA Can Spy on Smart Phone Data

SPIEGEL has learned from internal NSA documents that the US intelligence agency has the capability of tapping user data from the iPhone, devices using Android as well as BlackBerry, a system previously believed to be highly secure.

September 07, 2013 - 06:00 PM

Print | Send

Feedback

Tweet 4,188 | Recommend 3.6k | +1

TOPIC

NSA Spying Scandal

National Security Agency

Apple

Related SPIEGEL ONLINE links

iSpy: How the NSA Accesses Smartphone Data (09/09/2013)

'Success Story': NSA Targeted French Foreign

REUTERS

German Chancellor Angela Merkel holds a BlackBerry Z10 smart phone: Will the company face a setback following claims the NSA can spy on its phones?

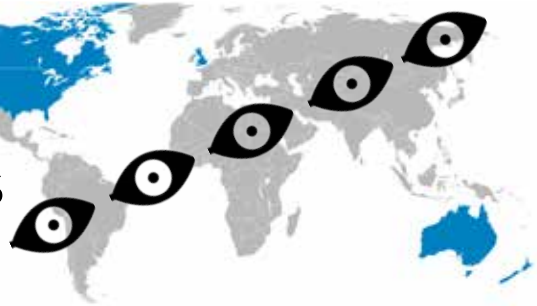
The United States' National Security Agency intelligence-gathering operation is capable of accessing user data from smart phones from all leading manufacturers. Top secret NSA documents that SPIEGEL has seen explicitly note that the NSA can tap into such information on Apple iPhones, BlackBerry devices and Google's Android mobile operating system.

Target in Sight: BlackBerry

http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html

At 3rd Parties

- Coerce them
  - See above
- Hack them
  - See above
- Data exchange between countries



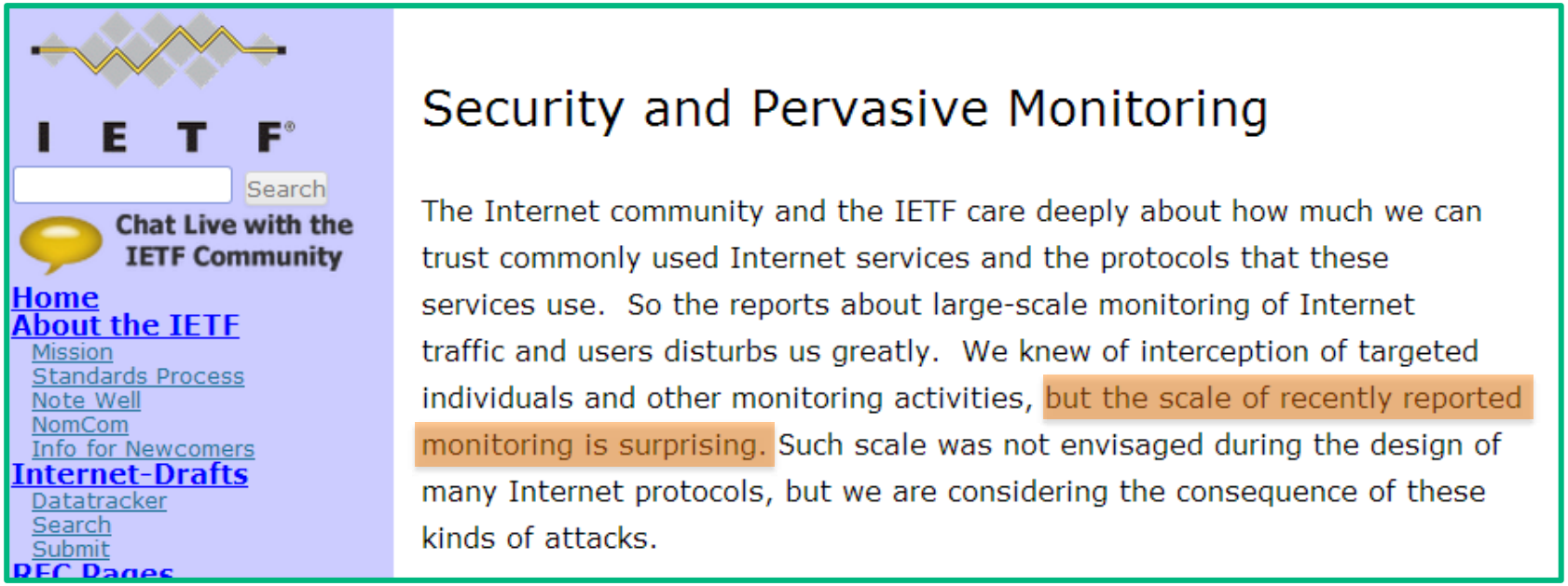
Interim Summary

Infographic: http://www.washingtonpost.com/wp-srv/special/national/black-budget/

- They do pretty much everything they want.
  - And which is in the arsenal of a typical attacker.
  - They have massive funding.
  - Apparently, they're not bound by any legal restrictions.

What Does this Mean?

On a Personal Level



ERNW
providing security.

What Does this Mean?

For Organizations / Enterprises

Please note: all of the following depends on the context of $INDIVIDUAL_ORGANIZATION.

There's no easy answers/recipes here...

Sorry, this space is intentionally left blank.

Some Questions from Corp_ISO's Daily Task

In no specific order ;-)

- Compliance anyone?

- Where/whom do we trust?

- What's our risk profile?

Compliance

Where German Organizations might be Affected

- Data Protection (*Bundesdatenschutzgesetz*).
- Choice of crypto algorithms, in various contexts.
- Banking secrecy (*Bankgeheimnis*)?

ERNW
providing security.

Compliance & Data Protection

Here's what the current chair of the Conference of Federal and State Data Protection Commissioners, Dr. Imke Sommer, stated on 07/24/2013

- "Companies that send personal data to the U.S. bear the responsibility for these data. Like everyone in Germany, they must therefore have an interest in ensuring that personal data flows are not subject to large-scale surveillance by intelligence services."

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf

ERNW
providing security.

Compliance & Data Protection

"The Conference therefore calls on the Federal Government to provide a plausible explanation of how the unlimited access of foreign intelligence services to personal data of persons in Germany is effectively limited in line with the principles referred to. Until this is guaranteed, the data protection supervisory authorities will not issue any new permission for data transfer to non-EU countries (for example also for the use of certain cloud services) and will examine whether such data transfers should be suspended on the basis of the Safe Harbour framework and the standard contractual clauses."

Trust

One Might Ask

After Edward Snowden's revelations, why trust US cloud providers?

The NSA's activities are a massive blow for US computer businesses

John Naughton
The Observer, Sunday 15 September 2013
Jump to comments (59)

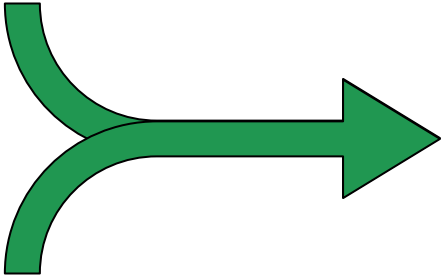
The NSA's activities were unmasked by Edward Snowden. Photograph: Ueslei Marcelino/Reuters

'It's an ill bird," runs the adage, "that fouls its own nest." Cue the US National Security Agency (NSA), which, we now know, has been busily doing this for quite a while. As the Edward Snowden revelations tumbled out, the scale of the fouling slowly began to dawn on us.

Source: http://www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing

The Role of Trust in Corp_InfoSec_Mgmt

TRUST



CONFIDENCE

CONTROL

Trust Properties

This is a Wide Field.

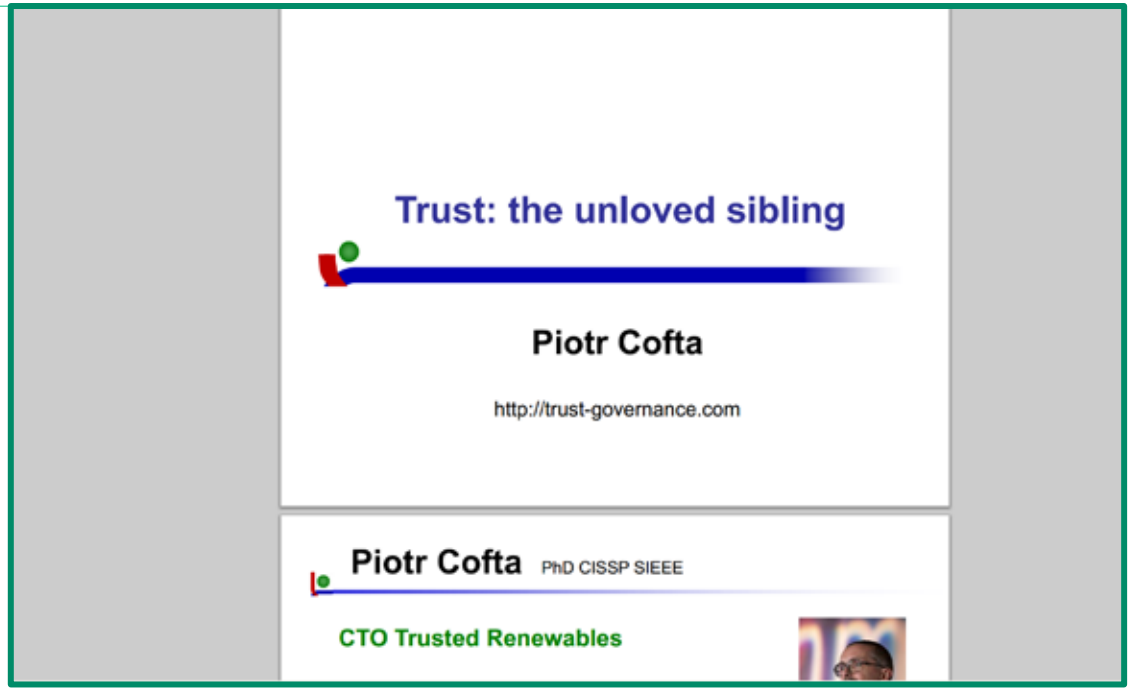
Here's some Approaches that Our Customers & We Use:

- Piotr Cofta's Work
  - Trust-O-Meter

- ISECOM

Piotr Cofta's Work

See TROOPERS Workshop ;-)



ISECOM


ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES
Vendor Security
Checklist

ISECOM Trust Properties

Their Earlier Model

http://dl.packetstormsecurity.net/papers/presentations/Mastering_Trust_Sampler.pdf

See also:

http://www.insinuator.net/2011/10/broken-trust-part-2-applying-the-approach-to-dropbox/

- Size
- Symmetry
- Transparency
- Consistency
- Integrity
- Value of Reward
- Components
  - Number of elements which currently provide resources which the subject relies on.
- Porosity
  - Amount of separation between the subject and the external environment.

Where Do We Trust?

- Network Level
  - MPLS
- OS Level
  - Microsoft
- Online Storage
- Cloud
  - Dropbox
- Cloud
  - Amazon Web Services
- Corporate
  - Office365
  - Salesforce
- Search
  - Google
- Outsourcing
- PKI Services
- Smartphones / BlackBerry
- Crypto Algorithms

Trust Properties

- Those must be carefully re-evaluated.
- In particular as for (in ancient ISECOM terminology)
  - Components
  - Porosity

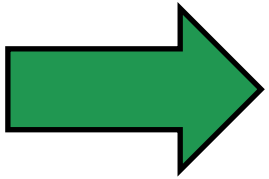
Re-Evaluating Trust Factors of $SERVICE

Some Samples

Risk

Risk

- **Risk: threat "viewed by some dimensions"**
  - How likely is it going to happen? [*Likelihood*]
  - Are we susceptible if it happens? [*Vulnerability (Factor)*]
  - What harm is caused in case it hits us? [*Impact*]



- **Talking about *threats* does not make too much sense**
  - At least not when it's about conclusions & actions…

Listing Threats

Simple Question Here

- Did you have the above stuff in your threat catalogue?
  - Does it matter?

Old Wisdom

Maybe the NSA should have considered this one as well ;-)))

ENISA

Cloud Computing Risk Assessment

November 2009 (!)

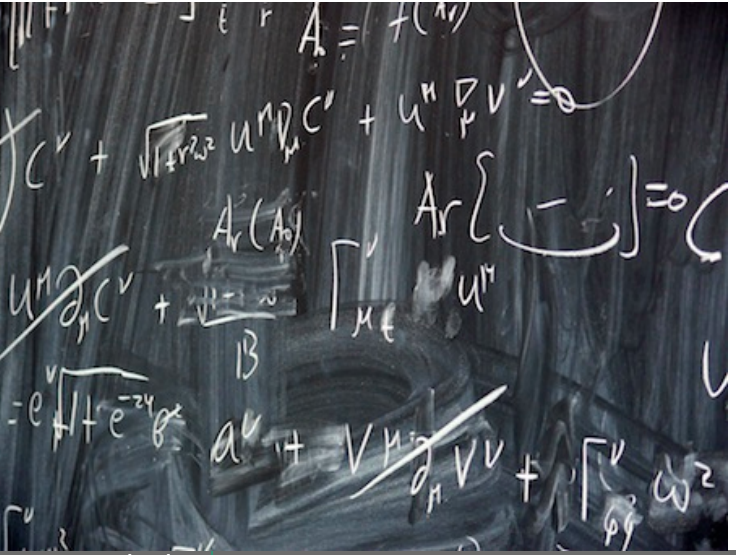
http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES

Probability	MEDIUM (Lower than traditional)	Comparative: Lower
Impac	VERY HIGH (Higher than traditional)	Comparative: Higher (aggregate) Comparative: Same (for a single customer)
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V1. AAA vulnerabilities V39. System or OS vulnerabilities V37. Inadequate physical security procedures V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	HIGH	

Do the Risk Factors of $THREAT Change in the Light of the Revelations?

Sure they do...



- Keep in mind, any NSA-induced vulnerabilities (e.g. weakened PNRGs) may be exploited by other parties as well.
  - There's some excellent math schools in Moscow. And I hear the Chinese have a few good mathematicians, too.

- The whole stuff will impact your threats/ vulnerabilities/risks model.
- New threats?
  - Intelligence agencies.
  - Competitor with ally in $INTELLIGENCE_ORG.
  - $AGENCY employee driven by malevolence (or need for money).
- Keep in mind: the capacity to look at your stuff is there. You can only hope it's not (ab-) used against you.

Conclusions

Nineteen Eighty-Four

- Out there, some bad stuff is going on. Worse than the conspiracy theorists used to tell us.
- This will affect our personal lives.
- In quite some cases this will affect corporate infosec space as well.
  - Think about it!

There's never enough time...

THANK YOU…

...for yours!

There are few things to know about TROOPERS:

ERNW
providing security.

DATE: March, 17-21. 2014
PLACE: Heidelberg, Germany
MISSION: Make the world a safer place.

REGISTRATION OPEN: www.troopers.de

ERNW providing security.

The Archive

Jeff Gough at TROOPERS13

- Feel the spirit – TROOPERS13 Teaser: https://www.youtube.com/watch?v=lfBo48r-Qho
- TROOPERS13 Talks:
  - Videos: http://www.youtube.com/playlist?list=PL1eoQr97VfJl1LdMzyQPz71uR6bwiUGog
  - Slides: https://www.troopers.de/archives/index.html
- We hope to see you in 2014!