The IT of another Europe
Building systems we can trust again

Arjen Kamphuis, lead advisor Brunel information security
Sept 10th 2016, Novi Sad
My First Cavity Search

Helping your child understand why he may pose a threat to National Security

Ages 6 and up
Cyber Attack

Data Breach
“I’m right there in the room, and no one even acknowledges me.”
EU policy 2000-2013

EU & Euro nations have known about Echelon since 2000

Euro nations have known about effective counter-measures since at least July 2001

Despite formal repeated requests from parliaments none of these measures have been implemented

Government is, at best, completely incompetent, at worst your enemy
Mein Vater sagt, Sie können in meinen Computer gucken

Das ist nicht dein Vater
Ex-BND-General: NSA wanted to pursue economic espionage

A former BND department chief has confirmed that the NSA wanted to scour the abgefischten in the operation elkonal data for keywords like "EADS" or "Eurocopter". Killer drones could be fed by "lucky strike".

Dieter Urmann, formerly Head of Technical education at the Federal Intelligence Service (BND) has, for the first time publicly admitted that the NSA a Frankfurt hub of Deutsche Telekom not only because of spying to combat terrorism and weapons proliferation. The retired Brigadier General confirmed on Thursday in NSA investigative committee of the Bundestag a report, after which it the US intelligence cooperation project in the elkonal was after about on "EADS", "Eurocopter" and "French authorities".

This was noticed from a list of "selectors", which tried to foist the BND the foreign partner, led the 63-year-old during his questioning of witnesses from. Generally I'm a project of this size, "every day something else, not just one of those things". In principle, however, was determined from the outset that "not German citizens or
WikiLeaks published documents from the National Security Agency showing details of economic espionage against France by the ‘Five Eyes’ alliance, which consists of the United States, Great Britain, Canada, Australia and New Zealand.

One document is an “information need” spying order that was first created in 2002. It shows that the alliance sought information on economic relations with the United States, French business practices, relations with least developed countries and transitional states, foreign contracts, French trade, French views, views on G8/G20 developments/issues, budgetary constraints/contributions to NATO, and “questionable

Graphic created by WikiLeaks for release of documents showing French economic espionage
For the NSA, espionage was a means to strengthen the US position in climate negotiations

At the Copenhagen Climate Summit in 2009, the world's nations were supposed to reach an agreement that would protect future generations against catastrophic climate change. But not everyone was playing by the rules. A leaked document now reveals that the US employed the NSA, its signals intelligence agency, to intercept information about other countries' views on the climate negotiations before and during the summit. According to observers, the spying may have contributed to the Americans getting their way in the negotiations.
The NSA's Porn-Surveillance Program: Not Safe for Democracy

Its targets extend beyond suspected terrorists—and some rhetoric that the First Amendment would protect is singled out.

CONOR FRIEDERSDORF | NOV 27 2013, 4:04 PM ET
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN

YEAH! AND EVEN THE FOOD IS FREE

FACEBOOK AND YOU
If you're not paying for it, you're not the customer. You're the product being sold.
There is no cloud, only other people's computers
NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations
Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms
- Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

EDS
AT&T
Qwest
H-P
Motorola
CISCO
Intel
IBM
Oracle
Microsoft
Qualcomm
Verizon
Recent Intel x86 processors implement a secret, powerful control mechanism that runs on a separate chip that no one is allowed to audit or examine. When these are eventually compromised, they’ll expose all affected systems to nearly unkillable, undetectable rootkit attacks. I’ve made it my mission to open up this system and make free, open replacements, before it’s too late.

The Intel Management Engine (ME) is a subsystem composed of a special 32-bit ARC microprocessor that’s physically located inside the chipset. It is an extra general purpose computer running a firmware blob that is sold as a management system for big enterprise deployments.

When you purchase your system with a mainboard and Intel x86 CPU, you are also buying this hardware add-on: an extra computer that controls the main CPU. This extra computer runs completely out-of-band with the main
An internal document issued by IT experts working for the German federal government warned national agencies and companies not to use Windows 8. The reason? An alleged backdoor exploit has been discovered, and the details were obtained and published by German site Zeit Online. The leaked message suggests that the NSA likely has access to a hidden feature which apparently can’t be shut off and allows Microsoft to remotely
Do you think this is a fucking game?

It rubs the Windows on its skin or else it gets the hose again.

You exist because we allow it, and you will upgrade because we demand it. Embrace the inevitable.
The DoJ is currently trying to force Apple to decrypt data stored on a defendant's iPhone, and Apple, to its great credit, is fighting back, arguing that on the one hand, it doesn't have the technical capability to do so; and on the other, should not be required to do so.

A new filing from the DoJ attacks this second point in a novel and far-reaching way. The Justice Department lawyers argue that because Apple can't decrypt the data, it must mean that it's not durable and therefore is not eligible for protection under copyright law, which grants creators exclusive rights to their work. If the data can't be decrypted, they claim, it can't be protected by copyright, and thus the encryption must be removed.
OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009. The attack started by infecting five carefully selected organizations.

- 23.06.2009: Foolad Technic International Engineering Co, ICS vendor
- 07.07.2009: Neda Industrial Group, component supplier
- 23.03.2010: Control-Gostar Jahed Company, ICS vendor
- 26.04.2010: Kala Electric, Centrifuge developer
- 11.05.2010
- 13.05.2010

GLOBAL EPIDEMIC
Tailored Access Operations

- TAO
- SSG
- TAO / R&T

OVERALL CLASSIFICATION: TOP SECRET//COMINT//REL to USA,FVEY
COTTONMOUTH-I
ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" reprogrammability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.
TIN FOIL
FREE YOUR MIND
W88 Warhead for Trident D-5 Ballistic Missile

1. The "Primary"
   Two-point, hollow-pit, fusion-boosted high explosive implosion

2. The "Secondary"
   Spherical, all-fissile, fusion-boosted radiation implosion

3. Radiation Case
   Peanut-shaped, channels x-rays from primary to secondary

4. Channel Filler
   Plastic foam plasma generator

5. Booster Gas Cannister
   Periodic replacement as tritium gas decays

- High Explosive Lens
  Two lenses drive primary implosion

- Plutonium-239 Pit
  Beryllium-reflected hollow pit

- Tritium & Deuterium
  Booster gas, fusion makes neutrons

- Lithium-6 Deuteride
  Lithium becomes tritium, fusion makes neutrons

- Uranium-235 "Sparkplug"
  Starts tritium generation and fusion in the secondary

- Uranium-235 "Pusher"
  Heat shield, tamper, and fission fuel (fission by all neutrons)

- Uranium-238 Case
  Fission by fusion neutrons only
Shadow Brokers: NSA Exploits of the Week

When your boy Serge is in charge of Cyber Attribution #DNCHack #InfoSec cc @Trevornoahpic.twitter.com/88prA2AjD5

— @msuiche

Today an unknown group called Shadow Brokers started an auction after claiming they hacked Equation Group (NSA entity named like that by Kaspersky, and believed to be the author of Stuxnet & Flame) here:
https://theshadowbrokers.tumblr.com/

Update: The Tumblr got taken down on 15 August (PST)
Deep rift between EU and US on privacy concerns continues to eat at profits of Yahoo, others...

4 August 2017 | Technology

Yahoo is investigating claims the hacker linked to "mega-breaches" at MySpace and LinkedIn has posted details of 200 million Yahoo accounts to a marketplace on the dark web. EU call for mandatory audit by Brunel experts.

"In total at least 1.3 billion online accounts have now breached, Brunel needs to be brought in to get this snafu under control", according to researcher Troy Hunt.
Security-centric IT-architecture
(network, hardware, hosting, OS, middleware, applications, processes & strategy)

Measures on securing IT-legacy
The Internetz
Coreboot + Tails
Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

— Edward Snowden —
Information Security for Journalists

By Silkie Carlo and Arjen Kamphuis

Download the book in PDF, ePub, MOBI, or view it online. For SHA-256 hashes for verifying the book, see the table below.

This handbook is a very important practical tool for journalists in understanding the importance of protecting their communications with sources, and subject to analysis and action. As this surveilling happens without scrutiny, transparency or any realistic form of accountability, the notion of the public’s right to know stories and our professional work itself is under threat.

Journalists were dismayed by the realisation that virtually every electronic communication we make is now being recorded; for them and their sources that trust them with the sensitive information that forms their work. This danger does not just worry reporters but also publishers and journalists whose personal information and whose privacy is considered fundamen
tal. Lawyers and accountants and their clients are now aware of the threat of secret surveillance of an increasingly authoritarian state.

After knowing how Snowden’s disclosures were secured, journalists looked for counter measures available. The CIJ’s latest handbook provides means of keeping your work private and safe from the prying eyes of the state. It explains how to safely receive, store and send information, and what you need to know, to have or to share. To ensure your privacy, it gives you the tools you need to help you to make your communications indecipherable to anyone else.

When planning work that must remain private and confidential, journalists and their sources will be associated with it. Shop floor maintenance, for example, is an area where the precautions and methods described in this book are invaluable. In these cases a phone call made at random to a source is not always enough. You must ensure that your communications are fully encrypted to prevent interception.

Protecting your story, your source and yourself online

By Silkie Carlo and Arjen Kamphuis

hQEMAxQ6GHdT/9WoAQf+PnS6MEmCisHF1QMrbD+tTPq4j4DI
OjI2erUIZfsNGBn526g5jwPoq2rFdku2bR1dePIYdgrZyXAn++kVQw
b2X9qaK8o4YTSWenE0fhBgWrvXmauXoKC9apkjt8gtNfCZC2V3N
zPzp/PyDK+9tUGXtp6lfjeelG1GbUuhHsBxwFOqLyrkvwR5HVS7eCY
icSh4C6yUfyuoLfwT/YkqZl2pZ3AScVBoGuX1sN6xUf6jC62sI0f1LH
NeLRomuA1dDj8fn2ApCdocuxDK7c815UyczjEWEBKkZWv4C1v0QMh
WE CAN BE HEROES
Call for Participation to SHA2017

SHA2017 is currently requesting proposals for participation, including content

SHA2017 is a five-day international outdoor technology and security conference in the Netherlands from the 4th till the 8th of August 2017. We are calling for participation in the form of talks, workshops, installations, volunteers, and more.

A motley bunch of around 5000 hackers, free-thinkers, philosophers, activists, geeks, scientists, artists, makers, creative minds, and others will convene from all over the world to contemplate, reflect, share, discuss, criticise, look ahead, code, build, and more.

The location is the Scoutinglandgoed in Zeewolde, 55km east of Amsterdam. SHA2017 is a non-commercial, self-organised community event; attending the event means that you are also volunteering to help us make it happen.

SHA2017 is the 8th edition with a proud lineage

Our dependence on information technology is still on an upward curve, to the point where it warrants serious discussions of the effects of its convenience and power on the resilience of our society, our fundamental rights, our democracy, the communities it is made up of, and our personal lives.

This dependence plays out from the mundane, too often facepalm-worthy levels of the Internet of Things, through our difficulties with escaping the network effects of large internet platforms, up to the geopolitical dimensions of unauthorised transparency through whistleblowing and leaks. This is why we chose this event’s theme:

Convenience & Resilience

Become a volunteer

Submit proposals for content

Help make SHA2017 become the exciting, inspiring and awesome community-driven event everyone is looking forward to. Submit your proposal now, and if you know of someone you think should be present, ask them to submit!

Submissions can be entered through the SHA2017 content submission system:
https://frab.sha2017.org/
Sometimes you need a bigger boat; discussing IT-security with @Brunel_NL customers at very secure, off-grid location.
The IT of another Europe
Building systems we can trust again

Arjen Kamphuis, lead advisor Brunel information security

a.kamphuis@brunel.net
03BC C848 7B4F 439D B137 4CC5 3A96 2BAF 7846 EC26