# Security Now! #491 - 01-20-14

# Cryptographic Backdoors

## This week on Security Now!

- Now we know why Barack was so sure it was North Korea.
- A few Sci-Fi recommendations.
- Yet another butt saved by SpinRite
- ... and separating fact from fiction about Cryptographic Backdoors.

Automata (2014)

## Security News:

**Don't underestimate the NSA**

- David Sanger / New York Times
- http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

  WASHINGTON — The trail that led American officials to blame North Korea for the destructive cyberattack on Sony Pictures Entertainment in November winds back to 2010, when the National Security Agency scrambled to break into the computer systems of a country considered one of the most impenetrable targets on earth.

  Spurred by growing concern about North Korea's maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations and a newly disclosed N.S.A. document.

  A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track the internal workings of many of the computers and networks used by the North's hackers, a force that South Korea's military recently said numbers roughly 6,000 people. Most are commanded by the country's main intelligence service, called the Reconnaissance General Bureau, and Bureau 121, its secretive hacking unit, with a large outpost in China.

  The evidence gathered by the "early warning radar" of software painstakingly hidden to monitor North Korea's activities proved critical in persuading President Obama to accuse the government of Kim Jong-un of ordering the Sony attack, according to the officials and experts, who spoke on the condition of anonymity about the classified N.S.A. operation.

- http://bit.ly/sn-491
  - http://bit.ly/sn-491/media/media-35679.pdf
- "Is there ''fifth-party' collection" -- > << see 3-page PDF >>

## SciFi

- SyFy: "12 Monkeys" ---> WOW!!!
- "The Signal" // weird
- "Automata" // haunting
  - http://www.imdb.com/title/tt1971325/ (6.1/10)
  - Antonio Banderas, Dylan McDermott, Melanie Griffith
  - <quote> Jacq Vaucan is an insurance agent of ROC robotics corporation who investigates cases of robots violating their primary protocols against altering themselves. What he discovers will have profound consequences for the future of humanity.
  - $4 on Amazon Instant Video.

## SpinRite:

Date: Tue, 16 Dec 2014 09:00:34 -0800
From: Jarred Sutherland
Subject: Whew!/SpinRite Success Story

Steve,

I have been listening to Security Now! for several years now and have been a fan of your site and research well before that time. I finally had a need for SpinRite for a friend who's Seagate drive which contained very important data went completely belly up. Now, this made me panic for a very specific reason ... I configured backups for this system but missed a poorly placed directory (online backup over a slower connection, so I was selective with folders chosen). So I was able to restore most of the data I needed from the backup, but not this particular crucial chunk .. I was sunk! Or so I thought! A combination of SpinRite on level 2 and a bit of fridge time, allowed me to mount this drive on my Macbook and pull the data off just in time. SpinRite saved my bacon!

What a fantastic piece of software you have here, I will pass along my recommendation to any and all who end up in a position like me... or who don't want to by keeping a good eye on their drive.

Thank you!!!

Jarred Sutherland

---

# Cryptographic Backdoors

- In computing, a "backdoor" is a method of bypassing the normal method of authentication.
- A cryptographic backdoor is a secret (initially) known only to the algorithm's designers or implementors.
    - And, being a "backdoor", the knowledge of that secret allows some aspects of the difficulty of decrypting the encrypted content to be bypassed, thus substantially weakening the algorithm's guarantee or promise of security.
- The DUAL_EC_DRBG is a classic example of what might have been a deliberately designed-in backdoor.
    - The presumption being that some undetected non-randomness in the presumably random number generation would allow "those who know the secret" to decrypt.

**But what's more interesting, and let's talk about,**
**a Law Enforcement Cryptographic FRONTdoor.**