Some Stuxnet Related Comments [excerpted from a longer presentation]

Joe St Sauver, Ph.D.

joe@uoregon.edu

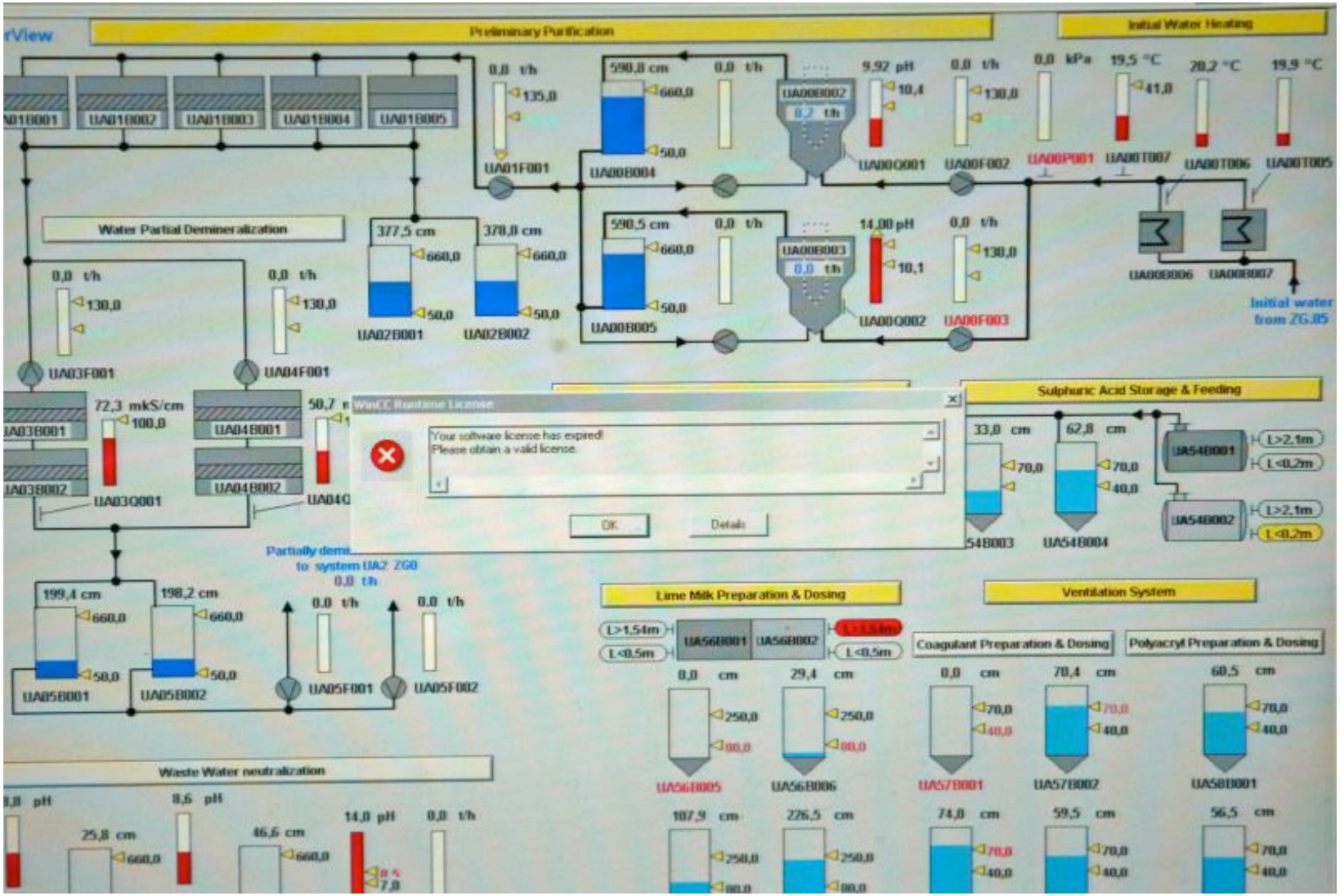
http://pages.uoregon.edu/joe/stuxnet-excerpt

Stuxnet: A Quick Overview

- June 2010: A sophisticated computer worm targeting Siemens WinCC industrial control system software is discovered. It exploits multiple 0day vulnerabilities, and surmounts “air gaps” using infected USB thumb drives.
- It exploits default (unchangeable?) passwords to spread.
- The malware is narrowly targeted against high speed variable-frequency programmable logic motor controllers from just two vendors: Vacon (Finland) and Fararo Paya (Iran), and then only when the controllers are running at 807Hz to 1210Hz. That’s an unusual frequency range.
- If a motor controller running in those frequencies is found, the malware makes the frequency of those controllers vary from 1410Hz to 2Hz to 1064Hz.
- See http://en.wikipedia.org/wiki/Stuxnet

But Why?

- Why would anyone release malware to do this strange thing? (The generally accepted wisdom is that most malware is released to further monetary aims, e.g., typically malware creates bots to use for spamming, pay-per-click click fraud, DDoS extortion schemes, etc.)
- Why would the malware select *those* particular odd frequencies (instead of just setting the frequency to be as high as it could go, or locking it as low as it could go, instead), and *JUST* those particular odd frequencies?
- There was a lot of speculation that this malware was targeting Iran's nuclear facilities, in part because of one image that was circulated, allegedly showing the Iranian Bushehr nuclear facility running Siemens WinCC (the product Stuxnet targeted), with an expired license.
- That image looks like…



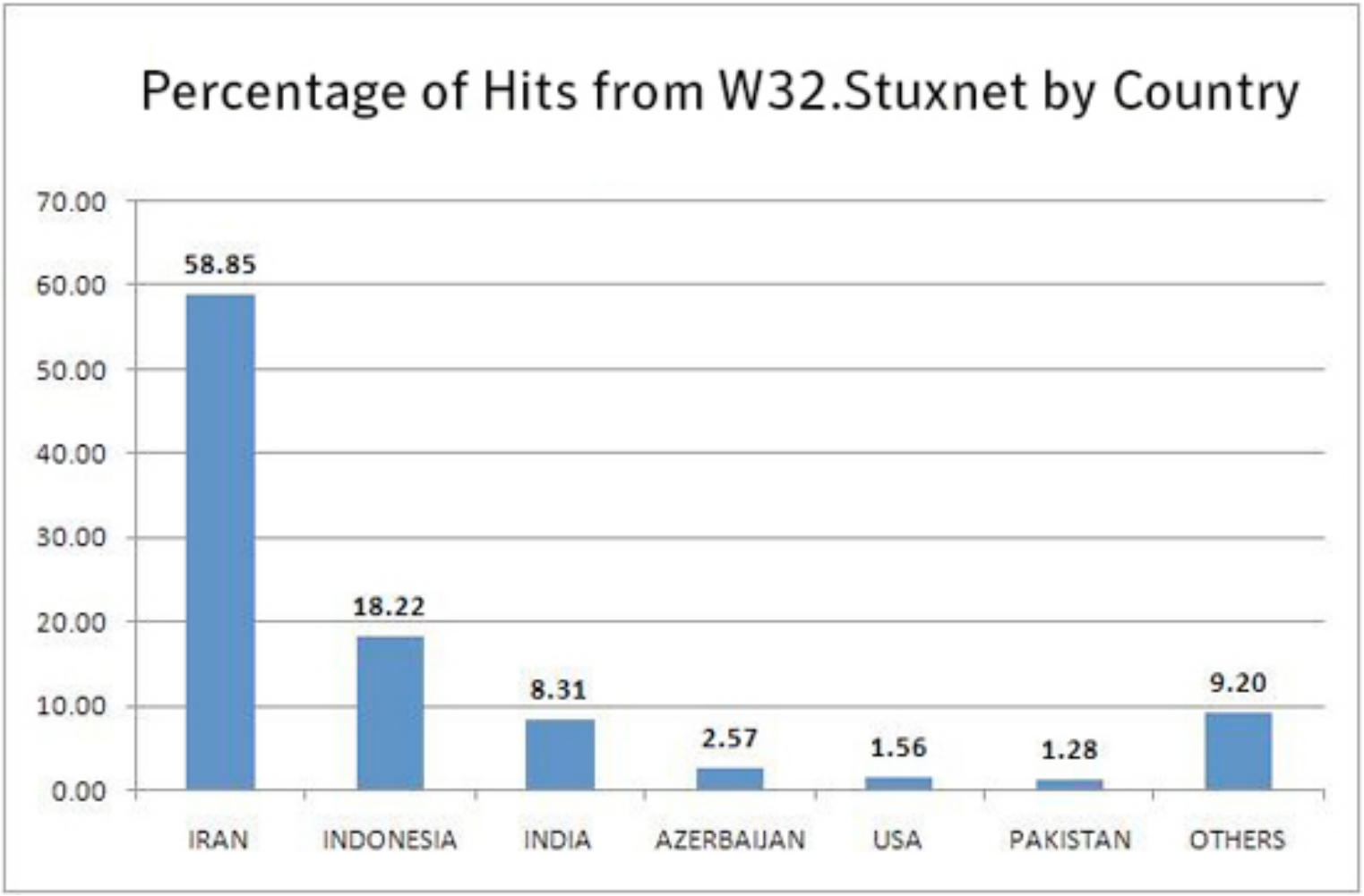
Slight problem: that's a picture of a water treatment plant. See the discussion at http://www.hackerfactor.com/blog/index.php?/archives/396-No-Nukes.html

Nonetheless…

- While I *don't* think that worm targeted the Iranian Bushehr Nuclear Power Plant, I *do* think it was likely targeting Iran's nuclear program, particularly the Iranian Natanz centrifuge facility.

- Let me explain…

Stuxnet *Was* Widely Seen In Iran



Source: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

What "Interesting" Industrial Facilities Does Iran Have?

- For example, could this worm have been targeting chemical plants, or maybe oil and gas facilities in Iran?

- Maybe, but that doesn't appear to be the likely target.

- The one thing that the international community has really been concerned about when it comes to Iran has been its industrial-scale efforts to develop nuclear weapons.

  See, for example, "Iran's Nuclear Program," http://www.nytimes.com/info/iran-nuclear-program/

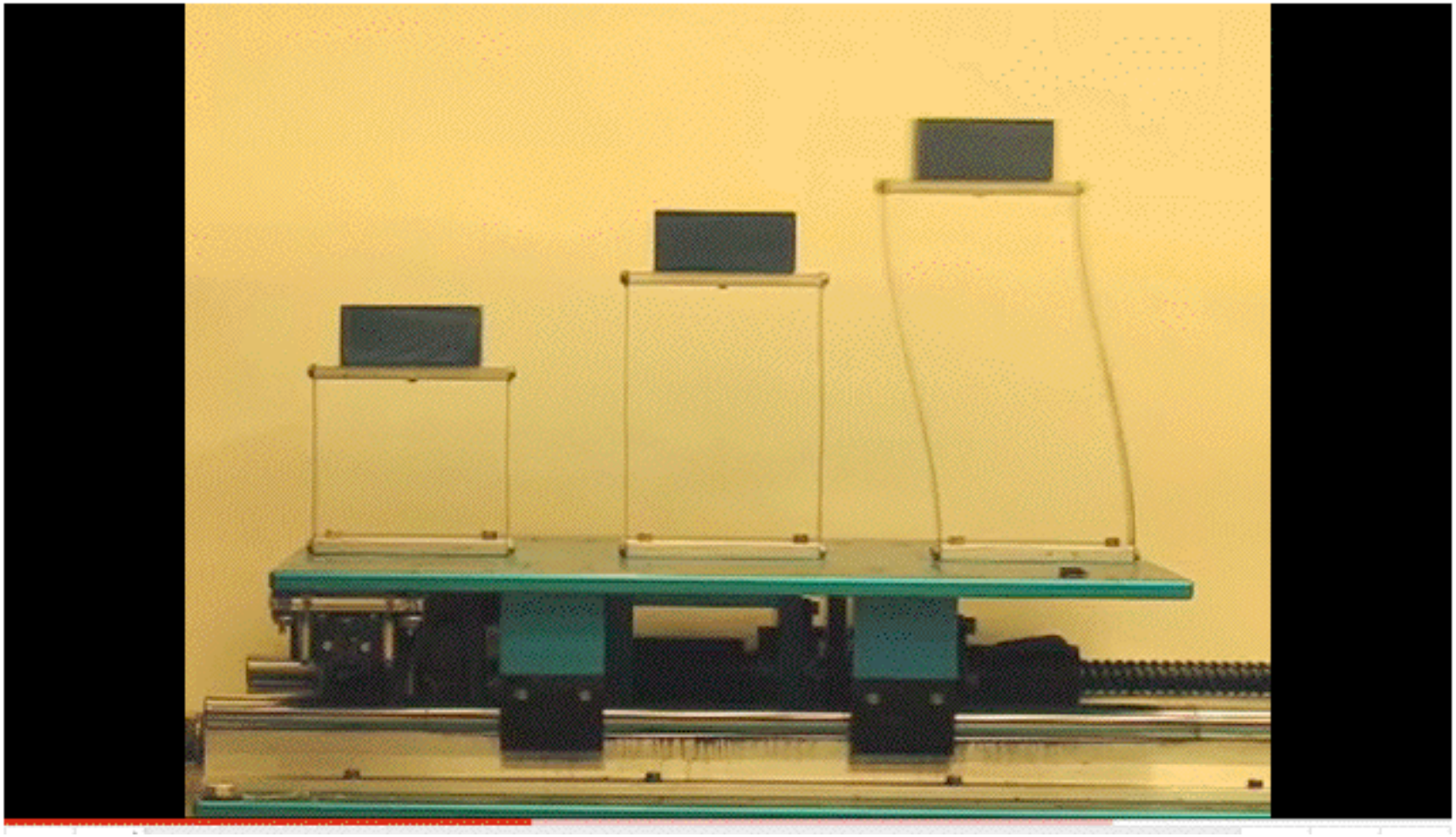
Uranium Enrichment

- It is widely known that fission weapons require special nuclear material, usually either U-235 or Pu-239, or both.
- While Pu-239 is produced as a natural by-product of nuclear reactor operation, and can be chemically separated from other elements in spent reactor fuel, U-235 is obtained by mechanically separating (rare) U-235 atoms from (far more common) U-238 atoms.
- During the middle of the last century, the United States separated uranium via gaseous diffusion at the Y-12 plant at Oak Ridge, however that was a hugely energy intensive and complex industrial process.
- An alternative uranium enrichment process involves the use of cascades of thousands of high speed centrifuges.
- A nice semi-technical overview of this process is at http://www.globalsecurity.org/wmd/intro/u-centrifuge.htm

Centrifuge Technology

- Separation efficiency is critically dependent on a number of factors, including the the centrifuges' speed of rotation
- Less efficient? You need more centrifuges (or more patience) to meet a given U-235 output target.
- Impatient? You can try using highly efficient advanced centrifuge designs running at high peripheral speeds. (Separation is theoretically proportional to the peripheral speed raised to the 4^{th} power, so obviously any increase in peripheral speed is potentially extremely helpful).
- That implies you need strong tubes, but brute strength isn't enough: centrifuge designs also run into problems with "shaking" as they pass through naturally resonant frequencies (and "shaking" at high speed can cause catastrophic failures to occur). See the discussion at www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/engineering.html

Conceptually Understanding “Shaking”



Video: http://www.youtube.com/watch?v=LV_UuzEznHs

Some Notes About That Video

- The natural resonant frequency for a given element is not always the “highest” speed – the “magic” frequency is dependent on a variety of factors including the length of the vibrating element and the stiffness of its material.
- While the tallest (rightmost) model exhibited resonant vibration first, the magnitude of its vibration didn’t necessarily continue to increase as the frequency was dialed up further – there was a particular value at which the vibration induced in each of the models was at its most extreme.
- Speculation: could the frequency values used by Stuxnet have been (somehow) selected to ***particularly target*** a specific family (or families) of Iranian centrifuges?
- The Iranians have admitted that *something* happened as a result of the malware that they saw…

Stuxnet and Centrifuge Problems

http://af.reuters.com/article/energyOilNews/idAFLDE6AS1L120101129?sp=true

UPDATE 2-Iran says cyber foes caused centrifuge problems

Mon Nov 29, 2010 3:06pm GMT

Print | Single Page [-] Text [+]

* Iran says for first time that cyberbug caused problems

* Ahmadinejad says experts found out enemies of Iran

* Those enemies unable to create problems any more, he says

(Adds details, background)

TEHRAN, Nov 29 (Reuters) - Enemies of Iran used computer code to make "limited" problems for centrifuges involved in uranium enrichment at some of its nuclear sites, President Mahmoud Ahmadinejad said on Monday.

"They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts," he told reporters at a media conference, the first time Iran has said a cyberbug affected its centrifuges.

"They did a bad thing. Fortunately our experts discovered that and today they are not able (to do that) anymore," he said.

Iran temporarily halted most of its uranium enrichment work earlier this month, a U.N. nuclear watchdog report said last week, a few days after former IAEA chief Olli Heinonen said the Islamic Republic had had problems with the equipment used in the programme for years and computer virus Stuxnet may be a factor.

Achieving A Persistent Impact

- But why would the author or authors of the Stuxnet malware want to make the centrifuges shake destructively? Wasn't infecting their systems disruptive enough in and of itself? No.
- If you only cause problems solely in the cyber sphere, it is, at least conceptually, possible to "wipe and reload" (e.g., cleanup and restore from backups), thereby fixing both the infected control systems and the modified programmable motor controllers at the targeted facility. Software-only cyber-only impacts are seldom "long term" or "persistent" in nature.
- However, if the cyber attack is able to cause ***physical damage***, such as causing thousands of centrifuges to shake themselves to pieces, or a generator to self destruct, that would take far longer to remediate.

A DHS Video Released Via CNN in 2007

See: http://www.youtube.com/watch?v=fJyWngDco3g

Another Key Point: Avoiding Blowback

- Why would a nation-state adversary release such a **narrowly targeted** piece of malware?
- Any use of malware for offensive purposes runs the risk of "blowback," a term borrowed from chemical warfare, where an unexpected change in wind patterns can send an airborne chemical weapon drifting away from its intended enemy target and back toward friendly troops.
- This can be seen in things like Stuxnet: while most of the Stuxnet infections apparently took place in Iran, some did happen in other countries, including the U.S.
- Prudent "cyber warriors" might take all prudent possible steps to insure that if Stuxnet did "get away from them," it wouldn't wreck havoc on friendly or neutral targets.
- So now you (may) know why Stuxnet appears to have been so narrowly tailored…

Talking More About Cyber Warfare

- I don't want to get ratholed for *too* long talking about just Stuxnet and its potential use as a weapon of cyber warfare.

- If you're interested in reading more about cyber warfare in particular, you may want to see the talk I did for some folks in North Dakota, entitled,

  "Cyber War, Cyber Terrorism and Cyber Espionage,"
  http://pages.uoregon.edu/joe/cyberwar/cyberwar.ppt
  (or .pdf)