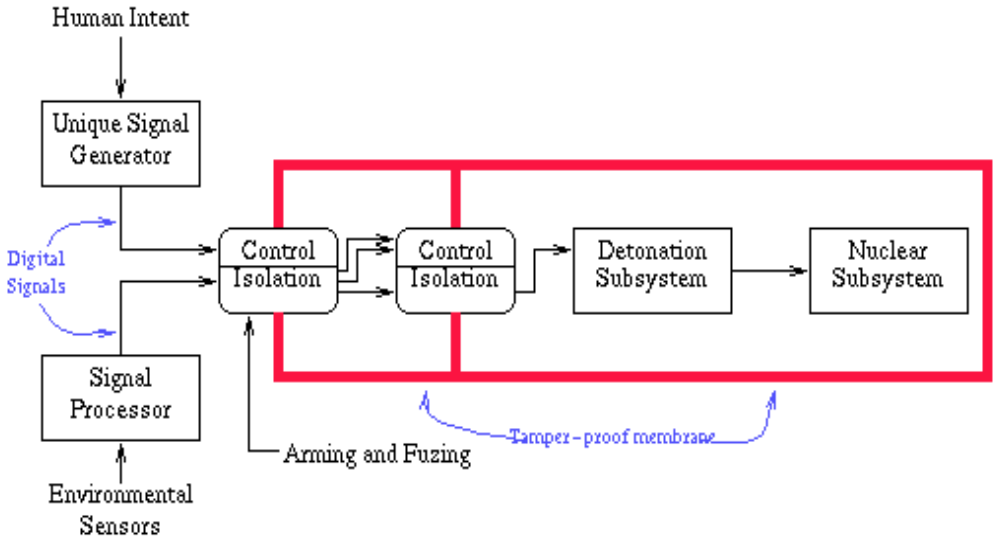
Security Now! #433 - 12-04-13

BULLRUN: Breaking SSL

Security News:

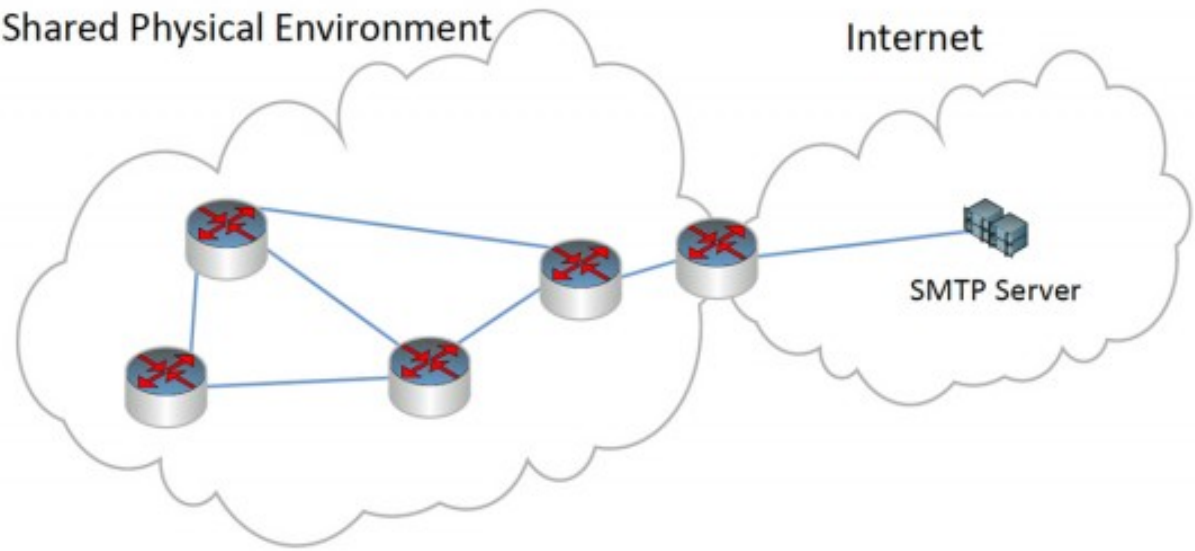
The Launch Code was: 00000000

- Website: "Today I Found Out" --via-- ArsTechnica: Sean Gallagher
- http://www.todayifoundout.com/index.php/2013/11/nearly-two-decades-nuclear-launch-code-minuteman-silos-united-states-00000000/
- http://arstechnica.com/tech-policy/2013/12/launch-code-for-us-nukes-was-00000000-for-20-years/
- In 1962 JFK signed "National Security Action Memorandum 160", which was supposed to ensure that every nuclear weapon the US had, be fitted with a so-called Permissive Action Link (PAL), a device that ensured that the missile could ONLY be launched with the proper code from the right authority.
- So the PALs were supposed to prevent the use of nuclear weapons—and the nuclear weapons under joint control with NATO countries in particular—without the authorization of the president of the United States.
- The nuclear devices in the U.S. that were fitted with PALs, such as ones in the Minuteman Silos, were installed under the close scrutiny of Robert McNamara, JFK's Secretary of Defence. However, The Strategic Air Command greatly resented McNamara's presence and almost as soon as he left, the code to launch the missile's, all 50 of them, was set to 00000000.
- FASCINATING READING about "PALs":
  - https://www.cs.columbia.edu/~smb/nsam-160/pal.html
  - PALs are powered by RTG's -- radioisotope thermoelectric generators [A94]. An RTG provides for very long lifetime with little maintenance required. They work by alpha decay of plutonium-238, a non-fissile isotope. The limiting factor on the lifetime of an RTG is helium buildup.



"Scientist-developed malware covertly jumps air gaps using inaudible sound."
"Malware communicates at a distance of 65 feet using built-in mics and speakers."

- Dan Goodin / ArsTechnica - Monday Dec 2nd
- http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/



- Diagram Title: "Topology of a covert mesh network that connects air-gapped computers to the Internet."
- Fraunhofer Institute for Communication
- <quoting Dan's Report>
  Computer scientists have developed a malware prototype that uses inaudible audio signals to communicate, a capability that allows the malware to covertly transmit keystrokes and other sensitive data even when infected machines have no network connection.

  The proof-of-concept software—or malicious trojans that adopt the same high-frequency communication methods—could prove especially adept in penetrating highly sensitive environments that routinely place an "air gap" between computers and the outside world. Using nothing more than the built-in microphones and speakers of standard computers, the researchers were able to transmit passwords and other small amounts of data from distances of almost 65 feet. The software can transfer data at much greater distances by employing an acoustical mesh network made up of attacker-controlled devices that repeat the audio signals.

- 20 baud - 65 feet - two Lenovo Laptops.

"Portable Car Killer"

- "Radio-beam device can disable car and boat engines from 50m (165 ft)"
- http://www.theengineer.co.uk/military-and-defence/news/radio-beam-device-can-disable-car-and-boat-engines-from-50m/1017308.article
- courtesy: Simon Zerafa (@SimonZerafa)
- "RF Safe-Stop": E2V has developed a non-lethal device that can disable the engines of motor vehicles and small boats at a distance of up to 50m in under three seconds.
- 350kg (772 pounds) - Nissan Nevara and Toyota Land Cruisers

- Frequencies in the L and S-Band - the wiring loom of, say a metre…is almost the perfect antenna.
- << discuss sheet metal / high-tech == higher vulnerability, security, etc. >>

Paul Thurrott (@thurrott)

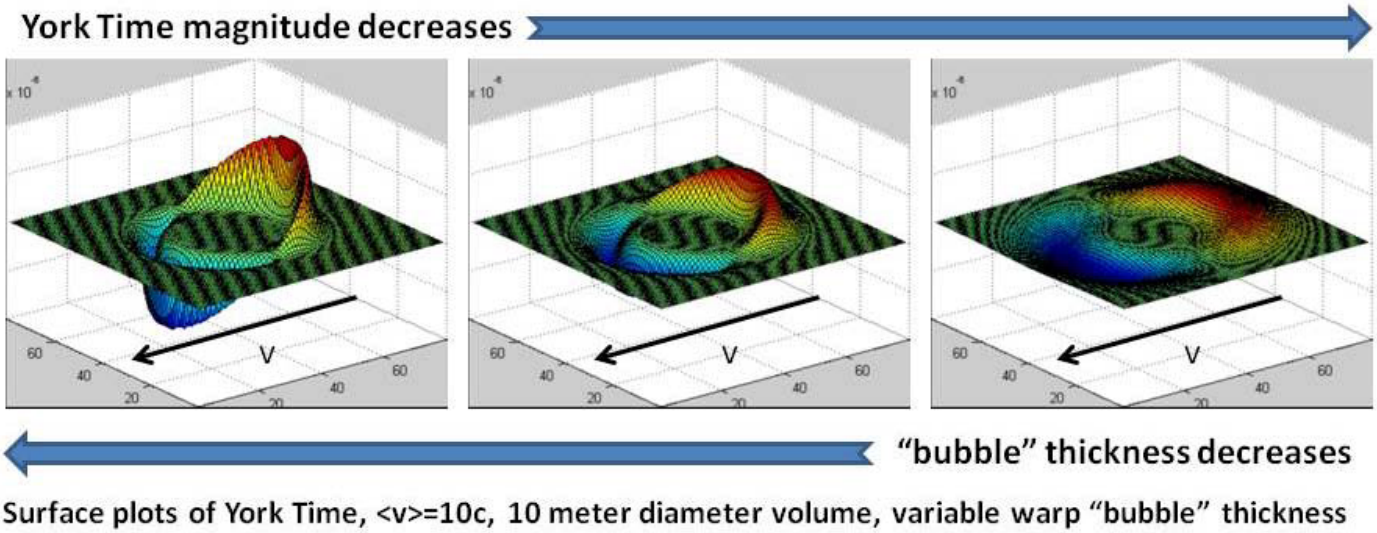
- Tweet: “The sheer amount of free PR that Amazon CEO Jeff Bezos got for his BS "drone delivery system" is awe-inspiring. Media, you just got played.”

"How NASA might build its very first warp drive"

- http://io9.com/5963263/how-nasa-will-build-its-very-first-warp-drive
  - Article begins: "A few months ago, physicist Harold White stunned the aeronautics world when he announced that he and his team at NASA ***had begun work*** on the development of a faster-than-light warp drive. His proposed design, an ingenious re-imagining of an Alcubierre Drive, may eventually result in an engine that can transport a spacecraft to the nearest star in a matter of weeks — and all without violating Einstein's law of relativity."

- Miguel Alcubierre (~50 Mexican theoretical physicist)
  - May 1994 Paper published in the Classical & Quantum Gravity journal.
  - Wikipedia: Alcubierre is best known for the proposal of "The Warp Drive: Hyper-fast travel within general relativity" which appeared in the science journal Classical and Quantum Gravity. In this, he describes the Alcubierre drive, a theoretical means of traveling faster than light that does not violate the physical principle that nothing can locally travel faster than light. In this paper, he constructed a model that might transport a volume of flat space inside a "bubble" of curved space. This bubble, named as Hyper-relativistic local-dynamic space, is driven forward by a local expansion of space-time behind it, and an opposite contraction in front of it, so that theoretically a spaceship would be placed in motion by forces generated in the change made by space-time.

- http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110015936_2011016932.pdf
  - Warp Field Mechanics 101, Dr. Harold "Sonny" White, NASA Johnson Space Center
  - White speculates that such a drive could result in "speeds" that could take a spacecraft to Alpha Centauri in a mere two weeks — even though the system is 4.3 light-years away.



Surface plots of York Time, <v>=10c, 10 meter diameter volume, variable warp "bubble" thickness

"It takes advantage of a quirk in the cosmological code that allows for the expansion and contraction of space-time, and could allow for hyper-fast travel between interstellar destinations. Essentially, the empty space behind a starship would be made to expand rapidly, pushing the craft in a forward direction — passengers would perceive it as movement ***despite the complete lack of acceleration***.

In terms of the engine's mechanics, a spheroid object would be placed between two regions of space-time (one expanding and one contracting). A "warp bubble" would then be generated that moves space-time *around* the object, effectively repositioning it — the end result being faster-than-light travel without the spheroid (or spacecraft) having to move with respect to its local frame of reference.

The trouble is energy: Space-Time is VERY STIFF and doesn't want to be warped.

The breakthrough occurred a year ago when White was preparing for a talk. He was assembling slides and realized how the power requirements might be dramatically reduced.

Miscellany:

bit.ly/sggrc is filtered

- Simon Paarlberg (@blamh)

What to do with an older, unused iDevice?

- A hot deal on a terrific 30-pin (pre-lightening) stand
- iLuv iMM190 App Station Alarm Clock Stereo Speaker Dock for iPod and iPhone (Black)
- www.amazon.com/gp/product/B0035WTCVI/
- Regularly $80, reduced to $20

Miscellany (continued)**:**

Two Kickstarter Projects:

The Temperfect Mug

- http://www.kickstarter.com/projects/deandavidv/the-temperfect-mug-coffee-and-tea-at-the-perfect-t
- vs my Contigo's: http://www.gocontigo.com/
- Concept: Pull the "too hot to drink" heat out immediately then use it it hold the coffee temperature steady.

Smartphone BTv4 LE Controlled Paper Airplane

- Just $30 - "Just the guts, Ma'am"
- Goal: $50,00 … Pledged: $434,130
- 51 days to go
- http://www.kickstarter.com/projects/393053146/powerup-30-smartphone-controlled-paper-airplane

SpinRite: Caleb Allen in Turlock, CA

Subject: Spinrite Helping Elementary School Children Read

<< see text of his eMail >>

BULLRUN

How the NSA breaks SSL

Based upon Matthew Green's Blog, Monday December 2nd:
http://blog.cryptographyengineering.com/2013/12/how-does-nsa-break-ssl.html

How does the NSA break SSL?

- Matthew's been bugged by the NSA BULLRUN briefing sheet which mentions that the NSA has been breaking quite a few encryption technologies.
    - (He's been a bit distracted, working on his "Zerocoin" project.)
- Matt starts out by explaining: "First, I'm well aware that NSA can install malware on your computer and pwn any cryptography you choose. That doesn't interest me at all, for the simple reason that it doesn't scale well. NSA can do this to you, but they can't do it for an entire population. And that's really what concerns me about the recent leaks: the possibility that NSA is breaking encryption for the purposes of mass surveillance."

Attack Vectors

Theft of RSA Keys.

- This technique is so obvious and easy that it's difficult to imagine NSA spending a lot of resources on sophisticated cryptanalytic attacks.
- We know that GCHQ and NSA are perfectly comfortable suborning even US providers overseas. And inside our borders, they've demonstrated a willingness to obtain TLS/SSL keys using subpoena powers and gag orders. If you're using an RSA connection to a major website, it may be sensible to assume the key is already known.

Suborning hardware encryption chips:

- http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
- A significant fraction of SSL traffic on the Internet is produced by hardware devices such as SSL terminators/accelerators.
- The NSA documents aren't clear on how this capability works, or if it even involves SSL.
- Matt suggests: the obvious guess is that each chip encrypts and exflitrates bits of the session key via 'random' fields such as IVs and handshake nonces. Indeed, this is relatively easy to implement on an opaque hardware device. The interesting question is how one ensures these backdoors can only be exploited by NSA -- and not by rival intelligence agencies.

Side-Channel Attacks:

- Operation time, resource consumption, cache timing, and RF emissions -- can often be used to extract secret key material.
- How do you get close enough?---> Virtualized TLS servers in a cloud setting, thus sharing hardware... the spy is on the same hardware.

Weak Random Number Generators:

- Where do we need good random numbers?
    - On the client side, during the RSA handshake:
      The RNG is used to generate the RSA pre-master secret and encryption padding. If the attacker can predict the output of this generator, it's possible to decrypt the entire session.

    - On the client or server side, during the Diffie-Hellman handshake:
      Since Diffie-Hellman requires a contribution from each side of the connection, a predictable RNG on either side renders the session completely transparent.

    - During long-term key generation, particularly of RSA keys:
      EFF Observatory --> We've already seen that many servers have been inadvertently using the same secret keys... due to poor random number generators.

Esoteric Weaknesses in PFS systems:

- Encrypted Session resumption is tricky in large server farms.
- DH parameters must be chosen with care. Bad code at either end can quickly destroy the system's security. DH is fragile in that it requires proper behavior by both ends of the handshake.

TINFOIL HAT CONCERNS (aka thought experiments):

Breaking RSA Keys:

- Matt: There's a persistent rumor in our field that NSA is cracking 1024-bit RSA keys. It's doubtful this rumor stems from any real knowledge of NSA operations. More likely it's driven by the fact that cracking 1024-bit keys is highly feasible for an organization with NSA's resources.
- Way back in 2003, Shamir and Tromer estimated $10 million for a purpose-built machine that could factor one 1024-bit key per year.
- In 2013, Tromer reduced those numbers to about $1 million, factoring in hardware advances. And it could be significantly lower.
- Large Distributed networks of PCs could be powerful too.
- Why is this 'tinfoil hat'?? Because, as far as we know, nobody's actually done it. So all we have are rough guesses. The guesses could be dramatically too high or too low. And 1024 RSA keys are now being rapidly being phased out.
- Matt writes: "Cracking 2048 bit keys would require significant mathematical advances, taking us much deeper into the tinfoil hat."

Cracking RC4:

- As we know, SSL/TLS support a large suite of cipher algorithms.
- But about 50% of all HTTPS traffic is still secured with the creaky old RC4 cipher.
- RC4 is starting to show its age: It's already vulnerable to marginally practical attacks.
- But... we don't know of any attack that would allow the NSA to usefully crack RC4! The known techniques require an attacker to collect thousands or millions of ciphertexts that are either (a) encrypted with related keys (as in WiFi's WEP) or (b) contain the same plaintext. The best known attack against SSL takes the latter form -- it requires the victim to establish billions of sessions... and even then it only recovers fixed plaintext elements like cookies or passwords.
- Matt writes: The counterargument is that the public research community hasn't been thinking very hard about RC4 for the past decade -- in part because we thought it was so broken people had stopped using it (oops!) If we'd been focusing all our attention on it (or better, the NSA's attention), who knows what we'd have today?

New Side Channel Attacks:

- Anything is possible... and crypto algorithms tends to so easily leak secret information.
- (One of the appeals for the use of Dan Bernstein's Curve25519 in SQRL was that he paid SO MUCH ATTENTION to side-channel issues. NO SECRETS control the algorithm's execution path or timing.)

True Tinfoil....

- Does the NSA have secret and completely surprising quantum computing capabilities?
- Do they have their own widely trusted and completely compromised Certificate Authority already planted in everyone's browser?

One bright spot is that the NSA/GCHQ disclosures DO describe their present capabilities as "Extremely Fragile." So that implies that the things we're already doing have significantly changed the game for them.