Secure Software Systems

CYBR 200 | Fall 2018 | University of the Pacific | Jeff Shafer

Cryptography

Let’s talk about cryptography

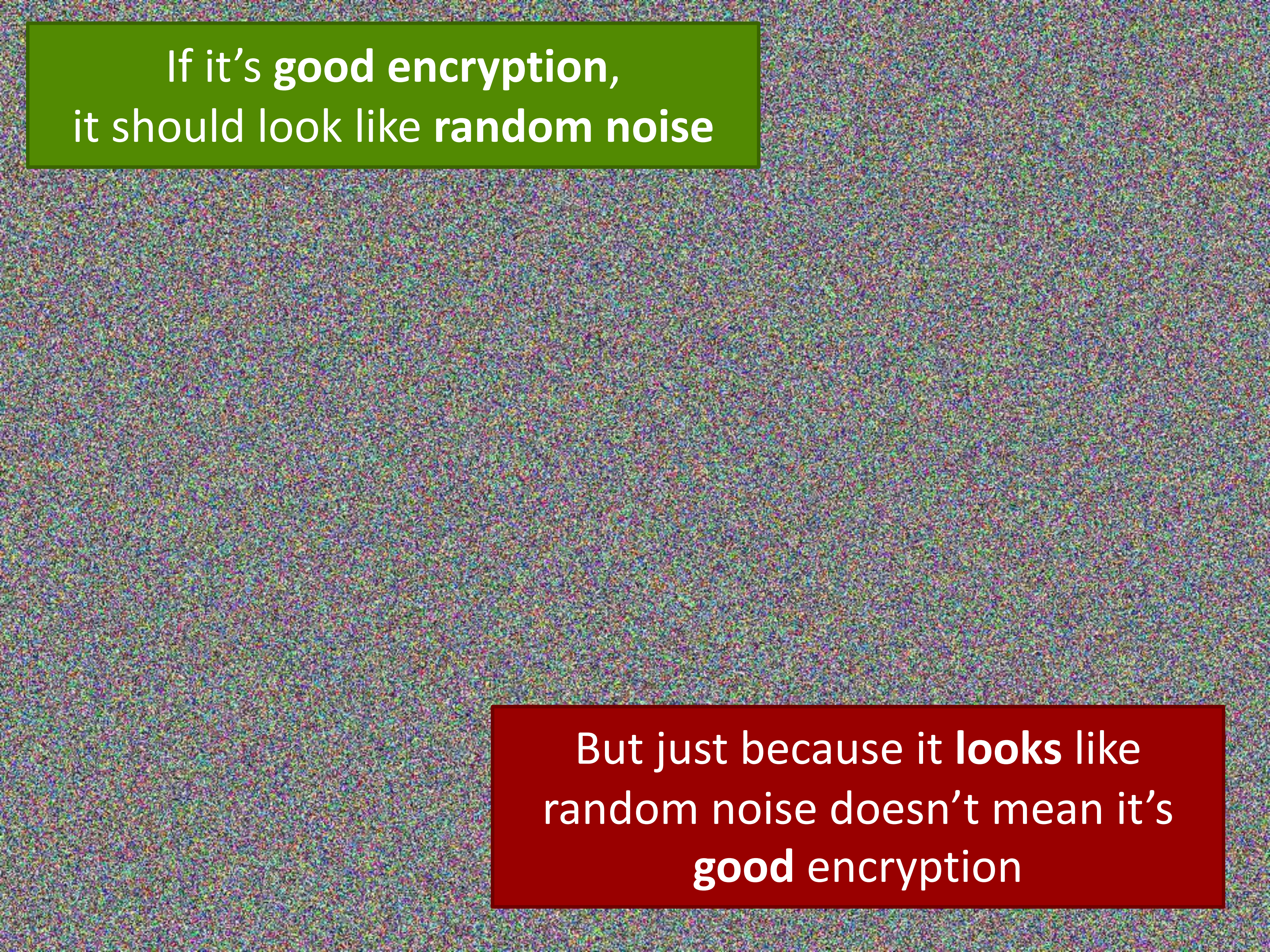
An hour ought to do it, right?

ACrJ0XSN2Jodf5/SLFJORIBGOCZD5YAAYxXLxkkatxO/Byg+Ooi
yjIXCzW4X6s7BoBGRGoMrlcVl1xrJOPidWbd6f2rmFzwXkM2F9h
AC70YJPjuDeCzB9BjKu43tDiJykpM9XdB5iE9P8n67olfdGvffs
OL6wyAw Q5ckmqfZxdGVH5RoEccn
m/rkz7k t0/NXeJDcLvS8E8tW20Z
DBoB+xV OiW4uxIzJNPXMzH3ZQxI
BkaxUfX X/9egvUrYDrDztlm7p5D
5n/QjKBRQOc7NfLhvCVk3b7GqSVprCKjjav48jR1bZqMpZaZZLs
W447y7cbPLiv GjopNV5yVs86bfV
18K+moU4Zjqz 6hZ2bcnpkbsCokt
sV9qAfTIMaW7 rLeW8jxaQARAQAB
yBWYXJlbGFzI aXN0b3MudmFyZWxh
2tlci5ncj6JAjkEEwECACMFAlSIDw0CGy8HCwkIBwMCAQYVCAIJ
QIXgAAKCRCxxfYVqPj RdZTsaBOO
qBB+NYlgJD23D9Sv9C 3CTmdPO6B
nrtT7JlTWMpomudNF9 gJWD62LZ0
vjYczDRBu3oZKPNHPmUayvlS/A/74YZwDb3HdgimfTAqmV8+Bce
ocx3UdZfscFNalS3ir7YXtqwCPdb2iB0vYJgaTwkCxtfvYyLWc2
d5dx+kthvdO8VHHaLc+o2onem/FKqeDDcA1ph0I6poBActa498g
n9JL+hZtOFNhxlEhVNV41Jjztm2/tWYTg9oIE5sX7BjqSG0HcIo

Cryptography is hard

Cryptography is hard

Cryptography is (very) hard



If it’s **good encryption**,
it should look like **random noise**

But just because it **looks** like random noise doesn’t mean it’s **good** encryption

"Trust the Math"

~ Bruce Schneier

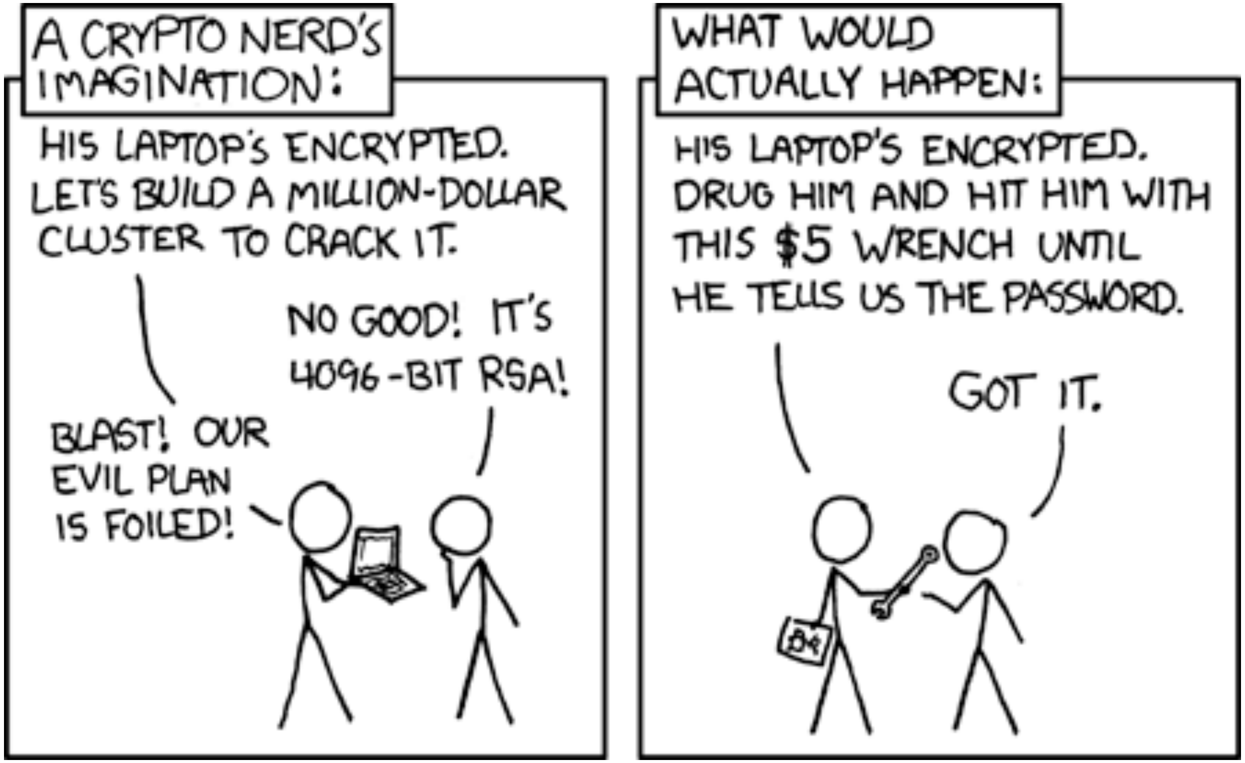
https://www.schneier.com/

Cryptography is Harder Than It Looks

- ***"Cryptography is harder than it looks"***
  - It looks like math, and we have smart mathematicians, so problem solved, right?
  - Problem: Math equations can't secure anything
    - Write equations into software
    - Embed in a larger software system
    - Manage by an OS
    - Run on hardware
    - Connect to a network
    - Configure and operate by users
  - **Commonly find vulnerabilities *not* in underlying mathematics but in the implementation**

https://www.schneier.com/blog/archives/2016/03/cryptography_is.html

Cryptography is Harder Than It Looks


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Cryptography is Harder Than It Looks

- ***"Complexity is the worst enemy of security"***
  - More lines of code
  - More interactions with other systems
  - More configuration options
  - **Result: More vulnerabilities!**

https://www.schneier.com/blog/archives/2016/03/cryptography_is.html

Great Disasters in Cryptography

Smart People Make Mistakes

Smart People Make Mistakes

- Do you believe that smart programmers can implement bugs?
  - Zero immunity from bugs just because you're working on `crypto.cpp` instead of `gui.cpp`
- Examples of cryptography implementation failures

Cryptography Failures

- Example: **RC4 Stream Ciphers (e.g., WEP) (2007)**
  - **(No CVE)**: Ability to reconstruct key from encrypted messages
  - Discovered by Fluhrer, Mantin and Shamir in 2001
    - “Weaknesses in the Key Scheduling Algorithm of RC4”
    - Research paper: http://www.crypto.com/papers/others/rc4_ksaproc.pdf
  - Applied to *aircrack* tool in 2007 – can recover WEP password in minutes, zero skill required

Cryptography Failures

- Example: **OpenSSH (2009)**
  - CVE-2008-5161: Error handling in the SSH protocol ... makes it easier for **remote attackers to recover certain plaintext data** from an **arbitrary block of ciphertext** in an SSH session
    - Attack that, with probability $2^{(-18)}$, verifiably recovers 32 bits of OpenSSH-encrypted plaintext at an attacker-selected position
  - Discovered by Albrecht, Paterson, Watson
    - "Plaintext Recovery Attacks Against SSH"
    - Research paper: http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf

Cryptography Failures

- Example: **SSL 3.0 / TLS 1.0 (2011)**
  - CVE-2011-3389: The SSL protocol … **allows man-in-the-middle attackers to obtain plaintext HTTP headers** …. via an attack on an HTTPS session in conjunction with JavaScript code
  - "BEAST" Attack - **B**rowser **E**xploit **A**gainst **S**SL/**T**LS
  - Discovered by Rizzo and Duong
    - "Here Come The ⊕ Ninjas" [XOR]
    - Research Paper: http://nerdoholic.org/uploads/dergln/beast_part2/ssl_jun21.pdf
    - Same authors also discovered "CRIME" in 2012 to hijack HTTPS sessions

Cryptography Failures

- Example: **Bitcrypt malware (2014)**
  - Encrypts your hardware, blackmails you to get decryption key
  - Authors intended to encrypt each file using a 128 byte key (1024 bits)
- Fatal flaw: File was actually encrypted with 128 digit key (426 bits)
  - Can be brute forced on standard PC in a few hours
- http://blog.cassidiancybersecurity.com/post/2014/02/Bitcrypt-broken

Cryptography Failures

- Example: **OpenSSL (2014)**
  - CVE-2014-0160 : The … TLS … implementations in OpenSSL .. do not properly handle Heartbeat Extension packets, which allows **remote attackers** to obtain **sensitive information from process memory** via crafted packets that trigger a buffer over-read, as **demonstrated by reading private keys**
  - "Heartbleed" attack - http://heartbleed.com/
  - Discovered by Neel Mehta (Google security team)

Cryptography Failures

- Example: **Apple iMessage (2016)**
  - CVE-2016-1788: Messages in Apple iOS … and watchOS … **does not properly implement a cryptographic protection mechanism**, which allows remote attackers to **read message attachments**…
  - Able to exploit remotely if either sender or receive phone are still online (“slow but silent”)
- Commentary:
  - https://blog.cryptographyengineering.com/2016/03/21/attack-of-week-apple-imessage/

Cryptography Failures

"The designers of this system aren't novices. They're an experienced team with some of the best security engineers in the field. If these guys can't get the security right, just imagine how much worse it is for smaller companies without this team's level of expertise and resources. Now imagine how much worse it would be if you added a government-mandated back door. There are more opportunities to get security wrong, and more engineering teams without the time and expertise necessary to get it right. It's not a recipe for security."

~ Bruce Schneier (2016)
In response to iMessage cryptography

https://www.schneier.com/blog/archives/2016/03/cryptography_is.html