A Different Kind of Crypto:
Crypto Algorithms Designed for Payload Obfuscation

WHOAMI

Parker Schmitt is currently working as a penetration tester and is working on some Network/Virtualization Management. He has made various contributions to Gentoo and the Gentoo-Hardened project (mostly in SELinux) and submitted some ebuilds (including Samba 4). In Gentoo he specializes in hardening layers (SELinux, PaX, GRSecurity), Virtualization, and Networking. He also loves mathematics, mathematical modeling, and is a serious crypto nerd. In the realm of security his interests include wifi attacks from drones, data exfiltration, and Linux hardening. Outside of security he loves flying airplanes and playing the piano.

WHO ELSE

Kyle Stone - @Essobi
Senior Consultant at RedLegg
Exploit development, rare exfiltration techniques, and hardware hacking. Released CVE-2013-2802 at Derbycon 3.0. He is the founding member of Louisville Organization of Locksport.

WHO ELSE

Chris Hodges - @gl11tch
Chris is a Arkansas native military reconnaissance officer, turned exploit hunter. After several tours of combat, he turned to a laptop and hasn't stopped hacking since.
http://www.exploit-db.com/exploits/18334
http://www.exploit-db.com/exploits/24526
http://www.exploit-db.com/exploits/19036
He enjoys exploit-development, tactical red team strategizing and rare exfiltration paths.

DISCLAIMER

This presentation is technical but presented at a high level for those with little to no cryptography experience.

I will be describing the problem space and identifying solutions.

It will vary from in-depth to a high-level overview.

OVERVIEW

- AV Evasion
- Crypto Vs Payload Crypto
- Automating Obfuscation

HOW DOES ANTI-VIRUS WORK?

- Signature Based Detections...
- Sandboxing...
- Dynamic Code Analysis...

WHAT ARE SIGNATURES?

```
00000000  48 31 ff b0 69 0f 05 48  31 d2 48 bb ff 2f 62 69  |H1..i..H1.H../bi|
00000010  6e 2f 73 68 48 c1 eb 08  53 48 89 e7 48 31 c0 50  |n/shH...SH..H1.P|
00000020  57 48 89 e6 b0 3b 0f 05  6a 01 5f 6a 3c 58 0f 05  |WH...;..j._j<X..|
```

SIGNATURE PITFALLS

- Code Obfuscation…
- Encrypted Payloads…
- Easily Bypassed…

WHAT IS A SANDBOX?

- Running code in a isolated manner…
- Checking it’s behavior while running…
- Malicious network behavior identification…

SANDBOX PITFALLS

- Execution/Analysis takes time…
- Can’t check all possible conditions…
- It is a run-time environment. It’s detectable…

WHAT IS DYNAMIC CODE ANALYSIS?

- Automated Reverse Engineering…
- Look for suspicious code…
- Examples: FireEye, Trustlook, Fidelis

DYNAMIC CODE ANALYSIS PITFALLS

- Encrypted Payloads…
- 2-Stage Payloads…
- It’s hard to detect ALL encryption routines..

WHAT IS A PAYLOAD?

- It’s the exploit’s counterpart…
- Post-Exploitation Run-time…
- It’s the bot in the malware…

EVASION TECHNIQUES

- Many AV products check the drive…
- Many anti-virus solutions check the network..
- It’s computationally expensive to scan RAM…
- Keep it encrypted until it’s in RAM…

WHAT IS PAYLOAD ENCRYPTION?

- Hiding your executable payload in plain sight…
- It’s decrypted when AV is not looking…

WHAT IS CRYPTOGRAPHY?

- Classical Cryptography…
  - Designed for messages written by hand..
  - Developed before automation…
- Modern Cryptography
  - Designed for electronic messages…
  - Sufficiently complex to deter automated analysis..

BASIC MODERN CRYPTO

- Confusion - No one part of the cipher text depends on one part off the key. Multiple bytes of the key affect each byte of the cipher text.
- Diffusion - Plaintext is scattered via permutation..
- Guessing plain text won’t get you the key!

PERMUTATION TABLES

- Most shared-key algorithms consist of permutations of bytes
- There are known standard permutations tables…
- The add to the **confusion** of the algorithm…

ONE WAY FUNCTIONS

- Big numbers can make math hard, even for computers…
- Some math is easy to compute, but hard to undo…
- Ever break a plate? It’s hard to put back together…
- How easy is it to factor 12702047 by hand?
- I can tell you it’s factors are 3571 and 3557…
- I got 12702047 by multiplying 3571 X 3557…

MODERN CRYPTO

- Public key or key exchange algorithm used to transmit key.
- Key is hashed into proper size...
- Cipher is converted into a stream cipher...
- Encrypted transmission begins...
- Keys are constantly renegotiated...

WHY IS THIS IRRELEVANT TO HIDE PAYLOADS?

- The target HAS to decrypt the message…
- Most payload crypters that use “modern” algorithms, use static keys, defeating the purpose…
- We are solving an entirely different problem space than traditional crypto…

WHAT ELSE?

- We don’t care about long term cryptanalysis…
- We’re only hiding when the anti-virus is looking…
- We want to hide the ENCRYPTION algorithm…

WHY NOT STANDARD CRYPTO?

- If you use a standard algorithm, library or kernal function, you will get caught.. STANDARD == SIGNATURE
- Shared-key algorithms have known permutation tables detectable by dynamic code analysis.

BACK TO BASICS

- Instead of Confusion/Diffusion we want obscurity
- It is harder to detect the unknown
- Easy to implement---in many ways

APPLYING CLASSIC CRYPTO

- Caesar Cipher (ROT-13/ROT-N)
- Substitution Ciphers…
- Viginaire Cipher..
  - Use a word as a “key” and alternate through the key shifting letters by the respective values (a->1, b->2..)

CAESAR CIPHER

SUBSTITUTION CIPHER

Attack Carthage on Tuesday

Wggwze Zwtghwuy fc Gkybrwq

VIGINAIRE CIPHER

e	v	l	l	p	l	a	n
k	e	y	k	e	y	k	e
11	5	25	11	5	25	11	5
p	a	h	w	u	k	l	s

CLASSIC CRYPTO ON MODERN COMPUTERS

- Instead of shifting we XOR
  - XOR is the practice of changing bits ...
  - XORS are easily reversed...
- We can easily do both a caesar cipher or even a viginaire cipher..
- Substitution ciphers can be done on the byte levels..

TEXTBOOK RSA

- Not secure but we don’t care (More on that later)…
- Decrypt data be raising it to a power mod n..
  - Hard to reverse but not impossible..
- Very innocuous and easy to obfuscate…

Known Plaintext Attack

- Make sure you’re solving the correct problem….
- Since the encryption key is public, it is possible to guess it.

HIDING ARITHMETIC

- When you learned to multiply... 4x3 = 4+4+4
- If you don't care about efficiency there is an infinite way to calculate the same thing...
- If it’s looking for a^b mod p you can calculate a*a*a*a*a.... mod p ...
- Want to hide mod p? Divide and find the remainder...

PUTTING IT TOGETHER

- Fooling a computer (with a short time limit) versus fooling person — Delay your code execution!
- Automating the process and avoiding future signatures..
- Some signatures will exist... but not specific to encryption..
- Algorithm randomization will make it harder to detect..

PUTTING IT TOGETHER

- Automatically generating payload ciphers to evade signature and reversing based controls.
- Using a two staged payloads to evade dynamic code analysis.

Glassdoor Exfiltration Toolkit

- Project announced at DerbyCon 2014...
- Open source Post-Exploitation Framework..
- Automated payload generation and obfuscation...
- Known and new exfiltration methods...
- Target 1.0 release expected August 2014...

THANK YOU!

- Thank you to our friends, family, employers, & BlackHat Sao Paulo, DerbyCon, CircleCityCon, LaDosaNostra...