RETICLE: DROPPING AN INTELLIGENT F-BOMB

a decentralized botnet for disposable computing

Brendan O’Connor, CTO/DSS
Malice Afterthought, Inc.
Think again.
BRENDAN O'CONNOR

- CTO/DSS, Malice Afterthought, Inc
- Rising 2L at the University of Wisconsin School of Law - IANAL,Y
- I've done DARPA stuff, security research, and even Network Warfare teaching for DoD (want to hire me? I'm always looking, so ping me!)
- BTW, No One Authorized Me To Say ANYTHING! I speak for nobody.
ROADMAP

• Scenarios (The Problem)
• F-BOMB (The Hardware)
• Reticle (The Software)
• Missions (What It Does)
• Next
SCENARIO 1: ENVIRONMENTAL RESEARCH
SCENARIO 2: BAD MEN WITH GUNS
SCENARIO 3: OCCUPY
WHAT WE WANT

• A system for cheap, disposable computers
• Deployable by untrained personnel
• Reconfigurable post-deployment
• Capable of independent or coordinated action
• With sufficient processing power to take on high-level tasks
• @Dakami - “Ever deployed hardware? It’s not fun.” I disagree!
ROADMAP

• Scenarios (The Problem)
• F-BOMB (The Hardware)
• Reticle (The Software)
• Missions (What It Does)
• Next
FALLING/BALLISTICALLY-LAUNCHED OBJECT THAT MAKES BACKDOORS

• Design Goals
  • Cheap -- < $75, < $50 if possible
  • Reconfigurable Hardware for Different Sensors
    • Ultimately, this will require USB for cheapest sensors
  • Light enough to be flown on a UAV, or thrown, hard
    • Durable enough to land poorly (we’ll come back to this)
  • Ubiquitous enough to be deniable-- no bespoke PCBs
WHY NOT THE PWNIE PLUG?
WHY NOT THE MINIPWNER?
WHY NOT THE WASP?
PogoPlug POGO-B01 Mainboard

Flash Drive

2x RTL8188

F-BOMB, VERSION 1

PogoPlug (v2/v3) Core
BRIGHT PINK INFRINGEMENT
RECONFIGURABLE
Nighthawk

Carbon Monoxide Alarm

Explosive Gas Alarm

International Spy Museum
Washington DC
EXCESSIVELY REAL-WORLD TESTING
WHOOPS
ROADMAP

• Scenarios (The Problem)
• F-BOMB (The Hardware)
• Reticle (The Software)
• Missions (What It Does)
• Next
RETCILE
RETICLE DESIGN GOALS

• Minimum Viable Hardware - exploit local WiFi for comms
• Deniable Deployment
  • Encrypted storage, with no local key storage!
  • Encrypted communications
• No Central C&C Server - fully peer-to-peer, no SPOF
• Resistance to Central Compromise / Node Compromise
• As easy to deploy as a life jacket, but still with crypto.
NOT DESIGN GOALS

• Mesh Network
  • Really great research, but hard for untrained users in the field to deploy in an efficient way
  • Instead we’ll use “the Cloud” as our mesh!

• Synchronous Communication / Simultaneous Command
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems
SOLUTION: A CLONE ARMY
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems **DARPA**

• How do we have encrypted storage without storing the key on-disk but still easy to use?
GRENADE-STYLE KEY MANAGEMENT
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems DARPA

• How do we have encrypted storage without storing the key on-disk but still easy to use? USB Drive

• Obfuscating Traffic Endpoints
SOLUTION: TOR
PROBLEMS TO SOLVE

- Enough hardware to test performance on embedded systems **DARPA**
- How do we have encrypted storage without storing the key on-disk but still easy to use? **USB Drive**
- Obfuscating Traffic **Tor**
- Easy Local Storage
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems **DARPA**

• How do we have encrypted storage without storing the key on-disk but still easy to use? **USB Drive**

• Obfuscating Traffic **Tor**

• Easy Local Storage **Couch**

• Peer-to-Peer Replication
SOLUTION: COUCHDB
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems **DARPA**

• How do we have encrypted storage without storing the key on-disk but still easy to use? **USB Drive**

• Obfuscating Traffic **Tor**

• Easy Local Storage **Couch**

• Peer-to-Peer Replication **Couch**

• Encrypted, Revokable Communications
SOLUTION: COUCHDB?
STEP 3.5: FILE A BUG REPORT
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems DARPA

• How do we have encrypted storage without storing the key on-disk but still easy to use? USB Drive

• Obfuscating Traffic Tor

• Easy Local Storage Couch

• Peer-to-Peer Replication Couch

• Encrypted, Revokable Communications
SOLUTION: NGINX
PROBLEMS TO SOLVE

- Enough hardware to test performance on embedded systems **DARPA**
- How do we have encrypted storage without storing the key on-disk but still easy to use? **USB Drive**
- Obfuscating Traffic **Tor**
- Easy Local Storage **Couch**
- Peer-to-Peer Replication **Couch**
- Encrypted, Revokable Communications **Nginx**
- Initial introductions to the peer-to-peer network
EXPLANATION: I WISH I HAD FRIENDS
STEP 6.1: REMEMBER USENET?
STEP 6.2: THE SASSAMAN MEMORIAL HACK

1980-2011
Len was our friend. A brilliant mind, a kind soul, and a devious schemer; husband to Meredith, brother to Calvin, son to Jim and Dana Hartshorn, coauthor and cofounder and Shmoo and so much more. We dedicate this silly hack to Len, who would have found it absolutely hilarious.

--Dan Kaminsky,
PROBLEMS TO SOLVE

• Enough hardware to test performance on embedded systems **DARPA**

• How do we have encrypted storage without storing the key on-disk but still easy to use? **USB Drive**

• Obfuscating Traffic **Tor**

• Easy Local Storage **Couch**

• Peer-to-Peer Replication **Couch**

• Encrypted, Revokable Communications **Nginx**

• Introductions to the peer-to-peer network **Usenet**
PROFIT!
ROADMAP

- Scenarios (The Problem)
- F-BOMB (The Hardware)
- Reticle (The Software)
- Missions (What It Does)
- Next
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment</td>
<td><code>attachment</code> 1.0 KB, application/octet-stream</td>
</tr>
</tbody>
</table>

**Testing Missions**
MISSIONS SO FAR

- Blinkenlights
- Stalkr
- OKCreepy
- Private Web Browsing (Auto-Tor)

- Note that we get wireless bridging / area extension for free!
OTHER EASY MISSIONS

• P25 listeners (SDRs are now $25!)
  • A shout-out to Matt Blaze / Travis Goodspeed
  • “Why (Special Agent) Johnny (Still) Can’t Encrypt”
  • …a thousand other things (and reconfigurable on the fly)
  • Also missions aren’t exclusive, though Reticle doesn’t attempt to negotiate sharing of devices; this isn’t designed as a public resource network
ROADMAP

• Scenarios (The Problem)
• F-BOMB (The Hardware)
• Reticle (The Software)
• Missions (What It Does)
• Next -- and how you can help!
NEXT STEPS FOR RETICLE

• Opportunistic Replication

• Change the scan+connect script to run continuously, and replicate whenever we find a connection

  • MIT did this, but won’t release the source code :-(

• Data Visualization for hordes of data

• New hardware (F-BOMB v2) - mmm, Raspberry Pi!
NEW PROJECT: SPOTLIGHT
SPOTLIGHT

• Hide and Seek

• No trained “seekers”
  • We’ll use bicycle couriers and bored students

• 20 Reticle Nodes

• 12 Hours

• 10 Targets (5 mobile, 5 static)
SPOTLIGHT

Anyone want to come play with us? We’d love to partner.

brendan@maliceafterthought.com