Effective Security
Going Back To The Basics

Merike Kaeo, CTO
merike@fsi.io

FARSIGHT SECURITY

DISCUSSION POINTS

- Attack Trends – A Historical View
- Attack Vectors in Recent Years
- Evolution of Mitigation Techniques
- Remembering The Basics
- Our Collective Responsibility

ATTACKS: EVERYTHING IS FAIR GAME

Internet Layer: basic communication, addressing and routing (IP, ICMP)
Transport Layer: handles communication among programs on a network (UDP, TCP)
Application Layer: end-user applications (NTP, DNS, FTP, etc.)

- Operators should understand fundamental networking behaviors
- Know which devices are communicating and what they are supposed to send and receive

HOW DO THESE ATTACKS OCCUR

- Protocols have flaws
- Implementations have bugs
- Implementations have poor default settings
- Operators main focus is transiting customer traffic
- End users are IoT operators but not network engineers
- If someone floods traffic, how do you NOT cause collateral damage to legitimate traffic?

HISTORICAL VIEW: DoS

- Single Machine and relatively unsophisticated
- Ping of Death (1996)
  - Attacker sends ping packet larger than 65,536 bytes
- Land.c (1997)
  - Attacker sends TCP SYN spoofed packet where source and destination IPs and ports are identical
- Smurf (1999)
  - Large number of ICMP messages sent using target spoofed source IP address and destination IP broadcast address
- Fraggle
  - Variation of SMURF attack using UDP port 7 (echo) and port 23 (chargen) instead of ICMP

HISTORICAL VIEW: DDoS

- Multiple Machines used to orchestrate attack
- Distributed and automated
- Trinoo (1999)
  - The attacker(s) control one or more "master" servers, each of which can control many "daemons”. The daemons are all instructed to coordinate a packet based attack against one or more victim systems.
  - Specific ports are used in communications
  - Utilizes UDP and ‘ICMP Port Unreachable’ messages

HISTORICAL VIEW: DDoS

- TFN (Tribal Flood Network) (1999)
  - More sophisticated tool that can cause ICMP flood, SYN flood, UDP flood and SMURT-style attacks
  - Communications between attack infrastructures uses ICMP echo and echo-reply packets
  - IP Identification and payload of ICMP echo-reply identify type of attack
  - IP address can be spoofed
- TFN2K (1999/2000)
  - Newer variant of TFN and doesn’t use specific ports
- Stacheldraht (2000)
  - Combines features of Trinoo and original TFN tool
  - It can encrypt communications

GAME CHANGERS

- Code Red
- Slammer
- StuxNet
- DNS-Changer
- Mirai
- WCry

Cybercrime: What is Changing?

- **Scale**
- **Sophistication**
- **Impact**

CONTINUING TRENDS

- Attackers will continue to try and change tactics to stay under detection
  - Packet size variations
  - Time of day variations
  - More utilization of encryption
- The bandwidth available for malicious intent will continue to increase
- The number of devices available for exploitation will continue to increase
- BotNets for hire will get more sophisticated

THE NEW NORMAL

- Adhoc Mesh Networks
- Prevalent Use of Tunneling
- “There’s an App for That”

Seeing a period of rapid change

- Intelligent, interconnected devices are continuing to be connected to the global Internet
- Data is accumulating faster than it can be organized or effectively protected
- The complexity of the Internet ecosystem creates a rich environment exploitable by activists, criminals, and nation states
- Data will continue be stolen or modified using subtle, persistent, directed attacks

TODAYS COMPLEX NETWORKS

What Communicates to What, and How?

YET SOME THINGS STAY THE SAME

- Most DDoS attacks use same mechanisms as have been used for last 20 years
- Credential compromises are a large part of how compromises occur
- Implementations will have flaws but patching is slow and/or not possible
- Security continues to be an exercise of blind trust
  - Technical standards
  - Vendor implementations
  - Operational deployments

DDoS: AMPLIFICATION HELL (and Extortion)

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

- Abusing Network Protocols for DDoS by Christian Rossow
- BAF: BW amplification factor
- PAF: Packet amplification factor
- Presented at NDSS 2014
- http://www.christian-rossow.de/articles/Amplification_DDoS.php

BACK TO THE BASICS: SECURITY GOALS

- Controlling Data Access
- Controlling Network Access
- Ensuring Network Availability
- Integrity of Information (at rest / in transit)
- Confidentiality of Information (at rest / in transit)
- Preventing Intrusions

BACK TO THE BASICS: SECURITY CONTROLS

- User Authentication/Authorization
- Device Authentication/Authorization
- Access Control (Packet or Route Filtering)
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation

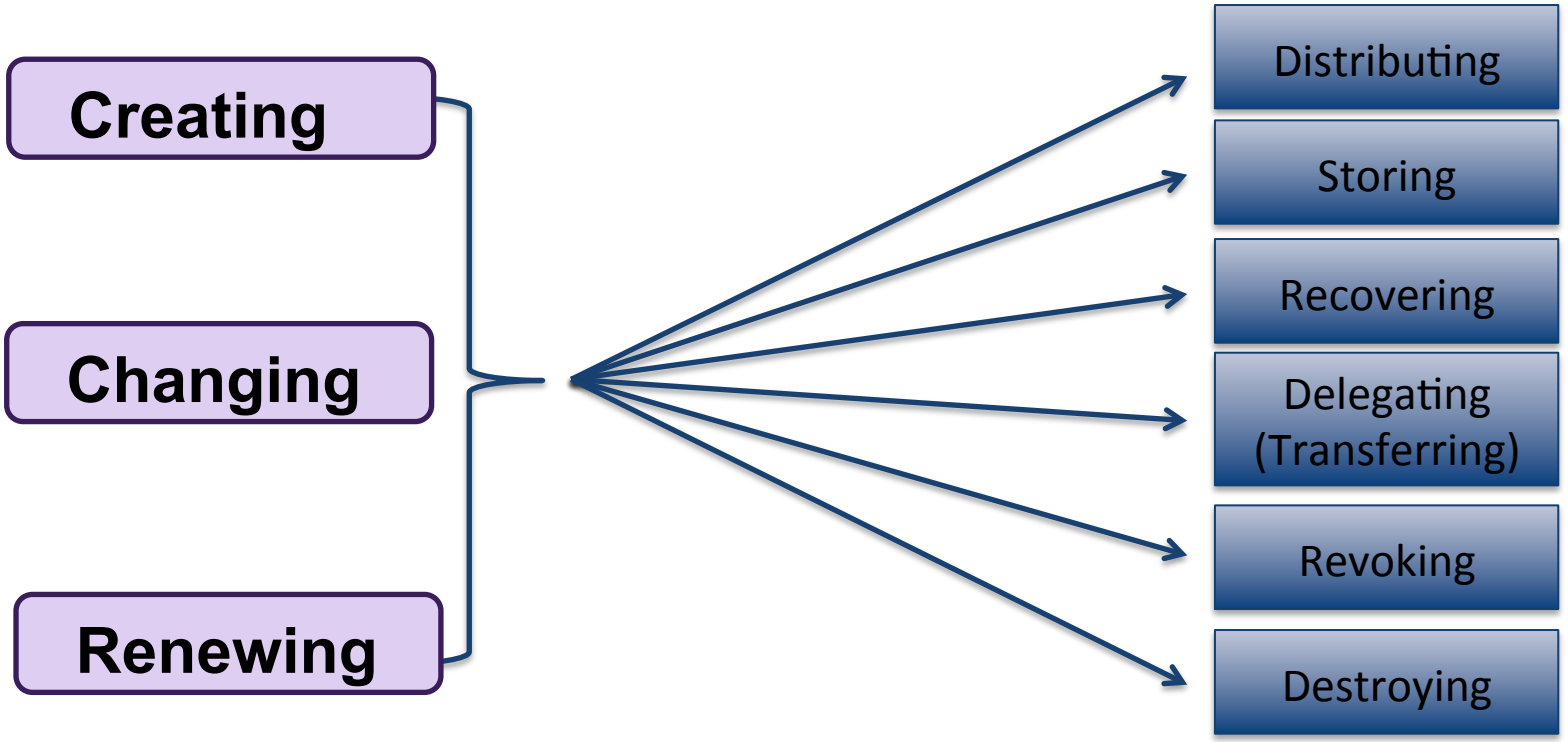
BACK TO THE BASICS: GOOD HYGIENE

- Have Sufficient BW to Absorb Attack
- Filter Unwanted Traffic
- Rate Limit
- Effective Logging and Alerting Mechanisms
- Log, Collect and Correlate Attack Data
  - SHARE DATA with trusted folks
- Create and Maintain Redundancy of Infrastructure
- Pay Attention to Credential Management Lifecycle
- Define Minimum Security Feature Set From Vendors

CREDENTIAL COMPROMISE IS ENABLER

- Being victim of a phishing attack
- Laptop gets stolen
- Sharing your password with another person
- Re-using same password on many systems
- Spyware on your computer installed a keylogger
- Storing your private key in an easily accessed file
- Sending credentials in cleartext emails
- Unpatched security vulnerabilities are exploited

CREDENTIAL MANAGEMENT LIFECYCLE



- Know ALL credentials used in your environment
- Encourage multi-factor authentication

BACK TO THE BASICS: CREDENTIALS

- Know ALL Credentials That Are Utilized
- Limit Fate Sharing
- Encourage Use of Multifactor Authentication
- Do NOT Send/Store Credentials In Cleartext
- Create Processes For Credential Changes
  - Identity Verification Is Critical Component
- Know Where You Are Storing Credentials

BACK TO THE BASICS: VULNERABILITIES

- Know Your Operating Systems and Application Versions
- Get on Mailing Lists For Vendor Security Announcements
- Subscribe to National CERT Alert Lists
- Follow Security Industry Blogs
- Create Trusted Sharing Groups

DO YOU KNOW YOUR DNS TRAFFIC ?

- Service provider automatically configures DNS Servers using automated mechanisms
  OR
- Service provider provides you with DNS Server IP addresses that get statically configured

DNS Server is:
203.0.113.231
2001:DB8::231

Home router automatically configures DNS Servers over wireless network

Computer
192.168.1.101

DNS Server is:
203.0.113.231
2001:DB8::231

DNS Server is:
203.0.113.231
2001:DB8::231

Home Router
WAN: 204.0.113.66
2001:DB8::66
LAN: 192.168.1.1
2001:DB8:8888::1

DNS Server is:
203.0.113.231
2001:DB8::231

Home router automatically configures DNS Servers over wired network

Smartphone
192.168.1.102

BACK TO THE BASICS: DNS

- Know What Domains You Own
- Validate The Registrars You Use
  - Do they use good security practices?
  - Identity validation
  - Internal processes
- Design Redundancy For Critical Services
- Monitor For Potential DNS Hijacking
- Monitor For Domain Phishing and SPAM Campaigns

SHARING – WE MUST GET BETTER

Criminals Have No Barriers

- Websites advertise Botnets and malware for hire
- Vulnerabilities and Exploits are traded on open market
- There are no enforced rules for NOT sharing
- Social media is making sharing more efficient

Choose Custom Botnet

- Number of Hosts
- Geographic Region
- Bandwidth
- Duration
- etc

CONTINUE TO INCREASE SHARING

- Initial Step – Build Trust Thru Networking
- Start by sharing for specific use cases that don’t impact privacy and personally identifiable information (PII)
  - SSH Brute Force Attacks
  - DNS/SMTP/NTP Amplification Attacks
  - Passive DNS Information
- Investigate how to share data that may impact privacy/ PII and what can be anonymized but still be useful
  - SPAM / Phishing details

GLOBAL EFFORTS FOR ACTION

- **DNS-OARC**: DNS System Security
- **FIRST**: Vulnerability management
- **ISACs**: Specialized Interest Groups
- **M3AAWG** / **APWG**: Anti SPAM, Phishing and Crime
- **NSP-SEC**: Big Backbone Providers and IP Based Remediation
- **OPSEC-Trust**: Situational Awareness

MOTIVATOR: SUCCESS STORY

- Estonia Example (May 2007)
  - Creating ***trust***
    - TC-FIRST
    - Global Operation Security Teams
  - Cross functional meetings
  - Known roles due to i-voting (2005)
  - Government ***facilitated*** communication and tactics
  - Openness with ***information sharing*** was critical
  - A variety of attacks used including Botnet for Hire

SOME THOUGHTS ON MEDIA AND THE NEWS

Don’t Believe Everything You Read

BEING PART OF THE SOLUTION

- Certify devices for fundamental security requirements
- Use ONLY cryptographically protected protocols (this implies integrity and non-repudiation and possibly confidentiality)
- Change ALL default usernames and credentials
- Keep up with vulnerabilities and patch/upgrade in a timely manner
- Share what you can and help cross-functional education


QUESTIONS ?