IoT Security by the Numbers

Leslie Daigle, Rufo De Francisco

Global Cyber Alliance

November 10, 2022.

IoT Security – Scope of the challenges

Why do we (GCA) care

- Global Cyber Alliance
  - Not for profit
  - Dedicated to reducing cyber risk
- GCA AIDE(*) project includes
  - global honeyfarm (hundreds of sensors)
  - 4 years of data
  - Our own honeypot technology (ProxyPot)

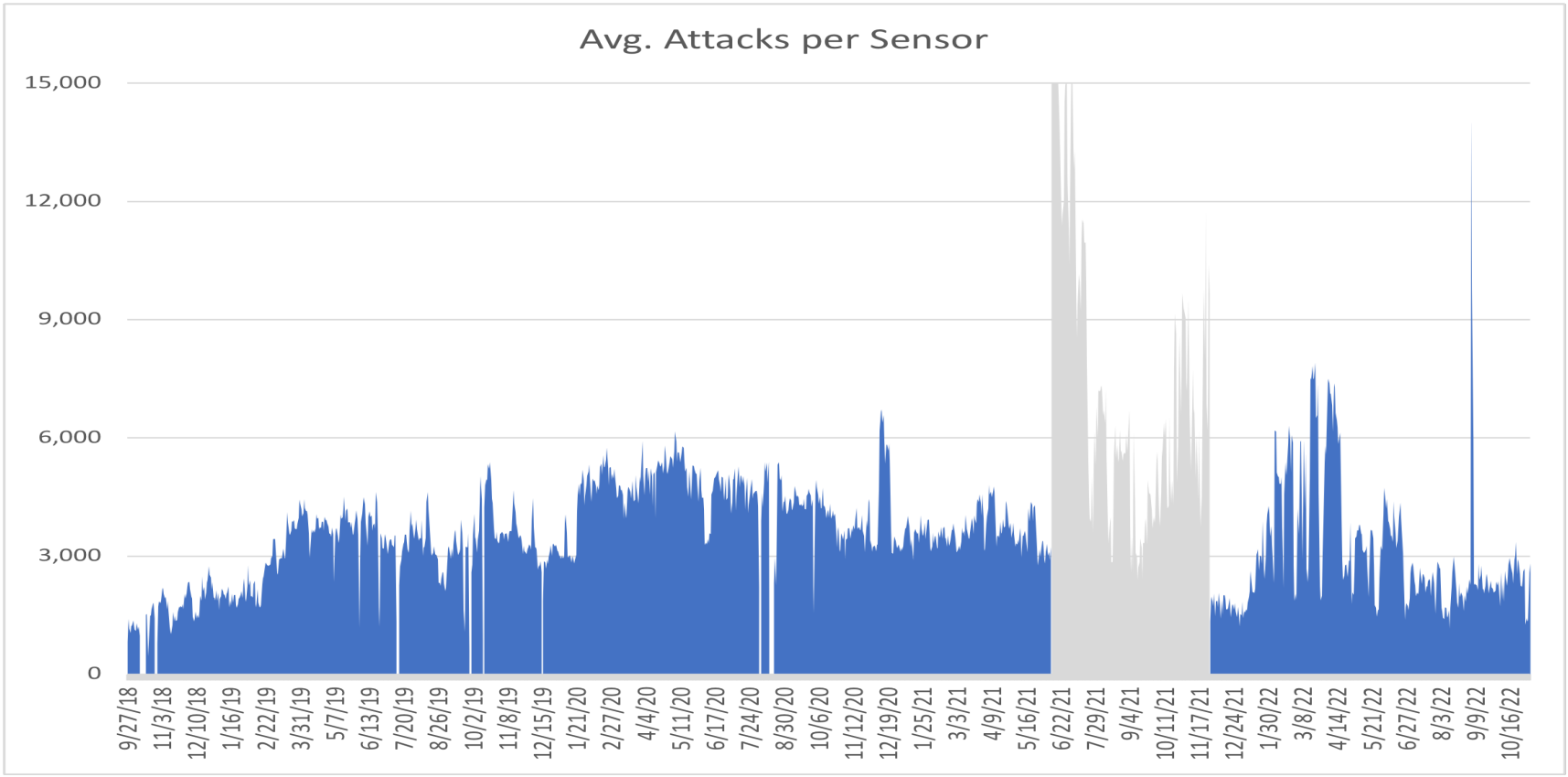
(*) *Automated IoT Defense Ecosystem*

IoT Security: Why do we (all) care

- Who remembers October 21, 2016?
  - MIRAI botnet distributed denial of service attack on Dyn services
  - https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn
- Aka – why so many laws against default passwords…
- Of course, it's not all about conscription of devices into the world's largest botnet

- The same actors are hitting everything (at least in IPv4 space)
  - Some are getting toe-holds on edge devices and escalating within networks

So many attackers knocking on your door



It’s coming from everywhere – nowhere to hide

March 2022 Attacks seen on US sensors and from US to other sensors

Some targeted A/B studies

Phase 1

Considering the relevance of policies requiring various security controls

What was Tested

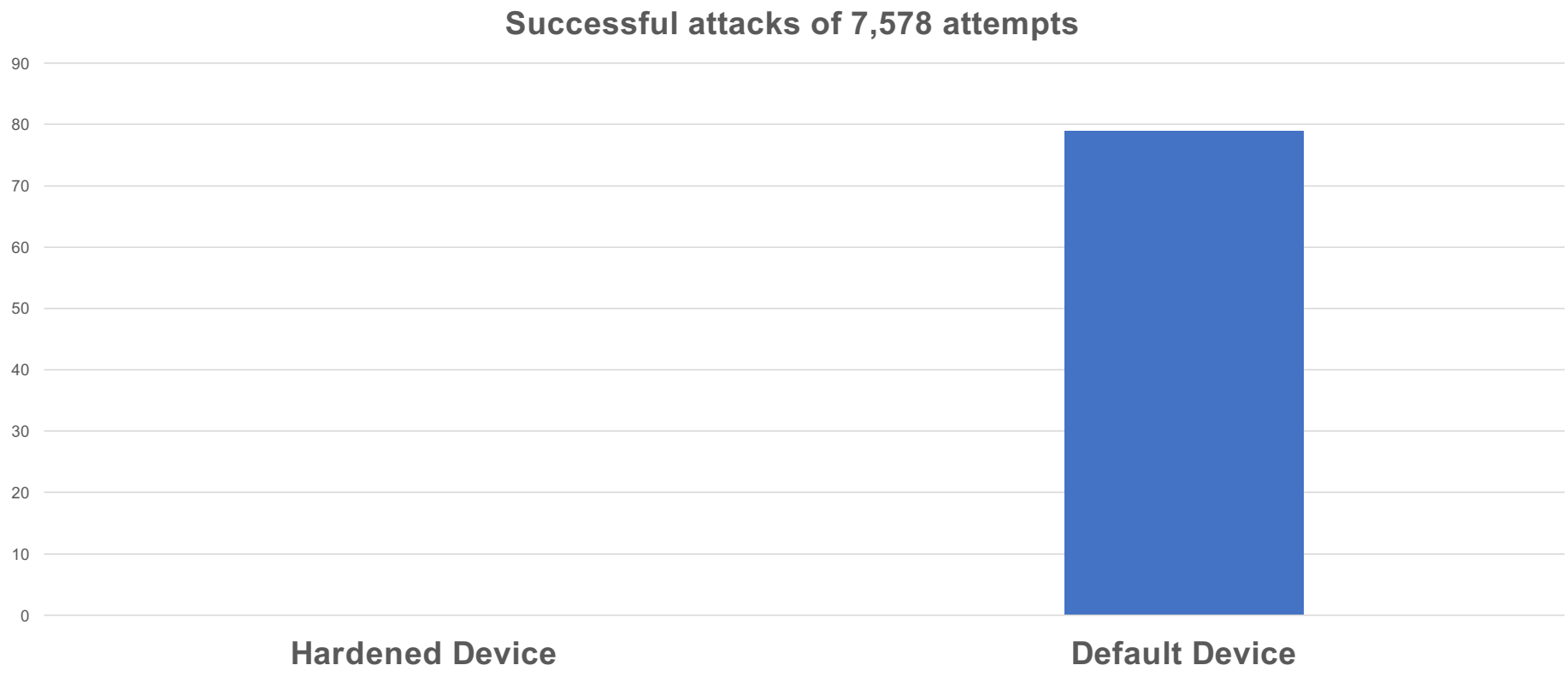
- Using ProxyPot honeyfarm, virtualized devices were configured with **common controls** from policy and standards to test their effectiveness “in the wild” against attacks:

  - “Secured access” (no default passwords)
  - Data in transit is protected
  - “Patchability” (keep software updated)

The A/B test setup

- Honeyfarm
  - 70 honeypots
  - Emulating open source firewalls, network-attached storage (NAS) solutions, and operating systems commonly found in IoT devices: FreeNAS, OpenMediaVault, OpenWrt, pfSense, XigmaNAS, M0n0Wall, and SmallWall.
  - For each of the 7 emulations, 10 honeypots were deployed, 5 with default passwords and 5 hardened with strong passwords.
- Data collected for almost 2 months
  - April 5 to June 3, 2021
- The system recorded 786,086 sessions, which resulted in 1,113,729 HTTP requests and 1,083,277 responses.
  - A small number (6,432) of those sessions were legitimate scans by search bots. The remaining 779,654 sessions were classified as “attacks”.

Default passwords fail. Period.



Findings: Validating Security Controls

- Common technical controls **significantly reduce** attack success
- **No default passwords**: tried and true
  - The only successful login attempts recorded were on devices with default passwords
- Attackers prefer non-secured **communications protocols**
  - Mirai is still the most common source of Telnet-based attacks over five years later
- **Updated software** prevents device break-ins

Findings: Policy Gap

- Attackers are attempting to **exploit the software stack** of devices
- The majority of login attempts observed were targeting the embedded **web servers** rather than the devices themselves
- **The gap:** The scope of software in IoT security policy and standards is generally focused on operating systems rather than applications
  - Which led to further exploration of the software stack…

Phase 2

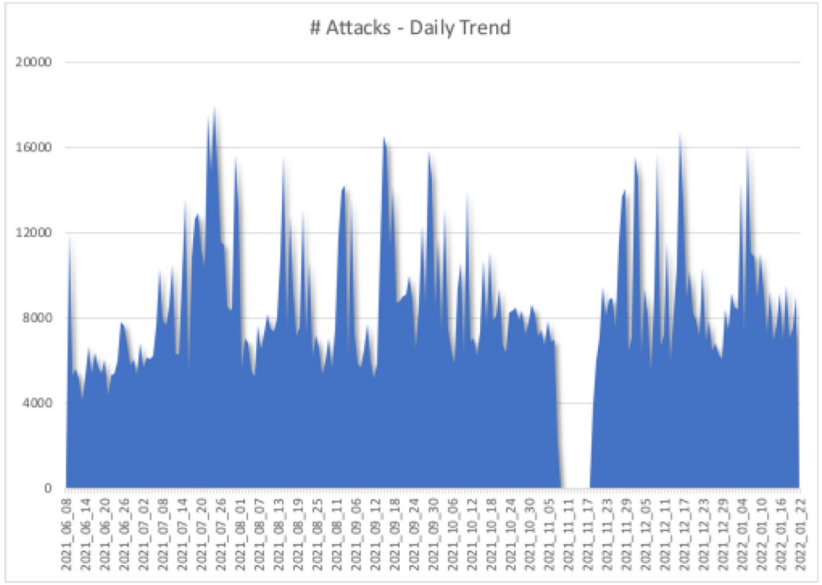
Beyond the device/device OS, how important is the security of the software stack?

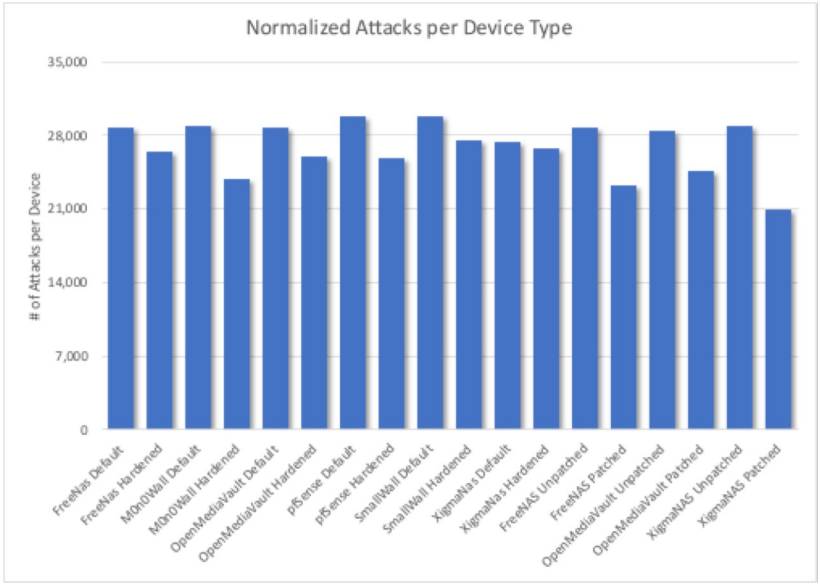
Phase 2 Honeyfarm

Control	Class	Device	Type	Credentials	Version	Count
Secured access	Default	FreeNAS v10.0	NAS Appliance	Default, weak	Recent	5
	Hardened	FreeNAS v10.0	NAS Appliance	Strong	Recent	5
Secured access	Default	M0n0Wall	Firewall	Default, weak	Latest, unsupported	5
	Hardened	M0n0Wall	Firewall	Strong	Latest, unsupported	2
Secured access	Default	OpenMediaVault v3.0	NAS Appliance	Default, weak	Recent	5
	Hardened	OpenMediaVault v3.0	NAS Appliance	Strong	Recent	5
Secured access	Default	pfSense v2.4.5	Router/Firewall	Default, weak	Recent	5
	Hardened	pfSense v 2.4.5	Router/Firewall	Strong	Recent	5
Secured access	Default	SmallWall v1.8.3	Firewall	Default, weak	Latest, unsupported	5
	Hardened	SmallWall v1.8.3	Firewall	Strong	Latest, unsupported	5
Secured access	Default	XigmaNAS v10.1.0	NAS Appliance	Default, weak	Recent	5
	Hardened	XigmaNAS v10.1.0	NAS Appliance	Strong	Recent	5
Patchability	Unpatched	FreeNAS v8.0	NAS Appliance	Strong	Old	2
	Patched	FreeNAS v11.3	NAS Appliance	Strong	Latest	2
Patchability	Unpatched	OpenMediaVault v1.9	NAS Appliance	Strong	Old	2
	Patched	OpenMediaVault v5.2	NAS Appliance	Strong	Latest	2
Patchability	Unpatched	XigmaNAS v9.3.0	NAS Appliance	Strong	Old	2
	Patched	XigmaNAS v12.2.0	NAS Appliance	Strong	Latest	2
TOTAL						**69**

High-Level Traffic Statistics

- Collected data for 227 days between 6/8/21 and 1/22/22
- Recorded 1,888,333 meaningful attacks (100 attacks per device per day)
- Although not obvious in the first chart, the peaks generally align with weekends.
- Normalized traffic distribution was fairly uniform, with a pattern of more traffic on more vulnerable devices





Attacks & Targeted Software

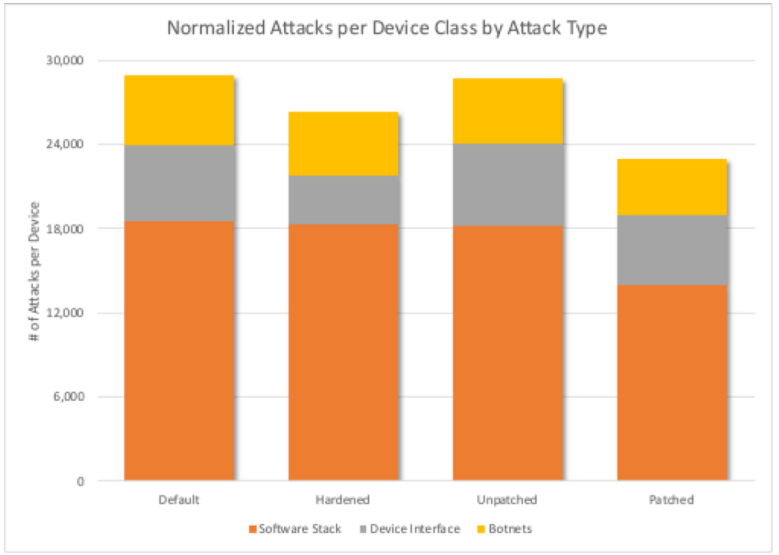
- Most attacks were attempts to exploit known vulnerabilities (CVEs) of the software stack
- PHP and SQL were the SW ingredients more often targeted
- Obfuscation, command injection, and environment variable parsing were observed techniques seen
- Unexpected result: Lots of attacks against a long-discontinued web server (Boa) - Many devices in the field still include it, new vulnerabilities still being reported (but not patched)
- Many attacks against ThinkPHP, a PHP framework popular in China, with few vulnerabilities disclosed. We believe this is caused by under-reporting

Attack Type	Attack Count
Software Stack	1,241,845
Device Interface	324,805
Botnets (Mozi, Mirai)	321,683
ALL	**1,888,333**

Software Component	Type	Attack Count	CVE Count
PHP	Server-Side Scripting	631,184	7,328
phpMyAdmin	Database	186,331	1,911
Apache HTTP Server	Web Server	94,942	584
Many	Env Scanners	80,038	73
Boa	Web Server	72,540	32
Other SQL	Database	33,774	7,408
ThinkPHP	PHP Framework	33,173	20
WordPress	Content Management	29,994	4,563
MySQL	Database	23,683	1,630
Laravel	PHP Framework	22,828	59
Device Firmware	Firmware	19,129	3,404
Bash	Shell	7,901	93
SQLite	Database	4,079	139
vBulletin	Forum Software	1,490	119
pfSense VPN	Firewall/Router VPN	759	53
ALL		**1,241,845**	**27,416**

Policy Control Implications

- Strong passwords provide effective protection against attacks on device interface
  - 36% fewer normalized attacks to the device interface on devices hardened with strong passwords than on default credential devices
  - Many of the credentials attempted are documented in CVEs
- Patching provides effective protection against attacks on software stack
  - 24% fewer attacks against the software stack on patched devices than on older, unpatched devices =>



- HTTP (unsecured) was preferred over HTTPS (secured) 90%-10%, matching the distribution of vulnerabilities over those protocols
- 17,440 attempts to modify files, 9,567 attempts to download files (wget, ftp, curl)

Conclusions, looking ahead

- Device security is necessary
  - Not sufficient
- There's (still) a whole world of hurt from known vulnerabilities, CVEs
  - And, can't assume
    - Devices are updated / updatable
    - Devices are even built with current software
    - 👉 Regulation may address some this going forward
- Even as we figure out how to do things right going forwared (IoTOPS WG), there's going to remain a large swath of vulnerable devices/software stacks.
  - Can't just airgap everything…
  - Deal with the attacks at source
  - Tools and techniques to monitor and manage the network on which the devices are connected?

Further details…

- Global Cyber Alliance Phase 1 report:
  - https://www.globalcyberalliance.org/reports_publications/iot-policy-and-attack-report/
- (Phase 2 report is forthcoming)
- Leslie Daigle – ldaigle@globalcyberalliance.org