RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-R03**

The Non-Social Distanced Reality of the Internet of Things

Leslie Daigle

Chief Technical Officer
Global Cyber Alliance
@LeslieLDaigle

Rachel Azafrani

Senior Program Manager
Microsoft
@razafrani

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

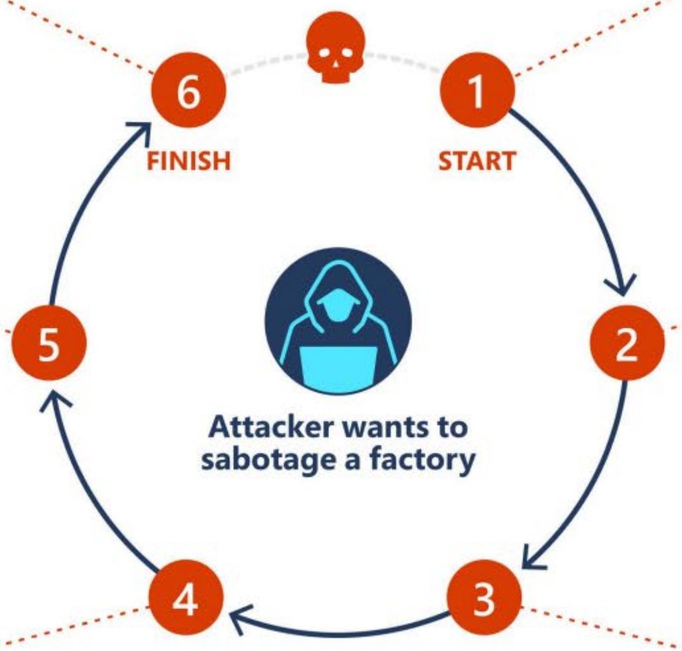
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The IoT threat landscape is not improving.

IoT Attack Trends

- The first half of 2021 saw *1.5 billion attacks* against IoT devices (Kaspersky 2021)
- The work-from-home environment led to increased targeting of corporate devices
- Attackers are creating botnets, stealing information, mining cryptocurrency, and gaining privileged access
- New and old vulnerabilities alike are being exploited

How an attacker can get into an enterprise through IoT



Reconnaissance

Attacker finds an employee on social media who talks about:

- Their employer.
- The TV they bought a few years ago.
- OT they are working on at home.

Email

Attacker sends email or direct message to the employee. Rather than attacking their laptop or phone, attacker targets the TV on their home network.

Exploit

- IoT, without endpoint protection and auditing, is a safe place for an attacker to hide.
- The attacker searches the employee's home network for the employee's work device or OT device.
- Can downgrade firmware, use exploit and install backdoor/payload.

Lateral movement

- Attacker moves from TV to the OT device that the employee took home. The OT device is now vulnerable to previously patched vulnerabilities.
- Attacker uses exploit and installs backdoor/payload.
- Payload lies about version.

Work from home

Employee continues about their business, unaware of the compromise.

Return to factory

- Employee takes OT device back to their place of work, such as at a factory.
- The factory trusts the hardware/OT device.
- Payload timed to go off (e.g. programmed to the DNS change; no longer on home network).

Source: Microsoft Digital Defense Report (2021)

New Rules of the Road

The technical standards community and policymakers are racing to set a baseline for IoT security. A few examples:

2020:

- NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline
- ETSI EN 303 645 Cyber Security for the Internet of Things: Baseline Requirements
- US IoT Cybersecurity Improvement Act
- Australia Code of Practice

2021:

- UK “Product Security and Telecommunications Infrastructure” proposed legislation
- ISO 27402 Device baseline requirements under development

Are IoT security policy and standards working?

The IoT Attack Data Project

Global Cyber Alliance Internet Integrity Program

THE POWER OF DIVERSITY

Addressing security and stability issues requires supporting and promoting diverse networks.

The Internet Integrity Program brings together key players in internet infrastructure operations, as well as adjacent industries, in order to identify top priorities for addressing cybersecurity issues that cannot be solved by any single actor, or subset of actors, independently.

KEY PARTNERS:

- Internet Ecosystem Institutions
- Network Operator Groups
- ISPs and other infra operators

IoT Attack Data Project Objective

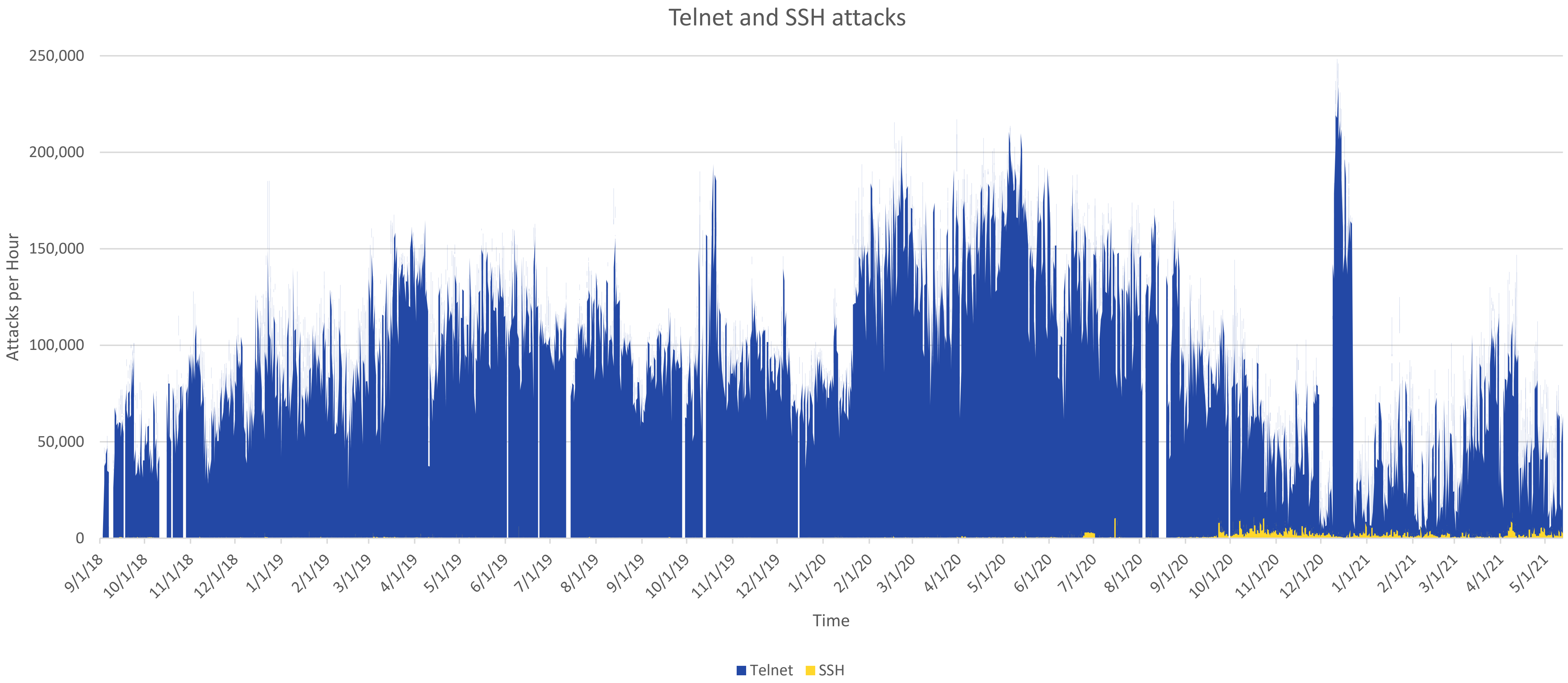
Use data on real IoT attacks to offer evidence on the validity of the most widely accepted IoT security policies and standards.

Support a **data-driven** approach to public policy for IoT security.

Methodology

- Analyze GCA's **Automated IoT Defense Ecosystem (AIDE)** historical data for trends and changes in IoT attack methodologies
- Configure **ProxyPot**, GCA's proprietary honeypot infrastructure, with common **technical controls** referenced in IoT security policy and standards and use **A/B testing** to measure changes in attack success

Most attack traffic is unencrypted



ProxyPot

- AIDE also includes ProxyPot, a proprietary **honeypot** technology that can combine physical or virtualized IoT devices to build honeyfarms in a **flexible** way
- The ProxyPot technology enables defenders to emulate thousands of different IoT devices in a virtual environment distributed around the globe
- The technology is also compatible with other deception technologies and can be deployed in any environment (GCA has plans to expand the **scalability** of the technology)

AIDE: Automated IoT Defense Ecosystem

THE PROXYPOT TECHNOLOGY

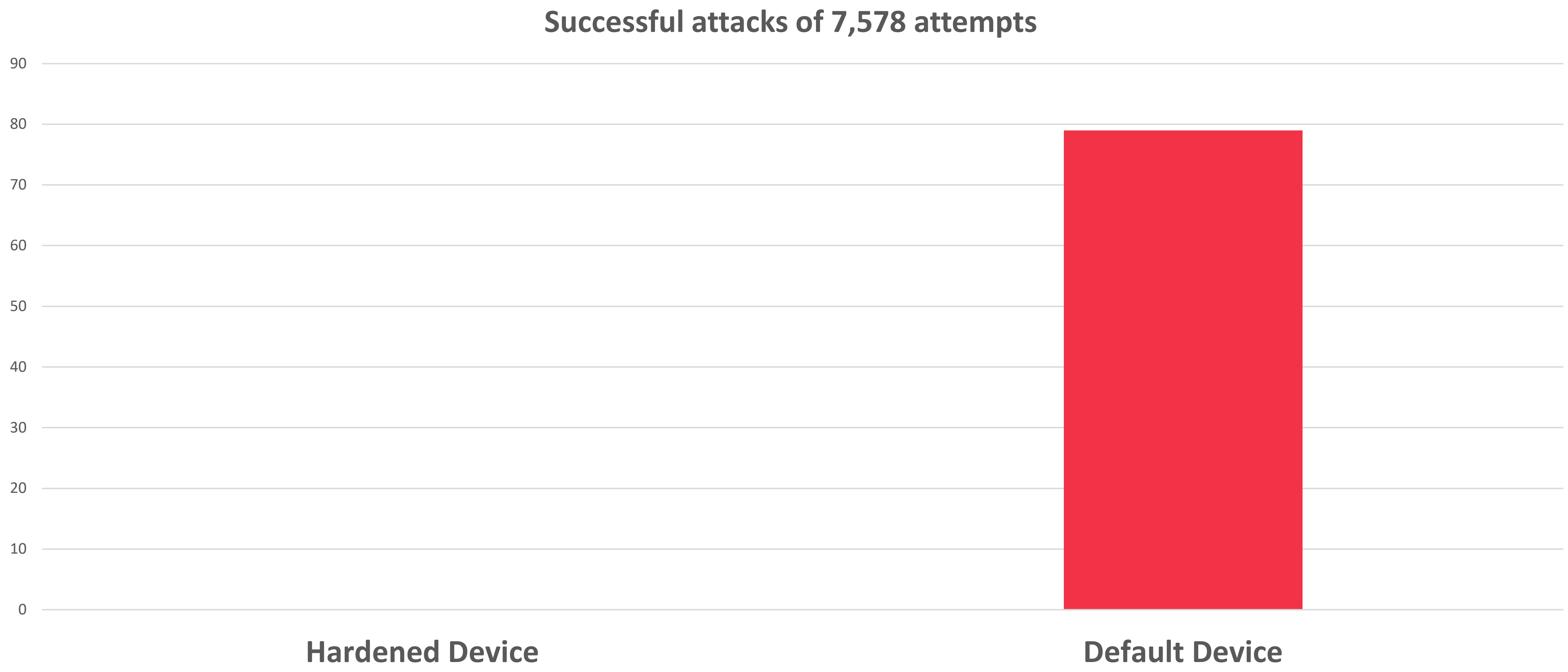
What was Tested

- Using ProxyPot honeyfarms, 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)

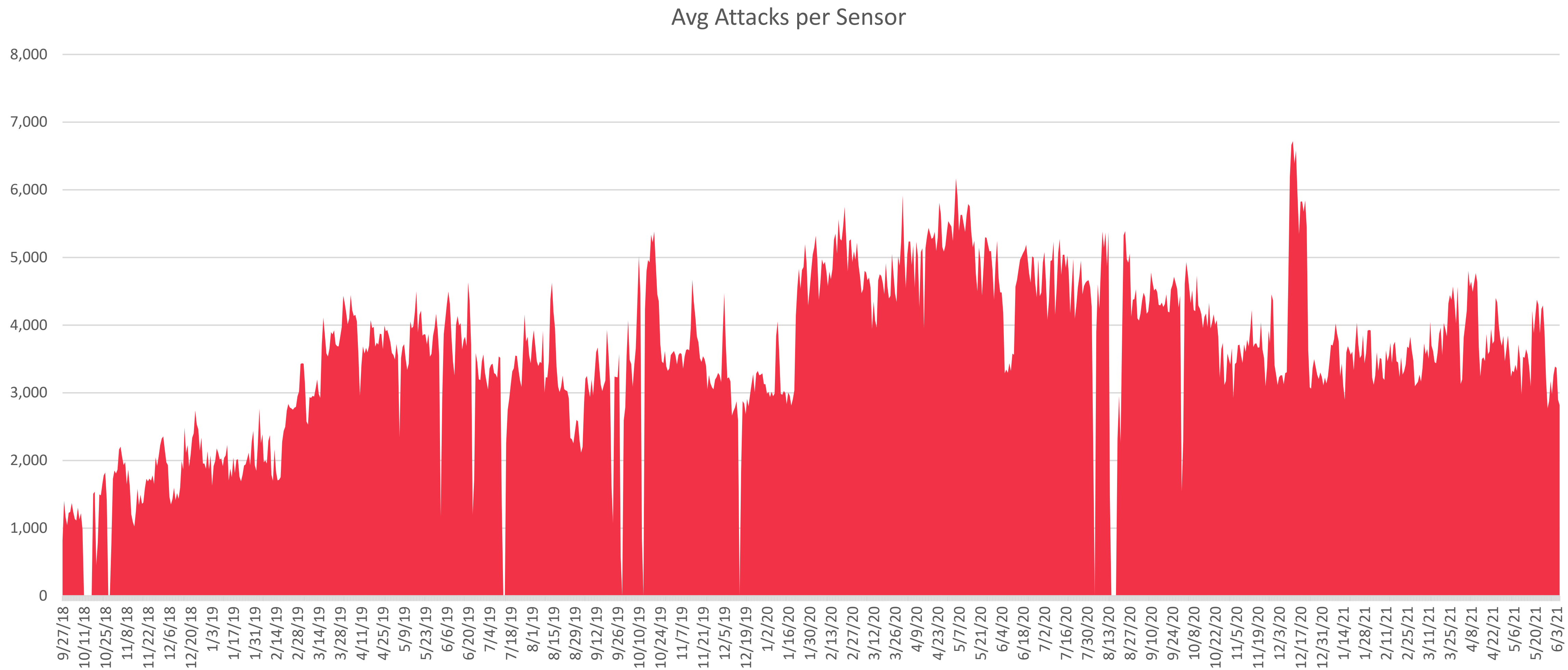
The A/B test setup

- Honeynet
  - 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.

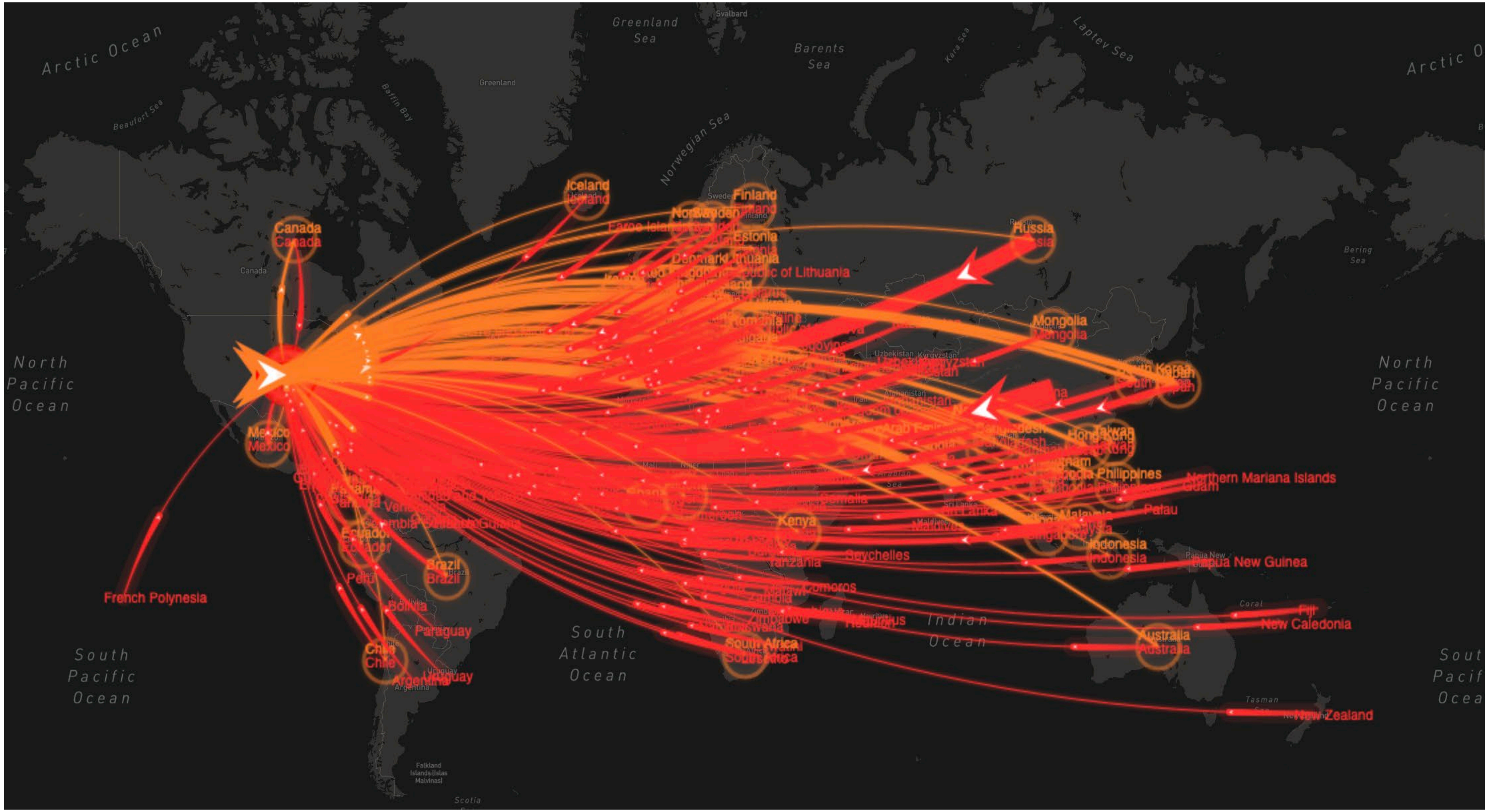


So many attackers knocking on your door



It’s coming from everywhere – nowhere to hide

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



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
  - Keeping application software updated matters

Apply the IoT Attack Data Project Findings

- As soon as you can you should:
  - Take every IoT device you have with a default password off the net
- In the near term, policymakers should:
  - Adopt recognized baseline IoT security standards for procurement and citizen-owned devices
- Security professionals should take these recommendations:
  1. No default passwords.
  2. Implement a vulnerability disclosure policy.
  3. Keep software updated.
  4. Continuously monitor IoT communication for unauthorized communications and attacks.

Discussion & Call for Partners

- How can the Global Cyber Alliance use AIDE data to be more constructive in IoT development and management going forward?
- How can we set up honeyfarms to collect indicators for informative patterns?
- How can we combine device transactions into larger trends?
- What should we be thinking about to generally improve IoT security?

RSAConference2022

Thank you

Resources

- https://www.globalcyberalliance.org
- https://www.globalcyberalliance.org/internet-integrity/
- https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
- https://www.globalcyberalliance.org/reports_publications/iot-policy-and-attack-report/