CENSUS
IT Security Works

www.census-labs.com

2nd Forum on Hybrid Threats, Cyber-security, and Artificial Intelligence

Challenges in Product Security

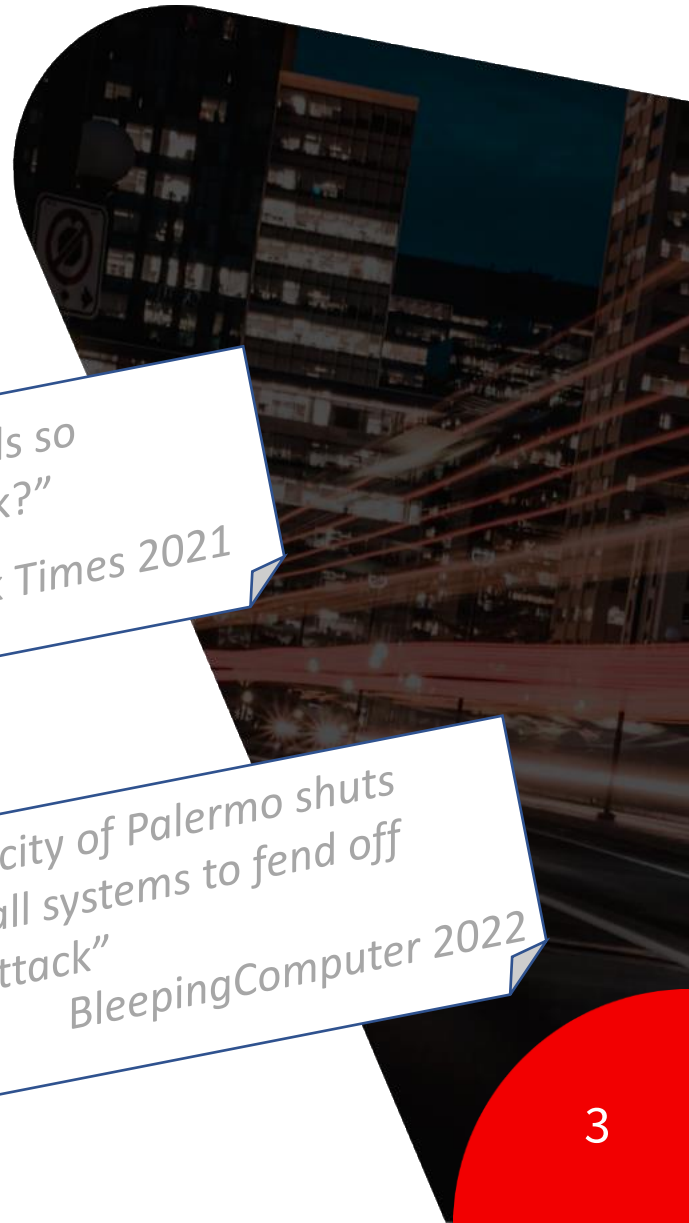
Dimitrios Glynos, Director of Product Security Services
(@dfunc on Twitter - dimitris@census-labs.com)

Why Product Security Matters

- Every organization depends on technology produced by **third parties**
- Software, services and devices may come with cybersecurity **vulnerabilities**
  - Modern technology is quite complex, expect security issues from any system component
  - Vulnerability exploitation may have **critical repercussions**
- System security is mostly at the vendor's mercy
  - The vendor might select **not to publish a fix** or **provide a delayed fix**
- Beyond vulnerabilities, **third-party access** to any part of the **supply** or **delivery chain** of a product may also induce privacy / operations issues to user organizations
- As consumers **we expect** that a product exhibits some resilience against cybersecurity threats - this is the essence of ***Product Security***

Why Product Security is Hard

- There are many **open challenges** in both **technical** and **non-technical** aspects of Product Security
- Let's break (some of) these down to the following categories
  - Technological challenges
  - Procedural challenges
  - Missing skills



Technological Challenges

- Our **building blocks** are tuned for *ease of development*, *delivery* and *management* – not secure operation
  - It's as if we expect a secure product only from IDEAL engineers
  - Programming languages and frameworks exist that hold certain security guarantees, but they're not widely known or used
- It is difficult to **enumerate** the primary components of a system and **verify** their origin
  - Baby steps through SBOMs and supply chain integrity frameworks, not widely adopted yet
- **Complex** and/or proprietary systems are hard to audit
- Technological advancements (AI, Quantum Computing, increased availability of computing resources etc.) may present **new adversarial capabilities** which must be anticipated

Procedural Challenges

- Some pre-market cybersecurity criteria **checks** are **enforced only for certain product categories** in the EU (e.g. radio equipment, medical devices) while USA is experimenting with labelling both consumer software and IoT products
  - A checklist-type certification of product security properties (e.g. CC) is not enough
- Many organizations are **missing** a **post-release issue handling** procedure
- Maintaining a **Secure SDLC** at the vendor is not easy
  - Requires an **investment** that may not be viable for smaller organizations
  - Requires a **unique path** which may not be known due to missing expertise
- There are many facets of product operations where **operators lack visibility**, enabling stealth attacks by adversaries

Missing Skills

- Regardless of the technology available, the human factor remains key in identifying and dealing with cybersecurity threats. However, there's **a global cybersecurity skills shortage**:
  - Fortinet reported in 2021 that "*global workforce needs to grow by 65%*"
  - CSIS reported in 2019 that "*61% of orgs. felt that <50% of applicants were actually qualified for the job and only 23% of employers found the engineers' education programs to be relevant*"
  - CENSUS finds a 30% of relevant CVs for sec. eng. positions, of which 7% pass the interview process
- Product Security Assessments require **experience** in the development of modern systems
  - i.e. experience in Software Engineering, Embedded Systems and Systems Administration projects
- Product Security Assessments also require **strong technical skills** in information security
  - E.g. Source code auditing skills, reverse engineering skills etc.
- This combination of experience and skillset is more common in seniors & hobbyists (rather than graduates)

Conclusions

- When dealing with product cybersecurity vulnerabilities, **all nations stand outnumbered**
- Countries may choose to **leverage private knowledge of vulnerabilities** to conduct offensive operations (see *Vulnerabilities Equities Process* regarding *selective* disclosure)
- Countries are forced to assemble their own teams to monitor systems (and threats), **conduct independent assessments** and apply countermeasures so as to limit their exposure to new risks
- Frameworks need to be established for the **pre-market** (or procurement time) **cybersecurity evaluation** of relevant products
- Orgs. must maintain a **supply chain risk management** strategy (not just for energy supplies!)
- It is important to engage, adopt and educate on **technologies** providing **security guarantees**
- University courses that spend more time on the **development** and **assessment** of **modern systems** would significantly help grow the Product Security Assessment expert pool

CENSUS
IT Security Works

Thank You!

Follow us on Twitter
https://twitter.com/census_labs

www.census-labs.com