nic.br cgi.br

20 years cert.br

VIII NIC.br Annual Workshop on Survey Methodology

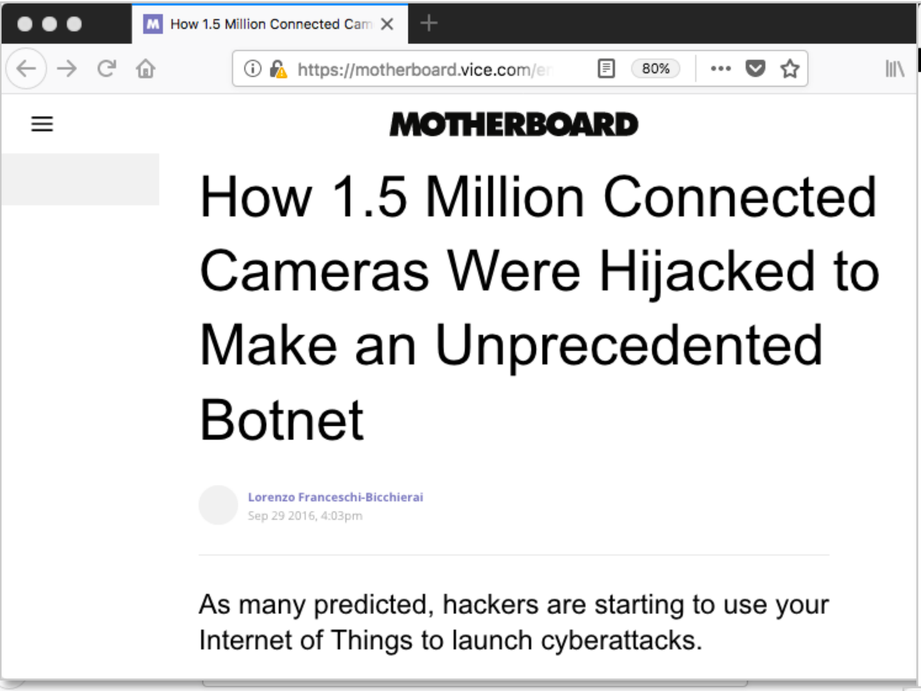
São Paulo, SP, Brazil

April 25, 2018

Cybersecurity & Privacy: Information Security

Dr. Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

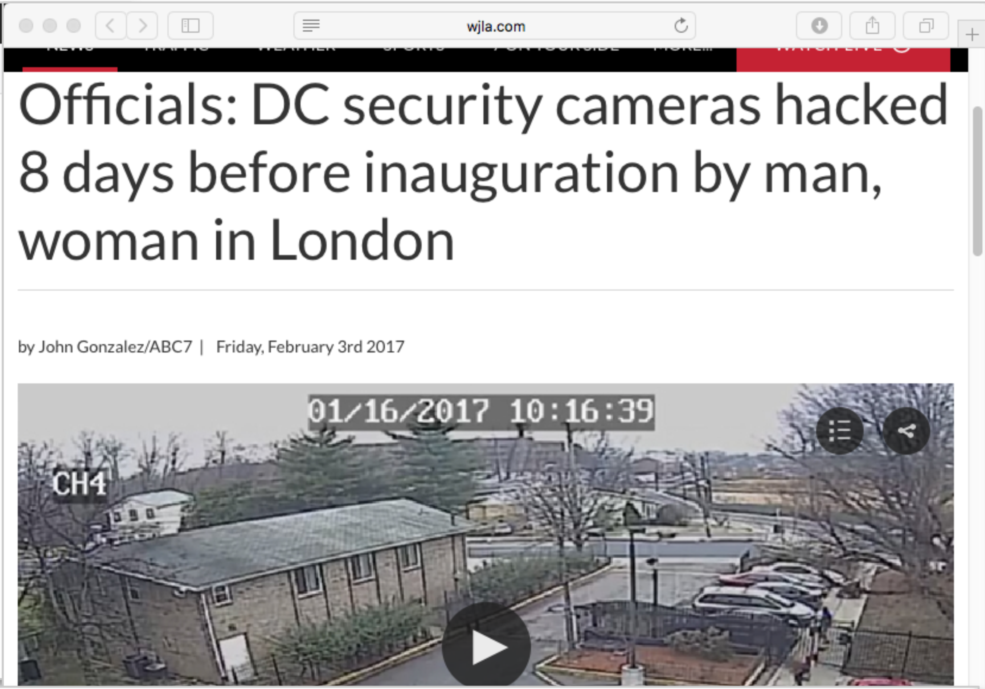
cert.br nic.br cgi.br



How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

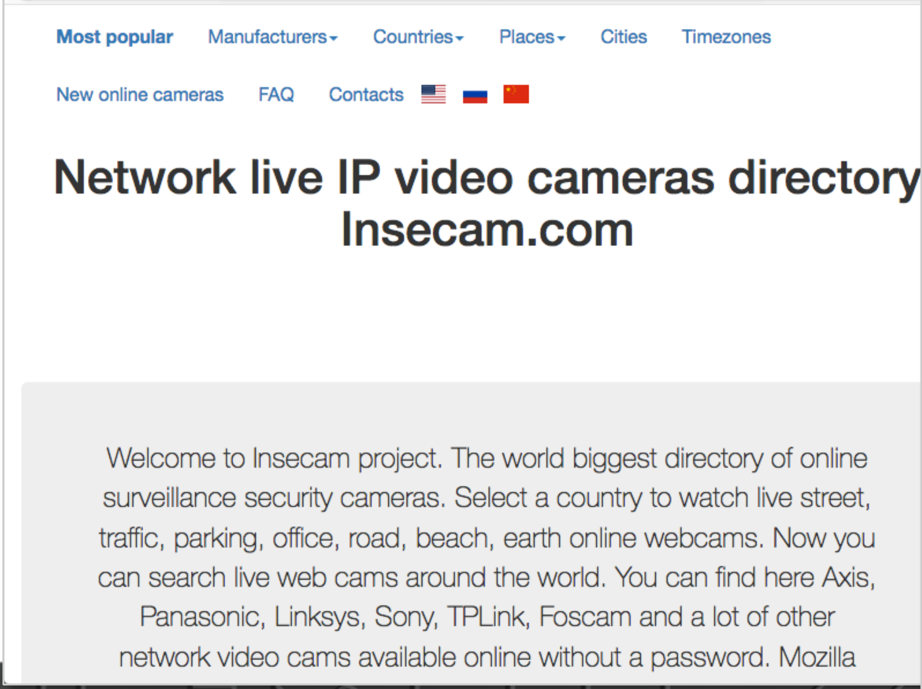
Lorenzo Franceschi-Bicchierai
Sep 29 2016, 4:03pm

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.



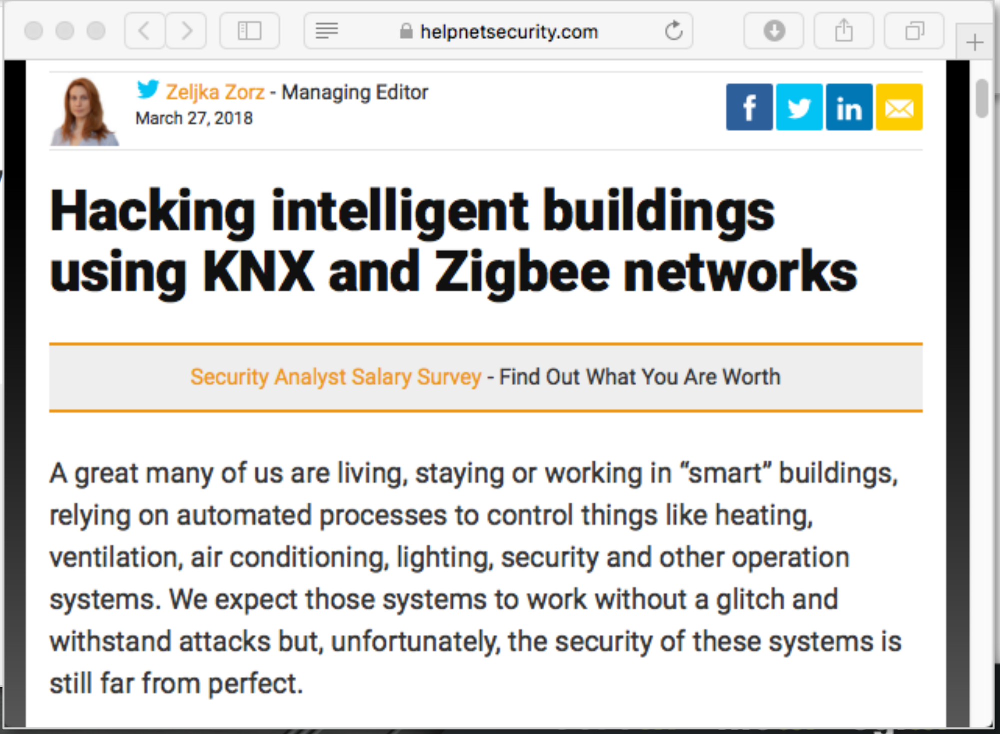
Officials: DC security cameras hacked 8 days before inauguration by man, woman in London

by John Gonzalez/ABC7 | Friday, February 3rd 2017



Network live IP video cameras directory Insecam.com

Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla

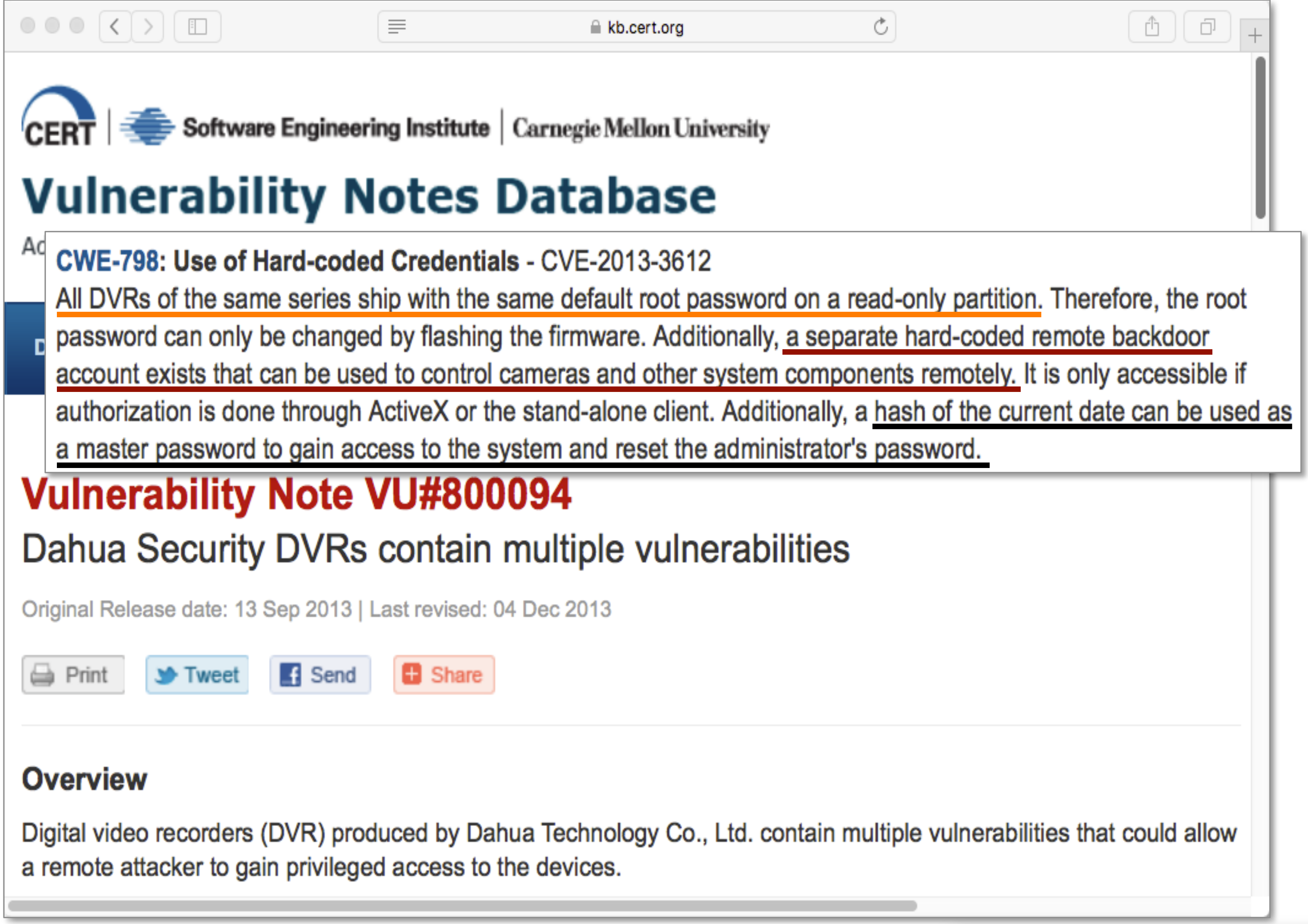


Zeljka Zorz - Managing Editor
March 27, 2018

Hacking intelligent buildings using KNX and Zigbee networks

Security Analyst Salary Survey - Find Out What You Are Worth

A great many of us are living, staying or working in “smart” buildings, relying on automated processes to control things like heating, ventilation, air conditioning, lighting, security and other operation systems. We expect those systems to work without a glitch and withstand attacks but, unfortunately, the security of these systems is still far from perfect.


kb.cert.org
CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

CWE-798: Use of Hard-coded Credentials - CVE-2013-3612

All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.

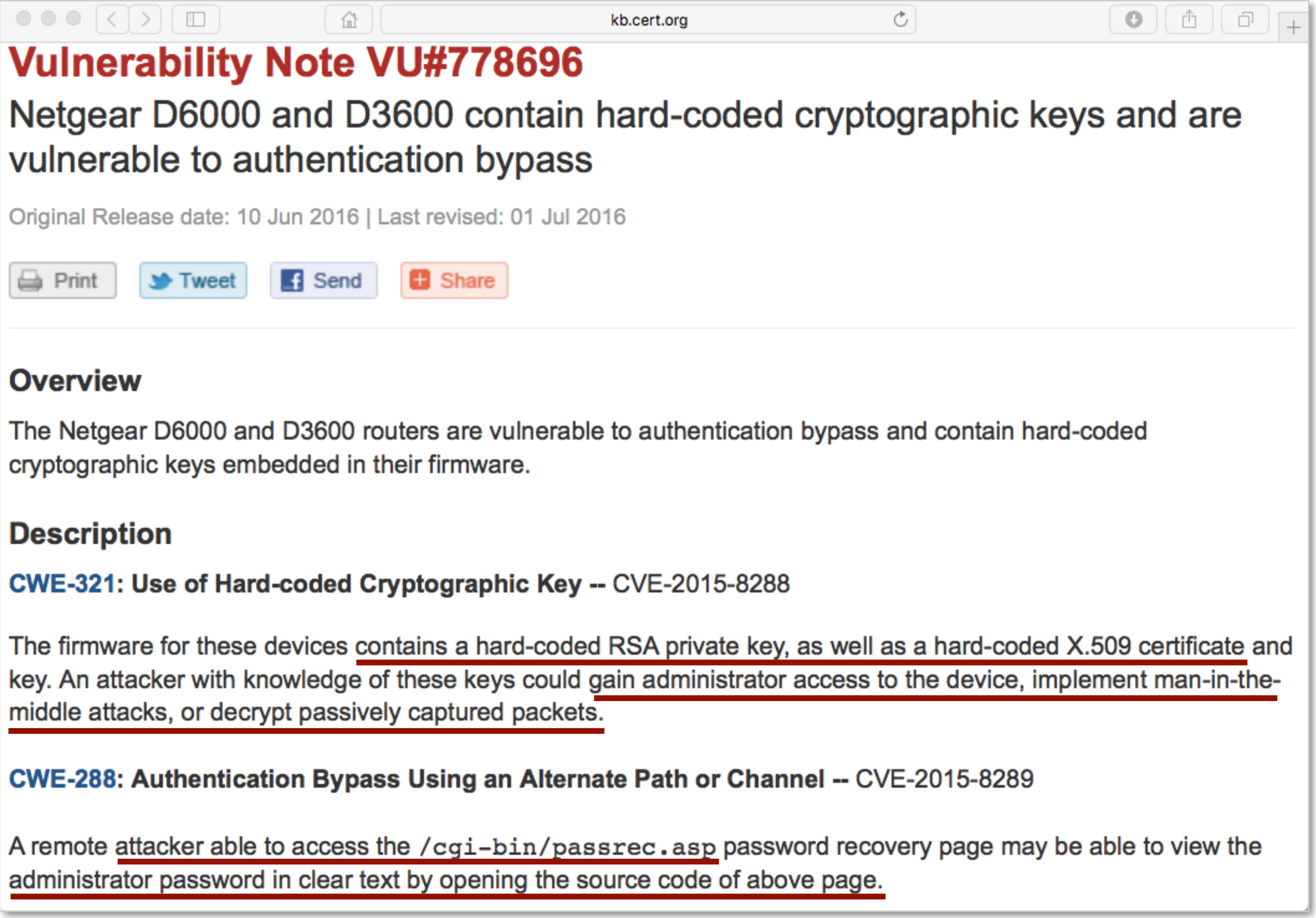
Vulnerability Note VU#800094

Dahua Security DVRs contain multiple vulnerabilities

Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013

Overview

Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.



Vulnerability Note VU#778696

Netgear D6000 and D3600 contain hard-coded cryptographic keys and are vulnerable to authentication bypass

Original Release date: 10 Jun 2016 | Last revised: 01 Jul 2016

Overview

The Netgear D6000 and D3600 routers are vulnerable to authentication bypass and contain hard-coded cryptographic keys embedded in their firmware.

Description

CWE-321: Use of Hard-coded Cryptographic Key -- CVE-2015-8288

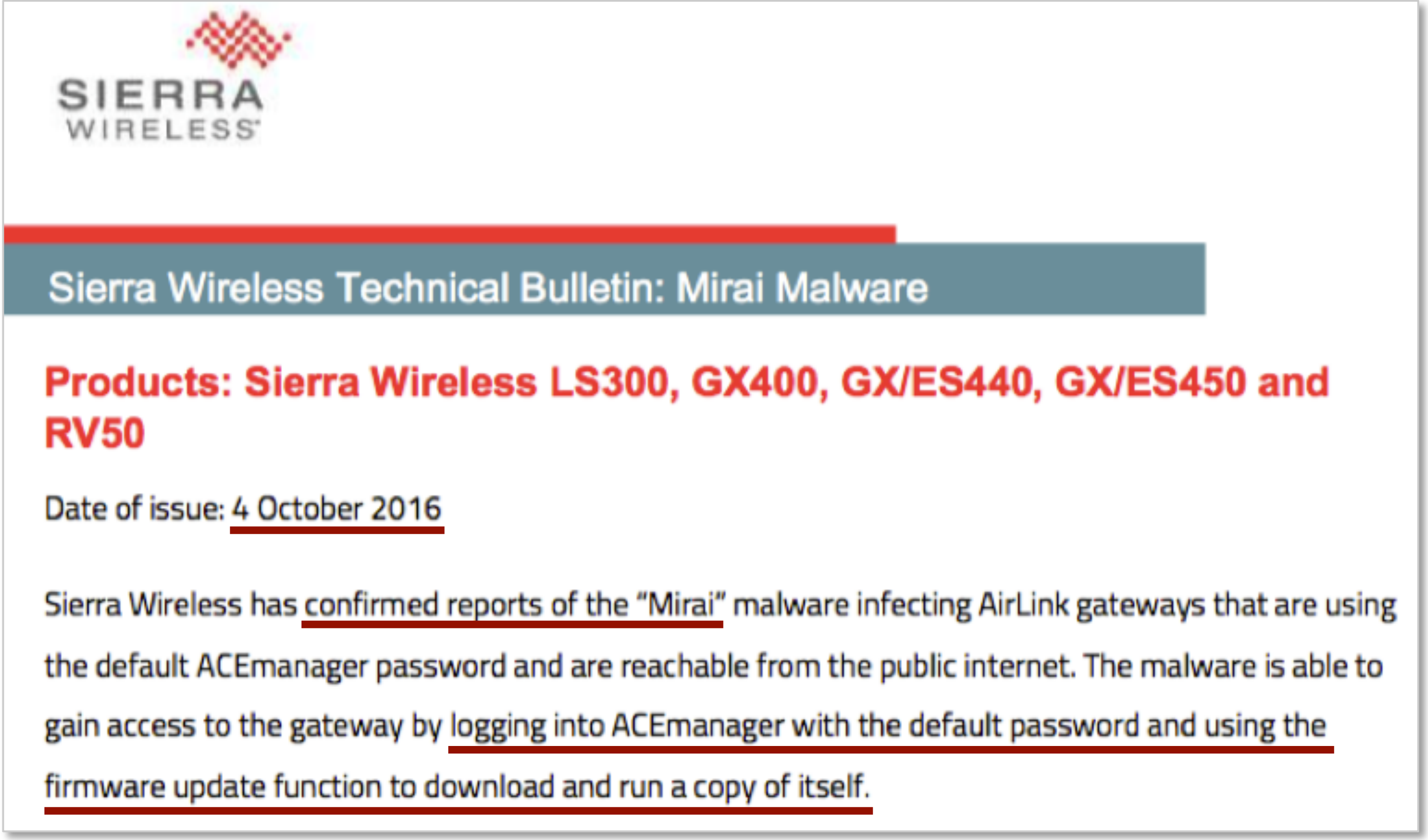
The firmware for these devices contains a hard-coded RSA private key, as well as a hard-coded X.509 certificate and key. An attacker with knowledge of these keys could gain administrator access to the device, implement man-in-the-middle attacks, or decrypt passively captured packets.

CWE-288: Authentication Bypass Using an Alternate Path or Channel -- CVE-2015-8289

A remote attacker able to access the `/cgi-bin/passrec.asp` password recovery page may be able to view the administrator password in clear text by opening the source code of above page.

4G-WiFi Gateways
Used in Critical Infrastructure Deployments

Used, among others, at: gasoducts, oleoducts, traffic lights, smart grids, police cars and ambulancies



SIERRA WIRELESS

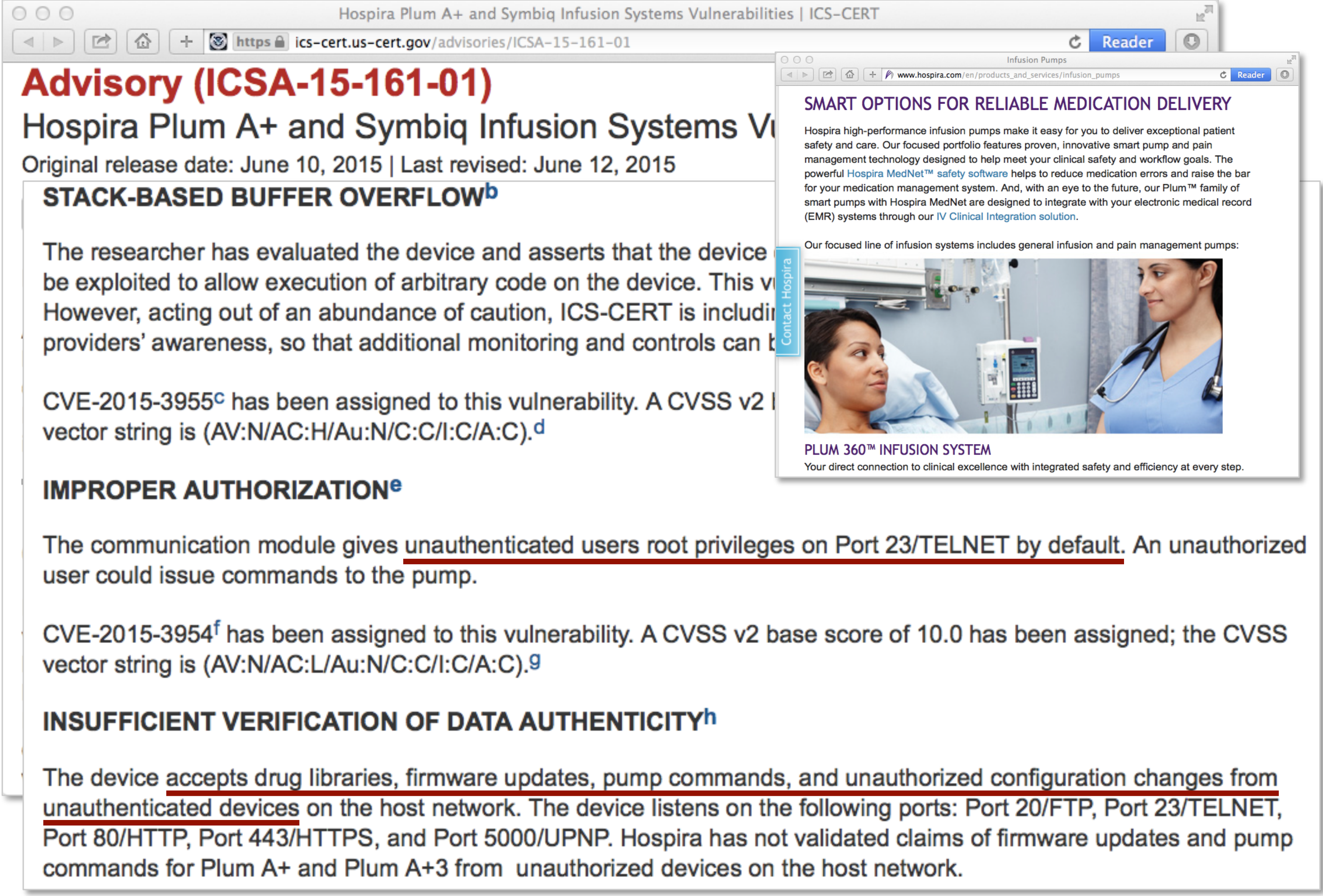
Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

Sierra Wireless has confirmed reports of the “Mirai” malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

http://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---mirai/


Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT
https ics-cert.us-cert.gov/advisories/ICSA-15-161-01
Reader

Advisory (ICSA-15-161-01)

Hospira Plum A+ and Symbiq Infusion Systems Vu

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device
be exploited to allow execution of arbitrary code on the device. This v
However, acting out of an abundance of caution, ICS-CERT is includi
providers' awareness, so that additional monitoring and controls can b

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2
vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Common ground in such diverse industries: **Old problems**

Zero concern with security

- “someone” will implement security[later]...
- firmware updates are not part of the requirements

Lack of authentication

- to connect and to receive commands
- for updates

Poor authentication and vendor “backdoors”

- default passwords, passwords of the day, “maintenance” passwords

WARNING: a wide range of industries is now develop software, but have no understanding of the process or the risks

- Patching and updates on the products’ life cicle?
- Secure Software Engineering?
- Product Security Incident Response Team?

Lots of vulnerabilities

“There is hardly anything in the world

that some man cannot

make a little worse

and sell a little cheaper,

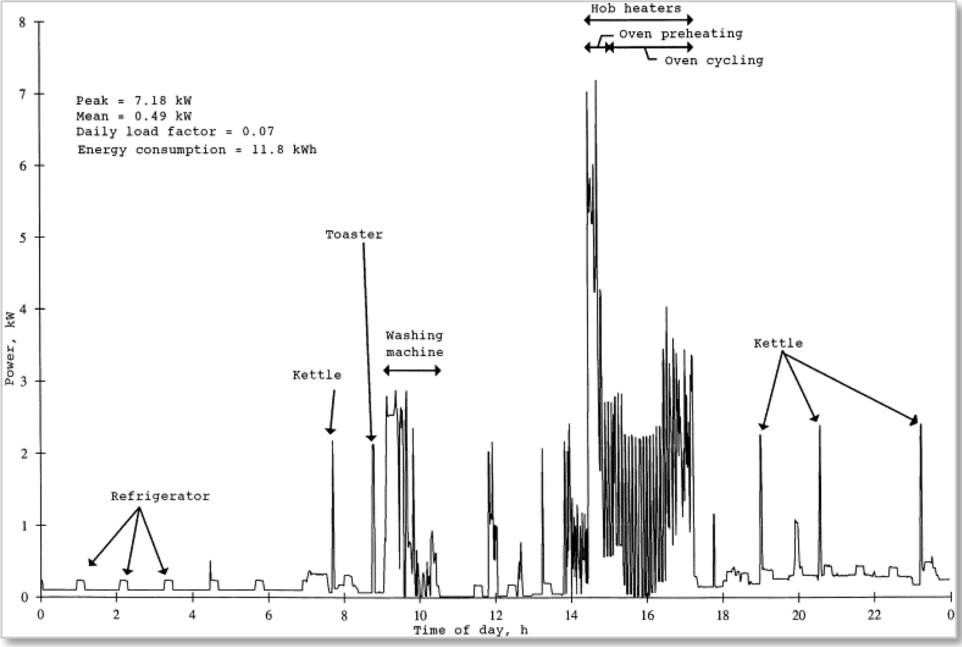
and the people who consider price only are this man's lawful prey.”

– John Ruskin(?)

Privacy Concerns

We need to consider more carefully the unintended consequences of technologies:

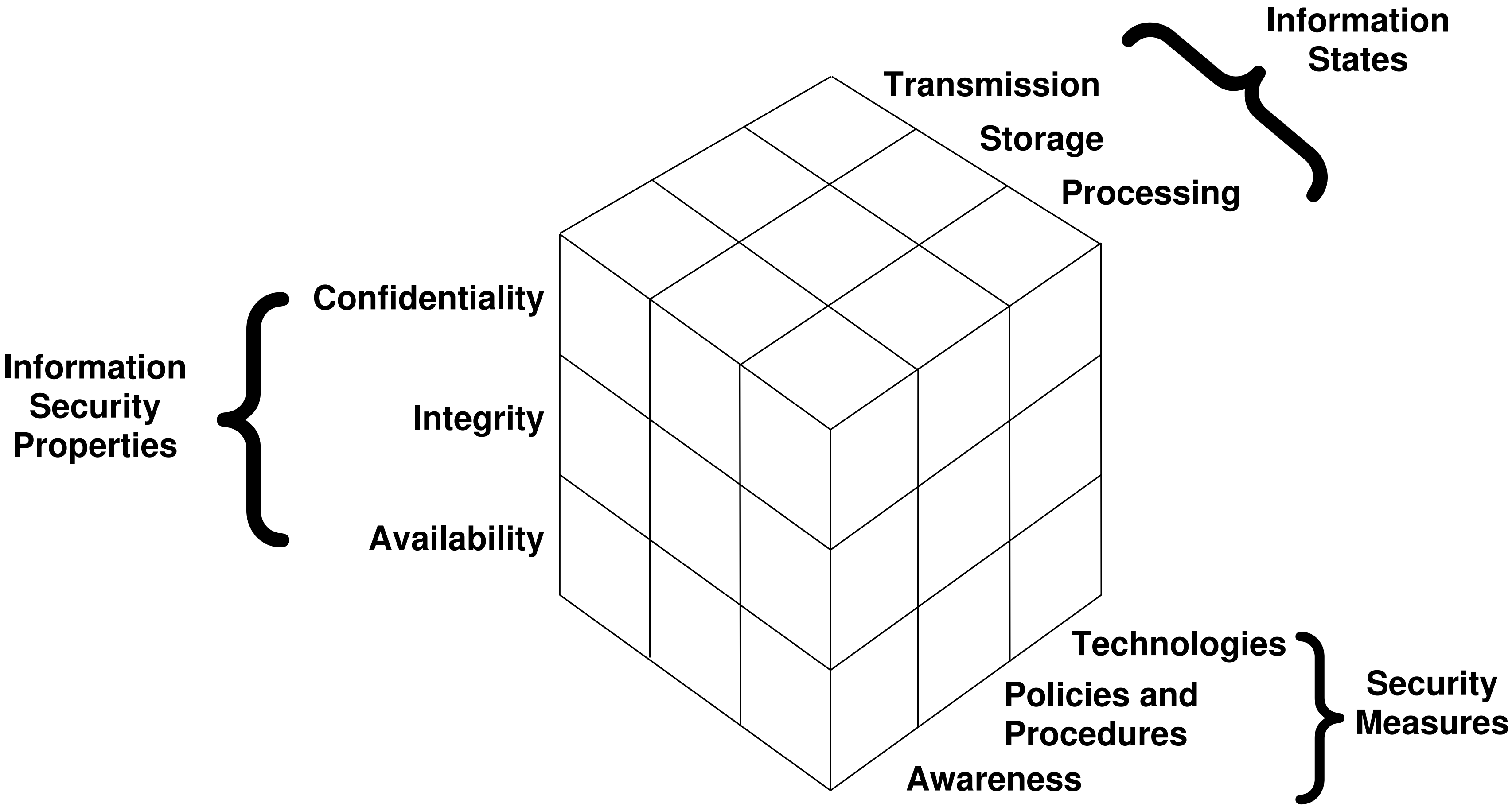
- **almost everything is now on "the cloud"**
  - voice activated services depend on it (TVs, personal assistants like "Alexa", etc)
  - centralized analysis has huge beneficial potential for sustainability and public welfare if we can have better data on energy consumption, global temperatures, traffic, health issues, etc
- **examples of privacy implications**
  - voice activated devices: everything you say is potentially public
  - fitness bands: data being sold to insurance companies
  - *smart grids*: energy consumption patters can be mapped to specific uses, easy to identify when there is someone home or traveling, for example



Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design
http://www.sciencedirect.com/science/article/pii/S0378778802002414

What is Information Security?

Information resides in multiple places and its security depends on multiple factors



Information States

Transmission

Storage

Processing

Information Security Properties

Confidentiality

Integrity

Availability

Security Measures

Technologies

Policies and Procedures

Awareness

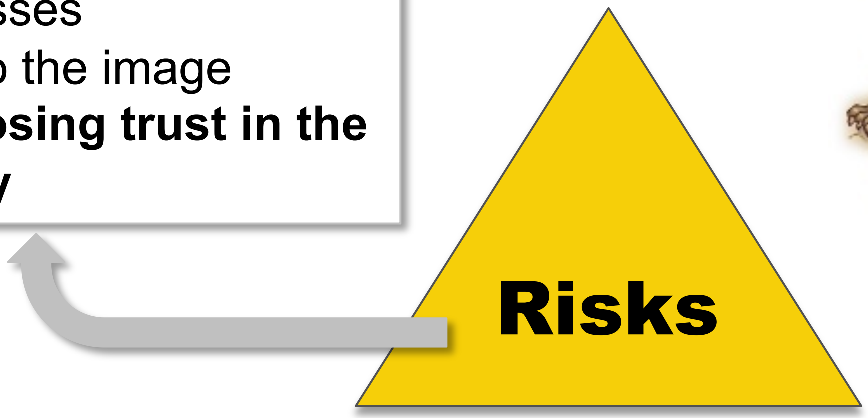
McCumber Information Security Model

http://www.ibm.com/developerworks/security/library/s-confnotes2/

Risks are inherent to systems/devices connected to the Internet

- unavailability
- privacy breaches
- data leak
- financial losses
- damages to the image
- **society loosing trust in the technology**

Internet Connected Systems



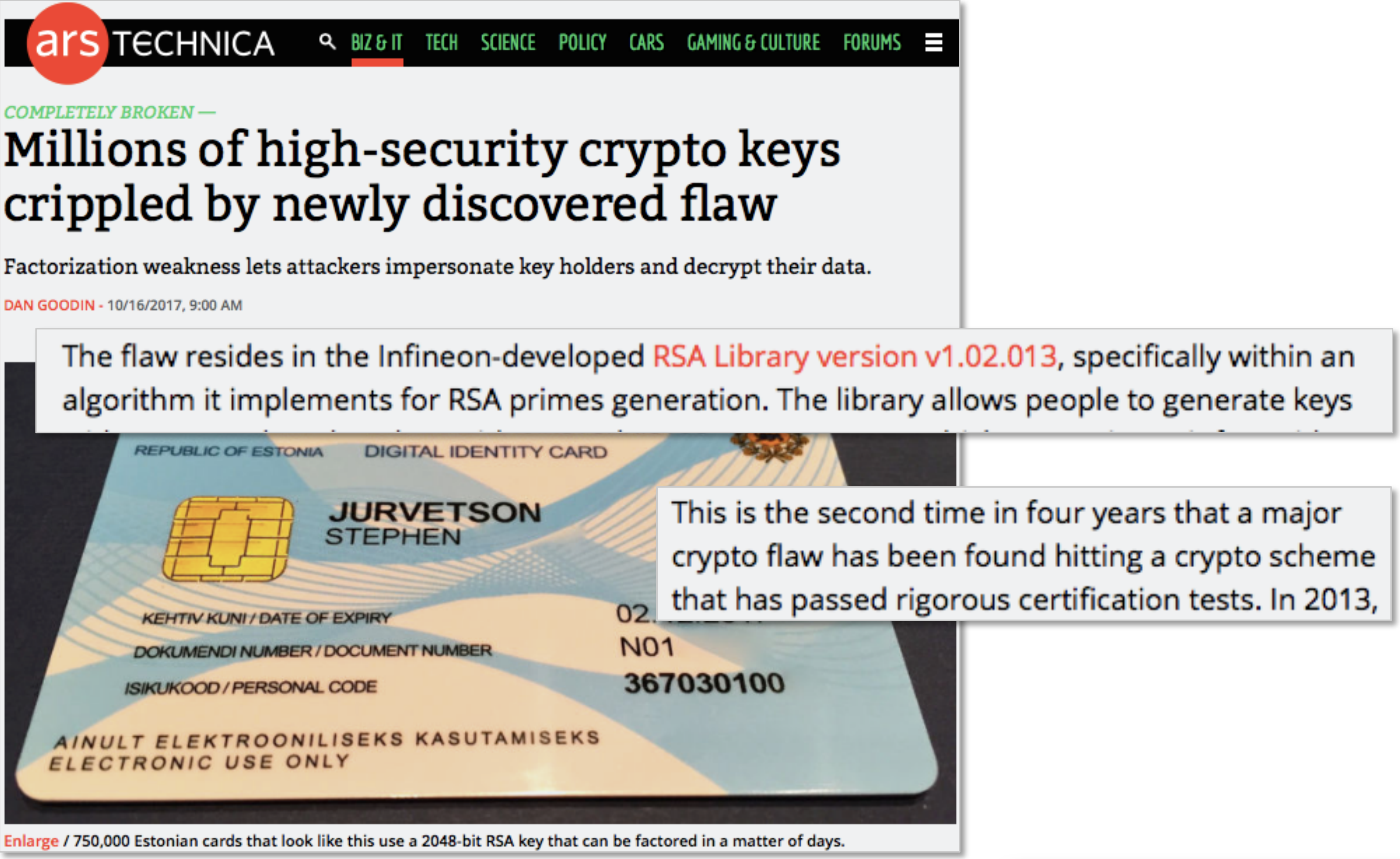
Attackers

- criminals
- industrial espionage
- nation states
- vandals

Vulnerabilities

- project does not consider security requirements
- software defects
- configuration errors
- inadequate use
- weaknesses due to the systems' complexity

Even “Secure and Certified” Products Fail



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

COMPLETELY BROKEN —

Millions of high-security crypto keys crippled by newly discovered flaw

Factorization weakness lets attackers impersonate key holders and decrypt their data.

DAN GOODIN - 10/16/2017, 9:00 AM

The flaw resides in the Infineon-developed RSA Library version v1.02.013, specifically within an algorithm it implements for RSA primes generation. The library allows people to generate keys

This is the second time in four years that a major crypto flaw has been found hitting a crypto scheme that has passed rigorous certification tests. In 2013,

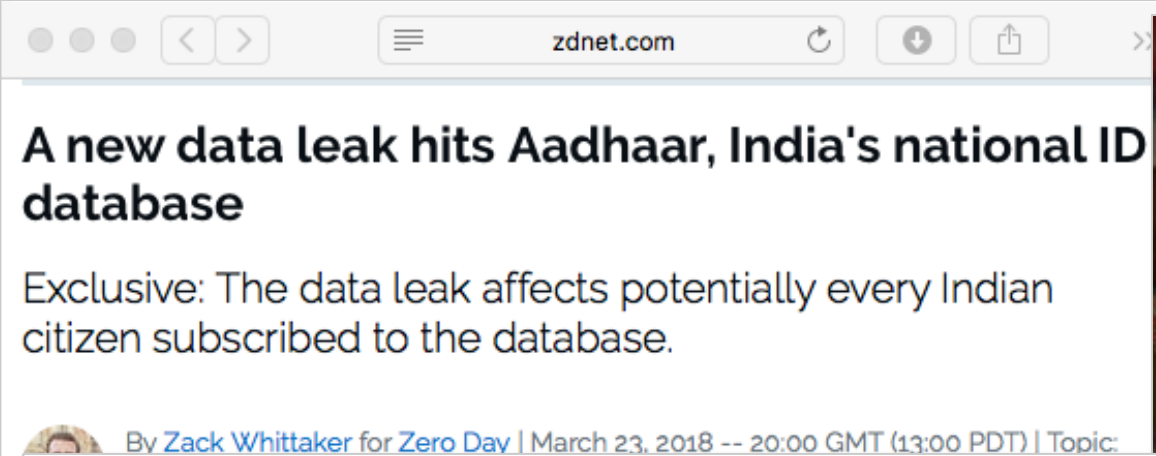
REPUBLIC OF ESTONIA
DIGITAL IDENTITY CARD
JURVETSON
STEPHEN
KEHTIV KUNI / DATE OF EXPIRY
02.
DOKUMENDI NUMBER / DOCUMENT NUMBER
N01
ISIKUKOOD / PERSONAL CODE
367030100
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Enlarge / 750,000 Estonian cards that look like this use a 2048-bit RSA key that can be factored in a matter of days.

“... the real security challenge is not the mathematics of cryptosystems; it is engineering, specifically the design and implementation of complex software systems.”

– *Keys Under Doormats,* Abelson et. al

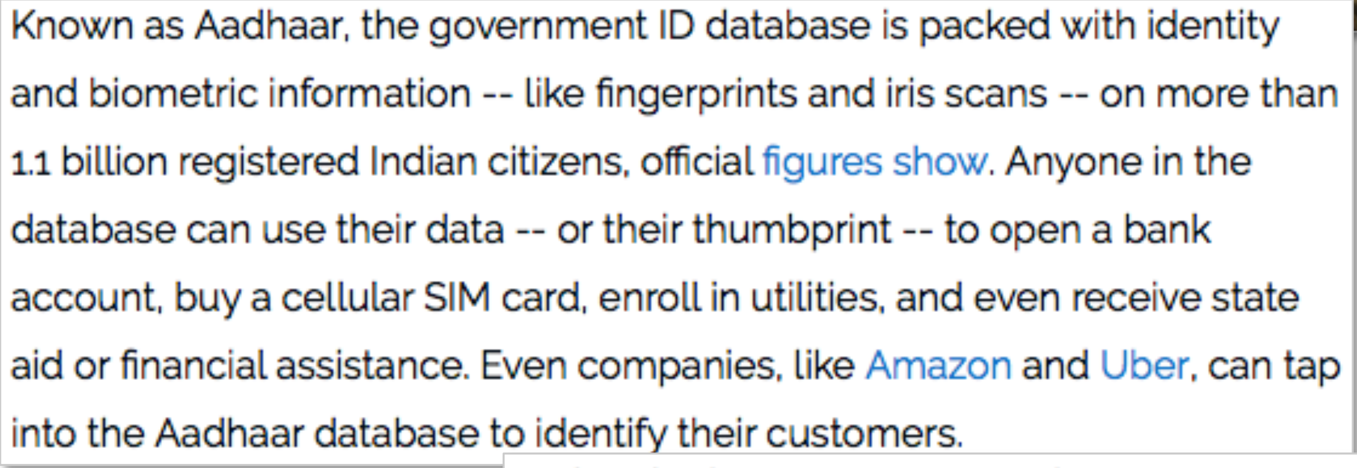
http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf



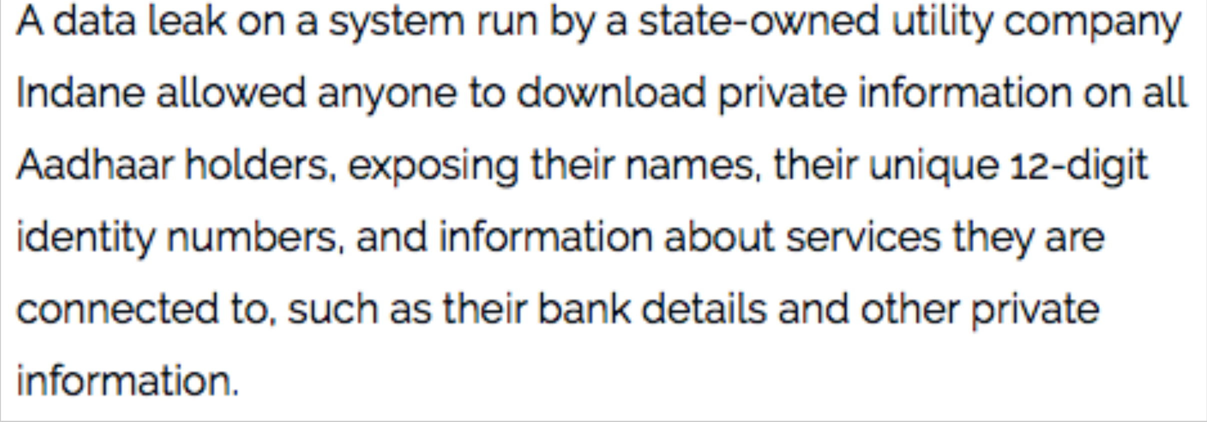
A new data leak hits Aadhaar, India's national ID database

Exclusive: The data leak affects potentially every Indian citizen subscribed to the database.

By Zack Whittaker for Zero Day | March 23, 2018 -- 20:00 GMT (13:00 PDT) | Topic:



Known as Aadhaar, the government ID database is packed with identity and biometric information -- like fingerprints and iris scans -- on more than 1.1 billion registered Indian citizens, official figures show. Anyone in the database can use their data -- or their thumbprint -- to open a bank account, buy a cellular SIM card, enroll in utilities, and even receive state aid or financial assistance. Even companies, like Amazon and Uber, can tap into the Aadhaar database to identify their customers.



A data leak on a system run by a state-owned utility company Indane allowed anyone to download private information on all Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and information about services they are connected to, such as their bank details and other private information.

What about metrics?

What can surveys measure?

Compliance to standards (ISO, COBIT, ITIL, etc)?

- Do you have policies?
- Do you have X or Y procedures?

Perception of security problems?

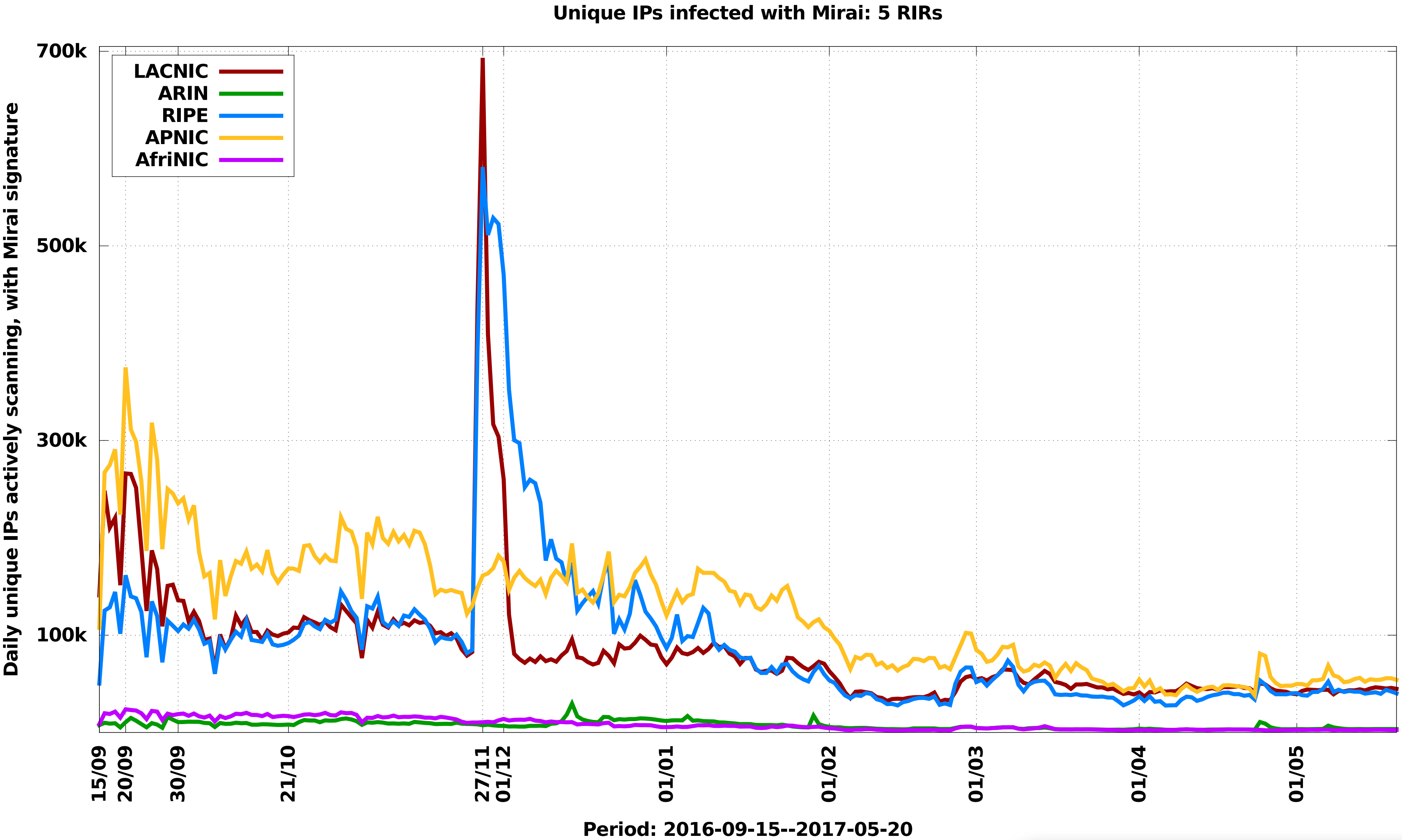
- How many incidents did you have?

  (What about those that were not detected?)

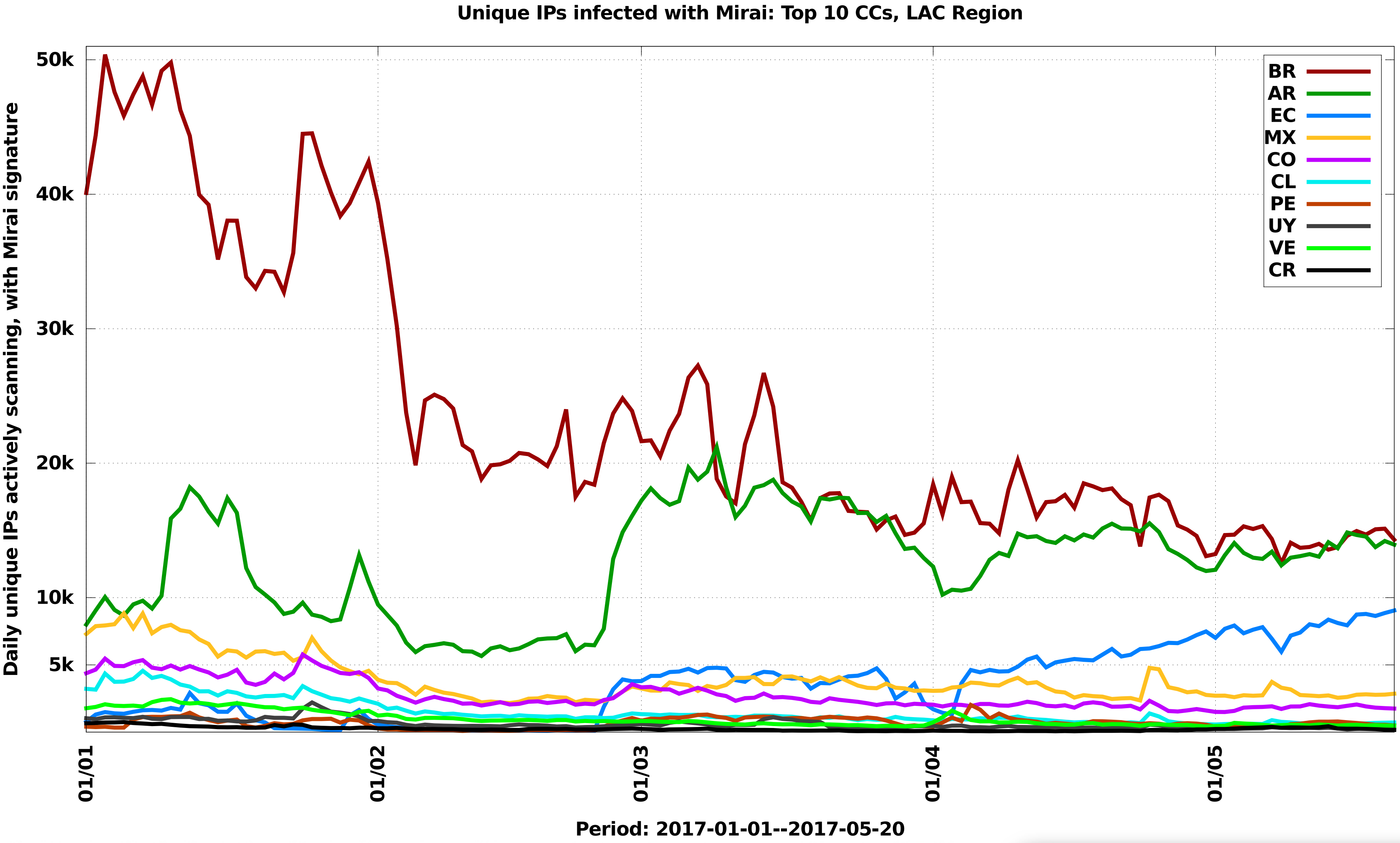
Challenges

- You can’t measure what you don’t know
  - In security almost everything that fails is part of the unknowns
- Compliance ≠ Security
- Certification does not apply to software
  - it is possible to certify maturity processes
  - software is bound to have bugs and defects
    - a percentage will bring security issues

CERT.br Passive Metrics of Internet Health:
Mirai botnet propagation (1/2)



CERT.br Passive Metrics of Internet Health: **Mirai botnet propagation (2/2)**



Challenges for the Future

Professional qualification

- Networking, system administration, information security, **secure software development**

Although proposed by some "experts", device certification is a bad idea

- There is no way to certify software (firmware is software)

Vulnerabilities will always exist

- How one handles them is the important point

We need a global discussion about maturity and security requirements for device manufacturers

- ALL products need a software/firmware update lifecycle
- ALL companies need a PSIRT (*Product Security Incident Response Team*) or at least a well defined contact for product security issues
  - References:
    - *FIRST PSIRT Services Framework* https://first.org/education/Draft_FIRST_PSIRT_Service_Framework_v1.0
    - *The Building Security In Maturity Model* https://www.bsimm.com/

Security is inheritably multistakeholder: **Cooperation for a Healthy Ecossystem**

No organization or agency alone will be able to secure the digital environment − everyone has a role

- academia
  - needs to include security thinking in all disciplines
  - secure development has to be a priority from the beginning
- developers / companies
  - security needs to be a requirement from early development stages
- managers / executives
  - think about security as in investment and allocate appropriate resources
- system and network administrators and security professionals
  - care about which type of traffic is leaving your network
    - mindset: do no harm, do not pollute the Internet
  - adopt best current practices
- end users
  - understand the risks and follow security practices
  - keep all devices updated and apply all patches

“The stability, security and overall functionality of the network must be actively preserved through the adoption of technical measures that are consistent with international standards and encourage the adoption of best practices.”

– Principle 8: Functionality, security and stability
Principles for the Governance and Use of the Internet, CGI.br

Thank You

www.cert.br

@ cristine@cert.br   @certbr

April 25, 2018

20 anos cert.br

nic.br   cgi.br

www.nic.br | www.cgi.br