Business in the Robot Age

Or, money can’t buy you love but it certainly helps with the actuators
Never chase headlines or ambulances

It takes 5-10 years to make an overnight success
disruption is much easier than it looks
web, mobile, things, you
Margins on physical things
Software is sweet
Erle-Spider
app store included

http://igg.me/at/erle-spider/x/7817776
snapcraft
name: timesink
version: 0.1
summary: NTP server with GPS support
description: |
   A snap that uses your GPS to provide a long-term accurate time service with NTP. If your GPS provide a "pulse per second" (PPS) signal, then the time can be accurate to microseconds.

parts:
gpsd:
   type: scons
   source: http://download-mirror.savannah.gnu.org/releases/gpsd/gpsd-3.15.tar.gz
   source-type: tar
   stage-packages: [ libncurses5-dev, ]
ntpd:
   type: autotools
   source: http://www.eecis.udel.edu/~ntp/ntp_spool/ntp4/ntp-dev/ntp-dev-4.3.72.tar.gz
   source-type: tar
parts:
spider:
  plugin: catkin
  source: ./software/

catkin-packages:
[ demos, joy, kdl_parser, orocos_kdl, ps3joy,
  spider_body_kinematics, spider_gait, spider_imu,
  spider_imu_dev, spider_joint_publisher,
  spider_leg_kinematics, spider_maestro_controller,
  spider_msgs, spider_teleop_joy, urdf,
  urdf_parser_plugin ]

stage-packages: [ bluez, cmake, joystick, libeigen3-dev, liburdfdom-dev,
  liburdfdom-headers-dev, libusb-dev, pkg-config, python-bluez,
  ros-indigo-xacro, libgtest-dev ]
Which comes to consumers first?
Autonomous driving or autonomous flying?

@ErleRobotics, make #ubuntu #erlespider go

backwards

forward
Services are sweeter!

Pay for what you use, not the tools.
Services businesses emphasize field ops

... and best alignment to customer interests
Transactional update and rollback
for the OS and kernel and applications, individually
any package can write to any file

filesystem

read-only snaps

writable spaces per snap

app snap

app writable area

app snap

app writable area

os writable files

os snap

kernel config

kernel snap
Anthropomorphic or functional?

@ErleRobotics, make
#ubuntu #erlespider go

backwards

forward
Data can be difficult

And potentially a liability
Security can be even more difficult!
In blunder threatening Windows users, D-Link publishes code-signing key

Leak of private key could give malware easier entry onto Windows computers.

by Dan Goodin - Sep 18, 2015 6:15pm BST

In a ham-fisted move that threatens computer users everywhere, developers at router manufacturer D-Link published a private cryptography key used to certify that software is trustworthy and not malware, a security researcher said.

The software signing key was released in late February on D-Link’s GPL source code sharing website, along with the source code from some of the company’s firmware. Yoanath Klijnmsa, a threat intelligence analyst at Dutch security firm Fox IT, told Ars in an e-mail. D-Link used the key to cryptographically sign its software so it could be installed on computers running Microsoft Windows without the operating system generating a security warning. With it leaked to the world, anyone—including developers of keystloggers, remote access trojans, and other types of malware—could use the key to sign their malicious wares as they’d accepted as trusted D-Link software.

It’s not unusual for malware providers to steal or otherwise appropriate valid signing keys to give their wares the appearance of legitimacy. Stuxnet, the computer worm jointly developed by the US and Israel to sabotage Iranian nuclear centrifuges, was among the early cases of malware to be signed this way. Since then, code signing has become almost standard practice among upper-tier malware distributors. Normally, malicious developers must hack a legitimate certificate holder and acquire the underlying private key. D-Link, it seems, may have saved bad guys this extra step by openly publishing its signing key and allowing it to remain online for seven months. The story was reported earlier by Techers.

The key expired earlier this month, but Klijnmsa said that any software that was signed before the expiration date could still work.

---

LATEST FROM ARS TECHNICA/UK

New rights for UK consumers buying digital content come into force

THE JINNY CAB IS NEAR!

Self-driving taxis take to Japan’s roads next year

TOO MUCH?

Oculus Rift will cost over $350 so there are “no compromises,” says founder

Battle for Zendikar review: Lovecraftian horror comes to Magic: The Gathering

IMAX with laser: Superb contrast, 4K resolution, and huge colour gamuts

LATEST FEATURE STORY

Huawei’s first Android Wear watch is a beautiful yet basic timepiece

Review: It looks great on the outside, but it’s still Google’s OS on the inside.
Internet of Things vigilante malware strikes tens of thousands of devices - to protect them

Linux Wifatch: A force for good or evil?


Researchers are puzzling over the Linux Wifatch malware -- sophisticated code which appears to help secure IoT devices, and yet also forces infected devices to a peer-to-peer network of infected systems.

On Thursday, Symantec researchers revealed their research into the activity of Wifatch, a peculiar piece of code which does not replicate the usual activities of malware such as bricking systems, conducting surveillance or stealing data.
Apps are contained and isolated.
and speaking of contained and isolated...
Should sex with robots be legal?

@ErleRobotics, make
#ubuntu #erlespider go

backwards

forward
Never underestimate porn entertainment
The Internet of Toys
FOCUS