new foundations for trust and the web

Rich Demillo

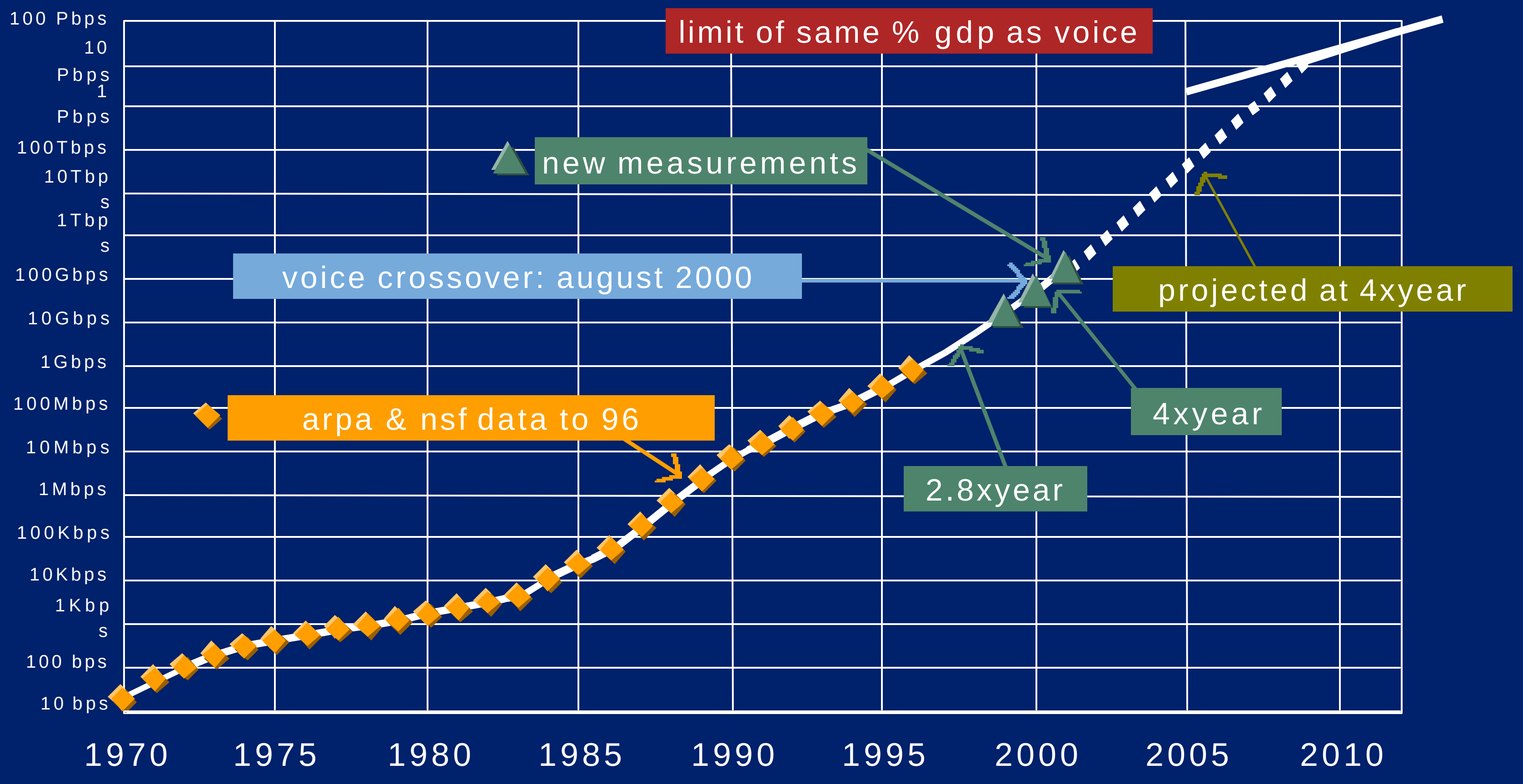
vice president, technology strategy

may 10, 2002

invent

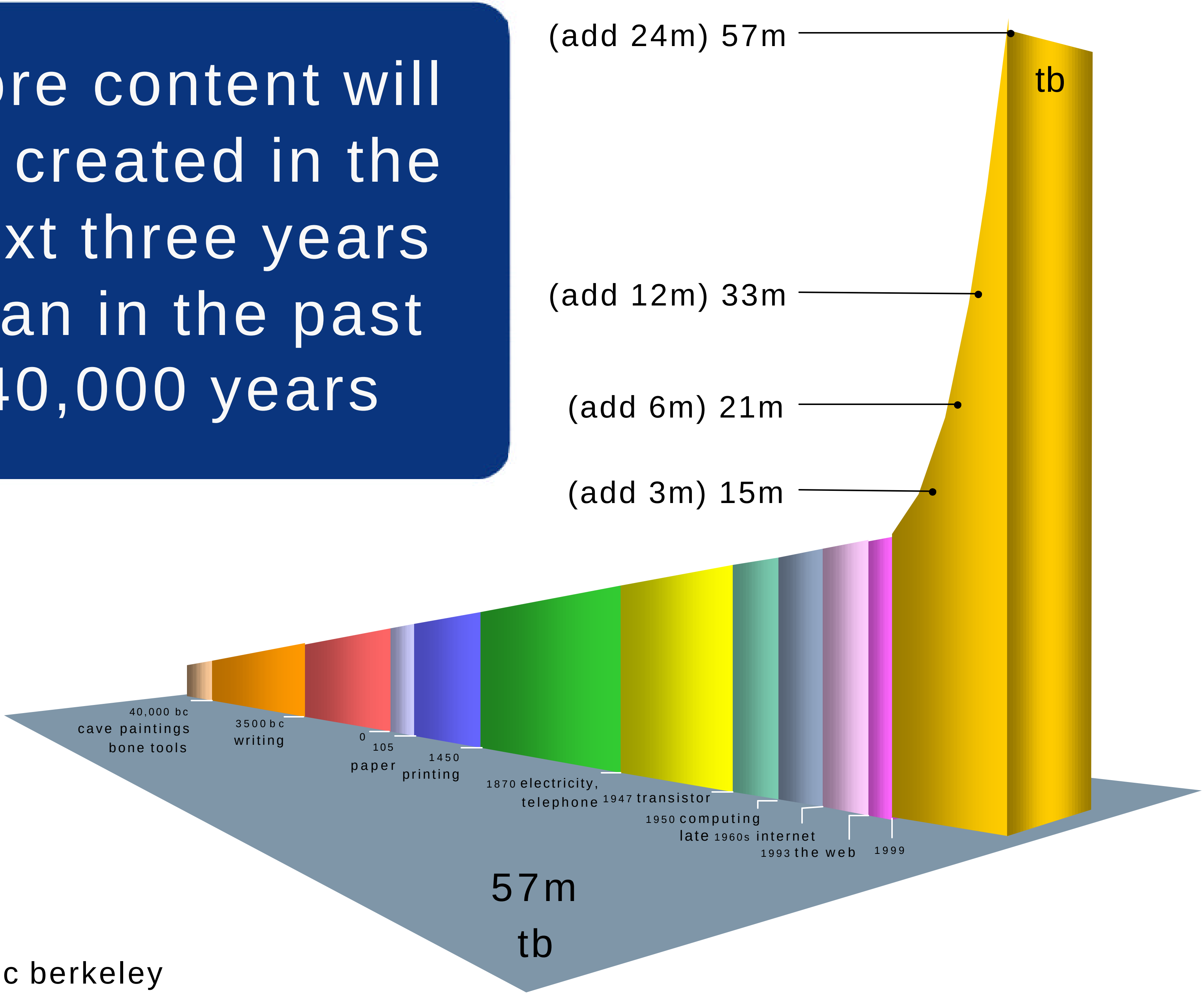
COMPAQ

total US internet traffic



source: roberts et al., 2001

more content will be created in the next three years than in the past 40,000 years



source: uc berkeley

elements of trust in IT

- authentication
- content
- capability
- context
- service quality
  - dependability
  - security
  - privacy
  - data integrity

what are the limitations of trust today?

- steel doors in paper walls
- ad hoc leads to patch-and-fill
- managing security does not scale
- technology islands
- public/private infrastructure
- privacy protection is not embedded in technology
- sept. 11

why look to IT infrastructure and the network to build trust?

- chain of trust must be grounded in infrastructure
- IT is agnostic
- bridges public and private infrastructure

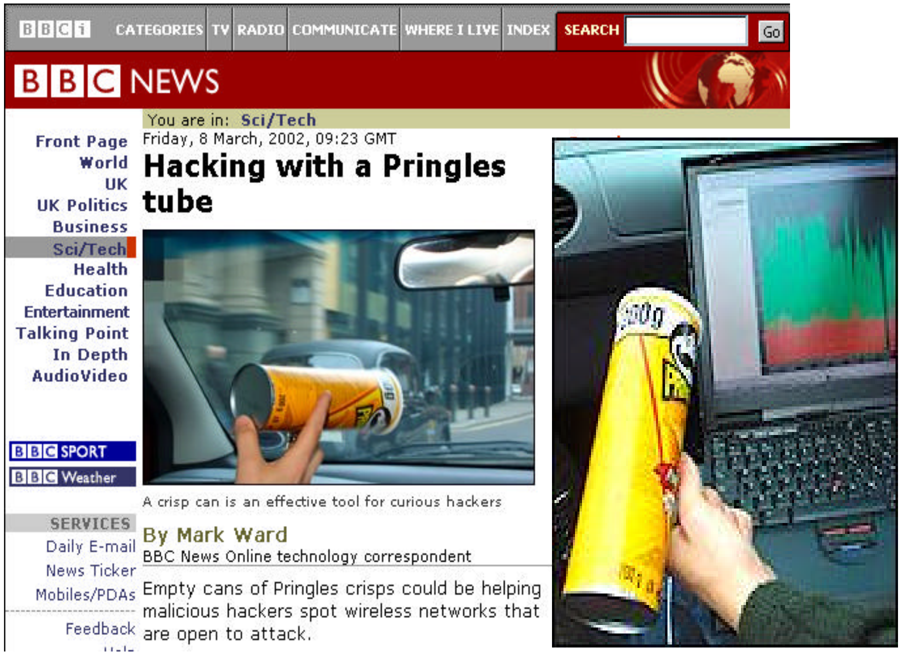
converging IT landscape

- mobility
- web-services
- the grid
- semantic web
- … a common thread for success is …

trust

… as table stakes

mobility



You are in: Sci/Tech

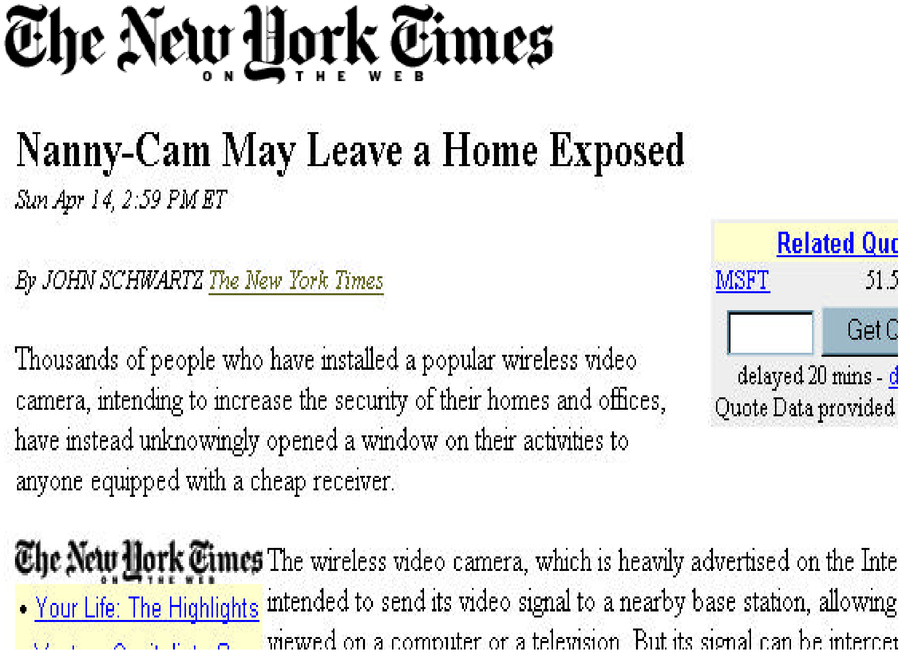
Friday, 8 March, 2002, 09:23 GMT

Hacking with a Pringles tube

A crisp can is an effective tool for curious hackers

By Mark Ward
BBC News Online technology correspondent

Empty cans of Pringles crisps could be helping malicious hackers spot wireless networks that are open to attack.



Nanny-Cam May Leave a Home Exposed

Sun Apr 14, 2:59 PM ET

By JOHN SCHWARTZ The New York Times

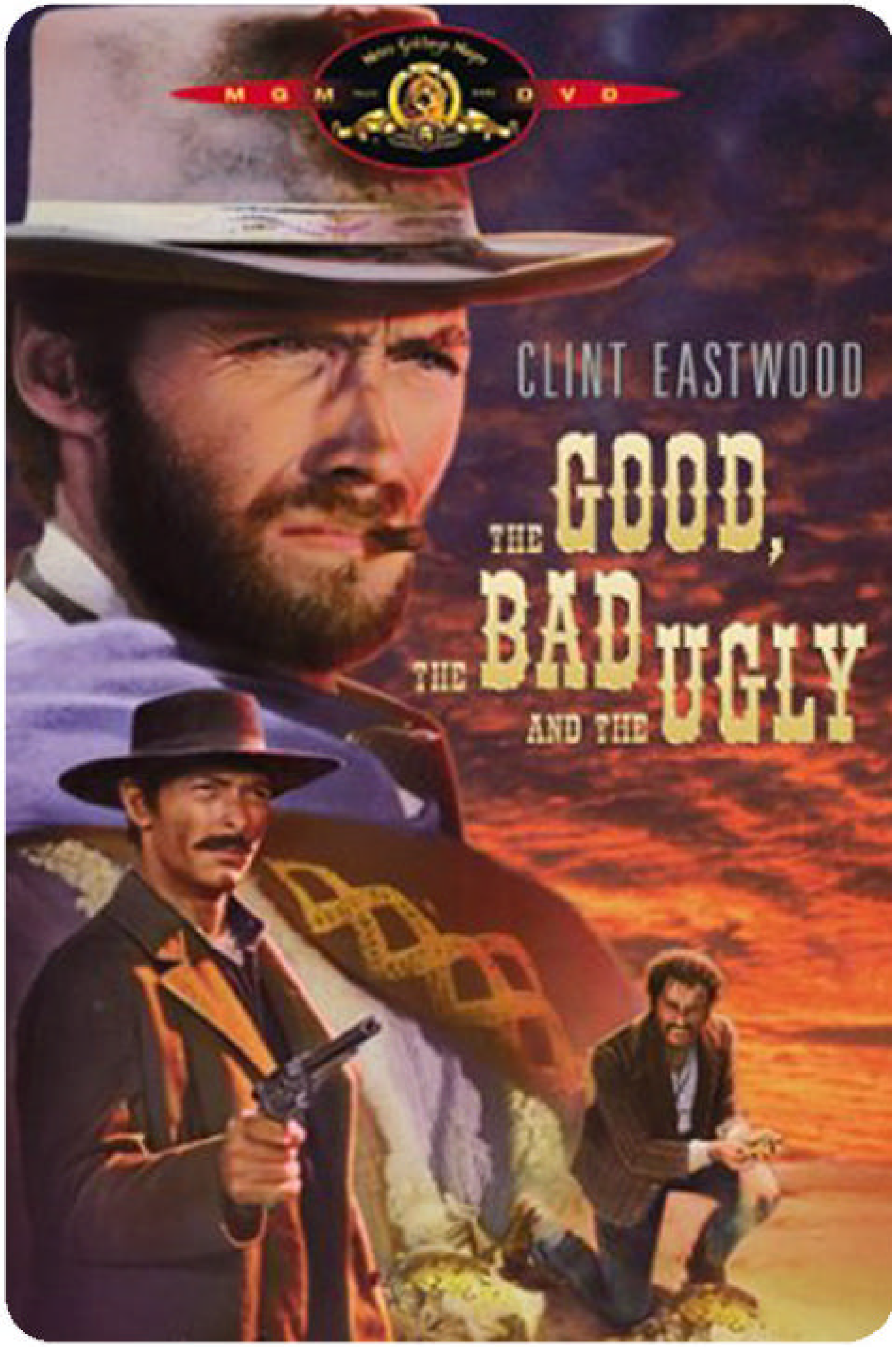
Thousands of people who have installed a popular wireless video camera, intending to increase the security of their homes and offices, have instead unknowingly opened a window on their activities to anyone equipped with a cheap receiver.

delayed 20 mins - d
Quote Data provided

The wireless video camera, which is heavily advertised on the Inte intended to send its video signal to a nearby base station, allowing viewed on a computer or a television. But its signal can be intercep

web-services

- the new e-commerce frontier
- big players…lots of potential outlaws
- trust can either fuel or inhibit growth



the grid

- distributed resource sharing requires new approaches
- a chain of trust limits threats as opposed to trying to lock them out

semantic web

- trusting the web's native language
- the web as a single global database
- authentication and credibility are critical
- context driven notions of trust

establishing a chain of trust

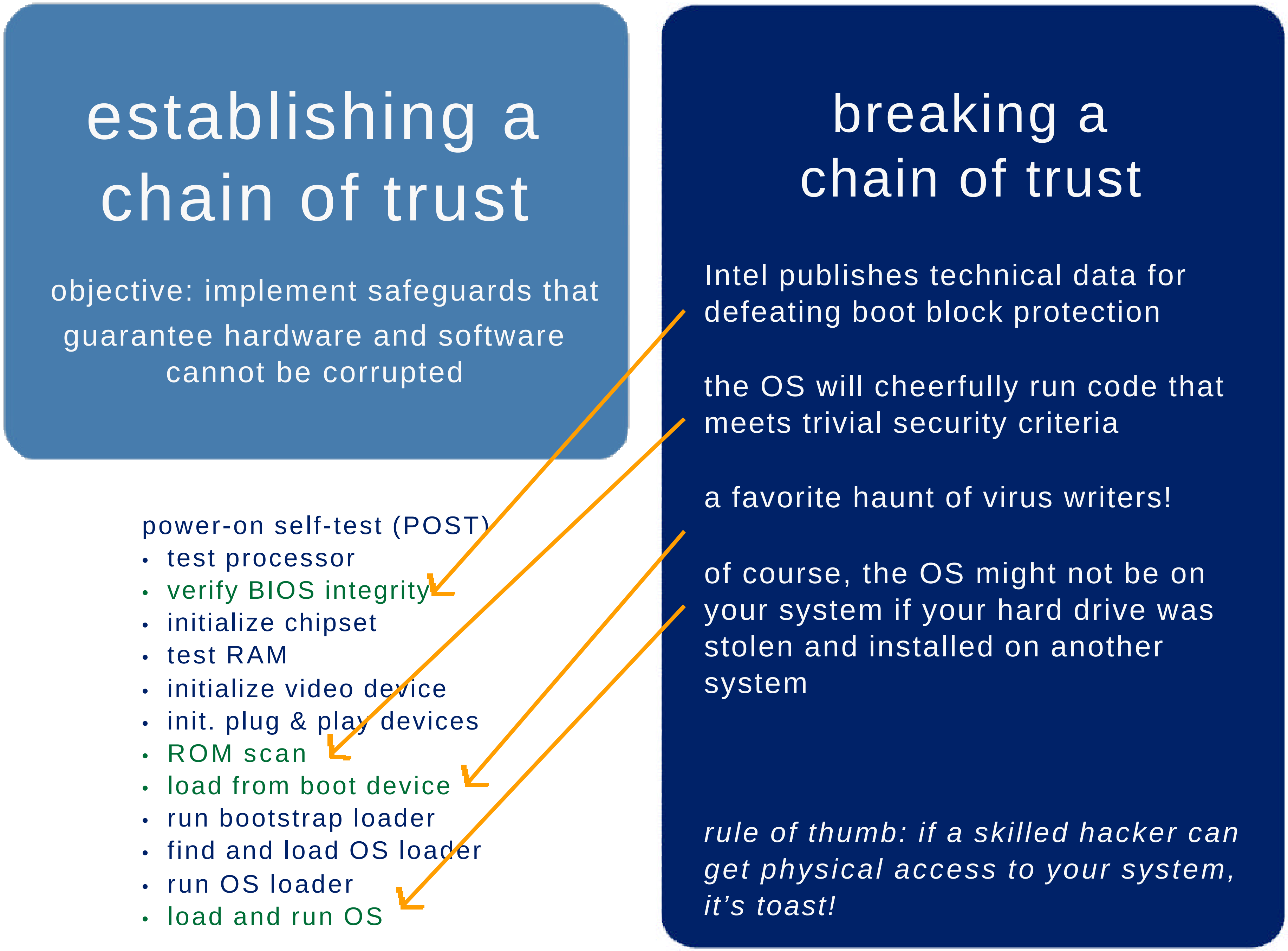
objective: implement safeguards that guarantee hardware and software cannot be corrupted

power-on self-test (POST)

- test processor
- verify BIOS integrity
- initialize chipset
- test RAM
- initialize video device
- init. plug & play devices
- ROM scan
- load from boot device
- run bootstrap loader
- find and load OS loader
- run OS loader
- load and run OS

overview:

- a chain of trust begins with a component or condition that is assumed to be secure
- the secure component is responsible for authenticating the next component in the chain before executing it
- each subsequent component authenticates the next component in sequence
- ultimately, the chain of trust must extend all the way to the user to guarantee security



establishing a chain of trust

objective: implement safeguards that guarantee hardware and software cannot be corrupted

power-on self-test (POST)

- test processor
- verify BIOS integrity
- initialize chipset
- test RAM
- initialize video device
- init. plug & play devices
- ROM scan
- load from boot device
- run bootstrap loader
- find and load OS loader
- run OS loader
- load and run OS

breaking a chain of trust

Intel publishes technical data for defeating boot block protection

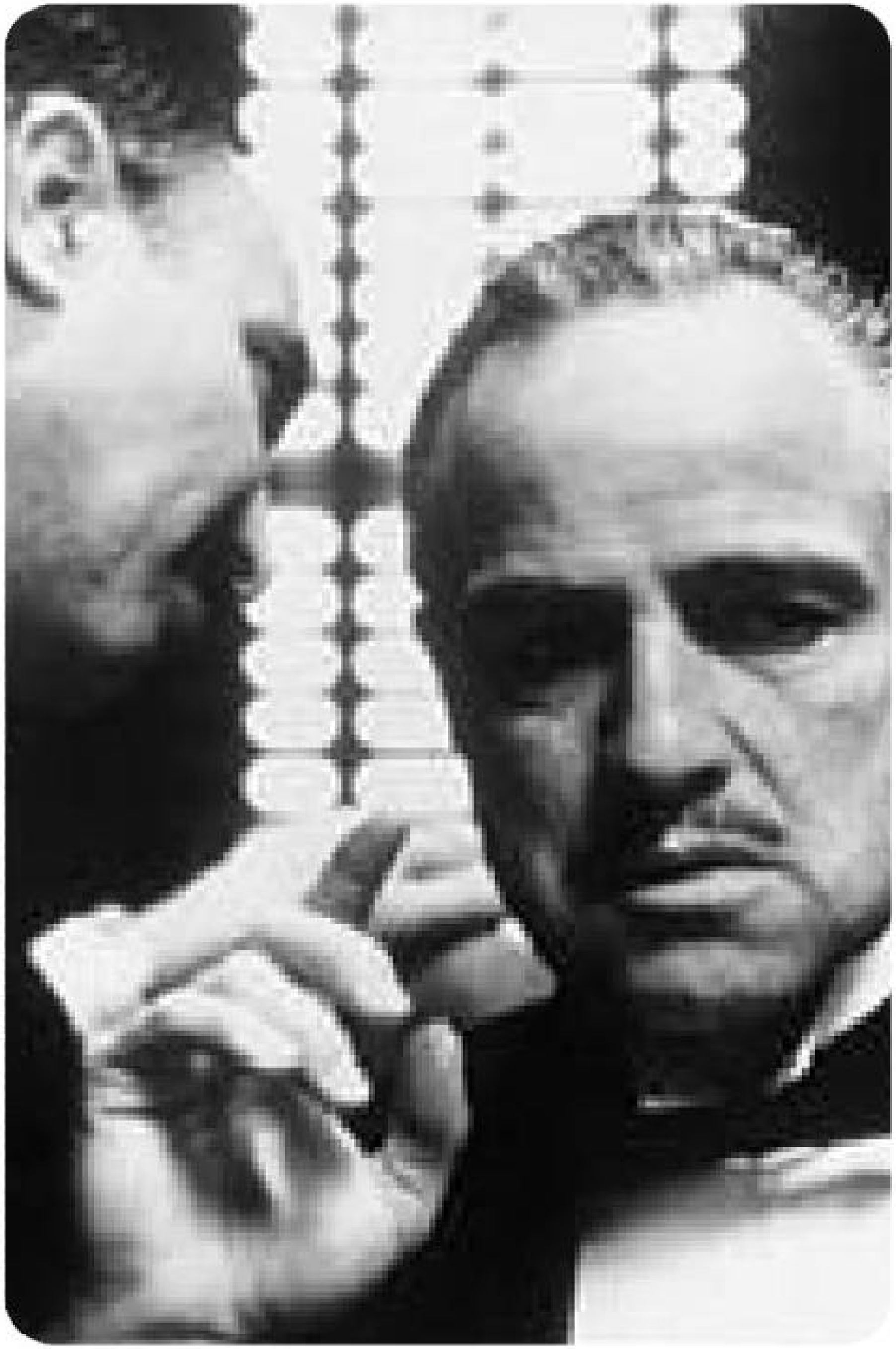
the OS will cheerfully run code that meets trivial security criteria

a favorite haunt of virus writers!

of course, the OS might not be on your system if your hard drive was stolen and installed on another system

rule of thumb: if a skilled hacker can get physical access to your system, it’s toast!

upper management hears about linux



Itanium® processor family

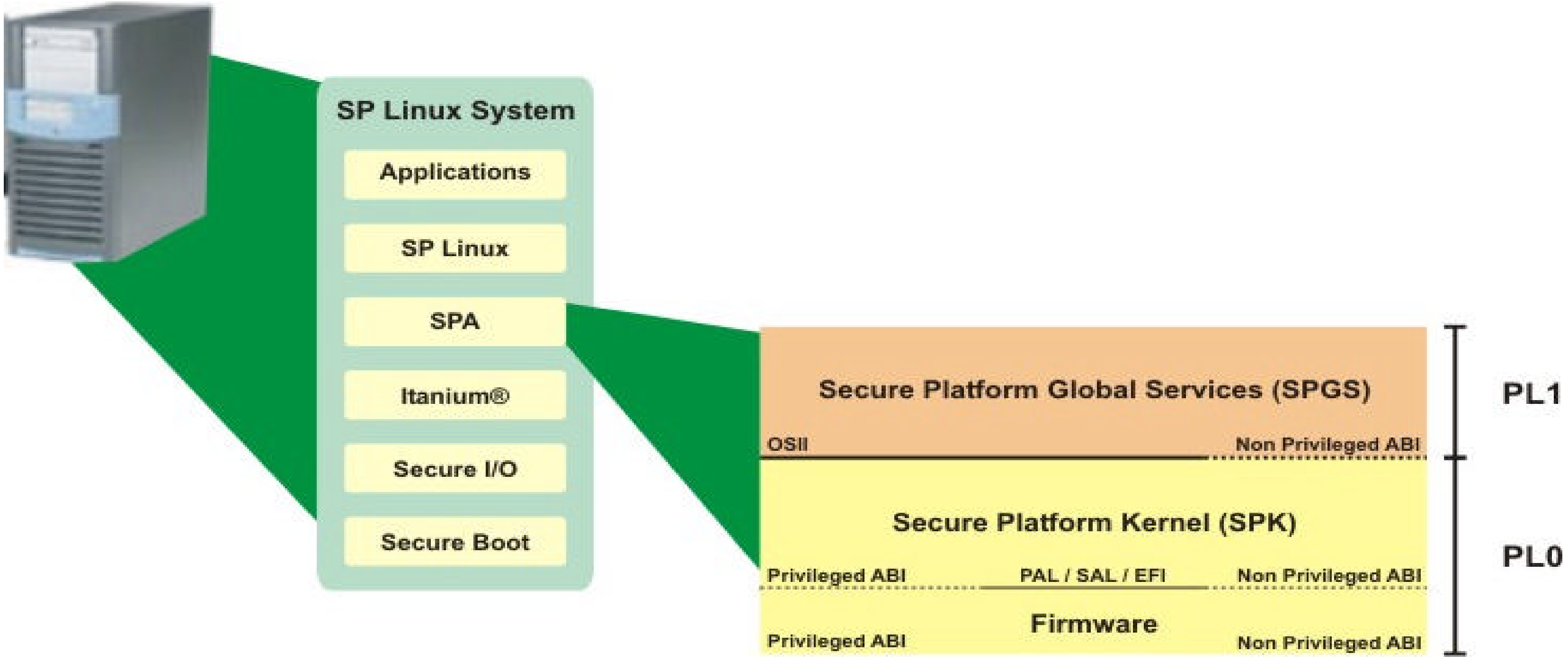
“industry standard basis for secure platform architecture”

- offers two additional levels of privilege protection
- inherent security through register stack engine
- superior performance on encryption protocols
- versatile fine-grained memory protection

secure platform architecture

“why is it different?”

- builds from designed-in security features of Itanium® architecture
  - 2 additional levels of privilege protection
  - advanced memory protection
- limits I/O access to the firmware (protects hardware)



SP Linux System

Applications

SP Linux

SPA

Itanium®

Secure I/O

Secure Boot

Secure Platform Global Services (SPGS)

OSII

Non Privileged ABI

Secure Platform Kernel (SPK)

Privileged ABI

PAL / SAL / EFI

Non Privileged ABI

Firmware

Privileged ABI

Non Privileged ABI

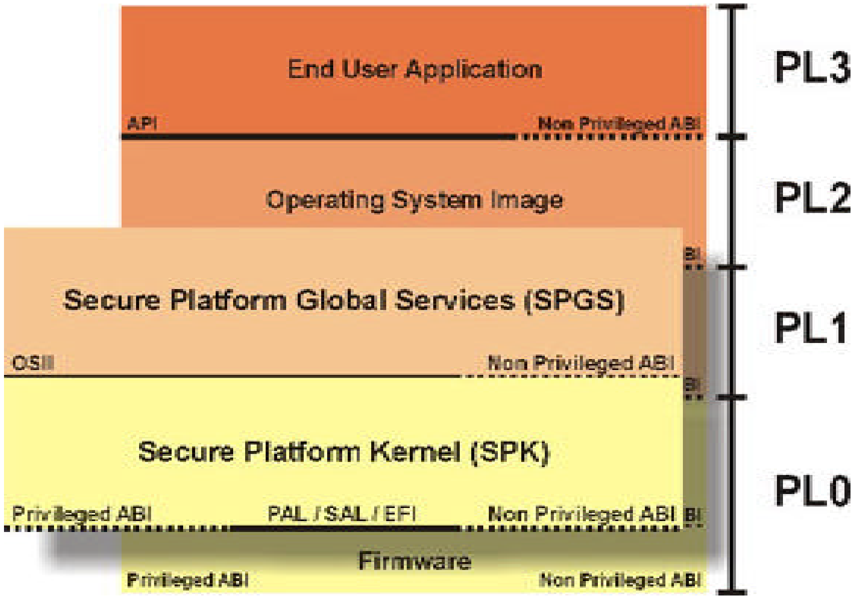
PL1

PL0

secure platform architecture

“how does it work?”

- multiple containment rings inherently limit intrusion
- operating systems and device drivers run as unprivileged tasks
- privileged operations are authenticated and performed by secure platform kernel
- code and data are protected from inadvertent and malicious execution or modification
- multiple OS images run securely on the same system



privacy

- user choice
- assurance
- embedded in corporate practices
- embedded in technology

accessibility and trust

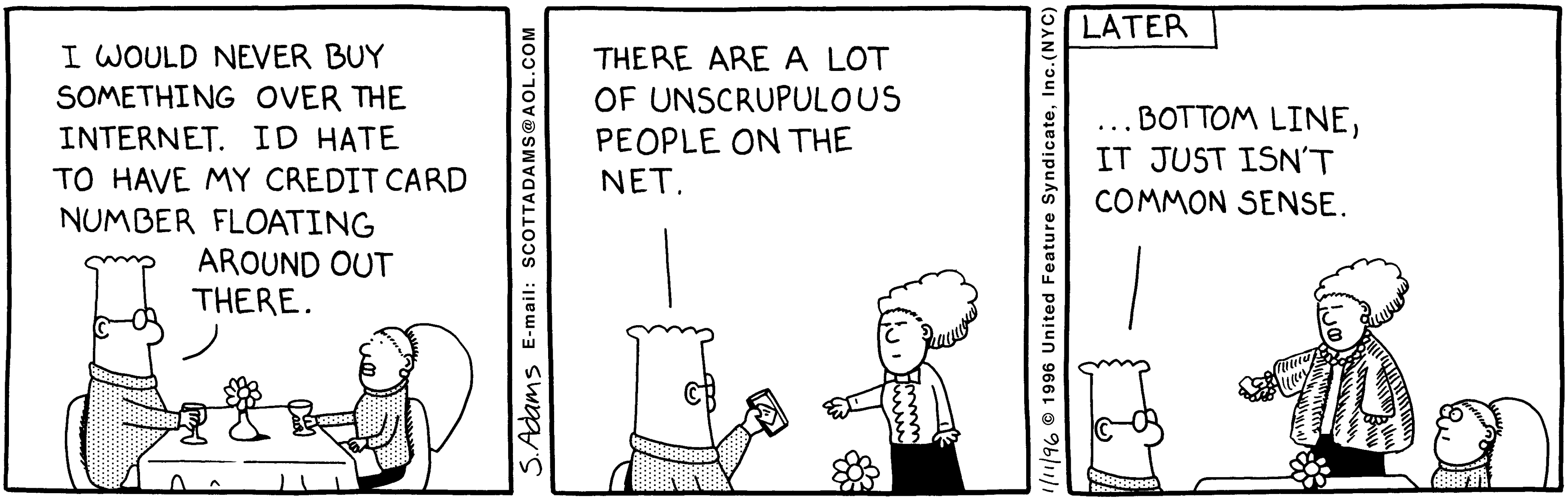
hp accessibility solutions

- trust that the web is truly accessible to all
- trust that applications enabling accessibility will remain royalty free

building out the the chain of trust

- establish the chain of trust
- rely on architecture to guarantee freedom from specified vulnerabilities/threats
- trust as a **quality-of-service**
- extend trust to
  - ipv6
  - rsvp
  - secure DNS
  - secure BGP
- leverage power of open interfaces/open source
- any golden age requires a build-out phase – trust must be an integral part, not an afterthought

the people problem


I WOULD NEVER BUY SOMETHING OVER THE INTERNET. I'D HATE TO HAVE MY CREDIT CARD NUMBER FLOATING AROUND OUT THERE.
S. Adams
E-mail: SCOTTADAMS@AOL.COM
THERE ARE A LOT OF UNSCRUPULOUS PEOPLE ON THE NET.
1/11/96 © 1996 United Feature Syndicate, Inc.(NYC)
LATER
...BOTTOM LINE, IT JUST ISN'T COMMON SENSE.

DILBERT reprinted by permission of United Feature Syndicate, Inc.

hp®

invent