DIGILE
CYBER TRUST

Global Forum 28th September 2015

Juha Röning – ACO
University of Oulu
OUSPG

c06-snmp

- Vulnerabilities found in SNMP implementations, used by most core components of the internet

❑146 vendors affected so far, each with several products, latest in 2008

❑Test suite developed in 3 months

❑Test generator developed 1999-2001

❑Public release
in 6 months
(Feb 2002)

-

Security Group Warns of Flaws in Internet Technology

February 12, 2002 03:36 PM ET

SAN FRANCISCO (Reuters) - An Internet security watchdog group Tuesday warned that a flaw in the way a popular Internet technology is used could leave corporate and university computer networks vulnerable to attack by hackers.

Cyber-Attacks by Al Qaeda Feared

Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say

By Barton Gellman
Washington Post Staff Writer
Thursday, June 27, 2002

Regarded until recently as remote, the risks of cyber-terrorism now command urgent White House attention. Discovery of one acute vulnerability -- in a data transmission standard known as ASN.1, short for Abstract Syntax Notification -- rushed government experts to the Oval Office on Feb. 7 to brief President Bush. The security flaw, according to a subsequent written assessment by the FBI, could have been exploited to bring down telephone networks and halt "all control information exchanged between ground and aircraft flight control systems."

c06-snmp

Changes in the InfoSec-Industry

Then…..
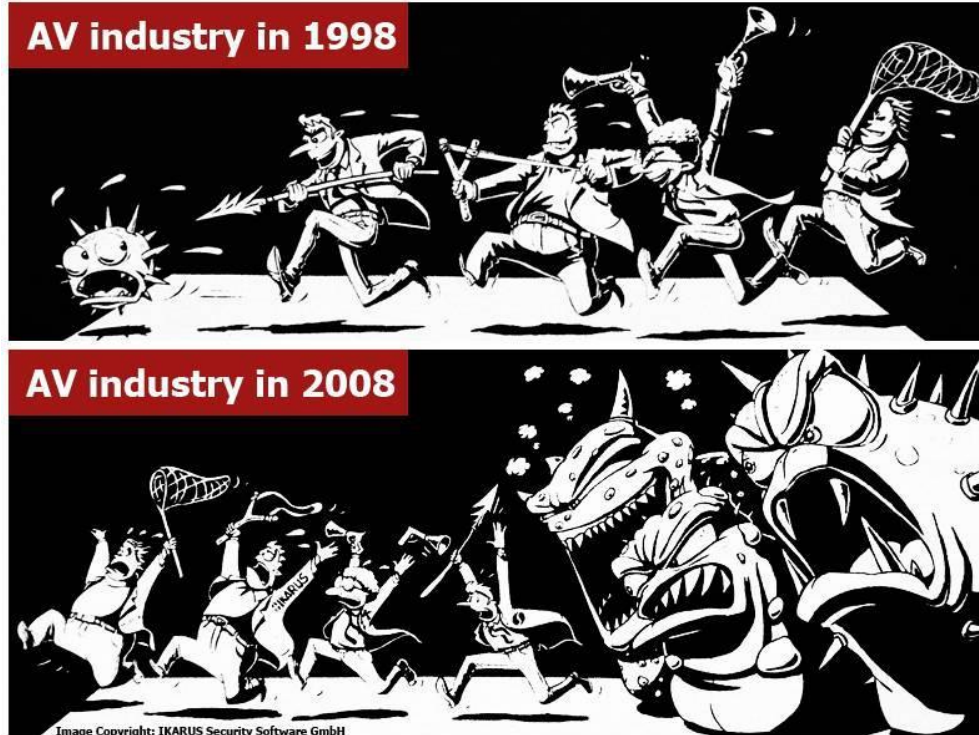
DIGILE

CYBER TRUST - Overview

➤ Cyber Trust -SHOK program is the leading research program of Cyber Security in Finland and one of the biggest in whole of Europe

➤ It utilizes industry driven Public-Private-Partnership model

➤ Program consortia includes:
   - ➤ 9 Small or Medium size companies
   - ➤ 10 Large industrial organizations
   - ➤ 9 Research institutes and universities

CYBER TRUST — Vision

Finland will be a globally recognized hub for trusted and trust enhancing digital services based on top level cyber security solutions and services actively developed and maintained in <u>international cooperation</u> by leading experts and companies.

CYBER TRUST – Breakthrough targets

Main breakthrough target is to **return privacy and trust in digital world and to gain a global competitive edge in security-related business** when we go towards 2019

Other breakthrough targets for the next 4 years are defined as follows:

➤ **Proactive – design for security**
   A new proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries

➤ **Self-healing – utilizing the toolbox**
   Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing

➤ **Changing the mindset – building the Brand**
   Enable seamless cyber security integration to every-day life. By efficiently utilizing tools and methods provided through this program, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public mindset and understanding will move towards accepting cyber security as natural element of connected world. As a result, *Finland will be recognized opinion leader in cyber domain*

➢ **Focus Area Director:**
Markku Korkiakoski, Bittium
Email: markku.korkiakoski@bittium.com
Tel: +358 40 344 5203

➢ **Academic Coordinator**
Juha Röning, Professor, University of Oulu
Email: juha.roning@oulu.fi
Tel: +358 40 518 1621

➢ **Program Coordinator**
Tapio Frantti, University of Oulu
Email: tfrantti@ee.oulu.fi
Tel: +358 40 547 0819